Evasive LWE: Attacks, Variants & Obfustopia

Shweta Agrawal* Anuja Modi† Anshu Yadav‡ Shota Yamada§

Abstract

Evasive LWE (Wee, Eurocrypt 2022 and Tsabary, Crypto 2022) is a recently introduced, popular lattice assumption which has been used to tackle long-standing problems in lattice based cryptography. In this work, we develop new counter-examples against Evasive LWE, in both the private and public-coin regime, propose counter-measures that define safety zones, and finally explore modifications to construct full compact FE/iO.

Attacks. Our attacks are summarized as follows.

- The recent work by Hseih, Lin and Luo [HLL23] constructed the first ABE for unbounded depth circuits by relying on the (public coin) "circular" evasive LWE assumption, which incorporates circularity into the Evasive LWE assumption. We provide a new attack against this assumption by exhibiting a sampler such that the pre-condition is true but post-condition is false.
- We demonstrate a counter-example against public-coin evasive LWE which exploits the freedom to choose the error distributions in the pre and post conditions. Our attack crucially relies on the error in the pre-condition being larger than the error in the post-condition.
- The recent work by Agrawal, Kumari and Yamada [AKY24a] constructed the first functional encryption scheme for pseudorandom functionalities (prFE) and extended this to obfuscation for pseudorandom functionalities (prIO) [AKY24c] by relying on private-coin evasive LWE. We provide a new attack against the stated assumption.
- The recent work by Branco et al. [BDJ+24] (concurrently to [AKY24c]) provides a construction of obfuscation for pseudorandom functionalities by relying on private-coin evasive LWE. By adapting the counter-example against [AKY24a], we provide an attack against this assumption.
- Branco et al. [BDJ+24] showed that there exist contrived, somehow "self-referential", classes of pseudorandom functionalities for which pseudorandom obfuscation cannot exist. We develop an analogous result to the setting of pseudorandom functional encryption.

While Evasive LWE was developed to specifically avoid zeroizing attacks as discussed above, our attacks show that in some (contrived) settings, the adversary may nevertheless obtain terms in the zeroizing regime.

Counter-measures: Guided by the learning distilled from the above attacks, we develop counter-measures to prevent against them. Our interpretation of the above attacks is that Evasive LWE, as defined, is too general – we suggest restrictions to identify safe zones for the assumption, using which, the broken applications can be recovered.

Variants to give full FE and iO. Finally, we show that certain modifications of Evasive LWE, which respect the counter-measures developed above, yield full compact FE in the standard model. We caution that the main goal of presenting these candidates is as goals for cryptanalysis to further our understanding of this regime of assumptions.

*IIT Madras, India, shweta@cse.iitm.ac.in
†IIT Madras, India, anujamodi97@gmail.com
‡ISTA, Austria, anshu.yadav06@gmail.com (Work initiated during a visit to IIT Madras)
§AIST Tokyo, Japan, yamada-shota@aist.go.jp

Contents

1 Introduction

A central goal in the theory of cryptography is to seek principled new assumptions to push the boundaries of feasible functionalities. One of the most action-packed research areas in this context over the last 15 years has been that of *encrypted computation*. Starting with Gentry's breakthrough work on Fully Homomorphic Encryption [Gen09], which was based on a non-standard lattice problem (which was subsequently shown to have problems, see for instance [CDPR16]), large strides have been taken in developing creative new solutions for primitives in this domain. Typically, the first candidate of a primitive is proposed from a new, non-standard assumption, subsequent to which, either (i) the construction and proof provide insights into improving the assumption until finally (often over a sequence of works), we obtain a construction from a well-understood assumption(s) or (ii) the assumption is subject to rigorous cryptanalysis, vulnerabilities are uncovered (again, often over a sequence of works) leading to either a stable assumption or, sometimes, only candidates with questionable/no security. Examples of (i) are FHE [BV11, GSW13] and iO [JLS21], examples of (ii) where a stable assumption was found are ROM [BR93, CGH04], NTRU [CS97, ABD16, PMS21, KF17] while an example where a secure candidate has not yet been found post cryptanalysis is multilinear maps [GGH13] (although the situation is mitigated somewhat by the weak multilinear map model [GMM+16a]). Along the way, we may also find applications of these assumptions, or variants thereof, to primitives other than the one originally being sought.

The present work follows direction (ii) above, by undertaking a systematic study of one of the most promising new lattice assumptions proposed in recent years – Evasive LWE [Wee22, Tsa22]. Originally proposed to give the first constructions to the long-standing problems of lattice-based broadcast encryption [Wee22] and witness encryption [Tsa22, VWW22], evasive LWE has been instrumental in making progress in several other challenging questions in lattice based cryptography, for instance [HLL23, AKY24b, WW24, WWW22a, MPV24a]. There has also been some progress in cryptanalysis by the very recent work of [BUW24].

In this work, we extend the study of Evasive LWE by developing several new counter-examples for different versions of the assumption, distill our learning into counter-measures that define safety zones, and finally, based on this new (as yet incomplete) understanding, explore modifications that allow us to interpolate the realm of evasive LWE and the realm of, the typically much more challenging, Functional Encryption (FE) and Indistinguishability Obfuscation (iO).

Functional Encryption and Friends. Functional encryption is a generalization of public key encryption where a ciphertext is associated with a vector $\mathbf{x}$, a secret key is associated with a circuit f and decryption enables recovery of $f(\mathbf{x})$ and nothing else. The related primitive of program obfuscation seeks to garble programs while preserving their input-output behaviour. Indistinguishability Obfuscation (iO) is a particular instance of obfuscation which provides the following indistinguishability-style guarantee: given two circuits C_0, C_1 such that they have the same size and compute the same function, and an obfuscation of one of them chosen at random, a bounded adversary cannot distinguish between the two cases. A line of exciting works uncovered the power of iO, showing that it can be used to instantiate almost every known cryptographic primitive [BGI+01, GGH+16, JLS21].

Another very important and much-studied primitive in the regime of encrypted computation is Attribute Based Encryption (ABE). ABE is a special case of FE that enables fine grained access control on encrypted data. In ABE, the ciphertext is associated with a public attribute $\mathbf{x}$ and a secret message m, the secret key is associated with a circuit f, and decryption succeeds to output m if and only if $f(\mathbf{x}) = 1$. Security posits that an adversary should be unable to distinguish between an encryption of $(m_0, \mathbf{x})$ and $(m_1, \mathbf{x})$, given secret keys for functions f_i so long as $f_i(\mathbf{x}) = 0$ for all i. The restriction that the adversary may only request *non-decrypting* keys makes ABE significantly easier to construct than the more general FE, where the adversary can also request keys that decrypt challenge ciphertexts (so long as the output of decryption does not reveal the challenge bit). Indeed, ABE for circuits has been known for over a decade

from the very well-understood and widely believed Learning With Errors (LWE) problem. On the other hand, FE for circuits has only been recently constructed [JLS21] and relies on multiple assumptions that must work closely together to achieve the desired goals. Notably, one of the assumptions required for FE is based on bilinear maps, which makes the construction insecure in the post-quantum regime. However, even notwithstanding the question of quantum hardness, it is believed important to explore constructions of FE from different assumptions.

Evasive LWE. The evasive LWE assumption was introduced independently by Wee [Wee22] and Tsabary [Tsa22] to interpolate assumptions underlying lattice based iO on the one hand (which are considered unstable) and solid assumptions like LWE on the other (which are very stable but afford limited power). At a very high level, the main rationale for introducing the Evasive LWE assumption was the following: all prior attacks on lattice based iO pertained to the so-called "zeroizing regime" where the adversary may obtain a large number of equations in low norm secret values over the integers, which can then be somehow solved to recover the secrets. Evasive LWE was defined to carefully sidestep the zeroizing regime in its entirety – this was done by ensuring that the attacker *only obtains large norm values* which wraparound the modulus. The hope was that this assumption would allow to make progress on some long-standing, presumably "intermediate" level hard problems such as broadcast encryption from lattices without going all the way to FE/iO. The evasive LWE assumption generated a lot of excitement in the community of lattice based cryptography since it was simple and general and enabled progress on challenging problems which had resisted progress for many years.

In more detail, the evasive LWE assumption roughly says that if

$$\left(\mathbf{B},\ \mathbf{P},\ \ \mathbf{s}^\intercal\mathbf{B}+\mathbf{e}_\mathbf{B}^\intercal,\ \ \mathbf{s}^\intercal\mathbf{P}+\mathbf{e}_\mathbf{P}^\intercal,\ \ \mathsf{aux}\ \right) \approx_c \left(\ \mathbf{B},\ \mathbf{P},\ \$,\ \ \$,\ \ \mathsf{aux}\right)$$

where $\$$ represents random, then

$$\left(\ \mathbf{B},\ \mathbf{P},\ \mathbf{s}^\intercal\mathbf{B}+\mathbf{e}_\mathbf{B}^\intercal,\ \ \mathbf{B}^{-1}(\mathbf{P}),\ \ \mathsf{aux}\right) \approx_c \left(\ \mathbf{B},\ \mathbf{P},\ \ \ \$,\ \ \mathbf{B}^{-1}(\mathbf{P}),\ \ \mathsf{aux}\right)$$

Above $\mathbf{B}^{-1}(\mathbf{P})$ refers to a low norm matrix, say $\mathbf{K}$, such that $\mathbf{BK} = \mathbf{P} \mod q$. Evidently, given $\mathbf{K} = \mathbf{B}^{-1}(\mathbf{P})$ and $\mathbf{s}^\intercal\mathbf{B}+\mathbf{e}_\mathbf{B}^\intercal$, the adversary can compute $\mathbf{s}^\intercal\mathbf{P}+\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}$. Here, the error $\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}$ is not i.i.d, unlike its counterpart $\mathbf{e}_\mathbf{P}^\intercal$ in the pre-condition. As discussed by Wee [Wee22], irregularities in the error distribution can be very dangerous for LWE security, but the hope here is that the large masking term $\mathbf{s}^\intercal\mathbf{P}$ prevents any exploitation of this correlation.

An important distinction between variants of Evasive LWE are "public-coin" and "private-coin", where the former means that the randomness used by the sampler is made available to the adversary, and the latter means that the sampler's random coins need to be hidden from the adversary. So far, counter-examples have been developed in the stronger private-coin setting but we did not know of any attacks in the public-coin setting.

1.1 Our Results

In this work, we develop new counter-examples against Evasive LWE, in both the private and public-coin regime, propose counter-measures that define safety zones, and finally explore modifications to construct full compact FE/iO.

Attacks. Our attacks are summarized as follows.

- The recent work by Hseih, Lin and Luo [HLL23] constructed the first ABE for unbounded depth circuits by relying on the (public coin) "circular" evasive LWE assumption, which incorporates circularity into the Evasive LWE assumption. We provide a new attack against this assumption by exhibiting a sampler such that the pre-condition is true but post-condition is false.

- We demonstrate a counter-example against public-coin evasive LWE which exploits the freedom to choose the error distributions in the pre and post conditions. Our attack crucially relies on the error in the pre-condition being larger than the error in the post-condition. We remark that Wee's original work [Wee22] suggested using a larger error in the post-condition for a more conservative assumption, but we are not aware of any attack that formalizes this intuition.
- The recent work by Agrawal, Kumari and Yamada [AKY24a] constructed the first functional encryption scheme for pseudorandom functionalities (prFE) and extended this to obfuscation for pseudorandom functionalities (prIO) [AKY24c] by relying on private-coin evasive LWE. We provide a new attack against this assumption by exhibiting a sampler such that the pre-condition is true but post-condition is false.
- The recent work by Branco et al. [BDJ+24] (concurrently to [AKY24c]) provides a construction of obfuscation for pseudorandom functionalities by relying on private-coin evasive LWE. By adapting the counter-example against [AKY24a], we can also attack their assumption by exhibiting a sampler such that the pre-condition is true but post-condition is false.
- Branco et al. [BDJ+24] showed that there exist contrived, somehow "self-referential", classes of pseudorandom functionalities for which pseudorandom obfuscation cannot exist. We develop an analogous result to the setting of pseudorandom functional encryption[1].

While evasive LWE was developed to specifically avoid zeroizing attacks as discussed above, our attacks show that in some (contrived) settings, the adversary may nevertheless obtain terms in the zeroizing regime.

Counter-measures: Guided by the learning distilled from the above attacks, we develop counter-measures to prevent against them. Our interpretation of the above attacks is that evasive LWE, as defined, is too general – the attacks rely on malicious samplers that exploit the structure of $\mathbf{P}$ or the error distribution to create problematic leakage. However, in the real world, the precise choices of parameters such as $\mathbf{P}$ and error distributions are made by honest parties which makes it meaningful to restrain the assumption to sidestep these barriers. We suggest restrictions to identify safe zones for the assumption, within which, we conjecture that the assumption still holds and the broken applications can be recovered.

Variants to give full FE and iO: The study of attacks and counter-measures sheds light not only on the weaknesses of evasive LWE but also on its strengths. To deepen our understanding of this regime of assumptions, we explore variants and show that certain modifications of evasive LWE (which make it "non-evasive"), that respect the counter-measures developed above, yield full compact FE in the standard model. We caution that the main goal of presenting these candidates is as goals for cryptanalysis to further our understanding of the assumption. While evidently evasive LWE is itself not on stable grounds yet, we find it interesting to study how far it is from FE/iO.

2 Technical Overview

2.1 Attacks

Attack when Pre-Condition has Larger Error. We start with describing an attack against evasive LWE in the public coin regime, since this is the simplest attack we present in this paper. Our attack works in the setting where $\|\mathbf{e}_{\mathbf{P}}\| \gg \|\mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}\|$. Intuitively, having this condition makes the assumption less

[1] Recall that while functional encryption implies obfuscation (even in the present setting [AKY24c]), this is with exponential loss.

reliable, since the post condition adversary can recover $\mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{B}^\intercal\mathbf{K}$, which is with much smaller noise than the pre-condition noise $\mathbf{e}_\mathbf{P}$. Our attack here confirms this intuition by showing that there is a concrete choice of parameters for which there is an explicit attack even in the public coin regime.

Our attack works in the setting where the modulus q is set to be $q = pr$ for prime numbers p and r. The sampler chooses random $\mathbf{D} \in [0, r-1]^{n\times\ell}$ and sets $\mathbf{P} = p\mathbf{D} \bmod q$ and $\mathsf{aux} = \mathbf{D}$. Furthermore, in this example, $\mathbf{s}$ is a short Gaussian vector. How to choose other parameters will become clear through the discussion below. We first show that the precondition holds. Even given $(\mathbf{B}, \mathbf{P}, \mathsf{aux} = \mathbf{D})$, we have

$$\begin{aligned}
(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal) &\equiv (\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{s}^\intercal(p\mathbf{D}) + \mathbf{e}_\mathbf{P}^\intercal) && (1)\\
&\approx_s (\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{s}^\intercal(p\mathbf{D}) + \mathbf{s}^\intercal\mathbf{D}' + \mathbf{e}_\mathbf{P}^\intercal) \quad \text{where } \mathbf{D}' \leftarrow [0, p-1]^{n\times\ell} && (2)\\
&\equiv (\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{s}^\intercal\mathbf{F} + \mathbf{e}_\mathbf{P}^\intercal) \quad \text{where } \mathbf{F} \leftarrow \mathbb{Z}_q^{n\times\ell} && (3)\\
&\approx_c (\mathbf{c}_\mathbf{B} \leftarrow \mathbb{Z}_q^m, \mathbf{c}_\mathbf{P} \leftarrow \mathbb{Z}_q^\ell) && (4)
\end{aligned}$$

In the above, Equation (1) follows by definition, Equation (2) by the smudging argument, where we need $\|\mathbf{e}_\mathbf{P}\| \gg \|\mathbf{s}^\intercal\mathbf{D}'\|$ so that $\mathbf{e}_\mathbf{P}^\intercal$ smudges $\mathbf{s}^\intercal\mathbf{D}'$, and Equation (3) from the fact that $p\mathbf{D} + \mathbf{D}'$ is distributed uniformly at random over $\mathbb{Z}_q^{n\times\ell}$, and Equation (4) from the LWE assumption. We then observe that the post-condition does not hold. Namely, we have to show that the following distributions are distinguishable:

$$(\mathbf{B}, \mathbf{P}, \mathbf{c}_\mathbf{B}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{K}, \mathbf{D}) \quad \text{and} \quad (\mathbf{B}, \mathbf{P}, \mathbf{c}_\mathbf{B}^\intercal \leftarrow \mathbb{Z}_q^m, \mathbf{K}, \mathbf{D}) \quad \text{where} \quad \mathbf{K} \leftarrow \mathbf{B}^{-1}(\mathbf{P}).$$

In the above, $\mathbf{B}^{-1}(\mathbf{P})$ denotes short Gaussian distribution whose output satisfies $\mathbf{BK} = \mathbf{P}$. To see this, observe

$$\mathbf{c}_\mathbf{B}^\intercal\mathbf{K} = (\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal)\mathbf{K} = p\mathbf{s}^\intercal\mathbf{D} + \mathbf{e}_\mathbf{B}^\intercal\mathbf{K} \bmod q.$$

holds when the given terms are from the LHS distribution. By taking modulo p of the above value, we get $\mathbf{e}_\mathbf{B}^\intercal\mathbf{K} \bmod p$. For the attack to work, we take p large enough so that we have $\|\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}\| < p$. This allows us to recover $\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}$ *over the integers*, which in turn allows us to recover $\mathbf{e}_\mathbf{B}^\intercal$ by solving linear equations. This completes the description of the attack. Recall that in order for the above attack to work, we need $\|\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}\| < p$ and $\|\mathbf{e}_\mathbf{P}\| \gg \|\mathbf{s}^\intercal\mathbf{D}'\|$. Since each entry of $\mathbf{D}'$ is chosen uniformly at random over $[0, p-1]$, the norm of $\mathbf{e}_\mathbf{P}$ should be much larger than p. These imply that we need $\|\mathbf{e}_\mathbf{P}\| \gg \|\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}\|$ for the attack. Please see Section 4.2.1 for more details.

Second Attack when Pre-Condition has Larger Error. One may argue that our first attack is contrived because $\mathbf{P}$ falls into the ideal generated by p in $\mathbb{Z}_q$. By modifying the sampler, we also show another example of an attack where $\mathbf{P}$ is uniformly random over $\mathbb{Z}_q^{n\times\ell}$. The counter-example works in a similar setting where $q = pr$ for prime p and r and $\mathbf{s}$ is short. In this example, the sampler chooses random $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{D} \in [0, r-1]^{n\times\ell}$, and $\mathbf{E} \in \{0,1\}^{m\times\ell}$. Then, it sets $\mathbf{P} = \mathbf{AE} + p\mathbf{D}$ and $\mathsf{aux} = (\mathbf{A}, \mathbf{D}, \mathbf{E})$. This is a public coin sampler, since there is no hidden coin that the sampler uses that is not shown to the adversary. We can see that $\mathbf{AE}$ is distributed uniformly at random by the leftover hash lemma and thus so is $\mathbf{P}$. In this example, pre-condition and post-condition adversary will be given additional term of $\mathbf{c}_\mathbf{A}$, which is either $\mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}$ or random, similarly to the original formulation of evasive LWE by Wee [Wee22]. We next show the precondition. Even given $(\mathbf{B}, \mathbf{P}, \mathsf{aux} = (\mathbf{A}, \mathbf{D}, \mathbf{E}))$, the following holds:

$$\begin{aligned}
&(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal,\ \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal)\\
\equiv\ &(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal,\ \mathbf{s}^\intercal(p\mathbf{D} + \mathbf{AE}) + \mathbf{e}_\mathbf{P}^\intercal) && (5)\\
\approx_s\ &(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal,\ \mathbf{s}^\intercal(p\mathbf{D} + \mathbf{AE}) + \mathbf{e}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{e}_\mathbf{P}^\intercal) && (6)\\
=\ &(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal,\ \mathbf{s}^\intercal(p\mathbf{D}) + \mathbf{e}_\mathbf{P}^\intercal + \mathbf{c}_\mathbf{A}^\intercal\mathbf{E})\\
\approx_s\ &(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal,\ \mathbf{s}^\intercal(p\mathbf{D}) + \mathbf{s}^\intercal\mathbf{D}' + \mathbf{e}_\mathbf{P}^\intercal + \mathbf{c}_\mathbf{A}^\intercal\mathbf{E}) \quad \text{where } \mathbf{D}' \leftarrow [0, p-1]^{n\times\ell}\\
\equiv\ &(\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal,\ \mathbf{s}^\intercal\mathbf{F} + \mathbf{e}_\mathbf{P}^\intercal + \mathbf{c}_\mathbf{A}^\intercal\mathbf{E}) \quad \text{where } \mathbf{F} \leftarrow \mathbb{Z}_q^{n\times\ell}\\
\approx_c\ &(\mathbf{c}_\mathbf{B} \leftarrow \mathbb{Z}_q^m,\ \mathbf{c}_\mathbf{A}^\intercal \leftarrow \mathbb{Z}_q^m,\ \mathbf{c}_\mathbf{P} \leftarrow \mathbb{Z}_q^\ell)
\end{aligned}$$

In the above, Equation (5) follows by definition, Equation (6) by the smudging argument, where we need $\|\mathbf{e}_\mathbf{P}^\intercal\| \gg \|\mathbf{e}_\mathbf{A}^\intercal \mathbf{E}\|$ so that $\mathbf{e}_\mathbf{P}^\intercal$ smudges $\mathbf{e}_\mathbf{A}^\intercal \mathbf{E}$. The rest of the indistinguishability follows similarly to our first counter-example. We then proceed to show that the post-condition distributions are distinguishable. Namely, we show that the following distributions are distinguishable given $(\mathbf{B}, \mathbf{P}, \mathsf{aux} = (\mathbf{A}, \mathbf{D}, \mathbf{E}))$:

$$(\mathbf{c}_\mathbf{B}^\intercal = \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal \mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal, \mathbf{K}) \quad \text{and} \quad (\mathbf{c}_\mathbf{B}^\intercal \leftarrow \mathbb{Z}_q^m, \mathbf{c}_\mathbf{A}^\intercal \leftarrow \mathbb{Z}_q^m, \mathbf{K}) \quad \text{where} \quad \mathbf{K} \leftarrow \mathbf{B}^{-1}(\mathbf{P}).$$

For the attack, the distinguisher computes $\mathbf{c}_\mathbf{B}^\intercal \mathbf{K} - \mathbf{c}_\mathbf{A}^\intercal \mathbf{E}$. If the terms come from the LHS distribution above, we have

$$\begin{aligned}\mathbf{c}_\mathbf{B}^\intercal \mathbf{K} - \mathbf{c}_\mathbf{A}^\intercal \mathbf{E} = (\mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal)\mathbf{K} - (\mathbf{s}^\intercal \mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal)\mathbf{E} = \mathbf{s}^\intercal(p\mathbf{D} + \mathbf{A}\mathbf{E}) + \mathbf{e}_\mathbf{B}^\intercal \mathbf{K} - (\mathbf{s}^\intercal \mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal)\mathbf{E} \\ = \mathbf{s}^\intercal(p\mathbf{D}) - \mathbf{e}_\mathbf{A}^\intercal \mathbf{E} + \mathbf{e}_\mathbf{B}^\intercal \mathbf{K}.\end{aligned}$$

Similarly to the case of our first attack, by taking modulo p, we can separate the error term $-\mathbf{e}_\mathbf{A}^\intercal \mathbf{E} + \mathbf{e}_\mathbf{B}^\intercal \mathbf{K}$ over the integer, if we set the parameters so that $\|-\mathbf{e}_\mathbf{A}^\intercal \mathbf{E} + \mathbf{e}_\mathbf{B}^\intercal \mathbf{K}\| < p$. By solving the linear equation, one can recover $\mathbf{e}_\mathbf{A}$ and $\mathbf{e}_\mathbf{B}$ if ℓ is sufficiently large. This allows the adversary to distinguish the above distributions. Please see Section 4.2.2 for more details.

Attack against the AKY24 Sampler. Next we describe the attack against the sampler used by [AKY24a], who propose the notion of pseudorandom functional encryption (prFE) and construct it from (certain variant of) evasive LWE. From here on unless stated otherwise, we will consider arithmetic operation on $\mathbb{Z}_q$ for a prime q. To explain their core idea, we recall a variant of the GSW FHE construction they use. In this variant, there are two types of ciphertexts. The first type of the ciphertext encrypts a binary string $\mathbf{x} \in \{0,1\}^\ell$ and is denoted by $\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{x})$, where pk_fhe is the public key of the FHE. The second type of the ciphertext encrypts a vector $\mathbf{y}$ in $\mathbb{Z}_q^L$ and is denoted by $\overline{\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{y})}$. Furthermore, the first type ciphertext $\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{x})$ can be converted into the second type ciphertext $\overline{\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(f(\mathbf{x}))}$ of $f(\mathbf{x})$ by a homomorphic computation with respect to a function $f : \{0,1\}^\ell \to \mathbb{Z}_q^{1\times L}$. For the resulting ciphertext (which is represented in a form of a matrix) and a secret key $\mathbf{s}$ corresponding to pk_fhe, we have $\mathbf{s}^\intercal \overline{\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(f(\mathbf{x}))} = \mathbf{e}_\mathsf{fhe}^\intercal + f(\mathbf{x})$, where $\mathbf{e}_\mathsf{fhe}^\intercal$ is some small noise. Note that the decryption is not able to recover lower order bits of $f(\mathbf{x})$ due to the noise, but it can still recover the higher order bit information of $f(\mathbf{x})$.

In their construction, a ciphertext $\mathsf{ct}(\mathbf{x})$ encrypting a message $\mathbf{x}$ consists of

$$\mathbf{c}_\mathbf{B}^\intercal = \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \quad \mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal(\mathbf{A} - \mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{x}) \otimes \mathbf{G}) + \mathbf{e}_\mathbf{A}^\intercal, \quad X = \mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{x}). \tag{7}$$

Notice that here, the secret key $\mathbf{s}$ for the FHE is used also as an LWE secret for other terms like $\mathbf{c}_\mathbf{B}$ and $\mathbf{c}_\mathbf{A}$. They show that one can compute a short-norm matrix $\mathbf{H}_f$ and $\mathbf{H}_{f,X}$ such that $(\mathbf{A} - \mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{x}) \otimes \mathbf{G})\mathbf{H}_{f,X} = \mathbf{A}\mathbf{H}_f - \overline{\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(f(\mathbf{x}))}$ following the idea from [BTVW17, HLL23]. This leads to the following equation:

$$\mathbf{c}_\mathbf{A}^\intercal \mathbf{H}_{f,X} = \mathbf{s}^\intercal(\mathbf{A}\mathbf{H}_f - \overline{\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(f(\mathbf{x}))}) + \mathbf{e}_\mathbf{A}^\intercal \mathbf{H}_{f,X} = \mathbf{s}^\intercal \mathbf{A}\mathbf{H}_f - \mathbf{e}_\mathsf{fhe}^\intercal - f(\mathbf{x}) + \mathbf{e}_\mathbf{A}^\intercal \mathbf{H}_{f,X}, \tag{8}$$

where the second equality follows from $\mathbf{s}^\intercal \overline{\mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(f(\mathbf{x}))} = \mathbf{e}_\mathsf{fhe}^\intercal + f(\mathbf{x})$. A secret sk_f for a function f consists of $\mathbf{K} \leftarrow \mathbf{B}^{-1}(\mathbf{A}\mathbf{H}_f)$. Given the secret key, one can decrypt the ciphertext by computing

$$\mathbf{c}_\mathbf{B}^\intercal \mathbf{K} - \mathbf{c}_\mathbf{A}^\intercal \mathbf{H}_{f,X} = \mathbf{s}^\intercal \mathbf{B}\mathbf{K} + \mathbf{e}_\mathbf{B}^\intercal \mathbf{K} - (\mathbf{s}^\intercal \mathbf{A}\mathbf{H}_f - \mathbf{e}_\mathsf{fhe}^\intercal - f(\mathbf{x}) + \mathbf{e}_\mathbf{A}^\intercal \mathbf{H}_{f,X}) = f(\mathbf{x}) + \underbrace{\mathbf{e}_\mathbf{B}^\intercal \mathbf{K} + \mathbf{e}_\mathsf{fhe}^\intercal - \mathbf{e}_\mathbf{A}^\intercal \mathbf{H}_{f,X}}_{\text{small error}}. \tag{9}$$

Similarly to the case of the FHE decryption, we can recover higher order bits of $f(\mathbf{x})$ by removing the error terms.

We outline the security proof of their construction, since it is relevant to us. For simplicity, we restrict to the case of single ciphertext and single secret key. The security of prFE stipulates that if $f(\mathbf{x})$ looks pseudorandom, then so is the ciphertext $\mathsf{ct}(\mathbf{x})$ even given $\mathsf{sk} = \mathbf{K}$. To show this, they invoke the evasive LWE assumption with respect to $\mathbf{P} = \mathbf{A}\mathbf{H}_f$. The assumption implies that for proving the security, it suffices to show the precondition, namely, pseudorandomness of $\mathbf{c}_\mathbf{B}^\intercal$, $\mathbf{c}_\mathbf{A}^\intercal$, X, and $\mathbf{c}_\mathbf{P}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal$, where $\mathbf{e}_\mathbf{P}^\intercal$ is a fresh Gaussian noise. This is proven by the following hybrids.

Hyb_0. In this hybrid, the adversary is given $\mathbf{c}_\mathbf{B}^\intercal$, $\mathbf{c}_\mathbf{A}^\intercal$, $X = \mathsf{E}_{\mathsf{pk}_\mathsf{fhe}}(\mathbf{x})$, and $\mathbf{c}_\mathbf{P}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal$.

Hyb_1. In this hybrid, we change how $\mathbf{c}_\mathbf{P}$ is computed. Here, we compute $\mathbf{c}_\mathbf{P}$ as $\mathbf{c}_\mathbf{P}^\intercal = \mathbf{c}_\mathbf{A}^\intercal\mathbf{H}_{f,X} + f(\mathbf{x}) + \mathbf{e}_\mathbf{P}^\intercal$. By Equation (8), we have $\mathbf{c}_\mathbf{A}^\intercal\mathbf{H}_{f,X} + f(\mathbf{x}) + \mathbf{e}_\mathbf{P}^\intercal = \mathbf{s}^\intercal\mathbf{P} - \mathbf{e}_\mathsf{fhe}^\intercal + \mathbf{e}_\mathbf{A}^\intercal\mathbf{H}_{f,X} + \mathbf{e}_\mathbf{P}^\intercal$. Therefore, the difference from the previous hybrid is in the error term. Since we take $\mathbf{e}_\mathbf{P}^\intercal$ large enough so that it smudges the small error term $-\mathbf{e}_\mathsf{fhe}^\intercal + \mathbf{e}_\mathbf{A}^\intercal\mathbf{H}_{f,X}$, this hybrid is statistically close to the previous hybrid.

Hyb_2. In this hybrid, we change $\mathbf{c}_\mathbf{B}^\intercal$, $\mathbf{c}_\mathbf{A}^\intercal$, and pk_fhe to be random by using the LWE assumption. Note that the public key pk_fhe of GSW is actually an LWE sample with respect to the secret key $\mathbf{s}$ and thus this is possible. This hybrid is indistinguishable from the previous one by the LWE assumption.

Hyb_3. In this hybrid, we change X to be a random string. The GSW encryption is essentially the same as Regev encryption [Reg09] and a random key is lossy [PW11]. Namely, the encryption under a random key is a random string. Therefore, this hybrid is statistically indistinguishable from the previous one.

Hyb_4. In this game, we change $\mathbf{c}_\mathbf{P}$ to be a random string. This follows from the pseudorandomness of $f(\mathbf{x})$, which can be invoked since the information of $\mathbf{x}$ is not used anywhere else in the previous hybrid.

We are ready to describe our counter-example. The sampler in our counter-example outputs prFE ciphertexts of AKY encrypting random secret $\mathbf{x}$ and $\mathbf{P}$ is computed so that $\mathbf{K} = \mathbf{B}^{-1}(\mathbf{P})$ constitutes a secret key for function f defined above. Namely, we set $\mathbf{P} = \mathbf{A}\mathbf{H}_f$. For the homomorphic evaluation of the circuit f, we need some contrived implementation, which we will discuss later. We show that the pre-condition distributions are indistinguishable, yet the post-condition distributions are distinguishable. The precondition with respect to this sampler essentially requires that $\mathbf{c}_\mathbf{B}, \mathbf{c}_\mathbf{A}$ defined as in Equation (7) along with $\mathbf{c}_\mathbf{P}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal$ is pseudorandom. This is exactly what we showed in the above discussion.

We now provide the description of the distinguisher for the post-condition. We note that the description here is oversimplified but conveys the main intuition. The distinguisher is given $\mathbf{c}_\mathbf{B}$, $\mathbf{c}_\mathbf{A}$, X, and $\mathbf{K}$ and tries to check whether $\mathbf{c}_\mathbf{B}$, $\mathbf{c}_\mathbf{A}$, and X are structured as in Equation (7) or random. The distinguisher first computes $\mathbf{v} = \mathbf{c}_\mathbf{B}^\intercal\mathbf{K} - \mathbf{c}_\mathbf{A}^\intercal\mathbf{H}_{f,X} \bmod q$. We need special contrived circuit implementation of f for the attack to work, which will be explained soon. The distinguisher interprets $\mathbf{v}$ as a vector in $[-(q-1)/2, (q-1)/2]^L$ by regarding the $\mathbb{Z}_q$ element as an integer in $[-(q-1)/2, (q-1)/2]$. By Equation (9), if the terms are structured, we have $\mathbf{v} = f(\mathbf{x}) + \mathbf{e}_\mathbf{B}^\intercal\mathbf{K} + \mathbf{e}_\mathsf{fhe}^\intercal - \mathbf{e}_\mathbf{A}^\intercal\mathbf{H}_{f,X}$. Our first observation is that when $f(\mathbf{x}) \in \mathbb{Z}_q^L$ is pseudorandom, each entry of $f(\mathbf{x})$ is unlikely to fall into $[-(q-1)/2, -(q-1)/2 + B] \cup [(q-1)/2 - B, (q-1)/2]$ for small B when it is represented as a vector in $[-(q-1)/2, (q-1)/2]^L$, where B is set so that we have $\left\|\mathbf{e}_\mathbf{B}^\intercal\mathbf{K} + \mathbf{e}_\mathsf{fhe}^\intercal - \mathbf{e}_\mathbf{A}^\intercal\mathbf{H}_{f,X}\right\| < B$. Therefore, wraparound does not occur with overwhelming probability in the computation of $f(\mathbf{x}) + (\mathbf{e}_\mathbf{B}^\intercal\mathbf{K} + \mathbf{e}_\mathsf{fhe}^\intercal - \mathbf{e}_\mathbf{A}^\intercal\mathbf{H}_{f,X}) \bmod q$ and we are able to recover $f(\mathbf{x}) + \mathbf{e}_\mathbf{B}^\intercal\mathbf{K} + \mathbf{e}_\mathsf{fhe}^\intercal - \mathbf{e}_\mathbf{A}^\intercal\mathbf{H}_{f,X}$ *over the integers*, by representing $\mathbf{v}$ as a vector in $[-(q-1)/2, (q-1)/2]^L$. If we were able to separate $f(\mathbf{x})$ from the error terms as is done in our first counter-example, the attack would have been very simple. However, this is impossible since lower-order bits of $f(\mathbf{x})$ are also pseudorandom and mask the error terms.

To overcome this issue, we borrow the idea from [HJL21] to correlate the least significant bit of $f(\mathbf{x})$ with $\mathbf{e}_{\mathsf{fhe}}^\intercal$. Namely, we show that we can make $f(\mathbf{x}) \equiv \mathbf{e}_{\mathsf{fhe}}^\intercal \bmod 2$ if we choose a contrived circuit implementation for the homomorphic computation of f. They induce such a correlation in the setting of dual GSW FHE, while here, we show that similar correlation can also be constructed for the variant of GSW that AKY use. Therefore, by taking $\mathbf{v} \bmod 2$, we get $\mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K} - \mathbf{e}_{\mathbf{A}}^\intercal \mathbf{H}_{f,X} \bmod 2$, since $f(\mathbf{x})$ and $\mathbf{e}_{\mathsf{fhe}}^\intercal$ cancel each other modulo 2. Then, the attacker tries to find $\bar{\mathbf{e}}_{\mathbf{A}}$ and $\bar{\mathbf{e}}_{\mathbf{B}}$ such that $\bar{\mathbf{e}}_{\mathbf{B}}^\intercal \mathbf{K} - \bar{\mathbf{e}}_{\mathbf{A}}^\intercal \mathbf{H}_{f,X} = \mathbf{v} \bmod 2$. If such $\bar{\mathbf{e}}_{\mathbf{A}}$ and $\bar{\mathbf{e}}_{\mathbf{B}}$ are found, it guesses that the given terms are structured and otherwise if not. From the above description, in the structured case, such vectors can be always found since $\bar{\mathbf{e}}_{\mathbf{B}} = \mathbf{e}_{\mathbf{B}}$ and $\bar{\mathbf{e}}_{\mathbf{A}} = \mathbf{e}_{\mathbf{A}}$ constitute a solution. We can also show that in the case when the given terms are random, then such vectors cannot be found with overwhelming probability if we take L to be sufficiently large. Therefore, this constitutes a valid attack. Please see Section 5.1 for more details.

Attack against the HLL23 Sampler. Here, we provide a counter-example against the evasive circular LWE assumption introduced in [HLL23]. Their assumption is similar to that of AKY, but with the crucial difference that there is no additional secret $\mathbf{x}$[2]. Instead of the encryption X of $\mathbf{x}$, the encryption S of $\mathbf{s}$ is included in the pre- and post-condition distributions. Note that S is a circular ciphertext, since $\mathbf{s}$ is a secret key corresponding to $\mathsf{pk}_{\mathsf{fhe}}$. Namely, the evasive circular LWE assumption says that if

$$\mathbf{c}_{\mathbf{B}}^\intercal = \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal, \quad \mathbf{c}_{\mathbf{A}}^\intercal = \mathbf{s}^\intercal (\mathbf{A} - S \otimes \mathbf{G}) + \mathbf{e}_{\mathbf{A}}^\intercal, \quad S = \mathsf{E}_{\mathsf{pk}_{\mathsf{fhe}}}(\mathbf{s}), \quad \mathbf{c}_{\mathbf{P}}^\intercal = \mathbf{s}^\intercal \mathbf{P} + \mathbf{e}_{\mathbf{P}}$$

are pseudorandom, then so are $\mathbf{c}_{\mathbf{B}}^\intercal$, $\mathbf{c}_{\mathbf{A}}^\intercal$, and S even given $\mathbf{K} = \mathbf{B}^{-1}(\mathbf{P})$. In our counter-example here, we regard $(\mathbf{c}_{\mathbf{B}}, \mathbf{c}_{\mathbf{A}}, S)$ as an AKY ciphertext encrypting $\mathbf{s}$ and set $\mathbf{P}$ so that $\mathbf{K}$ constitutes a secret key for a function f. We defer the discussion on how to instantiate f to later. The attack against the post-condition is essentially the same as that for AKY, where the only difference is that $\mathbf{x}$ is replaced with $\mathbf{s}$.

We now argue that the pre-condition holds, which requires some more work. For the precondition to hold, we need a stronger property than just requiring $f(\mathbf{s})$ to be pseudorandom. This is because $\mathbf{s}$ is used also for the computation of other terms, for example in $\mathbf{c}_{\mathbf{A}}$ and S, unlike $\mathbf{x}$ in the case of AKY, where $\mathbf{x}$ is a separate randomness chosen independently from other terms. Hence, we need that $(\mathbf{c}_{\mathbf{B}}, \mathbf{c}_{\mathbf{A}}, S, \mathsf{pk}_{\mathsf{fhe}}, f(\mathbf{s}))$ is *jointly* pseudorandom. Assuming we have such f, the precondition is proven by the following hybrids. The main difference from the AKY counter-example is that here, we collapse Hyb_2, Hyb_3, and Hyb_4 there into a single hybrid using the property of f.

Hyb_0**.** In this hybrid, the adversary is given $\mathbf{c}_{\mathbf{B}}^\intercal$, $\mathbf{c}_{\mathbf{A}}^\intercal$, $S = \mathsf{E}_{\mathsf{pk}_{\mathsf{fhe}}}(\mathbf{s})$, and $\mathbf{c}_{\mathbf{P}}^\intercal = \mathbf{s}^\intercal \mathbf{P} + \mathbf{e}_{\mathbf{P}}^\intercal$.

Hyb_1**.** In this hybrid, we change how $\mathbf{c}_{\mathbf{P}}$ is computed. Here, we compute $\mathbf{c}_{\mathbf{P}}$ as $\mathbf{c}_{\mathbf{P}}^\intercal = \mathbf{c}_{\mathbf{A}}^\intercal \mathbf{H}_{f,S} + f(\mathbf{s}) + \mathbf{e}_{\mathbf{P}}^\intercal$. By Equation (8) (where $\mathbf{x}$ is replaced with $\mathbf{s}$ and X with S), we have $\mathbf{c}_{\mathbf{A}}^\intercal \mathbf{H}_{f,S} + f(\mathbf{s}) + \mathbf{e}_{\mathbf{P}}^\intercal = \mathbf{s}^\intercal \mathbf{P} - \mathbf{e}_{\mathsf{fhe}}^\intercal + \mathbf{e}_{\mathbf{A}}^\intercal \mathbf{H}_{f,S} + \mathbf{e}_{\mathbf{P}}^\intercal$. Therefore, the difference from the previous hybrid is in the error term. Since we take $\mathbf{e}_{\mathbf{P}}^\intercal$ large enough so that it smudges the small error term $-\mathbf{e}_{\mathsf{fhe}}^\intercal + \mathbf{e}_{\mathbf{A}}^\intercal \mathbf{H}_{f,X}$, this hybrid is statistically close to the previous hybrid.

Hyb_2**.** In this hybrid, we change $\mathbf{c}_{\mathbf{B}}^\intercal$, $\mathbf{c}_{\mathbf{A}}^\intercal$, $\mathsf{pk}_{\mathsf{fhe}}$, S, $\mathbf{c}_{\mathbf{P}}$ to be random. This follows by the joint pseudorandomness property of f, by observing that $\mathbf{c}_{\mathbf{P}}$ is obtained by adding $f(\mathbf{s})$ to a known term.

To finish the description of the counter-example, it remains to find the implementation of such f. Simply treating $\mathbf{s}$ as a random seed for general PRG will not work, since there is a leakage of $\mathbf{s}$ in the form of LWE samples with respect to the secret $\mathbf{s}$. In this setting, we do not know how to prove the joint pseudorandomness that we require. A more promising approach is to make f randomized and define $f(\mathbf{s})$ to be an LWE instance with respect to some public matrix $\mathbf{F}$, which describes the function f. If f is allowed to be randomized, this works since $(f(\mathbf{s}), \mathbf{c}_{\mathbf{B}}, \mathbf{c}_{\mathbf{A}}, \mathsf{pk}_{\mathsf{fhe}}, S)$ forms LWE samples along with

[2]We observe that this difference stems from the difference between ABE in FE – in the former, $\mathbf{x}$ can be public and therefore HLL does not need to hide it. OTOH, AKY constructs an FE and hence does need to hide it.

circular encoding and thus the pseudorandomness of them follows from the circular LWE assumption. However, since f is deterministic, this approach does not work.

Our solution is to define $f(\mathbf{s})$ to be learning with rounding instance [BPR12] with respect to the public matrix $\mathbf{F}$ and secret $\mathbf{s}$. Namely, we define $f(\mathbf{s}) = \lceil (p/q)\mathbf{s}^\intercal \mathbf{F} \rceil$. The joint pseudorandomness is proven by first arguing that $\lceil (p/q)\mathbf{s}^\intercal \mathbf{F} \rceil = \lceil (p/q)(\mathbf{s}^\intercal \mathbf{F} + \mathbf{e}) \rceil$ holds with high probability for small noise $\mathbf{e}$. Then, we replace $\mathbf{s}^\intercal \mathbf{F} + \mathbf{e}$ along with other LWE terms and the circular encoding $\mathbf{S}$ with random values using the circular LWE assumption. This completes the proof, since $\lceil (p/q)\mathbf{v} \rceil$ for random vector $\mathbf{v}$ will result in a random string in $\mathbb{Z}_p$ for appropriately chosen p and q. Please see Section 4.1 for more details.

Attack against the BDJMMPV24 Sampler. Next, we show a counter-example for the sampler used in [BDJ+24]. For the sake of explanation, we describe a simplified version of their sampler in this overview. However, the attack applies to the full-fledged version as well. They construct a primitive they call pseudorandom obfuscation (PRO) and prove the security of the construction using evasive LWE. Roughly speaking, this primitive allows us to obfuscate a PRF. Here, we consider a function f which takes as input a key $\mathbf{x}$ of the PRF and outputs the truth table of the PRF under the key $\mathbf{x}$. We assume that the truth table of the PRF is represented as an element of $\mathbb{Z}_q^{k \times \kappa}$. In our context, we set k and κ to be some huge polynomials and thus the input space of the PRF is of polynomial size. For the primitive to be non-trivial, we want the size of the obfuscation to be much smaller than the size of the truth table (i.e., $O(k\kappa \log q)$). The security of PRO says that if the truth table $f(\mathbf{x}) \in \mathbb{Z}_q^{k \times \kappa}$ is pseudorandom, then so is the description of the obfuscation.

To describe their sampler, we follow their notation that is different from AKY and HLL, where $\mathbf{B}$ is a tall matrix of size $m \times n$ and the LWE sample with respect to it will be $\mathbf{C} = \mathbf{BS} + \mathbf{E}$, where $\mathbf{S} \in \mathbb{Z}_q^{n \times \kappa}$ is an LWE secret and $\mathbf{E}$ is a noise term. Furthermore, we follow their syntax where the sampler does not choose $\mathbf{P} \in \mathbb{Z}_q^{k \times n}$ by itself. Instead, $\mathbf{P}$ is chosen uniformly at random outside of the control by the sampler. The sampler takes as input $\mathbf{P}$, chooses $\mathbf{S}$ by itself, and computes auxiliary information aux depending on $\mathbf{P}$ and $\mathbf{S}$, where aux is defined as follows:

$$\mathsf{aux} = \left(\mathbf{A} = \mathbf{PR} + \overline{\mathbf{E}} + \mathsf{encode}(\mathbf{s}), \quad X = \mathsf{E}_{\mathsf{pk}_{\mathsf{fhe}}}(\mathbf{x}), \quad \mathbf{H} = \mathbf{S} + \mathbf{RF}\right).$$

In the above, $\mathbf{x}$ is a secret value, $\mathbf{R}$ is a random matrix, $\overline{\mathbf{E}}$ is a matrix with low norm, and encode is an encoding function with certain property that we will specify soon. The matrix $\mathbf{F}$ is a low norm matrix that is computed by first evaluating the FHE ciphertext X with respect to the function f to obtain $\overline{\mathsf{E}_{\mathsf{pk}_{\mathsf{fhe}}}(f(\mathbf{x}))}$ and then processing it so that

$$\mathsf{encode}(\mathbf{s})\mathbf{F} = f(\mathbf{x}) + \mathbf{E}_{\mathsf{fhe}}$$

holds for low norm $\mathbf{E}_{\mathsf{fhe}}$. They show that the pre-condition holds for a slight modification of the above sampler. We omit the details here.

We proceed to explain the distinguishing attack against the post-condition distribution. Namely, we show that given $\mathbf{D}$ such that $\mathbf{DB} = \mathbf{P}$ and aux, the following distribution is not pseudorandom

$$(\ \mathbf{B},\ \mathbf{P},\ \mathbf{C} = \mathbf{BS} + \mathbf{E},\ \mathsf{aux}\ ).$$

Before giving an attack, we first observe the following equation:

$$\begin{aligned}\mathbf{AF} + \mathbf{DC} - \mathbf{PH} &= (\mathbf{PR} + \overline{\mathbf{E}} + \mathsf{encode}(\mathbf{s}))\mathbf{F} + \mathbf{D}(\mathbf{BS} + \mathbf{E}) - \mathbf{P}(\mathbf{S} + \mathbf{RF}) \\ &= \underbrace{\overline{\mathbf{E}}\mathbf{F} + \mathbf{DE} + \mathbf{E}_{\mathsf{fhe}}}_{\text{small error}} + f(\mathbf{x}).\end{aligned}$$

One can see that the noisy version of the truth table $f(\mathbf{x})$ is obtained by the above computation. Roughly speaking, their obfuscation consists of $(\mathbf{A}, \mathbf{C}, \mathbf{D}, \mathbf{F}, \mathbf{H}, \mathbf{P})$ and the size of it is much smaller than that of

the truth table itself. This is an approximate version of PRO in the sense that the lower-order bits cannot be recovered. However, by embedding the information that we want to recover into the higher-order bits, it can be made precise.

The distinguishing strategy is again similar to those for AKY and HLL, which uses contrived circuit for the homomorphic computation to make a correlation between the encrypted value and the noise appearing when we decrypt. Namely, we create a correlation such that $f(\mathbf{x}) \equiv \mathbf{E}_{\mathsf{fhe}} \bmod 2$ by a contrived homomorphic operation for the underlying GSW FHE. If given terms are structured, we can recover $\overline{\mathbf{E}}\mathbf{F} + \mathbf{D}\mathbf{E} + \mathbf{E}_{\mathsf{fhe}} + f(\mathbf{x})$ over the integer by computing $\mathbf{A}\mathbf{F} + \mathbf{D}\mathbf{C} - \mathbf{P}\mathbf{H}$ and representing it as a matrix in $[-\lfloor q/2 \rfloor, \lfloor q/2 \rfloor]^{k \times \kappa}$, similarly to the case of AKY and HLL. We then take modulus 2 for the resulting term, which gives us $\overline{\mathbf{E}}\mathbf{F} + \mathbf{D}\mathbf{E} \bmod 2$. Since $\mathbf{F}$ and $\mathbf{D}$ are public, we can recover $\overline{\mathbf{E}}$ and $\mathbf{E}$ by solving the linear system of equations. On the other hand, if the given terms are random, we can show that the linear system of equations cannot be solved with high probability. This constitutes a valid distinguishing attack. Please see Section 5.2 for more details.

Interpreting the Attacks. With the development of new attacks, the most pressing question that arises is – are applications built from evasive LWE dead? Indeed, our work shows that in certain settings, even public-coin versions of evasive LWE can be subject to attack. Does this mean we lose our only candidates for lattice based broadcast encryption [Wee22], witness encryption [VWW22, Tsa22], ABE for unbounded depth circuits [HLL23], ABE for Turing machines [AKY24b], multi-input ABE [ARYY23] and such other painstakingly earned results, none of which are known outside Obfustopia?

To address this question, let us take a step back try to understand the high level learning obtained from these attacks. Towards this, let us revisit the primary intuition of evasive LWE as formulated by Wee. One way to interpret the original formulation of Wee's evasive LWE is that it is really two assumptions rolled into one[3]:

1. **Preimages $\mathbf{B}^{-1}(\mathbf{P})$ can only be used semi-honestly**: Short Gaussian preimages $\mathbf{K} = \mathbf{B}^{-1}(\mathbf{P})$ can only be used semi-honestly to compute samples $\mathbf{s}\mathbf{P} + \mathbf{e}\mathbf{K}$ from $\mathbf{s}\mathbf{B} + \mathbf{e}$ and cannot be exploited in any other way. Here, note that this condition implicitly demands that $\mathbf{P}$ is sufficiently "well-behaved", and in particular does not contain low norm linear dependencies that would permit "mix and match" attacks of preimages [Agr17][4].

2. **LWE with correlated error is "no worse" than standard LWE**: By using $\mathbf{B}^{-1}(\mathbf{P})$ as above, the adversary can compute an LWE sample $\mathbf{s}\mathbf{P} + \mathbf{e}\mathbf{K}$ with correlated, overdefined error as against i.i.d. error. However, the intuition here is that this LWE with correlated noise can be conjectured "as good as" LWE since the attacker should never be able to remove the large mask $\mathbf{s}\mathbf{P}$ and therefore should never obtain anything in the zeroizing regime.

We now study the two assumptions above in turn, as though they are separate. We observe that the first assumption above has so far appeared sound – we do not know even a single attack that exploits $\mathbf{K}$ to compute anything other than $\mathbf{s}\mathbf{P} + \mathbf{e}\mathbf{K}$, which is explicitly desired. All the problems come from the second assumption, where an i.i.d error would have sufficed for some flooding argument (allowing the pre-condition to be proven), but the correlated, overdefined error does not. Here, we observe that all our attacks are oblivious to how $\mathbf{s}\mathbf{P} + \mathbf{e}\mathbf{K}$ was constructed, and rely only on exploiting the correlated error. So perhaps if we refine the second assumption to prevent vulnerabilities, we can hope to regain security.

In our judgment, a rigorous approach towards buttressing the second assumption is to enforce explicit checks to ensure that the intuition that "LWE with correlated noise is secure" can be made to function

[3]These cannot be separated in general, needless to say.

[4]As an extreme example of badly behaved $\mathbf{P} = [\mathbf{P}_1, \mathbf{P}_2]$, suppose the adversary could obtain $\mathbf{K}_1$, $\mathbf{K}_2$ such that $\mathbf{B}\mathbf{K}_1 = \mathbf{P}_1 \bmod q$ and $\mathbf{B}\mathbf{K}_2 = 2\mathbf{P}_1 \bmod q$. Then, the adversary could compute a short trapdoor to $\mathbf{B}$ simply as $2\mathbf{K}_1 - \mathbf{K}_2$, which is clearly disastrous. However, such "pre-image combination" attacks are prevented by the requirement in the pre-condition, that $\underline{\mathbf{s}\mathbf{P}_1}$, $\underline{\mathbf{s}\mathbf{P}_2}$ are jointly pseudorandom.

for the settings *required by the desired applications*. We use the above understanding to guide our development of counter-measures – we suggest safeguards to ensure that $\mathbf{sP} + \mathbf{eK}$, given other information, can indeed be safely replaced by $\mathbf{sP} + \mathbf{e}_{\mathsf{iid}}$, where $\mathbf{e}_{\mathsf{iid}}$ is fresh i.i.d error, in the application of evasive LWE. Below, we summarize counter-measures guided by attacks, using which we believe that the original intuition by Wee [Wee22] and Tsabary [Tsa22] can be recovered, so that the loss of the aforementioned applications can be prevented.

Going forward, we hope that progress on understanding evasive LWE will lead to formulation of simpler, safer assumptions that can be used to build the desired applications. We are optimistic that the new constructions and new attacks will bring us closer to realizing advanced encrypted computation from lattices from assumptions that satisfy all the desired desiderata – simplicity, instance-independence, falsifiability, ease of cryptanalysis and good (at least better) performance in the "test of time"!

2.2 Counter-Measures

We begin by categorizing known attacks.

Attacks by withholding information about B or P: The work of [BUW24] presents attacks against classes of evasive LWE where either $\mathbf{B}$ or $\mathbf{P}$ are not known to the adversary. In more detail, consider the distinguisher of the pre-condition who receives the matrix $\mathbf{B}$, but not $\mathbf{P}$ – in this case, the distinguisher of the post-condition can easily recover $\mathbf{P}$ by simply computing $\mathbf{B} \cdot \mathbf{B}^{-1}(\mathbf{P})$. This may create leakage in scenarios where $\mathbf{P}$ contains secret information that was deliberately withheld from the adversary. The case where $\mathbf{B}$ is not available to the distinguisher of the pre-condition but $\mathbf{P}$ is partially available is similar. These attacks can be prevented by ensuring that the distinguisher in the pre-condition also has access to complete information about $\mathbf{B}$ and $\mathbf{P}$. The authors define "Private-coin Binding Evasive LWE" to capture the setting where Samp is private-coin, and $\mathbf{B}, \mathbf{P}$ are explicitly included in the joint distributions, and conjecture this as a plausible class for Evasive LWE. Another counter-example that they define is when Samp takes the matrix $\mathbf{B}$ as input – but in general, $\mathbf{B}$ is not touched by the sampler even in private coin versions of Evasive LWE and we do not believe this is a real problem.

We observe that [BUW24] also defined three main families of evasive LWE assumptions where these counterexamples do not apply. However, since our attacks fall within families they conjecture as plausible, we refrain from using this classification in our work, and also refrain from providing a different classification. Our opinion is that such a classification may be better made after the state of attacks on Evasive LWE has stabilized.

Malicious sampler attacks: These attacks show that Evasive LWE, both public and private coin, does not hold for arbitrary samplers, who may choose circuit implementations and error distributions in a malicious way. A common theme that runs through these attacks (Sections 4.1, 4.2, 5.1 and 5.2) is that they exploit flexibility in design of $\mathbf{P}$, which in turn encodes some functionality F, so that the error in the post-condition lends itself to manipulation that is not captured by the well-distributed i.i.d error in the pre-condition. It is very interesting to us that even though the assumption of evasive LWE originated in the desire to avoid the so-called "zeroizing regime" where attacks against iO candidates had traditionally been found [CHL+15, MSZ16, CVW18, HJL21], the new attacks show that by constructing malicious samplers, we can still end up in the zeroizing regime by cleverly manipulating the computation!

In more detail, according to Wee [Wee22], the "zeroizing regime" is where the adversary may obtain a large number of equations in secret values over the integers, which can then be somehow solved to recover the secrets (or more generally lead to leakage on secret values). The attacks we present in Sections 4.1, 4.2, 5.1 and 5.2 can be seen as zeroizing attacks since we can recover equations over the integers, notably since there is no wraparound modulo q. This in particular, allows us to reduce the equations modulo some small number, for instance $\bmod 2$ and obtain leakage. Note that if the equations are modulo q (i.e. there

is wraparound modulo q), then computing modulo 2 is not well defined and does not (appear to) lead to any leakage that can be exploited. Our attacks crucially exploit the flexibility of the sampler to strip away large terms that cause wraparound modulo q and obtain equations over the integers.

We suggest the following approaches to mitigate this risk:

1. *Restricting the Sampler.* Based on the learning from the attacks, we can restrict the sampler as follows.

   - Controlling the Structure of $\mathbf{P}$: Frequently, the structure of $\mathbf{P}$ is quite restricted for applications, and moreover chosen by honest algorithms in the real world. As a notable example, for functionality, both [HLL23] as well as [AKY24a] only need $\mathbf{P}$ to have a structure like $\mathbf{A}_F$ which is constructed using homomorphic evaluation of a public function on public matrices. Moreover, in the real world, the circuit implementation of F is chosen by the key generator, who is an honest party – this suggests it better models the real world if the adversary's control on the structure of $\mathbf{P}$ is removed/reduced. This can be achieved by making the circuit structure in $\mathbf{P}$, namely $\mathbf{A}_F$ canonical using the universal circuit or randomized encodings.
   - Pre-Condition Error should not be Larger: The attack presented in Section 4.2 crucially exploits the fact that the error in the pre-condition is larger than that in the post-condition. Wee's original paper introducing evasive LWE [Wee22] intuited that this should not be the case and suggested choosing a larger error in the post-condition than in the pre-condition for a more conservative assumption. Our attack formalizes this intuition and suggests this as a check for safe-zone.

2. *More Stringent Pre-Condition.* Another approach is to make the pre-condition of evasive LWE more stringent so that the error in the pre-condition is not chosen as i.i.d without discretion but captures real world correlated error in some meaningful way. We formulate one such version in Section 6, where an additional check is performed before the error in the pre-condition is replaced by i.i.d. error. The extra check that we add can be seen as capturing the spirit of the "LWE with correlated noise is secure" family of conjectures. Based on current knowledge, this extra check serves to separate the schemes that can and cannot be broken (barring functionalities which suffer from incompressibility style impossibilities). To be cautious, we suggest that it is prudent to wait until attacks have stabilized before using this assumption to prove security of constructions.

Contrived functionality, or Incompressibility attacks: The attack by Branco et al. [BDJ+24][Sec 9] and that in Section 5.3 show that there exists a contrived "self-referential" functionality for which pseudorandom obfuscation or compact functional encryption satisfying simulation style security cannot exist. We believe these results are analogous to the impossibilities known for the random oracle model [CGH04] or VBB obfuscation [BGI+01] and can be handled using the same philosophical approach as in these settings.

It is well known that a true random oracle cannot exist – the work of Canetti, Goldreich and Halevi [CGH04] showed that there exist signature and encryption schemes that are secure in the Random Oracle Model, but for which any implementation of the random oracle results in insecure schemes. However, despite the impossibility, it is widely believed that proving a cryptographic scheme secure in the Random Oracle Model provides strong and meaningful evidence of its practical security. Similarly, the work of Barak et al. [BGI+01] shows that virtual black box obfuscation is impossible in general by exhibiting a specific functionality for which such strong security cannot exist (indeed the spirit of the subclass of counter-examples being discussed here is very similar to the counter-example by [BGI+01]) but this does not disallow constructing VBB obfuscation for specific functionalities [Wee05, CRV10]. The pseudorandom functionalities that are useful for applications, such as computing blind garbled circuits or FE ciphertexts, are quite natural and do not fall prey to such attacks. We believe that the proof from

evasive LWE for these functionalities provides strong evidence for real world security of the schemes, similar to proofs in the ROM. An intriguing future line of work would be to construct some variant of evasive LWE that only admits constructions satisfying weaker security notions that are not known to be generally impossible.

We additionally remark that the incompressibility style arguments underlying these counter-examples do not apply in the *single challenge* setting. Translated into the evasive LWE assumption, single-challenge means that $\mathbf{S}$ is a vector and not a matrix. Hence, one natural way to avoid these counter-examples is to use evasive LWE in the single-challenge regime. We refer the reader to Section 6 for a more detailed discussion.

2.3 Variants and Obfustopia

An important question in the light of the new attacks is: if evasive LWE does not respect the boundaries of the non-zeroizing regime in any case, then how far are we from Obfustopia? The new attacks against evasive LWE give insights not only into the weaknesses of evasive LWE but also into its strengths – we ask if these strengths can be used to make progress to bridging the distance to Obfustopia. Towards this, we demonstrate that additional *strengthenings* of evasive LWE imply compact functional encryption or succinct randomized encodings which can be bootstrapped to iO using known results. The rationale behind suggesting these variants is that the modifications (i) do not appear to worsen known weaknesses further, (ii) can benefit from known strengths, and, (iii) while they certainly **do introduce new regimes of attack, notably the zeroizing regime**, these can be handled using knowledge that the community gained from existing lattice based iO candidates. We believe our candidates are of value, since we only have a handful of candidates from lattices that can be conjectured secure in the standard model [GMM+16b, AP20, BDGM20, WW21, GP21][5] and one in the pseudorandom oracle model [BDJ+24]. We emphasize that these variants are presented primarily as an invitation for cryptanalysis.

FE from Correlated Flooding, or "Fixed-Bit" Evasive LWE. Our starting point is the AKY FE construction we introduced in Section 2.1. We recall that the ciphertext $\mathsf{ct}(\mathbf{x}')$ along with a secret key $\mathsf{sk}_{f'}$ reveals $f'(\mathbf{x}') + \text{error}$, where $f'(\mathbf{x}') \in \mathbb{Z}_q^L$. Though the lower-order bits of $f'(\mathbf{x}')$ are not recoverable due to the error term, the higher-order bits are still recoverable. Based on this observation, AKY construct a prFE by embedding the decryption result into the higher order bits of $f'(\mathbf{x}')$. Namely, in order to encrypt a message $\mathbf{x}$, an encryptor chooses random seed sd of PRG and then computes $\mathsf{ct}(\mathbf{x}, \mathsf{sd})$. In order to generate a secret key for boolean circuit f whose output space is $\{0,1\}^L$, we consider a function f' that takes as input $(\mathbf{x}, \mathsf{sd})$ and outputs $\lfloor q/2 \rfloor f(\mathbf{x}) + \mathsf{PRG}(\mathsf{sd})$, where the output of the PRG is in $[-\lfloor q/4 \rfloor, -\lfloor q/4 \rfloor]^L$, and generate $\mathsf{sk}_{f'}$. By decryption, we obtain $\lfloor q/2 \rfloor f(\mathbf{x}) + \mathsf{PRG}(\mathsf{sd}) + \text{error}$ and we are able to extract $f(\mathbf{x}) \in \{0,1\}^L$ from it[6].

