CS 276: Homework 7

Due Date: Friday November 8th, 2024 at 8:59pm via Gradescope

1 Circular-Secure Encryption

We saw in lecture that fully homomorphic encryption (FHE) can be constructed from a leveled FHE scheme that also satisfies circular security. [BGV11] constructed leveled FHE from LWE, but it is not known whether their scheme satisfies circular security. In fact, for every leveled FHE scheme that we have, we do not know how to prove circular security without simply assuming it by fiat.

This begs the question: is circular security hard to prove for every encryption scheme? In fact it is not. We will prove below that a natural encryption scheme based on LWE is circular-secure.

Defining Circular Security: Circular security states that the encryption scheme remains CPA-secure even when the adversary receives $\mathsf{Enc}(\mathsf{sk})$.

Definition 1.1 (Circular Security) *Given an encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *and an adversary* $\mathcal{A}$*, let us define the circular security game* $\mathsf{Circ\text{-}Game}(\Pi, \mathcal{A}, 1^\lambda)$ *to be the same as the CPA security game except the adversary receives* $\mathsf{Enc}(\mathsf{sk})$ *right after the challenger runs* $\mathsf{Gen}(1^\lambda)$*.*

Π *satisfies* ***circular security*** *if for every PPT adversary* $\mathcal{A}$*,*

$$\Pr[\mathsf{Circ\text{-}Game}(\Pi, \mathcal{A}, 1^\lambda) \to 1] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Circular security does not hold for every CPA-secure encryption scheme because in the CPA security game, the only ciphertexts the adversary sees are encryptions of messages chosen by the adversary. Since the adversary does not know sk a priori, it will not, except with negligible probability, receive $\mathsf{Enc}(\mathsf{sk})$. So the fact that the circular security game gives $\mathsf{Enc}(\mathsf{sk})$ to the adversary seems to give the adversary additional power.

Question 1: Construct a public key encryption (PKE) scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ that is CPA-secure and correct, *but not circular-secure*. Your construction can start with a CPA-secure PKE scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as well as any other primitive implied by that primitive.

Tip: In your answer, you should prove that your construction satisfies CPA security and correctness, and does not satisfy circular security.

Now we will consider an encryption scheme that is circular-secure. The following secret-key encryption scheme is correct and CPA-secure, assuming LWE.[1]

- $\mathsf{Gen}(1^n)$: Sample $\mathbf{s} \xleftarrow{\$} \{0,1\}^n$ and output $\mathsf{sk} = \mathbf{s}$.

[1] We will not state the parameters explicitly for this scheme, but they can be assumed to be similar to the parameters of the IBE scheme from homework 6.

- $\mathsf{Enc}(\mathsf{sk}, \mathbf{m})$: Let $\mathbf{m} \in \{0,1\}^m$ for any $m = \mathsf{poly}(n)$. Sample $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ and $\mathbf{e} \leftarrow \chi^m$. Finally compute
$$\mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{m}$$
and output $c = (\mathbf{A}, \mathbf{u})$

- $\mathsf{Dec}(\mathsf{sk}, c)$: Compute
$$\vec{\mu} = \mathbf{u} - \mathbf{A}^T \cdot \mathbf{s}$$
For each index $i \in [m]$, if $\left|\vec{\mu}_i - \left\lfloor \frac{q}{2} \right\rfloor\right| \leq q/4$, then set $\mathbf{m}'_i = 1$. Else set $\mathbf{m}'_i = 0$. Finally, output $\mathbf{m}' = (\mathbf{m}'_1, \ldots, \mathbf{m}'_m)$.

Question 2: Prove that the encryption scheme constructed above is circular-secure, assuming that it is CPA-secure.

References

[BGV11] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. Fully homomorphic encryption without bootstrapping. Cryptology ePrint Archive, Paper 2011/277, 2011.