CS 171: Discussion Section 8 (March 11)

1 CPA-Secure Public-Key Encryption From Two-Round Key Exchange

Question: Given a two-round key-exchange protocol that outputs keys of length n, construct a CPA-secure public-key encryption (PKE) scheme for messages of length n and prove its security. Do not use any other cryptographic primitive.

1.1 Two-Round Key Exchange

A two-round key-exchange protocol comprises three randomized algorithms (P_1, P_2, P_3) and has the following form:

1. Alice computes $(\mathsf{msg}_1, \mathsf{st}) \leftarrow P_1(1^n)$ and sends msg_1 to Bob.
2. Bob computes $(\mathsf{msg}_2, k) \leftarrow P_2(\mathsf{msg}_1)$, sends msg_2 to Alice, and outputs k.
3. Alice computes $k \leftarrow P_3(\mathsf{st}, \mathsf{msg}_2)$ and outputs k.

Here is the security game for the key-exchange protocol.

$\underline{\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)}$:

1. The challenger executes the key exchange protocol to produce $(\mathsf{msg}_1, \mathsf{msg}_2, k)$.
2. The challenger samples a bit $b \leftarrow \{0, 1\}$. If $b = 0$, the challenger sets $\hat{k} = k$. If $b = 1$, they set $\hat{k} \leftarrow \mathcal{K}$, where $\mathcal{K}$ is the set of all possible keys. Then $\mathcal{A}$ is given $(\mathsf{msg}_1, \mathsf{msg}_2, \hat{k})$.
3. $\mathcal{A}$ outputs a guess b' for b. The output of the experiment is 1 if $b = b'$, and 0 otherwise.

We say that a key-exchange protocol is **secure** if for all PPT adversaries $\mathcal{A}$, there exists a negligible function negl such that:

$$\Pr[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(1^n) \to 1] = \mathsf{negl}(n)$$

1.2 Definition of CPA security for PKE

Let's write the definition of CPA security for public-key encryption. It will resemble the definition we've seen previously for secret-key encryption.

Given an adversary $\mathcal{A}$, define the following game:

$\underline{\mathsf{PubK}_{\mathcal{A},\Pi}(n)}$:

1. The challenger samples the keys $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$. Then they give $(1^n, \mathsf{pk})$ to the adversary $\mathcal{A}$.
2. $\mathcal{A}$ outputs a pair of messages (m_0, m_1) such that $|m_0| = |m_1|$.

3. The challenger samples $b \leftarrow \{0,1\}$ and computes the challenge ciphertext:

$$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b) \tag{1.1}$$

   Then they give c to $\mathcal{A}$.

4. $\mathcal{A}$ outputs a bit b'. The output of the experiment is 1 if $b = b'$ and 0 otherwise.

A public-key encryption scheme is **CPA-secure** if for any probabilistic polynomial-time adversary $\mathcal{A}$, there is a negligible function negl such that:

$$\Pr[\mathsf{PubK}_{\mathcal{A},\Pi}(n) \to 1] = \mathsf{negl}(n)$$

2 One-way functions from Pseudorandom Permutations

One-way functions can be constructed from many other cryptographic primitives, including from pseudorandom permutations.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation. This can be written as $F(k, x)$ or equivalently $F_k(x)$, where k is the key. Note that an adversary can compute $F_k^{-1}(\cdot)$ in addition to $F_k(\cdot)$ if they are given the key k.

1. Let $x = (x_0, x_1) \in \{0,1\}^n \times \{0,1\}^n$, and

   $$\text{let } f_1(x) = F_{x_0}(x_1)$$

   Show that f_1 is not a one-way function.

2. Let $x \in \{0,1\}^n$, and

   $$\text{let } f_2(x) = F_{0^n}(x)$$

   Show that f_2 is not a one-way function.