Deniable Fully Homomorphic Encryption from LWE

Shweta Agrawal, Shafi Goldwasser, Saleet Mossel

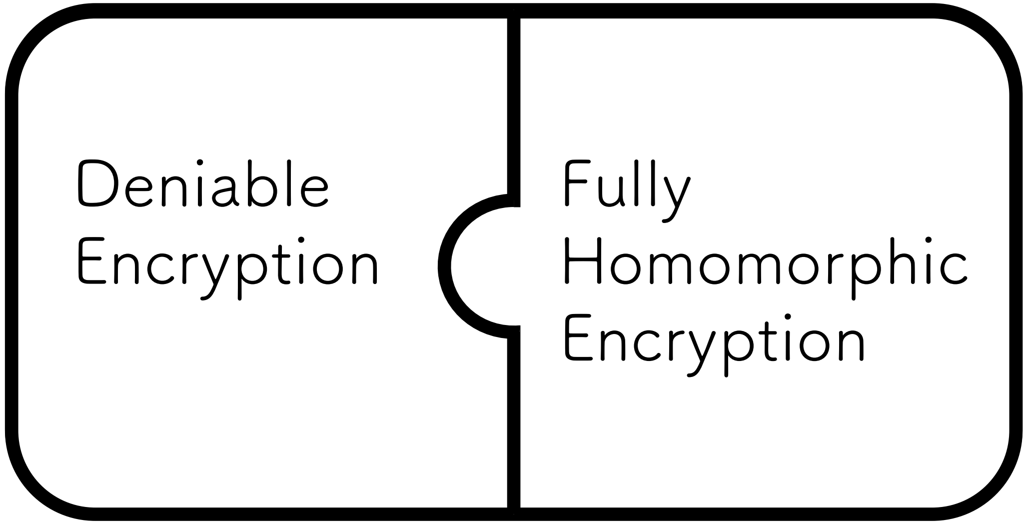
Crypto, 2021 (To appear)

Deniable Fully Homomorphic Encryption from LWE

Shweta Agrawal, Shafi Goldwasser, Saleet Mossel

Crypto, 2021 (To appear)

