Modern Cryptography

Stronger Security Notions

Sep 4, 2025

Dr Shashank Singh

Table of Content

Stronger Seucrity Notions

- Consider a scenario where the same key is used for multiple message exchanges by two communicating parties. An adversary, denoted as $\mathscr{A}$, eavesdrops on all the messages.

- Consider a scenario where the same key is used for multiple message exchanges by two communicating parties. An adversary, denoted as $\mathscr{A}$, eavesdrops on all the messages.

$\mathrm{PrivK}^{\mathrm{mult}}_{\mathscr{A},\Pi}(n)$:

1. $\mathscr{A}$ is given $\Pi(n)$. $\mathscr{A}$ outputs $\boldsymbol{m}_0 := (m_{00}, m_{01}, \ldots, m_{0t})$ and $\boldsymbol{m}_1 := (m_{10}, m_{11}, \ldots, m_{1t})$, where $m_{ij} \in \{0,1\}^\star$ with $|m_{0i}| = |m_{1i}|\ \forall i$.
2. $k \leftarrow \mathrm{GEN}(n)$, $b \xleftarrow{\$} \{0,1\}$ and $\boldsymbol{c} := (c_0, c_1, \ldots c_t)$ is given to the $\mathscr{A}$, where $c_i \leftarrow \mathrm{ENC}(k, m_{bi})$
3. $\mathscr{A}$ return a bit b'.
4. The output of the experiment is $b' \stackrel{?}{=} b$.

♣

Definition 1

A private key encryption scheme $\Pi(n)$ has an indistinguishable multiple encryption in the presence of an eavesdropper, or is EAV-secure, if for all PPT adversaries $\mathcal{A}$, there is a negligible function $\varepsilon()$ such that, for all n,

$$\Pr\left[\mathrm{PrivK}^{\mathrm{mult}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n). \tag{1}$$

♣

Remark

- The one-time pad encryption scheme does not have indistinguishable multiple encryptions in the presence of an eavesdropper.

CPA Seucrity

Let $\Pi(n)$ be an encryption scheme and $\mathscr{A}$ be a CPA adversary.

$\mathrm{PrivK}^{\mathrm{cpa}}_{\mathscr{A},\Pi}(n)$:

1. $k \xleftarrow{\$} \mathrm{GEN}(n)$ and the encryption oracle $\mathrm{ENC}_k(\cdot)$ is given to $\mathscr{A}$.
2. $\mathscr{A}$ outputs $m_0, m_1 \in \{0,1\}^\star$ with $|m_0| = |m_1|$.
3. $b \xleftarrow{\$} \{0,1\}$ and $c \leftarrow \mathrm{ENC}(k, m_b)$ is given to $\mathscr{A}$.
4. $\mathscr{A}$ return b'.
5. The output of the experiment is $b' \stackrel{?}{=} b$.

♣

Definition 1

A private key encryption scheme $\Pi(n)$ has an indistinguishable encryption under the chosen plain text attack, or is CPA-secure, if for all PPT adversaries $\mathscr{A}$, there is a negligible function $\varepsilon()$ such that, for all n,

$$\Pr\left[\mathrm{PrivK}^{\mathrm{cpa}}_{\mathscr{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n). \tag{2}$$

♣

Note

- We can also define CPA-security for multiple encryptions in a similar manner.

Theorem 1

Any private-key encryption scheme that is CPA-secure is also CPA-secure for multiple encryptions.

♡

Remark

- The theorem has positive consequences.
- We only need a CPA-secure fixed-length encryption scheme.
- Since multiple encryption is also CPA secure, we can use the same key to encrypt longer messages as needed.

Construction of CPA secure schemes

- We have observed that CPA security (IND-CPA) remains intact even when the same key is used to encrypt multiple messages.
- The key takeaway from this observation is that we should concentrate on designing a CPA-secure scheme for encrypting fixed-length messages only, i.e., for $\mathscr{M} = \{0,1\}^n$ for some n.
- The encryption schemes for encrypting fixed-length messages will be referred to as block ciphers. A block cipher is represented by an abstract concept known as a Pseudorandom Function, more precisely by Pseudorandom Permutations.
- When we talk about the pseudorandomness of functions, we are essentially referring to the pseudorandomness of a distribution over functions.

Pseudo random function

- We have observed that large discrete distributions are frequently defined by algorithms that efficiently sample elements according to the distribution.
- We are interested in the random functions of the set $\mathscr{F}_n$.

$$\mathscr{F}_n = \left\{ f : \{0,1\}^n \mapsto \{0,1\}^n \right\}$$

- $\left|\mathscr{F}_n\right| = 2^{n \cdot 2^n}$ is very large even for very small n.

Keyed Function

We define a keyed function as a function

$$F_k : \{0,1\}^{\ell_{\text{in}}(n)} \mapsto \{0,1\}^{\ell_{\text{out}}(n)},$$

which takes as input a key, $k \leftarrow \{0,1\}^n$, completely specifies function

$$F_k : \{0,1\}^{\ell_{\text{in}}(n)} \mapsto \{0,1\}^{\ell_{\text{out}}(n)} \in \mathscr{F}_n.$$

Remark

- $\left|\left\{F_k : F_k \text{ is a keyed function and } k \in \{0,1\}^n\right\}\right| = 2^n \ll |\mathscr{F}_n|$.
- If $\ell_{\text{in}}(n) = \ell_{\text{out}}(n) = n$, F_k is called length preserving.
- The size of the keyed function, though very, very small in comparison to $|\mathscr{F}|$ but is still too large (2^n) for us.

Definition 1

An efficient, length-preserving keyed function F_k, where $k \in \{0,1\}^n$ is said to pseudorandom function if for all probabilistic polynomial-time distinguishers (algorithms) $\mathscr{D}$, there is a negligible function $\varepsilon()$ such that,

$$\left|\Pr_{k \xleftarrow{\$} \{0,1\}^n}\left[\mathscr{D}\left(F_k(\cdot)\right) = 1\right] - \Pr_{f \xleftarrow{\$} \mathscr{F}}\left[\mathscr{D}\left(f(\cdot)\right) = 1\right]\right| \leq \varepsilon(n).$$

♣

Informally, if it's nearly impossible to determine whether a given function (oracle access) is a keyed function or a random function from the set $\mathscr{F}$ with a probability better than $\frac{1}{2} + \varepsilon(n)$, then we can consider the distribution of keyed functions to be pseudorandom.