CS 276: Homework 7

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

1 Circular-Secure Encryption

[1] 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.

Solution

$(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ will be similar to $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ but with the following main difference. $\mathsf{Enc}'(\mathsf{pk}, m)$ will test if m is good at decrypting the encryption of a random message. $m = \mathsf{sk}$ will pass the test, and any messages that the CPA adversary can find will fail the test with overwhelming probability. Next, Enc' outputs m in the clear if m passes the test. This means that $\mathsf{Enc}'(\mathsf{pk}, \mathsf{sk})$ will leak sk, but any ciphertext in the CPA security game will not.

[1] This problem is based on [Vai23]

- $\mathsf{Gen}'(1^\lambda)$: Same as $\mathsf{Gen}(1^\lambda)$.
- $\mathsf{Enc}'(\mathsf{pk}, m)$:
  1. Sample $r \xleftarrow{\$} \{0,1\}^\lambda$, and compute $r' = \mathsf{Dec}(m, \mathsf{Enc}(\mathsf{pk}, r))$.
     (a) Case 1: If $r' = r$, then set $\mathsf{aux} = m$.
     (b) Case 2: Otherwise, set $\mathsf{aux} = \perp$.
  2. Compute $c_m = \mathsf{Enc}(\mathsf{pk}, m)$ and output $c = (c_m, \mathsf{aux})$.
- $\mathsf{Dec}(\mathsf{sk}, c)$: Output $\mathsf{Dec}(\mathsf{sk}, c_m)$.

Lemma 1.2 $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ *is correct.*

Proof. This follows from the correctness of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

$$\mathsf{Dec}'(\mathsf{sk}, \mathsf{Enc}'(\mathsf{pk}, m)) = \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m))$$

For any message m, $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) = m$ with overwhelming probability.

Lemma 1.3 $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ *is CPA-secure.*

Proof.

1. Let us consider some hybrids:
   - $\mathcal{H}_0$: The CPA security game for $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$. In particular, when the challenger computes $c_b = \mathsf{Enc}'(\mathsf{pk}, m_b)$, they check whether $r = \mathsf{Dec}(m_b, \mathsf{Enc}(\mathsf{pk}, r))$ for a random $r \in \{0,1\}^\lambda$. If so, they set $\mathsf{aux} = m$. If not, they set $\mathsf{aux} = \perp$.
   - $\mathcal{H}_1$: Same as $\mathcal{H}_0$ except that the challenger checks whether $r = \mathsf{Dec}(m_b, \mathsf{Enc}(\mathsf{pk}, 0))$.
   - $\mathcal{H}_2$: Same as $\mathcal{H}_1$ except that the challenger always sets $\mathsf{aux} = \perp$ (never $\mathsf{aux} = m$).
2. We claim that $|\Pr[\mathcal{H}_0 \to 1] - \Pr[\mathcal{H}_1 \to 1]| = \mathsf{negl}(\lambda)$, by the CPA security of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. In other words, $\mathsf{Enc}(\mathsf{pk}, r)$ and $\mathsf{Enc}(\mathsf{pk}, 0)$ are indistinguishable.
3. In $\mathcal{H}_1$, the probability that $r = \mathsf{Dec}(m_b, \mathsf{Enc}(\mathsf{pk}, 0))$ is negligible because $\mathsf{Dec}(m_b, \mathsf{Enc}(\mathsf{pk}, 0))$ is independent of r, and r is uniformly random over $\{0,1\}^\lambda$. Then the probability that $\mathcal{H}_1$ sets $\mathsf{aux} = m$ is negligible, so
$$|\Pr[\mathcal{H}_1 \to 1] - \Pr[\mathcal{H}_2 \to 1]| = \mathsf{negl}(\lambda)$$
4. $\mathcal{H}_2$ is equivalent to the CPA security game for $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. The only difference is that $\mathsf{Enc}'(\mathsf{pk}, m_b)$ outputs $(\mathsf{Enc}(\mathsf{pk}, m_b), \perp)$, but the $\perp$ is useless to the adversary. Since $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CPA-secure,
$$\Pr[\mathcal{H}_2 \to 1] = \mathsf{negl}(\lambda)$$

5. Putting everything together, we have that

$$\Pr[\mathcal{H}_0 \to 1] = \mathsf{negl}(\lambda)$$

so $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is CPA-secure.

Lemma 1.4 $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ *is not circular-secure.*

Proof. First, we will show that with overwhelming probability, $\mathsf{Enc}'(\mathsf{pk}, \mathsf{sk})$ returns $\mathsf{aux} = \mathsf{sk}$. In $\mathsf{Enc}'(\mathsf{pk}, \mathsf{sk})$, the function checks whether $r = \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, r))$. By the correctness of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$,

$$\Pr[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, r)) = r] \geq 1 - \mathsf{negl}(\lambda)$$

Then with overwhelming probability, $\mathsf{Enc}'(\mathsf{pk}, \mathsf{sk})$ executes case 1 and outputs $\mathsf{aux} = \mathsf{sk}$.

Next, in the circular security game, the adversary receives $c_{\mathsf{sk}} = \mathsf{Enc}'(\mathsf{pk}, \mathsf{sk})$, which we assume includes $\mathsf{aux} = \mathsf{sk}$. Then we will construct an adversary to break circular security as follows:

1. Receive $(\mathsf{pk}, c_{\mathsf{sk}})$ from the challenger.
2. Send two distinct messages (m_0, m_1) to the challenger and receive $c_b = \mathsf{Enc}'(\mathsf{pk}, m_b)$.
3. Compute $m' = \mathsf{Dec}(\mathsf{sk}, c_b)$. If $m' = m_0$, then output 0. Else if $m' = m_1$, then output 1. Else, sample $b' \xleftarrow{\$} \{0, 1\}$ and output b'.

