III. Pseudorandom functions & encryption

Eavesdropping attacks not satisfactory security model

- no security for multiple encryptions
- does not cover practical attacks

→ new and stronger security notion: indistinguishable encryption against chosen plaintext attacks

The indistinguishability game

Let A be a probabilistic polynomial time algorithm (ppt).

CPA indistinguishability game $\text{PrivK}_{A,\Pi}^{cpa}(n)$

1. $k \leftarrow \text{Gen}(1^n)$.
2. A receives input 1^n and has oracle access to $\text{Enc}_k(\cdot)$.
   Outputs two plaintexts $m_0, m_1 \in \{0,1\}^*$ with $|m_0| = |m_1|$.
3. $b \leftarrow \{0,1\}, c \leftarrow \text{Enc}_k(m_b)$. c given to A.
4. A continues to have oracle access to $\text{Enc}_k(\cdot)$.
   It outputs b'.
5. Output of experiment is 1, if $b = b'$, otherwise output is 0.

Write $\text{PrivK}_{A,\Pi}^{cpa}(n) = 1$, if output is 1. Say A has succeded or A has won.

Oracle access

Algorithm D has oracle access to function $f: U \rightarrow R$, if D

1. can write elements $x \in U$ into special memory cells,
2. in one step receives function value $f(x)$.

Notation Write $D^{f(\cdot)}$ to denote that algorithm D has oracle access to $f(\cdot)$.

The indistinguishability game

Definition 3.1 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions under chosen plaintext attacks (is cpa-secure) if for every probabilistic polynomial time algorithm A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\text{PrivK}_{A,\Pi}^{\text{cpa}}(n) = 1\right] \leq 1/2 + \mu(n).$$

Observation A cpa-secure encryption scheme cannot have a deterministic encryption algorithm.

Multiple messages

Multiple messages cpa game $\mathrm{PrivK}_{A,\Pi}^{\text{mult-cpa}}(n)$

1. $k \leftarrow \mathrm{Gen}(1^n)$.
2. A receives input 1^n and has oracle access to $\mathrm{Enc}_k(\cdot)$.

   A outputs two vectors of messages $M_0 = (m_0^1, \ldots, m_0^t)$,

   $M_1 = (m_1^1, \ldots, m_1^t)$ with $|m_0^i| = |m_1^i|$ for all i.
3. $b \leftarrow \{0,1\}, c_i \leftarrow \mathrm{Enc}_k(m_b^i)$. $C = (c_1, \ldots, c_t)$ is given to A.
4. A continues to have oracle access to $\mathrm{Enc}_k(\cdot)$.

   A outputs bit b'.
5. Output of experiment is 1, if $b = b'$, otherwise output is 0.

Write $\mathrm{PrivK}_{A,\Pi}^{\text{mult-cpa}} = 1$, if output is 1. Say A has succeded or A has won.

CPA-security and multiple messages

Theorem 3.2 If encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is cpa-secure, then it also has indistinguishable multiple encryption under chosen plaintext attacks.

CPA-security and blocks of messages

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ fixed length, $l(n) = 1$.

Define $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ as follows

$$\text{Gen}': \quad \text{same as Gen}$$

$$\text{Enc}': \quad \text{Enc}'_k(m) = \text{Enc}_k(m_1)\ldots\text{Enc}_k(m_s),$$

$$m = m_1 \ldots m_s, m_i \in \{0,1\}^{l(n)}$$

$$\text{Dec}': \quad \text{Dec}'_k(c) = \text{Dec}_k(c_1)\ldots\text{Dec}_k(c_s)$$

Corollary 3.3 If encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is cpa-secure, then $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ is cpa-secure.

Truly random functions

$$\text{Func}_n := \left\{ f : \{0,1\}^n \rightarrow \{0,1\}^n \right\}$$

$$\left|\text{Func}_n\right| = 2^{n2^n}$$

random function: $f \leftarrow \text{Func}_n$

Keyed functions

$$F: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$$
$$(k,x) \mapsto F(k,x)$$

called keyed function. Write $F(k,x) = F_k(x)$.

- F called length-preserving, if for all $x,k \in \{0,1\}^*$ $|F_k(x)| = |k| = |x|$.
- F called efficient, if there is a polynomial time algorithm A with $A(k,x) = F_k(x)$ for all $x,k \in \{0,1\}^*$.
- F called permutation, if for every $n \in \mathbb{N}$ and $k \in \{0,1\}^n$ $F_k : \{0,1\}^n \to \{0,1\}^n$ is bijective.

Oracle access

Algorithm D has oracle access to function $f: U \rightarrow R$, if D

1. can write elements $x \in U$ into special memory cells,
2. in one step receives function value $f(x)$.

Notation Write $D^{f(\cdot)}$ to denote that algorithm D has oracle access to $f(\cdot)$.