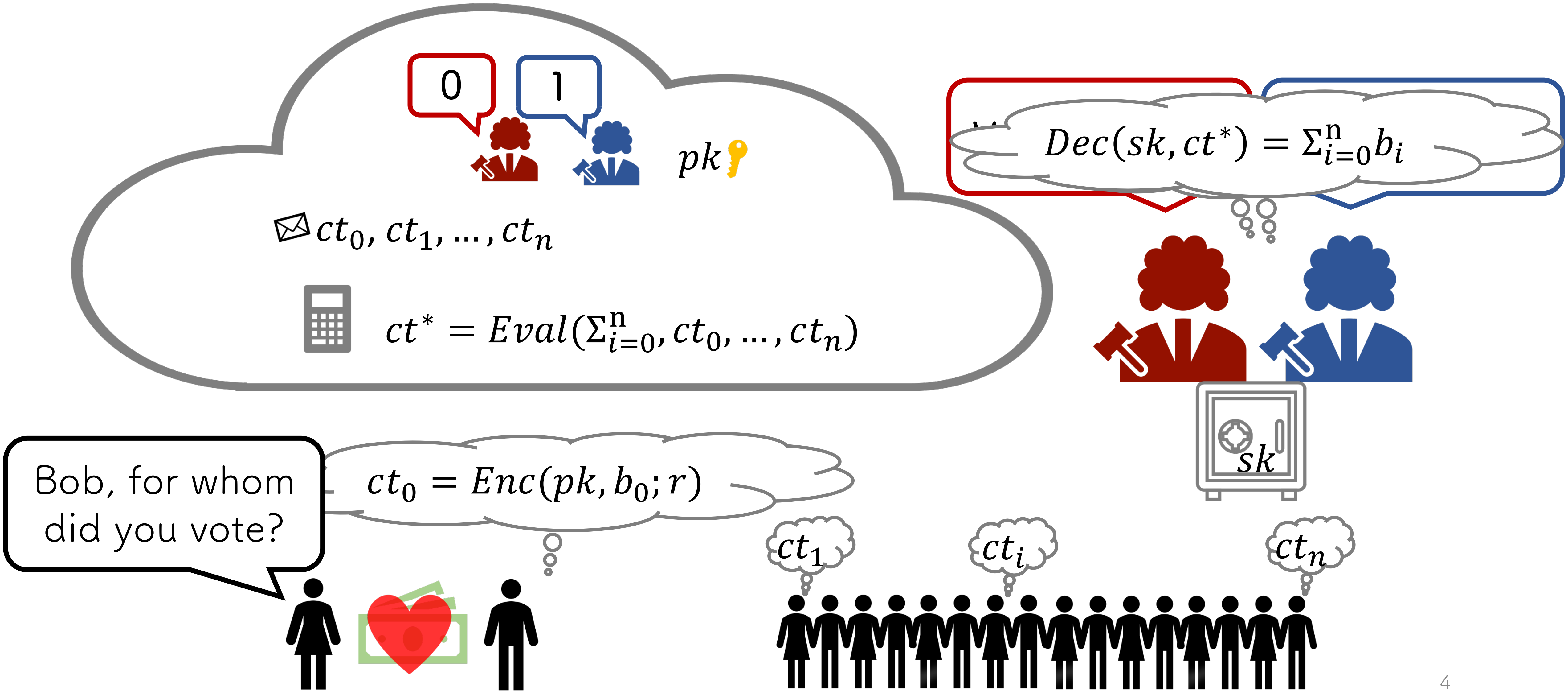
Most slides by Saleet Mossel



Deniable FHE

The notion of Deniable FHE

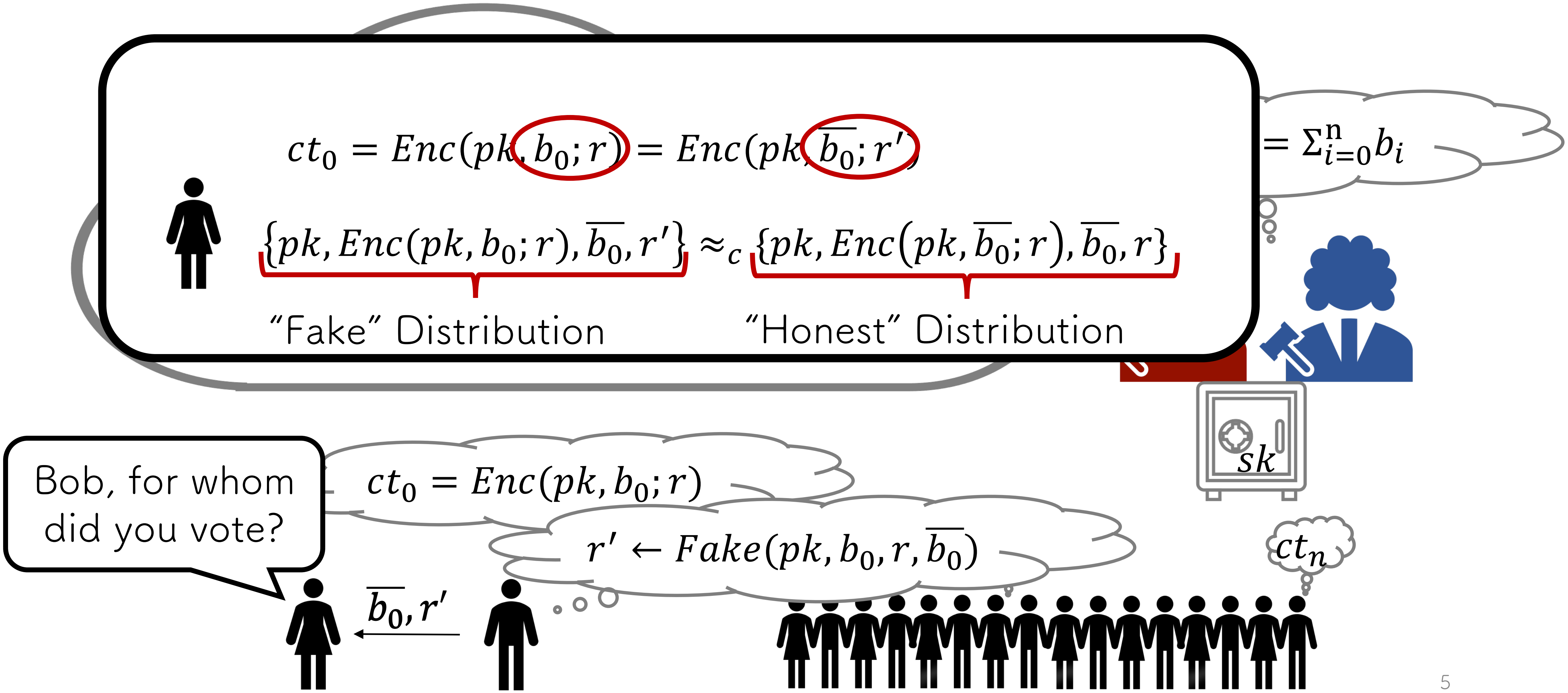
Deniable FHE



Deniable FHE

$$ct_0 = Enc(pk, b_0; r) = Enc(pk, \overline{b_0}; r')$$

$$\underbrace{\{pk, Enc(pk, b_0; r), \overline{b_0}, r'\}}_{\text{“Fake” Distribution}} \approx_c \underbrace{\{pk, Enc\left(pk, \overline{b_0}; r\right), \overline{b_0}, r\}}_{\text{“Honest” Distribution}}$$



Elections require Deniability & FHE

- Benefit of Deniable Encryption in Elections:
  - Honest Participation

- Benefit of Fully Homomorphic Encryption in Elections:
  - Homomorphically compute the voting result

Any data-driven algorithm

Store Encrypted Data

Natural upgrade for all DE apps!

Deniable Encryption

- Introduced by **Canetti, Dwork, Naor and Ostrovsky 1997**
  - construction from trapdoor permutations, unique SVP
  - size of ct is the inverse of the detection probability

- Weak Deniable Encryption
  - can also lie about the encryption algorithm (Enc, Denc)
  - construction with compact ct and negligible deniability

- Lower bound (Efficiency vs. Deniability)
  - It **seems inherent** that the length of ct grows with the inverse of the detection probability in "separable" constructions.

- A significant step forward [SW14]
  - construction from iO and OWF
  - compact ct and negligible deniability

What does this mean given recent iO results?

Deniable Encryption

CDNO

- Based on TDP
- CT size inverse of detection prob

SW

- Based on iO
- CT size indpt of detection prob

1997

2014

In full model, nothing else known!

