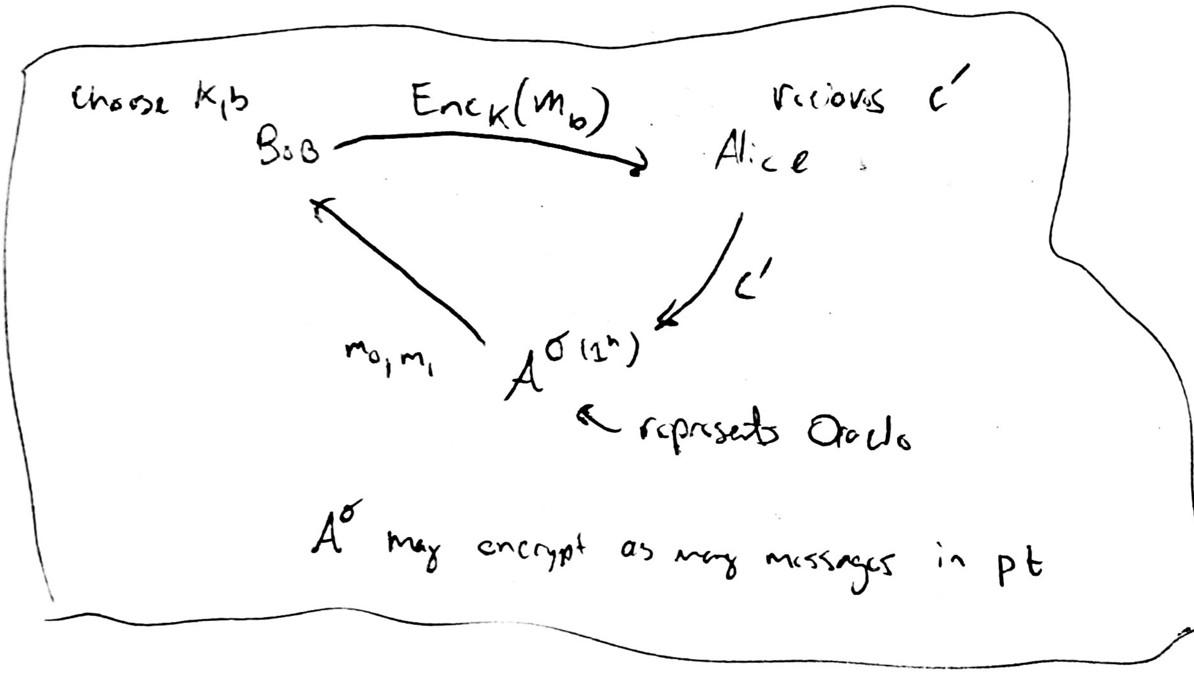
Quick Review

CPA Security

A private key encryption scheme $\pi(\text{Gen}, \text{Enc}, \text{Dec})$ is indistinguishable under CPA if for all PPT A, $\exists$ a negl(n) s.t.

$$\Pr\left[\text{PrivK}^{CPA}_{A,\pi}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n)$$



<u>Key Function</u>. A key function F is $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

- $F(k, x) := F_K(x)$
- Choosing F_K uniformly is done by choosing K from $\{0,1\}^n$ uniformly
- # of $F_K = 2^n$
- F is efficient if $F_K(x)$ is computable in PT

RRF.

A keyed function is pseudorandom if F_k is indistinguishable from $f_k \in Func_n$ in polynomial time.

- $Func_n = \left\{ f_n \;\middle|\; f_n : \{0,1\}^n \to \{0,1\}^n \right\}$
- $|Func_n| = 2^{n2^n}$

Def. F is efficient, keyed function. F is pseudorandom if for all PPT distinguishers D, there exist a negl function negl s.t.

$$\left| \Pr[D^{F_K}(1^n) = 1] - \Pr[D^{f_n}(1^n) = 1] \right| \leq negl(n)$$

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

A CPA - Secure encryption

Lets define the encryption:

Let F be a pseudorandom function. Then $\Pi = (Gen, Enc, Dec)$ is an cryption scheme for messages of length n:

