Crypto

日期: /

§§1. 知识点补充.

Discrete Probability.

(Rmk: a tool to prove security of cipher.)

1. Cipher到 rand var. 的对应:

Space of key $k := \mathcal{K}$ $\#\mathcal{K} < \infty$.

记encrypto cipher $E(m,k) := E(m) : \mathcal{K} \to V$.
$k \mapsto c$

$\Rightarrow$ 每个m对应一个随机变量$E(m)$.

2. Thm1(Xor Thm):

Thm: $\forall n$, a rand. var. Y over $\{0,1\}^n$, a uniform (均匀) rand. var. X over $\{0,1\}^n$,

X, Y indep.

$\Rightarrow Z := X \oplus Y$ is uniform var. on $\{0,1\}^n$

3. Thm2(生日悖论):

Thm: let $r_1, \cdots, r_n \in U$ be indep. uniform rand. var.s

if $n = 1.2\sqrt{|U|}$, then $P[\exists i \neq j, r_i = r_j] \geq \frac{1}{2}$

日期: /

④ Security: (Shannon).

Basic idea: Cipher text (CT) should reveal nothing about plain text (PT).

(即 there's No. ciphertext-only attack.)

(注意! attack of other types may 有效.)

Def: A cipher (E, D) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has perfect secrecy if:

$\forall\ m_0, m_1 \in \mathcal{M},\ len(m_0) = len(m_1),\ \forall\ c \in \mathcal{C}$.

记 K is uniform var. over $\mathcal{K}$. ($\mathcal{K} \xrightarrow{i.d.} \mathcal{K}$), 有:

$$P[E(k, m_0) = c] = P[E(k, m_1) = c].$$

2

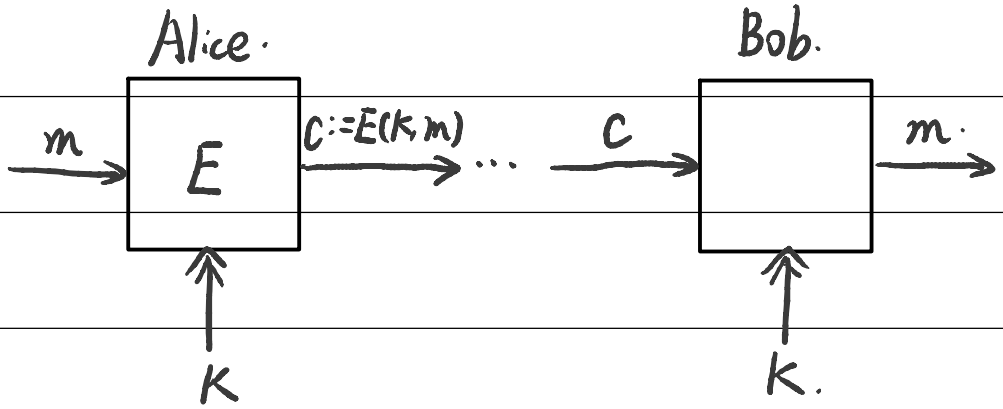
Stream Cipher

日期: /

§§2: Stream Cipher.

Symmetric Ciphers.

model:



§1: History:

1. Substitution cipher: (替换式密码).

① model:

$K :=$ { a→c, b→w, c→n, ⋮, z→a }.

eg. Caesar Cipher.

E:= shift K位.

the key space $\mathcal{K}$, $\Rightarrow \#\mathcal{K} = 26! \approx 2^{88}$.

② the way to break:

(1) Use the frequency of letters. (词频分析法)

"e": 12.7% "t": 9.1% "a": 8.1%

<= CT only attack. (ciphertext)

(2) Use the frequency of pairs of letters (diagrams)

"he", "an", "in", "th".

日期: /

2. Vigenère cipher.

① Model:

~~K is a word.~~ E: 重复书写后，与 plaintext mod26 相加，得到 ciphertext.

eg. K := CRYPTO.

C R Y P T O C R Y P T O . C R Y P T

m : W H A T A N I C E D A Y . T O D A Y

⇒ C : Z Z Z J U C L U D T U N W G C Q S

② 1° Assume the length of K is known: (:=l).