Our Results

- Notion of Deniable FHE (full and weak)
- Constructions based on Learning With Errors
- Compact ct : size does not depend on detection probability!
  - Our construction is separable (so not inherent)
  - Total encryption time grows with the inverse of the detection probability!
- Support large message space
  - All prior work encode large messages bit by bit
- Offline-Online Encryption
  - Online time independent of the detection probability

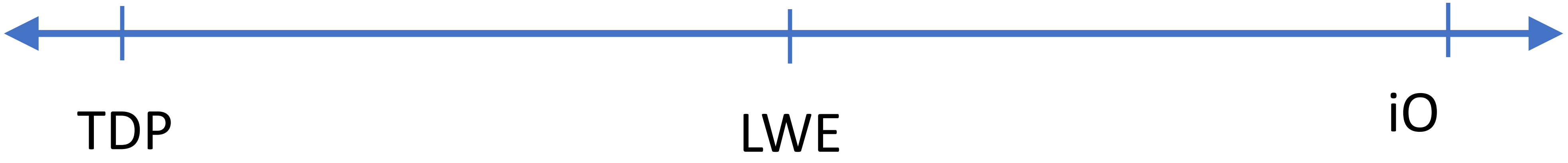
Our Results: Deniable Encryption

CDNO, 1997

CT size inverse of detection prob

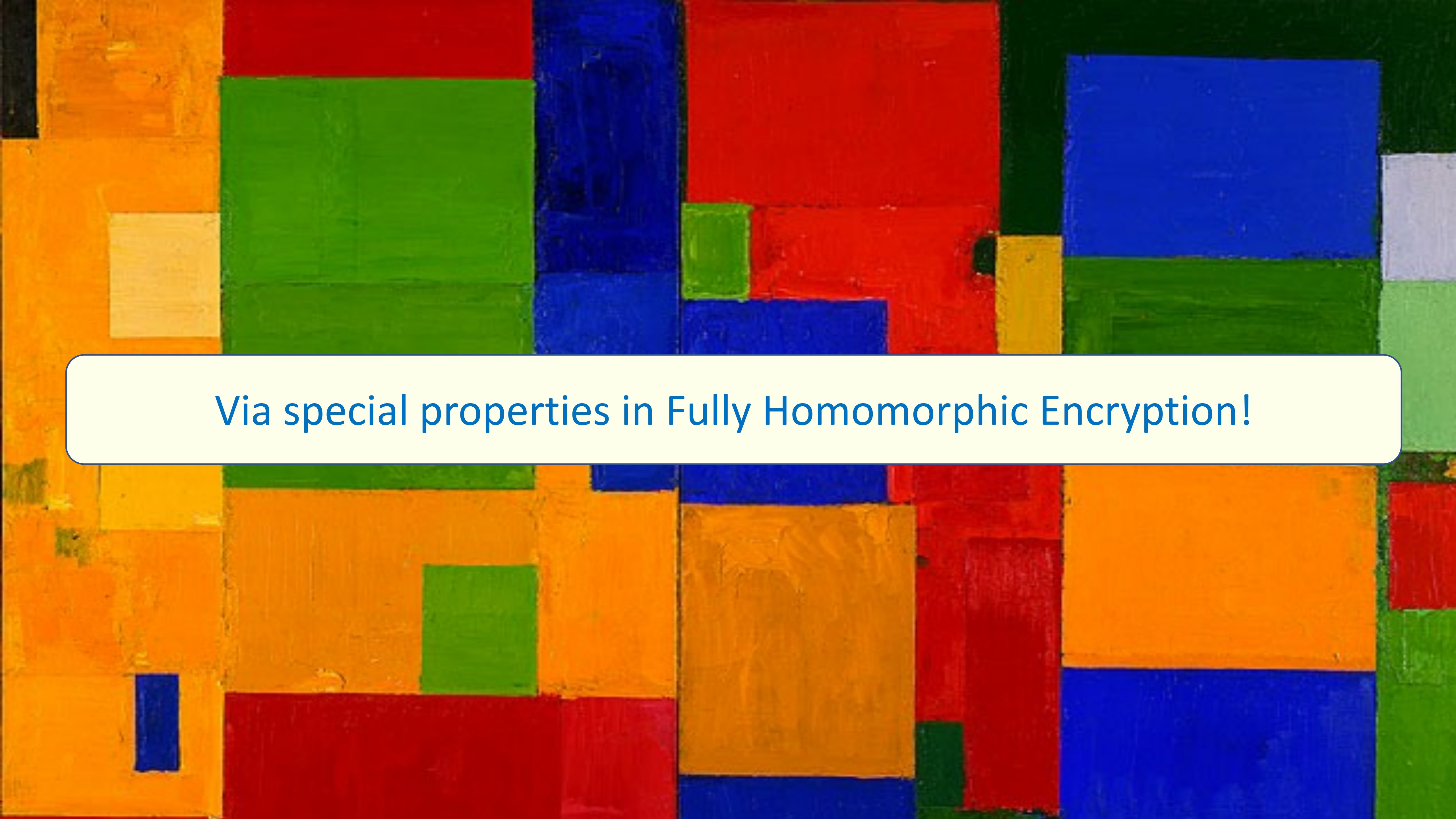
SW, 2014

CT size indpt of detection prob



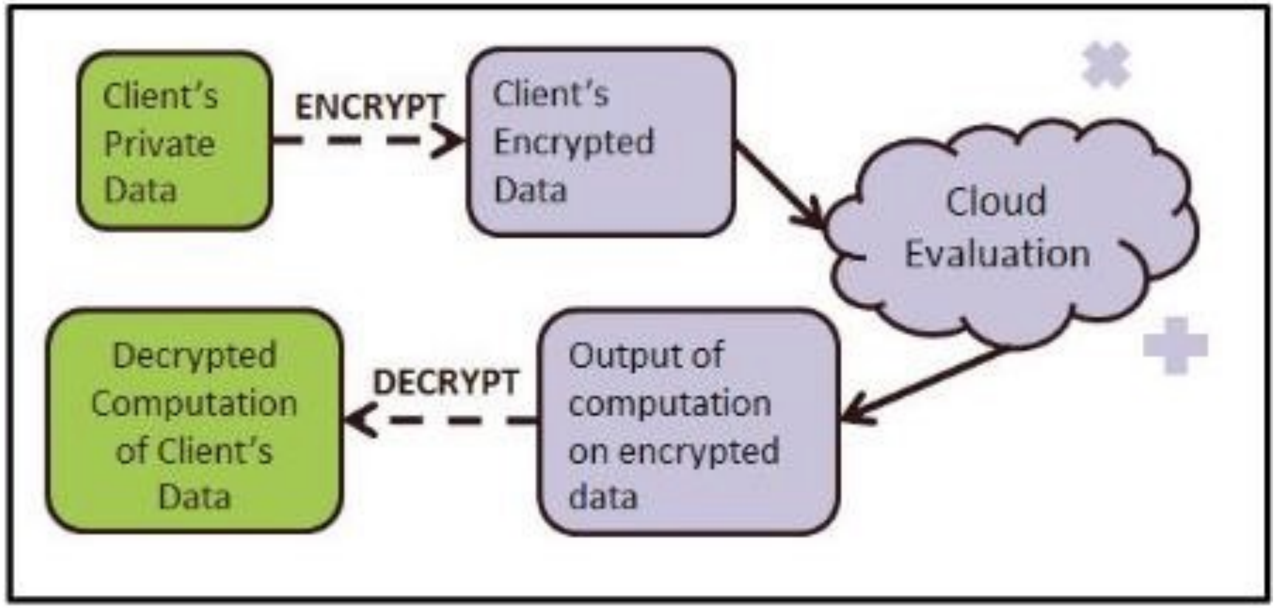
This Work

- CT size independent of detection prob
- (Offline) encryption time inverse of detection prob


Via special properties in Fully Homomorphic Encryption!

Fully Homomorphic Encryption

Can be built using LWE (BV11, BGV12, GSW13…)



Expressive Functionality: Supports arbitrary circuits

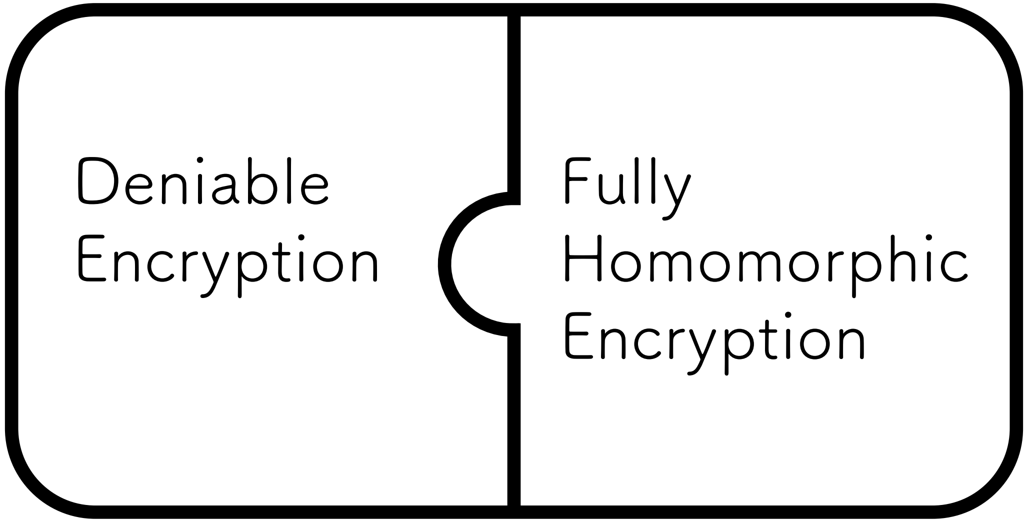
Compact ciphertext, independent of circuit size

Encryption and function evaluation commute!