Our first observation is that if we do not care about security, their construction works even for arbitrary functions, not limited to the functions with pseudorandom outputs. Let us examine where their security proof breaks down if we do not enforce the pseudorandomness requirement for f and consider general f instead. To do so, we try to prove the pseudorandomness of the pre-condition distribution $\mathbf{c}_\mathbf{B}^\intercal$, $\mathbf{c}_\mathbf{A}^\intercal$, X, and $\mathbf{c}_\mathbf{P}^\intercal$ by using the same hybrids as those for AKY prFE. We observe that the transition from Hyb_0 to Hyb_3 follows from the same reasoning. However, in Hyb_4, since $f(\mathbf{x})$ is not guaranteed to be pseudorandom, we cannot change $\mathbf{c}_\mathbf{P}$ into a random string. Nevertheless, we can assert something weaker: due to the security of the PRG, we can change $\mathbf{c}_\mathbf{P}$ to be a random distribution over half the space of $\mathbb{Z}_q$. The evasive LWE is not useful in this situation, since it says the indistinguishability of the post-condition distributions only when $\mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal$ is pseudorandom over the whole space of $\mathbb{Z}_q$.

[5] Note that the assumptions underlying [WW21, GP21] can be broken but the constructions are still believed to be secure.

[6] We use a PRG here rather than a PRF for simplicity, since we are in the single key setting.

Here, we consider a strengthening of the evasive LWE assumption that we call correlated flooding *a.k.a.* fixed bit evasive LWE assumption. This assumption guarantees the security of the post-condition, if the pre-condition distribution is half the space pseudorandom. Namely, it says that if

$$\left(\mathbf{B},\ \mathbf{P},\ \ \mathbf{s}^\intercal\mathbf{B}+\mathbf{e}_\mathbf{B}^\intercal,\ \ \mathbf{s}^\intercal\mathbf{P}+\mathbf{e}_\mathbf{P}^\intercal,\ \ \mathsf{aux}\ \right) \approx_c \left(\ \mathbf{B},\ \mathbf{P},\ \mathbf{c}_\mathbf{B}^\intercal \leftarrow \$,\ \ \mathbf{t}^\intercal+\mathbf{d}^\intercal,\ \ \mathsf{aux}\right)$$

where $\mathbf{d}$ represents a random vector with each entry being distributed over $[-\lfloor q/4\rfloor, \lfloor q/4\rfloor]$ and $\mathbf{t}$ is a vector that can be efficiently and deterministically computed from aux, then

$$\left(\ \mathbf{B},\ \mathbf{P},\ \mathbf{c}_\mathbf{B}^\intercal=\mathbf{s}^\intercal\mathbf{B}+\mathbf{e}_\mathbf{B}^\intercal,\ \mathbf{K}\leftarrow\mathbf{B}^{-1}(\mathbf{P}),\ \ \mathsf{aux}\right) \approx_c \left(\ \mathbf{B},\ \mathbf{P},\ \ \mathbf{c}_\mathbf{B}^\intercal\leftarrow\$,\ \ \mathbf{K}\leftarrow\begin{bmatrix}\mathbf{B}\\ \mathbf{c}_\mathbf{B}^\intercal\end{bmatrix}^{-1}\left(\begin{bmatrix}\mathbf{P}\\ \mathbf{t}^\intercal+\mathbf{d}^\intercal\end{bmatrix}\right)\ \ \mathsf{aux}\right).$$

The additional restriction on $\mathbf{K}$ in the RHS that $\mathbf{c}_\mathbf{B}^\intercal\mathbf{K}=\mathbf{t}^\intercal+\mathbf{d}^\intercal$ is necessary for the assumption to be not trivially broken. To see this, we first observe that $\mathbf{s}^\intercal\mathbf{P}$ and $\mathbf{t}^\intercal$ are within distance $q/4$ in terms of the infinity norm with high probability, since otherwise the pre-condition distributions are easy to distinguish. Without the additional restriction, $\mathbf{c}_\mathbf{B}^\intercal\mathbf{K}$ in the RHS will be random, which should not be within distance $q/4$ from $\mathbf{t}^\intercal$ with high probability, while $(\mathbf{s}^\intercal\mathbf{B}+\mathbf{e}_\mathbf{B}^\intercal)\mathbf{K}=\mathbf{s}^\intercal\mathbf{P}+\mathbf{e}_\mathbf{B}^\intercal\mathbf{K}$ is within distance $q/4$ from $\mathbf{t}^\intercal$ with high probability. Therefore, the post-condition distributions are distinguishable by computing $\mathbf{c}_\mathbf{B}^\intercal\mathbf{K}$ and seeing whether it is close to $\mathbf{t}$ or not.

This new assumption implies that the AKY prFE construction satisfies the standard indistinguishability security notion for FE [7]. However, we must be careful to restrict the sampler appropriately since we showed that general samplers are susceptible to attack. We adopt two counter-measures. The first one is to make the circuit used to perform the homomorphic computation canonical/fixed so that it evades the contrived designs like the ones we used for the attack. Another counter-measure is to find a way to "throw away" the leaky error thus breaking the correlation which led to the attack. This is possible by using a modulus reduction technique suggested in (the revised version of) [AKY24a] (for fixing their scheme), which allows to get rid of the problematic correlated noise by rounding it away. In more detail, we change the homomorphic evaluation so that FHE decryption error $\mathbf{e}_{\mathsf{fhe}}^\intercal$ does not appear in the final decryption equation (i.e., Equation (9)), even in the masked form.

Security. In terms of security, we analyze the new assumption for all known attacks in the literature. For the distributions used in our particular construction, we show that the "fixed bit" evasive LWE assumption implies regular evasive LWE. We currently do not know any additional attacks against the fixed bit version as compared to regular evasive LWE – while the fixed bit version explicitly opens into the zeroizing regime, attacks from prior work do not seem to apply and the new attacks developed in the present work can be protected against using some of the ideas discussed above. Having said that, we emphasize again that our chief goal in presenting this assumption and construction is to explore the distance of this family of assumptions from obfustopia, and while we do not know attacks, it would be premature to claim security. We invite the community to attack these assumptions. Please see Section 7 for more details.

SRE from Succinct LWE Sampler. Finally, we adapt our ideas to provide a succinct LWE sampler as defined by Devdas et al. [DQV+21] (referred from now as DQVWW). Recall that DQVWW provided a compiler to construct a succinct randomized encoding (SRE) from any succinct LWE sampler, which in turn implies iO. Informally speaking, upon input a size parameter N, a succinct LWE sampler outputs a seed, seed_{B^*} for LWE matrix $\mathbf{A}^*\mathbf{S}^*+\mathbf{E}^*$, such that the size of seed_{B^*} is sub-linear in size of $\mathbf{B}^*\in\mathbb{Z}_q^{M\times K}$, where $MK=N$. The security definition of the succinct LWE sampler (SLS) is non-falsifiable. To remedy this, DQVWW then defines a weak SLS with a falsifiable security definition and provides an amplifier to lift any weak succinct LWE sampler to a succinct LWE sampler.

[7] Interestingly, single challenge security suffices and therefore the incompressibility attack from Section 5.3 does not apply.

The starting point of our work is the observation that the prFE construction by [AKY24a] naturally lends itself to building a weak SLS – the key idea is to generate K ciphertexts and M keys so that their combinations output MK entries of the matrix $\mathbf{B}^*$. In more detail, we use a PRF to generate the LWE errors as follows. To generate $\mathbf{E}^*[i,j]$, we encrypt a PRF seed sd_j and provide a key for PRF function F_i, such that $\mathrm{F}_i(\mathsf{sd}_j) = \mathsf{PRF}(\mathsf{sd}_j, i)$. We use the learning obtained via the attacks to ensure that the PRF circuit implementation is chosen carefully so that security can be conjectured.

To compute $\mathbf{A}^*\mathbf{S}^*[i,j] = \mathbf{A}^*[i,\cdot]\mathbf{S}^*[\cdot,j]$, we use ideas from inner product functional encryption (IPFE) – we hide $\mathbf{S}^*[\cdot,j]$ inside an IPFE ciphertext, and provide the corresponding IPFE key for $\mathbf{A}^*[i,\cdot]$. By using IPFE to generate the linear mask in the LWE sample being constructed, we ensure that no contrived circuit attacks can apply. Next, it remains to tie the LWE mask and error together so that $\mathbf{A}^*\mathbf{S}^*$ and $\mathbf{E}^*$ cannot be computed separately. To ensure this, we join the prFE and the IPFE keys into one key that prevents piecewise decryption. For weak security, we formulate a falsifiable, instance independent hardness assumption.

Security. The rationale behind the security here is the same as in the previously described "fixed-bit evasive LWE", namely heuristic evidence that can be formulated as a kind of computational flooding conjecture. The advantage is that this assumption is instance independent and falsifiable. The disadvantage is that it is fairly messy and does not easily lend itself to cryptanalysis. Nevertheless, we find it interesting that the prFE construction of [AKY24a] based on evasive LWE can be used to compress $\mathbf{B}^*$ as desired in DQVWW and that it suggests a family of computational flooding conjectures which appear plausible. Indeed, our hope is that even if the exact flooding conjecture we make turns out to be problematic, some variant of it is likely to stand the test of time. Please see Section 8 for details.

2.4 Takeaways: Evasive versus Non-Evasive assumptions

We provide a very high level takeaway of the assumptions we discussed. For evasive LWE, we now know that for the most general formulation, zeroizing attacks do apply but by adopting the suggested countermeasures, the assumption can regain its "non-zeroizing" status. Thus, we hope that appropriately curtailed versions of evasive LWE can still respect the intuition that "LWE with correlated error" (or more generally "correlated flooding with mask") is secure. This assumption can be used to build evasive functionalities like ABE where the decryptor does not obtain any keys that decrypt the challenge ciphertext. Using this assumption in its safe zone (which may still take some time to stabilize) gives us many important constructions that are not known outside Obfustopia [Wee22, VWW22, Tsa22, HLL23, AKY24b, ARYY23].

Next we saw that by providing a controlled entry into the zeroizing regime, variants of the evasive LWE assumption (having shed its "evasiveness"), can be used to build full fledged compact FE and iO thus bridging the distance all the way to Obfustopia. This family of assumptions intuitively capture the "(computational) correlated flooding" conjectures discussed previously, notably *without* the protection of a large masking term that characterized the previous class. We believe that family of assumptions provides a different and (in our opinion) principled way to approach iO.

3 Preliminaries

Notations. We use bold capital letters to denote a matrix and bold small letters to represent vectors. By default, a vector $\mathbf{v}$ is a column vector and $\mathbf{v}^\intercal$ is a row vector. ι_i represents a unit vector with 1 at position i. Throughout the paper, we use λ to denote the security parameter. For any $x \in \mathbb{Z}_q$, $\lfloor x \rceil_p \in \mathbb{Z}_p = \left\lfloor x \cdot \frac{p}{q} \right\rceil$. Sometimes, we regard an element in $x \in \mathbb{Z}_q$ as an integer in $[-q/2, q/2]$. When we take an absolute value $|x|$ for $x \in \mathbb{Z}_q$, this operation means that first regarding x as an integer and then taking the absolute value. For any function f, we write $|f|$ to represent its size. For any set S, $|S|$ denotes the number of

elements in set S. For any vector $\mathbf{v}$, we use $\mathbf{v}[\ell;\ell']$ to denote the part of vector $\mathbf{v}$ starting from ℓ-th element and ending at ℓ'-th element where $\ell,\ell' \in \mathbb{Z}_q$. For any vector $\mathbf{v}$, $\mathbf{v}[i,j]$ denotes the jth lowest order bit of i-th element of $\mathbf{v}$. For any matrix $\mathbf{V}$, $\mathbf{V}[i,j]$ denotes the element at i-th row and j-th column, $\mathbf{V}[i,\cdot]$ denotes the ith row of $\mathbf{V}$ and $\mathbf{V}[\cdot,j]$ denotes the jth column of $\mathbf{V}$. We consider the infinity norm:

$$\|\mathbf{v}\| = \mathsf{max}_i|\mathbf{v}[i]|, \qquad \|\mathbf{V}\| = \mathsf{max}_i \sum_j |\mathbf{V}[i,j]|$$

With slight overload of notation, we also define $|\mathbf{v}| = \mathsf{max}_i|\mathbf{v}[i]|$ and $|\mathbf{V}| = \mathsf{max}_{i,j}|\mathbf{V}[i,j]|$. We define the most-significant bit operator $\mathsf{MSB} : \mathbb{Z}_q \to \{0,1\}$ as

$$\mathsf{MSB}(x) = \begin{cases} 0, & \text{if } x \in [-q/4, q/4) \\ 1, & \text{otherwise} \end{cases}$$

We slightly overload the notation and represent MSB of a vector $\mathbf{v} \in \mathbb{Z}_q^n$ as $\mathsf{MSB}(\mathbf{v}) = (\mathsf{MSB}(\mathbf{v}[1]), \ldots, \mathsf{MSB}(\mathbf{v}[n]))$.

3.1 Functional Encryption

Consider a function family $\{\mathcal{F}_{\mathsf{prm}} = \{f : \mathcal{X}_{\mathsf{prm}} \to \mathcal{Y}_{\mathsf{prm}}\}\}_{\mathsf{prm}}$ for a parameter $\mathsf{prm} = \mathsf{prm}(\lambda)$. Each function $f \in \mathcal{F}_{\mathsf{prm}}$ takes as input a string $x \in \mathcal{X}_{\mathsf{prm}}$ and outputs $f(x) \in \mathcal{Y}_{\mathsf{prm}}$.

Syntax. A functional encryption scheme FE for function family $\mathcal{F}_{\mathsf{prm}}$ consists of four polynomial time algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ defined as follows.

$\mathsf{Setup}(1^\lambda, \mathsf{prm}) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm takes as input the security parameter λ and a parameter prm and outputs a public key mpk and a master secret key msk.

$\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{sk}_f$. The key generation algorithm takes as input the master secret key msk and a function $f \in \mathcal{F}_{\mathsf{prm}}$ and it outputs a functional secret key sk_f.

$\mathsf{Enc}(\mathsf{mpk}, x) \to \mathsf{ct}$. The encryption algorithm takes as input the public key mpk and an input $x \in \mathcal{X}_{\mathsf{prm}}$ and outputs a ciphertext $\mathsf{ct} \in \mathcal{CT}$, where $\mathcal{CT}$ is the ciphertext space.

$\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}) \to y$. The decryption algorithm takes as input a functional secret key sk_f and a ciphertext ct and outputs $y \in \mathcal{Y}_{\mathsf{prm}}$.

Definition 3.1 (Correctness). A FE scheme is said to be correct if for all prm, any input $x \in \mathcal{X}_{\mathsf{prm}}$ and function $f \in \mathcal{F}_{\mathsf{prm}}$, we have

$$\Pr\left[\begin{matrix}(\mathsf{mpk},\mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, 1^{\mathsf{prm}})\ ,\ \mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f), \\ \mathsf{Dec}\big(\mathsf{sk}_f, \mathsf{Enc}(\mathsf{mpk}, x)\big) = f(x)\end{matrix}\right] = 1.$$

where the probability is taken over the coins of Setup, KeyGen, and Enc.

In this paper we will consider the standard indistinguishability based definition.

Definition 3.2 (Selective Security). A functional encryption scheme for function family $\{\mathcal{F}_{\mathsf{prm}} = \{f : \mathcal{X}_{\mathsf{prm}} \to \mathcal{Y}_{\mathsf{prm}}\}\}_{\mathsf{prm}}$, parameter $\mathsf{prm} = \mathsf{prm}(\lambda)$ is said to be selectively secure if for any PPT adversary $\mathcal{A}$ the following holds

$$\Pr\left[\begin{matrix}\mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(\mathsf{mpk},\mathsf{ct}) = b : \\ \end{matrix}\begin{matrix}(x_0,x_1) \leftarrow \mathcal{A}; \\ (\mathsf{mpk},\mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda,\mathsf{prm}); \\ b \leftarrow \{0,1\}; \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_b)\end{matrix}\right] \leq 1/2 + \mathsf{negl}(\lambda),$$

where each key query for a function $f \in \mathcal{F}_{\mathsf{prm}}$, queried by $\mathcal{A}$ to the $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$ oracle must satisfy the condition that $f(x_0) = f(x_1)$.

In this paper, we consider the weaker notion of *very selective* security where the adversary announces all its function queries at the first step, together with the challenge messages.

Compactness. Intuitively, an FE scheme is compact if the length of its ciphertext does not depend on the size of the circuit it supports [AJ15, BV18]. Formally, we say an FE scheme is compact if the encryption algorithm runs in time $\mathrm{poly}(\lambda, |\mathbf{x}|, \log S)$ where $\mathbf{x}$ is the input and S is the size of the circuit. The notion of weak compactness asks that the encryption algorithm run in time $\mathrm{poly}(\lambda, |\mathbf{x}|) \cdot S^{1-\epsilon}$ for any constant $\epsilon \in (0,1)$.

3.2 Functional Encryption for Pseudorandom Functionalities

In this section, we give the definition of functional encryption for pseudorandom functionalities prFE [AKY24a]. Consider a function family $\{\mathcal{F}_{\mathsf{prm}} = \{f : \mathcal{X}_{\mathsf{prm}} \to \mathcal{Y}_{\mathsf{prm}}\}\}_{\mathsf{prm}}$ for a parameter $\mathsf{prm} = \mathsf{prm}(\lambda)$. Each function $f \in \mathcal{F}_{\mathsf{prm}}$ takes as input a string $x \in \mathcal{X}_{\mathsf{prm}}$ and outputs $f(x) \in \mathcal{Y}_{\mathsf{prm}}$. The Syntax and correctness of prFE is the same as that of FE as in Section 3.1.

prCT security. [AKY24a] For a prFE scheme for function family $\{\mathcal{F}_{\mathsf{prm}} = \{f : \mathcal{X}_{\mathsf{prm}} \to \mathcal{Y}_{\mathsf{prm}}\}\}_{\mathsf{prm}}$ parameter $\mathsf{prm} = \mathsf{prm}(\lambda)$, let Samp be a PPT algorithm that on input 1^λ, outputs $(f_1, \ldots, f_{Q_{\mathsf{key}}}, x_1, \ldots, x_{Q_{\mathsf{msg}}}, \mathsf{aux} \in \{0,1\}^*)$ where Q_{key} is the number of key queries, Q_{msg} is the number of message queries, and $f_i \in \mathcal{F}_{\mathsf{prm}}$, $x_j \in \mathcal{X}_{\mathsf{prm}}$ for all $i \in [Q_{\mathsf{key}}]$, $j \in [Q_{\mathsf{msg}}]$. We define the following advantage functions:

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{pre}}_{\mathcal{A}_0}(\lambda) &\stackrel{\text{def}}{=} \Pr\Big[\mathcal{A}_0(\mathsf{aux}, \{f_i, f_i(x_j)\}_{i\in[Q_{\mathsf{key}}], j\in[Q_{\mathsf{msg}}]}) = 1\Big] \\
&\quad - \Pr\Big[\mathcal{A}_0(\mathsf{aux}, \{f_i, \Delta_{i,j} \leftarrow \mathcal{Y}_{\mathsf{prm}}\}_{i\in[Q_{\mathsf{key}}], j\in[Q_{\mathsf{msg}}]}) = 1\Big] \\
\mathsf{Adv}^{\mathsf{post}}_{\mathcal{A}_1}(\lambda) &\stackrel{\text{def}}{=} \Pr\Big[\mathcal{A}_1(\mathsf{mpk}, \mathsf{aux}, \{f_i, \mathsf{Enc}(\mathsf{mpk}, x_j), \mathsf{sk}_{f_i}\}_{i\in[Q_{\mathsf{key}}], j\in[Q_{\mathsf{msg}}]}) = 1\Big] \\
&\quad - \Pr\Big[\mathcal{A}_1(\mathsf{mpk}, \mathsf{aux}, \{f_i, \delta_j \leftarrow \mathcal{CT}, \mathsf{sk}_{f_i}\}_{i\in[Q_{\mathsf{key}}], j\in[Q_{\mathsf{msg}}]}) = 1\Big]
\end{aligned}$$

where $(f_1, \ldots, f_{Q_{\mathsf{key}}}, x_1, \ldots, x_{Q_{\mathsf{msg}}}, \mathsf{aux} \in \{0,1\}^*) \leftarrow \mathsf{Samp}(1^\lambda)$, $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathsf{prm})$ and $\mathcal{CT}$ is the ciphertext space. We say that a prFE scheme for function family $\mathcal{F}_{\mathsf{prm}}$ satisfies prCT security if for every PPT Samp there exists a polynomial $Q(\cdot)$ such that for every PPT adversary $\mathcal{A}_1$, there exists another PPT $\mathcal{A}_0$ such that

$$\mathsf{Adv}^{\mathsf{pre}}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{\mathsf{post}}_{\mathcal{A}_1}(\lambda)/Q(\lambda) - \mathsf{negl}(\lambda)$$

and $\mathrm{time}(\mathcal{A}_0) \leq \mathrm{time}(\mathcal{A}_1) \cdot Q(\lambda)$.

3.3 Indistinguishability Obfuscation

A uniform P.P.T machine $i\mathcal{O}$ is an indistinguishability obfuscator for a class of circuits $\{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$, if the following conditions are satisfied:

1. **Correctness.** For all security parameters $\lambda \in \mathbb{N}$, for any $C \in \mathcal{C}_\lambda$ and every input $\mathbf{x}$ from the domain of C, we have that:

   $$\Pr\left[C' \leftarrow i\mathcal{O}(1^\lambda, C) : C'(\mathbf{x}) = C(\mathbf{x})\right] = 1$$

   where the probability is taken over the coin-tosses of the obfuscator $i\mathcal{O}$.

2. **Indistinguishability of Equivalent Circuits.** For every ensemble of pairs of circuits $\{C_{0,\lambda}, C_{1,\lambda}\}_{\lambda\in\mathbb{N}}$ such that $C_{0,\lambda}(\mathbf{x}) = C_{1,\lambda}(\mathbf{x})$ for all $\mathbf{x}$, we have that the following ensembles of pairs of distributions are indistinguishable to any P.P.T Adv:

$$\left\{C_{0,\lambda}, C_{1,\lambda}, i\mathcal{O}(1^\lambda, C_{0,\lambda})\right\} \overset{c}{\approx} \left\{C_{0,\lambda}, C_{1,\lambda}, i\mathcal{O}(1^\lambda, C_{1,\lambda})\right\}$$

3.4 Instance Hiding Witness Encryption with Pseudorandom Ciphertext

Definition 3.3 (Witness Encryption). [GGSW13, BDJ+24] A witness encryption scheme for an NP language $\mathcal{L}$ (with the corresponding witness relation R) consists of the following two polynomial-time algorithms:

$\mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}, \mu) \to \mathsf{wct}$**.** [8] On input security parameter λ, an unbounded-length string stmt and message $\mu \in \{0,1\}$, outputs ciphertext wct.

$\mathsf{WE.Dec}(\mathsf{wt}, \mathsf{wct}) = \mu/\perp$**.** On input an unbounded length string wt and ciphertext wct, it either outputs message μ or the symbol $\perp$.

These algorithms satisfy the following conditions:

- **Correctness.** For any security parameter λ, for any $\mu \in \{0,1\}$, for any $\mathsf{stmt} \in \mathcal{L}$, such that $R(\mathsf{stmt}, \mathcal{L})$ holds i.e. $\mathsf{stmt} \in \mathcal{L}$, we have $\Pr\left[\mathsf{WE.Dec}(\mathsf{wt}, \mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}, \mu)) = \mu\right] = 1$.
- **Soundness.** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for any $\mathsf{stmt} \notin \mathcal{L}$, we have: $|\Pr\left[\mathcal{A}(\mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}, 0)) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}, 1)) = 1\right]| \leq \mathsf{negl}(\lambda)$.
- **Instance Hiding.** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for any $\mu \in \{0,1\}$ and for any $\mathsf{stmt}, \mathsf{stmt}' \notin \mathcal{L}$, we have: $|\Pr\left[\mathcal{A}(\mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}, \mu)) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}', \mu)) = 1\right]| \leq \mathsf{negl}(\lambda)$.
- **Pseudorandom Ciphertext.** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for any $\mathsf{stmt} \notin \mathcal{L}$ and any $\mu \in \{0,1\}$, we have: $|\Pr\left[\mathcal{A}(\mathsf{WE.Enc}(1^\lambda, \mathsf{stmt}, \mu)) = 1\right] - \Pr[\mathcal{A}(\mathcal{U}) = 1]| \leq \mathsf{negl}(\lambda)$ where $\mathcal{U}$ is sampled uniformly from the ciphertext space.

3.5 Lattice Preliminaries

Here, we recall some facts on lattices that are needed for the exposition of our construction. Throughout this section, n, m, and q are integers such that $n = \mathrm{poly}(\lambda)$ and $m \geq n\lceil \log q \rceil$. In the following, we define a function ρ_σ as $\rho_\sigma = \exp(-\pi\|\mathbf{x}/\sigma\|_2^2)$, where $\|\cdot\|_2$ is the Euclidean norm. We will overload the notation to denote by $\rho_\sigma(S)$ the summation of $\rho_\sigma(\mathbf{x})$ over all $\mathbf{x} \in S$ for a countable set X. For a countable set S, $\mathcal{D}_{S,\gamma}$ refers to a distribution that outputs $\mathbf{x} \in S$ with probability $\rho_\sigma(\mathbf{x})/\rho(S)$. In the following, let $\mathsf{SampZ}(\gamma)$ be a sampling algorithm for the truncated discrete Gaussian distribution over $\mathbb{Z}$ with parameter $\gamma > 0$ whose support is restricted to $z \in \mathbb{Z}$ such that $|z| \leq \sqrt{n}\gamma$. Namely, $\mathsf{SampZ}(\gamma)$ is the truncated version of $\mathcal{D}_{\mathbb{Z},\gamma}$.

Let

$$\mathbf{g} = (2^0, 2^1, \ldots, 2^{\frac{m}{n+1}-1})^\intercal\,, \quad \mathbf{G} = \mathbf{I}_{n+1} \otimes \mathbf{g}^\intercal$$

be the gadget vector and the gadget matrix. For $\mathbf{p} \in \mathbb{Z}_q^n$, we write $\mathbf{G}^{-1}(\mathbf{p})$ for the m-bit vector $(\mathsf{bits}(\mathbf{p}[1]), \ldots, \mathsf{bits}(\mathbf{p}[n+1]))^\intercal$, where $\mathsf{bits}(\mathbf{p}[i])$ are $m/(n+1)$ bits for each $i \in [n+1]$. The notation extends column-wise to matrices and it holds that $\mathbf{G}\mathbf{G}^{-1}(\mathbf{P}) = \mathbf{P}$.

[8] In the main body, we drop the first input and implicitly assume 1^λ as an input.

Trapdoors. Let us consider a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. For all $\mathbf{V} \in \mathbb{Z}_q^{n \times m'}$, we let $\mathbf{A}^{-1}(\mathbf{V})$ be an output distribution of $\mathsf{SampZ}(\gamma)^{m \times m'}$ conditioned on $\mathbf{A} \cdot \mathbf{A}^{-1}(\mathbf{V}, \gamma) = \mathbf{V}$. A γ-trapdoor for $\mathbf{A}$ is a trapdoor that enables one to sample from the distribution $\mathbf{A}^{-1}(\mathbf{V}, \gamma)$ in time $\mathrm{poly}(n, m, m', \log q)$ for any $\mathbf{V}$. We slightly overload notation and denote a γ-trapdoor for $\mathbf{A}$ by $\mathbf{A}_\gamma^{-1}$. The following properties had been established in a long sequence of works [GPV08, CHKP10, ABB10a, ABB10b, MP12, BLP+13].

Lemma 3.4 (Properties of Trapdoors). Lattice trapdoors exhibit the following properties.

1. Given $\mathbf{A}_\tau^{-1}$, one can obtain $\mathbf{A}_{\tau'}^{-1}$ for any $\tau' \geq \tau$.
2. Given $\mathbf{A}_\tau^{-1}$, one can obtain $[\mathbf{A}\|\mathbf{B}]_\tau^{-1}$ and $[\mathbf{B}\|\mathbf{A}]_\tau^{-1}$ for any $\mathbf{B}$.
3. There exists an efficient procedure $\mathsf{TrapGen}(1^n, 1^m, q)$ that outputs $(\mathbf{A}, \mathbf{A}_{\tau_0}^{-1})$ where $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some $m = O(n \log q)$ and is 2^{-n}-close to uniform, where $\tau_0 = \omega(\sqrt{n \log q \log m})$.

Useful Lemmata.

Lemma 3.5 (tail and truncation of $\mathcal{D}_{\mathbb{Z},\gamma}$). There exists $B_0 \in \Theta(\sqrt{\lambda})$ such that

$$\Pr\left[x \leftarrow \mathcal{D}_{\mathbb{Z},\gamma} : |x| > \gamma B_0(\lambda)\right] \leq 2^{-\lambda} \quad \text{for all} \quad \gamma \geq 1 \text{ and } \lambda \in \mathbb{N}.$$

Let $B \geq 0$, the distribution $\mathcal{D}_{\mathbb{Z},\gamma,\leq B}$ is sampled by first sampling $x \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}$, then returning x if $|x| \leq B$, and 0 otherwise. Let $\gamma \geq 1$ and $B = \gamma\Theta(\sqrt{\lambda})$, then $\mathcal{D}_{\mathbb{Z},\gamma,\leq B}$ is $2^{-\Omega(\lambda)}$-close to $\mathcal{D}_{\mathbb{Z},\gamma}$.

Lemma 3.6 ([[Lyu12, Lemma 4.4]]). The following hold.

1. For any $k > 0$, $\Pr[|z| > k\sigma; z \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}] \leq 2\exp(-k^2/2)$.
2. For any $k > 1$,
$$\Pr\left[\|\mathbf{z}\| > k\sigma\sqrt{m};\ \mathbf{z} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}\right] < k^m \exp\left(\frac{m}{2}(1-k^2)\right).$$

Lemma 3.7. [PR06, Adapted from Lemma 2.11] For all but 2^{-n} fraction of $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, we have

$$H_\infty(\mathbf{v}) \geq \log(\sigma/\lambda)$$

where $\mathbf{v} \leftarrow \mathbf{B}_\sigma^{-1}(\mathbf{u})$ for any vector $\mathbf{u} \in \mathbb{Z}_q^n$.

Proof. By Lemma 2.10 of [PR06], for any $\mathbf{c} \in \mathbb{R}^m$ and m-dimensional lattice Λ, we have $\rho_\sigma(\Lambda + \mathbf{c}) \in [\sigma^m \det(\Lambda^*)(1-\epsilon), \sigma^m \det(\Lambda^*)(1+\epsilon)]$ if $\sigma \geq \eta_\epsilon(\Lambda)$, where $\eta_\epsilon(\Lambda)$ is the smoothing parameter of Λ w.r.t the parameter ϵ and $\det(\Lambda^*)$ is the determinant of the dual lattice Λ^* of Λ.[9] This also implies $1 \leq \rho_\tau(\Lambda + \mathbf{c}) \leq \tau^m \det(\Lambda^*)(1+\epsilon)$ for $\tau > \eta_\epsilon(\Lambda)$. These together imply that

$$\mathcal{D}_{\Lambda+\mathbf{c},\sigma}(\mathbf{v}) = \frac{\rho_\sigma(\mathbf{v})}{\rho_\sigma(\Lambda + \mathbf{c})} \leq \frac{1}{\sigma^m \det(\Lambda^*)(1-\epsilon)} \leq (\tau/\sigma)^m \cdot \frac{1+\epsilon}{1-\epsilon}.$$

We then consider the lattice

$$\Lambda^\perp(\mathbf{B}) = \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{B}\mathbf{v} = \mathbf{u} \bmod q\}$$

and $\mathbf{c} \in \mathbb{Z}^m$ such that $\mathbf{B}\mathbf{c} = \mathbf{u} \bmod q$. We then observe that $\mathbf{v}$ follows the distribution $\mathcal{D}_{\Lambda+\mathbf{c},\sigma}$. Then, the lemma follows since as shown in [GPV08], for $\tau = \omega(\log m)$, we have $\eta_{2^{-n}}(\Lambda^\perp(\mathbf{B})) < \tau$ for all but 2^{-n} fraction of $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$. Taking $\tau = \lambda/2$, the lemma follows. □

[9] We refer to the definitions of the smoothing parameter, dual lattice, and its determinant to [PR06], since this is not necessary for our purpose.

Lemma 3.8 ([[ABB10a, Lemma 2.14 (Generalized Leftover Hash Lemma)]]). Let $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}$ be a 2-universal hash function family and $f : \mathcal{X} \to \mathcal{Z}$ be a function. Then for any random variable X taking value in $\mathcal{X}$, the distributions

$$(h, h(X), f(X)) \text{ and } (h, \mathcal{U}(\mathcal{Y}), f(X))$$

are within statistical distance $\sqrt{2^{-H_\infty(X)} \cdot |\mathcal{Y}||\mathcal{Z}|}$, where $\mathcal{U}(\mathcal{Y})$ represents the uniform distribution over $\mathcal{Y}$. More generally, let $X_1, \ldots X_Q$ be independent random variables taking values in $\mathcal{X}$ and let $\gamma = \min_{i \in [Q]} H_\infty(X_i)$. Then, the distributions

$$(h, h(X_1), \ldots, h(X_Q), f(X_1), \ldots, f(X_Q)) \text{ and } (h, \mathcal{U}_1(\mathcal{Y}), \ldots, \mathcal{U}_Q(\mathcal{Y}), f(X_1), \ldots, f(X_Q))$$

are within statistical distance $Q\sqrt{2^{-\gamma} \cdot |\mathcal{Y}||\mathcal{Z}|}$.

We note that even in the special case where there is no side information of the form $f(X)$, the above lemma can be applied by setting $f(X) = \perp$ for all X and $|\mathcal{Z}| = 1$. In this case, we call the above lemma "leftover hash lemma". We also note that the family $\{\mathbf{A} \in \mathbb{Z}_q^{n \times m} : \mathbf{r} \mapsto \mathbf{A}\mathbf{r}\}_{\mathbf{A}}$ is 2-universal for any prime q. Furthermore, if we restrict the input space to be $\{0,1\}^m$, the same family is 2-universal for any integer q.

Lemma 3.9 (Smudging Lemma [WWW22b]). Let λ be a security parameter. Take any $a \in \mathbb{Z}$ where $|a| \leq B$. Suppose $\gamma \geq B\lambda^{\omega(1)}$. Then the statistical distance between the distributions $\{z : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ and $\{z + a : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ is $\mathsf{negl}(\lambda)$.

Lemma 3.10. For $\gamma \geq c\lambda^{\omega(1)}$, $\{z \bmod 2 : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ is statistically close to the uniform distribution over $\{0,1\}$.

Proof. By Lemma 3.9, $\{z : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ and $\{z+1 : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ are statistically close. Therefore, $\{z \bmod 2 : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ and $\{z+1 \bmod 2 : z \leftarrow \mathcal{D}_{\mathbb{Z},\gamma}\}$ are statistically close. This implies what we want to show. □

3.5.1 Hardness Assumptions

Assumption 3.11 (The LWE Assumption). Let $n = n(\lambda)$, $m = m(\lambda)$, and $q = q(\lambda) > 2$ be integers and $\chi = \chi(\lambda)$ be a distribution over $\mathbb{Z}_q$. We say that the $\mathrm{LWE}(n, m, q, \chi)$ hardness assumption holds if for any PPT adversary $\mathcal{A}$ we have

$$|\Pr[\mathcal{A}(\mathbf{A}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal) \to 1] - \Pr[\mathcal{A}(\mathbf{A}, \mathbf{v}^\intercal) \to 1]| \leq \mathsf{negl}(\lambda)$$

where the probability is taken over the choice of the random coins by the adversary $\mathcal{A}$ and $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$, and $\mathbf{v} \leftarrow \mathbb{Z}_q^m$. We also say that $\mathrm{LWE}(n, m, q, \chi)$ problem is subexponentially hard if the above probability is bounded by $2^{-n^\epsilon} \cdot \mathsf{negl}(\lambda)$ for some constant $0 < \epsilon < 1$ for all PPT $\mathcal{A}$.

As shown by previous works [Reg09, BLP+13], if we set $\chi = \mathsf{SampZ}(\gamma)$, the $\mathrm{LWE}(n, m, q, \chi)$ problem is as hard as solving worst case lattice problems such as gapSVP and SIVP with approximation factor $\mathrm{poly}(n) \cdot (q/\gamma)$ for some $\mathrm{poly}(n)$. Since the best known algorithms for 2^k-approximation of gapSVP and SIVP run in time $2^{\tilde{O}(n/k)}$, it follows that the above $\mathrm{LWE}(n, m, q, \chi)$ with noise-to-modulus ratio 2^{-n^ϵ} is likely to be (subexponentially) hard for some constant ϵ.

Assumption 3.12 ((Circular) Small Secret LWE Assumption). [HLL23] Let $n.m, m', q, \sigma, \sigma'$ be functions of λ and

$$\overline{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n \times m}, \quad \overline{\mathbf{A}}_0 \leftarrow \mathbb{Z}_q^{n \times m'}, \quad \mathbf{r} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma,\leq\sigma\lambda}, \quad \mathbf{s} \leftarrow (\mathbf{r}^\intercal, -1)^\intercal,$$
$$\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma,\leq\sigma\lambda}, \quad \mathbf{e}_0 \leftarrow \mathcal{D}^{m'}_{\mathbb{Z},\sigma',\leq\sigma'\lambda}, \quad \mathbf{R} \leftarrow \{0,1\}^{m \times (n+1)\lceil \log_2 q \rceil m}$$

The circular small-secret LWE assumption $\mathsf{csLWE}_{n.m,m',q,\sigma,\sigma'}$ states that

$$\left\{\left(1^\lambda, \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}}\\ \mathbf{c}_{\mathsf{fhe}}^\intercal = \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^\intercal\end{pmatrix}, \mathbf{C} = \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}}\\ \mathbf{c}_{\mathsf{fhe}}^\intercal = \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^\intercal\end{pmatrix}\mathbf{R} - \mathsf{bits}(\mathbf{s})\otimes\mathbf{G}, \begin{pmatrix}\overline{\mathbf{A}}_0\\ \mathbf{c}_0^\intercal = \mathbf{r}^\intercal\overline{\mathbf{A}}_0 + \mathbf{e}_0^\intercal\end{pmatrix}\right)\right\}_{\lambda\in\mathbb{N}}$$

$$\approx_c \left\{\left(1^\lambda, \underbrace{\begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}}\\ \mathbf{c}_{\mathsf{fhe}}^\intercal \leftarrow \mathbb{Z}_q^{1\times m}\end{pmatrix}, \quad \mathbf{C}\leftarrow\mathbb{Z}_q^{n+1\times(n+1)\lceil\log_2 q\rceil m}}_{\text{circular terms}}, \quad \begin{pmatrix}\overline{\mathbf{A}}_0\\ \mathbf{c}_0^\intercal \leftarrow \mathbb{Z}_q^{1\times m'}\end{pmatrix}\right)\right\}_{\lambda\in\mathbb{N}}$$

For the small-secret LWE assumption $\mathsf{sLWE}_{n.m,m',q,\sigma,\sigma'}$, the circular terms are removed from both distributions.

Assumption 3.13 (Evasive LWE). [Wee22, ARYY23] Let $n, m, t, m', q \in \mathbb{N}$ be parameters and λ be a security parameter. Let σ_{pre}, σ'_{pre}, σ_{post} and τ be parameters for Gaussian distributions. Let Samp be a PPT algorithm that outputs

$$\mathbf{S}\in\mathbb{Z}_q^{m'\times n}, \mathbf{P}\in\mathbb{Z}_q^{n\times t}, \mathsf{aux}\in\{0,1\}^*$$

on input 1^λ. For a PPT adversary $\mathcal{A}_0, \mathcal{A}_1$, we define the following advantage functions:

$$\mathsf{Adv}^{\mathsf{pre}}_{\mathcal{A}_0}(\lambda) \stackrel{\text{def}}{=} \Pr\left[\mathcal{A}_0(\mathbf{B},\mathbf{P},\mathbf{SB}+\mathbf{E},\mathbf{SP}+\mathbf{E}',\mathsf{aux})=1\right] - \Pr\left[\mathcal{A}_0(\mathbf{B},\mathbf{P},\mathbf{C}_0,\mathbf{C}',\mathsf{aux})=1\right]$$
$$\mathsf{Adv}^{\mathsf{post}}_{\mathcal{A}_1}(\lambda) \stackrel{\text{def}}{=} \Pr\left[\mathcal{A}_1(\mathbf{B},\mathbf{P},\mathbf{SB}+\mathbf{E}'',\mathbf{K},\mathsf{aux})=1\right] - \Pr[\mathcal{A}_1(\mathbf{B},\mathbf{P},\mathbf{C}_0,\mathbf{K},\mathsf{aux})=1]$$

$$\begin{aligned}\text{where}\quad & (\mathbf{S},\mathbf{P},\mathsf{aux})\leftarrow\mathsf{Samp}(1^\lambda),\ \ \mathbf{B}\leftarrow\mathbb{Z}_q^{n\times m},\ \ \mathbf{C}_0\leftarrow\mathbb{Z}_q^{m'\times m},\ \ \mathbf{C}'\leftarrow\mathbb{Z}_q^{m'\times t},\\ & \mathbf{E}\leftarrow\mathcal{D}^{m'\times m}_{\mathbb{Z},\sigma_{\mathsf{pre}}},\ \ \mathbf{E}'\leftarrow\mathcal{D}^{m'\times t}_{\mathbb{Z},\sigma'_{\mathsf{pre}}},\ \ \mathbf{E}''\leftarrow\mathcal{D}^{m'\times t}_{\mathbb{Z},\sigma_{\mathsf{post}}},\\ & \mathbf{K}\leftarrow\mathbf{B}^{-1}(\mathbf{P}) \text{ with standard deviation } \tau\end{aligned}$$

We say that the *evasive* LWE (EvLWE) assumption holds if for every PPT Samp and $\mathcal{A}_1$, there exists another PPT $\mathcal{A}_0$ and a polynomial $Q(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{pre}}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{\mathsf{post}}_{\mathcal{A}_1}(\lambda)/Q(\lambda) - \mathsf{negl}(\lambda).$$

We also consider a slight variant of the above, as is introduced by Wee [Wee22]. In this variant, $\mathsf{Samp}(1^\lambda)$ outputs $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$ along with $(\mathbf{S},\mathbf{P},\mathsf{aux})$. Furthermore, the adversary is given $\mathbf{A}$ and corresponding LWE challenge $\mathbf{c}_{\mathbf{A}}$ in the pre- and post-condition distributions. We have $\mathbf{c}_{\mathbf{A}}^\intercal = \mathbf{s}^\intercal\mathbf{A}+\mathbf{e}_{\mathbf{A}}^\intercal$ in the LHS distribution and $\mathbf{c}_{\mathbf{A}}\leftarrow\mathbb{Z}_q^m$ in the RHS distribution, where $\mathbf{e}_{\mathbf{A}}\leftarrow\mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{post}}}$ in post-condition and $\mathbf{e}_{\mathbf{A}}\leftarrow\mathcal{D}^m_{\mathbb{Z},\sigma''_{\mathsf{pre}}}$ in pre-condition.

Public versus Private Coin. Evasive LWE has been studied both in the "public-coin" and "private-coin" setting, where the former means that the randomness used by the sampler is made available to the adversary, and the latter means that the sampler's random coins need to be hidden from the adversary. Here, note that it is necessary that the LWE secret $\mathbf{S}$ and error remain hidden from the adversary, whether in the public or private coin setting. In the public-coin setting, these are generated randomly from the appropriate distribution and are the *only* secrets not known to the adversary, whereas in the private coin setting, there may be additional randomness that is not known to the adversary.

3.6 GSW Homomorphic Encryption and Evaluation

We recall the format of the (leveled fully) homomorphic encryption due to [GSW13] and the correctness property. We adapt the syntax from [HLL23].

Lemma 3.14. The leveled FHE scheme works as follows:

- The keys are

$$\text{(public)} \quad \mathbf{A}_{\mathsf{fhe}} = \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^{\intercal}\bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^{\intercal} \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}, \quad \text{(secret)} \quad \mathbf{s}^{\intercal} = (\bar{\mathbf{s}}^{\intercal}, -1),$$

  where $\bar{\mathbf{s}} \in \mathbb{Z}^n$,$\bar{\mathbf{A}}_{\mathsf{fhe}} \in \mathbb{Z}_q^{n\times m}$, and $\mathbf{e}_{\mathsf{fhe}}^{\intercal} \in \mathbb{Z}^m$.

- A ciphertext of $x \in \{0,1\}$ is $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - x\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m}$, where $\mathbf{R} \in \mathbb{Z}_q^{m\times m}$ is the encryption randomness. The decryption equation is

$$\mathbf{s}^{\intercal}\mathbf{X} = -\mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R} - x\mathbf{s}^{\intercal}\mathbf{G} \in \mathbb{Z}_q^m,$$

  which can be used to extract x via multiplication by $\mathbf{G}^{-1}(\lfloor q/2 \rfloor\, \iota_{n+1})$.

Lemma 3.15. (homomorphic evaluation for vector-valued functions [HLL23]) For the scheme in Lemma 4, there is an efficient algorithm

$$\text{MakeVEvalCkt}(n, m, q, C) = \mathsf{VEval}_C$$

that takes as input n, m, q and a vector-valued circuit $C : \{0,1\}^L \to \mathbb{Z}_q^{1\times m'}$ and outputs a circuit

$$\mathsf{VEval}_C(\mathbf{X}_1, ..., \mathbf{X}_L) = \mathbf{C},$$

taking L ciphertexts as input and outputting a new ciphertext $\mathbf{C}$ of different format.

- The depth of VEval_C is $dO(\log m \log\log q) + O(\log^2 \log q)$ for C of depth d.
- Suppose $\mathbf{X}_\ell = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_\ell - \mathbf{x}[\ell]\mathbf{G}$ for $\ell \in [L]$ with $\mathbf{x} \in \{0,1\}^L$, then

$$\mathbf{C} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_C - \begin{pmatrix} 0^{n\times m'} \\ C(\mathbf{x}) \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m'},$$

  where $\left\|\mathbf{R}_C^{\intercal}\right\| \le (m+2)^d \lceil \log q \rceil \max_{\ell\in[L]} \left\|\mathbf{R}_\ell^{\intercal}\right\|$. The new decryption equation is

$$\mathbf{s}^{\intercal}\mathbf{C} = -\mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_C + C(\mathbf{x}) \in \mathbb{Z}_q^{1\times m'}.$$

We implement the above homomorphic computation in the following specific manner. Let us represent each entry of $C(\mathbf{x})$ by an element in $[-\lfloor q/2 \rfloor, \lfloor q/2 \rfloor]$. We then let $C(\mathbf{x})[u,v] \in \{-1,0,1\}$ be the signed version of the v-th bit of $C(\mathbf{x})[u]$, for $u \in [m']$ and $v \in [0,w)$, $w = \lceil \log_2 q \rceil$. Namely, we have $\sum_{v\in[0,w)} C(\mathbf{x})[u,v]2^v = C(\mathbf{x})[u]$, where if $C(\mathbf{x})[u] \in [-\lfloor q/2 \rfloor, -1]$, then $C(\mathbf{x})[u,v] \in \{-1,0\}$ and $C(\mathbf{x})[u,v] \in \{0,1\}$ otherwise, for all u and v. Note that the parity of $C(\mathbf{x})[u]$ represented as an element in $[-\lfloor q/2 \rfloor, \lfloor q/2 \rfloor]$ equals to that of $C(\mathbf{x})[u,0]$.[10]

Then VEval_C computation firstly homomorphically computes GSW encryption of $C(\mathbf{x})[u,v]$, which is of the form $\mathbf{C}_{u,v} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C,u,v} - C(\mathbf{x})[u,v]\mathbf{G}$. This is done by first computing the GSW encryption of

[10] We do not have this equality when we do not represent $C(\mathbf{x})[u]$ in a signed form. This is because for an integer $x \in [-\lfloor q/2 \rfloor, -1]$, $x \bmod 2$ (i.e., the LSB of the signed form) does not equal to $x + q \bmod 2$ (i.e., the LSB of the non-signed form) when q is an odd number.

$C[\mathbf{x}]$ in non-signed binary form (i.e., $C[\mathbf{x}]$ is treated as an element in $[0, q-1]$ and is represented in a binary form) using the GSW homomorphic evaluation and adding the sign by the homomorphic operation. Then for each $u \in [m']$, it linearly aggregates $\{\mathbf{C}_{u,v}\}_{v\in[0,w-1]}$ to get $\mathbf{C}_u = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C,u} - \begin{pmatrix} 0^{n\times 1} \\ C(\mathbf{x})[u] \end{pmatrix}$ as $\mathbf{C}_u = \sum_v \mathbf{C}_{u,v}\mathbf{G}^{-1}(2^v \iota_{n+1})$. In particular,

$$\mathbf{R}_{C,u} = \sum_v \mathbf{R}_{C,u,v}\mathbf{G}^{-1}(2^v \iota_{n+1}), \text{ and } \mathbf{R}_C = (\mathbf{R}_{C,1}, \ldots, \mathbf{R}_{C,m'}).$$

3.7 Homomorphic Evaluation Procedures

In this section we describe the properties of the attribute encoding and its homomorphic evaluation. We adapt the syntax from [HLL23].

- For L-bit input, the public parameter is $\mathbf{A}_{\mathsf{att}} \in \mathbb{Z}_q^{(n+1)\times(L+1)m}$.
- The encoding of $\mathbf{x} \in \{0,1\}^L$ is

  $$\mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathbf{x}^\intercal) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal,$$

  where $\mathbf{s}^\intercal = (\bar{\mathbf{s}}^\intercal, -1)$ with $\bar{\mathbf{s}} \in \mathbb{Z}^n$ and $\mathbf{e}_{\mathsf{att}}^\intercal \in \mathbb{Z}^{(L+1)m}$.
- There are efficient deterministic algorithms [BTVW17]

  $$\mathsf{MEvalC}(\mathbf{A}_{\mathsf{att}}, C) = \mathbf{H}_C \quad \text{and} \quad \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{att}}, C, \mathbf{x}) = \mathbf{H}_{C,x}$$

  that take as input $\mathbf{A}_{\mathsf{att}}$, a matrix-valued circuit $C : \{0,1\}^L \to \mathbb{Z}_q^{n+1\times m'}$, and (for $\mathsf{MEvalCX}$) some $\mathbf{x} \in \{0,1\}^L$, and output some matrix in $\mathbb{Z}^{(L+1)m\times m'}$.
  - Suppose C is of depth d, then $\left\|\mathbf{H}_C^\intercal\right\|, \left\|\mathbf{H}_{C,\mathbf{x}}^\intercal\right\| \le (m+2)^d \lceil \log q \rceil$.
  - The matrix encoding homomorphism is $(\mathbf{A}_{\mathsf{att}} - (1, \mathbf{x}^\intercal) \otimes \mathbf{G})\mathbf{H}_{C,\mathbf{x}} = \mathbf{A}_{\mathsf{att}}\mathbf{H}_C - C(\mathbf{x})$.

Dual-Use Technique and Extension. In [BTVW17], the attribute encoded with secret $\mathbf{s}^\intercal$ is FHE ciphertexts under key $\mathbf{s}^\intercal$ (the same, "dual-use") and the circuit being $\mathsf{MEvalCX}$'ed is some HEval_C. This leads to automatic decryption. Let C be a vector-valued circuit, with co-domain $\mathbb{Z}_q^{1\times m'}$, then VEval_C is $\mathbb{Z}_q^{(n+1)\times m'}$-valued and

$$\begin{aligned} & (\mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal) \cdot \mathbf{H}_{\mathsf{VEval}_C,\mathbf{X}} \\ (\mathsf{MEvalCX}) \quad & = \mathbf{s}^\intercal \mathbf{A}_{\mathsf{att}} \mathbf{H}_{\mathsf{VEval}_C} - \mathbf{s}^\intercal \mathsf{VEval}_C(\mathbf{X}) + (\mathbf{e}')^\intercal \\ (\mathsf{VEval\ decryption}) \quad & = \mathbf{s}^\intercal \mathbf{A}_{\mathsf{att}} \mathbf{H}_{\mathsf{VEval}_C} - C(\mathbf{x}) + (\mathbf{e}'')^\intercal. \end{aligned}$$

3.8 Succinct LWE Sampler: Definition and Amplification

In this section, we define the succinct LWE sampler as in [DQV+21].

Syntax. A succinct LWE sampler is a tuple of PPT algorithms $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ with the following syntax:

$\mathsf{SampCRSGen}(1^\lambda, 1^N, \alpha)$**:** on input the security parameter λ, a size parameter N and a blowup factor α, samples a common reference string crs, which include parameters $\mathsf{params} = (q, M, K, \overline{\chi}, \overline{B})$.

$\mathsf{LWEGen}(\mathsf{crs})$**:** samples $(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*)$.

$\mathsf{Expand}(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*})$**:** is a deterministic algorithm that outputs a matrix $\mathbf{B}^*$.

Domains and Parameters. The outputs of LWEGen and Expand satisfy:

$$\mathbf{A}^* \in \mathbb{Z}_q^{M\times W}, \mathbf{S}^* \in \mathbb{Z}_q^{W\times K}, \mathbf{B}^* \in \mathbb{Z}_q^{M\times K}$$

for some integer W. We require that $N = MK$, $\overline{B} = \mathrm{poly}(N), \overline{\chi}$ is a $\overline{B}$-bounded noise distribution and $q \geq 8 \cdot 2^\lambda \cdot \alpha \cdot \overline{B}$.

Correctness. We require that

$$|\mathbf{B}^* - \mathbf{A}^*\mathbf{S}^*| := \beta \leq q/8$$

where $\mathsf{crs} \leftarrow \mathsf{SampCRSGen}(1^\lambda, 1^N, \alpha)$, $(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*) \leftarrow \mathsf{LWEGen}(\mathsf{crs})$ and $\mathbf{B}^* = \mathsf{Expand}(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*})$. Furthermore, we require that $\mathbf{A}^*$ is full-rank with overwhelming probability over the randomness of $\mathsf{SampCRSGen}$ and LWEGen.

δ-Succinctness. We require the total bit length of the output of LWEGen is small. That is

$$\mathsf{bitlength}(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*) \leq N^\delta \cdot \mathrm{poly}(\lambda, \log q) = (MK)^\delta \cdot \mathrm{poly}(\lambda, \log q)$$

where $\delta < 1$ is a constant.

Definition 3.16 (LWE with respect to $\mathbf{A}^*$). We require that

$$(\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{A}^*\mathbf{s}' + \mathbf{e}') \approx_c (\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{b})$$

where $\mathsf{crs} = \mathsf{SampCRSGen}(1^\lambda, 1^N, \alpha; \mathsf{coins}_{\mathsf{crs}})$, $(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*) \leftarrow \mathsf{LWEGen}(\mathsf{crs}; \mathsf{coins}_{\mathsf{seed}})$, $\mathbf{s}' \leftarrow \mathbb{Z}_q^W$ and $\mathbf{e}' \leftarrow \overline{\chi}^M$.

Definition 3.17 (Strong security or strong β_0-Flooding). Let D_0, D_1 be any two polynomial-time samplable distributions such that $(\mathsf{aux}_b, \mathbf{Z}_b) \leftarrow D_b(\mathbf{A}^*)$ satisfies $\mathbf{Z}_b \in \mathbb{Z}_q^{M\times K}$, $|\mathbf{Z}_b| \leq \beta_0$ where $\beta_0 \cdot 2^\lambda \leq \beta$ and

$$(\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{A}^*\mathbf{S}' + \mathbf{Z}_0, \mathsf{aux}_0) \approx_c (\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{A}^*\mathbf{S}' + \mathbf{Z}_1, \mathsf{aux}_1)$$

where $\mathsf{crs} = \mathsf{SampCRSGen}(1^\lambda, 1^N, \alpha; \mathsf{coins}_{\mathsf{crs}})$, $(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*) \leftarrow \mathsf{LWEGen}(\mathsf{crs}; \mathsf{coins}_{\mathsf{seed}})$, and $\mathbf{S}' \leftarrow \mathbb{Z}_q^{W\times K}$. Then,

$$(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{A}^*\mathbf{S}^* + \mathbf{Z}_0, \mathsf{aux}_0) \approx_c (\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{A}^*\mathbf{S}^* + \mathbf{Z}_1, \mathsf{aux}_1).$$

We will refer to the assumption on D_0, D_1 as the pre-condition for security, and the resulting indistinguishability the post-condition.

Definition 3.18 (Weak security or weak β_0-Flooding). Let D_0, D_1 as follows.

$$D_b: \qquad \mathsf{aux}_b = (\hat{\mathbf{B}} := \mathbf{A}^*\hat{\mathbf{S}} + \hat{\mathbf{E}}, \quad \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - b \cdot \mathbf{G})$$

$$\mathbf{Z}_b = \mathbf{E}\mathbf{G}^{-1}(\hat{\mathbf{B}}) - b\hat{\mathbf{E}},$$

where

- $\mathsf{SampCRSGen}$ defines $(q, M, K, \overline{\chi}, \overline{B}) = \mathsf{params}$;
- LWEGen defines $\mathbf{A}^* \in \mathbb{Z}_q^{M\times W}$;
- $\hat{\mathbf{B}} \in \mathbb{Z}_q^{M\times K}, \hat{\mathbf{S}} \leftarrow \mathbb{Z}_q^{W\times K}$ and $\hat{\mathbf{E}} \leftarrow [-B_{\mathsf{flood}}, B_{\mathsf{flood}}]^{M\times K}$ where $B_{\mathsf{flood}} = (\beta_0 + \overline{B}) \cdot 2^\lambda$;

- $\mathbf{C} \in \mathbb{Z}_q^{M \times M \log q}$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{W \times M \log q}$ and $\mathbf{E} \leftarrow \overline{\chi}_q^{M \times M \log q}$.

We say that the sampler $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ is weakly secure if

$$(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{A}^*\mathbf{S}^* + \mathbf{Z}_0, \mathsf{aux}_0) \approx_c (\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{A}^*\mathbf{S}^* + \mathbf{Z}_1, \mathsf{aux}_1).$$

Remark 3.19 (Alternate formulation of strong and weak security). Since the sampler allows us to compute $\mathsf{Expand}(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}) = \mathbf{B}^* = \mathbf{A}^*\mathbf{S}^* + \mathbf{E}^*$, the security post-condition can be equivalently stated as:

$$(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{Z}_0, \mathsf{aux}_0) \approx_c (\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{Z}_1, \mathsf{aux}_1). \tag{10}$$

Theorem 3.20. [DQV+21] Let $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ be a weakly secure, δ-succinct LWE sampler (Definition 3.18) and $M^2 \leq N^\delta \mathrm{poly}(\lambda, \log q)$. There exists an amplifier that amplifies $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ to a secure δ-succinct LWE sampler $(\overline{\mathsf{SampCRSGen}}, \overline{\mathsf{LWEGen}}, \overline{\mathsf{Expand}})$, satisfying strong security (Definition 3.17) with the parameters of Definition 3.18.

Theorem 3.21 ([DQV+21]). Let $\mathcal{F}_{\ell,N,d} = \{f : \{0,1\}^\ell \to \{0,1\}^N\}$ of depth-d circuits. Let $g(d) = O(d)$. Suppose there exists a succinct LWE sampler $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ satisfying δ succinctness and β_0-flooding (Definition 3.17) with $\beta_0 = \overline{B} N^{g(d)}$ and $M^2 = N^\delta \mathrm{poly}(\lambda, \ell, d)$ for $M, \overline{B}$ defined in SLS. Then there exists a succinct randomized encoding scheme (SRE) for $\mathcal{F}_{\ell,N,d}$ satisfying δ-succinctness.

Theorem 3.22 ([AJ15, BV15, LPST16]). Assuming sub-exponentially secure succinct randomized encoding (SRE) exist and subexponentially secure LWE, there exists an $i\mathcal{O}$ scheme.

4 Counter-Examples for Public-Coin Evasive LWE

4.1 Counter-Example for HLL's Circular Evasive LWE

We first recall the assumption from [HLL23].

Assumption 4.1 (Evasive Circular Small-Secret LWE). Let n, m, m', J, q be parameters. Let $\mathsf{Samp}(1^\lambda; \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}})$ be a public coin sampler that, given randomness $\mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}$, outputs

$$\mathbf{A}_{\mathsf{circ}} \in \mathbb{Z}_q^{(n+1)\times(L_{\mathbf{S}}+1)m},\ \overline{\mathbf{A}}' \in \mathbb{Z}_q^{n\times m'},\ \mathbf{P} \in \mathbb{Z}_q^{n\times J},\ \sigma,\ \sigma',\ \sigma_{-1},\ \sigma_{\mathsf{post}},\ \sigma_{\mathsf{pre}}, \mathsf{aux}$$

where $m \geq O(n \log q)$, $\sigma_{-1} = \omega(\sqrt{n \log q \log m})$ and $\sigma_{\mathsf{post}} \geq \sigma_{\mathsf{pre}}$. Suppose

$$\overline{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m},\ (\mathbf{B}, \mathbf{B}_{\sigma_{-1}}^{-1}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q),\ \mathbf{K} \leftarrow \mathbf{B}_{\sigma_{-1}}^{-1}(\mathbf{P}),$$

$$\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma,\leq\sigma\sqrt{\lambda}},\ \mathbf{e}_{\mathsf{circ}} \leftarrow \mathcal{D}^{(L_{\mathbf{S}}+1)m}_{\mathbb{Z},\sigma',\leq\sigma'\sqrt{\lambda}},\ \mathbf{e}' \leftarrow \mathcal{D}^{m'}_{\mathbb{Z},\sigma',\leq\sigma'\sqrt{\lambda}},\ \mathbf{e}_{\mathbf{B}} \in \mathbb{Z}^m,\ \mathbf{e}_{\mathbf{P}} \in \mathbb{Z}^J,$$

$$\mathbf{r} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma,\leq\sigma\sqrt{\lambda}},\ \mathbf{R} \leftarrow \{0,1\}^{m\times((n+1)\lceil\log_2 q\rceil+1)m}, \mathbf{A}_{\mathsf{fhe}} = \left(\begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{r}^\intercal \overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^\intercal \end{pmatrix}\right)$$

$$\mathbf{s} = (\mathbf{r}^\intercal, -1)^\intercal,\ L_{\mathbf{S}} = (n+1)((n+1)\lceil\log q\rceil + 1)m\lceil\log q\rceil$$

where $\mathbf{p}_i$ is the ith column of $\mathbf{P}$. In the precondition, the entries of $\mathbf{e}_\mathbf{B}, \mathbf{e}_\mathbf{P}$ are independent and follow $\mathcal{D}_{\mathbb{Z},\sigma_{\mathsf{pre}},\leq\sigma_{\mathsf{pre}}\sqrt{\lambda}}$ and $\mathsf{evcsLWE}^{\mathsf{Samp}}_{\mathsf{pre}}$ states that

$$D_0^{\mathsf{pre}} := \left\{ \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{r}^\intercal \overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}}, \\ \mathbf{S} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{circ}}, \\ (\mathbf{c}')^\intercal = \mathbf{r}^\intercal \overline{\mathbf{A}}' + (\mathbf{e}')^\intercal, \mathbf{c}^\intercal_{\mathbf{B}} = \mathbf{r}^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \\ \mathbf{c}^\intercal_{\mathbf{P}} = \mathbf{r}^\intercal \mathbf{P} + \mathbf{e}^\intercal_{\mathbf{P}} \end{array} \right) \right\}_{\lambda\in\mathbb{N}}$$

$$\approx_c \; D_1^{\mathsf{pre}} := \left\{ \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{1\times m}, \\ \mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^{1\times(L_\mathbf{S}+1)m}, \\ (\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times m'}, \mathbf{c}^\intercal_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{1\times m}, \\ \mathbf{c}^\intercal_{\mathbf{P}} \leftarrow \mathbb{Z}_q^{1\times J} \end{array} \right) \right\}_{\lambda\in\mathbb{N}} \tag{11}$$

In the postcondition, the entries of $\mathbf{e}_\mathbf{B}$, are independent and follow $\mathcal{D}_{\mathbb{Z},\sigma_{\mathsf{post}},\leq\sigma_{\mathsf{post}}\sqrt{\lambda}}$ and $\mathsf{evcsLWE}^{\mathsf{Samp}}_{\mathsf{post}}$ states that

$$D_0^{\mathsf{post}} := \left\{ \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{r}^\intercal \overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}}, \\ \mathbf{S} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{circ}}, \\ (\mathbf{c}')^\intercal = \mathbf{r}^\intercal \overline{\mathbf{A}}' + (\mathbf{e}')^\intercal, \mathbf{c}^\intercal_{\mathbf{B}} = \mathbf{r}^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \; \mathbf{K} \end{array} \right) \right\}_{\lambda\in\mathbb{N}}$$

$$\approx_c \; D_1^{\mathsf{post}} := \left\{ \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{1\times m}, \\ \mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^{1\times(L_\mathbf{S}+1)m}, \\ (\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times m'}, \mathbf{c}^\intercal_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{1\times m}, \; \mathbf{K} \end{array} \right) \right\}_{\lambda\in\mathbb{N}} \tag{12}$$

The *evasive circular small-secret LWE assumption* states that $\mathsf{evcsLWE}^{\mathsf{Samp}}_{\mathsf{pre}}$ implies $\mathsf{evcsLWE}^{\mathsf{Samp}}_{\mathsf{post}}$ for all efficient sampler Samp.