考察 kl+i 的字母，对之进行词频分析即可.

eg.

	C R Y P T O	C R Y P T O	C R Y P T
m :	(W) H A T A N	(I) C E D A Y	(T) O D A Y
⇒ C :	(Z) Z Z J U C	(L) U D T U N	(W) G C Q S

词频. E → H ⇒ K[1] = H − E = C.

(词频分析法).

2°. If the length is unknown:

从 1 开始遍历尝试.

⇐ CT only attack. (ciphertext)

3. Rotor machines.

eg. Hebern Machine, Enigma Machine.

4. Data Encryption Standard.

(1974): DES. #keys = 2^{56}. block size = 64 bits.

Today: AES(2001), Salsa20(2008), ...

block cipher. stream cipher.

日期: /

§2: Def: a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$.

is a pair of "efficient" algs. (E, D). s.t.

$D(K, E(K, m)) = m$. (一致性方程 (consistency equation)).

Rmk: ① $\mathcal{K}$: 密钥空间 $\mathcal{M}$: 信息空间 $\mathcal{C}$: 密文空间.

② encrypto: $E: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$.

decrypto: $D: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

③ "efficient" $\xrightarrow{\text{theorically}}$ poly. time.

$\xrightarrow{\text{practically}}$ eg. E: 1G/min.

④ E can be rand. alg.

D must be deterministic alg.

§3: The One Time Pad (Vernam Cipher) (OTP).

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$.

$E(K, m) = k \oplus m$. $D(k, C) = K \oplus C$

(Rmk: $1^\circ\ 0 \oplus a = a$ $2^\circ\ a \oplus a = 0$. $3^\circ\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$. $4^\circ\ a \oplus b = b \oplus a$.)

①. proof of consistency eq.:

$D(k, E(k, m)) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$.

日期: /

② Prop: $k = m \oplus c$. (即 Given m, c, 可 get k).

proof: $m \oplus c = m \oplus (k \oplus m) = k$.

③ Security:

Pf: $\forall m, c$: $P[E(k,m)=c] = \frac{\#\{\text{keys } k \in \mathcal{K} \text{ s.t. } E(k,m)=c\}}{\#\mathcal{K}}$

$= \frac{\#\{\text{keys } k \in \mathcal{K} \text{ s.t. } k \oplus m = c\}}{\#\mathcal{K}}$

$= \frac{1}{\#\mathcal{K}} = \text{const}$.

④ 优点: 迅速, 性能优越.

缺点: key k too long.

Q1: Is there a way to shorten the key?

Thm: (Shannon). perfect secrecy $\Rightarrow \#\mathcal{K} \geq \#\mathcal{M}$.

Q2: How to make it useful?

§4: Stream Cipher.

① idea: "random" key $\xrightarrow{\text{PRG}}$ "pseudorandom" key.

② model: PRG: a "eff." function $G: \underbrace{\{0,1\}^s}_{\text{seed space}} \to \{0,1\}^n$. $(n >> s)$.

$C = E(k,m) = m \oplus G(k)$.

$D(k,C) = C \oplus G(k)$.

日期: /

③ Prop: PRG must be unpredictable.

Def: $G: K \to \{0,1\}^n$ is predictable if:

$\exists$ "eff." alg. A, $\exists\ 1 \le i \le n-1$. s.t.

$$P\left[A(G(k)|_{1,\cdots,i}) = G(k)|_{i+1}\right] \ge \frac{1}{2} + \varepsilon.$$

for some "non-negl." ε.

Def: $G: K \to \{0,1\}^n$ is unpredictable if:

$\forall i$. $\nexists$ "eff" alg A. s.t. bit $(i+1)$ can be predict for "non-negl" ε.

Rmk: In theory: ε is a function $\varepsilon: \mathbb{Z}^{\ge 0} \to \mathbb{R}^{\ge 0}$.

ε is non-negl if $\exists d: \varepsilon(\lambda) \ge 1/\lambda^d$ inf. often.

In practice: ε is non-negl: $\varepsilon \ge 1/2^{30}$.

ε is negligible: $\varepsilon \le 1/2^{80}$.