Enc(f(x)) =* f(Enc(x))

* : roughly

Adding Deniability to the Mix

- A Deniable FHE scheme $(Gen, Enc, Eval, Dec, Fake)$
  - $(Gen, Enc, Eval, Dec)$ is an FHE scheme
  - $(Gen, Enc, Dec, Fake)$ is a Deniable Encryption scheme



Deniable FHE

A Deniable FHE scheme $(Gen, Enc, Eval, Dec, Fake)$ syntax

- $Gen \rightarrow (pk, sk)$
- $Enc(pk, m; r) = ct$
- $Dec(sk, ct) = b$
- $Eval(pk, f, ct_1, \dots, ct_k) = ct^*$
- $Fake(pk, b, r, \bar{b}) \rightarrow r'$

Deniable FHE

A Deniable FHE scheme $(Gen, Enc, Eval, Dec, Fake)$

1. Correctness
2. CPA-Security
3. Deniability
4. Compactness

Correctness versus Deniability

Correctness:

For every $\boldsymbol{f}$ and $\boldsymbol{m_1, \dots, m_k}$:

$$\mathbf{Pr}\left[\boldsymbol{Dec}\big(\boldsymbol{sk}, \boldsymbol{Eval}(\boldsymbol{pk}, \boldsymbol{f}, \boldsymbol{ct_1}, \dots, \boldsymbol{ct_k})\big) = \boldsymbol{f}(\boldsymbol{m_1}, \dots, \boldsymbol{m_k})\right] = \mathbf{1} - \boldsymbol{negl}$$

where $\boldsymbol{ct_i} \leftarrow \boldsymbol{Enc}(\boldsymbol{pk}, \boldsymbol{m_i})$ and $(\boldsymbol{pk}, \boldsymbol{sk}) \leftarrow \boldsymbol{Gen}$