Note 4.2. The above definition of evasive circular small secret LWE is slightly different from that in [HLL23], where $\mathbf{S}$ encrypts $\mathsf{bits}(\mathbf{s})$ and $\mathbf{c}^\intercal_{\mathsf{circ}}$ is computed as $\mathbf{r}^\intercal(\overline{\mathbf{A}}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \overline{\mathbf{G}}) + \mathbf{e}^\intercal_{\mathsf{circ}}$. However, it is easy to see that the two forms are equivalent, because given $\mathbf{A}_{\mathsf{fhe}}$, $\overline{\mathbf{A}}_{\mathsf{circ}}$, one can sample $\mathbf{R}' \leftarrow \{0,1\}^{m\times m}$, $\mathbf{a}_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^{(L_\mathbf{S}+1)m}$ and compute the extra block in $\mathbf{S}$ as $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}' - \mathbf{G}$, and the extra additive term in $\mathbf{c}^\intercal_{\mathsf{circ}}$ as: $-(\mathbf{a}^\intercal_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \underline{\mathbf{G}})$. Here, $\overline{\mathbf{G}}$ and $\underline{\mathbf{G}}$ represent the top n and the lat rows of $\mathbf{G}$, respectively.

4.1.1 Preliminaries for the attack

We will use the following lemmas adapted from [HJL21] to GSW encryption.

Lemma 4.3 (Even-randomness gate for GSW). Let q be an odd number and $\mathsf{ct}_x = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - x\mathbf{G}$ be a GSW encryption of some $x \in \{0,1\}$, where $\mathbf{A}_{\mathsf{fhe}}$ is the public key, $|\mathbf{R}[i,j]| \leq B$ for some $B \leq q/(100m)$ and let ct'_x be the result of homomorphically evaluating the following two (arithmetic) gates:

1. $g_1(x) = \frac{1}{2}x$ and $\mathsf{Eval}(g_1, \mathsf{ct}_x) = \mathsf{ct}_x \cdot \mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right)$.
2. $g_2(x) = x + x$ and $\mathsf{Eval}(g_2, \mathsf{ct}_x) = \mathsf{ct}_x + \mathsf{ct}_x$,

where ct_x is treated as a matrix in $\mathbb{Z}_q^{(n+1)\times m}$.[11] That is, $\mathsf{ct}'_x = \mathsf{Eval}(g_2, \mathsf{Eval}(g_1, \mathsf{ct}_x))$. Then $\mathsf{ct}'_x = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}' - x\mathbf{G}$ for some $\mathbf{R}' \in \mathbb{Z}_q^{m\times m}$ (here $m = O(n \log q)$) for which every entry satisfies $\mathbf{R}'[i,j] = 2 \cdot r_{i,j}$ for some $r_{i,j} \in \mathbb{Z}_q$ and $i,j \in [m]$ with $|r_{i,j}| \leq O(mB)$.

Proof. We first expand $\mathsf{Eval}(g_1, \mathsf{ct}_x)$.

$$\begin{aligned}\mathsf{Eval}(g_1, \mathsf{ct}_x) &= (\mathbf{A}_{\mathsf{fhe}}\mathbf{R} - x\mathbf{G}) \cdot \mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right) = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right) - x\mathbf{G}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right) \\ &= \mathbf{A}_{\mathsf{fhe}}\left(\mathbf{R}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right)\right) - \frac{x}{2}\mathbf{G}.\end{aligned}$$

$$\begin{aligned}\text{Then,}\quad \mathsf{Eval}(g_2, \mathsf{Eval}(g_1, \mathsf{ct}_x)) &= \mathbf{A}_{\mathsf{fhe}}\left(\mathbf{R}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right)\right) - \frac{x}{2}\mathbf{G} + \mathbf{A}_{\mathsf{fhe}}\left(\mathbf{R}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right)\right) - \frac{x}{2}\mathbf{G} \\ &= \mathbf{A}_{\mathsf{fhe}}\left(2 \cdot \mathbf{R}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right)\right) - x\mathbf{G}\end{aligned}$$

Note that $\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right) \in \{0,1\}^{m\times m}$, hence $\left|\left(\mathbf{R}\mathbf{G}^{-1}\left(\frac{1}{2}\mathbf{G}\right)\right)[i,j]\right| \leq O(Bm)$. □

Lemma 4.4 (Multiplication-by-one gate for GSW). Let $\mathsf{ct}^* = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}^* - \mathbf{G}$ be a GSW encryption for constant 1, where $|\mathbf{R}^*[i,j]| \leq q/10$ for all $i,j \in [m]$. Let $x \in \{-1,0,1\}$, and let $\mathsf{ct}_x = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - x\mathbf{G}$ be the GSW encryption of x such that $\mathbf{R}[i,j] = 2 \cdot r_{i,j}$ where $r_{i,j} \in \mathbb{Z}$ and $|r_{i,j}| \leq q/(100m)$, for all $i,j \in [m]$. Let $g(x,y) = x \cdot y$. Then $\mathsf{Eval}(g, \mathsf{ct}_x, \mathsf{ct}^*) = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}' - x \cdot \mathbf{G}$[12] where $\mathbf{R}' \in \mathbb{Z}_q^{m\times m}$ and $\mathbf{R}' = x \cdot \mathbf{R}^* \bmod 2$.

Proof. On expanding,

$$\begin{aligned}\mathsf{Eval}(g, \mathsf{ct}_x, \mathsf{ct}^*) &= -(\mathbf{A}_{\mathsf{fhe}}\mathbf{R} - x\mathbf{G})\mathbf{G}^{-1}(\mathbf{A}_{\mathsf{fhe}}\mathbf{R}^* - \mathbf{G}) \\ &= \mathbf{A}_{\mathsf{fhe}}(-\mathbf{R}\mathbf{G}^{-1}(\mathbf{A}_{\mathsf{fhe}}\mathbf{R}^* - \mathbf{G}) + x\mathbf{R}^*) - x \cdot \mathbf{G}\end{aligned}$$

Now, firstly, we note that each entry, $\mathbf{R}\mathbf{G}^{-1}(\mathbf{A}_{\mathsf{fhe}}\mathbf{R}^* - \mathbf{G})[i,j]$ is small, i.e., $\leq (q/(100m)) * m = q/100$. Further we observe that since each entry $\mathbf{R}[i,j]$ is even, $\mathbf{R}\mathbf{G}^{-1}(\mathbf{A}_{\mathsf{fhe}}\mathbf{R}^* - \mathbf{G})[i,j] = 0 \bmod 2, \forall\, i,j \in [m]$. Hence, we have $\mathbf{R}' = x \cdot \mathbf{R}^* \bmod 2$. □

Corollary 4.5. Let $\mathsf{ct}^* = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}^* - \mathbf{G}$ be a GSW encryption of the constant 1, where $|\mathbf{R}^*[i,j]| \leq q/10$ for all $i,j \in [m]$. Let $x \in \{-1,0,1\}$ and let $\mathsf{ct}_x = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - x\mathbf{G}$ be a GSW encryption of x such that $|\mathbf{R}[i,j]| \leq q/\mathrm{poly}(n, \log q)$ for all i,j. Then, for g_1, g_2 as in Lemma 4.3 and g as in Lemma 4.4,

$$\mathsf{Eval}(g, \mathsf{Eval}(g_2, \mathsf{Eval}(g_1, \mathsf{ct}_x)), \mathsf{ct}^*) = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}' - x\mathbf{G},$$

where $\mathbf{R}' = x\mathbf{R}^* \bmod 2$.

[11] Here, we specify the homomorphic evaluation circuit concretely, since there are multiple different homomorphic evaluation circuits implementing the same operation on the encoded message.

[12] Here the GSW multiplicative homomorphism is computed by $-\mathbf{C}_1\mathbf{G}^{-1}(\mathbf{C}_2)$ where $\mathbf{C}_1$ and $\mathbf{C}_2$ encrypts x_1 and x_2 respectively.

4.1.2 The Attack

Theorem 4.6. There exists an efficient evasive circular small-secret LWE (evcsLWE) sampler Samp as defined in Assumption 4.1 such that the pre-condition holds, but the post-condition does not- i.e., there exists a distinguisher $\mathcal{A}^{\mathsf{post}}$ that distinguishes post-condition with non-negligible probability.

Proof. We first describe the *contrived* circuit used by our sampler. Let $q, p, \tilde{\beta}, B, \sigma, \sigma', \sigma_{-1}, \sigma_{\mathsf{pre}}, \sigma_{\mathsf{post}}, Q$ be parameters. The parameters will be set after we describe the sampler.

Defining Evasive Circular small-secret LWE Sampler. The public coin sampler Samp of the evcsLWE assumption, on input $(1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}} = (\mathsf{coins}, \overline{\mathbf{A}}_{\mathsf{circ}}, \overline{\mathbf{A}}'))$, does the following:

1. Let $\mathcal{F}_{\mathsf{prm}} = \{f : \{1 \in \{0,1\}\} \times \mathbb{Z}^{n+1} \to [-q/2 + B, q/2 - B]^{1\times\ell}\}$ be a family of functions where $f \in \mathcal{F}_{\mathsf{prm}}$ can be computed by a circuit of depth $d(\lambda)$, $\mathsf{prm} = (n, 1^{\ell(\lambda)}, 1^{d(\lambda)})$ and B is chosen to be exponentially smaller than $q/2$. Choose $\{f_i \in \mathcal{F}_{\mathsf{prm}}\}_{i\in[Q]}$ such that for $\mathbf{r} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma,\le\sigma\sqrt{\lambda}}$, $\mathbf{s}^\intercal = (\mathbf{r}^\intercal, -1)$,

$$\left(\begin{array}{r} 1^\lambda, \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \end{pmatrix}, \\ \mathbf{C} = \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \end{pmatrix}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s}))\otimes\mathbf{G}, \\ \begin{pmatrix} \overline{\mathbf{A}}_0 \\ \mathbf{c}^\intercal_0 = \mathbf{r}^\intercal\overline{\mathbf{A}}_0 + \mathbf{e}^\intercal_0 \end{pmatrix}, \\ \{f_i, \mathbf{c}^\intercal_i = f_i(1,\mathbf{s})\}_{i\in[Q]} \end{array}\right) \approx_c \left(\begin{array}{r} 1^\lambda, \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}^\intercal_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{1\times m} \end{pmatrix}, \\ \mathbf{C} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}, \\ \begin{pmatrix} \overline{\mathbf{A}}_0 \\ \mathbf{c}^\intercal_0 \leftarrow \mathbb{Z}_q^{1\times m'} \end{pmatrix}, \\ \{f_i, \mathbf{c}^\intercal_i \leftarrow \mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]} \end{array}\right) \tag{13}$$

where $\overline{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\overline{\mathbf{A}}_0 \leftarrow \mathbb{Z}_q^{n\times m'}$, $\mathbf{R} \leftarrow \{0,1\}^{m\times((n+1)\lceil\log_2 q\rceil+1)m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma,\le\sigma\sqrt{\lambda}}$, $\mathbf{e}_0 \leftarrow \mathcal{D}^{m'}_{\mathbb{Z},\sigma',\le\sigma'\sqrt{\lambda}}$. A concrete example of the choice for such f_i would be to index f_i with a random matrix $\mathbf{A}_i \leftarrow \mathbb{Z}_q^{(n+1)\times\ell'}$ and define $f_i(1,\mathbf{s})$ as follows. Ignore the first bit, 1, and compute $\lfloor\mathbf{s}^\intercal\mathbf{A}_i\rceil_p$ in binary and interpret it as a vector in $\mathbb{Z}_q^\ell$. Finally, map each such element $x \in \mathbb{Z}_q$ (in the output vector) such that $x \notin [-q/2 + B, q/2 - B]$ to 0. Here, $\ell' = \lceil\ell(\lceil\log q\rceil / \lceil\log p\rceil)\rceil$ and $q \ge p\lambda^{\omega(1)}\sigma$ (σ is LWE error bound and is defined later). Concretely, $f_i(1,\mathbf{s}) = [\mathbf{G}_q\mathbf{G}_p^{-1}(\lfloor(\mathbf{s}^\intercal\mathbf{A}_i)^\intercal\rceil_p)]_B$[13], where $\mathbf{G}_q = \mathbf{I}_\ell \otimes (1, 2, 2^2, \ldots, 2^{\lceil\log_2 q\rceil-1})$ and $\mathbf{G}_p^{-1}(x \in \mathbb{Z}_p)$ represents bit decomposition of x, resulting in a vector in $\{0,1\}^{\lceil\log p\rceil}$ (similarly for a vector), and $[\mathbf{x}]_B$ for any $\mathbf{x} \in \mathbb{Z}_q^*$ represents truncating the range to $[-q/2 + B, q/2 - B]^*$ by mapping the out of range values to 0. In Lemma 4.7, we show that indistinguishability in (13) indeed holds for this choice of f_i. We observe that such a function f_i can be implemented by a circuit of depth $d(\lambda) = \mathrm{poly}(\log q)$. Also, we include these matrices, $\{\mathbf{A}_i\}_{i\in[Q]}$, as a part of $\mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}$. Define the following circuit C'_{f_i} (with depth at most $d + 3$) implementing f_i.

   (a) Start with any circuit C_{f_i} (of depth at most d) outputting $f_i(1,\mathbf{s})$ (in binary) on input $(1,\mathbf{s})$.

   (b) Let C_0 be a circuit which outputs the first bit of its input $\mathbf{x}$. We further assume that the first bit of $\mathbf{x}$ is always 1.

[13] to keep the notations simple, we set q and p in such a way that $\ell(\lceil\log q\rceil / \lceil\log p\rceil)$ is an integer.

(c) To the output wire of C_{f_i} corresponding to the lowest-order bit of $f_i(1,\mathbf{s})[1]$, attach a new gate which performs the correlation-inducing transformation described in Corollary 4.5, using the output wire of C_0 as the special "1" input. Inputs to C_0 can be $(1, \mathsf{bits}(\mathbf{s}))$.

(d) To all the other output wires of C_{f_i}, attach a gate performing "even randomness" transformation as in Lemma 4.3.

2. Samples $\mathbf{a}_{\mathsf{circ}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times(L_{\mathbf{S}}+1)m}$ and set $\mathbf{A}_{\mathsf{circ}} = \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{circ}} \\ \mathbf{a}_{\mathsf{circ}}^{\mathsf{T}} \end{pmatrix}$.

3. Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{f_i}} = \mathsf{MakeVEvalCkt}(n,m,q,C'_{f_i})$. Compute $\mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}}} = \mathsf{MEvalC}(\mathbf{A}_{\mathsf{circ}}, \mathsf{VEval}_{C'_{f_i}}) \in \mathbb{Z}_q^{(L_{\mathbf{S}}+1)m\times\ell}$ for all $i \in [Q]$. It then computes $\mathbf{A}_{f_i} = \mathbf{A}_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}}} \in \mathbb{Z}_q^{n+1\times\ell}$ for all $i \in [Q]$ and sets $\mathbf{P} = [\overline{\mathbf{A}}_{f_1}, \ldots, \overline{\mathbf{A}}_{f_Q}]$, where $\overline{\mathbf{A}}_{f_i}$ is the matrix formed by taking upper n rows of $\mathbf{A}_{f_i}$.

4. Output
$$\mathbf{A}_{\mathsf{circ}},\ \overline{\mathbf{A}}',\ \mathbf{P} \in \mathbb{Z}_q^{n\times\ell\cdot Q}, \mathsf{aux} = (\{f_i\}_{i\in[Q]}), \sigma,\ \sigma',\ \sigma_{-1},\ \sigma_{\mathsf{post}},\ \sigma_{\mathsf{pre}}$$
where $\sigma,\ \sigma',\ \sigma_{-1},\ \sigma_{\mathsf{post}},\ \sigma_{\mathsf{pre}}$ are as defined later in parameter settings.

Proof of Equation (13).

Claim 4.7. Let $\{f_{\mathbf{A}_i} \in \mathcal{F}_{\mathsf{prm}}\}_{i\in[Q]}$ be a set of functions such that $f_{\mathbf{A}_i}(1,\mathbf{s}) = [\mathbf{G}_q\mathbf{G}_p^{-1}(\lfloor(\mathbf{s}^{\mathsf{T}}\mathbf{A}_i)^{\mathsf{T}}\rfloor_p)]_B$, for all $i \in [Q]$; $\mathbf{r} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma,\le\sigma\sqrt{\lambda}}$, $\mathbf{s}^{\mathsf{T}} = (\mathbf{r}^{\mathsf{T}}, -1)$. Then, for all PPT adversary $\mathcal{A}$, the indistinguishability in equation (13) holds assuming the hardness of circular small secret LWE (csLWE) assumption.

Proof. We rewrite equation (13) here, with the above definition of f_i's.[14]

$$D_0 := \left(\begin{array}{r} 1^\lambda, \left(\begin{matrix}\overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}_{\mathsf{fhe}}^{\mathsf{T}} = \mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\end{matrix}\right), \\ \mathbf{C} = \left(\begin{matrix}\overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}_{\mathsf{fhe}}^{\mathsf{T}} = \mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\end{matrix}\right)\mathbf{R} - (1,\mathsf{bits}(\mathbf{s}))\otimes\mathbf{G}, \\ \left(\begin{matrix}\overline{\mathbf{A}}_0 \\ \mathbf{c}_0^{\mathsf{T}} = \mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_0 + (\mathbf{e}')^{\mathsf{T}}\end{matrix}\right), \\ \{\begin{pmatrix}\overline{\mathbf{A}}_i \\ \mathbf{a}_i^{\mathsf{T}}\end{pmatrix}, \mathbf{c}_i^{\mathsf{T}} = [\mathbf{G}_q\mathbf{G}_p^{-1}(\lfloor(\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}})^{\mathsf{T}}\rfloor_p)]_B\}_{i\in[Q]} \end{array}\right) \approx_c D_1 := \left(\begin{array}{r} 1^\lambda, \left(\begin{matrix}\overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}_{\mathsf{fhe}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times m}\end{matrix}\right), \\ \mathbf{C} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}, \\ \left(\begin{matrix}\overline{\mathbf{A}}_0 \\ \mathbf{c}_0^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times m'}\end{matrix}\right), \\ \{\begin{pmatrix}\overline{\mathbf{A}}_i \\ \mathbf{a}_i^{\mathsf{T}}\end{pmatrix}, \mathbf{c}_i^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]} \end{array}\right),$$

where $\overline{\mathbf{A}}_i \leftarrow \mathbb{Z}_q^{n\times\ell'}$ and $\mathbf{a}_i \leftarrow \mathbb{Z}_q^{\ell'}$. Let us define an intermediate distribution D' between D_0 and D_1, where $\mathbf{c}_i^{\mathsf{T}} = [\mathbf{G}_q\mathbf{G}_p^{-1}(\lfloor\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}} + \mathbf{e}_i^{\mathsf{T}}\rfloor_p)]_B$, for $\mathbf{e}_i \leftarrow \mathcal{D}^{\ell'}_{\mathbb{Z},\sigma,\sigma\sqrt{\lambda}}$. Then D_0 and D' are statistically indistinguishable because of the following arguments. First we observe that since $\mathbf{a}_i \leftarrow \mathbb{Z}_q^{\ell'}$, $\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}}$ is also uniformly distributed over $\mathbb{Z}_q^{1\times\ell'}$. Then we observe that since $\mathbf{e}_i \leftarrow \mathcal{D}^{\ell'}_{\mathbb{Z},\sigma,\sigma\sqrt{\lambda}}$, $\|\mathbf{e}_i\| \le \sigma\sqrt{\lambda}$, and hence,

$$\Pr\left(\lfloor\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}}\rfloor_p \neq \lfloor\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}} + \mathbf{e}_i^{\mathsf{T}}\rfloor_p\right) \le \sigma\sqrt{\lambda}p/q = \mathsf{negl}(\lambda) \text{ due to the choice of } p \text{ and } q.$$

Thus, probability that $(\lfloor\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}}\rfloor_p \neq \lfloor\mathbf{r}^{\mathsf{T}}\overline{\mathbf{A}}_i - \mathbf{a}_i^{\mathsf{T}} + \mathbf{e}_i^{\mathsf{T}}\rfloor_p)$, for any $i \in [Q]$ is at most $Q\sigma\sqrt{\lambda}p/q$, which is again negligible.

[14] With slight overload of notation, we denote $f_{\mathbf{A}_i}$ as $\begin{pmatrix}\overline{\mathbf{A}}_i \\ \mathbf{a}_i^{\mathsf{T}}\end{pmatrix}$.

Next, we show that if there exists an adversary $\mathcal{A}$ who can distinguish between D' and D_1 with non-negligible advantage, then there is a reduction $\mathcal{B}$ that breaks csLWE security with non-negligible advantage. The reduction is as follows.

1. On receiving 1^λ from $\mathcal{A}$, forward it to csLWE challenger.
2. The csLWE challenger samples $\beta \leftarrow \{0,1\}$, $\overline{\mathbf{A}}_{\mathsf{fhe},\mathsf{csLWE}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\overline{\mathbf{A}}_{0,\mathsf{csLWE}} \leftarrow \mathbb{Z}_q^{n\times m'+\ell' Q}$, $\mathbf{r} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma,\le\sigma\sqrt{\lambda}}$, and returns
$$\left(1^\lambda, \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe},\mathsf{csLWE}}\\ \mathbf{c}^\intercal_{\mathsf{fhe},\mathsf{csLWE}}\end{pmatrix}, \mathbf{C}_{\mathsf{csLWE}}, \begin{pmatrix}\overline{\mathbf{A}}_{0,\mathsf{csLWE}}\\ \mathbf{c}^\intercal_{0,\mathsf{csLWE}}\end{pmatrix}\right),$$
where $\mathbf{c}^\intercal_{\mathsf{fhe},\mathsf{csLWE}} = \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe},\mathsf{csLWE}} + \mathbf{e}^\intercal_{\mathsf{fhe},\mathsf{csLWE}}$, $\mathbf{C}_{\mathsf{csLWE}} = \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe},\mathsf{csLWE}}\\ \mathbf{c}^\intercal_{\mathsf{fhe},\mathsf{csLWE}} = \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe},\mathsf{csLWE}} + \mathbf{e}^\intercal_{\mathsf{fhe},\mathsf{csLWE}}\end{pmatrix}\mathbf{R} - \mathsf{bits}(\mathbf{s})\otimes\mathbf{G}$, and $\mathbf{c}^\intercal_{0,\mathsf{csLWE}} = \mathbf{r}^\intercal\overline{\mathbf{A}}_{0,\mathsf{csLWE}} + \mathbf{e}^\intercal_{0,\mathsf{csLWE}}$, if $\beta = 0$, and $\mathbf{c}^\intercal_{\mathsf{fhe},\mathsf{csLWE}} \leftarrow \mathbb{Z}_q^{1\times m}$, $\mathbf{c}^\intercal_{0,\mathsf{csLWE}} \leftarrow \mathbb{Z}_q^{1\times m'+\ell' Q}$ and $\mathbf{C}_{\mathsf{csLWE}} \leftarrow \mathbb{Z}_q^{(n+1)\times(n+1)\lceil\log_2 q\rceil m}$, if $\beta = 1$. Then $\mathcal{B}$ does the following:
   (a) Parse $\overline{\mathbf{A}}_{0,\mathsf{csLWE}} = (\overline{\mathbf{A}}_0, \overline{\mathbf{A}}_1, \ldots, \overline{\mathbf{A}}_Q)$ where $\overline{\mathbf{A}}_0 \in \mathbb{Z}_q^{n\times m'}$ and $\overline{\mathbf{A}}_i \in \mathbb{Z}_q^{n\times\ell'}$ for all $i \in [Q]$. Also, parse $\mathbf{c}^\intercal_{0,\mathsf{csLWE}} = (\mathbf{c}^\intercal_0, \mathbf{c}^\intercal_1, \ldots, \mathbf{c}^\intercal_Q)$ where $\mathbf{c}^\intercal_0 \in \mathbb{Z}_q^{1\times m'}$ and $\mathbf{c}^\intercal_i \in \mathbb{Z}_q^{1\times\ell'}$ for all $i \in [Q]$.
   (b) For all $i \in [Q]$, sample $\mathbf{a}^\intercal_i \leftarrow \mathbb{Z}_q^{1\times\ell'}$ and set $\tilde{\mathbf{c}}^\intercal_i = \mathbf{c}^\intercal_i - \mathbf{a}^\intercal_i$.
   (c) Compute and set $\mathbf{c}^\intercal_i = [\mathbf{G}_q\mathbf{G}_p^{-1}(\lfloor\tilde{\mathbf{c}}_i\rfloor_p)]_B \in [-q/2+B, q/2-B]^{1\times\ell}$.
   (d) Set $\overline{\mathbf{A}}_{\mathsf{fhe}} = \overline{\mathbf{A}}_{\mathsf{fhe},\mathsf{csLWE}}$, $\mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{c}^\intercal_{\mathsf{fhe},\mathsf{csLWE}}$.
   (e) Sample $\mathbf{R}' \leftarrow \{0,1\}^{m\times m}$, computes $\mathbf{C}' = \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}}\\ \mathbf{c}^\intercal_{\mathsf{fhe}}\end{pmatrix}\mathbf{R}' - \mathbf{G}$ and $\mathbf{C} = (\mathbf{C}', \mathbf{C}_{\mathsf{csLWE}})$.
   (f) Forward the following to $\mathcal{A}$.
$$\left(1^\lambda, \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}}\\ \mathbf{c}^\intercal_{\mathsf{fhe}}\end{pmatrix}, \mathbf{C}, \begin{pmatrix}\overline{\mathbf{A}}_0\\ \mathbf{c}^\intercal_0\end{pmatrix}, \left\{\begin{pmatrix}\overline{\mathbf{A}}_i\\ \mathbf{a}^\intercal_i\end{pmatrix}, \mathbf{c}^\intercal_i\right\}_{i\in[Q]}\right)$$
3. On receiving β' from $\mathcal{A}$, forward β' to csLWE challenger.

We observe that if $\beta = 0$, then $\mathcal{B}$ simulates the distribution D'. When $\beta = 1$, then we observe that $\mathbf{C}'$ is statistically close to uniform distribution due to LHL, and thus $\mathcal{B}$ simulates the distribution D_1, except that in D_1, $\mathbf{c}^\intercal_i \leftarrow \mathbb{Z}_q^{1\times\ell}$, while $\mathcal{B}$ returns $\mathbf{c}^\intercal_i \in [-q/2+B, q/2-B]^{1\times\ell}$. However, since B is exponentially smaller than $q/2$, the two distributions are negligibly close. Hence, the advantage of $\mathcal{B}$ is same as the advantage of $\mathcal{A}$.

□

Parameter Setting. We recall the parameters from [HLL23] except $p, \tilde{\beta}$ and B, which we define and set for our purpose.

$$q \in (2^{15\lambda-1}, 2^{15\lambda}], \quad p \in (2^{5\lambda-1}, 2^{5\lambda}], \quad \tilde{\beta} = 2^\lambda, \quad B = 2^{8\lambda}, \quad \sigma = 2^\lambda,$$
$$\sigma' = 2^{2\lambda}, \quad \sigma_{-1} = 2^\lambda, \quad \sigma_{\mathsf{pre}} = 2^{6\lambda}, \quad \sigma_{\mathsf{post}} = 2^{7\lambda}, \quad Q = \lambda + m + (L_{\mathbf{S}}+1)m$$

Counter-example Roadmap. Now, for our counter-example, we need to show that for $(\mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \mathbf{P}, \mathsf{aux}, \sigma, \sigma', \sigma_{-1}, \sigma_{\mathsf{post}}, \sigma_{\mathsf{pre}}) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}} = (\mathsf{coins}, \overline{\mathbf{A}}_{\mathsf{circ}}, \overline{\mathbf{A}}', \{\mathbf{A}_i\}_{i\in[Q]}))$ where $\mathsf{aux} = (\{f_i\}_{i\in[Q]})$,

1. (Pre-condition) For all PPT adversary $\mathcal{A}^{\mathsf{pre}}$, the two distributions, D_0^{pre} and D_1^{pre} as defined in Equation (11) are indistinguishable. We prove this in Claim 4.10.
2. (Attack against postcondition) There exists an adversary $\mathcal{A}^{\mathsf{post}}$ who distinguishes the distributions, D_0^{post} and D_1^{post} as in Equation (12) with non-negligible probability.

Distinguishing Algorithm/Attack Strategy. The adversary $\mathcal{A}^{\mathsf{post}}$ holds the distribution D_β^{post} for $\beta \leftarrow \{0,1\}$. Thus, if $\beta = 0$, $\mathbf{c}_{\mathbf{B}}^\intercal = \mathbf{r}^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal$, $\mathbf{S} = \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{r}^\intercal\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^\intercal \end{pmatrix} \mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}$, $\mathbf{c}_{\mathsf{circ}}^\intercal = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{circ}}^\intercal$ and if $\beta = 1$, $\mathbf{c}_{\mathbf{B}}^\intercal \leftarrow \mathbb{Z}_q^m$, $\mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}$, $\mathbf{c}_{\mathsf{circ}}^\intercal \leftarrow \mathbb{Z}_q^{(L_{\mathbf{S}}+1)m}$. It does the following:

1. For each $i \in [Q]$, compute $\mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} = \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{circ}}, \mathsf{VEval}_{C'_{f_i}}, (1, \mathsf{bits}(\mathbf{S})))$ and $\mathbf{z}_i = \mathbf{c}_{\mathbf{B}}^\intercal \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{circ}}^\intercal \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^\intercal \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \mod q$ where $\mathbf{K}_i \leftarrow \mathbf{B}_{\sigma_{-1}}^{-1}(\overline{\mathbf{A}}_{f_i})$ and $\mathbf{a}_{\mathsf{circ}}^\intercal$ is the $(n+1)$th row of $\mathbf{A}_{\mathsf{circ}}$.
2. Let $L = (L_{\mathbf{S}} + 1)m$. $\mathcal{A}^{\mathsf{post}}$ defines the following set of linear equations (Equation (14)) in variables $\mathbf{e}_{\mathbf{B}}[1], \ldots, \mathbf{e}_{\mathbf{B}}[m]$ and $\mathbf{e}_{\mathsf{circ}}[1], \ldots, \mathbf{e}_{\mathsf{circ}}[L]$ and outputs $\beta' = 0$ if Equation (14) is solvable; otherwise, outputs $\beta' = 1$.

$$\begin{aligned}
\mathbf{e}_{\mathbf{B}}[1]\mathbf{K}_1[1,1] + \ldots + \mathbf{e}_{\mathbf{B}}[m]\mathbf{K}_1[m,1] - \mathbf{e}_{\mathsf{circ}}[1]\mathbf{H}^{f_1}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[1,1] - \ldots \\
-\mathbf{e}_{\mathsf{circ}}[L]\mathbf{H}^{f_1}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[L,1] = \mathbf{z}_1[1] \bmod 2 \\
\mathbf{e}_{\mathbf{B}}[1]\mathbf{K}_2[1,1] + \ldots + \mathbf{e}_{\mathbf{B}}[m]\mathbf{K}_2[m,1] - \mathbf{e}_{\mathsf{circ}}[1]\mathbf{H}^{f_2}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[1,1] - \ldots \\
-\mathbf{e}_{\mathsf{circ}}[L]\mathbf{H}^{f_2}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[L,1] = \mathbf{z}_2[1] \bmod 2 \qquad (14) \\
\vdots \\
\mathbf{e}_{\mathbf{B}}[1]\mathbf{K}_Q[1,1] + \ldots + \mathbf{e}_{\mathbf{B}}[m]\mathbf{K}_Q[m,1] - \mathbf{e}_{\mathsf{circ}}[1]\mathbf{H}^{f_Q}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[1,1] - \ldots \\
-\mathbf{e}_{\mathsf{circ}}[L]\mathbf{H}^{f_Q}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[L,1] = \mathbf{z}_Q[1] \bmod 2
\end{aligned}$$

Next, we analyze the success probability of $\mathcal{A}^{\mathsf{post}}$.

Claim 4.8. $\mathcal{A}^{\mathsf{post}}$ wins (i,e., $\beta = \beta'$) with at least $3/4 - \mathsf{negl}(\lambda)$ probability when $Q \geq \lambda + m + (L_{\mathbf{S}} + 1)m$.

Proof. Let us first analyze the solvability of equations defined in Equation (14) for the two cases: $\beta = 0$ and $\beta = 1$.

When $\beta = 0$, $\forall i \in [Q]$,

$$
\begin{aligned}
\mathbf{z}_i &= \mathbf{c}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \\
&= (\mathbf{r}^{\intercal}\mathbf{B} + \mathbf{e}_{\mathbf{B}}^{\intercal}) \cdot \mathbf{K}_i - (\mathbf{s}^{\intercal}(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{circ}}^{\intercal}) \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \\
&= \mathbf{r}^{\intercal}\mathbf{B}\mathbf{K}_i + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}_i - \mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{circ}} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}}} + \mathbf{s}^{\intercal}\mathsf{VEval}_{C'_{f_i}}(1, \mathsf{bits}(\mathbf{S})) - \mathbf{e}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \\
&= \mathbf{r}^{\intercal}\mathbf{B}\mathbf{K}_i + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}_i - \mathbf{s}^{\intercal} \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{circ}} \\ \mathbf{a}_{\mathsf{circ}}^{\intercal} \end{pmatrix} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}}} + \mathbf{s}^{\intercal}\mathsf{VEval}_{C'_{f_i}}(1, \mathsf{bits}(\mathbf{S})) - \mathbf{e}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \\
&= \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{f_i} + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}_i - (\mathbf{r}^{\intercal}, -1) \begin{pmatrix} \overline{\mathbf{A}}_{f_i} \\ \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \end{pmatrix} + (\mathbf{r}^{\intercal}, -1) \left(\begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^{\intercal} \end{pmatrix} \mathbf{R}_{f_i} - \begin{pmatrix} 0^{n \times \ell} \\ f_i(\mathbf{s}) \end{pmatrix}^{15} \right) \\
&\quad - \mathbf{e}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \\
&= \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{f_i} + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}_i - \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{f_i} + \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_{f_i} + f_i(\mathbf{s}) - \mathbf{e}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \\
&= \mathbf{e}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K}_i + f_i(\mathbf{s}) - \mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_{f_i} - \mathbf{e}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}
\end{aligned}
\tag{15}
$$

Here, we argue that $\mathbf{z}_i \bmod q \in [-q/2, q/2]$ gives $\mathbf{e}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K}_i + f_i(\mathbf{s}) - \mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_{f_i} - \mathbf{e}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}$ over the integer. This can be seen by observing $f_i(\mathbf{s}) \in [-q/2 + B, q/2 - B]$ and $\mathbf{e}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K}_i - \mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_{f_i} - \mathbf{e}_{\mathsf{circ}}^{\intercal} \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} \in [-B, B]$, where the latter follows from $|\mathbf{e}_B| \leq \sigma_{\mathsf{pre}}\sqrt{\lambda}$, $|\mathbf{B}^{-1}(\mathbf{P})| \leq \sigma_{-1}\sqrt{\lambda}$, $\|\mathbf{e}_{\mathsf{fhe}}\| \leq \sigma\sqrt{\lambda}$, $\|\mathbf{e}_{\mathsf{circ}}\| \leq \sigma'\sqrt{\lambda}$, $\|\mathbf{R}_{f_i}\| \leq (m+2)^{d+3} \lceil \log q \rceil m$, $\|\mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}\| \leq (m+2)^{d+3} \lceil \log q \rceil$ (from Lemma 3.15 and Section 3.7), and our choice of B.

We prove in Claim 4.9 that with probability $1/2 + \mathsf{negl}(\lambda)$, we have $\forall i \in [Q]$, $(f_i(\mathbf{s}) - \mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_{f_i})[1] = 0 \bmod 2$. This gives us that with probability $1/2 + \mathsf{negl}(\lambda)$,

$$
\forall i \in [Q],\ \mathbf{z}_i[1] = \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}_i[1] - \mathbf{e}_{\mathsf{circ}}^{\intercal}\mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}[1] \mod 2.
$$

Here, $\mathbf{K}_i[1]$ is the first column of $\mathbf{K}_i$. Observe that this is the same as the set of equations defined in Equation (14). Hence, in case of $\beta = 0$, Equation (14) is solvable with probability $1/2 + \mathsf{negl}(\lambda)$. This gives us

$$
\Pr(\beta' = 0 \mid \beta = 0) = 1/2 + \mathsf{negl}(\lambda). \tag{16}
$$

When $\beta = 1$,

$$
\forall i \in [Q],\ \mathbf{z}_i = \mathbf{c}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - \mathbf{a}_{\mathsf{circ}}^{\intercal} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}\ ,
$$

where $\mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^m$. Here, we argue that the distribution of $\{\mathbf{c}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K}_i \bmod q\}_{i \in [Q]}$ is statistically close to uniform distribution over $(\mathbb{Z}_q^{1 \times \ell})^Q$, even given $\{\mathbf{K}_i \bmod 2\}_{i \in [Q]}$. To see this, we first observe that by Lemma 3.7, each column of $\mathbf{K}_i[\cdot, j]$ has min-entropy at least $m \log(\sigma_{-1}/\lambda) > 2m$ except for negligible probability over $\mathbf{B}$ and $(\mathbf{K}_i[\cdot, j] \bmod 2)$ can be represented by a string of m-bits. We then apply the generalized Leftover Hash Lemma (Lemma 3.8), which implies that the two distributions are within statistical distance $Q\sqrt{2^m \cdot 2^{-2m} q} = \mathsf{negl}(\lambda)$ by our choice of parameters. We therefore have that $\{\mathbf{z}_i \bmod q\}_{i \in [Q]}$ is distributed uniformly at random over $(\mathbb{Z}_q^{1 \times \ell})^Q$, even given $\{\mathbf{K}_i \bmod 2\}_i$. This, in turn, implies $\{\mathbf{z}_i \bmod 2\}_{i \in [Q]}$ (which forms the RHS of equations in Equation (14)) is also statistically close to a uniform distribution independent of $\{\mathbf{K}_i \bmod 2\}_i$ when $\beta = 1$. Hence, Equation (14), having $m + (L_{\mathbf{S}} + 1)m$ number of variables, is unsolvable with overwhelming probability if $Q > \lambda + m + (L_{\mathbf{S}} + 1)m$, since the RHS of the equation falls into the space for which there exists a solution with probability at most $2^{m + (L_{\mathbf{S}}+1)m} / 2^{\lambda + m + (L_{\mathbf{S}}+1)m} = 2^{-\lambda}$.

[15] Since $f_i(1, \mathbf{s})$ ignores its first bit input, 1, we write $f_i(\mathbf{s})$ in place of $f_i(1, \mathbf{s})$ at many places.

This gives us

$$\Pr(\beta' = 1 \mid \beta = 1) \geq 1 - \mathsf{negl}(\lambda). \tag{17}$$

Thus, from Equation (16) and Equation (17), we get $\Pr(\beta' = \beta) \geq 3/4 - \mathsf{negl}(\lambda)$. □

Claim 4.9. $\forall i \in [Q]$, $(f_i(\mathbf{s}) - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_i})[1] = 0 \bmod 2$ with probability $= 1/2 + \mathsf{negl}(\lambda)$.

Proof. Let us start by analyzing the $\tilde{\mathbf{e}}_{\mathsf{fhe}}^{\mathsf{T}}[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_i}$ error. Recall that $\mathbf{R}_{f_i}$ is the randomness in the homomorphically evaluated encryption of $f_i(\mathbf{s})$ (of different form: $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{f_i} - \begin{pmatrix} 0^{n\times\ell} \\ f_i(\mathbf{s}) \end{pmatrix}$), output by $\mathsf{VEval}_{C'_{f_i}}$ circuit.

We recall from Section 3.6 that for any circuit $C : \{0,1\}^L \to \mathbb{Z}_q^{1\times\ell}$, VEval_C on input $\mathbf{X}$ - a GSW encryption of some $\mathbf{x} \in \{0,1\}^L$ - outputs $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}_C - \begin{pmatrix} 0^{n\times\ell} \\ C(\mathbf{x}) \end{pmatrix}$. Let $C(\mathbf{x})[u,v] \in \{-1,0,1\}$ be (the signed version of) the v-th bit of $C(\mathbf{x})[u]$, for $u \in [\ell]$ and $v \in [0,w)$, $w = \lceil \log_2 q \rceil$, then VEval_C computation firstly homomorphically computes GSW encryption of $C(\mathbf{x})[u,v]$, which is of the form $\mathbf{C}_{u,v} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C,u,v} - C(\mathbf{x})[u,v]\mathbf{G}$. Then for each $u \in [\ell]$, it linearly aggregates $\{\mathbf{C}_{u,v}\}_{v\in[0,w-1]}$ to get $\mathbf{C}_u = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C,u} - \begin{pmatrix} 0^{n\times 1} \\ C(\mathbf{x})[u] \end{pmatrix}$ as $\mathbf{C}_u = \sum_v \mathbf{C}_{u,v}\mathbf{G}^{-1}(2^v \iota_{n+1})$. In particular,

$$\mathbf{R}_{C,u} = \sum_v \mathbf{R}_{C,u,v}\mathbf{G}^{-1}(2^v\iota_{n+1}), \text{ and } \mathbf{R}_C = (\mathbf{R}_{C,1}, \ldots, \mathbf{R}_{C,\ell}).$$

Coming back to our analysis, $(\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_i})[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_{i,1}} = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=0}^{w-1}\mathbf{R}_{f_{i,1,v}}\mathbf{G}^{-1}(2^v\iota_{n+1})$, where $\mathbf{R}_{f_{i,1}}$ is the first column of $\mathbf{R}_{f_i}$ and $\mathbf{R}_{f_{i,1,v}}$ is the randomness in homomorphically computed GSW encryption of the v-th bit of $f_i(\mathbf{s})[1]$. Here $v \in [0,w)$ where $w = \lceil \log_2 q \rceil$. Since f_i is implemented by C'_{f_i}, in which all the output bits pass through even randomness, except the lowest order bit of the first element, which passes through the correlation inducing gate, we have

$$\begin{aligned}
& f_i(\mathbf{s})[1] - (\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_i})[1] \bmod 2 \\
= \; & f_i(\mathbf{s})[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_{i,1,0}}\mathbf{G}^{-1}(\iota_{n+1}) - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=1}^{w-1}\mathbf{R}_{f_{i,1,v}}\mathbf{G}^{-1}(2^v\iota_{n+1}) \bmod 2 \\
= \; & f_i(\mathbf{s})[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_{i,1,0}}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \quad \text{(due to Lemma 4.3)} \\
= \; & f_i(\mathbf{s})[1,0] + \sum_{v=1}^{w-1} 2^v f_i(\mathbf{s})[1,v] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_{i,1,0}}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
= \; & f_i(\mathbf{s})[1,0] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{f_{i,1,0}}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
= \; & f_i(\mathbf{s})[1,0] - f_i(\mathbf{s})[1,0]\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \quad \text{(due to Corollary 4.5)} \\
= \; & 0 \bmod 2, \text{ if } \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \text{ is odd}
\end{aligned}$$

In the above, $f_i(\mathbf{s})[u,v]$ represents the v-th bit in the binary representation of $f_i(\mathbf{s})[u]$ and $\mathbf{R}^*$ is the randomness in the ciphertext of special "1" input used in Corollary 4.5. We then argue that $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1})$ is odd with probability negligibly close to $1/2$. To see this, we first observe that each entry of $\mathbf{R}^*$ is distributed over $\{0,1\}$ uniformly at random and thus so is each entry of $\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2$. In particular, this implies that $\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2$ is a non-zero vector with overwhelming probability. We then observe that each entry of $\mathbf{e}_{\mathsf{fhe}} \bmod 2$ is statistically close to the uniform distribution over $\{0,1\}$ by Lemma 3.10. Combining these facts, it follows that the distribution of $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2$ is statistically close to the uniform distribution over $\{0,1\}$, as desired. Note that the term $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1})$ does not depend on i and hence, for all $i \in [Q]$, the probability that $f_i(\mathbf{s})[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{F}_i}}[1] = 0 \bmod 2$ is $1/2 + \mathsf{negl}(\lambda)$. Hence, the proof. □

Proving the pre-condition. We now show that the pre-condition of evcsLWE holds with respect to the above sampler defined in Section 4.1.2.

Claim 4.10. For $(\mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \mathbf{P}, \mathsf{aux}, \sigma, \sigma', \sigma_{-1}, \sigma_{\mathsf{post}}, \sigma_{\mathsf{pre}}) \leftarrow \mathsf{Samp}(1^\lambda; \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}} = (\mathsf{coins}, \overline{\mathbf{A}}_{\mathsf{circ}}, \overline{\mathbf{A}}', \{\mathbf{A}_i\}_{i\in[Q]}))$ where $\mathsf{aux} = (\{f_i\}_{i\in[Q]})$ and for a $\lambda \in \mathbb{N}$,

$$D_0^{\mathsf{pre}} := \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{r}^\intercal \overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}}, \mathbf{S} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{circ}}, \\ (\mathbf{c}')^\intercal = \mathbf{r}^\intercal \overline{\mathbf{A}}' + (\mathbf{e}')^\intercal, \mathbf{c}^\intercal_{\mathbf{B}} = \mathbf{r}^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \\ \mathbf{c}^\intercal_{\mathbf{P}} = \mathbf{r}^\intercal \mathbf{P} + \mathbf{e}^\intercal_{\mathbf{P}} \end{array}\right)$$

$$\approx_c D_1^{\mathsf{pre}} := \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{1\times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil \log_2 q\rceil+1)m}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^{1\times(L_{\mathbf{S}}+1)m}, \\ (\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times m'}, \mathbf{c}^\intercal_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{1\times m}, \\ \mathbf{c}^\intercal_{\mathbf{P}} \leftarrow \mathbb{Z}_q^{1\times J} \end{array}\right) \tag{18}$$

where $J = \ell \cdot Q$, sampler Samp is as defined in Section 4.1.2 and the vectors and matrices are sampled as in Assumption 4.1.

Proof. We can write $\mathbf{r}^\intercal \mathbf{P} + \mathbf{e}^\intercal_{\mathbf{P}} = \mathbf{r}^\intercal[\overline{\mathbf{A}}_{f_1}, \ldots, \overline{\mathbf{A}}_{f_Q}] + [\mathbf{e}^\intercal_{\mathbf{P},1}, \ldots, \mathbf{e}^\intercal_{\mathbf{P},Q}]$ where $\mathbf{e}^\intercal_{\mathbf{P},i}$ is the ith block of $\mathbf{e}^\intercal_{\mathbf{P}}$ with length ℓ . Hence, we can re-write Equation (18) as:

$$D_0^{\mathsf{pre}} := \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} = \mathbf{r}^\intercal \overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}}, \mathbf{S} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{circ}}, \\ (\mathbf{c}')^\intercal = \mathbf{r}^\intercal \overline{\mathbf{A}}' + (\mathbf{e}')^\intercal, \mathbf{c}^\intercal_{\mathbf{B}} = \mathbf{r}^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \\ \{\mathbf{c}^\intercal_{\mathbf{P},i} = \mathbf{r}^\intercal \overline{\mathbf{A}}_{f_i} + \mathbf{e}^\intercal_{\mathbf{P},i}\}_{i\in[Q]} \end{array}\right)$$

$$\approx_c D_1^{\mathsf{pre}} := \left(\begin{array}{r} 1^\lambda, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \\ \mathbf{c}^\intercal_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{1\times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil \log_2 q\rceil+1)m}, \\ \mathbf{c}^\intercal_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^{1\times(L_{\mathbf{S}}+1)m}, \\ (\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times m'}, \mathbf{c}^\intercal_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{1\times m}, \\ \{\mathbf{c}^\intercal_{\mathbf{P},i} \leftarrow \mathbb{Z}_q^{1\times \ell}\}_{i\in[Q]} \end{array}\right) \tag{19}$$

We now prove Equation (19) by a series of hybrids Hyb_0 to Hyb_2 where Hyb_0 is the D_0^{pre} distribution and Hyb_2 is the D_1^{pre} distribution of Equation (19). We prove that $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1 \approx \mathsf{Hyb}_2$.

Hyb_1**:** This hybrid is same as Hyb_0, except that for all $i \in [Q]$, $\mathbf{c}^\intercal_{\mathbf{P},i}$ can be computed as:

$$\mathbf{c}^\intercal_{\mathbf{P},i} = \mathbf{c}^\intercal_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} + f_i(\mathbf{s}) + \mathbf{a}^\intercal_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} + \mathbf{e}^\intercal_{\mathbf{P},i}$$

where $\mathbf{e}_{\mathbf{P},i} \leftarrow \mathcal{D}^{\ell}_{\mathbb{Z},\sigma_{\mathsf{pre}},\le\sigma_{\mathsf{pre}}\sqrt{\lambda}}$. We claim that Hyb_0 and Hyb_1 are statistically indistinguishable. To see this, note that from Equation (15),

$$\mathbf{c}^\intercal_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} = \mathbf{r}^\intercal \overline{\mathbf{A}}_{f_i} - \mathbf{a}^\intercal_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} - f_i(\mathbf{s}) + \mathbf{e}^\intercal_{\mathsf{fhe}} \mathbf{R}_{f_i} + \mathbf{e}^\intercal_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}$$

where $\mathbf{R}_{f_i}$ is the randomness in the homomorphically evaluated encryption (of different form) of $f_i(\mathbf{s})$, output by $\mathsf{VEval}_{C'_{f_i}}$. This implies,

$$\mathbf{c}^{\intercal}_{\mathbf{P},i} = \mathbf{c}^{\intercal}_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} + f_i(\mathbf{s}) + \mathbf{a}^{\intercal}_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}} + \mathbf{e}^{\intercal}_{\mathbf{P},i} = \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{f_i} + \tilde{\mathbf{e}}_i{}^{\intercal} + \mathbf{e}^{\intercal}_{\mathbf{P},i}$$

where $\tilde{\mathbf{e}}_i{}^{\intercal} = \mathbf{e}^{\intercal}_{\mathsf{fhe}}\mathbf{R}_{f_i} + \mathbf{e}^{\intercal}_{\mathsf{circ}} \cdot \mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}$.

Let $d' = d_{\mathsf{VEval}_{C'_{f_i}}} \leq d+3$. Then, we have, $\|\mathbf{e}_{\mathsf{fhe}}\| \leq \sigma\sqrt{\lambda}$, $\|\mathbf{e}_{\mathsf{circ}}\| \leq \sigma'\sqrt{\lambda}$, $\|\mathbf{R}_{f_i}\| \leq (m+2)^{d+3}\lceil \log q \rceil m$, $\|\mathbf{H}^{f_i}_{\mathbf{A}_{\mathsf{circ}},\mathbf{S}}\| \leq (m+2)^{d+3}\lceil \log q \rceil$ (from Lemma 3.15 and Section 3.7). Hence, $\|\tilde{\mathbf{e}}_i\| \leq m^2\sigma\sqrt{2\lambda}(m+2)^{d+3}\lceil \log q \rceil + L\sigma'\sqrt{2\lambda}(m+2)^{d'+3}\lceil \log q \rceil \leq 2^{O(d\log^3\lambda)}\sigma' \leq 2^{3\lambda}$ (as $d = \mathrm{poly}(\log\lambda)$). Further, since $\mathbf{e}_{\mathbf{P},i} \leftarrow \mathcal{D}^{\ell}_{\mathbb{Z},\sigma_{\mathsf{pre}},\leq\sigma_{\mathsf{pre}}\sqrt{\lambda}}$, where $\sigma_{\mathsf{pre}} \leq 2^{6\lambda}$ and hence, by noise flooding (Lemma 3.9), $\mathbf{e}^{\intercal}_{\mathbf{P},i} \approx_s \mathbf{e}^{\intercal}_{\mathbf{P},i} + \tilde{\mathbf{e}}_i{}^{\intercal}$ with a statistical distance of $\mathrm{poly}(\lambda)2^{-4\lambda}$. Therefore, the statistical distance Δ between Hyb_0 and Hyb_1 is:

$$\Delta(\mathsf{Hyb}_0, \mathsf{Hyb}_1) = \frac{Q \cdot \mathrm{poly}(\lambda)}{2^{4\lambda}}$$

Hence, it suffices to show the pseudorandomness of the following distribution:

$$\left(\begin{array}{r} 1^{\lambda}, \mathsf{coins}^{\mathsf{pub}}_{\mathsf{Samp}}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \mathbf{c}^{\intercal}_{\mathsf{fhe}} = \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^{\intercal}_{\mathsf{fhe}}, \mathbf{S} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}, \\ \mathbf{c}^{\intercal}_{\mathsf{circ}} = \mathbf{s}^{\intercal}(\mathbf{A}_{\mathsf{circ}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \mathbf{G}) + \mathbf{e}^{\intercal}_{\mathsf{circ}}, \\ (\mathbf{c}')^{\intercal} = \mathbf{r}^{\intercal}\overline{\mathbf{A}}' + (\mathbf{e}')^{\intercal}, \mathbf{c}^{\intercal}_{\mathbf{B}} = \mathbf{r}^{\intercal}\mathbf{B} + \mathbf{e}^{\intercal}_{\mathbf{B}}, \{\tilde{\mathbf{y}}_i = f_i(\mathbf{s}) + \mathbf{e}^{\intercal}_{\mathbf{P},i}\}_{i\in[Q]} \end{array}\right)$$

Hyb_2**:** This hybrid is same as Hyb_1, except that, we sample $\mathbf{c}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^m, \mathbf{c}_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^L, (\mathbf{c}') \leftarrow \mathbb{Z}_q^{m'}, \mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^m$, $\mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}$ and $\tilde{\mathbf{y}}_i \leftarrow \mathbb{Z}_q^{1\times\ell}$, where $L = (L_{\mathbf{S}}+1)m$. We prove that $\mathsf{Hyb}_1 \approx \mathsf{Hyb}_2$ via the following claim.

Claim 4.11. $\mathsf{Hyb}_1 \approx_c \mathsf{Hyb}_2$, assuming the indistinguishability in Equation (13).

Proof. We show that if there exists an adversary $\mathcal{A}$ who can distinguish between the two hybrids with non-negligible advantage, then there is a reduction $\mathcal{B}$ that can distinguish L.H.S and R.H.S of Equation (13) with non-negligible advantage. The reduction is as follows.

1. On receiving 1^{λ} from $\mathcal{A}$, forward it to challenger of Equation (13).
2. Equation (13) challenger samples $\beta \leftarrow \{0,1\}$, $\overline{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\overline{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times L+m+m'}$, and $\mathbf{r} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma,\leq\sigma\sqrt{\lambda}}$, and returns

$$\left(1^{\lambda}, \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}^{\intercal}_{\mathsf{fhe}}\end{pmatrix}, \mathbf{C}, \begin{pmatrix}\overline{\mathbf{A}} \\ \mathbf{c}^{\intercal}\end{pmatrix}, \{f_i, \mathbf{c}^{\intercal}_i\}_{i\in[Q]}\right)$$

where $\mathbf{c}^{\intercal}_{\mathsf{fhe}} = \mathbf{r}^{\intercal}\overline{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^{\intercal}_{\mathsf{fhe}}$, $\mathbf{c}^{\intercal} = \mathbf{r}^{\intercal}\overline{\mathbf{A}} + \mathbf{e}^{\intercal}, \mathbf{C} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (1, \mathsf{bits}(\mathbf{s})) \otimes \mathbf{G}$ and $\{\mathbf{c}^{\intercal}_i = f_i(\mathbf{s})\}_{i\in[Q]}$ if $\beta = 0$; else $\mathbf{c}^{\intercal}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{1\times m}$, $\mathbf{c}^{\intercal} \leftarrow \mathbb{Z}_q^{1\times L+m+m'}, \mathbf{C} \leftarrow \mathbb{Z}_q^{(n+1)\times((n+1)\lceil\log_2 q\rceil+1)m}$ and $\{\mathbf{c}^{\intercal}_i \leftarrow \mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]}$, if $\beta = 1$. Here $\mathbf{A}_{\mathsf{fhe}} = \begin{pmatrix}\overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}^{\intercal}_{\mathsf{fhe}}\end{pmatrix}$. Then $\mathcal{B}$ does the following.

   (a) Parse $\overline{\mathbf{A}} = (\overline{\mathbf{A}}'_{\mathsf{circ}}, \mathbf{B}, \overline{\mathbf{A}}')$ where $\overline{\mathbf{A}}'_{\mathsf{circ}} \in \mathbb{Z}_q^{n\times L}, \mathbf{B} \in \mathbb{Z}_q^{n\times m}, \overline{\mathbf{A}}' \in \mathbb{Z}_q^{n\times m'}$ and $\mathbf{c}^{\intercal} = (\tilde{\mathbf{c}}^{\intercal}_{\mathsf{circ}}, \mathbf{c}^{\intercal}_{\mathbf{B}}, (\mathbf{c}')^{\intercal})$ where $\tilde{\mathbf{c}}^{\intercal}_{\mathsf{circ}} \in \mathbb{Z}_q^{1\times L}, \mathbf{c}^{\intercal}_{\mathbf{B}} \in \mathbb{Z}_q^{1\times m}, (\mathbf{c}')^{\intercal} \in \mathbb{Z}_q^{1\times m'}$.

(b) Sample coins. For all $i \in [Q]$, samples $\mathbf{e}_{\mathbf{P},i} \leftarrow \mathcal{D}^{\ell}_{\mathbb{Z},\sigma_{\mathsf{pre}},\leq\sigma_{\mathsf{pre}}\sqrt{\lambda}}$. Set $\mathsf{aux} = \{f_i\}_{i\in[Q]}$ and $\tilde{\mathbf{y}}_i = \mathbf{c}_i^{\mathsf{T}} + \mathbf{e}_{\mathbf{P},i}^{\mathsf{T}}$.

(c) Set $\mathbf{S} = \mathbf{C}$. Also set $\overline{\mathbf{A}}_{\mathsf{circ}} = \overline{\mathbf{A}}'_{\mathsf{circ}} + (1, \mathsf{bits}(\mathbf{S})) \otimes \overline{\mathbf{G}}$, $\mathbf{A}_{\mathsf{circ}} = \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{circ}} \\ \mathbf{a}_{\mathsf{circ}}^{\mathsf{T}} \end{pmatrix}$, where $\mathbf{a}_{\mathsf{circ}} \leftarrow \mathbb{Z}_q^L$, and $\mathbf{c}_{\mathsf{circ}}^{\mathsf{T}} = \tilde{\mathbf{c}}_{\mathsf{circ}}^{\mathsf{T}} - (\mathbf{a}_{\mathsf{circ}}^{\mathsf{T}} - (1, \mathsf{bits}(\mathbf{S})) \otimes \underline{\mathbf{G}})$, where $\overline{\mathbf{G}}$ and $\underline{\mathbf{G}}$ denotes the first n rows and $n+1$-th row of the gadget matrix $\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m}$, respectively.

3. Forward the following to $\mathcal{A}$.

$$\left(1^{\lambda}, \mathsf{coins}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \mathbf{c}_{\mathsf{fhe}}^{\mathsf{T}}, \mathbf{S}, \mathbf{c}_{\mathsf{circ}}^{\mathsf{T}}, (\mathbf{c}')^{\mathsf{T}}, \mathbf{c}_{\mathbf{B}}^{\mathsf{T}}, \tilde{\mathbf{y}}_i\}_{i\in[Q]}\right)$$

4. $\mathcal{A}$ outputs a bit β'. $\mathcal{B}$ forwards the bit β' to the Equation (13) challenger.

We observe that if $\beta = 0$, then $\mathcal{B}$ simulates the distribution of Hybrid 1, and if $\beta = 1$, then the distribution of Hybrid 2. The indistinguishability of Hyb_1 and Hyb_2 follows from the indistinguishability of Equation (13). □

Hence, we achieve the following distribution:

$$\left(\begin{array}{r} 1^{\lambda}, \mathsf{coins}, \mathsf{aux}, \mathbf{A}_{\mathsf{circ}}, \overline{\mathbf{A}}', \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{B}, \mathbf{c}_{\mathsf{fhe}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times m}, \mathbf{S} \leftarrow \mathbb{Z}_q^{(n+1)\times(n+1)\lceil\log_2 q\rceil m}, \\ \mathbf{c}_{\mathsf{circ}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times(m(n+1)^2\lceil\log_2 q\rceil^2+1)m}, \\ (\mathbf{c}')^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times m'}, \mathbf{c}_{\mathbf{B}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times m}, \{\mathbf{c}_{\mathbf{P},i}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]} \end{array}\right) \tag{20}$$

where $\mathbf{A}_{\mathsf{fhe}} = \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{c}_{\mathsf{fhe}}^{\mathsf{T}} \end{pmatrix}$. The distribution as in Equation (20) is the same as D_1^{pre} as in Equation (19). Hence, the proof.

□

□

4.2 Attacks when Pre-Condition Error is Larger

In this section, we develop new attacks that exploit the case where the error in the pre-condition is set larger than the error in the post-condition.

4.2.1 Attack 1

Theorem 4.12. There exists an efficient and public-coin ELWE sampler Samp as defined in Assumption 3.13 (with $\mathbf{A}$ and LWE sample with respect to it) such that the pre-condition holds under the LWE assumption, but the post-condition does not- i.e., there exists a distinguisher $\mathcal{A}^{\mathsf{post}}$ that distinguishes post-condition with non-negligible probability.

Proof. We first define the sampler.

Defining Evasive LWE Sampler. Let $n, m, \ell, p, q, r, B \in \mathbb{N}$ be parameters and λ be the security parameter. We assume that p and r are primes and $q = pr$. The public coin sampler Samp of the Evasive LWE assumption is defined as follows.

1. Sample $\mathbf{D} \leftarrow [0, r-1]^{n \times \ell}$ and set $\mathbf{P} = p\mathbf{D} \bmod q$.
2. Samples $\mathbf{s} \leftarrow \mathcal{D}^n_{\mathbb{Z}, \sigma_{\mathbf{s}}}$.
3. Output $\mathbf{S} = \mathbf{s}^\intercal$, $\mathbf{P}$, and $\mathsf{aux} = \mathbf{D}$.

We can see that the sampler is public-coin, since the only randomness that should be kept secret is $\mathbf{s}$.

Parameter Setting. We set the parameters as follows.

$$n = \mathrm{poly}(\lambda),\ \ \ell = n^2,\ \ m = O(n \log q),\ \ r > 2^{9\lambda},\ \ p > 2^{11\lambda},\ \ q = pr,\ \ B = 2^{6\lambda},$$
$$\sigma_{\mathsf{post}} = 2^{5\lambda},\ \ \sigma_{\mathsf{pre}} = \sigma'_{\mathsf{pre}} = 2^{15\lambda},\ \ \sigma_{\mathbf{s}} = 2^{2\lambda},\ \ \tau = O\left(\sqrt{(n+1)\log q}\right)$$

Here r and p are primes greater than $2^{9\lambda}$ and $2^{11\lambda}$ respectively.