---

④ Attack1: two time pad is insecure.

$$\text{if} \begin{cases} C_1 \leftarrow m_1 \oplus PRG(k). \\ C_2 \leftarrow m_2 \oplus PRG(k). \end{cases}$$

$\Rightarrow C_1 \oplus C_2 = m_1 \oplus m_2$.

for: Enough redundancy in English & ASCII encoding:

$m_1 \oplus m_2 \Rightarrow m_1, m_2$.

日期: /

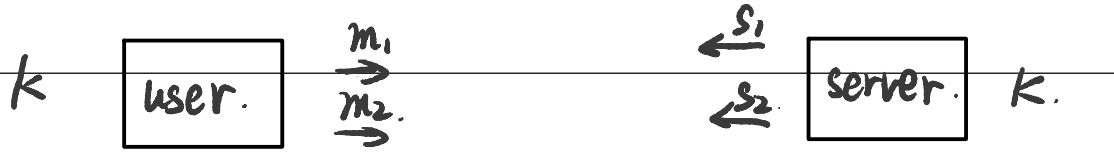
Rmk: Can't be used in Disk Encryption.

---

⑤ Weak Stream Ciphers:

1) Project Venona: 1941-1946 苏联 多次采用相同key K.

2) MS-PPTP:



$[m_1 \| m_2 \| \cdots] \oplus PRG(k)$ $[s_1 \| s_2 \| \cdots] \oplus PRG(k)$.

(Lesson: $k = (k_{s\to c}, k_{c\to s})$).

3) 802.11b WEP:

PRG(IV||K): { IV对应帧数. ⇒ 24 bits. ≈ 16M.
K对应一个固定密钥.

* 经过 16M frames 即有重复密钥.
* 重启时, IV被赋为0. ↑
* 其PRG (RC4) 有缺陷. $\xrightarrow[\text{proved}]{\text{has been}}$ 约40000帧即可还原key K.

Better-Construction:

* 通过PRG将key K扩展成大数位密码并分段应用给多次信息传输.
* 多次PRG复合.

日期: /

⑥ PRGs:

1) RC4: (software)

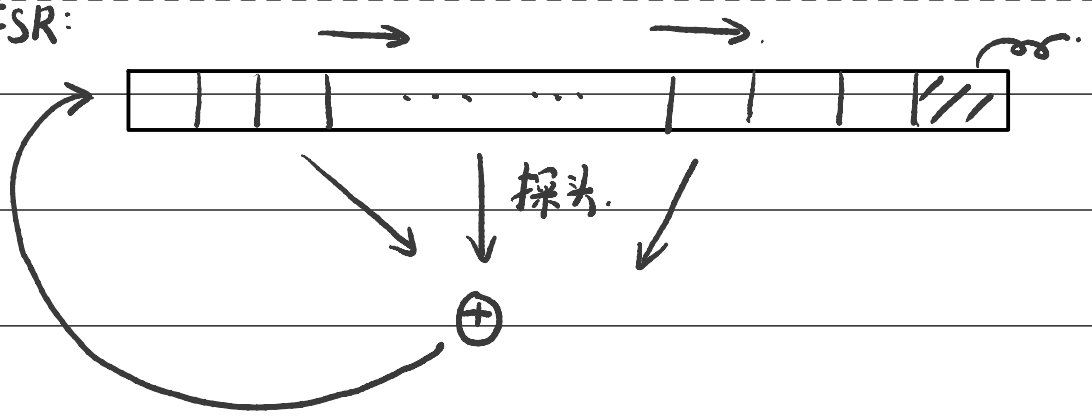
Used in HTTPS, WEP.

256位初始密钥流:

PRG:

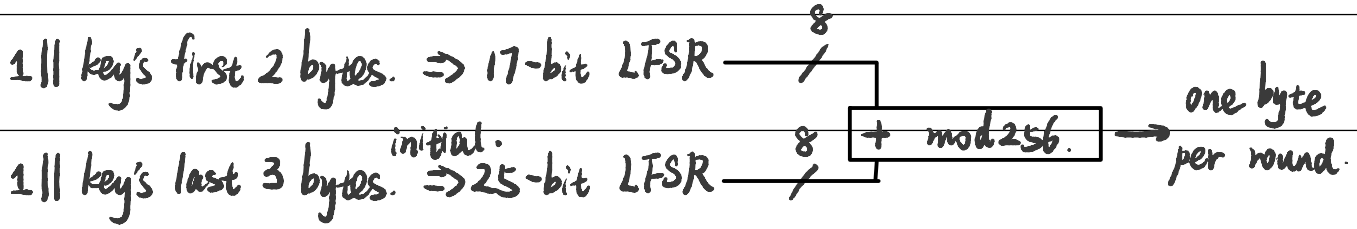
2) CSS: (hardware: DVD).

