

CS 409: Introduction to Cryptography

September 11, 2024

Chalk & Talk 1: Semantic Security and Indistinguishability

Instructor: Sruthi Sekar

Submitted by: Ashok Nayak and Rohan Arrvind

1 Formal Definitions of Security

Recall the notions of *semantic security* and *indistinguishability* of encryption schemes.

Semantic security tries to capture the notion that, no matter what prior information the adversary has, the knowledge of the ciphertext will not afford him any additional knowledge.

Definition 1.1. An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is *semantically secure (under ciphertext-only attack)* if, for every PPT algorithm \mathcal{A} , and polynomial-time computable functions $f(\cdot)$ and $g(\cdot)$, there exists another PPT algorithm \mathcal{A}' such that

$$\left| \Pr[\mathcal{A}(1^n, \text{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(1^n, |m|, h(m)) = f(m)] \right|_{m \in_R \mathcal{M}}$$

is negligible.

Definition 1.2. An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is *indistinguishable under ciphertext-only attack* if, for every probabilistic polynomial-time algorithm \mathcal{A} and two arbitrary messages m_0, m_1 ,

$$\Pr[\mathcal{A}(1^n, \text{Enc}_k(m_b)) = b] \leq \frac{1}{2} + \epsilon(n)$$

where ϵ is a negligible function.

2 Equivalence of the Definitions

Theorem: *Definitions 1.1 and 1.2 are equivalent: i.e., an encryption scheme is semantically secure under a ciphertext-only attack if and only if it is indistinguishable for any ciphertext-only adversary.*

Claim 2.1. If an encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is indistinguishable for all ciphertext-only adversaries, then Π is semantically secure under ciphertext-only attack.

Proof: Consider an arbitrary message m , $k \leftarrow \text{Gen}(1^n)$, $c = \text{Enc}_k(m)$ and some polynomial-time computable functions $h(\cdot)$ and $f(\cdot)$. Consider any p.p.t. algorithm \mathcal{A} that takes as input $(1^n, c, h(m))$ and outputs $f(m)$ with probability $p(n)$. We construct another algorithm \mathcal{A}' , that takes as input $(1^n, |m|, h(m))$ and outputs $f(m)$ with probability $p'(n)$ such that $p(n) - p'(n)$ is negligible if Π satisfies the indistinguishability property.

The algorithm \mathcal{A}' , on input $(1^n, |m|, h(m))$, runs $\mathcal{A}(1^n, c', h(m))$ (here c' is any random cipher-text given as an input to \mathcal{A} by \mathcal{A}') and output whatever \mathcal{A} outputs.

If $p(n) - p'(n)$ is not negligible, we could use \mathcal{A} to construct a distinguisher \mathcal{D} as follows. What we now know is that there exists m , $h(\cdot)$ and $f(\cdot)$ such that

$$\Pr[\mathcal{A}(1^n, \text{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(1^n, |m|, h(m)) = f(m)]$$

is non-negligible. Our distinguisher \mathcal{D} works as follows:

- Set $m_0 = m$ and $m_1 = 1^{|m|}$, and send m_0, m_1 to the challenger. The challenger returns $c \leftarrow \text{Enc}_k(m_b)$ for a randomly chosen b .
- Run $\mathcal{A}(1^n, c, h(m))$. If $\mathcal{A}(1^n, c, h(m)) = f(m)$, return 0, else return 1.

We have,

$$\Pr[\mathcal{A}(1^n, c, h(m)) = f(m) \mid c = \text{Enc}_k(m_0)] = p(n)$$

and

$$\Pr[\mathcal{A}(1^n, c', h(m)) = f(m) \mid c' = \text{Enc}_k(m_1)] = p'(n)$$

since if $c' = \text{Enc}_k(m_1)$, c' doesn't give any extra information as it is a dummy ciphertext, we have:

$$\Pr[\mathcal{A}(1^n, c', h(m)) = f(m) \mid c' = \text{Enc}_k(m_1)] = p'(n) = 1/2$$

This is because \mathcal{A}' does not have access to the actual cipher-text so it generates a dummy cipher-text to provide as an input to \mathcal{A} , and this is nothing better than a random guess.