Distinguishing Algorithm/Attack Strategy. The adversary $\mathcal{A}^{\mathsf{post}}$ holds the distribution D^{post}_β for $\beta \leftarrow \{0,1\}$. Thus, for $\beta = 0$, $\mathbf{c}^\intercal_{\mathbf{B}} = \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}$ and for $\beta = 1$, $\mathbf{c}^\intercal_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{1 \times m}$. It does the following:

1. Compute a vector $\mathbf{d}^\intercal \stackrel{\mathrm{def}}{=} \mathbf{c}^\intercal_{\mathbf{B}} \cdot \mathbf{B}^{-1}(\mathbf{P}) \bmod q$.
2. Find (the unique) $\mathbf{d}_1 \in [0, r-1]^n$ and $\mathbf{d}_2 \in [0, p-1]^n$ such that $\mathbf{d} = p\mathbf{d}_1 + \mathbf{d}_2 \bmod q$.
3. Find $\mathbf{s}_0 \in [-(r-1)/2, (r-1)/2]^n$ such that $\mathbf{s}_0^\intercal \mathbf{D} = \mathbf{d}_1^\intercal \bmod r$.
4. Compute $\gamma = \left\| \mathbf{c}^\intercal_{\mathbf{B}} - \mathbf{s}_0^\intercal \mathbf{B} \bmod q \right\|$.
5. Output 1 if $\gamma < B$ and 0 otherwise.

We observe that in the case of $\beta = 0$, we have

$$\mathbf{c}^\intercal_{\mathbf{B}} \cdot \mathbf{B}^{-1}(\mathbf{P}) = (\mathbf{s}^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}) \mathbf{B}^{-1}(\mathbf{P}) = p\mathbf{s}^\intercal \mathbf{D} + \mathbf{e}^\intercal_{\mathbf{B}} \mathbf{B}^{-1}(\mathbf{P}).$$

By our parameter setting, $\left\| \mathbf{e}^\intercal_{\mathbf{B}} \mathbf{B}^{-1}(\mathbf{P}) \right\| \le \lambda \sigma_{\mathsf{post}} \tau m < p$. We therefore have $\mathbf{s}^\intercal \mathbf{D} = \mathbf{d}_1 \bmod r$. Since $\mathbf{D}$ is full rank over $\mathbb{Z}_r$ with probability $\prod_{i=0}^{n}(1 - 1/r^{\ell - i}) \ge 1 - n/r^{\ell - n} = 1 - \mathsf{negl}(\lambda)$, we have $\mathbf{s}^\intercal = \mathbf{s}_0^\intercal \bmod r$. By our choice of $\sigma_{\mathbf{s}}$ and B, we have $\|\mathbf{s}\| < r$ with overwhelming probability and thus $\mathbf{s}_0 = \mathbf{s}$ holds over the integer. Therefore, $\gamma = \|\mathbf{e}_{\mathbf{B}}\| < B$ with overwhelming probability by our choice of σ_{post}. In the case of $\beta = 1$, we argue that such $\mathbf{s}$ does not exist with overwhelming probability. This can be observed by the counting argument. For an arbitrarily fixed $\mathbf{B}$, for each $\mathbf{s}_0 \in \mathbb{Z}_q^n$, there are $(2B+1)^m$ points whose distance from $\mathbf{s}_0^\intercal \mathbf{B}$ is within B in infinity norm. The probability that random $\mathbf{c}_{\mathbf{B}}$ is within distance B is thus at most $(2B+1)^m/q^m$. Taking union bound over $\mathbf{s}_0$, the probability that random $\mathbf{c}_{\mathbf{B}}$ is within distance B from the span of $\mathbf{B}$ is at most $q^n(2B+1)^m/q^m$. By our choice of B, q, and m, this probability is negligible. Summarizing the above discussion, the adversary distinguishes the distributions with high advantage.

Proving the pre-condition. Here, we prove that the pre-condition with respect to the sampler holds. To do so, we prove the pre-condition of Assumption 3.13 by a series of hybrids Hyb_0 to Hyb_3 where Hyb_0 is the D_0^{pre} distribution and Hyb_3 is the D_1^{pre} distribution of (32). We prove that $\mathsf{Hyb}_0 \approx_c \mathsf{Hyb}_1 \approx_c \ldots \approx_c \mathsf{Hyb}_3$.

Hyb_0**:** This is the D_0^{pre} distribution. Namely, the adversary is given $(\mathbf{B}, \mathbf{P}, \mathbf{c}_{\mathbf{B}}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal, \mathbf{c}_{\mathbf{P}}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_{\mathbf{P}}^\intercal, \mathbf{D})$.

Hyb_1**:** This is identical to Hyb_0 except that we replace the term $\mathbf{c}_{\mathbf{P}}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_{\mathbf{P}}^\intercal$ with $\mathbf{s}^\intercal\mathbf{P} + \mathbf{s}^\intercal\mathbf{D}' + \mathbf{e}_{\mathbf{P}}^\intercal$, where $\mathbf{D}' \leftarrow [0, p-1]^{n\times\ell}$. By our choice of σ_{pre}, $\sigma_{\mathbf{s}}$, and p, we have $\|\mathbf{e}_{\mathbf{P}}\| > \lambda^{\omega(1)}\|\mathbf{s}^\intercal\mathbf{D}'\|$ and thus $\mathbf{e}_{\mathbf{P}}^\intercal \approx_s \mathbf{s}^\intercal\mathbf{D}' + \mathbf{e}_{\mathbf{P}}^\intercal$. Therefore, this hybrid is statistically indistinguishable from the previous one.

Hyb_2 **:** In this hybrid, we further replace $\mathbf{c}_{\mathbf{P}}^\intercal$ and $\mathbf{D}$. Here, we sample $\mathbf{F} \leftarrow \mathbb{Z}_q^{n\times\ell}$ and set $\mathbf{c}_{\mathbf{P}}^\intercal = \mathbf{s}^\intercal\mathbf{F} + \mathbf{e}_{\mathbf{P}}^\intercal$ and $\mathbf{D} = \lfloor \mathbf{F}/p \rfloor \bmod r$. This hybrid is essentially the same as previous hybrid. To see this, it suffices to see that the distribution of $(\mathbf{P} + \mathbf{D}' \bmod q, \mathbf{D} \bmod r) = (p\mathbf{D} + \mathbf{D}' \bmod q, \mathbf{D} \bmod r)$ in the previous hybrid is the same as $(\mathbf{F} \bmod q, \lfloor \mathbf{F}/p \rfloor \bmod r)$ in this hybrid.

Hyb_3**:** This is the D_1^{pre} distribution. Compared with the previous hybrid, here we replace $\mathbf{c}_{\mathbf{B}}^\intercal$ and $\mathbf{c}_{\mathbf{P}}^\intercal$ with random vectors with the same dimensions. The indistinguishability from the previous hybrid can be shown by a straightforward reduction to LWE.

This completes the proof of the theorem. □

4.2.2 Attack 2.

Our first attack is a bit unnatural in that each entry of $\mathbf{P}$ is in the ideal generated by p in $\mathbb{Z}_q$ (i.e., a multiple of p). Here, we show here another example for uniform $\mathbf{P}$ over $\mathbb{Z}_q^{n\times\ell}$.

Theorem 4.13. Let us consider a variant of ELWE as defined in Assumption 3.13. There exists an efficient and public-coin ELWE sampler Samp such that the pre-condition holds under the LWE assumption, but the post-condition does not- i.e., there exists a distinguisher $\mathcal{A}^{\mathsf{post}}$ that distinguishes post-condition with non-negligible probability. In this example, $\mathbf{P}$ is distributed uniformly over $\mathbb{Z}_q^{n\times\ell}$.

Proof. Let $n, m, \ell, p, q, r, B \in \mathbb{N}$ be parameters and λ be the security parameter. We assume that p and r are primes and $q = pr$. The public coin sampler Samp of the Evasive LWE assumption is defined as follows.

1. Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{D} \leftarrow [0, r-1]^{n\times\ell}$, and $\mathbf{E} \leftarrow \{0,1\}^{m\times\ell}$ and set $\mathbf{P} = \mathbf{A}\mathbf{E} + p\mathbf{D} \bmod q$.
2. Samples $\mathbf{s} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_{\mathbf{s}}}^n$.
3. Output $\mathbf{S} = \mathbf{s}^\intercal$, $\mathbf{P}$, $\mathbf{A}$, and $\mathsf{aux} = (\mathbf{D}, \mathbf{E})$.

We can see that the sampler is public-coin, since the only randomness that should be kept secret is $\mathbf{s}$.

Parameter Setting. We set the parameter as follows.

$$n = \mathrm{poly}(\lambda),\ \ \ell = n^2,\ \ m = O(n\log q),\ \ r > 2^{9\lambda},\ \ p > 2^{11\lambda},\ \ q = pr,\ \ B = 2^{6\lambda},$$
$$\sigma_{\mathsf{post}} = 2^{5\lambda},\ \ \sigma_{\mathsf{pre}} = 2^{15\lambda},\ \ \sigma'_{\mathsf{pre}} = 2^{12\lambda},\ \ \sigma_{\mathbf{s}} = 2^{2\lambda},\ \ \tau = O\left(\sqrt{m\log q}\right)$$

Distinguishing Algorithm/Attack Strategy. The adversary $\mathcal{A}^{\mathsf{post}}$ holds the distribution D_β^{post} for $\beta \leftarrow \{0,1\}$. Thus, for $\beta = 0$, $\mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal$ and $\mathbf{c}_\mathbf{B}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal$ where $\mathbf{e}_\mathbf{A}, \mathbf{e}_\mathbf{B} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{post}}}$, and for $\beta = 1$, $\mathbf{c}_\mathbf{A}^\intercal, \mathbf{c}_\mathbf{B}^\intercal \leftarrow \mathbb{Z}_q^{1\times m}$. It does the following:

1. Compute a vector $\mathbf{d}^\intercal \stackrel{\text{def}}{=} \mathbf{c}_\mathbf{B}^\intercal \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathbf{c}_\mathbf{A}^\intercal \cdot \mathbf{E} \bmod q$.
2. Find $\mathbf{d}_1 \in [0, r-1]^n$ and $\mathbf{d}_2 \in [0, p-1]^n$ such that $\mathbf{d} = p\mathbf{d}_1 + \mathbf{d}_2 \bmod q$.
3. Find $\mathbf{s}_0 \in [-(r-1)/2, (r-1)/2]$ such that $\mathbf{s}_0^\intercal\mathbf{D} = \mathbf{d}_1^\intercal \bmod r$.
4. Compute $\gamma = \left\|\mathbf{c}_\mathbf{B}^\intercal - \mathbf{s}_0^\intercal\mathbf{B} \bmod q\right\|$.
5. Output 1 if $\gamma < B$ and 0 otherwise.

We observe that in the case of $\beta = 0$, we have

$$\mathbf{c}_\mathbf{B}^\intercal \cdot \mathbf{B}^{-1}(\mathbf{P}) - \mathbf{c}_\mathbf{A}^\intercal \cdot \mathbf{E} = (\mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal)\mathbf{B}^{-1}(\mathbf{P}) - (\mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal)\mathbf{E} = p\mathbf{s}^\intercal\mathbf{D} + \mathbf{e}_\mathbf{B}^\intercal\mathbf{B}^{-1}(\mathbf{P}) - \mathbf{e}_\mathbf{A}^\intercal\mathbf{E}.$$

By our parameter setting, $\left\|\mathbf{e}_\mathbf{B}^\intercal\mathbf{B}^{-1}(\mathbf{P}) - \mathbf{e}_\mathbf{A}^\intercal\mathbf{E}\right\| \le m\sigma_{\mathsf{post}}\sqrt{\lambda}(\tau\sqrt{\lambda}+1) < p$. We therefore have $\mathbf{s}^\intercal\mathbf{D} = \mathbf{d}_1 \bmod r$. Since $\mathbf{D}$ is full rank over $\mathbb{Z}_r$ with probability $\prod_{i=0}^{n}(1-1/r^{\ell-i}) \ge 1 - n/r^{\ell-n} = 1 - \mathsf{negl}(\lambda)$, we have $\mathbf{s}^\intercal = \mathbf{s}_0^\intercal \bmod r$. By our choice of $\sigma_\mathbf{s}$ and B, we have $\|\mathbf{s}\| < r$ with overwhelming probability and thus $\mathbf{s}_0 = \mathbf{s}$ holds over the integer. Therefore, $\gamma = \|\mathbf{e}_\mathbf{B}\| < B$ with overwhelming probability by our choice of σ_{post}. Furthermore, in the case of $\beta = 1$, we argue that $\mathbf{s}_0$ such that $\left\|\mathbf{c}_\mathbf{B}^\intercal - \mathbf{s}_0^\intercal\mathbf{B} \bmod q\right\| < B$ does not exist with overwhelming probability. This is shown by the same argument as that of Theorem 4.12. Therefore, the above constitutes a valid adversary.

Proving the pre-condition. Here, we prove that the pre-condition with respect to the sampler holds. To do so, we prove pre-condition of Assumption 3.13 by a series of hybrids Hyb_0 to Hyb_3 where Hyb_0 is the D_0^{pre} distribution and Hyb_3 is the D_1^{pre} distribution of Equation (32). We prove that $\mathsf{Hyb}_0 \approx_c \mathsf{Hyb}_1 \approx_c \ldots \approx_c \mathsf{Hyb}_3$.

Hyb_0**:** This is the D_0^{pre} distribution. Namely, the adversary is given $(\mathbf{B}, \mathbf{P}, \mathbf{c}_\mathbf{B}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}_\mathbf{B}^\intercal, \mathbf{c}_\mathbf{A}^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal, \mathbf{c}_\mathbf{P}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{P}^\intercal, \mathbf{A}, \mathbf{D}, \mathbf{E})$, where $\mathbf{e}_\mathbf{A} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma'_{\mathsf{pre}}}$, $\mathbf{e}_\mathbf{B} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{pre}}}$ and $\mathbf{e}_\mathbf{P} \leftarrow \mathcal{D}^\ell_{\mathbb{Z},\sigma_{\mathsf{pre}}}$.

Hyb_1**:** This is identical to Hyb_0 except that we replace the term $\mathbf{c}_\mathbf{P}^\intercal$ with $\mathbf{c}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{s}^\intercal(p\mathbf{D} + \mathbf{D}') + \mathbf{e}_\mathbf{P}^\intercal$, where $\mathbf{D}' \leftarrow [0, p-1]^{n\times\ell}$. We have

$$\mathbf{c}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{s}^\intercal(p\mathbf{D} + \mathbf{D}') + \mathbf{e}_\mathbf{P}^\intercal = (\mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_\mathbf{A}^\intercal)\mathbf{E} + \mathbf{s}^\intercal(p\mathbf{D} + \mathbf{D}') + \mathbf{e}_\mathbf{P}^\intercal = \mathbf{s}^\intercal\mathbf{P} + \mathbf{e}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{s}^\intercal\mathbf{D}' + \mathbf{e}_\mathbf{P}^\intercal$$

By our choice of σ_{pre}, $\sigma_\mathbf{s}$, and p, we have $\|\mathbf{e}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{s}^\intercal\mathbf{D}'\| < \sqrt{\lambda}(m\sigma'_{\mathsf{pre}} + n(p-1)\sigma_\mathbf{s})$ and thus $\|\mathbf{e}_\mathbf{P}\| > \lambda^{\omega(1)}\|\mathbf{e}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{s}^\intercal\mathbf{D}'\|$. This implies $\mathbf{e}_\mathbf{P}^\intercal \approx_s \mathbf{e}_\mathbf{P}^\intercal + \mathbf{e}_\mathbf{A}^\intercal\mathbf{E} + \mathbf{s}^\intercal\mathbf{D}'$. Therefore, this hybrid is statistically indistinguishable from the previous one.

Hyb_2 **:** In this hybrid, we further replace $\mathbf{c}_\mathbf{P}$ and $\mathbf{D}$. Here, we sample $\mathbf{F} \leftarrow \mathbb{Z}_q^{n\times\ell}$ and set $\mathbf{c}_\mathbf{P} = \mathbf{s}^\intercal\mathbf{F} + \mathbf{e}_\mathbf{P}^\intercal$ and $\mathbf{D} = \lfloor \mathbf{F}/p \rfloor \bmod r$. This hybrid is essentially the same as previous hybrid. To see this, it suffices to see that the distribution of $(\mathbf{P} \bmod q, \mathbf{D} \bmod r) = (p\mathbf{D} + \mathbf{D}' \bmod q, \mathbf{D} \bmod r)$ in the previous hybrid is the same as $(\mathbf{F} \bmod q, \lfloor \mathbf{F}/p \rfloor \bmod r)$ in this hybrid.

Hyb_3**:** This is the D_1^{pre} distribution. Compared with the previous hybrid, here we replace $\mathbf{c}_\mathbf{B}$ and $\mathbf{c}_\mathbf{P}$ with random vectors with the same dimensions. The indistinguishability from the previous hybrid can be shown by a straightforward reduction to LWE.

Proving that $\mathbf{P}$ is distributed uniformly at random over $\mathbb{Z}_q^{n\times\ell}$. We argue that $\mathbf{P}$ is distributed uniformly at random over $\mathbb{Z}_q^{n\times\ell}$ since so is $\mathbf{AE}$. The latter can be shown by the leftover hash lemma (Lemma 3.8), which can be applied since the function family $\{\mathbf{e}\mapsto\mathbf{Ae}\}_{\mathbf{A}}$ is 2-universal. □

5 Counter-Examples for Private-Coin Evasive LWE

In this section, we present counter-examples for various versions of private coin Evasive LWE that have appeared in the literature.

5.1 Counter-Example for AKY Assumption

Theorem 5.1. There exists an efficient ELWE sampler Samp as defined in Assumption 3.13 such that the pre-condition holds, but the post-condition does not- i.e., there exists a distinguisher $\mathcal{A}^{\mathsf{post}}$ that distinguishes post-condition with non-negligible probability.

Proof. Our sampler uses a PRF with a contrived circuit implementation as described below.

PRF Circuit Description. Let $\mathsf{PRF}:\{\{1\}\times\{0,1\}^\lambda\}\times\{0,1\}^\lambda\to[-q/4+B,q/4-B]^\ell$ where B is chosen to be exponentially smaller than $q/4$[16]. Let $C_{\mathsf{PRF}_\mathbf{r}}$, with hardwired $\mathbf{r}$, outputting $\mathsf{PRF}(\mathsf{sd},\mathbf{r})$ (in binary) on input $\mathsf{sd}=(1,\widetilde{\mathsf{sd}})$, be any circuit implementing PRF. We construct a modified circuit $C'_{\mathsf{PRF}_\mathbf{r}}$ implementing PRF as follows.

1. Let C_0 be a circuit which outputs the first bit of its input $\mathbf{x}$. Further assume that the first bit of $\mathbf{x}$ is always 1.
2. To the output wire of $C_{\mathsf{PRF}_\mathbf{r}}$ corresponding to the lowest-order bit of $\mathsf{PRF}(\mathsf{sd},\mathbf{r})[1]$, attach a new gate which performs the correlation-inducing transformation described in Corollary 4.5, using the output wire of C_0 as the special "1" input. Inputs to C_0 can be the bits of sd.
3. To all the other output wires of $C_{\mathsf{PRF}_\mathbf{r}}$, attach a gate performing "even randomness" transformation as in Lemma 4.3.

Defining Evasive LWE Sampler. Let $n,m,\ell,Q,q\in\mathbb{N}$ be parameters and λ be the security parameter. The private coin sampler Samp with private coins $\mathsf{coins}^{\mathsf{Samp}}_{\mathsf{priv}}=(\mathsf{sd},\mathbf{R},\mathbf{e}_{\mathsf{att}},\mathbf{e}_{\mathsf{fhe}},\overline{\mathbf{A}}_{\mathsf{fhe}})$ of the Evasive LWE assumption is defined as follows. The sampler is almost the same as the one used by AKY [AKY24a] except that it uses contrived implementation of the PRF circuit. The sampler Samp on input 1^λ does the following:

1. Let $\{\mathcal{F}_{\mathsf{prm}}=\{f:\{0,1\}^L\to\{0,1\}^{1\times\ell}\}\}_{\mathsf{prm}}$ be a family of functions, where $f\in\mathcal{F}_{\mathsf{prm}}$ can be computed by a circuit of depth $\mathsf{dep}(\lambda)=\mathsf{poly}(\lambda)$ and $\mathsf{prm}=(1^{L(\lambda)},1^{\ell(\lambda)},1^{\mathsf{dep}(\lambda)})$. Choose $\{f_i\in\mathcal{F}_{\mathsf{prm}}\}_{i\in[Q]}$ and an input vector $\mathbf{x}\in\{0,1\}^L$ so that

$$(1^\lambda,\{f_i,f_i(\mathbf{x})\}_{i\in[Q]})\approx_c(1^\lambda,\{f_i,\Delta_i\}_{i\in[Q]}),$$

   where $\Delta_i\leftarrow\{0,1\}^{1\times\ell}$ for $i\in[Q]$. A concrete example of the choice for such $\mathbf{x}$ and f_i would be to define $\mathbf{x}$ as a random PRF seed and $f_i(\mathbf{x})$ as the PRF value on input i w.r.t the key $\mathbf{x}$.

   Define the following circuit C'_{f_i} implementing a scaled version of f_i. That is, C'_{f_i} takes $\mathbf{x}\in\{0,1\}^L$ as input and outputs $\lfloor q/2\rceil f_i(\mathbf{x})$. Start with any circuit C_{f_i} outputting $\lfloor q/2\rceil f_i(\mathbf{x})$ (in binary) on

[16] Note that fixing the first bit of seed to 1 does not affect PRF security, since the actual computation can always ignore the first bit.

input $\mathbf{x}$. To all the output wires of C_{f_i}, attach a gate performing "even randomness" transformation as in Lemma 4.3. We can observe that C'_{f_i} is of depth at most $d+3$.

2. Samples $\{\mathbf{r}_i \leftarrow \{0,1\}^\lambda\}_{i\in[Q]}$, $\widetilde{\mathsf{sd}} \leftarrow \{0,1\}^\lambda$ and set $\mathsf{sd} = (1, \widetilde{\mathsf{sd}})$.

3. Then it defines a function $\mathrm{F}_i = \mathrm{F}[f_i, \mathbf{r}_i]$ with $f_i, \mathbf{r}_i$ hardwired as follows: On input $(\mathbf{x}, \mathsf{sd})$, compute and output $f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) \in \mathbb{Z}_q^{1\times\ell}$. Let C'_{F_i} be a circuit that implements F_i and uses circuits C'_{f_i} and $C'_{\mathsf{PRF}_{\mathbf{r}_i}}$ to compute the respective components, and adds their outputs to get the final output of C'_{F_i}.

4. Samples $\mathbf{A}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(n+1)\times(\mathrm{L_X}+1)m}$ where $\mathrm{L_X} = m(\lambda+L+1)(n+1)\lceil\log q\rceil$. Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathsf{MakeVEvalCkt}(n, m, q, C'_{\mathrm{F}_i})$. Compute $\mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}}} = \mathsf{MEvalC}(\mathbf{A}_{\mathsf{att}}, \mathsf{VEval}_{C'_{\mathrm{F}_i}}) \in \mathbb{Z}_q^{(\mathrm{L_X}+1)m\times\ell}$ for all $i \in [Q]$. It then computes $\mathbf{A}_{\mathrm{F}_i} = \mathbf{A}_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}}}$ for all $i \in [Q]$ and sets $\mathbf{P} = (\mathbf{A}_{\mathrm{F}_1}, \ldots, \mathbf{A}_{\mathrm{F}_Q})$.

5. It then samples $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{s}}}$ and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.

6. Sample $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{R}_j \leftarrow \{0,1\}^{m\times m}$ for all $1 \le j \le (\mathrm{L}+\lambda+1)$ and compute a GSW encryption as follows.

$$\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \end{pmatrix}, \qquad \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L}+1)}$$

where $\mathbf{R} = (\mathbf{R}_1, \ldots, \mathbf{R}_{(\lambda+\mathrm{L}+1)})$. Let $\mathrm{L_X} = m(\lambda+\mathrm{L}+1)(n+1)\lceil\log q\rceil$ be the bit length of $\mathbf{X}$.

7. Sample $\mathbf{e}_{\mathsf{att}} \leftarrow \mathcal{D}^{(\mathrm{L_X}+1)m}_{\mathbb{Z},\sigma_{\mathsf{att}}}$ and compute $\mathbf{c}^\intercal_{\mathsf{att}} := \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X}))^{17} \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}}$.

8. Output

$$\begin{aligned} \mathbf{S} &= \mathbf{s}^\intercal \\ \mathsf{aux} &= (\mathbf{X},\ \mathbf{c}^\intercal_{\mathsf{att}}, f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}}) \\ \mathbf{P} &= (\mathbf{A}_{\mathrm{F}_1}, \ldots, \mathbf{A}_{\mathrm{F}_Q}). \end{aligned}$$

Counter-example Roadmap. Now, we show a counterexample to Evasive LWE (Assumption 3.13) with respect to the sampler specified above. This is proven by showing that the precondition distributions, as defined in Assumption 3.13 are computationally indistinguishable, while the postcondition distributions as defined in Assumption 3.13 are distinguishable.

Concretely, for our counter-example, we need to show that for $(\mathbf{s}^\intercal, \mathsf{aux}, \mathbf{P}) \leftarrow \mathsf{Samp}(1^\lambda)$, where $\mathsf{aux} = (\mathbf{X},\ \mathbf{c}^\intercal_{\mathsf{att}}, f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}})$ and $(\mathbf{B}, \mathbf{B}_\tau^{-1}) \leftarrow \mathsf{TrapGen}(1^{n+1}, 1^{m\log q}, q)$,

1. (Precondition) For all PPT adversary $\mathcal{A}^{\mathsf{pre}}$, the following two distributions, D^{pre}_0 and D^{pre}_1 are indistinguishable.

$$D^{\mathsf{pre}}_0 := \begin{pmatrix} \mathbf{B}, \mathbf{P},\ \mathbf{c}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \mathbf{s}^\intercal\mathbf{P} + (\mathbf{e}')^\intercal, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{att}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}}, \\ f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}} \end{pmatrix} \approx D^{\mathsf{pre}}_1 := \begin{pmatrix} \mathbf{B}, \mathbf{P},\ \mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1\times m\log q}, (\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times\ell Q}, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{att}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}}, \\ f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}} \end{pmatrix},$$

where, $\mathbf{e}_{\mathbf{B}} \leftarrow \mathcal{D}^{m\log q}_{\mathbb{Z},\sigma_{\mathbf{B}}}, \mathbf{e}' \leftarrow \mathcal{D}^{\ell Q}_{\mathbb{Z},\sigma_1}$. We prove this in claim 5.4.

[17] Note that AKY uses $\mathsf{bits}(1, \mathbf{X})$ in place of $(1, \mathsf{bits}(\mathbf{X}))$ to represent the same thing.

2. (Attack against postcondition) There exists an adversary $\mathcal{A}^{\mathsf{post}}$ who distinguishes the following distributions, D_0^{post} and D_1^{post} with non-negligible probability:

$$D_0^{\mathsf{post}} := \begin{pmatrix} \mathbf{B}, \mathbf{P}, & \mathbf{c}^\intercal = \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal, \mathbf{K}, \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \\ & \mathbf{c}_{\mathsf{att}}^\intercal = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal, \\ & f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}} \end{pmatrix}$$

$$D_1^{\mathsf{post}} := \begin{pmatrix} \mathbf{B}, \mathbf{P}, & \mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1 \times m \log q}, \mathbf{K}, \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \\ & \mathbf{c}_{\mathsf{att}}^\intercal = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal, \\ & f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}} \end{pmatrix}$$

where $\mathbf{e}_{\mathbf{B}} \leftarrow \mathcal{D}_{\mathbb{Z}, \sigma_{\mathbf{B}}}^{m \log q}, \mathbf{K}_i \leftarrow \mathbf{B}_\tau^{-1}(\mathbf{A}_{\mathrm{F}_i})$ and $\mathbf{K} = (\mathbf{K}_1, \ldots, \mathbf{K}_Q)$.

Parameter Setting. We set our parameters the same as AKY.

$$\tilde{\beta} = 2^{O(\mathsf{dep} \cdot \log^3 \lambda)}, \quad q \in (2^{8\lambda}\tilde{\beta}, 2^{8\lambda+1}\tilde{\beta}], \quad n = \mathrm{poly}(\lambda, \mathsf{dep}), \quad m = O(n \log q),$$
$$\tau = O\left(\sqrt{(n+1)\log q}\right), \quad B = 2^{6\lambda}\tilde{\beta}, \quad \sigma_{\mathbf{s}} = \sigma_{\mathsf{fhe}} = \sigma_{\mathsf{att}} = \sigma = 2^{2\lambda}, \quad \sigma_{\mathbf{B}} = 2^{5\lambda}\tilde{\beta},$$
$$\sigma_1 = 2^{4\lambda + O(1)}\tilde{\beta}/\mathrm{poly}(\lambda), \quad Q = \lambda + mw + (\mathrm{L_X} + 1)m$$

Distinguishing Algorithm/Attack Strategy. The adversary $\mathcal{A}^{\mathsf{post}}$ holds the distribution D_β^{post} for $\beta \leftarrow \{0, 1\}$. Thus, for $\beta = 0$, $\mathbf{c}^\intercal = \mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal$, and for $\beta = 1$, $\mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1 \times m \log q}$. It does the following:

1. For each $i \in [Q]$, compute $\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} = \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{att}}, \mathsf{VEval}_{C'_{\mathrm{F}_i}}, (1, \mathsf{bits}(\mathbf{X})))$ and

$$\mathbf{z}_i = \mathbf{c}^\intercal \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} \mod q$$

2. For all $i \in [Q]$ and $j \in [\ell]$, set $y_{i,j} = 0$, if $z_{i,j} \in [-q/4, q/4)$ and $y_{i,j} = 1$ otherwise, where $z_{i,j}$ is the j-th element of $\mathbf{z}_i$. Now it subtracts $\mathbf{y}_i^\intercal \lfloor q/2 \rceil$ [18] from $\mathbf{z}_i$ to get

$$\begin{aligned} \forall i \in [Q], \ \tilde{\mathbf{z}}_i &= \mathbf{z}_i - \mathbf{y}_i^\intercal \lfloor q/2 \rceil \mod q \\ &= \mathbf{c}^\intercal \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} - \mathbf{y}_i^\intercal \lfloor q/2 \rceil \mod q \end{aligned}$$

where $\mathbf{y}_i^\intercal = (y_{i,1}, \ldots, y_{i,\ell})$.

3. Let $w = \lceil \log_2 q \rceil$. $\mathcal{A}^{\mathsf{post}}$ defines the following set of linear equations (Equation (21)) in variables $\mathbf{e}_{\mathbf{B}}[1], \ldots, \mathbf{e}_{\mathbf{B}}[mw]$ and $\mathbf{e}_{\mathsf{att}}[1], \ldots, \mathbf{e}_{\mathsf{att}}[(\mathrm{L_X} + 1)m]$ and outputs $\beta' = 0$ if (21) is solvable; otherwise, output $\beta' = 1$.

$$\begin{aligned} &\mathbf{e}_{\mathbf{B}}[1]\mathbf{K}_1[1,1] + \ldots + \mathbf{e}_{\mathbf{B}}[mw]\mathbf{K}_1[mw,1] - \mathbf{e}_{\mathsf{att}}[1]\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_1}[1,1] - \ldots \\ &\qquad - \mathbf{e}_{\mathsf{att}}[(\mathrm{L_X} + 1)m]\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_1}[(\mathrm{L_X} + 1)m, 1] = \tilde{\mathbf{z}}_1[1] \bmod 2 \\ &\mathbf{e}_{\mathbf{B}}[1]\mathbf{K}_2[1,1] + \ldots + \mathbf{e}_{\mathbf{B}}[mw]\mathbf{K}_2[mw,1] - \mathbf{e}_{\mathsf{att}}[1]\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_2}[1,1] - \ldots \\ &\qquad - \mathbf{e}_{\mathsf{att}}[(\mathrm{L_X} + 1)m]\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_2}[(\mathrm{L_X} + 1)m, 1] = \tilde{\mathbf{z}}_2[1] \bmod 2 \\ &\qquad \vdots \\ &\mathbf{e}_{\mathbf{B}}[1]\mathbf{K}_Q[1,1] + \ldots + \mathbf{e}_{\mathbf{B}}[mw]\mathbf{K}_Q[mw,1] - \mathbf{e}_{\mathsf{att}}[1]\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_Q}[1,1] - \ldots \\ &\qquad - \mathbf{e}_{\mathsf{att}}[(\mathrm{L_X} + 1)m]\mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_Q}[(\mathrm{L_X} + 1)m, 1] = \tilde{\mathbf{z}}_Q[1] \bmod 2 \end{aligned} \tag{21}$$

[18] observe that $\mathbf{y}_i^\intercal = f_i(\mathbf{x})$ in case of $\beta = 0$.

Analyzing success probability of $\mathcal{A}^{\mathsf{post}}$.

Claim 5.2. $\mathcal{A}^{\mathsf{post}}$ wins (i,e., $\beta = \beta'$) with $3/4 - \mathsf{negl}(\lambda)$ probability when $Q \geq \lambda + mw + (\mathrm{L_X} + 1)m$.

Proof. Let us first analyze the solvability of equations defined in (21) for the two cases: $\beta = 0$ and $\beta = 1$.

When $\beta = 0$,

$$\begin{aligned}
\forall i \in [Q],\ \mathbf{z}_i &= \mathbf{c}^\intercal \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= (\mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal) \cdot \mathbf{K}_i - (\mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal) \cdot \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= \mathbf{s}^\intercal \mathbf{B} \mathbf{K}_i + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{s}^\intercal \mathbf{A}_{\mathsf{att}} \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}}} + \mathbf{s}^\intercal \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathsf{bits}(\mathbf{X})) - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= \mathbf{s}^\intercal \mathbf{A}_{\mathrm{F}_i} + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{s}^\intercal \mathbf{A}_{\mathrm{F}_i} + \mathrm{F}_i(\mathbf{x}, \mathsf{sd}) - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i + f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}
\end{aligned} \tag{22}$$

where $\mathbf{R}_{C'_{\mathrm{F}_i}}$ is the randomness in the homomorphically evaluated encryption of $\mathrm{F}_i(\mathbf{x}, \mathsf{sd})$. Let the depth of C_{F_i} be $d = \mathrm{poly}(\lambda)$ and from Lemma 3.15, the depth of $\mathsf{VEval}_{C_{\mathrm{F}_i}}$ is

$$d_{\mathsf{VEval}_{C_{\mathrm{F}_i}}} = (dO(\log m \log\log q) + O(\log^2 \log q)).$$

The depth of circuit C'_{F_i} increases at most by constant $O(1)$ from d due to the addition of even randomness and correlation-inducing gate, and hence, it is $d + O(1)$. The depth of $\mathsf{VEval}_{C'_{\mathrm{F}_i}}$ is

$$d_{\mathsf{VEval}_{C'_{\mathrm{F}_i}}} = ((d + O(1))O(\log m \log\log q) + O(\log^2 \log q)).$$

From Lemma 3.15 and parameter setting, we have

$$\begin{aligned}
||\mathbf{R}_{C'_{\mathrm{F}_i}}|| &\leq (m+2)^{d+O(1)} \lceil \log q \rceil \max_{\ell \in [L+\lambda+1]} ||\mathbf{R}_\ell^\intercal|| \\
&\leq (m+2)^{d+O(1)} \lceil \log q \rceil\, m \\
&\leq (m+2)^{d+O(1)} \lceil \log q \rceil \leq \tilde{\beta}
\end{aligned}$$

and using the depth bound as in Section 3.7, we have

$$\left\| \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \right\| \leq (m+2)^{d_{\mathsf{VEval}_{C'_{\mathrm{F}_i}}}} \lceil \log q \rceil \leq \tilde{\beta}$$

Now, from parameter setting, we have

$$||\mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} + \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}|| \leq 2^{2\lambda+1}\sqrt{\lambda}\tilde{\beta} \leq 2^{3\lambda}\tilde{\beta}$$

and

$$||\mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}|| \leq 2^{5\lambda+1}\sqrt{\lambda}\tilde{\beta} + 2^{3\lambda}\tilde{\beta} < 2^{6\lambda}\tilde{\beta} < B$$

Hence, $||\mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}|| < (q/4 - B) + B = q/4$, $\mathcal{A}^{\mathsf{post}}$ will correctly recover $f_i(\mathbf{x})$ i.e. $\mathbf{y}_i^\intercal = f_i(\mathbf{x})$ and hence, we will have

$$\begin{aligned}
&\forall i \in [Q], \\
&\tilde{\mathbf{z}}_i = f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} - f_i(\mathbf{x}) \lfloor q/2 \rceil \\
&= \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \in [-q/4, q/4] \quad \text{over integer}
\end{aligned}$$

We prove in Claim 5.3 that $\forall i \in [Q],\ \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}} \mathbf{R}_{C'_{\mathrm{F}_i}}[1] = 0 \bmod 2$ with probability $\geq 1/2$. This gives us that with probability $\geq 1/2$,

$$\forall i \in [Q],\ \tilde{\mathbf{z}}_i[1] = \mathbf{e}_{\mathbf{B}}^{\mathsf{T}} \mathbf{K}_i[1] - \mathbf{e}_{\mathsf{att}}^{\mathsf{T}} \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}[1] \mod 2.$$

Observe that this is the same as the set of equations defined in (21). Hence, in case of $\beta = 0$, (21) is solvable with probability $1/2 + \mathsf{negl}(\lambda)$. This gives us

$$\Pr\left(\beta' = 0 \mid \beta = 0\right) = 1/2 + \mathsf{negl}(\lambda). \tag{23}$$

When $\beta = 1$,

$$\forall i \in [Q],\ \mathbf{z}_i = \mathbf{c}^{\mathsf{T}} \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}'},$$

where $\mathbf{c} \leftarrow \mathbb{Z}_q^{mw}$.

Here, we argue that the distribution of $\{\mathbf{c}_{\mathbf{B}}^{\mathsf{T}} \cdot \mathbf{K}_i \bmod q\}_{i \in [Q]}$ is statistically close to uniform distribution over $(\mathbb{Z}_q^{1 \times \ell})^Q$, even given $\{\mathbf{K}_i \bmod 2\}_{i \in [Q]}$. To see this, we first observe that by Lemma 3.7, each column of $\mathbf{K}_i[\cdot, j]$ has min-entropy at least $mw \log(\sigma_{-1}/\lambda) > 2mw$ except for negligible probability over $\mathbf{B}$ and $(\mathbf{K}_i[\cdot, j] \bmod 2)$ can be represented by a string of mw-bits. We then apply the generalized Leftover Hash Lemma Lemma 3.8, which implies that the two distributions are within statistical distance $Q\sqrt{2^{mw} \cdot 2^{-2mw} q} = \mathsf{negl}(\lambda)$ by our choice of parameters. We therefore have that $\{\mathbf{z}_i \bmod q\}_{i \in [Q]}$ is distributed uniformly at random over $(\mathbb{Z}_q^{1 \times \ell})^Q$, even given $\{\mathbf{K}_i \bmod 2\}_i$. This, in turn, implies $\{\mathbf{z}_i \bmod 2\}_{i \in [Q]}$ (which forms the RHS of equations in Equation (21)) is also statistically close to a uniform distribution independent of $\{\mathbf{K}_i \bmod 2\}_i$ when $\beta = 1$. Hence, Equation (21), having $mw + (\mathrm{L_X} + 1)m$ number of variables, is unsolvable with overwhelming probability if $Q > \lambda + mw + (\mathrm{L_X} + 1)m$, since the RHS of the equation falls into the space for which there exists a solution with probability at most $2^{mw + (\mathrm{L_X}+1)m} / 2^{\lambda + mw + (\mathrm{L_X}+1)m} = 2^{-\lambda}$.

This gives us

$$\Pr\left(\beta' = 1 \mid \beta = 1\right) \geq 1 - \mathsf{negl}(\lambda). \tag{24}$$

Thus, from Equation (23) and (24), we get $\Pr(\beta' = \beta) \geq 3/4 - \mathsf{negl}(\lambda)$. □

Claim 5.3. $\forall i \in [Q],\ \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}} \mathbf{R}_{C'_{\mathrm{F}_i}}[1] = 0 \bmod 2$ with probability $1/2 + \mathsf{negl}(\lambda)$.

Proof. Let us start by analyzing the $\tilde{\mathbf{e}}_{\mathsf{fhe}}^{\mathsf{T}}[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}} \mathbf{R}_{C'_{\mathrm{F}_i}}[1]$ error. Recall that $\mathbf{R}_{C'_{\mathrm{F}_i}}$ is the randomness in the homomorphically evaluated encryption of $\mathrm{F}_i(\mathbf{x}, \mathsf{sd})$ (of different form: $\mathbf{A}_{\mathsf{fhe}} \mathbf{R}_{C'_{\mathrm{F}_i}} - \begin{pmatrix} 0^{n \times \ell} \\ \mathrm{F}_i(\mathbf{x}, \mathsf{sd}) \end{pmatrix}$), output by $\mathsf{VEval}_{C'_{\mathrm{F}_i}}$ circuit. Since $\mathrm{F}_i(\mathbf{x}, \mathsf{sd}) = f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)$, we can write $\tilde{\mathbf{e}}_{\mathsf{fhe}}^{\mathsf{T}}[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}} \mathbf{R}_{C'_{\mathrm{F}_i}}[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}} \mathbf{R}_{C'_{f_i}}[1] + \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}} \mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}}}[1]$ because the additive property is preserved after homomorphic addition.

We recall from Section 3.6 that for any circuit $C : \{0,1\}^L \to \mathbb{Z}_q^{1 \times \ell}$, VEval_C on input $\mathbf{X}$ - a GSW encryption of some $\mathbf{x} \in \{0,1\}^L$ - outputs $\mathbf{A}_{\mathsf{fhe}} \mathbf{R}_C - \begin{pmatrix} 0^{n \times \ell} \\ C(\mathbf{x}) \end{pmatrix}$. Let $C(\mathbf{x})[u, v] \in \{-1, 0, 1\}$ be (the signed version of) the v-th bit of $C(\mathbf{x})[u] \in \mathbb{Z}_q$, for $u \in [\ell]$ and $v \in [0, w)$, $w = \lceil \log_2 q \rceil$, then VEval_C computation firstly homomorphically computes GSW encryption of $C(\mathbf{x})[u, v]$, which is of the form $\mathbf{C}_{u,v} = \mathbf{A}_{\mathsf{fhe}} \mathbf{R}_{C,u,v} - C(\mathbf{x})[u, v]\mathbf{G}$. Then for each $u \in [\ell]$, it linearly aggregates $\{\mathbf{C}_{u,v}\}_{v \in [0, w-1]}$ to get $\mathbf{C}_u = \mathbf{A}_{\mathsf{fhe}} \mathbf{R}_{C,u} - \begin{pmatrix} 0^{n \times 1} \\ C(\mathbf{x})[u] \end{pmatrix}$ as $\mathbf{C}_u = \sum_v \mathbf{C}_{u,v} \mathbf{G}^{-1}(2^v \iota_{n+1})$. In particular,

$$\mathbf{R}_{C,u} = \sum_v \mathbf{R}_{C,u,v} \mathbf{G}^{-1}(2^v \iota_{n+1}), \text{ and } \mathbf{R}_C = (\mathbf{R}_{C,1}, \ldots, \mathbf{R}_{C,\ell}).$$

Coming back to our analysis, $(\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{f_i}})[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{f_i},1} = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=0}^{w-1}\mathbf{R}_{C'_{f_i},1,v}\mathbf{G}^{-1}(2^v\iota_{n+1})$, where $\mathbf{R}_{C'_{f_i},1}$ is the first column of $\mathbf{R}_{C'_{f_i}}$ and $\mathbf{R}_{C'_{f_i},1,v}$ is the randomness in homomorphically computed GSW encryption of the v-th bit of $f_i(\mathbf{x})\,\lfloor q/2\rceil\,[1]$. Since $f_i(\mathbf{x})\,\lfloor q/2\rceil$ is implemented by C'_{f_i}, which involves the even randomness transformation (Lemma 4.3) on all its output bits, $\mathbf{R}_{C'_{f_i},1,v}$ has all the entries as even due to Lemma 4.3. This implies $\mathbf{R}_{C'_{f_i},1}$ has even entries, which in turn implies that $(\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{f_i}})[1]$ is even.

So, now our goal is to show that

$$\mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1] - (\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}}})[1] = 0 \bmod 2$$

Similar to above, we have $(\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}}})[1] = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1} = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=0}^{w-1}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1,v}\mathbf{G}^{-1}(2^v\iota_{n+1})$.

Again, since in $C'_{\mathsf{PRF}_{\mathbf{r}_i}}$ all the output bits pass through even randomness, except the lowest order bit of the first entry, which passes through the correlation inducing gate, we have

$$\begin{aligned}
& \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1] - (\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}}})[1] \bmod 2 \\
= \;& \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1,0}\mathbf{G}^{-1}(\iota_{n+1}) - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=1}^{w-1}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1,v}\mathbf{G}^{-1}(2^v\iota_{n+1}) \bmod 2 \\
= \;& \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1,0}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \quad \text{(due to Lemma 4.3)} \\
= \;& \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1,0] + \sum_{v=1}^{w-2}2^v\mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1,v] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1,0}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
= \;& \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1,0] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_{\mathbf{r}_i}},1,0}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
= \;& \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1,0] - \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1,0]\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
& \qquad\qquad\qquad\qquad\qquad\qquad \text{(due to Corollary 4.5)} \\
= \;& 0 \bmod 2, \text{ if } \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \text{ is odd.}
\end{aligned}$$

In the above, $\mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[u,v]$ represents the v-th bit in the binary representation of $\mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[u]$ and $\mathbf{R}^*$ is the randomness in the ciphertext of special "1" input used in Corollary 4.5. We then argue that $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1})$ is odd with probability negligibly close to $1/2$. To see this, we first observe that each entry of $\mathbf{R}^*$ is distributed over $\{0,1\}$ uniformly at random and thus so is each entry of $\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2$. In particular, this implies that $\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2$ is a non-zero vector with overwhelming probability.We then observe that each entry of $\mathbf{e}_{\mathsf{fhe}} \bmod 2$ is statistically close to the uniform distribution over $\{0,1\}$ by Lemma 3.10. Combining these facts, it follows that the distribution of $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2$ is statistically close to the uniform distribution over $\{0,1\}$, as desired. Note that the term $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1})$ does not depend on i and hence, for all $i \in [Q]$, the probability that $\mathsf{PRF}(\mathsf{sd},\mathbf{r}_i)[1] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{F}_i}}[1] = 0 \bmod 2$ is $1/2 + \mathsf{negl}(\lambda)$.Hence, the proof. □

Proving the pre-condition. We now show that the pre-condition of ELWE holds with respect to the above sampler defined in Section 5.1.

Claim 5.4. For $(\mathbf{s}^{\mathsf{T}}, \mathsf{aux}, \mathbf{P}) \leftarrow \mathsf{Samp}(1^\lambda)$, where $\mathsf{aux} = (\mathbf{X}, \mathbf{c}_{\mathsf{att}}^{\mathsf{T}}, f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}})$,

$$D_0^{\mathsf{pre}} := \begin{pmatrix} \mathbf{B}, \mathbf{P}, \;\; \mathbf{c}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\mathbf{B} + \mathbf{e}_{\mathbf{B}}^{\mathsf{T}}, (\mathbf{c}')^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\mathbf{P} + (\mathbf{e}')^{\mathsf{T}}, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \\ \mathbf{c}_{\mathsf{att}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^{\mathsf{T}}, \\ f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}} \end{pmatrix} \approx D_1^{\mathsf{pre}} := \begin{pmatrix} \mathbf{B}, \mathbf{P}, \;\; \mathbf{c}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times m\log q}, (\mathbf{c}')^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times \ell Q}, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \\ \mathbf{c}_{\mathsf{att}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^{\mathsf{T}}, \\ f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}} \end{pmatrix}$$

where Samp is as defined in Section 5.1, $\mathbf{e}_{\mathbf{B}} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_{\mathbf{B}}}^{m\log q}$ and $\mathbf{e}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_1}^{\ell Q}$.

Proof. To prove this, we introduce one intermediate distribution $D^{\mathsf{pre}}_{\mathsf{inter}}$ as

$$D^{\mathsf{pre}}_{\mathsf{inter}} := \left(\begin{array}{r} \mathbf{B}, \mathbf{P}, \quad \mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1\times m\log q}, (\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times \ell Q}, \\ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))}, \\ \mathbf{c}^\intercal_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{1\times(\mathrm{L}_\mathbf{X}+1)m}, \\ f_1,\ldots,f_Q,\mathbf{r}_1,\ldots,\mathbf{r}_Q,\mathbf{A}_{\mathsf{att}} \end{array}\right)$$

and then prove that $D^{\mathsf{pre}}_0 \approx D^{\mathsf{pre}}_{\mathsf{inter}}$ and $D^{\mathsf{pre}}_{\mathsf{inter}} \approx D^{\mathsf{pre}}_1$. This implies, $D^{\mathsf{pre}}_0 \approx D^{\mathsf{pre}}_1$.

Proof of $D^{\mathsf{pre}}_0 \approx D^{\mathsf{pre}}_{\mathsf{inter}}$

Note that the distribution D^{pre}_0 and $D^{\mathsf{pre}}_{\mathsf{inter}}$ is exactly the same as the L.H.S and R.H.S distribution (respectively) in equation (4) of the security proof of Functional Encryption for pseudorandom functionality (prFE) construction as in [AKY24a]. Hence, almost the same security proof of prFE applies to the proof of Claim 5.4. However, for completeness, we provide the full proof here.Since, $(\mathbf{c}')^\intercal = \mathbf{s}^\intercal\mathbf{P} + (\mathbf{e}')^\intercal = (\mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_1} + (\mathbf{e}_{\mathbf{P},1})^\intercal, \ldots, \mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_Q} + (\mathbf{e}_{\mathbf{P},Q})^\intercal) = \{\mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_i} + (\mathbf{e}_{\mathbf{P},i})^\intercal\}_{i\in[Q]} = \{\mathbf{c}^\intercal_{\mathbf{P},i}\}_{i\in[Q]}$, it suffices to prove the following Equation (25).

$$D^{\mathsf{pre}}_0 := \left(\begin{array}{r} \mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}, \quad \mathbf{c}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \{\mathbf{c}_{\mathbf{P},i} = \mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_i} + (\mathbf{e}'_i)^\intercal\}_{i\in[Q]}, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x},\mathsf{sd})\otimes\mathbf{G}, \\ \mathbf{c}^\intercal_{\mathsf{att}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1,\mathsf{bits}(\mathbf{X}))\otimes\mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}}, \\ f_1,\ldots,f_Q,\mathbf{r}_1,\ldots,\mathbf{r}_Q,\mathbf{A}_{\mathsf{att}} \end{array}\right) \tag{25}$$

$$\approx D^{\mathsf{pre}}_{\mathsf{inter}} := \left(\begin{array}{r} \mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}, \quad \mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1\times m\log q}, \{\mathbf{c}_{\mathbf{P},i} \leftarrow \mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]}, \\ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))}, \\ \mathbf{c}^\intercal_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{1\times(\mathrm{L}_\mathbf{X}+1)m}, \\ f_1,\ldots,f_Q,\mathbf{r}_1,\ldots,\mathbf{r}_Q,\mathbf{A}_{\mathsf{att}} \end{array}\right)$$

where $\mathbf{e}'_i \leftarrow \mathcal{D}^\ell_{\mathbb{Z},\sigma_1}$ for all $i \in [Q]$. We prove Equation (25) via the following sequence of hybrids.

Hyb_0**.** This is L.H.S distribution of Equation (25).

Hyb_1**.** This hybrid is same as Hyb_0, except we compute $\mathbf{c}^\intercal_{\mathbf{P},i}$ as

$$\mathbf{c}^\intercal_{\mathbf{P},i} = \mathbf{c}^\intercal_{\mathsf{att}}\cdot\mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} + f_i(\mathbf{x})\lfloor q/2\rceil + \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i) + \mathbf{e}^\intercal_{\mathbf{P},i}$$

where $\mathbf{e}_{\mathbf{P},i} \leftarrow \mathcal{D}^\ell_{\mathbb{Z},\sigma_1}$. We claim that Hyb_1 and Hyb_2 are statistically indistinguishable. To see this, note that from Equation (22), we have :

$$\mathbf{c}^\intercal_{\mathsf{att}}\cdot\mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} = \mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_i} - f_i(\mathbf{x})\lfloor q/2\rceil - \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i) + \mathbf{e}^\intercal_{\mathrm{F}_i}$$

where $\mathbf{e}^\intercal_{\mathrm{F}_i} = \mathbf{e}^\intercal_{\mathsf{fhe}}\mathbf{R}_{C'_{\mathrm{F}_i}} + \mathbf{e}^\intercal_{\mathsf{att}}\mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}$. This implies,

$$\mathbf{c}^\intercal_{\mathbf{P},i} = \mathbf{c}^\intercal_{\mathsf{att}}\cdot\mathbf{H}^{\mathrm{F}_i}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} + f_i(\mathbf{x})\lfloor q/2\rceil + \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i) + \mathbf{e}^\intercal_{\mathbf{P},i} = \mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_i} + \mathbf{e}^\intercal_{\mathrm{F}_i} + \mathbf{e}^\intercal_{\mathbf{P},i}$$

where $||\mathbf{e}^\intercal_{\mathrm{F}_i}|| \le 2^{3\lambda}\tilde{\beta}$ as proved in Claim 5.2.

Next, we note that $||\mathbf{e}^\intercal_{\mathrm{F}_i}|| \le 2^{4\lambda+O(1)}\beta/\mathrm{poly}(\lambda) = ||\mathbf{e}_{\mathbf{P},i}||$. Thus by noise flooding (Lemma 3.9) we have $\mathbf{e}^\intercal_{\mathrm{F}_i} + \mathbf{e}^\intercal_{\mathbf{P},i} \approx_s \mathbf{e}^\intercal_{\mathbf{P},i}$ with a statistical distance of $\mathsf{negl}(\lambda)$. Thus, it suffices to show the pseudorandomness of the following distribution given $f_1,\ldots,f_Q,\mathbf{r}_1,\ldots,\mathbf{r}_Q,\mathbf{A}_{\mathsf{att}}$.

$$\left(\begin{array}{r} \mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}, \quad \mathbf{c}^\intercal = \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}, \{\tilde{\mathrm{F}}_i = f_i(\mathbf{x})\lfloor q/2\rceil + \mathsf{PRF}(\mathsf{sd},\mathbf{r}_i) + \mathbf{e}^\intercal_{\mathbf{P},i}\}_{i\in[Q]}, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x},\mathsf{sd})\otimes\mathbf{G}, \mathbf{c}^\intercal_{\mathsf{att}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1,\mathsf{bits}(\mathbf{X}))\otimes\mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}} \end{array}\right)$$

Hyb_2. This hybrid is same as Hyb_1 except that, we sample $\mathbf{c} \leftarrow \mathbb{Z}_q^{mw}$, $\mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{m}$ and $\mathbf{A}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$, where $\mathbf{A}_{\mathsf{fhe}}$ is the fhe public key used to compute $\mathbf{X}$. We have $\mathsf{Hyb}_1 \approx_c \mathsf{Hyb}_2$ using LWE.
To prove this, we show that if there exists an adversary $\mathcal{A}$ who can distinguish between the two hybrids with non-negligible advantage, then there is a reduction $\mathcal{B}$ that breaks LWE security with non-negligible advantage. The reduction is as follows.

1. On receiving security parameter from $\mathcal{A}$, forward it to LWE challenger.
2. The LWE challenger samples $\beta \leftarrow \{0,1\}$. It also samples $\mathbf{A}_{\mathsf{LWE}} \leftarrow \mathbb{Z}_q^{n\times(mw+m+(\mathrm{L}_{\mathrm{X}}+1)m)}$, $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathsf{s}}}$ and sets $\mathbf{b}^\intercal = \bar{\mathbf{s}}^\intercal\mathbf{A}_{\mathsf{LWE}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \in \mathbb{Z}_q^{1\times(mw+m+(\mathrm{L}_{\mathrm{X}}+1)m)}$ if $\beta = 0$, else it samples $\mathbf{b}^\intercal \leftarrow \mathbb{Z}_q^{1\times(mw+m+(\mathrm{L}_{\mathrm{X}}+1)m)}$ if $\beta = 1$. Sends $(\mathbf{A}_{\mathsf{LWE}}, \mathbf{b})$ to $\mathcal{B}$.
3. $\mathcal{B}$ parses $\mathbf{A}_{\mathsf{LWE}} = (\mathbf{B}',\ \hat{\mathbf{A}}_{\mathsf{fhe}},\ \mathbf{A}'_{\mathsf{att}})$, where $\mathbf{B}' \in \mathbb{Z}_q^{n\times mw}$, $\hat{\mathbf{A}}_{\mathsf{fhe}} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{A}'_{\mathsf{att}} \in \mathbb{Z}_q^{n\times((\mathrm{L}_{\mathrm{X}}+1)m)}$ and $\mathbf{b}^\intercal = (\mathbf{b}^\intercal_{\mathbf{B}},\ \mathbf{b}^\intercal_{\mathsf{fhe}},\ \mathbf{b}^\intercal_{\mathsf{att}})$.
4. Choose $\{f_i \in \mathcal{F}_{\mathsf{prm}}\}_{i\in[Q]}$ and an input vector $\mathbf{x} \in \{0,1\}^L$.
5. Samples $\{\mathbf{r}_i \leftarrow \{0,1\}^\lambda\}_{i\in[Q]}$, $\widetilde{\mathsf{sd}} \leftarrow \{0,1\}^\lambda$ and set $\mathsf{sd} = (1, \widetilde{\mathsf{sd}})$.
6. Samples $\hat{\mathbf{b}} \leftarrow \mathbb{Z}_q^{mw}$ and sets $\mathbf{B} = \begin{pmatrix}\mathbf{B}'\\ \hat{\mathbf{b}}^\intercal\end{pmatrix}$ and $\mathbf{c}^\intercal := \mathbf{b}^\intercal_{\mathbf{B}} - \hat{\mathbf{b}}^\intercal$.
7. Sets $\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix}\hat{\mathbf{A}}_{\mathsf{fhe}}\\ \mathbf{b}^\intercal_{\mathsf{fhe}}\end{pmatrix}$ and computes $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}$ as in the construction.
8. Sets $\bar{\mathbf{A}}_{\mathsf{att}} = \mathbf{A}'_{\mathsf{att}} + (1, \mathsf{bits}(\mathbf{X})) \otimes \bar{\mathbf{G}}$, $\mathbf{A}_{\mathsf{att}} = \begin{pmatrix}\bar{\mathbf{A}}_{\mathsf{att}}\\ \mathbf{a}^\intercal_{\mathsf{att}}\end{pmatrix}$, where $\mathbf{a}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L}_{\mathrm{X}}+1)m}$, and $\mathbf{c}^\intercal_{\mathsf{att}} = \mathbf{b}^\intercal_{\mathsf{att}} - (\mathbf{a}^\intercal_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \underline{\mathbf{G}})$, where $\bar{\mathbf{G}}$ and $\underline{\mathbf{G}}$ denotes the first n rows and $n+1$-th row of the gadget matrix $\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m}$, respectively.
9. Compute $\tilde{\mathrm{F}}_i$ and $\{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}$ as in hybrid 1.
10. Sends $(\mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}, \mathbf{c}^\intercal, \tilde{\mathrm{F}}_i, \mathbf{X}, \mathbf{c}^\intercal_{\mathsf{att}}, f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}})$ to $\mathcal{A}$.
11. $\mathcal{A}$ outputs a bit β'. $\mathcal{B}$ forwards the bit β' to the LWE challenger.

It is easy to see that if LWE challenger sent $\mathbf{b}^\intercal = \bar{\mathbf{s}}^\intercal\mathbf{A}_{\mathsf{LWE}} + \mathbf{e}^\intercal_{\mathsf{LWE}}$, then $\mathcal{B}$ simulated Hyb_1 with $\mathcal{A}$ else if LWE challenger sent random $\mathbf{b} \leftarrow \mathbb{Z}_q^{mw+m+(\mathrm{L}_{\mathrm{X}}+1)m}$ then $\mathcal{B}$ simulated Hyb_2 with $\mathcal{A}$.
Thus, it suffices to show the pseudorandomness of the following distribution given $f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}}$.

$$\left(\mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]},\ \ \mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1\times m\log q}, \{\tilde{\mathrm{F}}_i = f_i(\mathbf{x})\,\lfloor q/2\rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}^\intercal_{\mathbf{P},i}\}_{i\in[Q]},\right.$$
$$\left.\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}, \mathbf{c}^\intercal_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{1\times(\mathrm{L}_{\mathrm{X}}+1)m}\right)$$

Hyb_3. This hybrid is same as Hyb_2 except that we sample $\mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))}$. We have $\mathsf{Hyb}_2 \approx_s \mathsf{Hyb}_3$ using leftover hash lemma. We now argue that $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}$ is statistically close to a uniform distribution over $\mathbb{Z}_q^{(n+1)\times(m(\lambda+L+1))}$. This can be seen by noting that, for a uniformly sampled vector of length m where the entries are sampled from $\{0,1\}$, the min-entropy is m. This implies the min-entropy of each column of $\mathbf{R}$ is m. Furthermore, by the Leftover Hash Lemma (Lemma 3.8), each entry of $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}$ is statistically close to being uniformly distributed over $\mathbb{Z}_q$, with statistical distance $\mathsf{negl}(\lambda)$. This implies that the same holds for $\mathbf{X}$. Thus, it suffices to show the pseudorandomness of the following distribution given $f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}}$.

$$\left(\mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]},\ \ \mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1\times m\log q}, \{\tilde{\mathrm{F}}_i = f_i(\mathbf{x})\,\lfloor q/2\rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}^\intercal_{\mathbf{P},i}\}_{i\in[Q]},\right.$$
$$\left.\mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))}, \mathbf{c}^\intercal_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{1\times(\mathrm{L}_{\mathrm{X}}+1)m}\right)$$

Hyb_4. This hybrid is the same as the previous one except that we replace $\mathsf{PRF}(\mathsf{sd},\cdot)$ with the real random function $\mathsf{R}(\cdot)$. Since sd is not used anywhere else, we can use the security of PRF to conclude that this hybrid is computationally indistinguishable from the previous one.

Hyb_5. This hybrid is same as the previous one except that we output a failure symbol if the set $\{\mathbf{r}_i\}_{i\in[Q]}$, in aux, contains a collision. We prove that the probability with which there occurs a collision is negligible in λ. To prove this it suffices to show that there is no $i,i' \in [Q]$ such that $i \neq i'$ and $\mathbf{r}_i = \mathbf{r}_{i'}$. The probability of this happening can be bounded by $Q^2/2^\lambda$ by taking the union bound with respect to all the combinations of i,i'. Thus, the probability of outputting the failure symbol is $Q^2/2^\lambda$, which is $\mathsf{negl}(\lambda)$.