Cannot simultaneously satisfy <u>perfect</u> correctness and <u>deniability</u>

$\delta(\lambda)$- Deniability

We consider (inverse) polynomial deniability

For every bit $\boldsymbol{b}$, and PPT adversary $\boldsymbol{A}$

detection probability

$$\left|\mathbf{Pr}\big[\boldsymbol{A}\underbrace{(\boldsymbol{pk},\boldsymbol{Enc}(\boldsymbol{pk},\boldsymbol{b};\boldsymbol{r}),\boldsymbol{b},}_{\text{“Honest” Distribution}}\boldsymbol{r})\big]-\mathbf{Pr}\big[\boldsymbol{A}\big(\underbrace{\boldsymbol{pk},\boldsymbol{Enc}(\boldsymbol{pk},\overline{\boldsymbol{b}};\boldsymbol{r}),\boldsymbol{b},\boldsymbol{r}'}_{\text{“Fake” Distribution}}\big)\big]\right|\leq\boldsymbol{\delta}(\boldsymbol{\lambda})$$

where $(\boldsymbol{pk},\boldsymbol{sk})\leftarrow\boldsymbol{Gen}$, $\boldsymbol{r}\leftarrow\{\mathbf{0},\mathbf{1}\}^{\ell'}$, and $\boldsymbol{r}'\leftarrow\boldsymbol{Fake}(\boldsymbol{pk},\overline{\boldsymbol{b}},\boldsymbol{r},\boldsymbol{b})$

Evaluation & Deniability Compactness

a) For every $\boldsymbol{f}$ and $\boldsymbol{m_1, \ldots, m_k}$:

$$|\boldsymbol{Eval}(\boldsymbol{pk}, \boldsymbol{f}, \boldsymbol{ct_1}, \ldots, \boldsymbol{ct_k})| \leq \boldsymbol{poly}$$

where $\boldsymbol{ct_i} \leftarrow \boldsymbol{Enc}(\boldsymbol{pk}, \boldsymbol{m_i})$ and $(\boldsymbol{pk}, \boldsymbol{sk}) \leftarrow \boldsymbol{Gen}$

Independent of k and the complexity of f

b) For every $\boldsymbol{m}$:

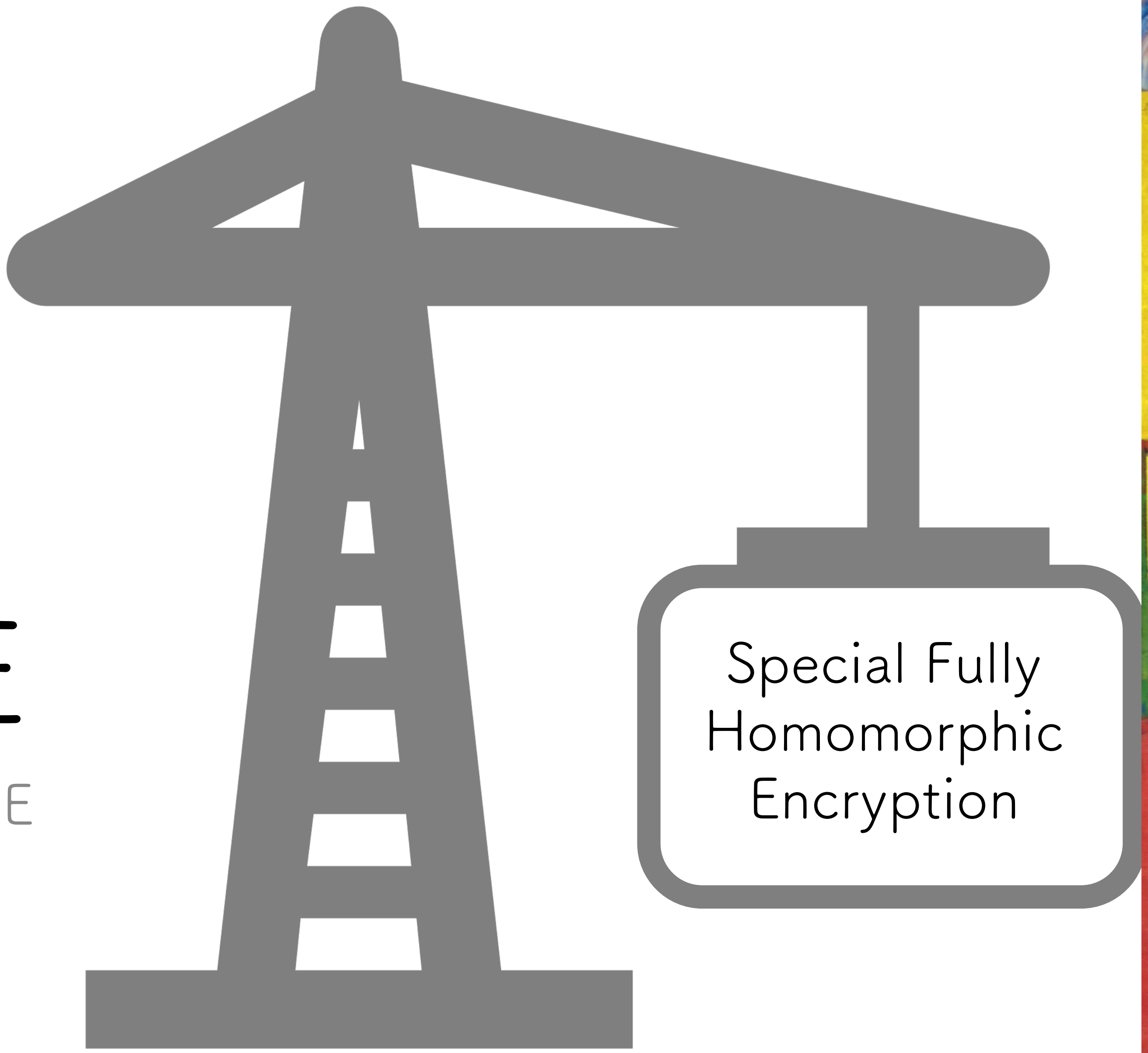
$$|\boldsymbol{Enc}(\boldsymbol{pk}, \boldsymbol{m})| \leq \boldsymbol{poly}$$

where $(\boldsymbol{pk}, \boldsymbol{sk}) \leftarrow \boldsymbol{Gen}$, regardless of the encryption running time