Gen: On input 1^n, choose $k \leftarrow \{0,1\}^n$ uniformly

Enc: input key $k \in \{0,1\}^n$ and message $m \in \{0,1\}^n$,

Choose $r \leftarrow \{0,1\}^n$ uniformly and output the ciphertext

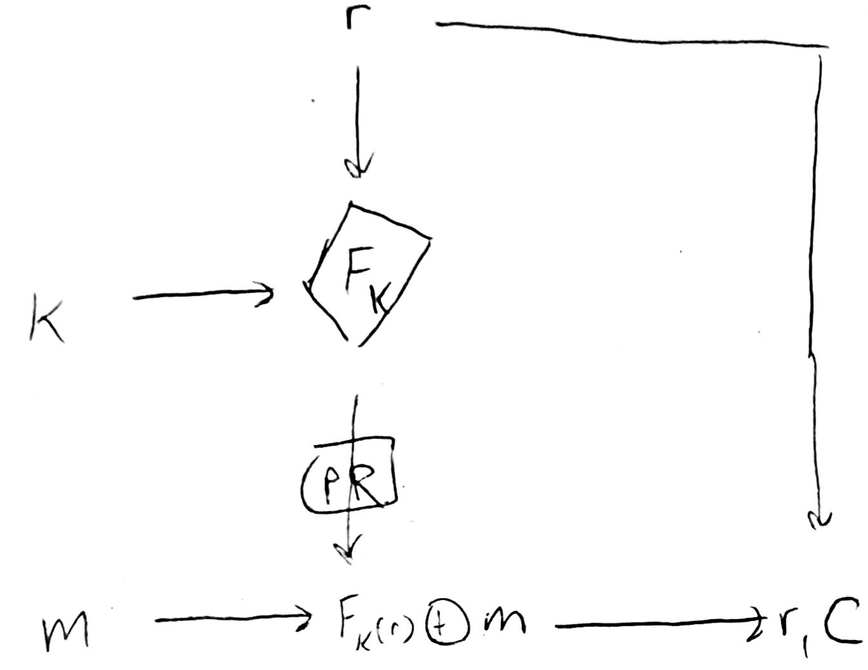
$$C := \langle r, F_k(r) \oplus m \rangle$$ length is $2n$

Dec: Input key $k \in \{0,1\}^n$ and cipher text $c = \langle r, s \rangle$

output

$$m := F_k(r) \oplus s$$

Diagram



1. First a Key is chosen by random parties and message m

2. Then the string r is randomly chosen

$F_K(r)$ produces a different string with prob

$\frac{1}{2^n}$ of occurring

3. Probabilistic meaning $Enc_K(m_1) \neq Enc_K(m_2)$

4. r is sent so the reciver can decrypt

Notes

1. Key is as long as the message. (We can fix this with PRG)

2. We can safely encrypt multiple messages!

3. A Bad event can happen when r value is drawn more than once. But this occurs with negligible probability

4. Can you prove correctness of scheme?

Thm If F is a pseudorandom function, then Π is a fixed length private key encryption scheme with length param $l(n) = n$ that is indistinguishable under CPA.

1. Show Security when $F_k = f_K$. I.E when f_K is a random function

Proof.

Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ and

$\tilde{\Pi} = (\tilde{\text{Gen}}, \tilde{\text{Enc}}, \tilde{\text{Dec}})$ except f_n is a uniform

function used in place of F_n.

I.E. $\tilde{\text{Gen}}(1^n)$ chooses a uniform funct f_n from

funcn

We claim (aka asymptotic security) the scheme is

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

Where $q(n)$ is # of queries made by the oracle. in polynomial time.

- $\forall m$ encrypted by A^O or when a cipher text

is encrypted, $r \in \{0,1\}^n$ is uniformly chosen

and the ciphertext is $\langle r, f_n(r) \oplus m \rangle$

Let r_c be from the challenge cipher: $c = \langle r_c, f_n(r_c) \oplus m_b \rangle$

Case 1

r_c is used by encryption oracle A^O at least once.