Hyb_6. In this hybrid we compute $\tilde{\mathsf{F}}_i$ as

$$\tilde{\mathsf{F}}_i = f_i(\mathbf{x})\,\lfloor q/2\rceil + R_i + \mathbf{e}^\mathsf{T}_{\mathbf{P},i}$$

for all $i \in [Q]$. Namely, we use fresh randomness $R_i \leftarrow [-q/4+B, q/4-B]^{1\times\ell}$ instead of deriving the randomness by $R(\mathbf{r}_i)$. We claim that this change is only conceptual. To see this, we observe that unless the failure condition introduced in Hyb_5 is satisfied, every invocation of the function R is with respect to a fresh input, and thus, the output can be replaced with a fresh randomness.
Thus, it suffices to show the pseudorandomness of the following distribution given $f_1,\ldots,f_Q,\mathbf{r}_1,\ldots,\mathbf{r}_Q,\mathbf{A}_{\mathsf{att}}$.

$$\left(\mathbf{B},\{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]},\ \mathbf{c}^\mathsf{T}\leftarrow\mathbb{Z}_q^{1\times m\log q},\{\tilde{\mathrm{F}}_i = f_i(\mathbf{x})\,\lfloor q/2\rceil + R_i + \mathbf{e}^\mathsf{T}_{\mathbf{P},i}\}_{i\in[Q]},\right.$$
$$\left.\mathbf{X}\leftarrow\mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))},\mathbf{c}^\mathsf{T}_{\mathsf{att}}\leftarrow\mathbb{Z}_q^{1\times(\mathrm{L}_\mathrm{X}+1)m}\right)$$

Hyb_7. This hybrid is same as the previous one except we sample $\tilde{\mathrm{F}}_i \leftarrow \mathbb{Z}_q^\ell$ for $i \in [Q]$. This follows from the pseudorandomness of $\{f_i(\mathbf{x})\}_i$ and the fact that B is exponentially smaller than $q/4$. To see this note that we have

$$(1^\lambda,\{f_i,\ f_i(\mathbf{x})\}_{i\in[Q]}) \approx_c (1^\lambda,\{f_i,\ \Delta_i\leftarrow\{0,1\}^{1\times\ell}\}_{i\in[Q]})$$

which implies

$$(1^\lambda,\{f_i,\ \tilde{\mathrm{F}}_i = f_i(\mathbf{x})\,\lfloor q/2\rceil + R_i + \mathbf{e}^\mathsf{T}_{\mathbf{P},i}\}_{i\in[Q]}) \approx_c (1^\lambda,\ \{f_i,\ \tilde{\mathrm{F}}_i\leftarrow\mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]})$$

Hence, we achieve the following distribution

$$\left(\mathbf{B},\{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]},\ \mathbf{c}^\mathsf{T}\leftarrow\mathbb{Z}_q^{1\times m\log q},\{\tilde{\mathrm{F}}_i\leftarrow\mathbb{Z}_q^{1\times\ell}\}_{i\in[Q]},\mathbf{X}\leftarrow\mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))},\right.$$
$$\left.\mathbf{c}^\mathsf{T}_{\mathsf{att}}\leftarrow\mathbb{Z}_q^{1\times(\mathrm{L}_\mathrm{X}+1)m},f_1,\ldots,f_Q,\mathbf{r}_1,\ldots,\mathbf{r}_Q,\mathbf{A}_{\mathsf{att}}\right)$$

which is the R.H.S distribution of Equation (25), hence the proof.

Proof of $D^{\mathsf{pre}}_{\mathsf{inter}} \approx D^{\mathsf{pre}}_1$

We prove $D^{\mathsf{pre}}_{\mathsf{inter}} \approx D^{\mathsf{pre}}_1$ via the following sequence of hybrids.

Hyb_0. This is L.H.S distribution i.e. $D^{\mathsf{pre}}_{\mathsf{inter}}$.

Hyb_1. This hybrid is same as Hyb_0 except that we compute $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x},\mathsf{sd})\otimes\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times(m(\lambda+\mathrm{L}+1))}$, where $\mathbf{A}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$. We have $\mathsf{Hyb}_0 \approx_s \mathsf{Hyb}_1$ using leftover hash lemma. We can argue that the uniform distribution $\mathbb{Z}_q^{(n+1)\times(m(\lambda+L+1))}$ is statistically close to $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}$ using the same argument as used to prove $\mathsf{Hyb}_2 \approx \mathsf{Hyb}_3$ in proof of $D^{\mathsf{pre}}_0 \approx D^{\mathsf{pre}}_{\mathsf{inter}}$. Hence, we skip the indistinguishability argument.

Hyb_2. This hybrid is same as Hyb_1 except that we compute $\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \hat{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{b}_{\mathsf{fhe}}^\intercal = \bar{\mathbf{s}}^\intercal \mathbf{A}_{\mathsf{LWE}} + \mathbf{e}_{\mathsf{fhe}}^\intercal \end{pmatrix}$ and $\mathbf{c}_{\mathsf{att}}^\intercal = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal$. To prove this, we show that if there exists an adversary $\mathcal{A}$ who can distinguish between the two hybrids with non-negligible advantage, then there is a reduction $\mathcal{B}$ that breaks LWE security with non-negligible advantage. The reduction is as follows.

1. On receiving security parameter from $\mathcal{A}$, forward it to LWE challenger.
2. The LWE challenger samples $\beta \leftarrow \{0,1\}$. It also samples $\mathbf{A}_{\mathsf{LWE}} \leftarrow \mathbb{Z}_q^{n\times(m+(\mathrm{L_X}+1)m)}$, $\bar{\mathbf{s}} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_{\mathsf{s}}}^n$ and sets $\mathbf{b}^\intercal = \bar{\mathbf{s}}^\intercal \mathbf{A}_{\mathsf{LWE}} + \mathbf{e}_{\mathsf{fhe}}^\intercal \in \mathbb{Z}_q^{1\times(m+(\mathrm{L_X}+1)m)}$ if $\beta = 1$, else it samples $\mathbf{b}^\intercal \leftarrow \mathbb{Z}_q^{1\times(m+(\mathrm{L_X}+1)m)}$ if $\beta = 0$. Sends $(\mathbf{A}_{\mathsf{LWE}}, \mathbf{b})$ to $\mathcal{B}$.
3. $\mathcal{B}$ parses $\mathbf{A}_{\mathsf{LWE}} = (\hat{\mathbf{A}}_{\mathsf{fhe}},\ \mathbf{A}'_{\mathsf{att}})$, where $\hat{\mathbf{A}}_{\mathsf{fhe}} \in \mathbb{Z}_q^{n\times m}, \mathbf{A}'_{\mathsf{att}} \in \mathbb{Z}_q^{n\times(\mathrm{L_X}+1)m}$ and $\mathbf{b}^\intercal = (\mathbf{b}_{\mathsf{fhe}}^\intercal,\ \mathbf{b}_{\mathsf{att}}^\intercal)$.
4. Choose $\{f_i \in \mathcal{F}_{\mathsf{prm}}\}_{i\in[Q]}$ and an input vector $\mathbf{x} \in \{0,1\}^L$.
5. Samples $\{\mathbf{r}_i \leftarrow \{0,1\}^\lambda\}_{i\in[Q]}$, $\widetilde{\mathsf{sd}} \leftarrow \{0,1\}^\lambda$ and set $\mathsf{sd} = (1, \widetilde{\mathsf{sd}})$.
6. Sets $\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \hat{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{b}_{\mathsf{fhe}}^\intercal \end{pmatrix}$ and computes $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G}$ as in the construction.
7. Sets $\bar{\mathbf{A}}_{\mathsf{att}} = \mathbf{A}'_{\mathsf{att}} + (1, \mathsf{bits}(\mathbf{X})) \otimes \bar{\mathbf{G}}$, $\mathbf{A}_{\mathsf{att}} = \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{att}} \\ \mathbf{a}_{\mathsf{att}}^\intercal \end{pmatrix}$, where $\mathbf{a}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L_X}+1)m}$, and $\mathbf{c}_{\mathsf{att}}^\intercal = \mathbf{b}_{\mathsf{att}}^\intercal - (\mathbf{a}_{\mathsf{att}}^\intercal - (1, \mathsf{bits}(\mathbf{X})) \otimes \underline{\mathbf{G}})$, where $\bar{\mathbf{G}}$ and $\underline{\mathbf{G}}$ denotes the first n rows and $n+1$-th row of the gadget matrix $\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m}$, respectively.
8. Sample $\mathbf{B} \leftarrow \mathbb{Z}_q^{(n+1)\times m\log q}$, $\mathbf{c}^\intercal \leftarrow \mathbb{Z}_q^{1\times m\log q}$, $(\mathbf{c}')^\intercal \leftarrow \mathbb{Z}_q^{1\times \ell Q}$.
9. Compute $\{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}$ as in hybrid 1.
10. Sends $(\mathbf{B}, \{\mathbf{A}_{\mathrm{F}_i}\}_{i\in[Q]}, \mathbf{c}^\intercal, (\mathbf{c}')^\intercal, \mathbf{X}, \mathbf{c}_{\mathsf{att}}^\intercal, f_1, \ldots, f_Q, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}})$ to $\mathcal{A}$.
11. $\mathcal{A}$ outputs a bit β'. $\mathcal{B}$ forwards the bit β' to the LWE challenger.

It is easy to see that if LWE challenger sent random $\mathbf{b} \leftarrow \mathbb{Z}_q^{m+(\mathrm{L_X}+1)m}$ then $\mathcal{B}$ simulated Hyb_1 with $\mathcal{A}$, else if LWE challenger sent $\mathbf{b}^\intercal = \bar{\mathbf{s}}^\intercal \mathbf{A}_{\mathsf{LWE}} + \mathbf{e}_{\mathsf{LWE}}^\intercal$, then $\mathcal{B}$ simulated Hyb_2 with $\mathcal{A}$.

Hence, $D_{\mathsf{inter}}^{\mathsf{pre}} \approx D_1^{\mathsf{pre}}$. Hence, the proof.

□

□

5.2 Counter-Example for BDJMMPV Assumption

Assumption 5.5 (Evasive LWE [BDJ+24]). We recall the version of evasive LWE assumption considered in BDJMMPV, which is adapted from [MPV24b] and [BUW24]. Let $m, n, k, \kappa > 0$ be integers and let q be a modulus. Let $\tau, \sigma, \sigma' > 0$. Let Samp be an algorithm which takes 1^λ and a matrix $\mathbf{P} \in \mathbb{Z}_q^{k\times n}$ and outputs a matrix $\mathbf{S} \in \mathbb{Z}_q^{n\times\kappa}$ and auxiliary information aux. Let

$$\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}, \quad \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}, \quad \mathbf{P} = \mathbf{D}\cdot\mathbf{B}, \quad (\mathbf{S}, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{P}),$$
$$\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa}, \quad \mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma'}^{k\times\kappa}, \quad \mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}, \quad \mathbf{C}' \leftarrow \mathbb{Z}_q^{k\times\kappa}$$

For PPT distinguishes, $\mathcal{A}^{\mathsf{pre}}$ and $\mathcal{A}^{\mathsf{post}}$ define the following functions:

$$\mathsf{Adv}_{\mathcal{A}_0}^{\mathsf{pre}}(\lambda) = |\Pr[\mathcal{A}_0(\mathbf{B}, \mathbf{P}, \mathbf{BS}+\mathbf{E}, \mathbf{PS}+\mathbf{E}', \mathsf{aux}) = 1] - \Pr[\mathcal{A}_0(\mathbf{B}, \mathbf{P}, \mathbf{C}, \mathbf{C}', \mathsf{aux}) = 1]|$$
$$\mathsf{Adv}_{\mathcal{A}_1}^{\mathsf{post}}(\lambda) = |\Pr[\mathcal{A}_1(\mathbf{B}, \mathbf{P}, \mathbf{BS}+\mathbf{E}, \mathbf{D}, \mathsf{aux}) = 1] - \Pr[\mathcal{A}_1(\mathbf{B}, \mathbf{P}, \mathbf{C}, \mathbf{D}, \mathsf{aux}) = 1]|$$

We say that the evasive LWE assumption $\mathsf{evLWE}(q, m, n, k, \kappa, \mathsf{Samp}, \tau, \sigma, \sigma')$ holds, if for every PPT distinguisher $\mathcal{A}_1$, there exists a PPT distinguisher $\mathcal{A}_0$ and polynomial $Q(\lambda)$ such that

$$\mathsf{Adv}^{\mathsf{pre}}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{\mathsf{post}}_{\mathcal{A}_1}(\lambda)/Q(\lambda) - \mathsf{negl}(\lambda)$$

and $\mathrm{time}(\mathcal{A}_0) \leq \mathrm{time}(\mathcal{A}_1) \cdot Q(\lambda)$.

Remark 5.6. In this section, we stick to the notation used in [BDJ+24], where $\mathbf{B}$ is of size $m \times n$ and thus "tall" matrix, whereas $\mathbf{B}$ is a "wide" matrix of size $n \times m$ in other sections.

Remark 5.7. We remark that this version of evasive LWE is different from that in [AKY24a] (considered in Section 5.1). In this version the matrix $\mathbf{P}$ is a random matrix and cannot be controlled by the sampler as it is provided to the sampler as an input. However, aux may contain contrived terms which are also related to $\mathbf{P}$ and thus can still leak some information making it vulnerable to attacks. Indeed, we exploit such a term in aux in our counterexample.

Theorem 5.8. There exists an efficient ELWE sampler Samp as defined in Assumption 5.5 such that the pre-condition holds, but the post-condition does not- i.e., there exists a distinguisher $\mathcal{A}^{\mathsf{post}}$ that distinguishes the post-condition with non-negligible probability.

The sampler used for proving the theorem is almost the same as the one used in the construction of exponentially efficient doubly pseudorandom obfuscation scheme (xdPRO) as in Section 4 of [BDJ+24], except that it uses a contrived implementation of the PRF and f (as defined below) circuit and set q to be an odd number rather than power of two.

Proof. Our sampler uses a PRF with a contrived circuit implementation, as described below.

PRF Circuit Description. Let $\mathsf{PRF} : \{\{1\} \times \{0,1\}^{\lambda}\} \times \{0,1\}^{\log(\kappa)} \to [-q/4 + \hat{B}, q/4 - \hat{B}]^k$ where $\hat{B}$ is chosen to be exponentially smaller than $q/4$. Let C_{PRF_i}, with hardwired i, outputting $\mathsf{PRF}(K', i)$ (in binary) on input $K' = (1, K'')$, be any circuit implementing PRF. We construct a modified circuit C'_{PRF_i} implementing PRF as follows.

1. Let C_0 be a circuit that outputs the first bit of its input $\mathbf{x}$. Further, assume that the first bit of $\mathbf{x}$ is always 1.
2. To the output wire of C_{PRF_i} corresponding to the lowest-order bit of $\mathsf{PRF}(K', i)[j]$ for all $j \in [k]$, attach a new gate which performs the correlation-inducing transformation described in Corollary 4.5, using the output wire of C_0 as the special "1" input. Inputs to C_0 can be the bits of K'.
3. To all the other output wires of C_{PRF_i}, attach a gate performing "even randomness" transformation as in Lemma 4.3.

Defining Evasive LWE Sampler. Let $n, m, k, \kappa, \eta \in \mathbb{N}$ be parameters, q be an odd number, and λ be the security parameter. They will be set after the description of the sampler below. The private coin sampler Samp with private coins $\mathsf{coins}^{\mathsf{Samp}}_{\mathsf{priv}} = (K'', \mathbf{R}, \overline{\mathbf{E}}, \mathbf{S}, \bar{\mathbf{s}}, \{\mathbf{R}_{\mathsf{fhe},\ell}\}_{\ell \in [\eta+1+\lambda]}, \overline{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{e}_{\mathsf{fhe}})$ of the Evasive LWE assumption as in Assumption 5.5 is defined as follows. The sampler Samp on input $(1^{\lambda}, \mathbf{P})$, where $\mathbf{P} \in \mathbb{Z}_q^{k \times n}$ does the following:

1. Let $\{\mathcal{F}_{\mathsf{prm}} = \{f : \{0,1\}^{\eta} \times \{0,1\}^{\log(\kappa)} \to \{0,1\}^k\}\}_{\mathsf{prm}}$ be a family of functions, where $f \in \mathcal{F}_{\mathsf{prm}}$ can be computed by a circuit of depth $d(\lambda) = \mathrm{poly}(\lambda)$ and $\mathsf{prm} = (1^{\eta(\lambda)}, 1^{k(\lambda)}, 1^{\kappa(\lambda)}, 1^{d(\lambda)})$. Let $\mathsf{KeySamp}$ be a sampling algorithm that, on input 1^{λ}, outputs key $K \in \{0,1\}^{\eta}$ and auxiliary information aux_K dependent on K. Choose $f \in \mathcal{F}_{\mathsf{prm}}$ so that

$$(\{f(K, i)\}_{i \in [\kappa]}, \mathsf{aux}_K) \approx_c (\{\mathbf{u}_i : \mathbf{u}_i \leftarrow \{0,1\}^k\}_{i \in [\kappa]}, \mathsf{aux}_K),$$

over the random choice of $(K, \mathsf{aux}_K) \leftarrow \mathsf{KeySamp}(1^\lambda)$. A concrete example of such $\mathsf{KeySamp}$ is an algorithm that chooses random PRF key K and sets $\mathsf{aux}_K = \perp$. The function $f(K,i)$ is defined to be a PRF value with respect to the key K and input i.

For all $i \in [\kappa]$, let C_{f_i}, with hardwired i, outputting scaled version of $f_i(K) = f(K,i)$, i.e. outputting $\lfloor q/2 \rceil f_i(K)$ (in binary) on input K, be any circuit implementing f_i. We construct a modified circuit C'_{f_i} implementing f_i as follows. To all the output wires of C_{f_i}, attach a gate performing "even randomness" transformation as in Lemma 4.3. We can observe that C'_{f_i} is of depth at most $d+3$.

2. Sample $K'' \leftarrow \{0,1\}^\lambda$ and set $K' = (1, K'')$ and $\overline{K} = (K, K')$.

3. Then it defines a function F_i with i hardwired as follows: On input $\overline{K}$, compute and output $f(K,i)\lfloor q/2 \rceil + \mathsf{PRF}(K', i) \in \mathbb{Z}_q^k$. Let C'_{F_i} be a circuit that implements F_i and uses circuits C'_{f_i} and C'_{PRF_i} to compute the respective components and adds their outputs to get the final output of C'_{F_i}.

4. Sample $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{s}}}$ and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.

5. Sample $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{R}_{\mathsf{fhe},\ell} \leftarrow \{0,1\}^{m\times m}$ for all $\ell \in [\eta+\lambda+1]$ and compute a GSW encryption as follows.

$$\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \end{pmatrix}, \qquad \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (\overline{K}) \otimes \mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m(\lambda+\eta+1)}$$

where $\mathbf{R}_{\mathsf{fhe}} = (\mathbf{R}_{\mathsf{fhe},1}, \ldots, \mathbf{R}_{\mathsf{fhe},(\lambda+\eta+1)})$.

6. Parse $\mathbf{s}^\intercal = (s_1, \ldots, s_n, -1) \in \mathbb{Z}_q^{1\times n+1}$, sample $\mathbf{R} \leftarrow \mathbb{Z}_q^{n\times(k+1)m}$ and $\overline{\mathbf{E}} \leftarrow \mathcal{D}^{k\times(k+1)m}_{\mathbb{Z},\rho}$ and compute $\mathbf{A} = \mathbf{P}\mathbf{R} + \overline{\mathbf{E}} + (\mathbf{I}_k, \mathbf{0}) \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal \in \mathbb{Z}_q^{k\times(k+1)m}$ where $\mathbf{0} \in \mathbb{Z}_q^k$ is all zero column vector and $\mathbf{I}_k$ is the identity matrix with k rows and columns.

7. For $i \in [\kappa]$

   - Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathrm{MakeVEvalCkt}(n, m, q, C'_{\mathrm{F}_i})$.
   - Compute $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathbf{X})$. Thus, $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C'_{\mathrm{F}_i}} - \begin{pmatrix} 0^{n\times k} \\ C'_{\mathrm{F}_i}(\overline{K}) \end{pmatrix} \in \mathbb{Z}_q^{n+1\times k}$, where $\mathbf{R}_{C'_{\mathrm{F}_i}}$ is the randomness after homomorphic evaluation.
   - Let $\mathbf{f}_i \in \mathbb{Z}_q^{k(n+1)}$ be the vectorization of $\mathbf{X}_{C'_{\mathrm{F}_i}}$ such that $(\mathbf{I}_k \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal)\mathbf{G}^{-1}(\mathbf{f}_i) \approx C'_{\mathrm{F}_i}(\overline{K})$. That is,

     $$\mathbf{f}_i = \left(\mathbf{X}_{C'_{\mathrm{F}_i}}[1,1], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,1], \mathbf{X}_{C'_{\mathrm{F}_i}}[1,2], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,2], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[1,k], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,k]\right)^\intercal.$$

   - Sample $\mathbf{r}_i \leftarrow \{0,1\}^m$.

8. Set $\mathbf{F} = (\mathbf{G}^{-1}_{\mathbf{r}_1}(\mathbf{f}_1), \ldots, \mathbf{G}^{-1}_{\mathbf{r}_\kappa}(\mathbf{f}_\kappa)) \in \{0,1\}^{(k+1)m\times\kappa}$. Here $\mathbf{G}^{-1}_{\mathbf{r}_i}(\mathbf{f}_i) = \begin{pmatrix} \tilde{\mathbf{f}}_i \\ \mathbf{r}_i \end{pmatrix}$ where $\tilde{\mathbf{f}}_i \in \mathbb{Z}_q^{k(n+1)\log q}$ is the unique vector with $(\mathbf{I}_k \otimes \mathbf{G})\tilde{\mathbf{f}}_i = \mathbf{f}_i$.

9. Sample $\mathbf{S} \leftarrow \mathbb{Z}_q^{n\times\kappa}$ and set $\mathbf{H} = \mathbf{S} + \mathbf{R}\mathbf{F}$.

10. Output $(\mathbf{S}, \mathsf{aux})$ where $\mathsf{aux} = (\mathbf{H}, \mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$.

Counter-example Roadmap. Now, for our counter-example, we need to show that for $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}, \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}, \mathbf{P} = \mathbf{D}\cdot\mathbf{B}, (\mathbf{S}, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{P})$ where $\mathsf{aux} = (\mathbf{H}, \mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$,

1. (Precondition) For all PPT adversary $\mathcal{A}^{\mathsf{pre}}$, the following two distributions, D_0^{pre} and D_1^{pre} are indistinguishable.

   $$D_0^{\mathsf{pre}} := (\mathbf{B}, \mathbf{P}, \mathbf{C} = \mathbf{BS} + \mathbf{E}, \mathbf{C}' = \mathbf{PS} + \mathbf{E}', \mathsf{aux}) \approx D_1^{\mathsf{pre}} := (\mathbf{B}, \mathbf{P}, \mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}, \mathbf{C}' \leftarrow \mathbb{Z}_q^{k\times\kappa}, \mathsf{aux}),$$

   where $\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa}, \mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma'}^{k\times\kappa}$. We prove this in claim 5.12.

2. (Attack against postcondition) There exists an adversary who distinguishes the following distributions, D_0^{post} and D_1^{post} with non-negligible probability.

   $$D_0^{\mathsf{post}} := (\mathbf{B}, \mathbf{P}, \mathbf{C} = \mathbf{BS} + \mathbf{E}, \mathbf{D}, \mathsf{aux}) \text{ and } D_1^{\mathsf{post}} := (\mathbf{B}, \mathbf{P}, \mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}, \mathbf{D}, \mathsf{aux}),$$

   where $\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa}$.
   We begin with Step 2. To prove this step, we introduce one extra distribution D_2^{post} as

   $$D_2^{\mathsf{post}} := (\mathbf{B}, \mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}, \mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}, \mathbf{D}, \mathsf{aux} = (\mathbf{H}, \mathsf{aux}'))$$

   where $(\mathbf{B}, \mathbf{B}_\tau^{-1}) \leftarrow \mathsf{TrapGen}(1^m, 1^n, q), \mathbf{D} \leftarrow \mathbf{B}_\tau^{-1}(\mathbf{P})$,[19] $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$ and $\mathsf{aux}' = (\mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$, and then prove that,

   (a) for all PPT adversary, the two distributions, D_1^{post} and D_2^{post} are statistically indistinguishable. We prove this in Claim 5.9.

   (b) there exists an adversary $\mathcal{A}^{\mathsf{post}}$ who distinguishes the distributions, D_0^{post} and D_2^{post} with non-negligible probability. We prove this in Claim 5.10.

   This implies the adversary $\mathcal{A}^{\mathsf{post}}$ distinguishes D_0^{post} and D_1^{post} with non-negligible probability.

Parameter Setting. We set our parameters the same as [BDJ+24], except that we explicitly define $\tilde{\beta}, \tilde{B}$ and explicitly set κ and k.

$$\begin{aligned}
&\tilde{\beta} = 2^{O(d\cdot\log^3\lambda)}, \quad \tilde{B} = \lambda\sigma_{\mathsf{fhe}}\tilde{\beta}m, \quad \hat{B} = \tilde{B} + \lambda m\tau\sigma + \lambda m(k+1)\rho,\\
&\sigma = \sigma' = 2^\lambda(\tilde{B} + \lambda(k+1)m\rho), \quad q \in (2^\lambda\kappa k\hat{B}, 2^{\lambda+1}\kappa k\hat{B}], \quad n = \mathrm{poly}(\lambda),\\
&m = (n+1)\lceil\log_2 q\rceil, \quad k = m^2, \quad \kappa = m^4
\end{aligned}$$

Proving $D_1^{\mathsf{post}} \approx_s D_2^{\mathsf{post}}$. We show below that $D_1^{\mathsf{post}} \approx_s D_2^{\mathsf{post}}$ holds with respect to the above sampler defined in Section 5.2.

Claim 5.9. For $(\mathbf{S}, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{P})$ where $\mathsf{aux} = (\mathbf{H}, \mathsf{aux}')$, $\mathsf{aux}' = (\mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$,

$$\begin{aligned}
D_1^{\mathsf{post}} := (\mathbf{B}, \mathbf{P}, \mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}, \mathbf{D}, \mathbf{H} = \mathbf{S} + \mathbf{RF}, \mathsf{aux}')\\
\approx_s D_2^{\mathsf{post}} := (\mathbf{B}, \mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}, \mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}, \mathbf{D}, \mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}, \mathsf{aux}'),
\end{aligned}$$

where in D_1^{post}, $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}, \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}, \mathbf{P} = \mathbf{D}\cdot\mathbf{B}$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{n\times(k+1)m}$ and in D_2^{post}, $(\mathbf{B}, \mathbf{B}_\tau^{-1}) \leftarrow \mathsf{TrapGen}(1^m, 1^n, q), \mathbf{D} \leftarrow \mathbf{B}_\tau^{-1}(\mathbf{P})$.

[19] Here, we overload the notation and $\mathbf{B}_\tau^{-1}(\mathbf{P})$ denotes a distribution over short $\mathbf{D}$ such that $\mathbf{DB} = \mathbf{P}$, rather than $\mathbf{BD} = \mathbf{P}$. This change is introduced due to our choice of the size of $\mathbf{B}$ in this section, where we choose $\mathbf{B}$ to be a tall matrix rather than the wide matrix.

Proof. We prove Claim 5.9 using a series of hybrids $\mathsf{Hyb}_0, \ldots, \mathsf{Hyb}_3$ and proving that $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1 \approx \ldots \approx \mathsf{Hyb}_3$, where Hyb_0 is the D_1^{post} distribution and Hyb_3 is the D_2^{post} distribution.

Hyb_1**:** This is identical to Hyb_0 except that we sample matrix $\mathbf{H}$ as $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$. In Hyb_0, $\mathbf{H}$ is computed by $\mathbf{H} = \mathbf{S} + \mathbf{RF}$ for a uniformly random $\mathbf{S} \leftarrow \mathbb{Z}_q^{n\times\kappa}$ that is not used anywhere else. Therefore, Hyb_0 and Hyb_1 are identically distributed.

Hyb_2**:** This is identical to Hyb_1 except that instead of uniformly sampling $\mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}$, we compute it as $(\mathbf{B}, \mathbf{B}_\tau^{-1}) \leftarrow \mathsf{TrapGen}(1^m, 1^n, q)$. Therefore, the statistical indistinguishability between Hyb_1 and Hyb_2 follows from Lemma 3.4.

Hyb_3**:** This is identical to Hyb_2 except that instead of first sampling $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}$ and setting $\mathbf{P} = \mathbf{D}\cdot\mathbf{B}$, we uniformly sample $\mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}$ and set $\mathbf{D} \leftarrow \mathbf{B}_\tau^{-1}(\mathbf{P})$. Therefore, the statistical indistinguishability between Hyb_2 and Hyb_3 follows from the trapdoor sampling property (Section 3.5). Note that this distribution is the same as D_2^{post}.

□

Distinguishing Algorithm/Attack Strategy for D_0^{post} and D_2^{post}. The adversary $\mathcal{A}^{\mathsf{post}}$ holds the distribution D_0^{post} if $\beta = 0$ and D_2^{post} if $\beta = 1$ for $\beta \leftarrow \{0,1\}$. Thus, for $\beta = 0$, $\mathbf{P} = \mathbf{DB}$, $\mathbf{C} = \mathbf{BS} + \mathbf{E}$, $\mathbf{H} = \mathbf{S} + \mathbf{RF}$ and for $\beta = 1$, $\mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}$, $\mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}$, $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$. It does the following:

1. For $i \in [\kappa]$
   - Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathrm{MakeVEvalCkt}(n, m, q, C'_{\mathrm{F}_i})$.
   - Compute $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathbf{X}) = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C'_{\mathrm{F}_i}} - \begin{pmatrix} 0^{n\times k} \\ C'_{\mathrm{F}_i}(\overline{K}) \end{pmatrix} \in \mathbb{Z}_q^{n+1\times k}$.
   - Compute $\mathbf{f}_i \in \mathbb{Z}_q^{k(n+1)}$ as the vectorization of $\mathbf{X}_{C'_{\mathrm{F}_i}}$ i.e.

   $$\mathbf{f}_i = \left(\mathbf{X}_{C'_{\mathrm{F}_i}}[1,1], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,1], \mathbf{X}_{C'_{\mathrm{F}_i}}[1,2], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,2], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[1,k], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,k]\right)^{\mathsf{T}}$$

2. Compute $\mathbf{F} = (\mathbf{G}_{\mathbf{r}_1}^{-1}(\mathbf{f}_1), \ldots, \mathbf{G}_{\mathbf{r}_\kappa}^{-1}(\mathbf{f}_\kappa))$ where $\{\mathbf{r}_i\}_{i\in[\kappa]} \in \mathsf{aux}$.
3. Compute $\mathbf{Y} = \mathbf{AF} + \mathbf{DC} - \mathbf{PH} \in \mathbb{Z}_q^{k\times\kappa}$ and parse $\mathbf{Y} = (\mathbf{y}_1, \ldots, \mathbf{y}_\kappa)$ column-wise.
4. For $i \in [\kappa]$, compute $\mathbf{z}_i = \mathbf{y}_i - \lfloor q/2 \rceil\, \mathsf{MSB}(\mathbf{y}_i)$[20].
5. $\mathcal{A}^{\mathsf{post}}$ defines the following set of linear equations (Equation (26)) in variables, all elements of $\overline{\mathbf{E}}, \mathbf{E}$ and outputs $\beta' = 0$ if (26) is solvable; otherwise, output $\beta' = 1$.

$$\left\{\begin{array}{l} \overline{\mathbf{E}}[j,1]\mathbf{F}[1,i] + \ldots + \overline{\mathbf{E}}[j,(k+1)m]\mathbf{F}[(k+1)m,i] + \\ \mathbf{D}[j,1]\mathbf{E}[1,i] + \ldots + \mathbf{D}[j,m]\mathbf{E}[m,i] = \mathbf{z}_i[j] \bmod 2 \end{array}\right\}_{i\in[\kappa], j\in[k]} \tag{26}$$

Analyzing success probability of $\mathcal{A}^{\mathsf{post}}$.

Claim 5.10. $\mathcal{A}^{\mathsf{post}}$ wins (i,e., $\beta = \beta'$) with probability $3/4 - \mathsf{negl}(\lambda)$ when $k(k+1)m + m\kappa \ll k\kappa$.

[20] Observe that $\mathsf{MSB}(\mathbf{y}_i) = f(K,i)$ when $\beta = 0$

Proof. Let us first analyze the solvability of equations defined in Equation (26) for the two cases: $\beta = 0$ and $\beta = 1$.

The Case of $\beta = 0$. When $\beta = 0$, for all $i \in [\kappa]$, it holds that

$$
\begin{aligned}
& ((\mathbf{I}_k, \mathbf{0}) \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal)\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) \\
= & \begin{pmatrix} (s_1\mathbf{g}^\intercal, \ldots, s_n\mathbf{g}^\intercal, -\mathbf{g}^\intercal) & 0^m & \ldots & 0^m & 0^m \\ 0^m & (s_1\mathbf{g}^\intercal, \ldots, s_n\mathbf{g}^\intercal, -\mathbf{g}^\intercal) & \ldots & 0^m & 0^m \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0^m & 0^m & \vdots & (s_1\mathbf{g}^\intercal, \ldots, s_n\mathbf{g}^\intercal, -\mathbf{g}^\intercal) & 0^m \end{pmatrix}_{k \times (k+1)m} \begin{pmatrix} \tilde{\mathbf{f}}_i \\ \mathbf{r}_i \end{pmatrix}_{(k+1)m \times 1} \\
= & \begin{pmatrix} (s_1\mathbf{g}^\intercal \tilde{\mathbf{f}}_i[1; \log q] + \ldots + s_n\mathbf{g}^\intercal \tilde{\mathbf{f}}_i[(n-1)\log q + 1; n \log q] - \mathbf{g}^\intercal \tilde{\mathbf{f}}_i[n \log q + 1; m]) \\ \vdots \\ (s_1\mathbf{g}^\intercal \tilde{\mathbf{f}}_i[(k-1)m + 1; (k-1)m + 1 + \log q] + \ldots \\ +s_n\mathbf{g}^\intercal \tilde{\mathbf{f}}_i[km - 2\log q + 01; km - \log q] - \mathbf{g}^\intercal \tilde{\mathbf{f}}_i[km - \log q + 1; km]) \end{pmatrix}_{k \times 1} \\
= & \begin{pmatrix} (s_1\mathbf{f}_i[1] + \ldots + s_n\mathbf{f}_i[n] - \mathbf{f}_i[n+1]) \\ \vdots \\ (s_1\mathbf{f}_i[(k-1)(n+1) + 1] + \ldots \\ +s_n\mathbf{f}_i[k(n+1) - 1] - \mathbf{f}_i[k(n+1)]) \end{pmatrix}_{k \times 1} \quad \text{(the equality follows from the property of } \mathbf{G}_{\mathbf{r}_i}^{-1}) \\
= & \begin{pmatrix} \mathbf{s}^\intercal \mathbf{X}_{C'_{\mathrm{F}_i}}[\cdot, 1] \\ \vdots \\ \mathbf{s}^\intercal \mathbf{X}_{C'_{\mathrm{F}_i}}[\cdot, k] \end{pmatrix}_{k \times 1} = \begin{pmatrix} C'_{\mathrm{F}_i}(\overline{K})[1] - \mathbf{e}_{\mathsf{fhe}}^\intercal(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, 1]) \\ \vdots \\ C'_{\mathrm{F}_i}(\overline{K})[k] - \mathbf{e}_{\mathsf{fhe}}^\intercal(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, k]) \end{pmatrix}_{k \times 1} = \mathrm{F}(\overline{K}, i) - \tilde{\mathbf{e}}_i \qquad \text{(by correctness of GSW)}
\end{aligned}
$$

where $\tilde{\mathbf{f}}_i[\ell; \ell']$ is the part of vector $\tilde{\mathbf{f}}_i$ starting from ℓ-th element and ending at ℓ'-th element and $\tilde{\mathbf{e}}_i = \begin{pmatrix} \mathbf{e}_{\mathsf{fhe}}^\intercal(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, 1]) \\ \vdots \\ \mathbf{e}_{\mathsf{fhe}}^\intercal(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, k]) \end{pmatrix}$ is the GSW decryption noise terms. Here, $\mathbf{s}^\intercal \mathbf{X}_{C'_{\mathrm{F}_i}}[\cdot, j]$ denotes the j-th column of $\mathbf{s}^\intercal \mathbf{X}_{C'_{\mathrm{F}_i}}$ with $n+1$ rows. Therefore, for all $i \in [\kappa]$,

$$
\begin{aligned}
\mathbf{A}\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) &= (\mathbf{P}\mathbf{R} + \overline{\mathbf{E}} + ((\mathbf{I}_k, \mathbf{0}) \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal))\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) \\
&= \mathbf{P}\mathbf{R}\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) + \overline{\mathbf{E}}\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) + ((\mathbf{I}_k, \mathbf{0}) \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal)\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) \\
&= \mathbf{P}\mathbf{R}\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) + \overline{\mathbf{E}}\mathbf{G}_{\mathbf{r}_i}^{-1}(\mathbf{f}_i) + \mathrm{F}(\overline{K}, i) - \tilde{\mathbf{e}}_i
\end{aligned}
$$

Hence, it holds that

$$\mathbf{A}\mathbf{F} = \mathbf{P}\mathbf{R}\mathbf{F} + \overline{\mathbf{E}}\mathbf{F} + (\mathrm{F}(\overline{K}, 1), \ldots, \mathrm{F}(\overline{K}, \kappa)) - \tilde{\mathbf{E}}$$

where $\tilde{\mathbf{E}} = (\tilde{\mathbf{e}}_1, \ldots, \tilde{\mathbf{e}}_\kappa)$. Also, $\mathbf{D}\mathbf{C} = \mathbf{D}(\mathbf{B}\mathbf{S} + \mathbf{E}) = \mathbf{D}\mathbf{B}\mathbf{S} + \mathbf{D}\mathbf{E} = \mathbf{P}\mathbf{S} + \mathbf{D}\mathbf{E}$ and $\mathbf{P}\mathbf{H} = \mathbf{P}(\mathbf{S} + \mathbf{R}\mathbf{F}) = \mathbf{P}\mathbf{S} + \mathbf{P}\mathbf{R}\mathbf{F}$. Hence, we have

$$\mathbf{Y} = \mathbf{A}\mathbf{F} + \mathbf{D}\mathbf{C} - \mathbf{P}\mathbf{H} = (\mathrm{F}(\overline{K}, 1), \ldots, \mathrm{F}(\overline{K}, \kappa)) - \tilde{\mathbf{E}} + \overline{\mathbf{E}}\mathbf{F} + \mathbf{D}\mathbf{E} \tag{27}$$

Let $\hat{\mathbf{E}} = -\tilde{\mathbf{E}} + \overline{\mathbf{E}}\mathbf{F} + \mathbf{D}\mathbf{E} = (\hat{\mathbf{e}}_1, \ldots, \hat{\mathbf{e}}_\kappa)$. Note that since $\overline{\mathbf{E}} \leftarrow \mathcal{D}_{\mathbb{Z},\rho}^{k \times (k+1)m}$, for each column $\overline{\mathbf{E}}[\cdot, i]$ of $\overline{\mathbf{E}}$, we have $||\overline{\mathbf{E}}[\cdot, i]|| \leq \sqrt{\lambda}\rho$. Therefore, $||\overline{\mathbf{E}} \cdot \mathbf{f}_i|| \leq \sqrt{\lambda}(k+1)m\rho$. Similarly, since $\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m \times \kappa}$, for each column $\mathbf{E}[\cdot, i]$ of $\mathbf{E}$, $||\mathbf{E}[\cdot, i]|| \leq \sqrt{\lambda}\sigma$ and every row $\mathbf{D}[j, \cdot]$ of $\mathbf{D}$, $||\mathbf{D}[j, \cdot]|| \leq \sqrt{\lambda}\tau$. Therefore, $||\mathbf{D} \cdot \mathbf{E}[\cdot, i]|| \leq \lambda m\tau\sigma$.

Now for the error bound $\tilde{\mathbf{e}}_i$, we have the following. From Lemma 3.15 and parameter setting, we have,

$$\begin{aligned}||\mathbf{R}_{C'_{\mathsf{F}_i}}|| &\leq (m+2)^{d+O(1)} \lceil \log q \rceil \max_{\ell \in [\eta+1+\lambda]} ||\mathbf{R}_\ell^\intercal|| \\ &\leq (m+2)^{d+O(1)} \lceil \log q \rceil \, m \\ &\leq (m+2)^{d+O(1)} \lceil \log q \rceil \leq \tilde{\beta}\end{aligned}$$

Now, from the parameter setting, we have

$$\begin{aligned}||\tilde{\mathbf{e}}_i|| &\leq \max_{j \in [k]} ||\mathbf{e}_{\mathsf{fhe}}^\intercal (\mathbf{R}_{C'_{\mathsf{F}_i}}[\cdot, j])|| \\ &\leq ||\mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathsf{F}_i}}|| \\ &\leq \sqrt{\lambda} \sigma_{\mathsf{fhe}} \tilde{\beta} m \leq \tilde{B}.\end{aligned}$$

Therefore, by setting

$$\hat{B} = \tilde{B} + \lambda m \tau \sigma + \lambda m (k+1)\rho, \text{ we get } ||\hat{\mathbf{e}}_i|| \leq \hat{B}.$$

Now, from Equation (27), we have for $i \in [\kappa]$, $\mathbf{y}_i = \lfloor q/2 \rceil \, f(K,i) + \mathsf{PRF}(K',i) + \hat{\mathbf{e}}_i$. Since, $\mathsf{PRF}(K',i) \in [-q/4 + \hat{B}, q/4 - \hat{B}]^k$, we have $\mathsf{PRF}(K',i) + \hat{\mathbf{e}}_i \in [-q/4, q/4]^k$. Hence, we have the following.

$$\mathsf{MSB}(\mathbf{y}_i) = \mathsf{MSB}(\lfloor q/2 \rceil \, f(K,i) + \mathsf{PRF}(K',i) + \hat{\mathbf{e}}_i) = f(K,i)$$

Now, for $i \in [\kappa]$, $\mathbf{z}_i = \mathbf{y}_i - \lfloor q/2 \rceil \, \mathsf{MSB}(\mathbf{y}_i) = \mathsf{PRF}(K',i) + \hat{\mathbf{e}}_i = \mathsf{PRF}(K',i) - \tilde{\mathbf{E}}[\cdot,i] + \overline{\mathbf{E}}\mathbf{F}[\cdot,i] + \mathbf{DE}[\cdot,i]$. where $\tilde{\mathbf{E}}[\cdot,i], \overline{\mathbf{E}}\mathbf{F}[\cdot,i], \mathbf{DE}[\cdot,i]$ denotes the ith column of $\tilde{\mathbf{E}}, \overline{\mathbf{E}}\mathbf{F}, \mathbf{DE}$ respectively. We prove in Claim 5.11 that $\mathsf{PRF}(K',i)[j] - \tilde{\mathbf{E}}[j,i] = 0 \bmod 2$ for all $i \in [\kappa], j \in [k]$ with probability $1/2 + \mathsf{negl}(\lambda)$. This gives us that with probability $1/2 + \mathsf{negl}(\lambda)$,

$$\forall \, i \in [\kappa], j \in [k], \overline{\mathbf{E}}\mathbf{F}[j,i] + \mathbf{DE}[j,i] = \mathbf{z}_i[j] \bmod 2 \tag{28}$$

We can rewrite Equation (28) as Equation (29) below for all $i \in [\kappa], j \in [k]$.

$$\overline{\mathbf{E}}[j,1]\mathbf{F}[1,i] + \ldots + \overline{\mathbf{E}}[j,(k+1)m]\mathbf{F}[(k+1)m,i] + \mathbf{D}[j,1]\mathbf{E}[1,i] + \ldots + \mathbf{D}[j,m]\mathbf{E}[m,i] = \mathbf{z}_i[j] \bmod 2 \tag{29}$$

Observe that this is the same as the set of equations defined in (26). Hence, in case of $\beta = 0$, (26) is solvable with probability $1/2 + \mathsf{negl}(\lambda)$. This gives us

$$\Pr(\beta' = 0 \mid \beta = 0) = 1/2 + \mathsf{negl}(\lambda). \tag{30}$$

The Case of $\beta = 1$. When $\beta = 1$, for all $i \in [\kappa]$, we have,

$$\mathbf{z}_i = \mathbf{y}_i - \lfloor q/2 \rceil \, \mathsf{MSB}(\mathbf{y}_i) = \mathbf{AF}[\cdot,i] + \mathbf{DC}[\cdot,i] - \mathbf{PH}[\cdot,i] - \lfloor q/2 \rceil \, \mathsf{MSB}(\mathbf{AF}[\cdot,i] + \mathbf{DC}[\cdot,i] - \mathbf{PH}[\cdot,i])$$

where $\mathbf{P} \leftarrow \mathbb{Z}_q^{k \times n}$, $\mathbf{C} \leftarrow \mathbb{Z}_q^{m \times \kappa}$, and $\mathbf{H} \leftarrow \mathbb{Z}_q^{n \times \kappa}$. We argue that Equation (29) is not solvable with overwhelming probability in this case. This is shown by the following sequence of hybrids. We denote the probability that Equation (29) is not solvable in $\mathsf{Hyb}_{\mathsf{xx}}$ by $\Pr[\mathsf{E}_{\mathsf{xx}}]$. Hyb_0 is the same as D_1^{post} and we want to prove $\Pr[\mathsf{E}_0] = 1 - \mathsf{negl}(\lambda)$.

Hyb_1**:** This hybrid is the same as D_2^{post}. As we have shown in Claim 5.9, $D_1^{\mathsf{post}} \approx_s D_2^{\mathsf{post}}$ and thus we have $|\Pr[\mathsf{E}_0] - \Pr[\mathsf{E}_1]| = \mathsf{negl}(\lambda)$.

Hyb_2**:** In this hybrid, we change the definition of $\mathbf{z}_i$ as

$$\mathbf{z}_i = \mathbf{y}_i - 2\mathbf{e}'_i - \lfloor q/2 \rceil \, \mathsf{MSB}(\mathbf{y}_i - 2\mathbf{e}'_i) \bmod q$$

for freshly chosen $\mathbf{e}'_i \leftarrow \mathcal{D}^k_{\mathbb{Z},\sigma'}$. We argue that the distribution of $\{\mathbf{z}_i \bmod 2\}_i$ is statistically close to that of the previous hybrid. To see this, we first observe that for any $y \in \mathbb{Z}_q$ outside of the "boundary" $[-q/4 - B, -q/4 + B] \cup [q/4 - B, q/4 + B]$, we have $\mathsf{MSB}(y) = \mathsf{MSB}(y - 2e')$ for any e' such that $|e'| < B/2$. For such y and e', we have

$$y - \lfloor q/2 \rceil \mathsf{MSB}(y) = y - \lfloor q/2 \rceil \mathsf{MSB}(y - 2e') = y - 2e' - \lfloor q/2 \rceil \mathsf{MSB}(y - 2e') \bmod 2.$$

We then set $B = 2\sigma'\sqrt{\lambda}$. Then, we have $|\mathbf{e}'_i| < B$ with overwhelming probability. Furthermore, each $\mathbf{y}_i$ is distributed uniformly at random over $\mathbb{Z}^k_q$, since $\mathbf{P}$ and $\mathbf{H}$ are independently and uniformly sampled. Therefore, by the union bound, the probability that there exists i such that some of $\mathbf{y}_i$'s entry falls into the boundary is negligible. Hence, we have $\mathbf{y}_i - \lfloor q/2 \rceil \mathsf{MSB}(\mathbf{y}_i) = \mathbf{y}_i - 2\mathbf{e}'_i - \lfloor q/2 \rceil \mathsf{MSB}(\mathbf{y}_i - 2\mathbf{e}'_i) \bmod 2$ with overwhelming probability, as desired. This implies $|\Pr[\mathsf{E}_1] - \Pr[\mathsf{E}_2]| = \mathsf{negl}(\lambda)$.

Hyb_3: In this hybrid, we further change the definition of $\mathbf{z}_i$ as

$$\mathbf{z}_i = \mathbf{y}'_i - \lfloor q/2 \rceil \mathsf{MSB}(\mathbf{y}'_i)$$

for $\mathbf{y}'_i \leftarrow \mathbb{Z}^k_q$. We argue that under the LWE assumption, we have $|\Pr[\mathsf{E}_2] - \Pr[\mathsf{E}_3]| = \mathsf{negl}(\lambda)$.

To show this, we consider the following reduction. The reduction algorithm is given an LWE challenge $(\mathbf{P}, \mathbf{U})$, where $\mathbf{U} = \mathbf{PH} + 2\mathbf{E}'$ if $\beta = 0$ and $\mathbf{U} \leftarrow \mathbb{Z}^{k\times\kappa}_q$. Then, the reduction algorithm chooses $(\mathbf{B}, \mathbf{B}^{-1}_\tau) \leftarrow \mathsf{TrapGen}(1^m, 1^n, q)$, $\mathbf{D} \leftarrow \mathbf{B}^{-1}_\tau(\mathbf{P})$, and $\mathsf{aux}' = (\mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$ by itself. Then, it defines

$$\mathbf{y}'_i = \mathbf{AF}[\cdot, i] + \mathbf{DC}[\cdot, i] - \mathbf{U}[\cdot, i] - \lfloor q/2 \rceil \mathsf{MSB}(\mathbf{AF}[\cdot, i] + \mathbf{DC}[\cdot, i] - \mathbf{U}[\cdot, i])$$

and $\mathbf{z}_i$ based on the value. The it outputs 0 if Equation (29) is solvable and 1 otherwise.

We can see that the advantage of the adversary above is $|\Pr[\mathsf{E}_2] - \Pr[\mathsf{E}_3]|$. Therefore, unless the LWE assumption is broken, we have that $|\Pr[\mathsf{E}_2] - \Pr[\mathsf{E}_3]| \le \mathsf{negl}(\lambda)$.

Hyb_4: In this hybrid, $\mathbf{z}_i$ is uniformly random in $[-q/4, q/4]^k$ for all $i \in [\kappa]$. It is easy to see that this game is statistically close to the previous hybrid, since $\mathbf{y}'_i$ is uniformly random.

We finally observe that $\{\mathbf{z}_i \bmod 2\}_i$ is statistically close to uniform distribution over $\{0,1\}^{k\times\kappa}$.

Therefore, Equation (26), consisting of $k(k+1)m + m\kappa$ variables, is unsolvable with overwhelming probability if $k(k+1)m + m\kappa \ll k\kappa$ in Hyb_4. Note that for our setting of parameters, this relation is indeed satisfied. Therefore, we have $\Pr[\mathsf{E}_0] = 1 - \mathsf{negl}(\lambda)$ from the above discussion.

This gives us

$$\Pr(\beta' = 1 \mid \beta = 1) = 1 - \mathsf{negl}(\lambda). \tag{31}$$

Thus, from Equation (30) and (31), we get $\Pr(\beta' = \beta) \approx 3/4$. □

Claim 5.11. $\forall i \in [\kappa], j \in [k]$, $\mathsf{PRF}(K', i)[j] - \tilde{\mathbf{E}}[j, i] = 0 \bmod 2$ with probability $1/2 + \mathsf{negl}(\lambda)$.

Proof. The proof is similar to that of Claim 5.3. Let us start by analyzing the error $\tilde{\mathbf{E}}[j, i]$. Note that $\forall\, i \in [\kappa], j \in [k]$, $\tilde{\mathbf{E}}[j, i] = \mathbf{e}^\mathsf{T}_{\mathsf{fhe}}(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, j])$ where $\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, j]$ is the randomness in the homomorphically evaluated encryption of $\mathrm{F}(\overline{K}, i)[j]$ (of different form: $\mathbf{A}_{\mathsf{fhe}}(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, j]) - \begin{pmatrix} 0^{n\times 1} \\ \mathrm{F}(\overline{K}, i)[j] \end{pmatrix}$), output by $\mathsf{VEval}_{C'_{\mathrm{F}_i}}$ circuit. Here, $\mathbf{A}_{\mathsf{fhe}}$ is the FHE public key used to compute $\mathbf{X}$, i.e. the encryption of key $\overline{K}$.

Recall that $\mathrm{F}(\overline{K}, i)[j] = f(K, i)\ \lfloor q/2 \rceil\ [j] + \mathsf{PRF}(K', i)[j]$ and we can write $\tilde{\mathbf{E}}[j, i] = \mathbf{e}^\mathsf{T}_{\mathsf{fhe}}(\mathbf{R}_{C'_{\mathrm{F}_i}}[\cdot, j]) = \mathbf{e}^\mathsf{T}_{\mathsf{fhe}}(\mathbf{R}_{C'_{f_i}}[\cdot, j]) + \mathbf{e}^\mathsf{T}_{\mathsf{fhe}}(\mathbf{R}_{C'_{\mathsf{PRF}_i}}[\cdot, j])$ follows by the way we implemented the homomorphic addition.

Now, $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}(\mathbf{R}_{C'_{f_i}}[\cdot,j]) = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{f_i},j} = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=0}^{\log_2 q-1}\mathbf{R}_{C'_{f_i},j,v}\mathbf{G}^{-1}(2^v\iota_{n+1})$, where $\mathbf{R}_{C'_{f_i},j} = \mathbf{R}_{C'_{f_i}}[\cdot,j]$ is the jth column of $\mathbf{R}_{C'_{f_i}}$ and $\mathbf{R}_{C'_{f_i},j,v}$ is the randomness in homomorphically computed GSW encryption of the v-th bit of $f(K,i)\lfloor q/2\rceil[j]$. Here $v \in [0,\log_2 q)$. Since $f(K,i)\lfloor q/2\rceil$ is implemented by C'_{f_i}, which involves the even randomness transformation (Lemma 4.3) on all its output bits, $\mathbf{R}_{C'_{f_i},j,v}$ has all the entries as even due to Lemma 4.3. This implies $\mathbf{R}_{C'_{f_i},j}$ has even entries, which in turn implies that $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{f_i},j}$ is even.

So, now our goal is to show that

$$\mathsf{PRF}(K',i)[j] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}(\mathbf{R}_{C'_{\mathsf{PRF}_i}}[\cdot,j]) = 0 \bmod 2$$

Similar to above, we have $\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}(\mathbf{R}_{C'_{\mathsf{PRF}_i}}[\cdot,j]) = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_i},j} = \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=0}^{w-1}\mathbf{R}_{C'_{\mathsf{PRF}_i},j,v}\mathbf{G}^{-1}(2^v\iota_{n+1})$.

Again, since in C'_{PRF_i} all the output bits pass through even randomness, except the lowest order bit of the jth entry of the output, for all $j \in [k]$, which passes through the correlation inducing gate, we have

$$\begin{aligned}
& \mathsf{PRF}(K',i)[j] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}(\mathbf{R}_{C'_{\mathsf{PRF}_i}}[\cdot,j]) \bmod 2 \\
= \;& \mathsf{PRF}(K',i)[j] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_i},j,0}\mathbf{G}^{-1}(\iota_{n+1}) - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\sum_{v=1}^{\log_2 q-1}\mathbf{R}_{C'_{\mathsf{PRF}_i},j,v}\mathbf{G}^{-1}(2^v\iota_{n+1}) \bmod 2 \\
= \;& \mathsf{PRF}(K',i)[j] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_i},j,0}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \quad \text{(due to Lemma 4.3)} \\
= \;& \mathsf{PRF}(K',i)[j,0] + \sum_{v=1}^{\log_2 q-2} 2^v\mathsf{PRF}(K',i)[j,v] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_i},j,0}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
= \;& \mathsf{PRF}(K',i)[j,0] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}_{C'_{\mathsf{PRF}_i},j,0}\mathbf{G}^{-1}(\iota_{n+1}) \bmod 2 \\
= \;& \mathsf{PRF}(K',i)[j,0] - \mathsf{PRF}(K',i)[j,0](\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1})) \bmod 2 \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(due to Corollary 4.5)} \\
= \;& 0 \bmod 2, \text{ if } (\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1})) \text{ is odd.}
\end{aligned}$$

In the above, $\mathsf{PRF}(K',i)[j,v] \in \{-1,0,1\}$ represents the v-th (signed) bit in the binary representation of $\mathsf{PRF}(K',i)[j]$ and $\mathbf{R}^*$ is the randomness in the ciphertext of special "1" input used in Corollary 4.5. Note that $(\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}))$ is odd with probability negligibly close to $1/2$ using the same argument as in Claim 5.3. Also, note that the term $(\mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}\mathbf{R}^*\mathbf{G}^{-1}(\iota_{n+1}))$ does not depend on i,j and hence, for all $i \in [\kappa]$, $j \in [k]$, the probability that $\mathsf{PRF}(K',i)[j] - \mathbf{e}_{\mathsf{fhe}}^{\mathsf{T}}(\mathbf{R}_{C'_{\mathsf{PRF}_i}}[\cdot,j]) = 0 \bmod 2$ is $1/2 + \mathsf{negl}(\lambda)$. Hence, the proof. □

Proving the pre-condition. We now show that the pre-condition of Evasive LWE as in Assumption 5.5 holds with respect to the above sampler defined in Section 5.2.

Claim 5.12. For $(\mathbf{S},\mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda,\mathbf{P})$ where $\mathsf{aux} = (\mathbf{H},\mathbf{A}_{\mathsf{fhe}},\mathbf{X},\mathbf{A},\{\mathbf{r}_i\}_{i\in[\kappa]},\mathsf{aux}_K)$,

$$D_0^{\mathsf{pre}} := (\mathbf{B},\mathbf{P},\mathbf{C} = \mathbf{BS}+\mathbf{E},\mathbf{C}' = \mathbf{PS}+\mathbf{E}',\mathsf{aux}) \approx D_1^{\mathsf{pre}} := (\mathbf{B},\mathbf{P},\mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa},\mathbf{C}' \leftarrow \mathbb{Z}_q^{k\times\kappa},\mathsf{aux}) \tag{32}$$

where $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m},\mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n},\mathbf{P} = \mathbf{D}\cdot\mathbf{B},\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa},\mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma'}^{k\times\kappa}$.

Proof. The proof of this claim is similar to the proof of pre-condition of evasive LWE used in the security proof of exponentially efficient doubly pseudorandom obfuscation scheme (xdPRO) as in Section 4 of [BDJ+24]. However, for completeness, we provide the proof here. We prove Claim 5.12 by a series of hybrids Hyb_0 to Hyb_{11} where Hyb_0 is the D_0^{pre} distribution and Hyb_{11} is the D_1^{pre} distribution of (32). We prove that $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1 \approx \ldots \approx \mathsf{Hyb}_{11}$.

Hyb_0**:** This is the D_0^{pre} distribution. We recall the distribution here.

1. Sample $\mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}$, $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}$ and set $\mathbf{P} = \mathbf{D}\cdot\mathbf{B}$.
2. Choose $(K, \mathsf{aux}_K) \leftarrow \mathsf{KeySamp}(1^\lambda)$, sample $K'' \leftarrow \{0,1\}^\lambda$ and set $K' = (1, K'')$ and $\overline{K} = (K, K')$.
3. Samples $\bar{\mathbf{s}} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_{\mathbf{s}}}^n$ and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.
4. Sample $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_{\mathsf{fhe}}}^m$, $\mathbf{R}_{\mathsf{fhe},\ell} \leftarrow \{0,1\}^{m\times m}$ for all $\ell \in [\eta+\lambda+1]$ and compute a GSW encryption as follows.

$$\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^\intercal \end{pmatrix}, \qquad \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (\overline{K}) \otimes \mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m(\lambda+\eta+1)}$$

   where $\mathbf{R}_{\mathsf{fhe}} = (\mathbf{R}_{\mathsf{fhe},1}, \ldots, \mathbf{R}_{\mathsf{fhe},(\lambda+\eta+1)})$.
5. Parse $\mathbf{s}^\intercal = (s_1, \ldots, s_n, -1) \in \mathbb{Z}_q^{1\times(n+1)}$, sample $\mathbf{R} \leftarrow \mathbb{Z}_q^{n\times(k+1)m}$ and $\overline{\mathbf{E}} \leftarrow \mathcal{D}_{\mathbb{Z},\rho}^{k\times(k+1)m}$ and compute $\mathbf{A} = \mathbf{P}\mathbf{R} + \overline{\mathbf{E}} + (\mathbf{I}_k, \mathbf{0}) \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal \in \mathbb{Z}_q^{k\times(k+1)m}$ where $\mathbf{0} \in \mathbb{Z}_q^k$ is all zero column vector and $\mathbf{I}_k$ is the identity matrix with k rows and columns.
6. For $i \in [\kappa]$
   - Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathsf{MakeVEvalCkt}(n, m, q, C'_{\mathrm{F}_i})$.
   - Compute $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathbf{X})$. Hence, $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{C'_{\mathrm{F}_i}} - \begin{pmatrix} 0^{n\times k} \\ C'_{\mathrm{F}_i}(\overline{K}) \end{pmatrix} \in \mathbb{Z}_q^{n+1\times k}$.
   - Let $\mathbf{f}_i \in \mathbb{Z}_q^{k(n+1)}$ be the vectorization of $\mathbf{X}_{C'_{\mathrm{F}_i}}$ i.e.

$$\mathbf{f}_i = \Big(\mathbf{X}_{C'_{\mathrm{F}_i}}[1,1], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,1], \mathbf{X}_{C'_{\mathrm{F}_i}}[1,2], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,2], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[1,k], \ldots, \mathbf{X}_{C'_{\mathrm{F}_i}}[n+1,k]\Big)^\intercal$$

   - Sample $\mathbf{r}_i \leftarrow \{0,1\}^m$.
7. Set $\mathbf{F} = (\mathbf{G}_{\mathbf{r}_1}^{-1}(\mathbf{f}_1), \ldots, \mathbf{G}_{\mathbf{r}_\kappa}^{-1}(\mathbf{f}_\kappa))$.
8. Sample $\mathbf{S} \leftarrow \mathbb{Z}_q^{n\times\kappa}$ and set $\mathbf{H} = \mathbf{S} + \mathbf{R}\mathbf{F}$.
9. Set $\mathsf{aux} = (\mathbf{H}, \mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$.
10. Compute $\mathbf{C} = \mathbf{B}\mathbf{S} + \mathbf{E}$ where $\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa}$.
11. Compute $\mathbf{C}' = \mathbf{P}\mathbf{S} + \mathbf{E}'$ where $\mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma'}^{k\times\kappa}$.
12. Output $(\mathbf{B}, \mathbf{P}, \mathbf{C}, \mathbf{C}', \mathsf{aux})$.

Hyb_1**:** This is same as Hyb_0 except the way we compute $\mathbf{P}$. Instead of sampling $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}$ and setting $\mathbf{P} = \mathbf{D}\cdot\mathbf{B}$, we sample $\mathbf{P}$ uniformly at random i.e. $\mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}$. We now prove that $\mathsf{Hyb}_0 \approx_s \mathsf{Hyb}_1$. We prove that $(\mathbf{B}, \mathbf{D}\mathbf{B}) \approx_s (\mathbf{B}, \mathbf{P})$ where $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}, \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}, \mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}$. This can be seen by observing that, by Lemma 3.6, the min-entropy of each row of $\mathbf{D}$ is at least m. Hence, by the Leftover Hash Lemma (Lemma 3.8), each entry of $\mathbf{D}\mathbf{B}$, is statistically close to being uniformly distributed over $\mathbb{Z}_q$.

Hyb_2**:** This is same as Hyb_1 except the way we compute $\mathbf{H}, \mathbf{C}, \mathbf{C}'$. Instead of choosing $\mathbf{S}$ uniformly at random, sample $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$ and set $\mathbf{S} = \mathbf{H} - \mathbf{R}\mathbf{F}$. Now,

- compute $\mathbf{U} = \mathbf{B}\mathbf{R} + \mathbf{E}^*$ where $\mathbf{E}^* \leftarrow \mathcal{D}_{\mathbb{Z},\rho}^{m\times(k+1)m}$.

- compute $\mathbf{C} = \mathbf{BH} - \mathbf{UF} + \mathbf{E}^*\mathbf{F} + \mathbf{E}$ where $\mathbf{E} \leftarrow \mathcal{D}^{m\times\kappa}_{\mathbb{Z},\sigma}$.
- compute $\mathbf{C}' = \mathbf{PH} - \mathbf{AF} + (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) + \overline{\mathbf{E}}\mathbf{F} + \tilde{\mathbf{E}} + \mathbf{E}'$ where $\mathbf{E}' \leftarrow \mathcal{D}^{k\times\kappa}_{\mathbb{Z},\sigma'}$ where $\tilde{\mathbf{E}}$ is such that $((\mathbf{I}_k,\mathbf{0})\otimes(s_1,\ldots,s_n,-1)\otimes\mathbf{g}^\intercal)\mathbf{F} = (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) + \tilde{\mathbf{E}}$.

It is easy to see that Hyb_1 and Hyb_2 are identically distributed. When we substitute $\mathbf{S} = \mathbf{H} - \mathbf{RF}$ in $\mathbf{C}$ and $\mathbf{C}'$, we get $\mathbf{C} = \mathbf{BS} + \mathbf{E} = \mathbf{B}(\mathbf{H} - \mathbf{RF}) + \mathbf{E} = \mathbf{BH} - \mathbf{UF} + \mathbf{E}^*\mathbf{F} + \mathbf{E}$ and $\mathbf{C}' = \mathbf{PS} + \mathbf{E}' = \mathbf{P}(\mathbf{H} - \mathbf{RF}) + \mathbf{E}' = \mathbf{PH} - \mathbf{PRF} + \mathbf{E}' = \mathbf{PH} - (\mathbf{AF} - (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) - \tilde{\mathbf{E}} - \overline{\mathbf{E}}\mathbf{F}) + \mathbf{E}' = \mathbf{PH} - \mathbf{AF} + (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) + \overline{\mathbf{E}}\mathbf{F} + \tilde{\mathbf{E}} + \mathbf{E}'$. Therefore, $\mathsf{Hyb}_1 \approx_s \mathsf{Hyb}_2$.