Pseudorandom function (PRF)

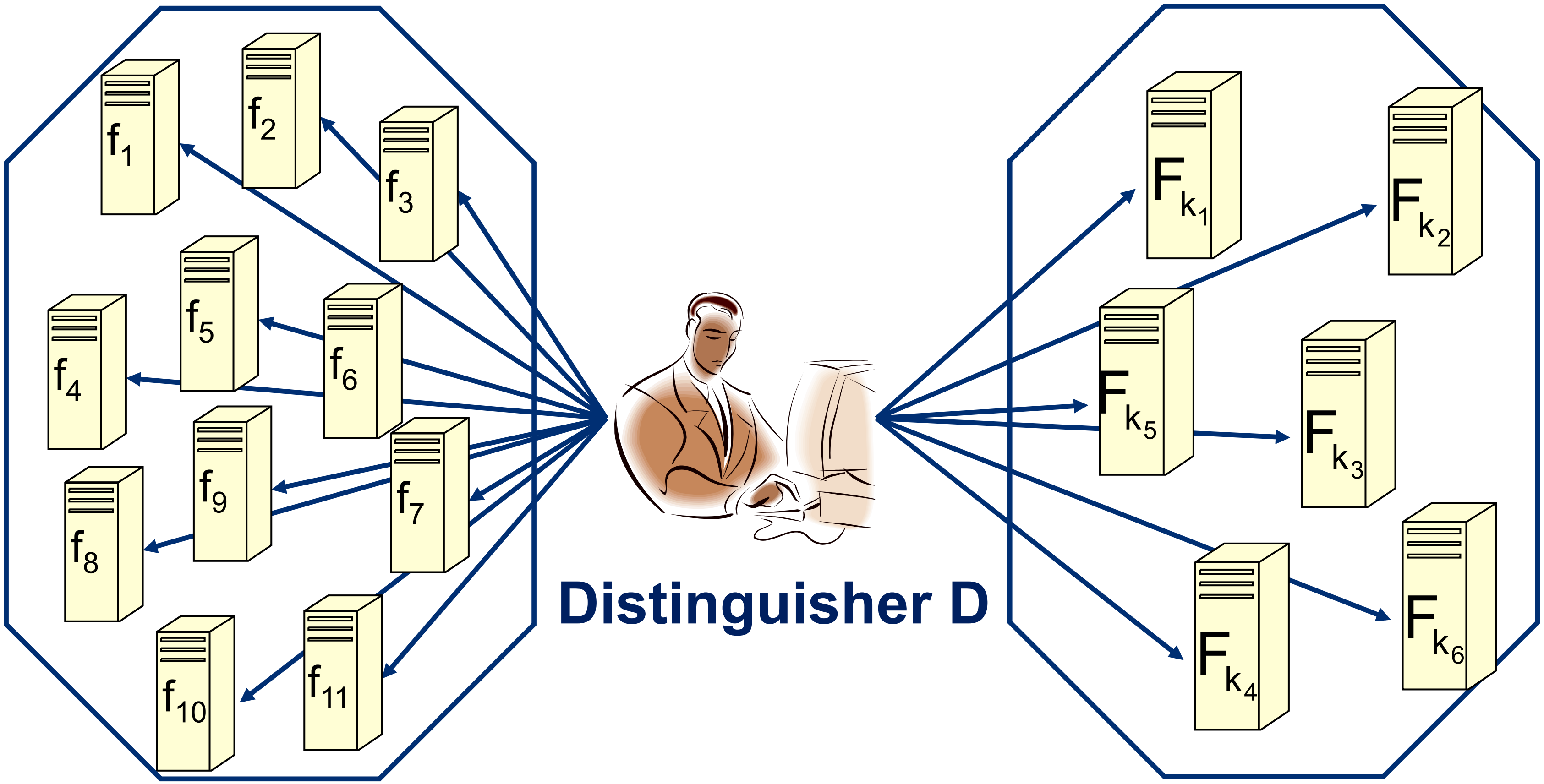
Definition 3.4 Let $F:\{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a keyed, efficient and length-preserving function. F is called a pseudorandom function, if for all ppt distinguishers D there is a negligible function μ such that for all $n \in \mathbb{N}$

$$\left|\Pr\left[D^{F_k(\cdot)}\left(1^n\right)=1\right]-\Pr\left[D^{f(\cdot)}\left(1^n\right)=1\right]\right| \leq \mu(n),$$

where $k \leftarrow \{0,1\}^n, f \leftarrow Func_n$.

$$Func_n := \left\{f:\{0,1\}^n \to \{0,1\}^n\right\}$$

Pseudorandom functions



Func$_n$
with uniform distribution

$$\mathcal{F}_n = \{F_k(\cdot)\}_{k \in \{0,1\}^n}$$

with distribution $k \leftarrow \{0,1\}^n$

Truly random permutations

$$\text{Perm}_n := \left\{ f : \{0,1\}^n \rightarrow \{0,1\}^n \,\middle|\, f \text{ is a permutation} \right\}$$

$$\left|\text{Perm}_n\right| = 2^n\,!$$

random permutation: $f \leftarrow \text{Perm}_n$

Pseudorandom permutation (PRP)

Definition 3.5 Let $F:\{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be a keyed, efficient and length-preserving permutation. F is called a pseudorandom permutation, if for all ppt distinguishers D there is a negligible function μ such that for all $n \in \mathbb{N}$

$$\left|\Pr\left[D^{F_k(\cdot)}\left(1^n\right)=1\right]-\Pr\left[D^{f(\cdot)}\left(1^n\right)=1\right]\right| \leq \mu(n),$$

where $k \leftarrow \{0,1\}^n, f \leftarrow \mathrm{Perm}_n$.