1. If so A receives $\langle r_c, f_n(r_c) \oplus m \rangle = c$

2. A removes r_c and computes $(f_n(r_c) \oplus m) \oplus m$ to find $f_n(r_c)$.

3. A can now use $f_n(r_c)$ to determine m_0, m_1 in the experiment.

4. However A makes at most $q(n)$ queries and r_c is choosen uniformly. So probability of Case 1 occuring is $\dfrac{q(n)}{2^n}$

Case 2 r_c is never used by A^{O} to answer A's queries.

1. $f_n(r_c)$ remains unknown
2. At best $f_n(r_c)$ is uniformly chosen for attacker A.
3. The probability $f_n(r_c)$ is xored with m_0 or m_1 is then $1/2$.

Let Repeat denote the event r_c is used by the oracle A^{O} to answer at least one of A's queries.

$$\Pr\left[\mathrm{Priv}_{A,\Pi}^{CPA}(n)=1\right] \overset{\text{LTP}}{=} \Pr\left[\mathrm{PrivK}_{A,\tilde{\Pi}}^{CPA}=1 \wedge \text{Repeat}\right] + \Pr\left[\mathrm{Priv}_{A,\tilde{\Pi}}^{CPA}=1 \wedge \overline{\text{Repeat}}\right]$$

definition of CProb

$$\leq \Pr\left[\text{Repeat}\right] + \Pr\left(\overline{\text{repeat}}\right)\Pr\left(\mathrm{PrivK}_{A\tilde{\Pi}}^{CPA}=1 \mid \overline{\text{Repeat}}\right)$$

$$\leq \Pr\left[\text{Repeat}\right] + \Pr\left[\mathrm{PrivK}_{A,\tilde{\Pi}}^{CPA}=1 \mid \overline{\text{Repeat}}\right]$$

$$= \frac{q(n)}{2^n} + \frac{1}{2}$$

Part 2

Let A be a PPT adversary. Define

$\varepsilon(n) = \Pr[\text{PrivK}^{cpa}_{A,\Pi}(n) = 1] - \frac{1}{2}$

Since A is running in Polynomial time, the # of oracle queries is bounded above by some poly $q(\cdot)$.

So

(1.) $\Pr[\text{PrivK}^{cpa}_{A,\tilde{\Pi}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$ $\boxed{\text{by previous work}}$

(2.) $\Pr[\text{PrivK}^{cpa}_{A,\Pi}(n) = 1] = \frac{1}{2} + \varepsilon(n)$

$$\boxed{|(1)-(2)| \leq \varepsilon(n) + \frac{q(n)}{2^n}}$$

NTS $\varepsilon(n)$ is negligible

We will use the fact F is a Pseudo random function!

Construct Distinguisher D

Intuition

1. D is given a function and must determine if F' is uniform or PR.

2. To do this, D returns 1 if A succeeds and return 0 if A doesn't succeed by running A as a subroutine.

1. Run $A(1^n)$. When A queries encryption oracle on a message m then

   a. $r \leftarrow \{0,1\}^n$

   b. Query $O(r)$ and obtain s'

   c. return $c = \langle r, s' \oplus m \rangle$ to A.

encryption oracle

2. When A outputs m_0, m_1, choose $b \leftarrow \{0,1\}$ then

   a. $r \leftarrow \{0,1\}^n$

   b. Query $O(r)$ and obtain s'

   c. Return $c = \langle r, s' \oplus m_b \rangle$ to A

Challenge cipher

③ Result

After all oracle queries of A

A outputs b' : ~~$b' = 1$ if $b' = b$~~

If $b' = b$ then D returns 1

If $b' \neq b$ then D returns 0

Observe

$$\Pr[D^{F_k}(1^n) = 1] = \Pr[\mathrm{PrivK}_{A,\Pi}(n) = 1]$$

where k is uniformly chosen from $\{0,1\}^n$.

B/c

① If D's oracle is a PRF, then the probability of A as a subroutine of D succeeding is equivalent to A succeeding in PrivK.

Observe 2

$$\Pr[D^{f_n}(1^n)=1] = \Pr[\mathrm{PrivK}^{CPA}_{A,\tilde{\pi}}(n)=1]$$

If f_n is a random function (oracle) then probability of D succeeding is equal to the probability of the randomized experiment succeeds since D is running A as a subroutine.