$$\begin{aligned} \Pr[\mathcal{D} \text{ succeeds}] &= \Pr[\mathcal{A}\Pi(n) = 1] = \Pr b \leftarrow \{0, 1\} [(\mathcal{A}_\Pi(1^n, c_b, h(m))) = 1] \\ &= \frac{1}{2} \cdot \Pr[\text{output}(\mathcal{A}_\Pi(1^n, c_0, h(m))) = 0] + \frac{1}{2} \cdot \Pr[(\mathcal{A}_\Pi(1^n, c_1, h(m))) = 1] \\ &= \frac{1}{2} \cdot (1 - \Pr[(\mathcal{A}_\Pi(1^n, c_0, h(m))) = 1]) + \frac{1}{2} \cdot \Pr[(\mathcal{A}_\Pi(1^n, c_1, h(m))) = 1] \\ &= \frac{1}{2} + \frac{1}{2} \cdot (\Pr[(\mathcal{A}_\Pi(1^n, c_1, h(m))) = 1] - \Pr[(\mathcal{A}_\Pi(1^n, c_0, h(m))) = 1]). \end{aligned}$$

Therefore, $\Pr[\mathcal{D} \text{ succeeds}] \geq \frac{1}{2} + \frac{1}{2}(p(n) - 1/2)$. If the difference is negligible, \mathcal{D} wins with non-negligible advantage over a random guess, which is indeed the case in semantic security.

Claim 2.2. *If an encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is semantically secure under ciphertext-only attack, then Π is indistinguishable for all ciphertext-only adversaries.*

Proof. To prove a contradiction, assume that Π is efficiently distinguishable, and there exist two messages m_0, m_1 and a distinguisher \mathcal{D} that can distinguish between the encryptions of m_0 and m_1 with non-negligible probability. We use \mathcal{D} to show that Π is not semantically secure.

Define the function f as follows:

$$f(m) = \begin{cases} 0 & \text{if } m = m_0 \\ 1 & \text{if } m = m_1 \\ \perp & \text{otherwise} \end{cases}$$

The function h could be chosen to be any computable function. Now, construct an algorithm \mathcal{A} that works as follows:

- \mathcal{A} takes as input $(1^n, \text{Enc}_k(m), h(m))$.
- \mathcal{A} runs the distinguisher $\mathcal{D}(1^n, \text{Enc}_k(m))$, and outputs whatever \mathcal{D} outputs.

It is easy to see that, for $m = m_0$

$$\Pr[\mathcal{A}(1^n, \text{Enc}_k(m), h(m)) = f(m)] = \Pr[\mathcal{D}(1^n, \text{Enc}_k(m_0)) = 0] \geq \frac{1}{2} + \epsilon(n)$$

which is non-negligibly more than $\frac{1}{2}$. On the other hand, for any algorithm that doesn't have access to $\text{Enc}_k(m)$, the best bet is a random guess, and the probability of success is $\frac{1}{2}$. Hence, Π violates the definition of semantic security.

We see that there exists a negligible function $\epsilon(n)$ such that

$$\begin{aligned} \epsilon(n) &\geq \Pr[\text{Priv}_A^{\text{eav}}(n) = 1] - \frac{1}{2} \\ &= \frac{1}{2} \cdot (\Pr[\text{output}(\text{Priv}_A^{\text{eav}}(n, 1)) = 1] - \Pr[\text{output}(\text{Priv}_A^{\text{eav}}(n, 0)) = 1]). \end{aligned} \quad (3.1)$$

Let \mathcal{A} denote an adversary that runs identically to \mathcal{A} except that it outputs the complement of whatever \mathcal{A} outputs. Then

$$\begin{aligned} \Pr[\text{Priv}_{\mathcal{A}, \Pi}^{\text{eav}}(n) = 1] &= 1 - \Pr[\text{Priv}_A^{\text{eav}}(n) = 1] \\ &= \frac{1}{2} + \frac{1}{2} \cdot (\Pr[\text{output}(\text{Priv}_A^{\text{eav}}(n, 0)) = 1] - \Pr[\text{output}(\text{Priv}_A^{\text{eav}}(n, 1)) = 1]). \end{aligned} \quad (3.2)$$

Combining Equations (3.1) and (3.2), we see that Π satisfies the claim as well.