LFSR:



* seed: 40 bits = 5 bytes.

* 2 LFSRs:



* a "eff" attack: $\approx 2^{17}$ times.

根据DVD内容可以推测出前x byte

m[1-x] ⊕ C[1-x] → PRG(K)[1-x].

日期: /

枚举 2^{17} bit 的LFSR初始状态

PRG[1-X]

$\Rightarrow$ 得到 2^{25} bit 的前 8X 次输出.

$\Rightarrow$ 可以判断输出是否符合LFSR特性.

3) eStream: Salsa 20 (2008, a good exmaple in eStream).

PRG: $\{0,1\}^s \times r \to \{0,1\}^n$.

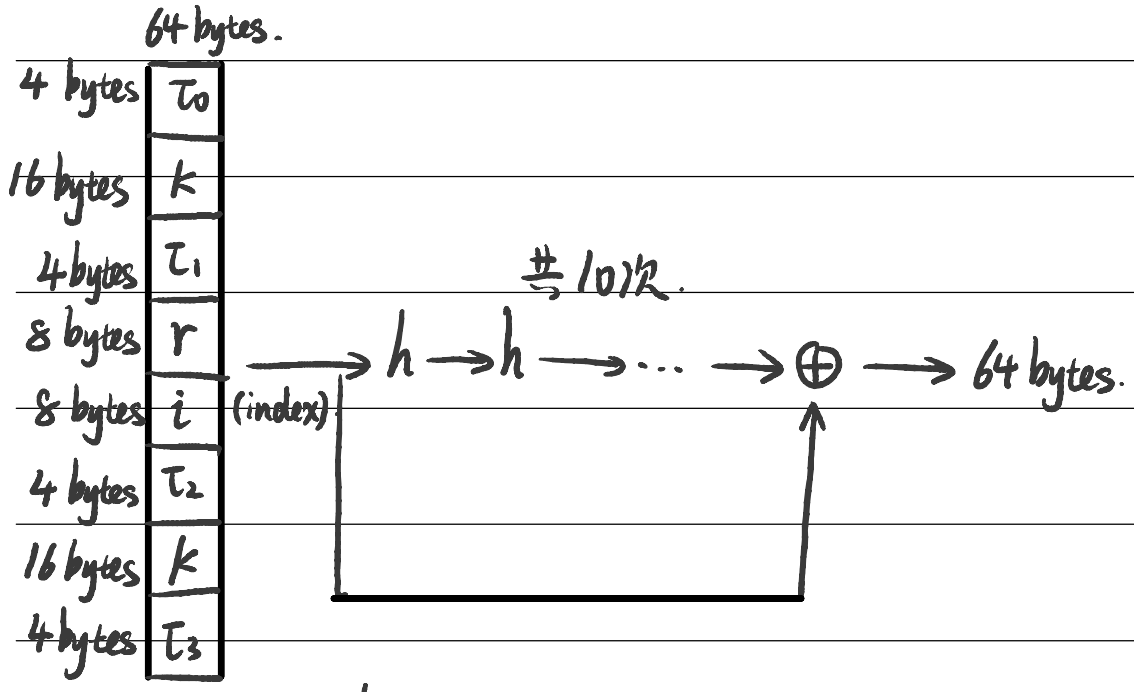
↑ seed ↑ nonce ↑ key

Rmk: nonce: a 不重复 value for given key.

$\Rightarrow$ (k,r) is never used more than once. (从而允许重复使用 key k).

$\{0,1\}^{128/256} \times \{0,1\}^{64} \to \{0,1\}^n$ (max $n = 2^{73}$ bits).

$Salsa20(k;r) := H(k,(r,0)) \,||\, H(k,(r,1)) \,||\cdots$



h = invertible. function.

