CS6115: Structure versus Hardness in Cryptography Sept 23, 2021

Lecture 15 : Other Applications iO

Lecturer: *Shweta Agrawal* Scribe: *Aditya Balachander*

1 Introduction

In the previous lectures, we studied in detail Deniable Encryption scheme using Indistinguishability Obfuscation presented in [SW14]. In today's lecture, we will explore other applications of Indistinguishability Obfuscation. Specifically, we will see Public Key Encryption using Private Key Encryption and study it's security.

2 Public Key Encryption using Private Key Encryption

Now why would we want to do something like this? The main reason is that Private Key Encryption Schemes are very efficient in practice. So if via Indistinguishability Obfscation, we can build a Public Key Encryption Scheme using Private Key encryption, we can achieve a much more efficient Public Key Encryption Scheme.

2.1 The Public Key Encryption Scheme

Let PRG be a length doubling pseudo random generator that maps $\{0,1\}^\lambda$ to $\{0,1\}^{2\lambda}$. Here, our scheme encrypts for the message space $\mathcal{M} = \{0,1\}^\ell$. The Public Key Encryption Scheme $\mathrm{PKE} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ is defined by the following [SW14]:

- $\mathsf{KeyGen}(1^\lambda)$:
  - Sample F, a puncturable PRF that takes inputs of 2λ bits and outputs ℓ bits. And let K be it's key.
  - Construct a program SKE Encrypt:

    SKE Encrypt

    Constants: Punctured PRF key K
    Input: Message $m \in \{0,1\}^\ell$ and randomness $r \in \{0,1\}^\lambda$

    $P_{\mathrm{K}}(m, r) \to c$:
    1. $t = \mathrm{PRG}(r)$
    2. $c = (c_1 = t, c_2 = F_{\mathrm{K}}(t) \oplus m)$

  - The public key $\mathrm{PK} = i\mathcal{O}(P_{\mathrm{K}})$ is set to be an obfuscation of the program SKE Encrypt and the secret key SK is set to be key K.

- $\mathsf{Enc}(\mathrm{PK}, m)$: Sample $r \leftarrow \{0,1\}^\lambda$ and output $\mathrm{PK}(m, r)$.
- $\mathsf{Dec}(\mathrm{SK}, c = (c_1, c_2))$: The decryption algorithm outputs $m' = F_K(c_1) \oplus c_2$.

Here note that we are using Indistinguishability Obfuscation (iO) to obfuscate SKE Encrypt which is given as the public key. We are able to preserve the functionality of encryption without revealing the secret key due to the correctness of Indistinguishability Obfuscation.

2.2 Correctness

We shall prove that the PKE scheme will decrypt correctly. Running the encryption algorithm on message m and randomness r we get ciphertext,

$$c = (c_1 = t, c_2 = F_{\mathrm{K}}(t) \oplus m)$$

So running the decryption algorithm on the above mentioned ciphertext we have,

$$\begin{aligned} F_K(c_1) \oplus c_2 &= F_K(t) \oplus F_{\mathrm{K}}(t) \oplus m \\ &= m \end{aligned}$$

Thus proving the correctness of the scheme.

2.3 Security

Let us recall the IND-CPA Security in the context of our scheme. The game consists of two parties - the Challenger and the Adversary. The game proceeds as follows:

Challenger		**Adversary**
(PK, SK) = $\mathsf{KeyGen}(1^\lambda)$	$\xrightarrow{\quad \mathrm{PK} \quad}$	
	$\xleftarrow{\quad \mathrm{m_0, m_1} \quad}$	picks $m_0, m_1 \in \{0,1\}^\ell$
Chooses $b \in \{0,1\}$ at random	$\xrightarrow{\quad \mathrm{c_b^* = (c_1^* = t^*, c_2^* = F_K(t^*) \oplus m_b)} \quad}$	
	$\xleftarrow{\quad \mathrm{b^* \in \{0,1\}} \quad}$	
Adversary wins game if b = b*		

Our security requirements will be that the adversary does not win the above mentioned game with probability non-negligibly greater than $\frac{1}{2}$. To prove the security of this system, we use a hybrid argument [SW14]:

- Hyb_0 : The first hybrid is just the real world that is,
  1. $r^* \in \{0,1\}^\lambda$ is chosen at random and $t^* = \mathrm{PRG}(r^*)$
  2. K is chosen as key for the puncturable PRF.
  3. The public key PK given out is an obfuscation of the program SKE Encrypt.
  4. The attacker receives PK and then gives $m_0, m_1 \in \{0,1\}^\ell$ to the challenger.
  5. The challenge ciphertext is $c_b^* = (c_1^* = t^*, c_2^* = F_{\mathrm{K}}(t^*) \oplus m_b)$ where $b \in \{0,1\}$ is chosen randomly.

- Hyb_1 : For the second hybrid, we will adjust PK such that $\mathrm{PK} = i\mathcal{O}(P^*_{\mathrm{K}^*,\mathrm{t}^*,\alpha^*})$ is an obfuscation of the program SKE* Encrypt mentioned below: (where $\alpha^* = F_{\mathrm{K}}(t^*)$)

  SKE* Encrypt

  Constants: Punctured PRF key $\mathrm{K}^*(\{t^*\})$
  Input: Message $m \in \{0,1\}^\ell$ and randomness $r \in \{0,1\}^\lambda$

  $P^*_{\mathrm{K}^*,\mathrm{t}^*,\alpha^*}(m, r) \to c$:

  1. $t = \mathrm{PRG}(r)$
  2. If $t = t^*$, then output $c = (c_1 = t^*, c_2 = \alpha^* \oplus m)$
  3. $c = (c_1 = t, c_2 = F_{\mathrm{K}}(t) \oplus m)$

  Note that this program does not change the output from P_K for any value.

- Hyb_2 : Is the same as Hyb_1 with the exception that t^* is chosen at random from $\{0,1\}^{2\lambda}$ (using PRG Security).

- Hyb_3 : Is the same as Hyb_2 with the exception that α^* is chosen at random from $\{0,1\}^\ell$.

At this point, m_b is masked with a truly random string and is thus hidden.

References

[SW14] Amit Sahai and Brent Waters. "How to Use Indistinguishability Obfuscation: Deniable Encryption, and More". In: ACM *Symposium on Theory of Computing* (STOC) (2014).