Hyb_3**:** This is same as Hyb_2 except the way we compute $\mathbf{C}, \mathbf{C}'$. In this hybrid, we compute $\mathbf{C} = \mathbf{BH} - \mathbf{UF} + \mathbf{E}$ where $\mathbf{E} \leftarrow \mathcal{D}^{m\times\kappa}_{\mathbb{Z},\sigma}$ and $\mathbf{C}' = \mathbf{PH} - \mathbf{AF} + (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) + \mathbf{E}'$ where $\mathbf{E}' \leftarrow \mathcal{D}^{k\times\kappa}_{\mathbb{Z},\sigma'}$. Note that by GSW noise bound setting, we have $||\tilde{\mathbf{E}}|| \le \tilde{B}$, from the analysis of $\beta = 0$ case in Claim 5.10, we have $||\overline{\mathbf{E}}\mathbf{F}|| \le \lambda(k+1)m\rho$ and $||\mathbf{E}^*\mathbf{F}|| \le \lambda(k+1)m\rho$ and by parameter setting we have $\sigma = \sigma' \ge 2^\lambda(\tilde{B} + \lambda(k+1)m\rho)$, we have $\mathbf{E}^*\mathbf{F} + \mathbf{E} \approx_s \mathbf{E}$ and $\overline{\mathbf{E}}\mathbf{F} + \tilde{\mathbf{E}} + \mathbf{E}' \approx_s \mathbf{E}'$. Therefore, $\mathsf{Hyb}_2 \approx_s \mathsf{Hyb}_3$.

Hyb_4**:** This is same as Hyb_3 except the way we compute $\mathbf{A}, \mathbf{U}$. In this hybrid, we sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{k\times(k+1)m}$ and $\mathbf{U} \leftarrow \mathbb{Z}_q^{m\times(k+1)m}$. We now prove that $\mathsf{Hyb}_3 \approx_c \mathsf{Hyb}_4$. Let $\mathcal{A}$ be the adversary that distinguishes between Hyb_3 and Hyb_4. Then we construct a reduction $\mathcal{B}$ that acts as an adversary against LWE. $\mathcal{B}$ does the following.

- Challenger of LWE samples $\beta \leftarrow \{0,1\}$ and sends $(\mathbf{V}, \mathbf{Z} = \mathbf{VR} + \mathbf{E})$, where $\mathbf{E} = \begin{pmatrix}\mathbf{E}'\\ \mathbf{E}^*\end{pmatrix}$ if $\beta = 0$ and $(\mathbf{V}, \mathbf{Z} \leftarrow \mathbb{Z}_q^{k+m\times(k+1)m})$ if $\beta = 1$. Here $\mathbf{V} \leftarrow \mathbb{Z}_q^{k+m\times n}$.
- Parse $\mathbf{V} = \begin{pmatrix}\mathbf{P}\\ \mathbf{B}\end{pmatrix}$ and $\mathbf{Z} = \begin{pmatrix}\mathbf{A}'\\ \mathbf{U}\end{pmatrix}$.
- Choose $(K, \mathsf{aux}_K) \leftarrow \mathsf{KeySamp}(1^\lambda)$, sample $K'' \leftarrow \{0,1\}^\lambda$ and set $K' = (1, K'')$ and $\overline{K} = (K, K')$.
- Samples $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{s}}}$ and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.
- Sample $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{R}_{\mathsf{fhe},\ell} \leftarrow \{0,1\}^{m\times m}$ for all $\ell \in [\eta+\lambda+1]$ and compute a GSW encryption as follows.

$$\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix}\bar{\mathbf{A}}_{\mathsf{fhe}}\\ \bar{\mathbf{s}}^\intercal\bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}}\end{pmatrix}, \qquad \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (\overline{K})\otimes\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m(\lambda+\eta+1)}$$

  where $\mathbf{R}_{\mathsf{fhe}} = (\mathbf{R}_{\mathsf{fhe},1},\ldots,\mathbf{R}_{\mathsf{fhe},(\lambda+\eta+1)})$.
- Set $\mathbf{A} = \mathbf{A}' + (\mathbf{I}_k,\mathbf{0})\otimes\mathbf{s}^\intercal\otimes\mathbf{g}^\intercal$.
- For $i \in [\kappa]$
  - Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathrm{MakeVEvalCkt}(n,m,q,C'_{\mathrm{F}_i})$.
  - Compute $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathbf{X})$.
  - Let $\mathbf{f}_i \in \mathbb{Z}_q^{k(n+1)}$ be the vectorization of $\mathbf{X}_{C'_{\mathrm{F}_i}}$.
  - Sample $\mathbf{r}_i \leftarrow \{0,1\}^m$.
- Set $\mathbf{F} = (\mathbf{G}^{-1}_{\mathbf{r}_1}(\mathbf{f}_1),\ldots,\mathbf{G}^{-1}_{\mathbf{r}_\kappa}(\mathbf{f}_\kappa))$.
- Sample $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$.
- Set $\mathsf{aux} = (\mathbf{H}, \mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$.

- Compute $\mathbf{C} = \mathbf{BH} - \mathbf{UF} + \mathbf{E}$ where $\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa}$.
- Compute $\mathbf{C}' = \mathbf{PH} - \mathbf{AF} + (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) + \mathbf{E}'$ where $\mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma'}^{k\times\kappa}$.
- Output $(\mathbf{B},\mathbf{P},\mathbf{C},\mathbf{C}',\mathsf{aux})$ to $\mathcal{A}$.
- On receiving β' from $\mathcal{A}$, outputs β'.

It is straightforward to see that if $\beta = 0$, then $\mathcal{B}$ simulated Hyb_3 as $\mathbf{A} = \mathbf{A}' + (\mathbf{I}_k,\mathbf{0}) \otimes \mathbf{s}^\intercal \otimes \mathbf{g}^\intercal = \mathbf{PR} + \mathbf{E}' + (\mathbf{I}_k,\mathbf{0}) \otimes \mathbf{s}^\intercal \otimes \mathbf{g}^\intercal$ and $\mathbf{U} = \mathbf{BR} + \mathbf{E}^*$, else it simulated Hyb_4 as $\mathbf{A} = \mathbf{A}' + (\mathbf{I}_k,\mathbf{0}) \otimes \mathbf{s}^\intercal \otimes \mathbf{g}^\intercal$ is uniformly random and $\mathbf{U}$ is uniformly random. Hence, $\mathsf{Hyb}_3 \approx_c \mathsf{Hyb}_4$ by the hardness of LWE.

Hyb_5**:** This is same as Hyb_4 except that we compute $\mathbf{X}$ as $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (0^{\eta+\lambda+1}) \otimes \mathbf{G}$. We now prove that $\mathsf{Hyb}_4 \approx_c \mathsf{Hyb}_5$. Let $\mathcal{A}$ be the adversary that distinguishes between Hyb_4 and Hyb_5. Then we construct a reduction $\mathcal{B}$ that breaks the IND-CPA security of the GSW FHE scheme. $\mathcal{B}$ does the following.

- Sample $\mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}, \quad \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}$.
- Choose $(K,\mathsf{aux}_K) \leftarrow \mathsf{KeySamp}(1^\lambda)$, sample $K'' \leftarrow \{0,1\}^\lambda$ and set $K' = (1,K'')$ and $\overline{K} = (K,K')$.
- $\mathcal{B}$ sends the messages, $\overline{K}$ and $0^{\eta+\lambda+1}$ to the challenger of GSW.
- Challenger of GSW FHE scheme samples $\beta \leftarrow \{0,1\}$ and sends $(\mathbf{A}_{\mathsf{fhe}}, \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (\overline{K}) \otimes \mathbf{G})$ if $\beta = 0$ and $(\mathbf{A}_{\mathsf{fhe}}, \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (0^{\eta+\lambda+1}) \otimes \mathbf{G})$ if $\beta = 1$.
- Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{k\times(k+1)m}$, $\mathbf{U} \leftarrow \mathbb{Z}_q^{m\times(k+1)m}$.
- For $i \in [\kappa]$
  - Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathrm{MakeVEvalCkt}(n,m,q,C'_{\mathrm{F}_i})$.
  - Compute $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathbf{X})$.
  - Let $\mathbf{f}_i \in \mathbb{Z}_q^{k(n+1)}$ be the vectorization of $\mathbf{X}_{C'_{\mathrm{F}_i}}$.
  - Sample $\mathbf{r}_i \leftarrow \{0,1\}^m$.
- Set $\mathbf{F} = (\mathbf{G}_{\mathbf{r}_1}^{-1}(\mathbf{f}_1),\ldots,\mathbf{G}_{\mathbf{r}_\kappa}^{-1}(\mathbf{f}_\kappa))$.
- Sample $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$.
- Set $\mathsf{aux} = (\mathbf{H},\mathbf{A}_{\mathsf{fhe}},\mathbf{X},\mathbf{A},\{\mathbf{r}_i\}_{i\in[\kappa]},\mathsf{aux}_K)$.
- Compute $\mathbf{C} = \mathbf{BH} - \mathbf{UF} + \mathbf{E}$ where $\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}^{m\times\kappa}$.
- Compute $\mathbf{C}' = \mathbf{PH} - \mathbf{AF} + (\mathrm{F}(\overline{K},1),\ldots,\mathrm{F}(\overline{K},\kappa)) + \mathbf{E}'$ where $\mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\sigma'}^{k\times\kappa}$.
- Output $(\mathbf{B},\mathbf{P},\mathbf{C},\mathbf{C}',\mathsf{aux})$ to $\mathcal{A}$.
- On receiving β' from $\mathcal{A}$, outputs β'.

It is straightforward to see that if $\beta = 0$, then $\mathcal{B}$ simulated Hyb_4, else it simulated Hyb_5. Hence, $\mathsf{Hyb}_4 \approx_c \mathsf{Hyb}_5$ by the IND-CPA security of the GSW FHE scheme.

Hyb_6**:** This is same as Hyb_5 except the we sample $\mathbf{C}'$ as $\mathbf{C}' \leftarrow \mathbb{Z}_q^{k\times\kappa}$. Note that for $f \in \mathcal{F}_{\mathsf{prm}}$,

$$(\{f(K,i)\}_{i\in[\kappa]},\mathsf{aux}_K) \approx_c (\{\mathbf{u}_i :\ \mathbf{u}_i \leftarrow \{0,1\}^k\}_{i\in[\kappa]},\mathsf{aux}_K),$$

which implies

$$(\{\lfloor q/2\rceil\, f(K,i) + \mathsf{PRF}(K',i) + \mathbf{E}'[\cdot,i]\}_{i\in[\kappa]},\mathsf{aux}_K) \approx_c (\{\tilde{\mathbf{c}}_i :\ \tilde{\mathbf{c}}_i \leftarrow \mathbb{Z}_q^k\}_{i\in[\kappa]},\mathsf{aux}_K),$$

where $||\mathbf{E}'[\cdot,i]|| \le \sqrt{\lambda}\sigma' \le \hat{B}$ and $\hat{B}$ is exponentially smaller than q. Therefore, $\mathsf{Hyb}_5 \approx_c \mathsf{Hyb}_6$.

Hyb_7**:** This is same as Hyb_6 except that in this hybrid, we sample $\mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}$. We prove that $\mathsf{Hyb}_6 \approx_c \mathsf{Hyb}_7$ using the hardness of LWE. Let $\mathcal{A}$ be the adversary that distinguishes between Hyb_6 and Hyb_7. Then we construct a reduction $\mathcal{B}$ that acts as an adversary against LWE. $\mathcal{B}$ does the following.

- Challenger of LWE samples $\beta \leftarrow \{0,1\}$ and sends $(\mathbf{V}, \mathbf{Z} = \mathbf{TV} + \mathbf{E} \in \mathbb{Z}_q^{m\times\kappa})$, if $\beta = 0$ and $(\mathbf{V}, \mathbf{Z} \leftarrow \mathbb{Z}_q^{m\times\kappa})$ if $\beta = 1$. Here $\mathbf{V} \leftarrow \mathbb{Z}_q^{(n+1)\times\kappa}$.
- Sample $\mathbf{U}' \leftarrow \mathbb{Z}_q^{m\times(k+1)m}$.
- Sample $\mathbf{P} \leftarrow \mathbb{Z}_q^{k\times n}$, $\mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}$.
- Samples $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{s}}}$ and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.
- Sample $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{R}_{\mathsf{fhe},\ell} \leftarrow \{0,1\}^{m\times m}$ for all $\ell \in [\eta+\lambda+1]$ and compute a GSW encryption as follows.

$$\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe}}^\intercal \end{pmatrix}, \quad \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathsf{fhe}} - (0^{\eta+\lambda+1}) \otimes \mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m(\lambda+\eta+1)}$$

  where $\mathbf{R}_{\mathsf{fhe}} = (\mathbf{R}_{\mathsf{fhe},1}, \ldots, \mathbf{R}_{\mathsf{fhe},(\lambda+\eta+1)})$.
- Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{k\times(k+1)m}$
- For $i \in [\kappa]$
  - Define the homomorphic evaluation circuit $\mathsf{VEval}_{C'_{\mathrm{F}_i}} = \mathrm{MakeVEvalCkt}(n, m, q, C'_{\mathrm{F}_i})$.
  - Compute $\mathbf{X}_{C'_{\mathrm{F}_i}} = \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathbf{X})$.
  - Let $\mathbf{f}_i \in \mathbb{Z}_q^{k(n+1)}$ be the vectorization of $\mathbf{X}_{C'_{\mathrm{F}_i}}$.
- Set $\mathsf{aux} = (\mathbf{H}, \mathbf{A}_{\mathsf{fhe}}, \mathbf{X}, \mathbf{A}, \{\mathbf{r}_i\}_{i\in[\kappa]}, \mathsf{aux}_K)$.
- Compute $\mathbf{C}' \leftarrow \mathbb{Z}_q^{k\times\kappa}$.
- For $i \in [k]$, set $\mathbf{r}_i = \mathbf{G}^{-1}(\mathbf{V}[\cdot, i])$ where $\mathbf{V}[\cdot, i]$ is the ith column of $\mathbf{V}$.
- Set $\mathbf{F} = (\mathbf{G}^{-1}_{\mathbf{r}_1}(\mathbf{f}_1), \ldots, \mathbf{G}^{-1}_{\mathbf{r}_\kappa}(\mathbf{f}_\kappa))$.
- Sample $\mathbf{H} \leftarrow \mathbb{Z}_q^{n\times\kappa}$.
- Compute $\mathbf{C} = \mathbf{BH} + \mathbf{Z} + \mathbf{U}'\mathbf{F}$.
- Output $(\mathbf{B}, \mathbf{P}, \mathbf{C}, \mathbf{C}', \mathsf{aux})$ to $\mathcal{A}$.
- On receiving β' from $\mathcal{A}$, outputs β'.

Since, $\mathbf{V}$ is uniformly random, $\mathbf{r}_i$ are i.i.d uniformly random. Now when $\mathbf{Z} = \mathbf{TV} + \mathbf{E}$, we have $\mathbf{Z} + \mathbf{U}'\mathbf{F} = \mathbf{TV} + \mathbf{E} + \mathbf{U}'\mathbf{F} = (0^{m\times km}, \mathbf{TG})\mathbf{F} + \mathbf{E} + \mathbf{U}'\mathbf{F} = ((0^{m\times km}, \mathbf{TG}) + \mathbf{U}')\mathbf{F} + \mathbf{E} = \mathbf{UF} + \mathbf{E}$. Here $\mathbf{U} = (0^{m\times km}, \mathbf{TG}) + \mathbf{U}'$ is uniformly random. Hence, in this case, we have $\mathbf{C} = \mathbf{BH} + \mathbf{Z} + \mathbf{U}'\mathbf{F} = \mathbf{BH} + \mathbf{UF} + \mathbf{E}$ which is identitcal to distribution of $\mathbf{C}$ in Hyb_6.

When $\mathbf{Z} \leftarrow \mathbb{Z}_q^{m\times\kappa}$, we have $\mathbf{C} \leftarrow \mathbb{Z}_q^{m\times\kappa}$. Therefore, $\mathsf{Hyb}_6 \approx_c \mathsf{Hyb}_7$ by the hardness of LWE.

Hyb_8**:** This is same as Hyb_7 except that we undo the changes made in Hyb_5. In this hybrid, we compute $c \leftarrow \mathsf{Enc}(\mathbf{A}_{\mathsf{fhe}}, \overline{K})$. $\mathsf{Hyb}_7 \approx_c \mathsf{Hyb}_8$ by the IND-CPA security of the GSW FHE scheme. We skip the indistinguishability argument as it is the same as that of $\mathsf{Hyb}_4 \approx \mathsf{Hyb}_5$.

Hyb_9**:** This is same as Hyb_8 except that we undo the changes made in Hyb_4. We compute $\mathbf{A}$ as: Parse $\mathbf{s} = (s_1, \ldots, s_n, -1) \in \mathbb{Z}_q^{n+1}$, sample $\mathbf{R} \leftarrow \mathbb{Z}_q^{n\times(k+1)m}$ and $\overline{\mathbf{E}} \leftarrow \mathcal{D}^{k\times(k+1)m}_{\mathbb{Z},\rho}$ and compute $\mathbf{A} = \mathbf{PR} + \overline{\mathbf{E}} + (\mathbf{I}_k, \mathbf{0}) \otimes (s_1, \ldots, s_n, -1) \otimes \mathbf{g}^\intercal \in \mathbb{Z}_q^{k\times(k+1)m}$. $\mathsf{Hyb}_8 \approx_c \mathsf{Hyb}_9$ by the hardness of LWE. We skip the indistinguishability argument as it is the same as that of $\mathsf{Hyb}_3 \approx \mathsf{Hyb}_4$.

Hyb_{10}**:** This is same as Hyb_9 except that we undo the changes made in Hyb_2. In this hybrid, we sample $\mathbf{S} \leftarrow \mathbb{Z}_q^{n\times\kappa}$ and set $\mathbf{H} = \mathbf{S} + \mathbf{RF}$. Hyb_9 and Hyb_{10} are identically distributed. We skip the indistinguishability argument as it is the same as that of $\mathsf{Hyb}_1 \approx \mathsf{Hyb}_2$.

Hyb_{11}**:** This is same as Hyb_{10} except that we undo the changes made in Hyb_1. We sample $\mathbf{D} \leftarrow \mathcal{D}_{\mathbb{Z},\tau}^{k\times m}$ and set $\mathbf{P} = \mathbf{D}\cdot\mathbf{B}$. We have $\mathsf{Hyb}_{10} \approx \mathsf{Hyb}_{11}$ from Lemma 3.6 and Lemma 3.8. We skip the indistinguishability argument as it is the same as that of $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1$.

The distribution as in Hyb_{11} is the same as $\mathsf{D}_1^{\mathsf{pre}}$. Hence, the proof. □

□

5.3 Extending BDJMMPV PRO Counterexample to Multi-Challenge PRFE

In this section, we adapt the counterexamples from [BDJ+24] against the existence of PRO for all function families to show that there exist pseudorandom function families for which multi-challenge PRFE is not possible. Similar to [BDJ+24] we construct the counterexample in two steps:

1. **Counterexample in the presence of auxiliary input**. In this section, we show that for all pseudorandom function families there exists auxiliary information, with respect to which, a multi-challenge PRFE cannot be constructed.

   Theorem 5.13. Assuming the existence of sub-exponentially secure, instance hiding witness encryption for NP, for every function family $\mathcal{F}_{\mathsf{prm}} = \{f : \mathcal{X}_{\mathsf{prm}} \to \mathcal{Y}_{\mathsf{prm}}\}$, where prm consist of polynomially bounded functions of λ[21], including bound $s = s(\lambda)$ on the size of the circuits computing any function in the family, satisfying

   $$\{f_i\}_{i\in[Q_k]}, \{f_i(x_j)\}_{i\in[Q_k],j\in[Q_c]} \approx_c \{f_i\}_{i\in[Q_k]}, \{u_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q_k],j\in[Q_c]}, \tag{33}$$

   where x_j's are chosen in such a way that they have enough entropy, there exists a dependent auxiliary input aux, such that there does not exist any PRFE scheme satisfying prCT security.

   Proof. Consider any pseudorandom function family $\mathcal{F}$ - for example, a PRF family, with the input of the form $x_j = (K, j)$, and function $f_i(x_j) = \mathsf{PRF}(K, (i, j))$. Suppose $\mathsf{PRFE} = (\mathsf{PRFE.Setup}, \mathsf{PRFE.Enc}, \mathsf{PRFE.KeyGen}, \mathsf{PRFE.Dec})$ be any functional encryption scheme for $\mathcal{F}$, with ciphertext of size at most $p_c(\lambda, s)$ and secret key of length at most $p_k(\lambda, s)$, where p_c, p_k and p are some polynomials. Let $\mathsf{prm}' = (p_c, p_k, Q_c, Q_k)$.

   Then, to prove the above theorem, we need to define an efficient sampler that outputs $(\mathsf{aux}, \{f_i\}_{i\in[Q_k]}, \{x_i\}_{i\in[Q_k]})$, such that

   (a) (Pre-condition holds) For all PPT adversary $\mathcal{A}$

   $$D_0^{\mathsf{pre}} := (\mathsf{aux}, \{f_i\}_{i\in[Q_k]}, \{f_i(x_j)\}_{i\in[Q_k],j\in[Q_c]}) \approx_c D_1^{\mathsf{pre}} := (\mathsf{aux}, \{f_i\}_{i\in[Q_k]}, \{u_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q_k],j\in[Q_c]}) \tag{34}$$

   (b) (Distinguisher for post condition) Define a distinguisher for

   $$\begin{aligned} D_0^{\mathsf{post}} &:= (\mathsf{aux}, \{f_i\}_{i\in[Q_k]}, \{\mathsf{ct}_j\}_{j\in[Q_c]}, \{\mathsf{sk}_i\}_{i\in[Q_k]}), \\ D_1^{\mathsf{post}} &:= (\mathsf{aux}, \{f_i\}_{i\in[Q_k]}, \{u_j \leftarrow \mathcal{CT}\}_{j\in[Q_c]}, \{\mathsf{sk}_i\}_{i\in[Q_k]}), \end{aligned} \tag{35}$$

   where $(\mathsf{fmpk}, \mathsf{fmsk}) \leftarrow \mathsf{PRFE.Setup}(1^\lambda, \mathsf{prm})$, $\mathsf{ct}_j = \mathsf{PRFE.Enc}(\mathsf{fmpk}, x_j)$ and $\mathsf{sk}_i = \mathsf{PRFE.KeyGen}(\mathsf{fmsk}, f_i)$, for $i \in [Q_k], j \in [Q_c]$, and $\mathcal{CT}$ is the ciphertext space of PRFE.

[21] We drop the subscript prm when not explicitly needed, to keep the notations simple.

Defining the sampler Samp**.** $\mathsf{Samp}(1^\lambda)$ does the following:

(a) Let Q_k and Q_c are such that $(\log|\mathcal{Y}|)Q_kQ_c > (Q_kp_k + Q_cp_c + 1) + \lambda$.
Define the following NP relation

$$\mathcal{L}_{\mathsf{prm}'} = \{(y_{1,1},\ldots,y_{1,Q_c},\ldots,y_{Q_k,1},\ldots,y_{Q_k,Q_c}) \mid \exists \mathsf{ct}_1,\ldots,\mathsf{ct}_{Q_c},\mathsf{sk}_1,\ldots\mathsf{sk}_{Q_k}\ s.t. \quad (36)$$
$$\forall\, i\in[Q_k], j\in[Q_c], y_{i,j} = \mathsf{PRFE.Dec}(\mathsf{sk}_i,\mathsf{ct}_j) \text{ and } |\mathsf{ct}_j| \le p_c \text{ and } |\mathsf{sk}_i| \le p_k\ \}.$$

Thus, the length of any witness can be at most $Q_kp_k + Q_cp_c$. Here, we assume that PRFE master public key, fmpk, is also a part of the ciphertexts.

(b) Choose $f_1,\ldots,f_{Q_k} \in \mathcal{F}_{\mathsf{prm}}$, and $\mathbf{x}_1,\ldots,\mathbf{x}_{Q_c} \leftarrow \mathcal{X}$, such that the indistinguishability in (33) holds. For example, for the PRF example above, f_i is the PRF function with i hardwired and $\mathbf{x}_j$ can be (K,j), where K is chosen uniformly from the PRF key space.

(c) Let $\mathsf{stmt} = (f_1(\mathbf{x}_1),\ldots f_1(\mathbf{x}_{Q_c}),\ldots,f_{Q_k}(\mathbf{x}_1),\ldots,f_{Q_k}(\mathbf{x}_{Q_c}))$.

(d) Define $\mathsf{aux} = (\mathsf{WE.Enc}(\mathsf{stmt},0),\mathsf{WE.Enc}(\mathsf{stmt},1))$.

(e) Output $(\mathsf{aux}, f_1,\ldots,f_{Q_k},\mathbf{x}_1,\ldots,\mathbf{x}_{Q_c})$.

Analyzing the post condition. We first prove the following claim that we will need to motivate/analyze the distinguisher's strategy.

Claim 5.14. In the absence of $\mathsf{ct}_1,\ldots,\mathsf{ct}_{Q_c}$ or any other terms dependent on $\{\mathbf{x}_j\}_{j\in[Q_c]}$, for all PPT adversary $\mathcal{A}$,

$$(\{f_i\}_{i\in[Q_k]},\{\mathsf{sk}_i\}_{i\in[Q_k]},\mathsf{WE.Enc}(\mathsf{stmt},0)) \approx_c (\{f_i\}_{i\in[Q_k]},\{\mathsf{sk}_i\}_{i\in[Q_k]},\mathsf{WE.Enc}(\mathsf{stmt},1))$$

Proof. We prove the above claim via the following hybrids.

Hyb_0**:** In this hybrid, $\mathcal{A}$ gets $\mathsf{WE.Enc}(\mathsf{stmt},0)$.

Hyb_1**:** In this hybrid, stmt is replaced with stmt', where $\mathsf{stmt}' = (u_{1,1},\ldots u_{1,Q_c},\ldots,u_{Q_k,1},\ldots u_{Q_kQ_c})$, where $u_{i,j} \leftarrow \{0,1\}^\ell$ for all $i\in[Q_k], j\in[Q_c]$. That is, $\mathcal{A}$ gets $\mathsf{WE.Enc}(\mathsf{stmt}',0)$.
Indistinguishability follows from pseudorandomness of $\mathcal{F}_{\mathsf{prm}}$. In particular, if $\mathcal{A}$ can distinguish between the two hybrids, then we can construct a reduction $\mathcal{B}$ against pseudorandomness of $\mathcal{F}$ as follows.

(a) Upon input $(\{f_i\}_{i\in[Q_k]},\{c_{i,j}\}_{i\in[Q_k],j\in[Q_c]})$, where $c_{i,j} = f_i(x_j)$, for some $x_j \in \mathcal{X}$, if $\beta = 0$, else $c_{i,j} \leftarrow \mathcal{Y}$, sample $(\mathsf{fmpk},\mathsf{fmsk}) \leftarrow \mathsf{PRFE.Setup}(1^\lambda,\mathsf{prm})$. Compute $\mathsf{sk}_i = \mathsf{PRFE.KeyGen}(\mathsf{fmsk},f_i)$, for $i\in[Q_k]$. Set $\mathsf{stmt} = (c_{1,1},\ldots,c_{Q_c,Q_k})$.

(b) Send $(\{f_i\}_{i\in[Q_k]},\{\mathsf{sk}_i\}_{i\in[Q_k]},\mathsf{WE.Enc}(\mathsf{stmt},0))$ to $\mathcal{A}$.

(c) In the end, $\mathcal{A}$ outputs its guess bit β'. $\mathcal{B}$ also outputs β'.

Clearly, if $\beta = 0$, $\mathcal{B}$ simulates Hyb_0, else Hyb_1 with $\mathcal{A}$. Hence, $\mathcal{B}$ wins with the same advantage as that of $\mathcal{A}$.

Hyb_2**:** In this hybrid, $\mathcal{A}$ is given $\mathsf{WE.Enc}(\mathsf{stmt}',1)$.
Indistinguishability follows from the soundness of WE scheme, since for a randomly chosen set of $\{c_{i,j}\}_{i\in[Q_k],j\in[Q_c]}$, the probability of this being in $\mathcal{L}_{\mathsf{prm}'}$ is negligible. This follows from the standard counting argument as follows: since any witness can be of length at most $Q_cp_c + Q_kp_k$, total number of possible witness is at most $2^{Q_cp_c+Q_kp_k+1}$. Further, since PRFE decryption is a deterministic operation, there can be at most $2^{Q_cp_c+Q_kp_k+1}$ members in the language $\mathcal{L}_{\mathsf{prm}'}$. On the other hand, total number of choices for $\{c_{i,j}\in\mathcal{Y}\}_{i\in[Q_k],j\in[Q_c]}$ is $2^{(\log|\mathcal{Y}|)Q_kQ_c}$. Hence, by the choice of the parameters, for a randomly chosen set of $\{c_{i,j}\}_{i,j}$, this being inside the language is $\le 2^{-\lambda}$.

Hyb_4: In this hybrid, $\mathcal{A}$ gets $\mathsf{WE.Enc}(\mathsf{stmt}, 1)$.

Indistinguishability, again follows from pseudorandomness of $\mathcal{F}$, similar to the indistinguishability between Hyb_0 and Hyb_1.

□

Based on the above claim, the strategy for the distinguisher, $\mathcal{A}^{\mathsf{post}}$, for the post condition is:

(a) Given $(\mathsf{aux} = (\mathsf{wct}_0, \mathsf{wct}_1), \{f_i\}_{i\in[Q_k]}, \{\mathsf{ct}_j\}_{j\in[Q_c]}, \{\mathsf{sk}_i\}_{i\in[Q_k]})$, where $\mathsf{ct}_j = \mathsf{PRFE.Enc}(\mathsf{fmpk}, x_j)$, if challenge bit $\beta = 0$, and $\mathsf{ct}_j \leftarrow \mathcal{CT}$, if $\beta = 1$.

(b) Define $\mathsf{wt} = (\mathsf{ct}_1, \ldots, \mathsf{ct}_{Q_c}, \mathsf{sk}_1, \ldots, \mathsf{sk}_{Q_k})$.

(c) Compute (μ_0, μ_1), where $\mu_b = \mathsf{WE.Dec}(\mathsf{wt}, \mathsf{wct}_b)$, for $b \in \{0,1\}$.

(d) If $(\mu_0, \mu_1) = (0,1)$, then output $\beta' = 0$, else return $\beta' = 1$.

With the above strategy, the adversary outputs $\beta' = \beta$ with probability $\approx 7/8$. This is because if $\beta = 0$, then $\Pr(\beta' = 0) = 1$ due to the correctness of WE. When $\beta = 1$, then the probability that $(\mu_0, \mu_1) = (0,1) \leq 1/4$ due to the above claim. In more detail, Claim 5.14 implies that for a random $\mathsf{ct}_1, \ldots, \mathsf{ct}_{Q_c}$, $\mathsf{wt} = (\mathsf{ct}_1, \ldots, \mathsf{ct}_{Q_c}, \mathsf{sk}_1, \ldots, \mathsf{sk}_{Q_k})$, $\Pr[\mathsf{WE.Dec}(\mathsf{wt}, \mathsf{wct}_0) = 0] = \Pr[\mathsf{WE.Dec}(\mathsf{wt}, \mathsf{wct}_1) = 0] = (p \leq 1, \text{ say})$. Because, otherwise $\mathcal{A}^{\mathsf{post}}$ could distinguish the L.H.S. and R.H.S in the claim, by sampling the random WE ciphertexts itself. Thus, $\Pr[\mathsf{WE.Dec}(\mathsf{wt}, \mathsf{wct}_0) = 1] = \Pr[\mathsf{WE.Dec}(\mathsf{wt}, \mathsf{wct}_1) = 1] = (1-p)$. This implies that $\Pr[(\mu_0, \mu_1) = (0,1)] = p(1-p) \leq 1/4$. Hence $\Pr(\beta' = 1) \geq 3/4$. This gives us the above probability of winning.

Analyzing the pre-condition

Claim 5.15. For all PPT adversary $\mathcal{A}$, $D_0^{\mathsf{pre}} \approx D_1^{\mathsf{pre}}$, where D_0^{pre} and D_1^{pre} are as defined in equation (34).

Proof. We prove the above claim via the following hybrids.

Hyb_0: This is D_0^{pre}. That is, $\mathcal{A}$ gets $((\mathsf{wct}_0, \mathsf{wct}_1), \{f_i\}_{i\in[Q_k]}, \{y_{i,j} = f_i(x_j)\}_{i\in[Q_k], j\in[Q_c]})$, where $\mathsf{wct}_b = \mathsf{WE.Enc}(\mathsf{stmt}, b)$ for $\mathsf{stmt} = (y_{1,1}, \ldots, y_{Q_k,Q_c})$ and $b \in \{0,1\}$.

Hyb_1: In this hybrid, $y_{i,j} \leftarrow \mathcal{Y}$ for all $i \in [Q_k], j \in [Q_c]$. stmt and hence, wct_0 and wct_1 are also computed using random $y_{i,j}$'s.

The indistinguishability between the two hybrids follows from the pseudorandomness of $\mathcal{F}$.

Hyb_2: In this hybrid, the challenger samples $\{u_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q_k], j\in[Q_c]}$ (independent of $y_{i,j}$'s which are also sampled randomly) and sets $\mathsf{stmt} = (u_{1,1}, \ldots, u_{Q_k,Q_c})$, and computes $\mathsf{wct}_b = \mathsf{WE.Enc}(\mathsf{stmt}, b)$ for $b \in \{0,1\}$.

Indistinguishability between the two hybrids follows from the instance hiding property of WE because both $(y_{1,1}, \ldots, y_{Q_k,Q_j})$ and $(u_{1,1}, \ldots, u_{Q_k,Q_j})$ are not in $\mathcal{L}_{\mathsf{prm}'}$ with $1 - \mathsf{negl}(\lambda)$ probability by the same argument as in the proof of claim 5.14 (in the step $\mathsf{Hyb}_1 \approx \mathsf{Hyb}_2$).

Hyb_3: In this hybrid, stmt is again set to $(f_1(x_1), \ldots, f_{Q_k}(x_{Q_c}))$ and $\mathsf{wct}_b = \mathsf{WE.Enc}(\mathsf{stmt}, b)$ for $b \in \{0,1\}$.

Since $\{u_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q_k], j\in[Q_c]}$ are independent of $\{y_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q_k], j\in[Q_c]}$, the indistinguishability between the two hybrids again follow from the pseudorandomness of $\mathcal{F}$.

Finally, the proof completes by observing that Hyb_3 corresponds to the distribution D_1^{pre}. □

This completes the proof of theorem 5.13. □

2. **Counterexample without auxiliary input:** To remove the auxiliary input aux, the idea is to output the WE ciphertexts as FE decryptions. However, since WE ciphertext can be polynomial in its witness size, we cannot perform its computation inside any circuit for which PRFE key is provided. This is because then PRFE ciphertext size and key size (p_c an p_k in above discussions) will be polynomial in Q_k and Q_c and we will not be able to apply incompressibility arguments as before. Instead, the sampler itself computes the WE ciphertext, wct, itself, as before, but now instead of providing it as aux, it divides wct into blocks of fixed lengths and encrypts each block into different PRFE ciphertexts, and provides an additional PRFE key for a function which simply outputs a part of its input. For this, to be able to argue the indistinguishability in the pre-condition, we need pseudorandomness of WE ciphertexts. This can be achieved by combining (plain) WE with compute-and-compare/lockable obfuscation [WZ17, GKW17]. Note that even though this increases the total number of PRFE ciphertexts, not all of them will be a part of the witness. Hence, we will still be able to apply the incompressibility argument as before.

   We prove the following theorem.

   Theorem 5.16. Assuming the existence of instance hiding WE with pseudorandom ciphertexts, there exists for all λ, a pseudorandom function family $\mathcal{F}_{\mathsf{prm}} = \{f : \mathcal{X}_{\mathsf{prm}} \to \mathcal{Y}_{\mathsf{prm}}\}$ as defined in equation (33), for which there does not exist a PRFE scheme satisfying prCT security. Here prm consists of some fixed polynomials in λ.

   Proof. To prove the above theorem, we need to define a function class $\mathcal{F}_{\mathsf{prm}}$ such that for any PRFE scheme PRFE for $\mathcal{F}_{\mathsf{prm}}$ there exists an efficient sampler Samp that on input (1^λ) outputs $(\{f_i\}_{i\in[Q'_k]}, \{x_j\}_{j\in[Q'_c]})$, for some Q'_k and Q'_c, we will set later, such that

   (a) (Pre-condition holds) For all PPT adversary $\mathcal{A}$,

   $$D_0^{\mathsf{pre}} := (\{f_i\}_{i\in[Q'_k]}, \{f_i(x_j)\}_{i\in[Q'_k],j\in[Q'_c]}) \approx_c D_1^{\mathsf{pre}} := (\{f_i\}_{i\in[Q'_k]}, \{u_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q'_k],j\in[Q'_c]}) \tag{37}$$

   (b) (Distinguisher for post condition) Define a distinguisher for

   $$D_0^{\mathsf{post}} := (\{f_i\}_{i\in[Q'_k]}, \{\mathsf{ct}_j\}_{j\in[Q'_c]}, \{\mathsf{sk}_i\}_{i\in[Q'_k]}),\ \ D_1^{\mathsf{post}} := (\{f_i\}_{i\in[Q'_k]}, \{u_j \leftarrow \mathcal{CT}\}_{j\in[Q'_c]}, \{\mathsf{sk}_i\}_{i\in[Q'_k]}),$$

   where $(\mathsf{fmpk}, \mathsf{fmsk}) \leftarrow \mathsf{PRFE.Setup}(1^\lambda)$, $\mathsf{ct}_j = \mathsf{PRFE.Enc}(\mathsf{fmpk}, x_j)$ and $\mathsf{sk}_i = \mathsf{PRFE.KeyGen}(\mathsf{fmsk}, f_i)$, for $i \in [Q'_k], j \in [Q'_c]$, and $\mathcal{CT}$ is the ciphertext space of PRFE.

   Defining the sampler. We first describe the ingredients needed to define our sampler.

   - Let $\mathsf{PRF} : \mathcal{K} \times (\mathbb{Z}_q \times \mathbb{Z}_q) \to \mathcal{Y}$ be a pseudorandom function that can be computed by circuits of size s_{F}, where $\mathcal{K}$ is the PRF key space.
   - Set $s = s_{\mathsf{F}}$.
   - Let $\mathcal{F}_s$ be a family of pseudorandom functions computable by circuits of size at most s. Let PRFE be any PRFE scheme for $\mathcal{F}_s$. Let $p_c = p_c(\lambda, s)$ and $p_k = p_k(\lambda, s)$, for some polynomials p_k and p_c, be the bound on the sizes of the ciphertexts and the secret keys, respectively, of PRFE scheme.
   - Let WE be a witness encryption scheme for the language defined in equation (36), wrt the above PRFE. Thus, witness is of size at most $Q_c p_c + Q_k p_k$. Let $p_w = p_w(Q_c p_c + Q_k p_k)$ be the bound on the size of the ciphertexts of WE. Thus, $p_w > Q_c, Q_k$.

We are now ready to define our sampler, Samp.

$\mathsf{Samp}(1^\lambda)$:

- Let Q_k and Q_c be such that

$$(\log|\mathcal{Y}|)Q_kQ_c > p_cQ_c + p_kQ_k + \lambda + 1. \tag{38}$$

- Let $Q_w = 2p_w/\log|\mathcal{Y}|$. To keep the notations simple, we assume that $\log|\mathcal{Y}|$ divides $2p_w$, else we can use padding. Also, since $p_w = \mathrm{poly}(\lambda, \log|\mathcal{Y}|, Q_c, Q_k)$, we assume $Q_w > Q_c$. In the otherwise case, we could set Q_w to be the maximum of Q_c and $2p_w/\log|\mathcal{Y}|$.
- Set $Q_k' = Q_k + 1$ and $Q_c' = Q_w$.
- For $i \in [Q_k]$, define function $f_i : \mathcal{K} \times \mathbb{Z}_q \times \mathcal{Y} \to \mathcal{Y}$, such that $f_i(K, j, c) = \mathsf{PRF}(K, (i, j))$.
- Define f_{Q_k+1} to be a selector function, g such that $g(K, j, c) = c$. Note that g is a simple function whose size is smaller than the PRF function and hence, lies in $\mathcal{F}_s$.
- Sample $K \leftarrow \mathcal{K}$ and do the following:
  (a) For all $i \in [Q_k]$ and $j \in [Q_c]$, compute $y_{i,j} = \mathsf{PRF}(K, (i, j))$.
  (b) Set $\mathsf{stmt} = (y_{1,1}, \ldots, y_{Q_k,Q_c})$.
  (c) Compute $\mathsf{wct}_0 = \mathsf{WE.Enc}(\mathsf{stmt}, 0)$ and $\mathsf{wct}_1 = \mathsf{WE.Enc}(\mathsf{stmt}, 1)$. Set $\mathsf{wct} = (\mathsf{wct}_0, \mathsf{wct}_1)$. Let w_l be the l-th block of wct, where each block is of length $\log|\mathcal{Y}|$ bits.
  (d) For $j \in [Q_w]$, set $x_j = (K, j, \mathsf{w}_j)$.
- Output $(\{f_1, \ldots, f_{Q_k}, g\}, \{x_1, \ldots, x_{Q_w}\})$.

Distinguisher's strategy for post condition. Let , $\mathcal{A}^{\mathsf{post}}$ be the distinguisher. It is given $(\{f_i\}_{i\in[Q_k]} \cup \{g\}, \{\mathsf{ct}_j\}_{j\in[Q_w]}, \{\mathsf{sk}_i\}_{i\in[Q_k]} \cup \{\mathsf{sk}_g\})$, where $\{\mathsf{sk}_i = \mathsf{PRFE.KeyGen}(\mathsf{fmsk}, f_i)\}_{i\in[Q_k]}$, $\mathsf{sk}_g = \mathsf{PRFE.KeyGen}(\mathsf{fmsk}, g)$ and $\{\mathsf{ct}_j = \mathsf{PRFE.Enc}(\mathsf{fmpk}, x_j)\}_{j\in[Q_w]}$, if the challenge bit $\beta = 0$, else $\{\mathsf{ct}_j \leftarrow \mathcal{CT}\}_{j\in[Q_w]}$, where $(\mathsf{fmpk}, \mathsf{fmsk}) \leftarrow \mathsf{PRFE.Setup}(1^\lambda)$, $\mathcal{CT}$ is the ciphertext space of PRFE. $\mathcal{A}^{\mathsf{post}}$ does the following:

(a) For $l \in [Q_w]$, compute $\widetilde{\mathsf{w}}_l = \mathsf{PRFE.Dec}(\mathsf{sk}_g, \mathsf{ct}_l)$; .
(b) Set $\widetilde{\mathsf{wct}} = (\widetilde{\mathsf{w}}_1, \ldots, \widetilde{\mathsf{w}}_{Q_w})$ and parse it as $\widetilde{\mathsf{wct}} = (\widetilde{\mathsf{wct}}_0, \widetilde{\mathsf{wct}}_1)$.
(c) Set witness $\widetilde{\mathsf{wit}} = (\mathsf{ct}_1, \ldots, \mathsf{ct}_{Q_c}, \mathsf{sk}_1, \ldots, \mathsf{sk}_{Q_k})$.
(d) Compute $b_0 = \mathsf{WE.Dec}(\widetilde{\mathsf{wit}}, \widetilde{\mathsf{wct}}_0)$ and $b_1 = \mathsf{WE.Dec}(\widetilde{\mathsf{wit}}, \widetilde{\mathsf{wct}}_1)$.
(e) If $(\mu_0, \mu_1) = (0, 1)$, output $\beta' = 0$,
Else, if any of the above steps fails, or if $(\mu_0, \mu_1) \neq (0, 1)$, output $\beta' = 1$.

Analyzing the distinguisher $\mathcal{A}^{\mathsf{post}}$. When $\beta = 0$, it is easy to see by inspection, that $\mathcal{A}^{\mathsf{post}}$ gets $(\mu_0, \mu_1) = (0, 1)$ in Step 2d. In particular, firstly, we observe that $\mathcal{A}^{\mathsf{post}}$ correctly recovers WE encryptions of 0 and 1 as $\widetilde{\mathsf{wct}} = (\widetilde{\mathsf{wct}}_0, \widetilde{\mathsf{wct}}_1)$ due to the correctness of PRFE. Next, we observe that $\widetilde{\mathsf{wit}}$ formed by first Q_c ciphertexts and Q_k keys indeed form a valid witness since for all $i \in [Q_k], j \in [Q_c]$, $\mathsf{PRFE.Dec}(\mathsf{sk}_i, c_j) = \mathsf{PRF}(K, (i, j)) = y_{i,j}$ due to the correctness of PRFE. Hence, by correctness of WE, $\mathsf{WE.Dec}(\widetilde{\mathsf{wit}}, \widetilde{\mathsf{wct}}_0) = 0$ and $\mathsf{WE.Dec}(\widetilde{\mathsf{wit}}, \widetilde{\mathsf{wct}}_1) = 1$. Hence, it outputs $\beta' = 0 = \beta$ with probability close to 1.

In case of $\beta = 1$, since all the Q_w ciphertexts are uniformly random, firstly it is unlikely that $\widetilde{\mathsf{wit}}$ formed by (random) c_j's (along with Q_k keys) will form a valid witness for WE ciphertext computed by $\mathcal{A}^{\mathsf{post}}$. Even if it does, bits 0 and 1 are information theoretically hidden by these ciphertexts.

Hence, $\Pr[(\mu_0, \mu_1) = (0,1)] \leq 1/4$. Thus, $\mathcal{A}^{\mathsf{post}}$ outputs $\beta' = 0$ with probability at most 1/4. That is, $\Pr(\beta' = 1 | \beta = 1) \geq 3/4$. This gives overall success probability of adversary close to at least $7/8$.

Analyzing the feasibility of equation (38). We note that the both input and output length of functions in $\mathcal{F}_s$ are independent of either Q_c and Q_k. Thus, $s = s_{\mathsf{F}}$ is independent of Q_k and Q_c since it simply computes a PRF. This implies that both p_k and p_c, which depend on s, are independent of Q_c and Q_k as well. Hence, it is possible to set the values of Q_c and Q_k such that the equation (38) is satisfied.

Analyzing the pre-condition We prove the following claim.

Claim 5.17. For all PPT adversary $\mathcal{A}^{\mathsf{pre}}$, $D_0^{\mathsf{pre}} \approx_c D_1^{\mathsf{pre}}$, where D_0^{pre} and D_1^{pre} are as defined in equation (37)

Proof. We prove the claim via the following hybrids.

Hyb_0**:** This is D_0^{pre}. That is, $\mathcal{A}^{\mathsf{pre}}$ gets $(\{f_i\}_{i\in[Q_k]} \cup \{g\}, \{y_{i,j}\}_{i\in[Q_k],j\in[Q_w]}, \{y'_l\}_{l\in[Q_w]})$, where $y_{i,j} = \mathsf{PRF}(K,(i,j))$ and $y'_l = g(K,l,\mathsf{w}_l) = \mathsf{w}_l$ which is the l-th block of $\mathsf{wct} = (\mathsf{wct}_0.\mathsf{wct}_1) = (\mathsf{WE.Enc}(\mathsf{stmt},0), \mathsf{WE.Enc}(\mathsf{stmt},0))$ for $\mathsf{stmt} = (y_{1,1},\ldots,y_{Q_k,Q_c})$.

Hyb_1**:** In this hybrid, $y_{i,j} \leftarrow \mathcal{Y}$ for all $i \in [Q_k], j \in [Q_w]$. Note that this also changes the computation of wct_0 and wct_1, which are now computed with respect to the statement formed by these (random) $y_{i,j}$'s for $i \in [Q_k], j \in [Q_c]$.

Indistinguishability from the previous hybrid follows directly from the pseudorandomness of PRF.

Hyb_2**:** In this hybrid, y'_j, for all $j \in [Q_w]$ is sampled uniformly randomly. In particular, the challenger samples $\mathsf{wct} = (\mathsf{wct}_0, \mathsf{wct}_1)$ randomly, which implies y'_j's are random. Observe that this is the same hybrid as D_1^{pre}.

Indistinguishability from the previous hybrid follows by firstly observing that $\mathsf{stmt} = (y_{1,1},\ldots,y_{Q_k,Q_c})$, for $\{y_{i,j} \leftarrow \mathcal{Y}\}_{i\in[Q_k],j\in[Q_c]}$, used in Hyb_1, is not in the language with probability $(1 - \mathsf{negl}(\lambda))$, due to the same arguments as in the proof of claim 5.14. Hence, the indistinguishability follows due to pseudorandomness of WE ciphertexts.

□

□

6 Counter-Measures

In this section we describe our understanding and implications of all known attacks in the literature, together with counter-measures to prevent them. Attacks by withholding information about **B** or **P** [BUW24] were discussed in Section 2 and can be prevented by ensuring that both **B** and **P** are known to the adversary. All other attacks we are aware of can be broadly categorized as:

1. Malicious sampler attacks: Attacks presented in Sections 4.1, 4.2, 5.1 and 5.2.
2. Contrived functionality attacks: Attack by Branco et al. [BDJ+24][Sec 9] and that in Section 5.2.

We discuss the learning from these attacks and suggest counter-measures against each of these below.

6.1 Malicious Sampler Attacks

The counter-examples in Sections 4.1, 4.2, 5.1 and 5.2 show that Evasive LWE, both public and private coin, does not hold for arbitrary samplers, who may choose circuit implementations and error distributions in a malicious way so as to make the post-condition false even when the pre-condition is true. Since the intuition was discussed in Section 2, we proceed to detail the counter-measures.

Controlling the Structure of P. Since a primary source of vulnerability is allowing adversarial control on the structure of $\mathbf{P}$, a natural counter-measure is to limit such control. Here, note that in the real world, the circuit implementation of F is chosen by the key generator, who is an honest party – this suggests it better models the real world if the adversary's control on the structure of $\mathbf{P}$ is removed/reduced.

Observe that for functionality, we want to support matrices $\mathbf{P}$ which have the structure of $\mathbf{A}_F$ where F represents the FHE evaluation circuit for the function f, where f is input to key generation. Here, an important point is that while f is chosen by the adversary, the circuit implementation of F can be made canonical and put outside the control of the adversary. We suggest two approaches below.

One approach is to use randomized encodings (RE) [IK02]. The usage of RE in the design of FE schemes is popular – it dates back to [GVW12] and has been used extensively since then, for instance in [JLS22]. Typically, RE is used in FE constructions to reduce the degree of the function. In our case however, we use RE to control the structure of the circuit. In more detail, the key generator for f does the following: let F represent the FHE evaluation circuit corresponding to f and let $\tilde{F}(\cdot, \mathbf{r})$ denote the randomized encoding of F. The key generator samples $\mathbf{r}$, computes $\tilde{F}(\cdot, \mathbf{r})$ and outputs the function secret key for this circuit [22]. The encryptor, given input $\mathbf{x}$, computes the ciphertext as before. Correctness of the FE is inherited from the correctness of randomized encodings. If we use Yao's garbled circuits to instantiate the randomized encoding, then $\tilde{F}$ involves computing SKE encryptions whose circuit can be fixed in the scheme. Thus, even if the attacker chooses f in some highly structured, adversarial manner, the function $\tilde{F}$ will have a fixed structure that the adversary cannot manipulate.

Another approach is to use the universal circuit [Val76] to restrict the structure of F and hence $\mathbf{P}$. Recall that a universal circuit (UC) is a circuit that can be programmed to simulate any Boolean circuit up to a given size. That is, a universal circuit U takes as input the bit representation of F in addition to an input $\mathbf{x}$, and produces as output $U(F, \mathbf{x}) = F(\mathbf{x})$. Since a universal circuit has fixed structure, this prevents the adversary from embedding contrived dependencies into $\mathbf{P}$. We observe that technically, there is also a fixed arithmetic computation that must be performed after the Boolean computation. Namely, we convert the Boolean output to $\mathbb{Z}_q$, divide the outcome by a constant and round to integer, and then multiply a constant again. However, these operations are fixed computation and the circuit structure remains fixed.

Error Size in Pre-Condition. The attack presented in Section 4.2 crucially exploits the fact that the error in the pre-condition is larger than that in the post-condition. Wee's original paper introducing evasive LWE [Wee22] intuited that this should not be the case and suggested choosing a larger error in the post-condition than in the pre-condition for a more conservative assumption. However, to the best of our knowledge, no attack was known to concretely exploit such a setting of parameters before our work. A natural fix to prevent such difficulties is to ensure that the error in the post-condition is as large or larger than that in the pre-condition.

Modifying Evasive LWE. Here, we suggest a more stringent version of evasive LWE with the goal of ensuring that the broken schemes fail to admit a proof under this modified assumption, while the unbroken ones do admit such a proof. We illustrate this using the scheme of AKY [AKY24a] – the analysis for [BDJ+24] is similar.

[22] Note that $\mathbf{r}$ need not be hidden in our setting as we do not require the security properties of randomized encodings.

Assumption 6.1 (Stringent Evasive LWE). Let $n, m, t, m', q \in \mathbb{N}$ be parameters and λ be a security parameter. Let χ, χ' and χ'' be parameters for Gaussian distributions. Let Samp be a PPT algorithm that, on input 1^λ, outputs

$$\mathbf{P} \in \mathbb{Z}_q^{n \times t}, \mathsf{aux} \in \{0,1\}^*$$

The modified Evasive LWE assumption says that, for every PPT Samp,

$$\begin{aligned} \text{If,} \quad & (i)(\mathbf{P}, \mathbf{SP} + \mathbf{EK}', \mathbf{K}', \mathsf{aux}) \overset{c}{\approx} (\mathbf{P}, \mathbf{SP} + \mathbf{E}', \mathbf{K}', \mathsf{aux}) \text{ and} \\ & (ii)(\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) \overset{c}{\approx} (\mathbf{B}, \mathbf{P}, \mathbf{C}_0, \mathbf{C}', \mathsf{aux}) \\ \text{Then,} \quad & (\mathbf{B}, \mathbf{P}, \mathbf{SB} + \mathbf{E}, \mathbf{K}, \mathsf{aux}) \overset{c}{\approx} (\mathbf{B}, \mathbf{P}, \mathbf{C}_0, \mathbf{K}, \mathsf{aux}) \end{aligned}$$

$$\begin{aligned} \text{where} \quad & (\mathbf{P}, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda), \mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{C}_0 \leftarrow \mathbb{Z}_q^{m' \times m}, \mathbf{C}' \leftarrow \mathbb{Z}_q^{m' \times t}, \\ & \mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z}, \chi}^{m' \times m}, \ \mathbf{K}' \leftarrow \mathcal{D}_{\mathbb{Z}, \chi''}^{m \times t}, \ \mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z}, \chi'}^{m' \times t}, \ \mathbf{S} \leftarrow \mathbb{Z}_q^{m' \times n} \\ & \mathbf{K} \leftarrow \mathbf{B}^{-1}(\mathbf{P}) \text{ with standard deviation } \chi''. \end{aligned}$$

In the *single-challenge* setting, $m' = 1$ whereas in the *multi-challenge* setting, m' can be an arbitrary polynomial in the security parameter.

Intuitively, we added an extra condition to check whether it is safe to replace the correlated error with i.i.d error given auxiliary information. We discuss the reasoning behind this in detail below, using AKY as the running example.

Why Evasive LWE is too strong as stated: As seen in Section 5.1, in the AKY construction, the term $\mathbf{s}^\intercal \mathbf{P} + \mathbf{e}_{\mathbf{P}}^\intercal$, given aux, can be simplified to:

$$\begin{aligned} \forall i \in [Q], \ \mathbf{z}_i &= \mathbf{c}^\intercal \cdot \mathbf{K}_i - \mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} \\ &= (\mathbf{s}^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B}}^\intercal) \cdot \mathbf{K}_i - (\mathbf{s}^\intercal (\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^\intercal) \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} \\ &= \mathbf{s}^\intercal \mathbf{B} \mathbf{K}_i + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{s}^\intercal \mathbf{A}_{\mathsf{att}} \mathbf{H}_{\mathbf{A}_{\mathsf{att}}}^{\mathrm{F}_i} + \mathbf{s}^\intercal \mathsf{VEval}_{C'_{\mathrm{F}_i}}(\mathsf{bits}(\mathbf{X})) - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} \\ &= \mathbf{s}^\intercal \mathbf{A}_{\mathrm{F}_i} + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{s}^\intercal \mathbf{A}_{\mathrm{F}_i} + \mathrm{F}_i(\mathbf{x}, \mathsf{sd}) - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} \\ &= f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \underbrace{\mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i}_{\text{Noise by ELWE}} \underbrace{- \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i}}_{\text{Evaluation Noise}} \end{aligned}$$

The usage of evasive LWE allows to replace the error $\mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i$ by a fresh i.i.d noise term $\mathbf{e}_{\mathbf{P}_i}^\intercal$ in the pre-condition. Thus, when analyzing the distribution in the pre-condition, this i.i.d noise term is used to break the correlation between $\mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)$ and $\mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}}$ and flood the leakage contained in the latter term. Subsequently, one can argue that $f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)$ is pseudorandom over the entire space as required by the proof.

However, in the real world, as shown in Claim 5.3, the circuit representation used to compute $\mathbf{A}_{\mathrm{F}_i}$ can be chosen so that $\forall i \in [Q], \ \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)[1] - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}}[1] = 0 \bmod 2$ with probability $\geq 1/2$. Since $f_i(\mathbf{x})$ is known by correctness, letting $\tilde{\mathbf{z}}_i = \mathbf{z}_i - f_i(\mathbf{x}) \lfloor q/2 \rceil$, we get:

$$\tilde{\mathbf{z}}_i = f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i - \mathbf{e}_{\mathsf{fhe}}^\intercal \mathbf{R}_{C'_{\mathrm{F}_i}} - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i} - f_i(\mathbf{x}) \lfloor q/2 \rceil$$

Then, due to Claim 5.3, we get that with probability $\geq 1/2$,

$$\forall i \in [Q], \ \tilde{\mathbf{z}}_i[1] = \mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i[1] - \mathbf{e}_{\mathsf{att}}^\intercal \mathbf{H}_{\mathbf{A}_{\mathsf{att}}, \mathbf{X}}^{\mathrm{F}_i}[1] \mod 2.$$

This in turn, leads to the attack. The core issue is that $\mathbf{e}_{\mathbf{B}}^\intercal \mathbf{K}_i$ does not have enough entropy since $\mathbf{K}_i$ is very wide and known publicly, hence it does not do a good job at flooding.

How the Modification Helps. Note that given the extra check in the pre-condition, we would need to explicitly check that the distribution $\mathbf{s}^\intercal \mathbf{A}_{\mathrm{F}_i} + \mathbf{e}^\intercal \mathbf{K}'_i$ (for random $\mathbf{e}^\intercal, \mathbf{K}'_i$) can be conjectured computationally indistinguishable from the distribution $\mathbf{s}^\intercal \mathbf{A}_{\mathrm{F}_i} + \mathbf{e}^\intercal_{\mathbf{P}_i}$ for i.i.d $\mathbf{e}^\intercal_{\mathbf{P}_i}$ in the presence of aux. For a contrived choice of $\mathbf{A}_{\mathrm{F}_i}$, we have seen that this conjecture does not hold – this would prevent the proof from going through. Similarly, when the pre-condition error is chosen larger as in the attack of Section 4.2, the above check will fail.

The AKY fix. Subsequent to these attacks, AKY fixed their construction so as to perform a modulus reduction step which gets rid of the problematic evaluation noise and replaces it with some rounding noise which cannot be correlated with the PRF output as before. We discuss why the revised AKY construction does admit a proof under the stricter assumption above.

In more detail, in the revised AKY construction, the term $\mathbf{s}^\intercal \mathbf{P} + \mathbf{e}^\intercal_{\mathbf{P}}$ (after simplification using aux as discussed above) in the real world now becomes:

$$\mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}^\intercal_{\mathbf{B}} \cdot \mathbf{K} - (M \cdot \mathbf{e}^\intercal_{\mathbf{s},\mathsf{high}} + \mathbf{e}^\intercal_{\mathbf{s},\mathsf{low}} + M \cdot \mathsf{err}_{\mathsf{high}} + \mathsf{err}_{\mathsf{low}})$$

where $\mathsf{err}_{\mathsf{high}}, \mathsf{err}_{\mathsf{low}} \in \{0,1\}^\ell$ is rounding error, $\mathbf{e}^\intercal_{\mathbf{s},\mathsf{high}} = \mathbf{s}^\intercal \left\lfloor \frac{\mathbf{A}_{\mathsf{high}}}{M} \right\rceil - \left\lfloor \mathbf{s}^\intercal \frac{\mathbf{A}_{\mathsf{high}}}{M} \right\rceil$ and $\mathbf{e}^\intercal_{\mathbf{s},\mathsf{low}} = \mathbf{s}^\intercal \left\lfloor \frac{\mathbf{A}_{\mathsf{low}}}{M} \right\rceil - \left\lfloor \mathbf{s}^\intercal \frac{\mathbf{A}_{\mathsf{low}}}{M} \right\rceil$, and $\mathbf{A}_{\mathsf{high}}, \mathbf{A}_{\mathsf{low}}$ are public matrices which do not encode any secrets.

Importantly, note that the evaluation error $(M \cdot \mathbf{e}^\intercal_{\mathbf{s},\mathsf{high}} + \mathbf{e}^\intercal_{\mathbf{s},\mathsf{low}} + M \cdot \mathsf{err}_{\mathsf{high}} + \mathsf{err}_{\mathsf{low}})$ cannot be arbitrarily made to depend on the PRF seed/value and can be conjectured to be flooded by $\mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)$ by setting the parameters appropriately. We emphasize the subtle circularity: the error depends on $\mathbf{s}$ which is used to hide the PRF seed in the FHE ciphertext, and the PRF output is used to flood the error, so we cannot claim that the new error is independent of the PRF seed. However, we can *conjecture* computational flooding since the new error seems very hard to exploit by the adversary.

Assuming computational flooding as above, the correlated evasive noise $\mathbf{e}^\intercal_{\mathbf{B}} \mathbf{K}_i$ is not required to break any dependence between the PRF output and the FHE evaluation noise and $f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)$ can be conjectured to be pseudorandom as desired in the original formulation of evasive LWE. In this setting, we can replace $\mathbf{e}^\intercal_{\mathbf{B}} \cdot \mathbf{K}$ by i.i.d error in the pre-condition and a proof under this assumption better captures the real world.

HLL Assumption. We note that the modified evasive LWE also captures the insecurity of the evasive circular LWE assumption used in [HLL23] by the same argument as above. In particular, we can see that the first condition of the pre-condition does not hold because of the same reason as [AKY24a]. This can be seen by replacing $f_i(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i)$ with $f_i(\mathbf{s})$ in the above analysis. However, the *scheme* of [HLL23] can be shown to satisfy the stricter pre-condition defined above, and is indeed not broken by the attack. Intuitively, this is because in the scheme of [HLL23], the attacker never recovers any value in the zeroizing regime, and hence cannot exploit the problematic correlations. Thus, the modified assumption separates the broken and unbroken schemes, by admitting a proof for the latter and denying a proof for the former.

The Hope. The strengthening suggested above would insert an extra check for when a "correlated flooding with mask" term (say LWE with correlated error) can be conjectured indistinguishable to a "i.i.d flooding with mask" term (say LWE) and would perform the replacement only if this appears safe. The extra check would fail for the attack scenarios discussed in the present work, such as the "malicious sampler" attacks as well as "pre-condition error is larger" attacks, cautioning about insecurity. While this extra check introduces new "flooding with mask" style conjectures, it captures more closely the subtleties in the noise distributions of these constructions and appears to admit a proof only for constructions that are secure.