Therefore

1. F is a PRF
2. D runs in PPT
3. $\Rightarrow \exists$ negl(n)

$$\left| \Pr[D^{F_k}(1^n)=1] - \Pr[D^{f_n}(1^n)=1] \right| \leq negl(n)$$

Then

$$\left| \Pr[\mathrm{PrivK}^{CPA}_{A,\pi}(n)=1] - \Pr[\mathrm{PrivK}^{CPA}_{A,\tilde{\pi}}(n)=1] \right| \leq$$

$$\frac{1}{2} + \varepsilon(n) \quad - \frac{1}{2} - \frac{q(n)}{2^n}$$

$$= \varepsilon(n) - q(n) \quad < negl(n)$$

$\varepsilon(n) \leq negl(n) + \frac{q(n)}{2^n}$. $q(n)$ is negligible $\Rightarrow$

$$negl(n) + \frac{q(n)}{2^n} \text{ is negl}$$

Therefore $\varepsilon(n)$ is negl and hence $\square$

3.6. Psudorandom Permutations and Block cipher

- We define a useful Keyed function called a Keyed permutation

- Essentially this is a Keyed function where each F_K is a bijection ...

Def. Let $F : \{0,1\}^* \times \{0,1\}^*$ be an efficient, length preserving, keyed function. Then F is a Keyed permutation if $\forall K$, the function F_K is a bijection.

- A Key permutation is efficient if there exists a Polynomial time algorith that can compute $F_K(x)$, $F_K^{-1}(x)$

- We can extend the idea of psudorandom permutation by requiring

1. F_K is indistinguishable from a random permutation
2. even if the oracle is given access to F_K, F_K^{-1}

For a PPT attacker pseudorandom permutations look like pseudorandom functions! In fact

Thm. If F is a pseudorandom permutation then it is a pseudorandom function.

Proof. Good test problem

Note.

Streamcipher $\approx$ pseudorandom gen

blockcipher $\approx$ pseudorandom permutation

Lets use a prandom permutation to construct a CPA secure scheme that encrypts arbitrary-length messages

Intuition

Different
Structure   Size

$\text{Auto}_n: \{f_n : f_n : \{0,1\}^n \to \{0,1\}^n\}$ $n!$

$F_\bullet : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ 2^n

F is pseudo random if F_k uniformly chosen from

F is indistinguishable from f_n uniformly chosen from Auto_n

Note. $2^n < n!$ for $n \geq 4$

Def. Let $F: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient keyed permutation. F is pseudorandom permutation if for all PPT distinguishers D, $\exists$ a negligible function negl s.t.

$$\left| \Pr\left[D^{F_k, F_k^{-1}}(1^n) = 1\right] - \Pr\left[D^{f_n, f_n^{-1}}(1^n) = 1\right] \right| \leq \text{negl}(n),$$

where $k \leftarrow \{0,1\}^n$ and $f_n \leftarrow \text{Auton}$

Def. Counter (CTR) Mode

1. Choose $IV \in \{0,1\}^n$ uniformly.
2. Let F be a pseudorandom premutation
3. Choose $k \leftarrow \{0,1\}^n$ using gen.

Set $C_0 = IV$

Let $M = m_1 \cdots m_t$ where $|m_i| = n$ bits

$Enc(m_1, m_2, \ldots m_t) = c_0 c_1 \cdots c_t$ where

$c_i = r_i \oplus m_i$ and $r_i = F_k(IV + i)$

$\oplus$ as bytes

$\oplus$ Byte addition

$IV + i$ = addition modu

$Dec_k(c_0 c_1 \cdots c_t) = m_1 \cdots m_t$ where

$m_i = r_i \oplus c_i$ and $r_i = F_k(IV + i)$

Conclusion: Cipher text is $t+1$ blocks long, message is t blocks long!

<u>Thm.</u> If F is a pseudorandom function then CTR Mode has indistinguishable encryptions under CPA.

<u>Proof.</u> Test Question!