Independent of the detection probability

Deniable FHE

Our Construction of Deniable FHE



FHE from LWE: A Very Brief Recap

- All* known FHE schemes add noise in CT for security.
- Homomorphic evaluation of CTs ($\text{eval}(f, ct_1 \cdots ct_n)$) cause noise to grow
- Kills correctness after noise grows too much
- Limits number of homomorphic operations

How to keep going: Gentry's bootstrapping [Gen09]!

The Magic of Bootstrapping

- Assume that an FHE is powerful enough to support evaluation of its own decryption circuit Dec.

- By correctness of decryption, Dec(ct_x, sk) = x

$$\mathrm{Dec}\left(\boxed{x}, sk\right) = x$$

- Define circuit $\mathrm{Dec}_{ct}(sk) = \mathrm{Dec}(sk, ct)$
- By correctness of homomorphic evaluation, Eval(F, ct_x) = ct(F(x))

$$\mathrm{Eval}\left(\mathrm{Dec}_{ct}, \boxed{sk}\right) = \boxed{\mathrm{Dec}_{ct}(sk)} = \boxed{x}$$

The Magic of Bootstrapping

- Originally introduced to reduce noise in evaluated ciphertext

- Homomorphic evaluation of decryption
  - removes large old noise
  - adds small new noise (size small since decryption shallow)

This work: Oblivious Sampling of FHE ciphertexts!

The Magic of Bootstrapping

- Assume that decryption <u>always</u> outputs 0 or 1
  - even if input ct is not well formed

- Then, bootstrapping <u>always</u> outputs proper encryption of 0 or 1!

$$\mathrm{Eval}\left(\mathrm{Dec}_{ct}, \boxed{sk}\right) = \boxed{\mathrm{Dec}_{ct}(sk)} = \boxed{x}$$

Even if input “ct” is a random element in ciphertext space!

The Magic of Bootstrapping

- Assume that decryption <u>outputs 0 w.o.p for random input</u>

- Then, bootstrapping outputs <u>encryption of 0 w.o.p for random input</u>

$$\text{Eval}\left(\text{Dec}_{\text{rand}}, \boxed{\text{sk}}\right) = \boxed{\text{Dec}_{\text{rand}}(\text{sk})} = \boxed{0}$$

Given enc(sk), run dec homomorphically on random to generate encryption of 0 w.o.p!

But, wait a minute…

- Given encryption of 1, decryption outputs 1 w.o.p
- Encryption of 1 is indistinguishable from random!

$$\mathrm{Eval}\left(\mathrm{Dec}_{ct1},\ \boxed{sk}\right) = \boxed{\mathrm{Dec}_{ct1}(sk)} = \boxed{1}$$

- Can pretend as if ct1 = enc(1) is a random string

Pretend bootstrapping outputs enc(0) but actually enc(1)!

Can provide randomness R so it looks like Bootstrap(R) = enc(0) but actually enc(1)

OK… but why is this useful?

Leveraging our trick (binary msg space)

- Let $B(x) = Eval(pk, Dec_x, ct_{sk})$ the bootstrapping procedure
  - recall $Dec_x(sk) = Dec(sk, x)$

- Denote homomorphic addition (mod 2) as

$$Eval(pk, +, ct_a, ct_b) = ct_a \oplus ct_b$$

$B(R_i)$
$= Enc(x_i)$

$$B(R_1) \oplus \cdots \oplus B(R_n) = \text{Enc}\left(\text{Parity}\left(x_1, \ldots, x_n\right)\right)$$

Construction

Gen:

1. $(pk, sk) \leftarrow Gen$
2. $ct_{sk} \leftarrow Enc(pk, sk)$
3. Output $pk = (pk, ct_{sk}), sk = sk$

Construction

$rand = (x_1, \dots, x_n, \{R_i\}_{x_i=0}, \{r_i\}_{x_i=1})$

$Enc(pk, b)$:

1. Sample $x_1, \dots, x_n \leftarrow \{0,1\}$ s.t. $\sum_i x_i = b\ (mod\ 2)$
2. For $x_i = 0$, sample $R_i \leftarrow \mathcal{R}^\ell$
3. For $x_i = 1$, sample $r_i \leftarrow \{0,1\}^{\ell'}$ and set $R_i = Enc(pk, 1; r_i)$
4. Compute $ct = B(R_1) \oplus \cdots \oplus B(R_n)$
5. Output ct

$B(\mathcal{R}^\ell)$ is a valid encryption of 0 w.h.p

Construction

$rand = (x_1, \dots, x_n, \{R_i\}_{x_i=0}, \{r_i\}_{x_i=1})$

$Fake(pk, b, rand, \bar{b})$:

1. If $b = \bar{b}$, output $rand$
2. Sample $k \leftarrow [n]$ s.t. $x_k = 1$
3. Set $x'_k = 0$ and $R'_k = Enc(pk, 1; r_k)$
4. For $i \neq k$, set $R'_i = R_i$ and $r'_i = r_i$
5. Output $rand' = (x'_1, \dots, x'_n, \{R'_i\}_{x'_i=0}, \{r'_i\}_{x'_i=1})$

Pseudorandom Ciphertext

By pretending one ciphertext enc(1) is random, parity flipped!