Currently, the vulnerabilities of evasive LWE are still being discovered but our hope is that as we stabilize in our understanding of counter-examples against evasive LWE, we can find meaningful strengthening of the pre-condition so that the security of the scheme is better fitted with the assumption.

6.2 Contrived Functionality Attacks.

The attack by Branco et al. [BDJ+24][Sec 9] and that in Section 5.2 show that there exists a contrived "self-referential" functionality for which pseudorandom obfuscation or compact functional encryption satisfying simulation style security cannot exist. We believe this result is analogous to the impossibilities known for the random oracle model [CGH04] or VBB obfuscation [BGI+01] and can be handled using the same high level approach as in these settings, as discussed in Section 2. The pseudorandom functionalities that are useful for applications, such as computing blind garbled circuits or FE ciphertexts [AKY24a, AKY24c], are quite natural and do not fall prey to such attacks. We believe that the proof from evasive LWE for these functionalities provides strong evidence for real world security of the schemes, similar to proofs in the ROM.

We additionally remark that the incompressibility style arguments underlying these counter-examples do not apply in the *single challenge* setting. Translated into the evasive LWE assumption, single-challenge means that $\mathbf{S}$ is a vector and not a matrix. Hence, one principled way to avoid these counter-examples is to use evasive LWE in the single-challenge regime.

7 Compact Functional Encryption from Correlated Flooding (or Fixed-Bit Evasive LWE)

In this section, we study a new modification of evasive LWE, which we call *correlated flooding* (or *fixed-bit* evasive LWE[23]). Intuitively, the idea in evasive LWE is that if the term $\mathbf{SP} + \mathbf{E}'$ in the pre-condition can be proven pseudorandom over the entire space (given other terms), then the post-condition can be conjectured secure. In this section, we show, perhaps somewhat surprisingly, that if $\mathbf{SP} + \mathbf{E}'$ is pseudorandom not over the entire space but only over *half* the space, then it can be used to build full fledged FE for P.

We remark that the term "correlated flooding" is generic and meant to capture the intuition that a flooding term, carefully generated using a PRF so as to avoid problematic dependencies, can be conjectured to flood some leaky noise terms revealed during decryption. While fixed-bit evasive LWE is a more intuitive name (to us), we believe it is misleading to have the word "evasive" in the assumption since it explicitly allows the adversary to compute values in the zeroizing regime. The construction closely follows the outline of the construction of compact FE for pseudorandom functionalities by [AKY24a].

7.1 Correlated Flooding (or Fixed-Bit Evasive LWE) Assumption

Assumption 7.1 (Correlated Flooding). Let $n, m, t, n', q \in \mathbb{N}$ be parameters and λ be a security parameter. Let χ and χ' be parameters for Gaussian distributions. Let Samp be a PPT algorithm that outputs

$$\mathbf{S} \in \mathbb{Z}_q^{n' \times n}, \mathbf{P} \in \mathbb{Z}_q^{n \times t}, \mathsf{aux} \in \{0,1\}^*$$

on input 1^λ. We define the following advantage functions:

$$\mathsf{Adv}^{\mathrm{pre}}_{\mathcal{A}_0}(\lambda) \stackrel{\mathrm{def}}{=} \Pr\left[\mathcal{A}_0(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}) = 1\right] - \Pr\left[\mathcal{A}_0(\mathbf{B}, \mathbf{C}_0, \mathbf{T} + \mathbf{C}', \mathsf{aux}) = 1\right]$$

$$\mathsf{Adv}^{\mathrm{post}}_{\mathcal{A}_1}(\lambda) \stackrel{\mathrm{def}}{=} \Pr[\mathcal{A}_1(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{K}, \mathsf{aux}) = 1] - \Pr\left[\mathcal{A}_1(\mathbf{B}, \mathbf{C}_0, \mathbf{K}', \mathsf{aux}) = 1\right]$$

[23] As we describe next, the randomness in pre-condition is only over half the space, thus fixing a bit (MSB) to zero.

where $\mathbf{T} \in \mathbb{Z}_q^{n' \times t}$ is a matrix computed by an efficient deterministic algorithm Compute as $\mathbf{T} \stackrel{\text{def}}{=} \mathsf{Compute}(\mathsf{aux})$ and

$$
\begin{aligned}
&(\mathbf{S}, \mathbf{P}, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda), \mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{C}_0 \leftarrow \mathbb{Z}_q^{n' \times m}, \mathbf{C}' \leftarrow [-q/4, q/4]^{n' \times t} \\
&\mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\chi}^{n' \times m}, \mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\chi'}^{n' \times t} \\
&\mathbf{K} \leftarrow \mathbf{B}^{-1}(\mathbf{P}) \text{ with standard deviation } O(\sqrt{m \log(q)}), \\
&\mathbf{K}' \leftarrow \begin{bmatrix} \mathbf{B} \\ \mathbf{C}_0 \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{P} \\ \mathbf{T} + \mathbf{C}' \end{bmatrix} \right) \quad \text{with standard deviation } O(\sqrt{m \log(q)})
\end{aligned}
$$

We say that the *correlated flooding* assumption holds for a particular Samp if for every PPT adversary $\mathcal{A}_1$, there exists another PPT $\mathcal{A}_0$ and a polynomial $Q(\cdot)$ such that

$$\mathsf{Adv}^{\text{pre}}_{\mathcal{A}_0}(\lambda) \geq \mathsf{Adv}^{\text{post}}_{\mathcal{A}_1}(\lambda)/Q(\lambda) - \mathsf{negl}(\lambda).$$

Note that if each entry of $\mathbf{C}'$ is sampled from $\mathbb{Z}_q$, the above assumption corresponds to the evasive LWE assumption. We also note that when n' is large enough (say, $n' > m$), there is no $\mathbf{K}'$ satisfying the equation $\begin{bmatrix} \mathbf{B} \\ \mathbf{C}_0 \end{bmatrix} \mathbf{K}' = \begin{bmatrix} \mathbf{P} \\ \mathbf{T} + \mathbf{C}' \end{bmatrix}$. The assumption is defined only for small n'. In our case, we use the assumption only for the case of $n' = 1$. Indeed, for such small n', the attack from Section 5.3, which requires large n' no longer applies.

Adapting Lemma from ARYY23. Next, we adapt a lemma from [ARYY23] to Correlated Flooding assumption.

Lemma 7.2. Let $n, m, t, n', q \in \mathbb{N}$ be parameters and λ be a security parameter. Let χ and χ' be Gaussian parameters. Let Samp be a PPT algorithm that outputs

$$\mathbf{S} \in \mathbb{Z}_q^{n' \times n}, \mathsf{aux} = (\mathsf{aux}_1, \mathsf{aux}_2) \in \mathcal{S} \times \{0,1\}^* \text{ and } \mathbf{P} \in \mathbb{Z}_q^{n \times t}$$

for some set $\mathcal{S}$. Furthermore, we assume that there exists a public deterministic poly-time algorithm Reconstruct that allows to derive $\mathbf{P}$ from aux_2, i.e. $\mathbf{P} = \mathsf{Reconstruct}(\mathsf{aux}_2)$.

We introduce the following advantage functions:

$$
\begin{aligned}
\mathsf{Adv}^{\text{pre}'}_{\mathcal{A}}(\lambda) &\stackrel{\text{def}}{=} \Pr\left[\mathcal{A}(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{SP} + \mathbf{E}', \mathsf{aux}_1, \mathsf{aux}_2) = 1\right] \\
&\qquad - \Pr\left[\mathcal{A}(\mathbf{B}, \mathbf{C}_0, \mathbf{T} + \mathbf{C}', \mathbf{c}, \mathsf{aux}_2) = 1\right] \\
\mathsf{Adv}^{\text{post}'}_{\mathcal{A}}(\lambda) &\stackrel{\text{def}}{=} \Pr[\mathcal{A}(\mathbf{B}, \mathbf{SB} + \mathbf{E}, \mathbf{K}, \mathsf{aux}_1, \mathsf{aux}_2) = 1] - \Pr\left[\mathcal{A}(\mathbf{B}, \mathbf{C}_0, \mathbf{K}', \mathbf{c}, \mathsf{aux}_2) = 1\right]
\end{aligned}
$$

where $\mathbf{T} \in \mathbb{Z}_q^{n' \times t}$ is a matrix computed by an efficient deterministic algorithm Compute as $\mathbf{T} \stackrel{\text{def}}{=} \mathsf{Compute}(\mathbf{c}, \mathsf{aux}_2)$ and

$$
\begin{aligned}
&(\mathbf{S}, \mathsf{aux} = (\mathsf{aux}_1, \mathsf{aux}_2), \mathbf{P}) \leftarrow \mathsf{Samp}(1^\lambda), \mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \\
&\mathbf{C}_0 \leftarrow \mathbb{Z}_q^{n' \times m}, \mathbf{C}' \leftarrow [-q/4, q/4]^{n' \times t}, \mathbf{c} \leftarrow \mathcal{S}, \mathbf{E} \leftarrow \mathcal{D}_{\mathbb{Z},\chi}^{n' \times m}, \mathbf{E}' \leftarrow \mathcal{D}_{\mathbb{Z},\chi}^{n' \times t} \\
&\mathbf{K} \leftarrow \mathbf{B}^{-1}(\mathbf{P}) \text{ with standard deviation } O(\sqrt{m \log(q)}) \\
&\mathbf{K}' \leftarrow \begin{bmatrix} \mathbf{B} \\ \mathbf{C}_0 \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{P} \\ \mathbf{T} + \mathbf{C}' \end{bmatrix} \right) \qquad (39)
\end{aligned}
$$

Then, under the Correlated Flooding Assumption (cited above in Assumption 7.1) with respect to Samp, if $\mathsf{Adv}^{\text{pre}'}_{\mathcal{A}}(\lambda)$ is negligible for any PPT adversary $\mathcal{A}$, so is $\mathsf{Adv}^{\text{post}'}_{\mathcal{A}}(\lambda)$ for any PPT adversary $\mathcal{A}$.

Proof. The proof follows the same outline as Lemma 3.4 of [ARYY23] but we detail it for completeness. By the assumption, we have $(\mathbf{B}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{B}, \mathbf{C}_0, \mathbf{T}+\mathbf{C}', \mathbf{c}, \mathsf{aux}_2)$. This in particular implies $(\mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{c}, \mathsf{aux}_2)$ since we discard the terms making the task of distinguishing the distributions harder. This further implies $(\mathbf{B}, \mathbf{C}_0, \mathbf{T}+\mathbf{C}', \mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{B}, \mathbf{C}_0, \mathbf{T}+\mathbf{C}', \mathbf{c}, \mathsf{aux}_2)$ since adding terms $(\mathbf{B}, \mathbf{C}_0, \mathbf{T}+\mathbf{C}')$ where $\mathbf{B}, \mathbf{C}_0, \mathbf{C}'$ are uniformly random and $\mathbf{T}$ can be computed efficiently from the given terms, $\mathbf{T} = \mathsf{Compute}(\mathsf{aux}_1, \mathsf{aux}_2)$ on the L.H.S and $\mathbf{T} = \mathsf{Compute}(\mathbf{c}, \mathsf{aux}_2)$ on the R.H.S, does not make the task of distinguishing the distributions easier. We therefore establish $(\mathbf{B}, \mathbf{SB}+\mathbf{E}, \mathbf{SP}+\mathbf{E}', \mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{B}, \mathbf{C}_0, \mathbf{T}+\mathbf{C}', \mathsf{aux}_1, \mathsf{aux}_2)$. Applying the correlated flooding assumption with respect to Samp defined in the statement, we have $(\mathbf{B}, \mathbf{SB}+\mathbf{E}, \mathbf{K}, \mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{B}, \mathbf{C}_0, \mathbf{K}', \mathsf{aux}_1, \mathsf{aux}_2)$. To complete the proof, it suffices to show

$$(\mathbf{B}, \mathbf{C}_0, \mathbf{K}', \mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{B}, \mathbf{C}_0, \mathbf{K}', \mathbf{c}, \mathsf{aux}_2),$$

where $\mathbf{K}'$ is sampled as Equation (39) with $\mathbf{T}$ being $\mathbf{T} = \mathsf{Compute}(\mathsf{aux}_1, \mathsf{aux}_2)$ on the L.H.S and $\mathbf{T} = \mathsf{Compute}(\mathbf{c}, \mathsf{aux}_2)$ on the R.H.S. To show this, we recall that the precondition implies $(\mathsf{aux}_1, \mathsf{aux}_2) \approx_c (\mathbf{c}, \mathsf{aux}_2)$. We then observe that $(\mathbf{B}, \mathbf{C}_0, \mathbf{K}')$ can be sampled publicly given aux_2. This suffices to complete the proof, since having extra terms that can be computed efficiently from the given terms does not make the task of distinguishing the distributions easier. To sample $(\mathbf{B}, \mathbf{C}_0, \mathbf{K})$, we first sample $\begin{bmatrix}\mathbf{B}\\ \mathbf{C}_0\end{bmatrix}$ with the trapdoor as $\left(\begin{bmatrix}\mathbf{B}\\ \mathbf{C}_0\end{bmatrix}, \tau\right) \leftarrow \mathsf{TrapGen}(1^{n+n'}, 1^m, q)$, then we compute $\mathbf{P} = \mathsf{Reconstruct}(\mathsf{aux}_2)$ and $\mathbf{T}$ and finally sample $\mathbf{K}'$ by using the trapdoor. □

In Section 7.3.1 we show that if we restrict ourselves to the particular samplers we consider for the security proof of our FE in the following section (Section 7.2), fixed-bit evasive LWE implies evasive LWE.

New Attacks? Note that the original intuition for evasive LWE was that pseudorandomness of $\mathbf{SP}+\mathbf{E}'$ over the entire space will ensure that zeroizing attacks do not apply. However, as we saw in previous sections, zeroizing attacks can be developed in certain cases even for evasive LWE and one must apply counter-measures to ensure safety against these. Given the countermeasures, if one conjectures security of vanilla evasive LWE, then can the same countermeasures also provide evidence for security in the half-space regime?

We currently do not know any additional attack strategies on this variant of the assumption as compared to the standard evasive LWE assumption. We already studied countermeasures for attacks against evasive LWE in Section 6, here we examine other avenues of attack that have been studied in the literature and discuss why they do not seem to apply to our setting.

- *Attacks against Tensor Structure:* The work of Jain et al. (JLLS) [JLLS23] attacked the tensor structure which was used crucially in the construction of Devdas et al. [DQV+21]. In particular, JLLS showed that Kilian randomization on highly tensored matrices does not kill the tensor structure, and this structure can be exploited for attacks. This attack does not appear to apply to our setting since we do not rely on tensors.

- *Linearization and Sum-Of-Squares.* Linearization attacks, as the name suggests, are attacks where a system of high degree polynomial equations are linearized and then solved using standard techniques like Gaussian elimination. The sum-of-squares paradigm has been used to develop attacks [LV17, BBKK18, BHJ+19] against general expanding families of low-degree polynomials over the reals. These attacks do not seem to apply to the current setting because there aren't enough equations for the former class of attacks and the latter class of attacks requires low degree equations

over the reals, whereas our PRF computation does not suffer any degree restriction, since we do not use pairings.

- *Attack against Gay-Pass Scheme.* The Gay-Pass assumption [GP21] asserts that *if* an encryption scheme is CPA secure when the adversary has access to certain leakage on the encryption randomness (called "Shielded Randomness Leakage"), then additionally publishing an encrypted key cycle does not hurt security. Counterexamples developed against this conjecture [HJL21] do not apply to our setting since the specific structure of their assumption is very different from ours.

7.2 Construction of Compact FE

In this section we provide our construction of functional encryption for function family $\mathcal{F}_{\mathrm{L}(\lambda),\ell(\lambda),d(\lambda)} = \{f : \{0,1\}^{\mathrm{L}} \to \{0,1\}^{1\times\ell}\}$, where the depth of a function $f \in \mathcal{F}$ is at most $d(\lambda) = \mathrm{poly}(\lambda)$.

Ingredients. Below, we list the ingredients for our construction.

1. A pseudorandom function $\mathsf{PRF} : \{0,1\}^{\lambda} \times \{0,1\}^{\lambda} \to [-q/4 + B, q/4 - B]^{1\times\ell}$ that can be evaluated by a circuit of depth at most $\mathsf{dep}(\lambda) = \mathrm{poly}(\lambda)$. Here B is chosen to be superpolynomially smaller than $q/4$. We note that for our choice of B the statistical distance between the uniform distribution over $[-q/4, q/4]$ and $[-q/4 + B, q/4 - B]$ is negligible.

$\mathsf{Setup}(1^{\lambda}, 1^{\mathrm{L}}) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm does the following.

- Set $\mathrm{L_X} = m(\lambda + \mathrm{L})(n+1)\lceil \log q \rceil$, sample $\mathbf{A}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(n+1)\times(\mathrm{L_X}+1)m}$ and $(\mathbf{B}, \mathbf{B}_{\tau}^{-1}) \leftarrow \mathsf{TrapGen}(1^{n+1}, 1^{mw}, q)$, where $w \in O(\log q)$.
- Fix a constant $C \in \mathbb{Z}$ such that C divides q, and satisfies the constraints given by parameter settings provided later.
- Output $\mathsf{mpk} := (\mathbf{A}_{\mathsf{att}}, \mathbf{B}, C)$[24] and $\mathsf{msk} := \mathbf{B}_{\tau}^{-1}$.

$\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{sk}_f$. The key generation algorithm does the following.

- Sample $\mathbf{r} \leftarrow \{0,1\}^{\lambda}$ and define function $\mathrm{F} = \mathrm{F}[f, \mathbf{r}]$ with $f, \mathbf{r}$ hardwired as follows.
  On input $(\mathbf{x}, \mathsf{sd})$, compute and output $f(\mathbf{x})\lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}) \in \mathbb{Z}_q^{1\times\ell}$.
  Using the fact that the PRF computation and $f(\mathbf{x})$ can be computed by a circuit of depth at most $\mathsf{dep}(\lambda) = \mathrm{poly}(\lambda)$, the function F can be computed by a circuit of depth $d = \mathrm{poly}(\mathsf{dep})$.
- Define functions $\mathrm{F}_{\mathsf{high}}$ and $\mathrm{F}_{\mathsf{low}}$ such that $\mathrm{F}(\mathbf{x}, \mathsf{sd}) = C \cdot \mathrm{F}_{\mathsf{high}}(\mathbf{x}, \mathsf{sd}) + \mathrm{F}_{\mathsf{low}}(\mathbf{x}, \mathsf{sd})$. Observe that both $C \cdot \mathrm{F}_{\mathsf{high}}$ and $\mathrm{F}_{\mathsf{low}}$ can also be computed by a circuit of depth $d = \mathrm{poly}(\mathsf{dep})$.
- Define the homomorphic evaluation circuit $\mathsf{VEval}_{\mathrm{F}_{\mathsf{high}}} = \mathrm{MakeVEvalCkt}(n, m, q, C \cdot \mathrm{F}_{\mathsf{high}})$ and $\mathsf{VEval}_{\mathrm{F}_{\mathsf{low}}} = \mathrm{MakeVEvalCkt}(n, m, q, C \cdot \mathrm{F}_{\mathsf{low}})$. From Lemma 3.15, the depth of both $\mathsf{VEval}_{\mathrm{F}_{\mathsf{high}}}$ and $\mathsf{VEval}_{\mathrm{F}_{\mathsf{low}}}$ is $dO(\log m \log\log q) + O(\log^2 \log q)$.
- Compute $\mathbf{H}_{\mathbf{A}_{\mathsf{att}}}^{\mathrm{F}_{\mathsf{high}}} = \mathsf{MEvalC}(\mathbf{A}_{\mathsf{att}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{high}}}) \in \mathbb{Z}_q^{(\mathrm{L_X}+1)m\times\ell}$,
  $\mathbf{H}_{\mathbf{A}_{\mathsf{att}}}^{\mathrm{F}_{\mathsf{low}}} = \mathsf{MEvalC}(\mathbf{A}_{\mathsf{att}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{low}}}) \in \mathbb{Z}_q^{(\mathrm{L_X}+1)m\times\ell}$.
- Compute $\mathbf{A}_{\mathrm{F}_{\mathsf{high}}} = \mathbf{A}_{\mathsf{att}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}}}^{\mathrm{F}_{\mathsf{high}}}$ and $\mathbf{A}_{\mathrm{F}_{\mathsf{low}}} = \mathbf{A}_{\mathsf{att}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}}}^{\mathrm{F}_{\mathsf{low}}}$.
- Compute $\mathbf{A}_{\mathrm{F}} = C \cdot \left\lfloor \frac{\mathbf{A}_{\mathrm{F}_{\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{A}_{\mathrm{F}_{\mathsf{low}}}}{C} \right\rceil$ and sample $\mathbf{K} \leftarrow \mathbf{B}_{\tau}^{-1}(\mathbf{A}_{\mathrm{F}})$.

[24] All the algorithms take mpk implicitly.

– Output $\mathsf{sk}_f = (\mathbf{K}, \mathbf{r})$.

$\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}) \to \mathsf{ct}$. The encryption algorithm does the following.

– Sample $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{s}}}$ and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.
– Sample $\mathbf{e}_{\mathbf{B}} \leftarrow \mathcal{D}^{mw}_{\mathbb{Z},\sigma_{\mathbf{B}}}$ and compute $\mathbf{c}^\intercal_{\mathbf{B}} := \mathbf{s}^\intercal\mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B}}$.
– Sample $\mathsf{sd} \leftarrow \{0,1\}^\lambda$, $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{R}_i \leftarrow \{0,1\}^{m\times m}$ for all $1 \le i \le (\lambda + \mathrm{L})$ and compute a GSW encryption as follows.

$$\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^\intercal\bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \end{pmatrix}, \qquad \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}, \mathsf{sd}) \otimes \mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})}$$

where $\mathbf{R} = (\mathbf{R}_1, \ldots, \mathbf{R}_{(\lambda+\mathrm{L})})$. Let $\mathrm{L}_{\mathrm{X}} = m(\lambda+\mathrm{L})(n+1)\lceil \log q \rceil$ be the bit length of $\mathbf{X}$.
– Compute a BGG^+ encoding as follows.

$$\mathbf{e}_{\mathsf{att}} \leftarrow \mathcal{D}^{(\mathrm{L}_{\mathrm{X}}+1)m}_{\mathbb{Z},\sigma_{\mathsf{att}}}, \qquad \mathbf{c}^\intercal_{\mathsf{att}} := \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}}$$

– Output $\mathsf{ct} = (\mathbf{c}_{\mathbf{B}}, \mathbf{c}_{\mathsf{att}}, \mathbf{X})$.

$\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}) \to \mathbf{y}$. The decryption algorithm does the following.

– Parse $\mathsf{sk}_f = (\mathbf{K}, \mathbf{r})$ and $\mathsf{ct} = (\mathbf{c}_{\mathbf{B}}, \mathbf{c}_{\mathsf{att}}, \mathbf{X})$.
– Compute $\mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} = \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{att}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{high}}}, \mathbf{X})$ and $\mathbf{H}^{\mathrm{F}_{\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} = \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{att}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{low}}}, \mathbf{X})$.
– Compute $\mathbf{z} := \mathbf{c}^\intercal_{\mathbf{B}} \cdot \mathbf{K} - \left(C \cdot \left\lfloor \frac{\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rfloor \right)$.
– For $i \in [\ell]$, set $y_i = 0$, if $z_i \in [-q/4, q/4)$ and $y_i = 1$ otherwise, where z_i is the i-th bit of $\mathbf{z}$.
– Output $\mathbf{y} = (y_1, \ldots y_\ell)$.

Parameters. We set our parameters as follows.

$$\beta = 2^{O(\mathsf{dep}\cdot\log^3\lambda)},\ q = 2^{10\lambda}\beta,\ n = \mathrm{poly}(\lambda, \mathsf{dep}),\ m = O(n\log q),\ \tau = O\left(\sqrt{(n+1)\log q}\right),$$
$$C = 2^{4\lambda}\beta,\ B = 2^{9\lambda}\beta,\ \sigma_{\mathsf{fhe}} = \sigma_{\mathsf{att}} = \sigma_{\mathbf{s}} = \sigma = 2^{2\lambda},\ \sigma_{\mathbf{B}} = 2^{8\lambda}\beta,\ \sigma_1 = 2^{7\lambda}\beta\lambda^{\omega(1)}.$$

Efficiency. Using the above set parameters, we have

$$|\mathsf{mpk}| = \mathrm{L}\cdot\mathrm{poly}(\mathsf{dep}, \lambda),\ |\mathsf{sk}_f| = \ell\cdot\mathrm{poly}(\mathsf{dep}, \lambda),\ |\mathsf{ct}| = \mathrm{L}\cdot\mathrm{poly}(\mathsf{dep}, \lambda).$$

7.2.1 Correctness.

We analyse the correctness of our scheme below.

– First, we note that

$$\begin{aligned}
\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} &= (\mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}})\mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= \mathbf{s}^\intercal\mathbf{A}_{\mathsf{att}}\mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}}} - \mathbf{s}^\intercal\mathsf{VEval}_{\mathrm{F}_{\mathsf{high}}}(\mathsf{bits}(\mathbf{X})) + \mathbf{e}^\intercal_{\mathsf{att}}\mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= \mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_{\mathsf{high}}} - C\cdot\mathrm{F}_{\mathsf{high}}(\mathbf{x}, \mathsf{sd}) + \mathbf{e}^\intercal_{\mathsf{fhe}}\mathbf{R}_{\mathrm{F}_{\mathsf{high}}} + \mathbf{e}^\intercal_{\mathsf{att}}\mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}} \\
&= \mathbf{s}^\intercal\mathbf{A}_{\mathrm{F}_{\mathsf{high}}} - C\cdot\mathrm{F}_{\mathsf{high}}(\mathbf{x}, \mathsf{sd}) + \mathbf{e}^\intercal_{\mathrm{F}_{\mathsf{high}}}.
\end{aligned}$$

where $\mathsf{VEval}_{\mathrm{F}_{\mathsf{high}}}(\mathsf{bits}(\mathbf{X})) = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathrm{F}_{\mathsf{high}}} - \begin{pmatrix} 0^{n\times\ell} \\ \mathrm{F}_{\mathsf{high}}(\mathbf{x}, \mathsf{sd}) \end{pmatrix}$ and $\mathbf{e}^\intercal_{\mathrm{F}_{\mathsf{high}}} = \mathbf{e}^\intercal_{\mathsf{fhe}}\mathbf{R}_{\mathrm{F}_{\mathsf{high}}} + \mathbf{e}^\intercal_{\mathsf{att}}\mathbf{H}^{\mathrm{F}_{\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}$.

– Similarly, $\mathbf{c}_{\mathsf{att}}^{\intercal} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{\mathsf{low}}} = \mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{low}}} - C \cdot \mathrm{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) + \mathbf{e}_{\mathrm{F}_{\mathsf{low}}}^{\intercal}$,
where $\mathsf{VEval}_{\mathrm{F}_{\mathsf{low}}}(\mathsf{bits}(\mathbf{X})) = \mathbf{A}_{\mathsf{fhe}}\mathbf{R}_{\mathrm{F}_{\mathsf{low}}} - \begin{pmatrix} 0^{n\times\ell} \\ \mathrm{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) \end{pmatrix}$ and $\mathbf{e}_{\mathrm{F}_{\mathsf{low}}}^{\intercal} = \mathbf{e}_{\mathsf{fhe}}^{\intercal}\mathbf{R}_{\mathrm{F}_{\mathsf{low}}} + \mathbf{e}_{\mathsf{att}}^{\intercal}\mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{\mathsf{low}}}$.

– Following analyses hold for both $b = \mathsf{high}$ and $b = \mathsf{low}$.
By Lemma 3.15,

$$\begin{aligned}\left\|\mathbf{R}_{\mathrm{F}_b}^{\intercal}\right\| &\leq (m+2)^d \lceil \log q \rceil \cdot \max_{i\in[\lambda+\mathrm{L}]} \left\|\mathbf{R}_i^{\intercal}\right\| \\ &\leq (m+2)^d \lceil \log q \rceil \cdot m \\ &\leq (m+2)^{d+1} O(\log q) \leq \beta.\end{aligned}$$

and using the depth bound from Section 3.7, we have,

$$\left\|\left(\mathrm{H}_{\mathbf{A}_{\mathsf{att}}}^{\mathrm{F}_b}\right)^{\intercal}\right\| \leq (m+2)^{d_{\mathsf{VEval}_{\mathrm{F}_b}}} \lceil \log q \rceil \leq 2^{d\cdot O(\log\lambda)} \leq \beta.$$

where $d_{\mathsf{VEval}_{\mathrm{F}_b}}$ denotes the depth of the circuit $\mathsf{VEval}_{\mathrm{F}_b}$. Thus $\|\mathbf{e}_{\mathrm{F}_b}\| \leq 2^{2\lambda+1}\sqrt{\lambda}\beta \leq 2^{3\lambda}\beta$

– Based on above, we have ,

$$\begin{aligned} C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\intercal} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{\mathsf{high}}}}{C} \right\rfloor &= C \cdot \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{high}}} - C \cdot \mathrm{F}_{\mathsf{high}}(\mathbf{x},\mathsf{sd}) + \mathbf{e}_{\mathrm{F}_{\mathsf{high}}}^{\intercal}}{C} \right\rfloor \\ &= C \cdot \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{high}}} + \mathbf{e}_{\mathrm{F}_{\mathsf{high}}}^{\intercal}}{C} \right\rfloor - C \cdot \mathrm{F}_{\mathsf{high}}(\mathbf{x},\mathsf{sd}) \\ &= C \cdot \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{high}}}}{C} \right\rfloor - C \cdot \mathrm{F}_{\mathsf{high}}(\mathbf{x},\mathsf{sd}) + C \cdot \tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal}, \\ &\quad \text{where } \|\tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal}\| \leq 1, \text{ since } \left\|\mathbf{e}_{\mathrm{F}_{\mathsf{high}}}\right\| \leq 2^{3\lambda}\beta < C \end{aligned} \tag{40}$$

By similar analysis,

$$\begin{aligned} \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\intercal} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{\mathsf{low}}}}{C} \right\rfloor &= \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{low}}} - C \cdot \mathrm{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) + \mathbf{e}_{\mathrm{F}_{\mathsf{low}}}^{\intercal}}{C} \right\rfloor \\ &= \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{low}}} + \mathbf{e}_{\mathrm{F}_{\mathsf{low}}}^{\intercal}}{C} \right\rfloor - \mathrm{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) \\ &= \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathrm{F}_{\mathsf{low}}}}{C} \right\rfloor - \mathrm{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) + \tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal}, \\ &\quad \text{where } \|\tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal}\| \leq 1, \text{ since } \|\mathbf{e}_{\mathrm{F}_{\mathsf{low}}}\| \leq 2^{3\lambda}\beta < C \end{aligned} \tag{41}$$

– Using the above, the Step 7.2 of decryption outputs

$$\begin{aligned}
\mathbf{z} &= \mathbf{c}_{\mathbf{B}}^{\intercal} \cdot \mathbf{K} - \left(C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\intercal} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},X}^{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\intercal} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},X}^{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right) \qquad (42) \\
&= \mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}} + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K} - \left(C \cdot \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil - C \cdot \mathsf{F}_{\mathsf{high}}(\mathbf{x},\mathsf{sd}) + \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil - \mathsf{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) \right) - C \cdot \tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal} + \tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal} \\
&= \mathbf{s}^{\intercal} \left(C \cdot \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right) + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K} - \left(C \cdot \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil + \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right) \\
&\quad + C \cdot \mathsf{F}_{\mathsf{high}}(\mathbf{x},\mathsf{sd}) + \mathsf{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd}) + C \cdot \mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} + \mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} - C \cdot \tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal} + \tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal} \\
&= \mathsf{F}(\mathbf{x},\mathsf{sd}) + C \cdot \mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} + \mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} - C \cdot \tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal} + \tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal} + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K} \\
&\qquad\qquad\qquad\qquad\qquad\qquad (\text{since } \mathsf{F}(\mathbf{x},\mathsf{sd}) = C \cdot \mathsf{F}_{\mathsf{high}}(\mathbf{x},\mathsf{sd}) + \mathsf{F}_{\mathsf{low}}(\mathbf{x},\mathsf{sd})) \\
&= f(\mathbf{x}) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd},\mathbf{r}) + C \cdot \mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} + \mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} - C \cdot \tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal} + \tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal} + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}
\end{aligned}$$

In the above, $\mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} = \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil - \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil$ and $\mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} = \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil - \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil$ are errors due to rounding. Let us analyze the sizes of these errors.

$$\begin{aligned}
\mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} &= \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil - \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil \\
&= \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil - \left\lfloor \mathbf{s}^{\intercal} \left(\left(\frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} - \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil \right) + \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil \right) \right\rfloor \\
&= \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil - \left\lfloor \mathbf{s}^{\intercal} \left(\frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} - \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil \right) \right\rfloor - \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil \\
&= - \left\lfloor \mathbf{s}^{\intercal} \underbrace{\left(\frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} - \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{high}}}}{C} \right\rceil \right)}_{<1} \right\rfloor \\
\implies \left\| \mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} \right\| &\leq n \cdot \|\mathbf{s}\|
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} &= \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil - \left\lfloor \frac{\mathbf{s}^{\intercal}\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \\
&= \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil - \left\lfloor \mathbf{s}^{\intercal} \left(\left(\frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} - \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right) + \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right) \right\rfloor \\
&= \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil - \left\lfloor \mathbf{s}^{\intercal} \left(\frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} - \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right) \right\rfloor - \mathbf{s}^{\intercal} \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \\
&= - \left\lfloor \mathbf{s}^{\intercal} \underbrace{\left(\frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} - \left\lfloor \frac{\mathbf{A}_{\mathsf{F}_{\mathsf{low}}}}{C} \right\rceil \right)}_{<1} \right\rfloor \\
\implies \left\| \mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} \right\| &\leq n \cdot \|\mathbf{s}\|
\end{aligned}$$

– Thus, from our parameter setting, we have $\left\| \mathsf{PRF}(\mathsf{sd},\mathbf{r}) + C \cdot \mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} + \mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} - C \cdot \tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal} + \tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal} + \mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K} \right\| \leq \|\mathsf{PRF}(\mathsf{sd},\mathbf{r})\| + C \left\| \mathbf{e}_{\mathbf{s},\mathsf{high}}^{\intercal} \right\| + \left\| \mathbf{e}_{\mathbf{s},\mathsf{low}}^{\intercal} \right\| + C\|\tilde{\mathbf{e}}_{\mathsf{h}}^{\intercal}\| + \|\tilde{\mathbf{e}}_{\mathsf{l}}^{\intercal}\| + \|\mathbf{e}_{\mathbf{B}}^{\intercal}\mathbf{K}\| < (q/4 - B) + B < q/4$. In par-

ticular, $C\left\|\mathbf{e}_{\mathbf{s},\mathsf{high}}^{\mathsf{T}}\right\| + \left\|\mathbf{e}_{\mathbf{s},\mathsf{low}}^{\mathsf{T}}\right\| + C\|\tilde{\mathbf{e}}_{\mathsf{h}}^{\mathsf{T}}\| + \|\tilde{\mathbf{e}}_{\mathsf{l}}^{\mathsf{T}}\| + \|\mathbf{e}_{\mathbf{B}}^{\mathsf{T}}\mathbf{K}\| \leq Cn\|\mathbf{s}\| + n\|\mathbf{s}\| + C + 1 + \lambda\sigma_{\mathbf{B}}\tau mw = (C+1)(n\|\mathbf{s}\|+1) + \lambda\sigma_{\mathbf{B}}\tau mw \leq 2^{8\lambda+O(\log\lambda)}\beta < B$. Hence, from Step 4 of decryption we have that Dec outputs $f(\mathbf{x})$ correctly with probability 1.

7.3 Proof of Security of Compact FE

Theorem 7.3. Suppose correlated flooding assumption (Assumption 7.1) for the sampler defined in Figure 1 and LWE (Assumption 3.11) holds. Then there exists a FE scheme satisfying VerSel-INDr security.

Proof. Suppose the adversary $\mathcal{A}$ with randomness $\mathsf{coins}_{\mathcal{A}}$ queries for challenge inputs $\mathbf{x}_0, \mathbf{x}_1$ and functions $f_1, \ldots, f_Q$. To prove the very selective security as per Definition 3.2, we want to show that

$$D_0 := \begin{pmatrix} \mathsf{aux}_{\mathcal{A}},\ \mathsf{mpk} = (\mathbf{A}_{\mathsf{att}}, \mathbf{B}, C),\ \ \mathbf{c}_{\mathbf{B}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\mathbf{B} + \mathbf{e}_{\mathbf{B}}^{\mathsf{T}}, \\ \mathbf{c}_{\mathsf{att}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^{\mathsf{T}}, \\ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G}, \{\mathbf{K}_i, \mathbf{r}_i\}_{i\in[Q]} \end{pmatrix} \approx_c D_1 := \begin{pmatrix} \mathsf{aux}_{\mathcal{A}},\ \mathsf{mpk} = (\mathbf{A}_{\mathsf{att}}, \mathbf{B}, C),\ \ \mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw}, \\ \mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L_X}+1)m} \\ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})}, \{\mathbf{K}'_i, \mathbf{r}_i\}_{i\in[Q]} \end{pmatrix} \tag{43}$$

where b is the challenge bit chosen by the challenger and $\mathsf{aux}_{\mathcal{A}} = (f_1, \ldots, f_Q, \mathbf{x}_0, \mathbf{x}_1, \mathsf{coins}_{\mathcal{A}}, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}})$. On the R.H.S, $\mathbf{K}'_i$ is generated as

$$\mathbf{K}'_i \leftarrow \begin{bmatrix} \mathbf{B} \\ \mathbf{c}_{\mathbf{B}}^{\mathsf{T}} \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{A}_{\mathrm{F}_i} \\ \mathbf{t}_i^{\mathsf{T}} + \mathbf{c}_i'^{\mathsf{T}} \end{bmatrix} \right),\ \mathbf{t}_i^{\mathsf{T}} = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil,\ \mathbf{c}'_i \leftarrow [-q/4, q/4]^{\ell}.$$

Here, for $i \in [Q]$, we have $\mathbf{r}_i \leftarrow \{0,1\}^{\lambda}$, $\mathrm{F}_i = \mathrm{F}[f_i, \mathbf{r}_i]$ and $\mathbf{A}_{\mathrm{F}_i} = C \cdot \left\lfloor \frac{\mathbf{A}_{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{A}_{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rceil$ as defined in the construction. Showing Equation (43) suffices to prove the theorem, as the distribution on the right-hand side is independent of b, which can be seen by observing that $f_i(\mathbf{x}_0) = f_i(\mathbf{x}_1)$ due to the constraints imposed on the adversary.
We prove the security in two steps.

1. **Step 1.** We first show that to prove Equation (43), it suffices to prove

$$\begin{pmatrix} \mathsf{aux},\ \mathbf{B},\ \ \mathbf{c}_{\mathbf{B}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\mathbf{B} + \mathbf{e}_{\mathbf{B}}^{\mathsf{T}},\ \ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G}, \\ \mathbf{c}_{\mathsf{att}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^{\mathsf{T}},\ \ \{\mathbf{c}_{1,i}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\mathbf{A}_{\mathrm{F}_i} + \mathbf{e}_{1,i}^{\mathsf{T}}\}_{i\in[Q]} \end{pmatrix} \tag{44}$$

$$\approx_c$$

$$\begin{pmatrix} \mathsf{aux},\ \mathbf{B},\ \ \mathbf{c}_{\mathbf{B}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{mw},\ \ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})}, \\ \mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \leftarrow \mathbb{Z}_q^{1\times(\mathrm{L_X}+1)m},\ \ \{\mathbf{c}_{1,i}^{\mathsf{T}} = \underbrace{C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil}_{=\mathbf{t}_i^{\mathsf{T}}} + (\mathbf{c}'_i)^{\mathsf{T}}\}_{i\in[Q]} \end{pmatrix} \tag{45}$$

   where $\mathsf{aux} = (f_1, \ldots, f_Q, \mathbf{x}_0, \mathbf{x}_1, \mathsf{coins}_{\mathcal{A}}, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}}, C)$ and $\mathbf{e}_{1,i} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_1}^{\ell}$.

2. **Step 2.** We prove Equation (44) $\approx_c$ Equation (45).

$$\mathsf{Samp}(1^\lambda, \mathsf{coins}^{\mathsf{priv}}_{\mathsf{Samp}} = (\mathsf{sd}, \mathbf{R}, b))$$

Do the following:

- Invoke the adversary $\mathcal{A}$ with $\mathsf{coins}_{\mathcal{A}}$ to obtain $f_1, \ldots, f_Q, \mathbf{x}_0, \mathbf{x}_1$.
- Fix a constant C as defined in the Setup algorithm.
- Sample $\bar{\mathbf{s}} \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{s}}}$, and set $\mathbf{s} = (\bar{\mathbf{s}}^\intercal, -1)^\intercal$.
- Sample $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{A}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(n+1)\times(\mathrm{L_X}+1)m}$,
- Sample $\mathbf{r}_1, \ldots, \mathbf{r}_Q \leftarrow \{0,1\}^\lambda$,
- Sample $\mathbf{e}_{\mathsf{fhe}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{e}_{\mathsf{att}} \leftarrow \mathcal{D}^{((\mathrm{L_X}+1)m)}_{\mathbb{Z},\sigma_{\mathsf{att}}}$,
- Compute $\mathbf{X} = \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{s}}^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe}} \end{pmatrix} \mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G}$, $\mathbf{c}^\intercal_{\mathsf{att}} = \mathbf{s}^\intercal(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{att}}$
- Define $\{\mathrm{F}_i\}_{i\in[Q]}$ and compute $\mathbf{A}_{\mathrm{F}_1}, \ldots, \mathbf{A}_{\mathrm{F}_Q}$ as defined in KeyGen algorithm.

Set $\mathbf{S} = \mathbf{s}^\intercal$

$\mathsf{aux}_1 = (\mathbf{X}, \mathbf{c}^\intercal_{\mathsf{att}})$

$\mathsf{aux}_2 = (f_1, \ldots, f_Q, \mathbf{x}_0, \mathbf{x}_1, \mathsf{coins}_{\mathcal{A}}, \mathbf{r}_1, \ldots, \mathbf{r}_Q, \mathbf{A}_{\mathsf{att}}, C)$

$\mathbf{P} = [\mathbf{A}_{\mathrm{F}_1} || \ldots || \mathbf{A}_{\mathrm{F}_Q}]$

$\mathsf{Compute}(\mathsf{aux}) = \mathbf{T} = [\mathbf{t}^\intercal_1 \| \cdots \| \mathbf{t}^\intercal_Q]$, where for all $i \in [Q]$,

$$\mathbf{t}^\intercal_i = C \cdot \left\lfloor \frac{\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rfloor + f_i(\mathbf{x}_b)\, \lfloor q/2 \rceil$$

Figure 1: Description of the Sampler.

Step 1. We invoke correlated flooding assumption (Lemma 7.2) assumption for a matrix $\mathbf{B}$ with the private coin sampler Samp with $\mathsf{coins}^{\mathsf{priv}}_{\mathsf{Samp}} = (\mathsf{sd}, \mathbf{R}, b)$ for the L.H.S of Equation (43). The sampler Samp on input 1^λ outputs $(\mathbf{S}, \mathbf{P}, \mathsf{aux} = (\mathsf{aux}_1, \mathsf{aux}_2))$ defined as in Figure 1.

By applying correlated flooding assumption w.r.t Samp, it suffices to show Equation (44) $\approx_c$ Equation (45) to prove Equation (43).

Step 2. Here, we prove Equation (44) $\approx_c$ Equation (45) by considering the following sequence of hybrids.

Hyb_0. This is the distribution as specified in Equation (44).

Hyb_1. This hybrid is same as Hyb_0, except that we abort the security game and output $\perp$ if the set $\{\mathbf{r}_i\}_{i\in[Q]}$ contains a collision. For any i and j with $i \neq j$, we have $\mathbf{r}_i = \mathbf{r}_j$ with probability $2^{-\lambda}$. By the union bound over all combinations of i and j, the probability that the collision occurs can be bounded by $Q^2/2^\lambda$, which is negligible.

Hyb_2. This hybrid is same as Hyb_1, except we compute

$$\mathbf{c}^\intercal_{1,i} = C \cdot \left\lfloor \frac{\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}^\intercal_{\mathsf{att}} \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rfloor + f_i(\mathbf{x}_b)\, \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}^\intercal_{1,i}.$$

We claim that Hyb_1 and Hyb_2 are statistically indistinguishable. To see this, note that:

– We have

$$
\begin{aligned}
& C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor \\
& = C \cdot \left\lfloor \frac{\mathbf{s}^{\mathsf{T}} \mathbf{A}_{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor - C \cdot \mathrm{F}_{i,\mathsf{high}}(\mathbf{x}_b, \mathsf{sd}) + C \cdot \tilde{\mathbf{e}}_{i,\mathsf{h}}^{\mathsf{T}} + \left\lfloor \frac{\mathbf{s}^{\mathsf{T}} \mathbf{A}_{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor - \mathrm{F}_{i,\mathsf{low}}(\mathbf{x}_b, \mathsf{sd}) + \tilde{\mathbf{e}}_{i,\mathsf{l}}^{\mathsf{T}}, \quad \text{(from (40) and (41))} \\
& = \mathbf{s}^{\mathsf{T}} C \cdot \left\lfloor \frac{\mathbf{A}_{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor + \mathbf{s}^{\mathsf{T}} \left\lfloor \frac{\mathbf{A}_{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor - \mathrm{F}_i(\mathbf{x}_b, \mathsf{sd}) + \mathbf{e}_i^{\mathsf{T}}, \quad \text{(from (42))} \\
& = \mathbf{s}^{\mathsf{T}} \mathbf{A}_{\mathrm{F}_i} - f_i(\mathbf{x}_b) - \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_i^{\mathsf{T}}
\end{aligned}
$$

In the above, $\mathbf{e}_i = C \cdot \mathbf{e}_{i,\mathbf{s},\mathsf{high}} + \mathbf{e}_{i,\mathbf{s},\mathsf{low}} + C \cdot \tilde{\mathbf{e}}_{i,\mathsf{h}}^{\mathsf{T}} + \tilde{\mathbf{e}}_{i,\mathsf{l}}^{\mathsf{T}}$, where the error components on R.H.S. are as defined in the correctness.

This implies, $\mathbf{s}^{\mathsf{T}} \mathbf{A}_{\mathrm{F}_i} = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor + f_i(\mathbf{x}_b) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) - \mathbf{e}_i^{\mathsf{T}}$, where $\|\mathbf{e}_i^{\mathsf{T}}\| \leq 2^{6\lambda + O(\log \lambda)} \beta$.

– Thus,

$$
\begin{aligned}
(\text{in } \mathsf{Hyb}_1) \quad \mathbf{c}_{1,i}^{\mathsf{T}} &= \mathbf{s}^{\mathsf{T}} \mathbf{A}_{\mathrm{F}_i} + \mathbf{e}_{1,i}^{\mathsf{T}} \\
&= C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor + f_i(\mathbf{x}_b) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) - \mathbf{e}_i^{\mathsf{T}} + \mathbf{e}_{1,i}^{\mathsf{T}}. \\
(\text{in } \mathsf{Hyb}_2) \quad \mathbf{c}_{1,i}^{\mathsf{T}} &= C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor + f_i(\mathbf{x}_b) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{1,i}^{\mathsf{T}}.
\end{aligned}
$$

– The statistical indistinguishability then follows by observing that $\mathbf{e}_{1,i}^{\mathsf{T}} \approx_s -\mathbf{e}_i^{\mathsf{T}} + \mathbf{e}_{1,i}^{\mathsf{T}}$ by noise flooding (Lemma 3.9) since $\|\mathbf{e}_i\| \leq 2^{7\lambda}\beta$ which gets flooded by $\mathbf{e}_{1,i} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_1}$, where $\sigma_1 = 2^{7\lambda}\beta\lambda^{\omega(1)}$ for our parameter setting.

It suffices to show that the following distribution is indistinguishable from Equation (45)

$$
\left(\begin{array}{c}
\mathsf{aux},\ \mathbf{B},\ \ \mathbf{c}_{\mathbf{B}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\mathbf{B} + \mathbf{e}_{\mathbf{B}}^{\mathsf{T}},\ \ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G}, \\
\\
\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}(\mathbf{A}_{\mathsf{att}} - (1, \mathsf{bits}(\mathbf{X})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{att}}^{\mathsf{T}}, \\
\\
\left\{ \mathbf{c}_{1,i}^{\mathsf{T}} = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^{\mathsf{T}} \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rfloor + f_i(\mathbf{x}_b) \lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{1,i}^{\mathsf{T}} \right\}_{i \in [Q]}
\end{array} \right)
$$

Hyb_3. This hybrid is same as Hyb_2 except we sample $\mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw}$, $\mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L}_\mathbf{X}+1)m}$ and $\mathbf{A}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$, where $\mathbf{A}_{\mathsf{fhe}}$ is the fhe public key used to compute $\mathbf{X}$. We have $\mathsf{Hyb}_2 \approx_c \mathsf{Hyb}_3$ using LWE. We show that if there exists an adversary $\mathcal{A}$ who can distinguish between the two hybrids with non-negligible advantage, then there is a reduction $\mathcal{B}$ that breaks LWE security with non-negligible advantage. The reduction is as follows.

1. The LWE challenger sends $\mathbf{A}_{\mathsf{LWE}} \in \mathbb{Z}_q^{n \times (mw+m+(\mathrm{L}_\mathbf{X}+1)m)}$ and $\mathbf{b} \in \mathbb{Z}_q^{mw+m+(\mathrm{L}_\mathbf{X}+1)m}$ to $\mathcal{B}$.
2. $\mathcal{B}$ parses $\mathbf{A}_{\mathsf{LWE}} = (\mathbf{B}',\ \bar{\mathbf{A}}_{\mathsf{fhe}},\ \mathbf{A}'_{\mathsf{att}})$, where $\mathbf{B}' \in \mathbb{Z}_q^{n \times mw}$, $\bar{\mathbf{A}}_{\mathsf{fhe}} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{A}'_{\mathsf{att}} \in \mathbb{Z}_q^{n \times (\mathrm{L}_\mathbf{X}+1)m}$ and $\mathbf{b}^{\mathsf{T}} = (\mathbf{b}_{\mathbf{B}}^{\mathsf{T}},\ \mathbf{b}_{\mathsf{fhe}}^{\mathsf{T}},\ \mathbf{b}_{\mathsf{att}}^{\mathsf{T}})$, and does the following.

– Samples $\underline{\mathbf{b}} \leftarrow \mathbb{Z}_q^{mw}$ and sets $\mathbf{c}_{\mathbf{B}}^\intercal := \mathbf{b}_{\mathbf{B}}^\intercal - \underline{\mathbf{b}}^\intercal$.

– Sets $\mathbf{A}_{\mathsf{fhe}} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \mathbf{b}_{\mathsf{fhe}}^\intercal \end{pmatrix}$ and computes $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G}$ as in the construction.

– Sets $\bar{\mathbf{A}}_{\mathsf{att}} = \mathbf{A}'_{\mathsf{att}} + ((1, \mathsf{bits}(\mathbf{X})) \otimes \overline{\mathbf{G}}$, $\mathbf{A}_{\mathsf{att}} = \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{att}} \\ \underline{\mathbf{a}}_{\mathsf{att}}^\intercal \end{pmatrix}$, where $\underline{\mathbf{a}}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L_X}+1)m}$, and $\mathbf{c}_{\mathsf{att}}^\intercal = \mathbf{b}_{\mathsf{att}}^\intercal - (\underline{\mathbf{a}}_{\mathsf{att}}^\intercal - (1, \mathsf{bits}(\mathbf{X})) \otimes \underline{\mathbf{G}})$, where $\overline{\mathbf{G}}$ and $\underline{\mathbf{G}}$ denote the first n and the last rows, respectively, of gadget matrix $\mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m}$.

– Sends $(\mathbf{c}_{\mathbf{B}},\ \mathbf{X},\ \mathbf{c}_{\mathsf{att}})$ to $\mathcal{A}$.

3. $\mathcal{A}$ outputs a bit β'. $\mathcal{B}$ forwards the bit β' to the LWE challenger.

We note that if the LWE challenger sent $\mathbf{b} = \mathbf{t}\mathbf{A}_{\mathsf{LWE}} + \mathbf{e}_{\mathsf{LWE}}$, then $\mathcal{B}$ simulated Hyb_2 with $\mathcal{A}$ else if LWE challenger sent random $\mathbf{b} \leftarrow \mathbb{Z}_q^{mw+m+(\mathrm{L_X}+1)m}$ then $\mathcal{B}$ simulated Hyb_3 with $\mathcal{A}$.
To see the latter case, we note that if $\mathbf{b} \leftarrow \mathbb{Z}_q^{mw+m+(\mathrm{L_X}+1)m}$ then it implies $\mathbf{b}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw}$, $\mathbf{b}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{m}$, $\mathbf{b}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L_X}+1)m}$. This implies the following.

– Randomness of $\mathbf{b}_{\mathbf{B}}$ implies the randomness of $\mathbf{c}_{\mathbf{B}}^\intercal := \mathbf{b}_{\mathbf{B}}^\intercal - \underline{\mathbf{b}}^\intercal$.

– Randomness of $\mathbf{b}_{\mathsf{fhe}}$ implies $\mathbf{A}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$.

– Randomness of $\mathbf{b}_{\mathsf{att}}$ implies randomness of $\mathbf{c}_{\mathsf{att}}^\intercal = \mathbf{b}_{\mathsf{att}}^\intercal - \left(\underline{\mathbf{a}}_{\mathsf{att}}^\intercal - (1, \mathsf{bits}(\mathbf{X})) \otimes \iota_{n+1}^\intercal \otimes \mathbf{g}\right)$.

Thus it suffices to show that the following distribution is indistinguishable from Equation (45)

$$\left(\mathsf{aux},\ \mathbf{B},\ \ \mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw},\ \ \mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G},\ \ \mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{(\mathrm{L_X}+1)m},\ \ \left\{\mathbf{c}_{1,i}^\intercal = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{1,i}^\intercal \right\}_{i\in[Q]}\right)$$

Hyb_4. This hybrid is same as Hyb_3 except we sample $\mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})}$. We have $\mathsf{Hyb}_3 \approx_s \mathsf{Hyb}_4$ using Leftover Hash Lemma (LHL). By LHL we have that $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}$ is statistically close to uniform. Thus $\mathbf{X} = \mathbf{A}_{\mathsf{fhe}}\mathbf{R} - (\mathbf{x}_b, \mathsf{sd}) \otimes \mathbf{G}$ is statistically close to uniform due to randomness from $\mathbf{A}_{\mathsf{fhe}}\mathbf{R}$. Thus it suffices to show that the following distribution is indistinguishable from Equation (45)

$$\left(\mathsf{aux},\ \mathbf{B},\ \ \mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw},\ \ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})},\ \ \mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{m},\ \ \left\{\mathbf{c}_{1,i}^\intercal = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil + \mathsf{PRF}(\mathsf{sd}, \mathbf{r}_i) + \mathbf{e}_{1,i}^\intercal \right\}_{i\in[Q]}\right)$$

Hyb_5.This hybrid is same as the previous hybrid except we change all the PRF values computed using sd to random. It is straightforward to see that Hyb_4 and Hyb_5 are indistinguishable due to the security of PRF. Thus it suffices to show that the following distribution is indistinguishable from Equation (45)

$$\left(\mathsf{aux},\ \mathbf{B},\ \mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw},\ \ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})},\ \ \mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{m},\ \ \left\{\mathbf{c}_{1,i}^\intercal = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{high}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}^{\mathrm{F}_{i,\mathsf{low}}}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil + R_i + \mathbf{e}_{1,i}^\intercal \right\}_{i\in[Q]}\right)$$

where $R_i \leftarrow [-q/4 + B, q/4 - B]^{1\times\ell}$ for all $i \in [Q]$.

Hyb_6. In this hybrid we compute $\mathbf{c}_{1,i}^\intercal = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil + (\mathbf{c}'_{1,i})^\intercal$ for $i \in [Q]$. $\mathsf{Hyb}_5 \approx_s \mathsf{Hyb}_6$. To see this note that for $i \in [Q]$

- for our choice of B the statistical distance between the uniform distribution over $[-q/4, q/4]$ and $[-q/4 + B, q/4 - B]$ is negligible. Thus $\mathbf{c}'_{1,i} \approx_s R_i$ where $\mathbf{c}'_{1,i} \leftarrow [-q/4, q/4]^{1\times\ell}$ and $R_i \leftarrow [-q/4 + B, q/4 - B]^{1\times\ell}$.
- Next, from our parameter setting, we have $\|\mathbf{e}_{1,i}\| \le \frac{1}{2^{2\lambda}} \times \frac{q}{4}$.
- We have $R_i \approx_s R_i + \mathbf{e}_{1,i}^\intercal$ by noise flooding (Lemma 3.9).

Thus we have the following distribution

$$\left(\begin{array}{c} \mathsf{aux},\ \mathbf{B},\ \ \mathbf{c}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{mw},\ \ \mathbf{X} \leftarrow \mathbb{Z}_q^{(n+1)\times m(\lambda+\mathrm{L})}, \mathbf{c}_{\mathsf{att}} \leftarrow \mathbb{Z}_q^{m}, \\ \{\mathbf{c}_{1,i}^\intercal = C \cdot \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{high}}}}{C} \right\rceil + \left\lfloor \frac{\mathbf{c}_{\mathsf{att}}^\intercal \cdot \mathbf{H}_{\mathbf{A}_{\mathsf{att}},\mathbf{X}}^{\mathrm{F}_{i,\mathsf{low}}}}{C} \right\rceil + f_i(\mathbf{x}_b)\lfloor q/2 \rceil + (\mathbf{c}'_{1,i})^\intercal\}_{i\in[Q]} \end{array} \right)$$

which is the distribution in Equation (45). Hence, the proof.

□

7.3.1 Connection to Evasive LWE

Here, we briefly discuss the connection between evasive and fixed-bit evasive LWE for our specific application. In particular, we show that if we restrict ourselves to the particular samplers we consider for the security proof (Section 7.3) of our FE (Section 7.2), fixed-bit evasive LWE implies evasive LWE.

To see this, we start with a pre-condition sampler of evasive LWE that outputs $\mathbf{P}$ that is induced by $(\{\mathbf{x}_i\}_i, \{f_j\}_j)$ such that $\{f_j(\mathbf{x}_i)\}_{i,j}$ is pseudorandom (even given the auxiliary information). By the same argument as the security proof of our FE in Section 7.3, it follows that even given $(\{\mathbf{x}_i\}_i, \{f_j\}_j)$, $\mathbf{SP} + \mathbf{E}'$ is half-space pseudorandom. This implies the indistinguishability of the post-condition distributions by the fixed-bit evasive LWE, namely, $\mathbf{T} + \mathbf{C}'$ is half-space pseudorandom. However, we can actually show that $\mathbf{T} + \mathbf{C}'$ is pseudorandom over the entire space, not only half-space random, since "the most significant bit" $\{f_j(\mathbf{x}_i)\}_{i,j}$ is also pseudorandom. The post-condition distributions of the fixed-bit evasive LWE with $\mathbf{T} + \mathbf{C}'$ being random correspond to those of evasive LWE, as desired.

8 iO via Weak Succinct LWE Sampling

In this section, we provide our candidate construction of weak succinct LWE sampler $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$. Since the intuition was discussed in Section 2, we proceed directly to the construction.

8.1 Construction.

Let $\mathcal{F} = \{\mathrm{F} : \{0,1\}^\lambda \times \mathbb{Z}_q \to [-q/8 + \widetilde{\beta}, q/8 - \widetilde{\beta}]\}$, where $\widetilde{\beta}$ is set such that it is exponentially smaller than q, be a family of PRF functions where $\mathrm{F} \in \mathcal{F}$ can be computed by a circuit of depth $\mathsf{dep}(\lambda) = \mathrm{poly}(\lambda)$. We construct weak succinct LWE sampler $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ as below.

$\mathsf{SampCRSGen}(1^\lambda, 1^N, \alpha; \mathsf{coins}_{\mathsf{crs}})$**:** On input the security parameter λ, a size parameter N, a blow up factor α and random coins used to sample crs ($\mathsf{coins}_{\mathsf{crs}}$), the $\mathsf{SampCRSGen}$ algorithm does the following.

1. Derive parameters $\mathsf{params} = (q, M, K, W, \overline{\chi}, \overline{B})$ as in parameter setting. Let $n = \mathrm{poly}(\lambda)$ and $m = O((n+1)\log q)$.
2. Fix a constant $C \in \mathbb{Z}$ such that C divides q.
3. Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{(n+1)\times W\lceil \log q\rceil}$ and $\mathbf{A}_{\mathsf{sd}} \leftarrow \mathbb{Z}_q^{(n+1)\times(L_{\mathsf{sd}}+1)m}$, where we set $L_{\mathsf{sd}} = (n+1)\lambda m \lceil \log q\rceil$.
4. Output $\mathsf{crs} = (C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params})$.

$\mathsf{LWEGen}(\mathsf{crs}; \mathsf{coins}_{\mathsf{seed}})$**:** On input common reference string crs and random coins used to sample $\mathsf{seed}_{\mathbf{B}^*}$, $\mathsf{coins}_{\mathsf{seed}}$, parsed as $(\mathbf{A}^*, \mathsf{coins})$, where $\mathbf{A}^* \leftarrow \mathbb{Z}_q^{M\times W}$, the LWEGen algorithm does the following:

1. Sample $\mathbf{S}^* \leftarrow \mathbb{Z}_q^{W\times K}$ and $\bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m}$.
2. Sample $(\mathbf{B}, \mathbf{B}_\tau^{-1}) \leftarrow \mathsf{TrapGen}(1^{n+1}, 1^{mw}, q)$ where $w \in O(\log q)$.
3. For $i \in [K]$, compute encodings as follows:
   (a) Sample $\bar{\mathbf{t}}_i \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{t}}}$ and set $\mathbf{t}_i = (\bar{\mathbf{t}}_i^\intercal, -1)^\intercal$.
   (b) Sample $\mathbf{e}_{\mathbf{B},i} \leftarrow \mathcal{D}^{mw}_{\mathbb{Z},\sigma_{\mathbf{B}}}$ and compute $\mathbf{c}^\intercal_{\mathbf{B},i} = \mathbf{t}_i^\intercal \mathbf{B} + \mathbf{e}^\intercal_{\mathbf{B},i} \in \mathbb{Z}_q^{1\times mw}$.
   (c) Sample PRF seed $\mathsf{sd}_i \in \{0,1\}^\lambda$.
   (d) Compute FHE ciphertext for PRF seed: Sample $\mathbf{e}_{\mathsf{fhe},i} \leftarrow \mathcal{D}^m_{\mathbb{Z},\sigma_{\mathsf{fhe}}}$, $\mathbf{R}_i \leftarrow \{0,1\}^{m\times m\lambda}$ and compute a GSW encryption as follows.
   $$\mathbf{A}_{\mathsf{fhe},i} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \\ \bar{\mathbf{t}}_i^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^\intercal_{\mathsf{fhe},i} \end{pmatrix}, \quad \widehat{\mathsf{sd}_i} = \mathbf{A}_{\mathsf{fhe},i}\mathbf{R}_i - \mathsf{sd}_i \otimes \mathbf{G} \in \mathbb{Z}_q^{(n+1)\times m\lambda}.$$
   We have that $L_{\mathsf{sd}} = (n+1)\lambda m \lceil \log q\rceil$ is the bit length of $\widehat{\mathsf{sd}_i}$.
   (e) Compute a BGG^+ encoding of $\widehat{\mathsf{sd}_i}$ as follows.
   $$\mathbf{e}_{\mathsf{sd},i} \leftarrow \mathcal{D}^{(L_{\mathsf{sd}}+1)m}_{\mathbb{Z},\sigma_{\mathsf{sd}}}, \quad \mathbf{c}^\intercal_{\mathsf{sd},i} = \mathbf{t}_i^\intercal(\mathbf{A}_{\mathsf{sd}} - (1, \mathsf{bits}(\widehat{\mathsf{sd}_i})) \otimes \mathbf{G}) + \mathbf{e}^\intercal_{\mathsf{sd},i} \in \mathbb{Z}_q^{1\times(L_{\mathsf{sd}}+1)m}$$
   (f) Compute IPFE encodings as follows.
   $$\mathbf{e}_i \leftarrow \mathcal{D}^{W\log q}_{\mathbb{Z},\sigma_{\mathsf{IPFE}}}, \qquad \mathbf{c}_i^\intercal = \mathbf{t}_i^\intercal \mathbf{A} + \mathbf{e}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal) \in \mathbb{Z}_q^{1\times W\log q}$$
   (g) Set $\mathsf{ct}_i = (\mathbf{c}_{\mathbf{B},i}, \mathbf{c}_{\mathsf{sd},i}, \widehat{\mathsf{sd}_i}, \mathbf{c}_i)$.
4. For $j \in [M]$, compute function keys as follows:
   (a) Let $\mathrm{F}_j \in \mathcal{F}$ be a PRF function with hardwired input j such that $\mathrm{F}_j(\mathbf{x}) = \mathrm{F}(\mathbf{x}, j)$. Let
   $$\mathrm{F}_j(\mathbf{x}) := C \cdot \mathrm{F}_{\mathsf{high},j}(\mathbf{x}) + \mathrm{F}_{\mathsf{low},j}(\mathbf{x})$$
   where $\mathbf{x} \in \{0,1\}^\lambda$, $\mathrm{F}_{\mathsf{high},j}(\mathbf{x}) \in [0, q/C]$ and $\mathrm{F}_{\mathsf{low},j}(\mathbf{x}) \in [0, C-1]$. Using the fact that the PRF computation and hence $\mathrm{F}_j(\mathbf{x})$ can be computed by a circuit of depth at most $\mathsf{dep}(\lambda) = \mathrm{poly}(\lambda)$, the function $\mathrm{F}_{\mathsf{high},j}(\mathbf{x})$ and $\mathrm{F}_{\mathsf{low},j}(\mathbf{x})$ can also be computed by a circuit of depth $d \le \mathrm{poly}(\mathsf{dep})$.
   (b) Define the homomorphic evaluation circuit $\mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}} = \mathsf{MakeVEvalCkt}(n, m, q, C \cdot \mathrm{F}_{\mathsf{high},j})$ and $\mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}} = \mathsf{MakeVEvalCkt}(n, m, q, C \cdot \mathrm{F}_{\mathsf{low},j})$. From Lemma 3.15, the depth of both $\mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}}$ and $\mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}}$ is $dO(\log m \log\log q) + O(\log^2 \log q)$.
   (c) Compute $\mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}}} = \mathsf{MEvalC}(\mathbf{A}_{\mathsf{sd}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}}) \in \mathbb{Z}_q^{(L_{\mathsf{sd}}+1)m}$,
   $\mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}}} = \mathsf{MEvalC}(\mathbf{A}_{\mathsf{sd}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}}) \in \mathbb{Z}_q^{(L_{\mathsf{sd}}+1)m}$

(d) Compute $\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}} = \mathbf{A}_{\mathsf{sd}} \cdot \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}}}$ and $\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}} = \mathbf{A}_{\mathsf{sd}} \cdot \mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}}}$.

