CSC 591 Cryptography 9/26/18

Lecture 6 – CPA-Secure Encryption Scheme

Lecturer: Alessandra Scafuro *Scribe: Bihan Zhang*

Topic/Problem

This is the second lecture on CPA-secure encryption scheme, with a focus on constructing a CPA-secure encryption scheme using PRF.

Definition

An encryption scheme is *CPA* secure if it is secure against chosen plaintext attacks.

The CPA game ($Priv^{CPA}_{A,\Pi}(n)$) is as follows (we sometimes omit the security parameter n in the following context by just denoting $Priv^{CPA}_{A,\Pi}$):

1. Let Π be an encryption oracle who generates a secret key k at the very beginning.
2. Let A be an adversary
3. Training Phase: A can query polynomial number of messages m_i to Π and get the encrypted ciphertext c_i back.
4. Challenge Phase:
   a. A passes a pair of messages $\{m_0, m_1\}$ to Π, where m_0 and m_1 are of the same length.
   b. The challenger picks a random bit $b \leftarrow_R \{0,1\}$ and returns the challenge ciphertext $c^* = Enc(k, m_b)$
   c. A guesses b' ($b' \in \{0,1\}$ corresponds to m_0 or m_1 that the adversary A_{PPT} thinks Π encrypted).
   d. A_{PPT} wins if $b = b'$

We say an encryption scheme is CPA-secure if

$$Pr[A \text{ wins } Priv^{CPA}_{A,\Pi}] = 1/2 + \epsilon$$

where ϵ is a negligible function and $Priv^{CPA}_{A,\Pi}$ is the security game constructed with a CPA secure scheme Π.

A function $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ is considered *pseudorandom* if for all PPT distinguishers D the following holds true:

$$|Pr[D^{F_k}(n) = 1] - Pr[D^{TR}(n) = 1]| \leq \epsilon$$

Where F_k is an oracle modelled as a pseudorandom function and TR is an oracle modelled as truly random function, and ϵ is a negligible function.

Or, in layman's terms, there does not exist a distinguisher that can tell apart the output of a PRF, and the output of a truly random function. The distinguisher can play the PRF Game in order to prove that it can tell these two apart. The PRF game is as follows:

The PRF Game:

1. Let O be an oracle instantiated with either F_k or with TR.
2. Let D be a distinguisher with access to O.
3. D passes x_i to the oracle O
4. O will either return $y_i = PRF(x_i)$ or $y_i = TR()$
5. D guesses whether y_i came from the PRF or from TR.

$$D \text{ wins if } |Pr[D^{F_k}(n) = 1] - Pr[D^{TR}(n) = 1]| = p(n)$$

Where $p(n)$ is a non-negligible function.

Scheme

CPA secure encryption: Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. We describe the encryption scheme (Gen, Enc, Dec) below:

Gen: Sample a PRF key $k \in \{0,1\}^n$ uniformly at random.

$Enc(k, m)$: Given $k \in \{0,1\}^n$ and $m \in \{0,1\}^n$ choose a uniformly random $r \in \{0,1\}^n$ and construct the ciphertext $c = \langle F_k(r) \oplus m, r \rangle$

$Dec(k, c)$: Given $k \in \{0,1\}^n$ and parse $c = \langle s, r \rangle$, decrypt the ciphertext c to the message $m = F_k(r) \oplus s$

Security Proof

If F is a PRF, (Gen, Enc, Dec) is a CPA secure encryption scheme.

Intuition:

Even though intuitively it feels insecure to reveal r it actually doesn't matter. Even when r is known, since k is unknown, the result of $F_k(r)$ is indistinguishable from a random function. And because the output of $F_k(r)$ is pseudo-random, $F_k(r) \oplus m$ should be secure, and because r is a random value each time, the scheme is non-deterministic, and should be CPA secure.

Formal Proof:

Let $Priv^{CPA}_{A,\Pi}$ be the CPA game constructed with Π as defined under the scheme section.

Let $Priv^{CPA}_{A,TR}$ be the same CPA game except that a truly random function is used in place of F_k in the construction.

Assume for the sake of contradiction that there exists an Adversary A_{CPA} that can win $Priv^{CPA}_{A,\Pi}$ with some non negligible probability $p(n)$.

$$Pr[A \text{ wins } Priv^{CPA}_{A,\Pi}] = 1/2 + p(n)$$
$$Pr[A \text{ wins } Priv^{CPA}_{A,TR}] = 1/2 + q/2^n$$

where q is the number of queries performed by the adversary. There is a chance that the adversary has seen the random string r repeating, and this chance increases with the number of queries. This is very unlikely, so we'll treat $q/2^n = \epsilon$, where ϵ is a negligible function.

$$|Pr[A \text{ wins } Priv^{CPA}_{A,TR}] - Pr[A \text{ wins } Priv^{CPA}_{A,\Pi}]| = p(n) - q/2^n$$

which is non-negligible.

Reduction A distinguisher D for F can be constructed as follows:

Assume D has oracle access to a function O. O is either instantiated with pseudo-random function F_k, or with a truly random function TF.

D can run adversary A

When A is in it's training phase, it'll ask for encryptions of messages m_i, when this happens D does the following:

1. Pick a random $r_i = \{0,1\}^n$
2. Query the Oracle O with r_i and receive y_i
3. Output $\langle r_i, m_i \oplus y_i \rangle$

When A challenges with m_0, m_1, D does the following:

1. Pick $b \leftarrow_R \{0,1\}$
2. Pick a random $r_i = \{0,1\}^n$
3. Query the Oracle O with r_i and receive y_i
4. Output $\langle r_i, m_b \oplus y_i \rangle$

When A enters its decision phase and outputs a bit b'. D should return 1 if $b = b'$, and 0 otherwise

Analysis:

If O is instantiated with F then the reduction is perfectly simulating the game $Priv^{CPA}_{A,\Pi}$ and therefore:

$$Pr[D^{F_k}(n) = 1] = Pr[A \text{ wins } Priv^{CPA}_{A,\Pi}] = 1/2 + p(n)$$

Where $p(n)$ is non-negligible.

If O is instantiated with TR then D is simulating $Priv^{CPA}_{A,TR}$ and so:

$$Pr[D^{TR}(n) = 1] = Pr[A \text{ wins } Priv^{CPA}_{A,TR}] = 1/2 + \epsilon$$

Where ϵ is negligible

$$|Pr[D^{F_k}(n) = 1] - Pr[D^{TR}(n) = 1]| = p(n) - \epsilon$$

This contradicts with our original assumption that F is a PRF and:

$$|Pr[D^{F_k}(n) = 1] - Pr[D^{TR}(n) = 1]| \leq \epsilon$$

Therefore if F is a PRF, (Gen, Enc, Dec) is a CPA secure encryption scheme.