日期: /

security $\approx 2^{128}$. unpredictable.

---

① Attack 2: No. integrity. (OTP is malleable).

$m \xrightarrow{E(m,k)} c = m \oplus k$.

$c = m \oplus k$ ↓ attack.

$m \oplus p \xleftarrow{D(c',k)} c' = m \oplus k \oplus p$.

Rmk: if want $m \to m'$. then $p = m \oplus m'$.

§5. Secure PRG.

① Goal: let $G: K \to \{0,1\}^n$ be a PRG.

s.t. $[k \xleftarrow{R} K$, output $G(k)]$ is "indistinguishable" from

$[r \xleftarrow{R} \{0,1\}^n$, output $r]$.

② Def:

Def1: Statistical Test on $\{0,1\}^n$: (Rmk: way to def. indist.)

an alg. A s.t. $A(x)$ outputs "0" or "1". $x \in \{0,1\}^n$.

"0" ↑ not random; "1" ↑ random.

eg. (1) $A(x)=1$ iff $|\#0(x) - \#1(x)| \le 10\sqrt{n}$.

(2) $A(x)=1$ iff $|\#00(x) - \frac{n}{4}| \le 10\sqrt{n}$.

日期: /

(3) $A(x)=1$ iff maxlen-of-consis-D(x) $\leq 10\cdot\log_2 n$.(即 $\approx \log_2 n$)

Def2: Advantage:

let $G: K \to \{0,1\}^n$ be a PRG, A a stat. test on $\{0,1\}^n$.

then, $Adv_{PRG}[A,G] ::= \left| \underset{k \xleftarrow{R} K}{P}[A(G(k))=1] - \underset{r \xleftarrow{R} \{0,1\}^n}{P}[A(r)=1] \right|$

* $Adv_{PRG} \approx 1$ $\Rightarrow$ A can distinguish G from rand.

* $Adv_{PRG} \approx 0$ $\Rightarrow$ A cannot distinguish G from rand.

Def3: Secure PRG:

$G: K \to \{0,1\}^n$ is a secure PRG if:

$\forall$ "eff" stat. test A:

$Adv_{PRG}[A,G]$ is "neg".

(Rmk: 1) 如果去掉"eff", 则 $G(k) \sim r \xleftarrow{R} \{0,1\}^n$.
$k \xleftarrow{R} K$

当 $\#K < 2^n$, 这会产生歧.

2) 事实上, $\exists$ secure PRG $\Leftrightarrow P \neq NP$.

即, 是否 $\exists$ secure PRG is unknown.

&, cannot prove a PRG is secure).

③ Thm: a secure PRG is unpredictable.

Pf: a PRG $G: K \to \{0,1\}^n$ is predictable.

日期: /

$\Rightarrow \exists$ "eff" A, s.t. $P[A(x|_{1,\cdots,i}) = x_{i+1}] > \frac{1}{2}+\varepsilon$. , ε is "non-negl".

$\Rightarrow$ def B as: $B(x) = \begin{cases} \text{if } A(x|_{1,\cdots,i}) = x_{i+1}, \text{ output } 1. \\ \text{else output } 0. \end{cases}$

$\Rightarrow P[B(r)=1] = \frac{1}{2}$, $r \xleftarrow{R} \{0,1\}^n$.

$P[B(G(k))=1] > \frac{1}{2}+\varepsilon$, $k \xleftarrow{R} \mathcal{K}$.

$\Rightarrow Adv_{PRG}[B, G] > \varepsilon$. $\Rightarrow G$ is not secure.

(逆命题).

Thm (Yao'82): an unpredictable PRG is secure.

(Rmk: 即, if $\forall i$, PRG is unpredictable at pos. i. then G is a secure PRG)

Pf: 待证.

日期: /

Cor: $G: K \to \{0,1\}^n$, if $\exists A, i$, s.t. $P[A(x|_{i,i+1,\cdots,n}) = x_{i-1}] > \frac{1}{2} + \varepsilon$.

then, $\exists B, j$, s.t. $P[B(x|_{1,\cdots,j}) = x_{j+1}] > \frac{1}{2} + \varepsilon$. ($\varepsilon$ is "non-neg.")