(e) Compute

$$\mathbf{a}_{\mathrm{F}_j,\mathsf{err}} = C \cdot \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \in \mathbb{Z}_q^{n+1}$$

(f) Let $\mathbf{a}_{\mathsf{mask},j} = \mathbf{A} \cdot \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) \in \mathbb{Z}_q^{n+1}$

(g) Sample $\mathbf{k}_j \leftarrow \mathbf{B}_\tau^{-1}\left(\mathbf{a}_{\mathrm{F}_j,\mathsf{err}} + \mathbf{a}_{\mathsf{mask},j}\right)$.

5. Set $\mathsf{seed}_{\mathbf{B}^*} = (\{\mathsf{ct}_i\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*)$.
6. Output $(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*)$.

$\mathsf{Expand}(\mathsf{crs}, \mathsf{seed}_{\mathbf{B}^*})$**:** On input common reference string crs and $\mathsf{seed}_{\mathbf{B}^*}$, parse $\mathsf{crs} = (C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params})$ and $\mathsf{seed}_{\mathbf{B}^*} = (\{\mathbf{c}_{\mathbf{B},i}, \mathbf{c}_{\mathsf{sd},i}, \widehat{\mathsf{sd}}_i, \mathbf{c}_i\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*)$ and do the following.

1. For all $i \in [K], j \in [M]$,
   (a) Compute $c_{\mathsf{mask},i,j} = \mathbf{c}_i^\intercal \cdot \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal)$.
   (b) Compute $\mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} = \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{sd}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}}, \widehat{\mathsf{sd}}_i)$
   $\mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} = \mathsf{MEvalCX}(\mathbf{A}_{\mathsf{sd}}, \mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}}, \widehat{\mathsf{sd}}_i)$
   (c) Compute $c_{\mathrm{F}_j,\mathsf{err},i} = C \left\lfloor \frac{\mathbf{c}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}}{C} \right\rfloor$.
   (d) Compute $z_{i,j} = c_{\mathsf{mask},i,j} + c_{\mathrm{F}_j,\mathsf{err},i} - \mathbf{c}_{\mathbf{B},i}^\intercal \mathbf{k}_j$
2. Set and output $\mathbf{B}^* = \begin{bmatrix} z_{1,1} & z_{2,1} & \cdots & z_{K,1} \\ \vdots & \vdots & \vdots & \vdots \\ z_{1,M} & z_{2,M} & \cdots & z_{K,M} \end{bmatrix}$

Parameters and Constraints. We set our parameters as follows.

$$\hat{\beta} = 2^{O(\mathsf{dep}\cdot\log^3\lambda)},\ \ n = \mathrm{poly}(\lambda, \mathsf{dep}),\ \ m = O(n\log q),\ \ \tau = O\left(\sqrt{(n+1)\log q}\right),\ \ \sigma_{\mathbf{B}} = 2^{4\lambda}\beta$$

$$\sigma_{\mathbf{t}} = \sigma_{\mathsf{fhe}} = \sigma_{\mathsf{sd}} = \sigma_{\mathsf{IPFE}} = 2^{2\lambda}, \tilde{\beta} = O((W+C)\cdot\sigma_{\mathsf{IPFE}} + \sigma_{\mathbf{B}})\mathrm{poly}(\lambda),\ \ C = 2^{3\lambda}\tilde{\beta},\ \ q = 2^{7\lambda}\tilde{\beta}$$

Constraints.

- $N = MK$ (constraint of the sampler).
- $(K+M)(1+2W) \le N^\delta$, for some constant $\delta < 1$ (for δ-succinctness).
- $M^2 \le N^\delta \mathrm{poly}(\lambda, \log q)$ (for SRE succinctness).

Correctness. We now analyze the correctness of our weak succinct LWE sampler.

Claim 8.1. Let $\beta = q/8$. Then the weak succinct LWE sampler $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ as described above satisfies correctness as in Section 3.8.

Proof. To prove the claim, we start by analyzing individual term as below and then aggregate them to get $\mathbf{B}^*$.

- We first start by analyzing the term $c_{\mathsf{mask},i,j}$ for all $i \in [K], j \in [M]$.

$$\begin{aligned}
c_{\mathsf{mask},i,j} &= \mathbf{c}_i^\intercal \cdot \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) \\
&= (\mathbf{t}_i^\intercal \mathbf{A} + \mathbf{e}_i^\intercal + ((\mathbf{S}^*[\cdot,i])^\intercal \otimes \mathbf{g}^\intercal)) \cdot \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) \\
&= \mathbf{t}_i^\intercal \mathbf{A}\mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) + \mathbf{e}_i^\intercal \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) + ((\mathbf{S}^*[\cdot,i])^\intercal \otimes \mathbf{g}^\intercal))\mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) \\
&= \mathbf{t}_i^\intercal \mathbf{a}_{\mathsf{mask},j} + \mathbf{e}_i^\intercal \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) + \langle \mathbf{S}^*[\cdot,i], \mathbf{A}^*[j,\cdot] \rangle \\
&\qquad\qquad \text{(as } \mathbf{A}\mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) = \mathbf{a}_{\mathsf{mask},j} \text{ from construction.)} \\
&= \mathbf{t}_i^\intercal \mathbf{a}_{\mathsf{mask},j} + \mathbf{e}_i^\intercal \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) + \langle \mathbf{A}^*[j,\cdot], \mathbf{S}^*[\cdot,i] \rangle
\end{aligned} \tag{46}$$

- Next, we analyze the term $\mathbf{c}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}$ for all $i \in [K], j \in [M]$.

$$\begin{aligned}
\mathbf{c}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} &= (\mathbf{t}_i^\intercal(\mathbf{A}_{\mathsf{sd}} - (1, \mathsf{bits}(\widehat{\mathsf{sd}}_i)) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{sd},i}^\intercal)\mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} \\
&= \mathbf{t}_i^\intercal \mathbf{A}_{\mathsf{sd}} \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}}} - \mathbf{t}_i^\intercal \mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}}(\widehat{\mathsf{sd}}_i) + \mathbf{e}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} \\
&= \mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}} - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + \mathbf{e}_{\mathsf{fhe},i}^\intercal \mathbf{r}_{\mathrm{F}_{\mathsf{high},j},i} + \mathbf{e}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} \\
&= \mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}} - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + e_{\mathrm{F}_{\mathsf{high},j},i}
\end{aligned} \tag{47}$$

where $\mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}}(\widehat{\mathsf{sd}}_i) = \mathbf{A}_{\mathsf{fhe},i}\mathbf{r}_{\mathrm{F}_{\mathsf{high},j},i} - \begin{pmatrix} 0^n \\ C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) \end{pmatrix}$ and $e_{\mathrm{F}_{\mathsf{high},j},i} = \mathbf{e}_{\mathsf{fhe},i}^\intercal \mathbf{r}_{\mathrm{F}_{\mathsf{high},j},i} + \mathbf{e}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}$.

- Similar to analysis of Equation (47), we have for all $i \in [K], j \in [M]$,

$$\mathbf{c}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i} = \mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{low},j}} - C \cdot \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) + e_{\mathrm{F}_{\mathsf{low},j},i}$$

where $\mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}}(\widehat{\mathsf{sd}}_i) = \mathbf{A}_{\mathsf{fhe},i}\mathbf{r}_{\mathrm{F}_{\mathsf{low},j},i} - \begin{pmatrix} 0^n \\ C \cdot \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) \end{pmatrix}$ and $e_{\mathrm{F}_{\mathsf{low},j},i} = \mathbf{e}_{\mathsf{fhe},i}^\intercal \mathbf{r}_{\mathrm{F}_{\mathsf{low},j},i} + \mathbf{e}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}$.

- We have following analysis for both $\mu = \mathsf{high}$ and $\mu = \mathsf{low}$.
  By Lemma 3.15 , we have $|\mathbf{r}_{\mathrm{F}_{\mu,j},i}| \leq (m+2)^d \lceil \log q \rceil \max_{k \in [\lambda]} ||\mathbf{R}_{i,k}^\intercal|| \leq (m+2)^d \lceil \log q \rceil m \leq \hat{\beta}$.
  and using depth bound from Section 3.7,
  $|\mathbf{h}_{\mathrm{F}_{\mu,j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}| \leq (m+2)^{d_{\mathsf{VEval}_{\mathrm{F}_{\mu,j}}} \lceil \log q \rceil} \leq 2^{dO(\log \lambda)} \leq \hat{\beta}$.
  Next, we have $|e_{\mathrm{F}_{\mu,j},i}| \leq |\mathbf{e}_{\mathsf{fhe},i}^\intercal \mathbf{r}_{\mathrm{F}_{\mu,j},i} + \mathbf{e}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mu,j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}| \leq |\mathbf{e}_{\mathsf{fhe},i}^\intercal \mathbf{r}_{\mathrm{F}_{\mu,j},i}| + |\mathbf{e}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mu,j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}| \leq \sqrt{\lambda}\sigma_{\mathsf{fhe}}\hat{\beta}m + \sqrt{\lambda}\sigma_{\mathsf{sd}}\hat{\beta}(L_{\mathsf{sd}}+1)m \leq 2^{3\lambda}\hat{\beta}$.

- Now, for all $i \in [K], j \in [M]$,

$$\begin{aligned}
C \left\lfloor \frac{\mathbf{c}_{\mathsf{sd},i}^\intercal \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}}{C} \right\rfloor &= C \left\lfloor \frac{\mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}} - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + e_{\mathrm{F}_{\mathsf{high},j},i}}{C} \right\rfloor \\
&= C \left\lfloor \frac{\mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}} - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i)}{C} \right\rfloor + C \cdot \tilde{e}_{h,j,i} \\
&\qquad\qquad \text{where } |\tilde{e}_{h,j,i}| \leq 1, \text{ since } |e_{\mathrm{F}_{\mathsf{high},j},i}| \leq 2^{3\lambda}\hat{\beta} < 2^{3\lambda}\tilde{\beta} = C \\
&= C \left\lfloor \frac{\mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + C \cdot \tilde{e}_{h,j,i}
\end{aligned}$$

By similar analysis, for all $i \in [K], j \in [M]$,

$$\begin{aligned}\left\lfloor \frac{\mathbf{c}_{\mathsf{sd},i}^{\mathsf{T}} \mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}}{C} \right\rfloor &= \left\lfloor \frac{\mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_{\mathsf{low},j}} - C \cdot \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) + e_{\mathrm{F}_{\mathsf{low},j},i}}{C} \right\rfloor \\ &= \left\lfloor \frac{\mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_{\mathsf{low},j}} - C \cdot \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i)}{C} \right\rfloor + \tilde{e}_{l,j,i} \\ &\qquad \text{where } |\tilde{e}_{l,j,i}| \leq 1, \text{ since } |e_{\mathrm{F}_{\mathsf{low},j},i}| \leq 2^{3\lambda}\hat{\beta} < 2^{3\lambda}\tilde{\beta} = C \\ &= \left\lfloor \frac{\mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor - \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) + \tilde{e}_{l,j,i}\end{aligned}$$

- For all $i \in [K], j \in [M]$,

$$\begin{aligned} c_{\mathrm{F}_j,\mathsf{err},i} &= C \left\lfloor \frac{\mathbf{c}_{\mathsf{sd},i}^{\mathsf{T}} \mathbf{h}_{\mathrm{F}_{\mathsf{high},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{c}_{\mathsf{sd},i}^{\mathsf{T}} \mathbf{h}_{\mathrm{F}_{\mathsf{low},j},\mathbf{A}_{\mathsf{sd}},\widehat{\mathsf{sd}}_i}}{C} \right\rfloor \qquad (48) \\ &= C \left\lfloor \frac{\mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + C \cdot \tilde{e}_{h,j,i} + \left\lfloor \frac{\mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor - \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) + \tilde{e}_{l,j,i} \\ &= C\mathbf{t}_i^{\mathsf{T}} \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor + Ce_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + C \cdot \tilde{e}_{h,j,i} + \mathbf{t}_i^{\mathsf{T}} \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor + e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} \\ &\qquad - \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) + \tilde{e}_{l,j,i} \\ &= \mathbf{t}_i^{\mathsf{T}} \left(C \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \right) - C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) - \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) + Ce_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} \\ &\qquad + C \cdot \tilde{e}_{h,j,i} + e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} + \tilde{e}_{l,j,i} \\ &= \mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_j,\mathsf{err}} - \mathrm{F}_j(\mathsf{sd}_i) + Ce_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} + C \cdot \tilde{e}_{h,j,i} + e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} + \tilde{e}_{l,j,i} \end{aligned}$$

where $\mathbf{a}_{\mathrm{F}_j,\mathsf{err}} = \left(C \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \right)$ from construction and $C \cdot \mathrm{F}_{\mathsf{high},j}(\mathsf{sd}_i) + \mathrm{F}_{\mathsf{low},j}(\mathsf{sd}_i) = \mathrm{F}_j(\mathsf{sd}_i)$ by definition of F_j. We will now analyze error $e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}}$ and $e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}}$.

– We have from above

$$\begin{aligned} e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} &= \mathbf{t}_i^{\mathsf{T}} \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor - \left\lfloor \frac{\mathbf{t}_i^{\mathsf{T}} \mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor \\ &= \mathbf{t}_i^{\mathsf{T}} \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor - \left\lfloor \mathbf{t}_i^{\mathsf{T}} \left(\left(\frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} - \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor \right) + \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor \right) \right\rfloor \\ &= \mathbf{t}_i^{\mathsf{T}} \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor - \left\lfloor \mathbf{t}_i^{\mathsf{T}} \left(\frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} - \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor \right) \right\rfloor - \mathbf{t}_i^{\mathsf{T}} \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor \\ &= - \left\lfloor \mathbf{t}_i^{\mathsf{T}} \underbrace{\left(\frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} - \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{high},j}}}{C} \right\rfloor \right)}_{<1} \right\rfloor \end{aligned}$$

$$\implies |e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}}| \leq n|\mathbf{t}_i|$$

– Similarly,

$$\begin{aligned}
e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} &= \mathbf{t}_i^\intercal \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor - \left\lfloor \frac{\mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \\
&= \mathbf{t}_i^\intercal \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor - \left\lfloor \mathbf{t}_i^\intercal \left(\left(\frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} - \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \right) + \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \right) \right\rfloor \\
&= \mathbf{t}_i^\intercal \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor - \left\lfloor \mathbf{t}_i^\intercal \left(\frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} - \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \right) \right\rfloor - \mathbf{t}_i^\intercal \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \\
&= - \left\lfloor \mathbf{t}_i^\intercal \underbrace{\left(\frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} - \left\lfloor \frac{\mathbf{a}_{\mathrm{F}_{\mathsf{low},j}}}{C} \right\rfloor \right)}_{<1} \right\rfloor
\end{aligned}$$

$$\implies |e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}}| \leq n|\mathbf{t}_i|$$

- For all $i \in [K], j \in [M]$,

$$\begin{aligned}
\mathbf{c}_{\mathbf{B},i}^\intercal \mathbf{k}_j &= (\mathbf{t}_i^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B},i}^\intercal)\mathbf{k}_j \\
&= \mathbf{t}_i^\intercal \mathbf{B}\mathbf{B}_\tau^{-1}(\mathbf{a}_{\mathrm{F}_j,\mathsf{err}} + \mathbf{a}_{\mathsf{mask},j}) + \mathbf{e}_{\mathbf{B},i}^\intercal \mathbf{k}_j \\
&= \mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_j,\mathsf{err}} + \mathbf{t}_i^\intercal \mathbf{a}_{\mathsf{mask},j} + \mathbf{e}_{\mathbf{B},i}^\intercal \mathbf{k}_j
\end{aligned} \tag{49}$$

- From Equation (46), (48), and (49), we have for all $i \in [K], j \in [M]$,

$$\begin{aligned}
z_{i,j} &= c_{\mathsf{mask},i,j}^\intercal + c_{\mathrm{F}_j,\mathsf{err},i}^\intercal - \mathbf{c}_{\mathbf{B},i}^\intercal \mathbf{k}_j \\
&= \mathbf{t}_i^\intercal \mathbf{a}_{\mathsf{mask},j} + \mathbf{e}_i^\intercal \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) + \langle \mathbf{A}^*[j,\cdot], \mathbf{S}^*[\cdot,i] \rangle + \mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_j,\mathsf{err}} - \mathrm{F}_j(\mathsf{sd}_i) + \\
&\quad Ce_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} + C \cdot \tilde{e}_{h,j,i} + e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} + \tilde{e}_{l,j,i} - \left(\mathbf{t}_i^\intercal \mathbf{a}_{\mathrm{F}_j,\mathsf{err}} + \mathbf{t}_i^\intercal \mathbf{a}_{\mathsf{mask},j} + \mathbf{e}_{\mathbf{B},i}^\intercal \mathbf{k}_j \right) \\
&= \langle \mathbf{A}^*[j,\cdot], \mathbf{S}^*[\cdot,i] \rangle + e_{i,j}^*
\end{aligned}$$

where $e_{i,j}^* = \mathbf{e}_i^\intercal \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) - \mathrm{F}_j(\mathsf{sd}_i) + Ce_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} + C \cdot \tilde{e}_{h,j,i} + e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} + \tilde{e}_{l,j,i} - \mathbf{e}_{\mathbf{B},i}^\intercal \mathbf{k}_j$.
We have $|\mathbf{e}_i^\intercal \mathbf{G}^{-1}((\mathbf{A}^*[j,\cdot])^\intercal) + Ce_{\mathbf{t}_i,\mathrm{F}_{\mathsf{high},j}} + C \cdot \tilde{e}_{h,j,i} + e_{\mathbf{t}_i,\mathrm{F}_{\mathsf{low},j}} + \tilde{e}_{l,j,i} - \mathbf{e}_{\mathbf{B},i}^\intercal \mathbf{k}_j| \leq \sqrt{\lambda}\sigma_{\mathsf{IPFE}} W \log q + (C+1)(n\sqrt{\lambda}\sigma_{\mathbf{t}} + 1) + \lambda\sigma_{\mathbf{B}}\tau mw \leq O((W+C)\sigma_{\mathsf{IPFE}} + \sigma_{\mathbf{B}})\mathrm{poly}(\lambda) = \tilde{\beta}$ where $\sigma_{\mathbf{t}} = \sigma_{\mathsf{IPFE}}$ by our parameter setting.
Since, $|\mathrm{F}_j(\mathsf{sd}_i)| \leq \frac{q}{8} - \tilde{\beta}$, we have $|e_{i,j}^*| \leq \frac{q}{8}$.

Finally, we have

$$\mathbf{B}^* = \begin{bmatrix} z_{1,1} & z_{2,1} & \cdots & z_{K,1} \\ \vdots & \vdots & \vdots & \vdots \\ z_{1,M} & z_{2,M} & \cdots & z_{K,M} \end{bmatrix}$$

$$\implies \mathbf{B}^* = \begin{bmatrix} \langle \mathbf{A}^*[1,\cdot], \mathbf{S}^*[\cdot,1] \rangle + e_{1,1}^* & \langle \mathbf{A}^*[1,\cdot], \mathbf{S}^*[\cdot,2] \rangle + e_{2,1}^* & \cdots & \langle \mathbf{A}^*[1,\cdot], \mathbf{S}^*[\cdot,K] \rangle + e_{K,1}^* \\ \vdots & \vdots & \vdots & \vdots \\ \langle \mathbf{A}^*[M,\cdot], \mathbf{S}^*[\cdot,1] \rangle + e_{1,M}^* & \langle \mathbf{A}^*[M,\cdot], \mathbf{S}^*[\cdot,2] \rangle + e_{2,M}^* & \cdots & \langle \mathbf{A}^*[M,\cdot], \mathbf{S}^*[\cdot,K] \rangle + e_{K,M}^* \end{bmatrix}$$

This implies $\mathbf{B}^* = \mathbf{A}^*\mathbf{S}^* + \mathbf{E}^*$ and $|\mathbf{B}^* - \mathbf{A}^*\mathbf{S}^*| = |e_{i,j}^*| \leq \frac{q}{8}$. Hence, the proof.

□

Claim 8.2. Suppose there exists $\delta < 1$ such that $(K+M)(1+2W) \leq N^\delta$. Then, weak succinct LWE sampler $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ as described above is δ-succinct.

Proof.

$$\begin{aligned}
\mathsf{bitlength}(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*) &= \mathsf{bitlength}((\{\mathsf{ct}_i\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*), \mathbf{A}^*, \mathbf{S}^*) \\
&= \mathsf{bitlength}((\{\mathbf{c}_{\mathbf{B},i}, \mathbf{c}_{\mathsf{sd},i}, \widehat{\mathsf{sd}}_i, \mathbf{c}_i\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*), \mathbf{A}^*, \mathbf{S}^*) \\
&= \big(K(mw + (L_{\mathsf{sd}}+1)m + (n+1)m\lambda + W\log q) + Mmw + 2MW + WK\big)\log q \\
&\leq \big(K\mathrm{poly}(\lambda, \log q) + KW\mathrm{poly}(\log q) + M\mathrm{poly}(\lambda, \log q) \\
&\qquad + 2MW\log q + WK\log q \\
&\leq (K + 2KW + M + 2MW)\mathrm{poly}(\lambda, \log q) \\
&\leq (K+M)(1+2W)\mathrm{poly}(\lambda, \log q) \\
&\leq N^{\delta}\cdot \mathrm{poly}(\lambda, \log q)
\end{aligned}$$

Hence, the proof. □

Next, we show that our construction satisfies Definition 3.16.

Claim 8.3. Assuming $\mathrm{LWE}(M, W, q, \overline{\chi})$ holds, where $\overline{\chi}$ is uniform distribution over $[-\overline{B}, \overline{B}]$,

$$D_0 := (\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{b} = \mathbf{A}^*\mathbf{s}' + \mathbf{e}') \approx_c D_1 := (\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{b} \leftarrow \mathbb{Z}_q^M)$$

where $\mathbf{s}' \leftarrow \mathbb{Z}_q^W$, $\mathbf{e}' \leftarrow \overline{\chi}^M$, $\mathsf{coins}_{\mathsf{crs}}$ are the random coins used to sample $(\mathbf{A}, \mathbf{A}_{\mathsf{sd}})$ and $\mathsf{coins}_{\mathsf{seed}} = (\mathbf{A}^*, \mathsf{coins})$ where coins are the random coins used to sample $(\mathbf{B}, \mathbf{S}^*, \bar{\mathbf{A}}_{\mathsf{fhe}}, \mathbf{e}_{\mathbf{B},i}, \{\bar{\mathbf{t}}_i, \mathsf{sd}_i, \mathbf{e}_{\mathsf{fhe},i}, \mathbf{R}_i, \mathbf{e}_{\mathsf{sd},i}, \mathbf{e}_i\}_{i\in[K]})$ such that $\mathsf{crs} = \mathsf{SampCRSGen}(1^\lambda, 1^N, \alpha; \mathsf{coins}_{\mathsf{crs}})$, $(\mathsf{seed}_{\mathbf{B}^*}, \mathbf{A}^*, \mathbf{S}^*) \leftarrow \mathsf{LWEGen}(\mathsf{crs}; \mathsf{coins}_{\mathsf{seed}})$.

Proof. To prove this claim, we show that if there exists an adversary $\mathcal{A}$ who can distinguish between D_0 and D_1 with non-negligible advantage, then there is a reduction $\mathcal{B}$ that breaks $\mathrm{LWE}(M, W, q, \overline{\chi})$ security with non-negligible advantage. The reduction is as follows.

1. On receiving 1^λ from $\mathcal{A}$, forward it to LWE challenger.
2. The LWE challenger samples $\beta \leftarrow \{0,1\}$, $\mathbf{A}^* \leftarrow \mathbb{Z}_q^{M\times W}, \mathbf{s}' \leftarrow \mathbb{Z}_q^W$, and returns $(\mathbf{A}^*, \mathbf{b})$ to $\mathcal{B}$ where $\mathbf{b} = \mathbf{A}^*\mathbf{s}' + \mathbf{e}'$ if $\beta = 0$ and $\mathbf{b} \leftarrow \mathbb{Z}_q^M$ if $\beta = 1$.
3. Sample random $\mathsf{coins}_{\mathsf{crs}}$ and coins, set $\mathsf{coins}_{\mathsf{seed}} = (\mathbf{A}^*, \mathsf{coins})$.
4. Output $(\mathsf{coins}_{\mathsf{crs}}, \mathsf{coins}_{\mathsf{seed}}, \mathbf{b})$ to $\mathcal{A}$.
5. On receiving β' from $\mathcal{A}$, forward β' to LWE challenger.

It is easy to see that if $\beta = 0$, then $\mathcal{B}$ simulated D_0 and if $\beta = 1$, then $\mathcal{B}$ simulated D_1. Hence, the proof. □

8.2 Security Conjecture

Finally, we state our conjecture that the above construction satisfies weak security or weak β_0-Flooding as stated in Definition 3.18.

Conjecture 8.4 (Conjectured security). Assuming $\mathrm{LWE}(M, W, q, \overline{\chi})$, our construction of SLS given by $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$ satisfies weak β_0 flooding (Definition 3.18), for $\beta_0 = \alpha\overline{B}$.

Conjecture 8.5 (Standalone β_0 flooding). We define following conjecture, which implies weak security of our construction of weak SLS given by $(\mathsf{SampCRSGen}, \mathsf{LWEGen}, \mathsf{Expand})$.

- Let $M, K, \overline{\chi}, \overline{B}, \beta, \widetilde{\sigma}, \sigma_{\mathbf{B}}, B_{\mathsf{flood}}$ be parameters. We will specify the constraints on these parameters later.
- Let $\mathsf{PRF} : \{0,1\}^\lambda \times \mathbb{Z}_q \to [-q/8 + \widetilde{\beta}, q/8 - \widetilde{\beta}]$ be a secure PRF.
- Let $\mathcal{F} = \{\mathrm{F}_j : \{0,1\}^\lambda \to [-q/8 + \widetilde{\beta}, q/8 - \widetilde{\beta}]; j \in \mathbb{Z}_q\}$ be a family of functions such that for $j \in \mathbb{Z}_q$, $\mathrm{F}_j(\mathsf{sd}_i) = \mathsf{PRF}(\mathsf{sd}_i, j)$ for some $i \in \mathbb{Z}_q$.
- Let C be a constant such that C divides q. For any function, $\mathrm{F}_j \in \mathcal{F}$, let $\mathrm{F}_j = C \cdot \mathrm{F}_{\mathsf{high},j} + \mathrm{F}_{\mathsf{low},j}$.
- Let MEvalC and VEval be as defined in Section 3.7. Then,

For

$$
\begin{aligned}
&\{\mathrm{F}_j \in \mathcal{F}\}_{j\in[M]},\ \ L_{\mathsf{sd}} = (n+1)\lambda m \lceil \log q \rceil, L = W \lceil \log q \rceil + m(L_{\mathsf{sd}}+1) + m,\\
&(\mathbf{B}, \mathbf{B}_\tau^{-1}) \leftarrow \mathsf{TrapGen}(1^{n+1}, 1^{mw}, q),\ \ \mathbf{A}_2 \leftarrow \mathbb{Z}_q^{(n+1)\times(L_{\mathsf{sd}}+1)m},\ \ \mathbf{A}_1 \leftarrow \mathbb{Z}_q^{(n+1)\times W\lceil \log q\rceil},\\
&\mathbf{A}_3 \leftarrow \mathbb{Z}_q^{n\times m},\ \ \widetilde{\mathbf{A}} := (\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3),\ \ \mathbf{A}^* \leftarrow \mathbb{Z}_q^{M\times W},\\
&\mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}} = \mathrm{MakeVEvalCkt}(n, m, q, C\cdot \mathrm{F}_{\mathsf{high},j}),\ \ \mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}} = \mathrm{MakeVEvalCkt}(n, m, q, C\cdot \mathrm{F}_{\mathsf{low},j}),\\
&\mathbf{h}_{\mathrm{F}_{\mathsf{high},j}} = \mathsf{MEvalC}(\mathbf{A}_2, \mathsf{VEval}_{\mathrm{F}_{\mathsf{high},j}}) \in \mathbb{Z}_q^{(L_{\mathsf{sd}}+1)m},\ \ \mathbf{h}_{\mathrm{F}_{\mathsf{low},j}} = \mathsf{MEvalC}(\mathbf{A}_2, \mathsf{VEval}_{\mathrm{F}_{\mathsf{low},j}}) \in \mathbb{Z}_q^{(L_{\mathsf{sd}}+1)m}\\
&\mathbf{H}_{\mathsf{high}} = (\mathbf{h}_{\mathrm{F}_{\mathsf{high},1}}, \ldots, \mathbf{h}_{\mathrm{F}_{\mathsf{high},M}}),\ \ \mathbf{H}_{\mathsf{low}} = (\mathbf{h}_{\mathrm{F}_{\mathsf{low},1}}, \ldots, \mathbf{h}_{\mathrm{F}_{\mathsf{low},M}})\\
&\mathbf{A}_{\mathsf{high}} = \mathbf{A}_2 \cdot \mathbf{H}_{\mathsf{high}},\ \ \mathbf{A}_{\mathsf{low}} = \mathbf{A}_2 \cdot \mathbf{H}_{\mathsf{low}},\\
&\mathbf{A}_{\mathsf{err}} = C \cdot \left\lfloor \frac{\mathbf{A}_{\mathsf{high}}}{C} \right\rfloor + \left\lfloor \frac{\mathbf{A}_{\mathsf{low}}}{C} \right\rfloor,\ \ \mathbf{A}_{\mathsf{mask}} = \mathbf{A}_1 \mathbf{G}^{-1}((\mathbf{A}^*)^\intercal),\ \ \mathbf{P} = \mathbf{A}_{\mathsf{err}} + \mathbf{A}_{\mathsf{mask}},\\
&\{\bar{\mathbf{t}}_i \leftarrow \mathcal{D}^n_{\mathbb{Z},\sigma_{\mathbf{t}}}\}_{i\in[K]},\ \ \{\mathbf{t}_i = (\bar{\mathbf{t}}_i^\intercal, -1)^\intercal\}_{i\in[K]},\ \ \mathbf{T}^\intercal = (\mathbf{t}_1, \ldots, \mathbf{t}_K),\\
&\widehat{\mathbf{S}} \leftarrow \mathbb{Z}_q^{W\times K},\ \ \widehat{\mathbf{E}} \leftarrow [-B_{\mathsf{flood}}, B_{\mathsf{flood}}]^{M\times K},\ \ \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}},\\
&\widetilde{\mathbf{C}} \leftarrow \mathbb{Z}_q^{K\times L},\ \ \mathbf{C}_{\mathbf{B}} \leftarrow \mathbb{Z}_q^{K\times mw},\\
&\widetilde{\mathbf{E}} \leftarrow \mathcal{D}^{K\times L}_{\mathbb{Z},\widetilde{\sigma}},\ \ \mathbf{E}_{\mathbf{B}} \leftarrow \mathcal{D}^{K\times mw}_{\mathbb{Z},\sigma_{\mathbf{B}}},\ \ \mathbf{E} \leftarrow \overline{\chi}^{m\times m\log q},\\
&\mathsf{aux} = (C, \mathrm{F}_1, \ldots, \mathrm{F}_M, M, K, \overline{\chi}, \overline{B}, \beta, \widetilde{\sigma}, \sigma_{\mathbf{B}}, B_{\mathsf{flood}}),
\end{aligned}
$$

the following two distributions are indistinguishable

$$
\begin{aligned}
D_0 &:= (\widetilde{\mathbf{A}}, \mathbf{B}, \mathbf{A}^*, \widehat{\mathbf{B}}, \mathbf{T}\widetilde{\mathbf{A}} + \widetilde{\mathbf{E}}, \mathbf{T}\mathbf{B} + \mathbf{E}_{\mathbf{B}}, \mathbf{B}_\tau^{-1}(\mathbf{P}), \mathsf{aux})\\
D_1 &:= (\widetilde{\mathbf{A}}, \mathbf{B}, \mathbf{A}^*, \widehat{\mathbf{B}}, \quad \widetilde{\mathbf{C}} \quad, \quad \mathbf{C}_{\mathbf{B}} \quad, \mathbf{B}_\tau^{-1}(\mathbf{P}), \mathsf{aux})
\end{aligned}
\tag{50}
$$

The rationale for security of the above is heuristic, and derived from the conjectured security of the "fixed bit" evasive LWE assumption. Essentially the assumption performs computational flooding by generating a flooding term using a well chosen PRF and uses ideas of modulus reduction discussed before to heuristically ensure that there are no exploitable dependencies between the error being flooded and the error used to perform the flooding.

Parameters.

Setting	Constraint/explanation
$\beta = q/8$	$\beta \leq q/8$
$\overline{B} < \beta/((\alpha+1)\cdot 2^{2\lambda})$	$\overline{B}$ is LWE error. $\beta_0 = \alpha\overline{B}$. $\beta \geq \beta_0 \cdot 2^{\lambda}$. For this setting, β floods B_{flood}, i.e. $\mathbf{E}^*$ floods $\widehat{\mathbf{E}}$.
$\beta_0 = \alpha\overline{B}$	$\beta_0 = \alpha\overline{B}$
$B_{\mathsf{flood}} = (\beta_0 + \overline{B})2^{\lambda}$	$B_{\mathsf{flood}} = (\beta_0 + \overline{B})2^{\lambda}$
$\sigma_{\mathbf{B}}, \widetilde{\sigma}$ are LWE noises $\bar{\chi}$ is $\bar{B}$ bounded distribution.	

Lemma 8.6. Assuming Conjecture 8.4 and subexponential LWE, there exists an $i\mathcal{O}$.

Proof. The lemma follows from results in [DQV+21] that shows following series of implications: a δ-succinct weak SLS implies δ–succinct (strong) SLS (Theorem 3.20) which in turn implies succinct randomized encoding (SRE) (Theorem 3.21) Finally, the proof completes by invoking Theorem 3.22 which says that assuming subexponential SRE, there exists an $i\mathcal{O}$. □

Lemma 8.7. Assuming Conjecture 8.5 and subexponential LWE, there exists an $i\mathcal{O}$.

Proof. The proof follows in two steps: (i) observing that assuming Conjecture 8.5 our construction of weak SLS satisfies weak security (weak β_0 flooding), (ii) weak SLS implies $i\mathcal{O}$ from the proof of lemma 8.6. We now prove Step (i). For this, we first observe that to prove weak SLS security (Equation (10)), we need to prove Equation (51).

$$
\begin{aligned}
D_0 &:= \begin{pmatrix} C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params}, \left\{\mathbf{c}^{\mathsf{T}}_{\mathbf{B},i}, \widehat{\mathsf{sd}_i}, \mathbf{c}^{\mathsf{T}}_{\mathsf{sd},i}, \mathbf{c}^{\mathsf{T}}_i,\right\}_{i\in[K]}, \\ \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}), \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} \end{pmatrix} \\
\approx_c \quad D_1 &:= \begin{pmatrix} C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params}, \left\{\mathbf{c}^{\mathsf{T}}_{\mathbf{B},i}, \widehat{\mathsf{sd}_i}, \mathbf{c}^{\mathsf{T}}_{\mathsf{sd},i}, \mathbf{c}^{\mathsf{T}}_i,\right\}_{i\in[K]}, \\ \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}) + \widehat{\mathbf{E}}, \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - \mathbf{G} \end{pmatrix}
\end{aligned} \tag{51}
$$

where in both D_0 and D_1 for all $i \in [K]$, $\mathbf{c}^{\mathsf{T}}_{\mathbf{B},i} = \mathbf{t}_i^{\mathsf{T}}\mathbf{B} + \mathbf{e}^{\mathsf{T}}_{\mathbf{B},i}, \widehat{\mathsf{sd}_i} = \mathbf{A}_{\mathsf{fhe},i}\mathbf{R}_i - \mathsf{sd}_i \otimes \mathbf{G}, \mathbf{c}^{\mathsf{T}}_{\mathsf{sd},i} = \mathbf{t}_i^{\mathsf{T}}(\mathbf{A}_{\mathsf{sd}} - (1, \mathsf{bits}(\widehat{\mathsf{sd}_i})) \otimes \mathbf{G}) + \mathbf{e}^{\mathsf{T}}_{\mathsf{sd},i}, \mathbf{c}^{\mathsf{T}}_i = \mathbf{t}_i^{\mathsf{T}}\mathbf{A} + \mathbf{e}^{\mathsf{T}}_i + ((\mathbf{S}^*[\cdot, i])^{\mathsf{T}} \otimes \mathbf{g}^{\mathsf{T}})$ and
$\mathbf{A}_{\mathsf{fhe},i} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{a}^{\mathsf{T}}_{\mathsf{fhe},i} = \bar{\mathbf{t}}_i^{\mathsf{T}}\bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}^{\mathsf{T}}_{\mathsf{fhe},i} \end{pmatrix}$.

We prove Equation (51) using a sequence of hybrids $\mathsf{Hyb}_0, \ldots, \mathsf{Hyb}_{12}$ and prove that $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1 \approx \ldots \approx \mathsf{Hyb}_{12}$, where Hyb_0 is the D_0 distribution and Hyb_{12} is the D_1 distribution of Equation (51).

Hyb_0**.** This is the D_0 distribution.

Hyb_1**.** This is the same as Hyb_0 except that we sample $\mathbf{C} \leftarrow \mathbb{Z}_q^{M\times M\log q}$. $\mathsf{Hyb}_0 \approx_c \mathsf{Hyb}_1$ by a straightforward reduction to LWE. This is because $\mathbf{A}^* \leftarrow \mathbb{Z}_q^{M\times W}$, $\mathbf{R}$ is not used anywhere else and $\mathbf{E} \leftarrow \overline{\chi}^{M\times M\log q}$ where $\overline{\chi}$ is $\overline{B}$ bounded.

Hyb_2**.** This is the same as Hyb_1 except that we compute for all $i \in [K]$, $\mathbf{c}^{\mathsf{T}}_{\mathbf{B},i} \leftarrow \mathbb{Z}_q^{1\times mw}, \mathbf{a}^{\mathsf{T}}_{\mathsf{fhe},i} \leftarrow \mathbb{Z}_q^{1\times m}, \mathbf{c}^{\mathsf{T}}_{\mathsf{sd},i} \leftarrow \mathbb{Z}_q^{1\times(L_{\mathsf{sd}}+1)m}, \widehat{\mathbf{c}}^{\mathsf{T}}_i \leftarrow \mathbb{Z}_q^{1\times W\log q}$. Then we set $\mathbf{A}_{\mathsf{fhe},i} = \begin{pmatrix} \overline{\mathbf{A}}_{\mathsf{fhe},i} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{a}^{\mathsf{T}}_{\mathsf{fhe},i} \end{pmatrix}$ and

$\mathbf{c}_i^\intercal = \widehat{\mathbf{c}}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal)$. The rest of the components are computed as in Hyb_1. $\mathsf{Hyb}_1 \approx_c \mathsf{Hyb}_2$ by a straightforward reduction to Conjecture 8.5.

Hyb_3. This is the same as Hyb_2 except that we compute $\widehat{\mathsf{sd}_i} \leftarrow \mathbb{Z}_q^{(n+1)\times m\lambda}$ for all $i \in [K]$. $\mathsf{Hyb}_2 \approx \mathsf{Hyb}_3$ using leftover hash lemma. Since the proof is the same as proof of $\mathsf{Hyb}_2 \approx \mathsf{Hyb}_3$ in proof of precondition as in Section 5.1, we skip the indistinguishability argument.

Hyb_4. This is the same as Hyb_3 except that we compute $\mathbf{c}_i^\intercal \leftarrow \mathbb{Z}_q^{1\times W\log q}$ for all $i \in [K]$. Since, $\widehat{\mathbf{c}}_i^\intercal \leftarrow \mathbb{Z}_q^{1\times W\log q}$ and $\widehat{\mathbf{c}}_i^\intercal$ is not used anywhere else, $\mathbf{c}_i^\intercal \leftarrow \mathbb{Z}_q^{1\times W\log q}$. Hence, $\mathsf{Hyb}_3 \approx \mathsf{Hyb}_4$.
At this point, we restate the distribution as in Hyb_4 for clarity.

$$D_{\mathsf{Hyb}_4} := \left(C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params}, \left\{ \begin{array}{c} \mathbf{c}_{\mathbf{B},i}^\intercal \leftarrow \mathbb{Z}_q^{1\times mw}, \widehat{\mathsf{sd}_i} \leftarrow \mathbb{Z}_q^{(n+1)\times m\lambda}, \\ \mathbf{c}_{\mathsf{sd},i}^\intercal \leftarrow \mathbb{Z}_q^{1\times (L_{\mathsf{sd}}+1)m}, \mathbf{c}_i^\intercal \leftarrow \mathbb{Z}_q^{1\times W\log q}, \end{array} \right\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}), \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}}, \mathbf{C} \leftarrow \mathbb{Z}_q^{M\times M\log q} \right)$$

Hyb_5. This is the same as Hyb_4 except that instead of computing each element of $\mathbf{E}^*$ as $\mathsf{PRF}(\mathsf{sd}_i, j)$ for all $i \in [K], j \in [M]$, we sample $\mathbf{U}^* \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_{\mathrm{F}}}^{M\times K}$. The indistinguishability between Hyb_4 and Hyb_5 follows from the PRF security. Hence, we get the following distribution.

$$D_{\mathsf{Hyb}_5} := \left(C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params}, \left\{ \begin{array}{c} \mathbf{c}_{\mathbf{B},i}^\intercal \leftarrow \mathbb{Z}_q^{1\times mw}, \widehat{\mathsf{sd}_i} \leftarrow \mathbb{Z}_q^{(n+1)\times m\lambda}, \\ \mathbf{c}_{\mathsf{sd},i}^\intercal \leftarrow \mathbb{Z}_q^{1\times (L_{\mathsf{sd}}+1)m}, \mathbf{c}_i^\intercal \leftarrow \mathbb{Z}_q^{1\times W\log q}, \end{array} \right\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*, \mathbf{U}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}), \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}}, \mathbf{C} \leftarrow \mathbb{Z}_q^{M\times M\log q} \right)$$

Hyb_6. This is the same as Hyb_5 except that we add $\widehat{\mathbf{E}}$ to $\mathbf{U}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}})$. Since, $\beta > (\beta_0 + \overline{B})2^{3\lambda} = 2^{2\lambda}B_{\mathsf{flood}}$, $\mathbf{U}^*$ floods $\widehat{\mathbf{E}}$. Therefore, $\mathbf{U}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}) \approx_s \mathbf{U}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}) + \widehat{\mathbf{E}}$. Hence, $\mathsf{Hyb}_5 \approx \mathsf{Hyb}_6$ by noise flooding.

Hyb_7. This is the same as Hyb_6 except that we undo the changes made in Hyb_5. We compute each element of $\mathbf{E}^*$ as $\mathsf{PRF}(\mathsf{sd}_i, j)$ for all $i \in [K], j \in [M]$. The indistinguishability between Hyb_6 and Hyb_7 follows from the PRF security.

Hyb_8. This is the same as Hyb_7 except that we undo the changes made in Hyb_4. We compute $\mathbf{c}_i^\intercal = \widehat{\mathbf{c}}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal)$ for all $i \in [K]$. Since, $\widehat{\mathbf{c}}_i^\intercal \leftarrow \mathbb{Z}_q^{1\times W\log q}$ and $\widehat{\mathbf{c}}_i^\intercal$ is not used anywhere else, $\mathbf{c}_i^\intercal = \widehat{\mathbf{c}}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal)$ is also uniformly distributed in $\mathbb{Z}_q^{1\times W\log q}$. Hence, $\mathsf{Hyb}_7 \approx \mathsf{Hyb}_8$.

Hyb_9. This is the same as Hyb_8 except that we undo the changes made in Hyb_3. Here we compute $\widehat{\mathsf{sd}_i} = \mathbf{A}_{\mathsf{fhe},i}\mathbf{R}_i - \mathsf{sd}_i \otimes \mathbf{G}$ where $\mathbf{A}_{\mathsf{fhe},i} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$ for all $i \in [K]$. We skip the indistinguishability argument as this is the same as $\mathsf{Hyb}_3 \approx \mathsf{Hyb}_2$.

Hyb_{10}. This is the same as Hyb_9 except that we undo the changes made in Hyb_2. Here we compute for all $i \in [K]$, $\mathbf{c}_{\mathbf{B},i}^\intercal = \mathbf{t}_i^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B},i}^\intercal, \mathbf{A}_{\mathsf{fhe},i} = \bar{\mathbf{t}}_i^\intercal\bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe},i}^\intercal, \mathbf{c}_{\mathsf{sd},i}^\intercal = \mathbf{t}_i^\intercal(\mathbf{A}_{\mathsf{sd}} - (1, \mathsf{bits}(\widehat{\mathsf{sd}_i})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{sd},i}^\intercal, \mathbf{c}_i^\intercal = \mathbf{t}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal)$. $\mathsf{Hyb}_9 \approx_c \mathsf{Hyb}_{10}$ assuming Conjecture 8.5. Hence, we get the following distribution.

$$D_{\mathsf{Hyb}_{10}} := \left(C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params}, \left\{ \begin{array}{r} \mathbf{c}_{\mathbf{B},i}^\intercal = \mathbf{t}_i^\intercal\mathbf{B} + \mathbf{e}_{\mathbf{B},i}^\intercal, \widehat{\mathsf{sd}_i} = \mathbf{A}_{\mathsf{fhe},i}\mathbf{R}_i - \mathsf{sd}_i \otimes \mathbf{G}, \\ \mathbf{c}_{\mathsf{sd},i}^\intercal = \mathbf{t}_i^\intercal(\mathbf{A}_{\mathsf{sd}} - (1, \mathsf{bits}(\widehat{\mathsf{sd}_i})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{sd},i}^\intercal, \\ \mathbf{c}_i^\intercal = \mathbf{t}_i^\intercal\mathbf{A} + \mathbf{e}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal), \end{array} \right\}_{i\in[K]}, \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}) + \widehat{\mathbf{E}}, \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}}, \mathbf{C} \leftarrow \mathbb{Z}_q^{M\times M\log q} \right)$$

where $\mathbf{A}_{\mathsf{fhe},i} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m} \\ \bar{\mathbf{t}}_i^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe},i}^\intercal \end{pmatrix}$.

Hyb_{11}. This is the same as Hyb_{10} except that we subtract $\mathbf{G}$ from $\mathbf{C}$. $\mathsf{Hyb}_{10} \approx \mathsf{Hyb}_{11}$ as subtracting $\mathbf{G}$ which is independent term from $\mathbf{C}$, does not make the task of distinguishing any easier.

Hyb_{12}. This is the same as Hyb_{11} except that we compute $\mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - \mathbf{G}$. $\mathsf{Hyb}_{11} \approx \mathsf{Hyb}_{12}$ using a straightforward reduction to LWE. Hence, we get the following distribution.

$$D_{\mathsf{Hyb}_{12}} := \left(\begin{array}{c} C, \mathbf{A}, \mathbf{A}_{\mathsf{sd}}, \mathsf{params}, \left\{ \begin{array}{r} \mathbf{c}_{\mathbf{B},i}^\intercal = \mathbf{t}_i^\intercal \mathbf{B} + \mathbf{e}_{\mathbf{B},i}^\intercal, \widehat{\mathsf{sd}_i} = \mathbf{A}_{\mathsf{fhe},i}\mathbf{R}_i - \mathsf{sd}_i \otimes \mathbf{G}, \\ \mathbf{c}_{\mathsf{sd},i}^\intercal = \mathbf{t}_i^\intercal(\mathbf{A}_{\mathsf{sd}} - (1, \mathsf{bits}(\widehat{\mathsf{sd}_i})) \otimes \mathbf{G}) + \mathbf{e}_{\mathsf{sd},i}^\intercal, \\ \mathbf{c}_i^\intercal = \mathbf{t}_i^\intercal \mathbf{A} + \mathbf{e}_i^\intercal + ((\mathbf{S}^*[\cdot, i])^\intercal \otimes \mathbf{g}^\intercal), \end{array} \right\}_{i\in[K]}, \\ \{\mathbf{k}_j\}_{j\in[M]}, \mathbf{A}^*, \mathbf{E}^* - \mathbf{E}\mathbf{G}^{-1}(\widehat{\mathbf{B}}) + \widehat{\mathbf{E}}, \widehat{\mathbf{B}} = \mathbf{A}^*\widehat{\mathbf{S}} + \widehat{\mathbf{E}}, \mathbf{C} = \mathbf{A}^*\mathbf{R} + \mathbf{E} - \mathbf{G} \end{array} \right)$$

where $\mathbf{A}_{\mathsf{fhe},i} := \begin{pmatrix} \bar{\mathbf{A}}_{\mathsf{fhe}} \leftarrow \mathbb{Z}_q^{n\times m} \\ \bar{\mathbf{t}}_i^\intercal \bar{\mathbf{A}}_{\mathsf{fhe}} + \mathbf{e}_{\mathsf{fhe},i}^\intercal \end{pmatrix}$.

Note that $D_{\mathsf{Hyb}_{12}} = D_1$. Hence, the proof. □

9 Acknowledgments

The first and last author thank Rachel Lin for expressing concern about the applicability of "HJL-style" attacks [HJL21] on the construction in [AKY24a] during a talk by the first author about [AKY24a]. This was the starting point of the investigation that led us to develop the attack in Section 5.1. The first author also thanks Hoeteck Wee for helpful discussions about his rationale for introducing evasive LWE and for sharing his broad perspective on this area.

References

[ABB10a] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572. Springer, Heidelberg, May / June 2010. (Cited on page 20, 21.)

[ABB10b] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 98–115. Springer, Heidelberg, August 2010. (Cited on page 20.)

[ABD16] Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched ntru assumptions: Cryptanalysis of some fhe and graded encoding schemes. In *Annual International Cryptology Conference*, pages 153–178. Springer, 2016. (Cited on page 3.)

[Agr17] Shweta Agrawal. Stronger security for reusable garbled circuits, general definitions and attacks. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 3–35. Springer, Heidelberg, August 2017. (Cited on page 11.)

[AJ15] Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 308–326. Springer, Heidelberg, August 2015. (Cited on page 18, 26.)

[AKY24a] Shweta Agrawal, Simran Kumari, and Shota Yamada. Compact pseudorandom functional encryption from evasive LWE. Cryptology ePrint Archive, Paper 2024/1719, 2024. (Cited on page 1, 5, 7, 13, 15, 16, 18, 41, 47, 51, 69, 71, 72, 93.)

[AKY24b] Shweta Agrawal, Simran Kumari, and Shota Yamada. Attribute Based Encryption for Turing Machines from Lattices. In *Crypto*, 2024. (Cited on page 3, 11, 16.)

[AKY24c] Shweta Agrawal, Simran Kumari, and Shota Yamada. Pseudorandom Multi-Input Functional Encryption and Applications, 2024. (Cited on page 1, 5, 72.)

[AP20] Shweta Agrawal and Alice Pellet-Mary. Indistinguishability obfuscation without maps: Attacks and fixes for noisy linear FE. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 110–140. Springer, Heidelberg, May 2020. (Cited on page 14.)

[ARYY23] Shweta Agrawal, Mélissa Rossi, Anshu Yadav, and Shota Yamada. Constant input attribute based (and predicate) encryption from evasive and tensor LWE. In *CRYPTO 2023, Part IV*, LNCS, pages 532–564. Springer, Heidelberg, August 2023. (Cited on page 11, 16, 22, 73, 74.)

[BBKK18] Boaz Barak, Zvika Brakerski, Ilan Komargodski, and Pravesh K Kothari. Limits on low-degree pseudorandom generators (or: Sum-of-squares meets program obfuscation). In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37*, pages 649–679. Springer, 2018. (Cited on page 74.)

[BDGM20] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Factoring and pairings are not necessary for io: Circular-secure lwe suffices. *Cryptology ePrint Archive*, 2020. (Cited on page 14.)

[BDJ+24] Pedro Branco, Nico Döttling, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, Spencer Peters, and Vinod Vaikuntanathan. Pseudorandom obfuscation and applications. Cryptology ePrint Archive, Paper 2024/1742, 2024. (Cited on page 1, 5, 10, 13, 14, 19, 50, 51, 53, 58, 63, 68, 69, 72.)

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 1–18. Springer, Heidelberg, August 2001. (Cited on page 3, 13, 72.)

[BHJ+19] Boaz Barak, Samuel B Hopkins, Aayush Jain, Pravesh Kothari, and Amit Sahai. Sum-of-squares meets program obfuscation, revisited. In *Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part I 38*, pages 226–250. Springer, 2019. (Cited on page 74.)

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 575–584. ACM Press, June 2013. (Cited on page 20, 21.)

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 719–737. Springer, Heidelberg, April 2012. (Cited on page 10.)

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993. (Cited on page 3.)

[BTVW17] Zvika Brakerski, Rotem Tsabary, Vinod Vaikuntanathan, and Hoeteck Wee. Private constrained PRFs (and more) from LWE. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 264–302. Springer, Heidelberg, November 2017. (Cited on page 7, 24.)

[BUW24] Chris Brzuska, Akin Unal, and Ivy K. Y. Woo. Evasive LWE assumptions: Definitions, classes, and counterexamples. Cryptology ePrint Archive, Paper 2024/2000, 2024. (Cited on page 3, 12, 50, 68.)

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In Rafail Ostrovsky, editor, *52nd FOCS*, pages 97–106. IEEE Computer Society Press, October 2011. (Cited on page 3.)

[BV15] Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In Venkatesan Guruswami, editor, *56th FOCS*, pages 171–190. IEEE Computer Society Press, October 2015. (Cited on page 26.)

[BV18] Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. *Journal of the ACM*, 65(6):39:1–39:37, 2018. (Cited on page 18.)

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 559–585. Springer, Heidelberg, May 2016. (Cited on page 3.)

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, 2004. (Cited on page 3, 13, 72.)

[CHKP10] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 523–552. Springer, Heidelberg, May / June 2010. (Cited on page 20.)

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 3–12. Springer, Heidelberg, April 2015. (Cited on page 12.)

[CRV10] Ran Canetti, Guy N. Rothblum, and Mayank Varia. Obfuscation of hyperplane membership. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 72–89. Springer, Heidelberg, February 2010. (Cited on page 13.)

[CS97] Don Coppersmith and Adi Shamir. Lattice attacks on ntru. In *International conference on the theory and applications of cryptographic techniques*, pages 52–61. Springer, 1997. (Cited on page 3.)

[CVW18] Yilei Chen, Vinod Vaikuntanathan, and Hoeteck Wee. GGH15 beyond permutation branching programs: Proofs, attacks, and candidates. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 577–607. Springer, Heidelberg, August 2018. (Cited on page 12.)

[DQV+21] Lalita Devadas, Willy Quach, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Succinct lwe sampling, random polynomials, and obfuscation. In *Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part II 19*, pages 256–287. Springer, 2021. (Cited on page 15, 24, 26, 74, 91.)

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009. (Cited on page 3.)

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 1–17. Springer, Heidelberg, May 2013. (Cited on page 3.)

[GGH+16] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM Journal on Computing*, 45(3):882–929, 2016. (Cited on page 3.)

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 467–476, 2013. (Cited on page 19.)

[GKW17] Rishab Goyal, Venkata Koppula, and Brent Waters. Lockable obfuscation. In Chris Umans, editor, *58th FOCS*, pages 612–621. IEEE Computer Society Press, October 2017. (Cited on page 66.)

[GMM+16a] Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry. Secure obfuscation in a weak multilinear map model. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 241–268. Springer, Heidelberg, October / November 2016. (Cited on page 3.)

[GMM+16b] Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry. Secure obfuscation in a weak multilinear map model. In *Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II 14*, pages 241–268. Springer, 2016. (Cited on page 14.)

[GP21] Romain Gay and Rafael Pass. Indistinguishability obfuscation from circular security. In Samir Khuller and Virginia Vassilevska Williams, editors, *53rd ACM STOC*, pages 736–749. ACM Press, June 2021. (Cited on page 14, 75.)

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008. (Cited on page 20.)

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 75–92. Springer, Heidelberg, August 2013. (Cited on page 3, 23.)

[GVW12] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption with bounded collusions via multi-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 162–179. Springer, Heidelberg, August 2012. (Cited on page 69.)

[HJL21] Sam Hopkins, Aayush Jain, and Huijia Lin. Counterexamples to new circular security assumptions underlying io. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II 41*, pages 673–700. Springer, 2021. (Cited on page 9, 12, 27, 75, 93.)

[HLL23] Yao-Ching Hsieh, Huijia Lin, and Ji Luo. Attribute-based encryption for circuits of unbounded depth from lattices. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 415–434. IEEE, 2023. (Cited on page 1, 3, 4, 7, 9, 11, 13, 16, 21, 23, 24, 26, 27, 31, 71.)

[IK02] Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In *Automata, Languages and Programming: 29th International Colloquium, ICALP 2002 Málaga, Spain, July 8–13, 2002 Proceedings 29*, pages 244–256. Springer, 2002. (Cited on page 69.)

[JLLS23] Aayush Jain, Huijia Lin, Paul Lou, and Amit Sahai. Polynomial-time cryptanalysis of the subspace flooding assumption for post-quantum i o. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 205–235. Springer, 2023. (Cited on page 74.)

[JLS21] Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from well-founded assumptions. In Samir Khuller and Virginia Vassilevska Williams, editors, *53rd ACM STOC*, pages 60–73. ACM Press, June 2021. (Cited on page 3, 4.)

[JLS22] Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from LPN over $\mathbb{F}_p$, DLIN, and PRGs in NC^0. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 670–699. Springer, Heidelberg, May / June 2022. (Cited on page 69.)

[KF17] Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched ntru parameters. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–26. Springer, 2017. (Cited on page 3.)

[LPST16] Huijia Lin, Rafael Pass, Karn Seth, and Sidharth Telang. Output-compressing randomized encodings and applications. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 96–124. Springer, Heidelberg, January 2016. (Cited on page 26.)

[LV17] Alex Lombardi and Vinod Vaikuntanathan. Minimizing the complexity of goldreich's pseudorandom generator. *Cryptology ePrint Archive*, 2017. (Cited on page 74.)

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 738–755. Springer, Heidelberg, April 2012. (Cited on page 20.)

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, Heidelberg, April 2012. (Cited on page 20.)

[MPV24a] Surya Mathialagan, Spencer Peters, and Vinod Vaikuntanathan. Adaptively sound zero-knowledge snarks for up. In *Annual International Cryptology Conference*, pages 38–71. Springer, 2024. (Cited on page 3.)

[MPV24b] Surya Mathialagan, Spencer Peters, and Vinod Vaikuntanathan. Adaptively sound zero-knowledge snarks for up. In *Advances in Cryptology – CRYPTO 2024: 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2024, Proceedings, Part X*, page 38–71, Berlin, Heidelberg, 2024. Springer-Verlag. (Cited on page 50.)

[MSZ16] Eric Miles, Amit Sahai, and Mark Zhandry. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 629–658. Springer, Heidelberg, August 2016. (Cited on page 12.)

[PMS21] Alice Pellet-Mary and Damien Stehlé. On the hardness of the ntru problem. In *Advances in Cryptology–ASIACRYPT*, pages 3–35. Springer, 2021. (Cited on page 3.)

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 145–166. Springer, Heidelberg, March 2006. (Cited on page 20.)

[PW11] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. *SIAM Journal on Computing*, 40(6):1803–1844, 2011. (Cited on page 8.)

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, 2009. (Cited on page 8, 21.)

[Tsa22] Rotem Tsabary. Candidate witness encryption from lattice techniques. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 535–559. Springer, Heidelberg, August 2022. (Cited on page 3, 4, 11, 12, 16.)

[Val76] Leslie G. Valiant. Universal circuits (preliminary report). In *Proceedings of the Eighth Annual ACM Symposium on Theory of Computing*, STOC '76, 1976. (Cited on page 69.)

[VWW22] Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Witness encryption and null-IO from evasive LWE. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part I*, volume 13791 of *LNCS*, pages 195–221. Springer, Heidelberg, December 2022. (Cited on page 3, 11, 16.)

[Wee05] Hoeteck Wee. On obfuscating point functions. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 523–532. ACM Press, May 2005. (Cited on page 13.)

[Wee22] Hoeteck Wee. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 217–241. Springer, Heidelberg, May / June 2022. (Cited on page 3, 4, 5, 6, 11, 12, 13, 16, 22, 69.)

[WW21] Hoeteck Wee and Daniel Wichs. Candidate obfuscation via oblivious LWE sampling. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part III*, volume 12698 of *LNCS*, pages 127–156. Springer, Heidelberg, October 2021. (Cited on page 14.)

[WW24] Brent Waters and Daniel Wichs. Adaptively secure attribute-based encryption from witness encryption. In *Theory of Cryptography Conference*, pages 65–90. Springer, 2024. (Cited on page 3.)

[WWW22a] Brent Waters, Hoeteck Wee, and David J Wu. Multi-authority abe from lattices without random oracles. In *Theory of Cryptography Conference*, pages 651–679. Springer, 2022. (Cited on page 3.)

[WWW22b] Brent Waters, Hoeteck Wee, and David J. Wu. Multi-authority ABE from lattices without random oracles. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 651–679. Springer, Heidelberg, November 2022. (Cited on page 21.)

[WZ17] Daniel Wichs and Giorgos Zirdelis. Obfuscating compute-and-compare programs under LWE. In Chris Umans, editor, *58th FOCS*, pages 600–611. IEEE Computer Society Press, October 2017. (Cited on page 66.)