Statistical distance from honest dist is 1/poly(n)

Construction

$Eval(pk, f, ct_1, \dots, ct_k)$:

1. Interpret ct_i as special FHE ciphertext ct_i
2. Output $Eval(pk, f, ct_1, \dots, ct_k)$

$Dec(dsk, ct)$:

1. Interpret ct as special FHE ciphertext ct
2. Output $Dec(sk, ct)$

As before!

Deniable FHE

Proof of Correctness, CPA-Security, Compactness, Deniability

Proof: Correctness

- The output is a ciphertext of the Special FHE.
- If with high probability $B(\mathcal{R}^\ell)$ is a valid encryption of 0, then with high probability $Enc(pk, b)$ is a valid encryption of b.

$Enc(pk, b)$:

1. Sample $x_1, \dots, x_n \leftarrow \{0,1\}$ s.t. $\sum_i x_i = b \ (mod\ 2)$
2. For $x_i = 0$, sample $R_i \leftarrow \mathcal{R}^\ell$
3. For $x_i = 1$, sample $r_i \leftarrow \{0,1\}^{\ell'}$ and set $R_i = Enc(pk, 1; r_i)$
4. Compute $ct = B(R_1) \oplus \cdots \oplus B(R_n)$
5. Output ct

1. Correctness

   For every $\boldsymbol{f}$ and $\boldsymbol{m_1, \dots, m_k}$:

   $$\mathbf{Pr}[\boldsymbol{Dec(sk, Eval(pk, f, ct_1, \dots, ct_k)) = f(m_1, \dots, m_k)}] = \mathbf{1} - \boldsymbol{negl}$$

   where $\boldsymbol{ct_i} \leftarrow \boldsymbol{Enc(pk, m_i)}$ and $\boldsymbol{(pk, sk)} \leftarrow \boldsymbol{Gen}$

Proof: CPA-Security

- The output is a ciphertext of the Special FHE.
- The public key is (pk, ct_{sk})
- If the special FHE is circular secure, then the scheme is secure.

2. CPA-Security

$$\{\boldsymbol{pk}, \boldsymbol{Enc}(\boldsymbol{pk}, \mathbf{0})\} \approx_c \{\boldsymbol{pk}, \boldsymbol{Enc}(\boldsymbol{pk}, \mathbf{1})\}$$

where $(\boldsymbol{pk}, \boldsymbol{sk}) \leftarrow \boldsymbol{Gen}$

Gen:

1. $(pk, sk) \leftarrow Gen$
2. $ct_{sk} \leftarrow Enc(pk, sk)$
3. Output $pk = (pk, ct_{sk}), sk = sk$

Proof: $\delta(\lambda)$-Deniability

- First, prove that $Enc(pk, \bar{b}; r) = Enc(pk, b, r')$.
- We can remove the ciphertext from A's input.
  - It is a function of A's input.
- Last, prove the distance is $\delta(\lambda)$

3. $\delta(\lambda)$-Deniability

For every bit $\boldsymbol{b}$, and PPT adversary $\boldsymbol{A}$

$$|\mathbf{Pr}[\boldsymbol{A}(\boldsymbol{pk}, \boldsymbol{b}, \boldsymbol{r})] - \mathbf{Pr}[\boldsymbol{A}(\boldsymbol{pk}, \boldsymbol{b}, \boldsymbol{r}')]| \leq \boldsymbol{\delta}(\boldsymbol{\lambda})$$

where $(\boldsymbol{pk}, \boldsymbol{sk}) \leftarrow \boldsymbol{Gen}$, $\boldsymbol{r} \leftarrow \{\mathbf{0}, \mathbf{1}\}^{\ell'}$, and $\boldsymbol{r}' \leftarrow \boldsymbol{Fake}(\boldsymbol{pk}, \bar{\boldsymbol{b}}, \boldsymbol{r}, \boldsymbol{b})$

Proof: $\delta(\lambda)$-Deniability

- Prove that $Enc(pk, \bar{b}; r) = Enc(pk, b, r')$
  - uniform r and $r' \leftarrow Fake(pk, \bar{b},$
- Real: $r = x_1, \dots, x_n, \{R_i\}_{x_i=0}, \{r_i\}$
  - r is uniform conditioned on $\sum x_i$
- Fake: $r' = x_1', \dots, x_n', \{R_i'\}_{x_i'=0}, \{r_i'\}_{x_i'=1}$
  - r' is equal to r except:
    - $x_k' = \overline{x_k} = 0$ and $R_k' = Enc(pk, 1; r_k)$

$Enc(pk, b)$:
1. Sample $x_1, \dots, x_n \leftarrow \{0,1\}$ s.t. $\sum_i x_i = b \ (mod\ 2)$
2. For $x_i = 0$, sample $R_i \leftarrow \mathcal{R}^{\ell}$
3. For $x_i = 1$, sample $r_i \leftarrow \{0,1\}^{\ell'}$ and set $R_i = Enc(pk, 1; r_i)$
4. Compute $ct = B(R_1) \oplus \cdots \oplus B(R_n)$
5. Output ct

$Fake(pk, b, rand, \bar{b})$:
1. If $b = \bar{b}$, output $rand$
2. Sample $k \leftarrow [n]$ s.t. $x_k = 1$
3. Set $x_k' = 0$ and $R_k' = Enc(pk, 1; r_k)$
4. For $i \neq k$, set $R_i' = R_i$ and $r_i' = r_i$
5. Output $rand' = (x_1', \dots, x_n', \{R_i'\}_{x_i'=0}, \{r_i'\}_{x_i'=1})$