From PRF to cpa-security

Construction 3.6 Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a keyed, efficient, and length-preserving function. Define $\Pi_F = (Gen_F, Enc_F, Dec_F)$ as follows:

Gen_F : on input 1^n, choose $k \leftarrow \{0,1\}^n$.

Enc_F : on input $k, m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ and output $c := (r, m \oplus F_k(r))$.

Dec_F : on input $c = (r, s) \in \{0,1\}^n \times \{0,1\}^n$ and $k \in \{0,1\}^n$ output $m := s \oplus F_k(r)$.

From PRF to cpa-security

Theorem 3.7 If F is a pseudorandom function, then Π_F as defined in Construction 3.6 is cpa-secure.

From adversaries to distinguishers

D on input 1^n and oracle access to $f:\{0,1\}^n \to \{0,1\}^n$

1. Simulate $A(1^n)$. When A queries for an encryption of $m \in \{0,1\}^n$, answer as follows:
   a) $r \leftarrow \{0,1\}^n$
   b) Query $f(\cdot)$ to obtain $f(r)$ and return $(r, m \oplus f(r))$.
2. When A outputs m_0, m_1, choose $b \leftarrow \{0,1\}$, then
   a) $r \leftarrow \{0,1\}^n$
   b) Query $f(\cdot)$ to obtain $f(r)$ and return $c := (r, m_b \oplus f(r))$.
3. Continue to simulate A and answer encryption queries as in 1. Let A's output be $b' \in \{0,1\}$. Output 1, if $b = b'$, otherwise output 0.

A conceptual scheme

Define $\Pi_{true} = (Gen_{true}, Enc_{true}, Dec_{true})$ as follows:

Gen_{true} : on input 1^n, choose $f \leftarrow Func_n$.

Enc_{true} : on input $f, m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ and output $c := (r, m \oplus f(r))$.

Dec_{true} : on input $c = (r,s) \in \{0,1\}^n \times \{0,1\}^n$ and $f \in Func_n$ output $m := s \oplus f(r)$.

Remark

- The scheme is not an encryption scheme, because it is not efficient. It is only used in the proof of Theorem 3.7.
- The CPA indistiguishability experiment can be defined for this scheme.

From PRF to cpa-security – two basic claims

Claim 1 For all ppts A

$$\left|\Pr\left[\mathrm{PrivK}^{cpa}_{A,\Pi_F}(n)=1\right]-\Pr\left[\mathrm{PrivK}^{cpa}_{A,\Pi_{true}}(n)=1\right]\right|$$

$$=\left|\Pr\left[D^{F_k(\cdot)}\left(1^n\right)=1\right]-\Pr\left[D^{f(\cdot)}\left(1^n\right)=1\right]\right|.$$

Claim 2 Let A be a ppt adversary in $\mathrm{PrivK}^{cpa}_{A,\cdot}$ that on input 1^n makes at most q(n) oracle queries. Then

$$\left|\Pr\left[\mathrm{Priv}^{cpa}_{A,\Pi_{true}}(n)=1\right]\right|\le\frac{1}{2}+\frac{q(n)}{2^n}.$$

The CCA indistinguishability game

CCA indistinguishability game $\mathrm{PrivK}^{cca}_{A,\Pi}(n)$

1. $k \leftarrow \mathrm{Gen}(1^n)$
2. A on input 1^n has access to encryption algorithm $\mathrm{Enc}_k(\cdot)$ and to decryption algorithm $\mathrm{Dec}_k(\cdot)$. A outputs 2 messages $m_0, m_1 \in \{0,1\}^*$ of equal length.
3. $b \leftarrow \{0,1\}$, $c \leftarrow \mathrm{Enc}_k(m_b)$. c is given to A.
4. $b' \leftarrow A(1^n, c)$, here A has access to encryption algorithm $\mathrm{Enc}_k(\cdot)$ and to decryption algorithm $\mathrm{Dec}_k(\cdot)$, but query $\mathrm{Dec}_k(c)$ is forbidden.
5. Output of experiment is 1, if $b = b'$. Otherwise output is 0.

CCA-security

Definition 3.8 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions under chosen ciphertext attacks (is cca-secure) if for every probabilistic polynomial time algorithm A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\text{PrivK}^{\text{cca}}_{A,\Pi}(n) = 1\right] \leq 1/2 + \mu(n).$$

Observation cpa-security does not imply cca-security.