By the correctness of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, $\mathsf{Dec}(\mathsf{sk}, c_b) = m_b$ with overwhelming probability, in which case, the adversary correctly guesses b. This adversary breaks circular-security because it wins the game with overwhelming advantage. ■

Now we will consider an encryption scheme that is circular-secure. The following secret-key encryption scheme is correct and CPA-secure, assuming LWE.[2]

- $\mathsf{Gen}(1^n)$: Sample $\mathbf{s} \xleftarrow{\$} \{0, 1\}^n$ and output $\mathsf{sk} = \mathbf{s}$.
- $\mathsf{Enc}(\mathsf{sk}, \mathbf{m})$: 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 $\mathbf{m}' = (\mathbf{m}'_1, \ldots, \mathbf{m}'_m)$.

[2] 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.

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

Solution The only extra information available to the adversary in the circular security game, when compared to the CPA security game, is $c_{\mathsf{sk}} = \mathsf{Enc}(\mathsf{sk}, \mathsf{sk})$. We will show in lemma 1.5 that c_{sk} can be computed in the CPA security game as well by querying $\mathsf{Enc}(\mathsf{sk}, \mathbf{0})$ and then doing some post-processing. This means that the circular security game gives the adversary as much power as the CPA security game, so the CPA security of the encryption scheme implies circular security as well.

Lemma 1.5 *For a given* sk*, the distribution of* $\mathsf{Enc}(\mathsf{sk}, \mathsf{sk})$ *can be perfectly simulated using one query to* $\mathsf{Enc}(\mathsf{sk}, \mathbf{0})$*, where* $\mathbf{0} \in \mathbb{Z}_q^n$*.*

Proof.
Procedure to compute $c_{\mathsf{sk}} = \mathsf{Enc}(\mathsf{sk}, \mathsf{sk})$:

1. Receive $c_{\mathbf{0}} = \mathsf{Enc}(\mathsf{sk}, \mathbf{0}) = (\mathbf{A_0}, \mathbf{u_0})$, where $\mathbf{0} \in \mathbb{Z}_q^n$, $\mathbf{A_0} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$, and $\mathbf{u_0} = \mathbf{A_0}^T \cdot \mathbf{s} + \mathbf{e}$ for some $\mathbf{e} \leftarrow \chi^n$.
2. Compute

$$\mathbf{A}_{\mathsf{sk}} = \mathbf{A_0} - \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{I}_n$$
$$\mathbf{u}_{\mathsf{sk}} = \mathbf{u_0}$$

   where $\mathbf{I}_n$ is the $n \times n$ identity matrix. Then output $c_{\mathsf{sk}} = (\mathbf{A}_{\mathsf{sk}}, \mathbf{u}_{\mathsf{sk}})$.

Note that $\mathbf{A}_{\mathsf{sk}}$ is uniformly random in $\mathbb{Z}_q^{n \times n}$, due to the randomness of $\mathbf{A_0}$. Subtracting $\left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{I}_n$ from a uniformly random matrix still produces a uniformly random matrix.
Next, note that

$$\begin{aligned}
\mathbf{u}_{\mathsf{sk}} = \mathbf{u_0} &= \mathbf{A_0}^T \cdot \mathbf{s} + \mathbf{e} \\
&= \left(\mathbf{A}_{\mathsf{sk}}^T + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{I}_n \right) \cdot \mathbf{s} + \mathbf{e} \\
&= \mathbf{A}_{\mathsf{sk}}^T \cdot \mathbf{s} + \mathbf{e} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{s}
\end{aligned}$$

This is exactly the distribution of $\mathbf{u}_{\mathsf{sk}}$ that Enc produces. In summary, for a given sk, the procedure to compute c_{sk} given above samples c_{sk} from the same distribution as $\mathsf{Enc}(\mathsf{sk}, \mathsf{sk})$.

Theorem 1.6 *The encryption scheme given above is circular-secure assuming that it is CPA-secure.*

Proof. If there exists an adversary $\mathcal{A}_{circ}$ that breaks the circular security of the encryption scheme, then we can construct an adversary $\mathcal{A}_{CPA}$ that breaks the CPA security of the encryption scheme.
Construction of $\mathcal{A}_{CPA}$:

1. Request $\mathsf{Enc}(\mathsf{sk}, \mathbf{0})$, where $\mathbf{0} \in \mathbb{Z}_q^n$, and then use the procedure to compute c_{sk} given above. Then give c_{sk} to $\mathcal{A}_{circ}$.

2. Whenever $\mathcal{A}_{circ}$ needs to communicate with the challenger, $\mathcal{A}_{CPA}$ forwards $\mathcal{A}_{circ}$'s messages to the challenger and forwards the challenger's responses back to $\mathcal{A}_{circ}$.

3. When $\mathcal{A}_{circ}$ outputs b', $\mathcal{A}_{CPA}$ outputs b' as well.

$\mathcal{A}_{CPA}$ correctly simulates the circular security game with $\mathcal{A}_{circ}$ as the adversary. Furthermore, whenever $\mathcal{A}_{circ}$ wins the simulated circular security game by guessing $b' = b$, $\mathcal{A}_{CPA}$ wins the CPA security game as well. ■

References

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