$\sum x_i' = b \ (mod\ 2)$

Output is identical

Proof: $\delta(\lambda)$-Deniability

- Last, prove the distance is $\delta(\lambda)$

- If special FHE has **pseudorandom ciphertext**, then the following are computational indistinguishable

  - Fake $r' = x'_1, \dots, x'_n, \{R'_i\}_{x'_i=0}, \{r'_i\}_{x'_i=1}$ s.t.
    - $R'_k = Enc(pk, 1; r_k)$ and $r_k \leftarrow \{0,1\}^{\ell'}$

  - Mid $r' = x'_1, \dots, x'_n, \{R'_i\}_{x'_i=0}, \{r'_i\}_{x'_i=1}$ s.t.
    - $R'_k \leftarrow \mathcal{R}^{\ell}$

Proof: $\delta(\lambda)$-Deniability

- Last, prove the distance is $\delta(\lambda)$

set $n = \frac{1}{\delta(\lambda)^2}$

- The Statistical Distance of the following two distributions is $\frac{1}{\sqrt{n}}$
  - Mid $r' = x_1', \dots, x_n', \{R_i'\}_{x_i'=0}, \{r_i'\}_{x_i'=1}$ s.t.
    - Sample $x_1, \dots, x_n \leftarrow \{0,1\}$ such that $\sum x_i = \bar{b} \ (mod\ 2)$
    - Sample $k \leftarrow [n]$ such that $x_i = 1$
    - Set $x_k' = 0$ and for $i \neq \mathrm{k}$ set $x_i' = x_i$

$\mathrm{E}[\sum x_i] > \mathrm{E}[\sum x_i']$

  - Real $r = x_1, \dots, x_n, \{R_i\}_{x_i=0}, \{r_i\}_{x_i=1}$ s.t.
    - Sample $x_1, \dots, x_n \leftarrow \{0,1\}$ such that $\sum x_i = b \ (mod\ 2)$

Proof: Compactness

- The output is a ciphertext of the Special FHE.

4. Compactness

   a) For every $\boldsymbol{f}$ and $\boldsymbol{m_1, \dots, m_k}$:

   $$|\boldsymbol{Eval(pk, f, ct_1, \dots, ct_k)}| \le \boldsymbol{poly}$$

   Independent of k and the complexity of f

   where $\boldsymbol{ct_i} \leftarrow \boldsymbol{Enc(pk, m_i)}$ and $\boldsymbol{(pk, sk)} \leftarrow \boldsymbol{Gen}$

   b) For every $\boldsymbol{m}$:

   $$|\boldsymbol{Enc(pk, m)}| \le \boldsymbol{poly}$$

   Independent of the faking probability

   where $\boldsymbol{(pk, sk)} \leftarrow \boldsymbol{Gen}$, regardless of the encryption running time

Deniability Compactness from Evaluation Compactness!

Special FHE

Definition and Instantiation

Special FHE

Circular security

Pseudo-random CT

Det. eval and dec

$B(\mathcal{R}^{\ell})$ is a valid encryption of 0 w.h.p

Can be removed

Usually OK

Can be weakened whp to wnnp

Weaker Special FHE

1. Pseudorandom Ciphertext
2. Deterministic evaluation and decry
3. Decryption always outputs a valid mess and

Almost always the case

$$\mathbf{Pr}[\boldsymbol{Dec}(\boldsymbol{sk},\boldsymbol{R}) = \mathbf{0}] = \mathbf{1}/\boldsymbol{poly}$$

where $\boldsymbol{R} \leftarrow \mathcal{R}^{\ell}$ and $(\boldsymbol{pk},\boldsymbol{sk}) \leftarrow \boldsymbol{Gen}$

[BGV14] FHE satisfies all properties!

Instantiation of Special FHE

- In [BGV14] given the sk one can check if ct is well-formed
- We modify the decryption algorithm of [BGV14]:

If well-formed:
then, output $Dec(sk, ct)$,
else output 0

$$Dec(sk, ct) = \left[[\langle sk, ct \rangle]_q \right]_2$$

Ciphertexts:

$$[\langle sk, ct \rangle]_q = b + 2e$$

where $|e| < B$

Random elements:

$$[\langle sk, R \rangle]_q = b + 2e$$

where $\Pr[|e| < B] = \frac{B}{q}$

Set q to be super polynomial, then $\frac{B}{q}$ is negligible

Online-Offline Encryption

Bulk of the computation is independent of the message, and may be performed in an offline pre-processing phase.

$Enc(dpk, b)$:

1. Select $x_1, \ldots, x_n \leftarrow \{0,1\}$ s.t. $\sum_i x_i = b \ (mod\ 2)$
2. For $x_i = 0$, select $R_i \leftarrow \mathcal{R}^\ell$
3. For $x_i = 1$, select $r_i \leftarrow \{0,1\}^{\ell'}$ and set $R_i = Enc(pk, 1; r_i)$
4. Output $dct = B(R_1) \oplus \cdots \oplus B(R_n)$

n-1 computations of $B(R_i)$ can be done offline:
choose R_n depending on b and compute $B(R_n)$ online

Main Takeaway:
Evaluation compactness in FHE implies deniability compactness in DE!

Going Forward

- Compact CT ➔ compact encryption runtime?
  - Analogy to FE [LPST16,GKPVZ13]
- Technical barrier: unidirectional cheating
- Need: Invertible oblivious sampling with bias
  - SW construction may be viewed through this lens
- From LWE: can have oblivious sampling with bias (this work) or oblivious sampling with inversion but not both (so far).

Thank You

Images Credit: Hans Hoffman