Pf: $\Rightarrow$ G is not secure.

$\Rightarrow$ G is predictable. $\Rightarrow$ #.

④ Generalization: computationally indistinguishable

Let P_1, P_2 be 2 distributions over $\{0,1\}^n$.

Def: P_1, P_2 are computationally indistinguishable (denoted as $P_1 \approx_p P_2$)

if $\forall$ "eff" stat. tests A,

$$\left| P[A(x)=1] - P[A(x)=1] \right| < \varepsilon \quad (\varepsilon \text{ is "neg".}).$$
$$x \leftarrow P_1 \qquad x \leftarrow P_2.$$

Cor: a PRG is secure if $\{k \xleftarrow{R} \mathcal{K} : G(k)\} \approx_p \text{uniform}(\{0,1\}^n)$.

§6. Semantic Security.

1.) Recall: Shannon's perfect secrecy:

A cipher (E, D) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has perfect secrecy if:

$\forall m_0, m_1 \in \mathcal{M}$, $\text{len}(m_0) = \text{len}(m_1)$., $\forall c \in \mathcal{C}$.

记 K is uniform var. over $\mathcal{K}$. ($\mathcal{K} \xrightarrow{i.d.} \mathcal{K}$)., 有

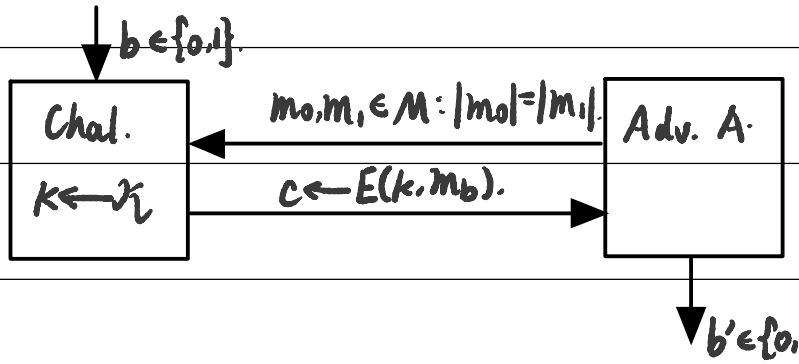
$P[E(K, m_0) = c] = P[E(K, m_1) = c]$. (即 $\{E(K, m_0)\} = \{E(K, m_1)\}$.)

this definition is too strong!

日期: /

2) Semantic Security.(语义安全).

Def: S.S. Adv:



for a adversary A, for b=0,1,

def: $W_b := [\text{event that } Exp(b)=1]$.

def: $Adv_{SS}[A,E] := |P[W_0]-P[W_1]|$.

Def: E is semantically secure if for all "eff" A,

$Adv_{SS}[A,E]$ is "negl".

(Rmk: that's to say, for all "explicit" $m_0,m_1 \in M$., $\{E(k,m_0)\} \approx_p \{E(k,m_1)\}$)

Adversary can think of.
⇒ 蕴含于"eff" A.

3) Thm: $\forall$ A, $Adv_{SS}[A,OPT]=0$.

Pf: $\forall m_0,m_1$, $\{k\leftarrow K : k\oplus m_0\} = \{k\leftarrow K : k\oplus m_1\}$.

$\Rightarrow Adv_{SS}[A,OPT]=|P[W_0]-P[W_1]|=0$.

(Rmk: even 不要求 A "eff".)

日期: /

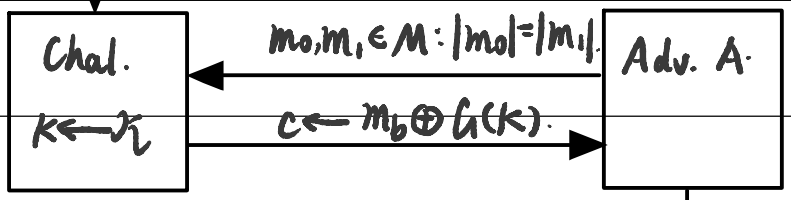
4) Thm: Stream cipher E derived from a secure PRG G is sem. sec.

Pf: 想法: 考察用 $r \xleftarrow{R} \{0,1\}^n$ 替换PRG G 的影响.

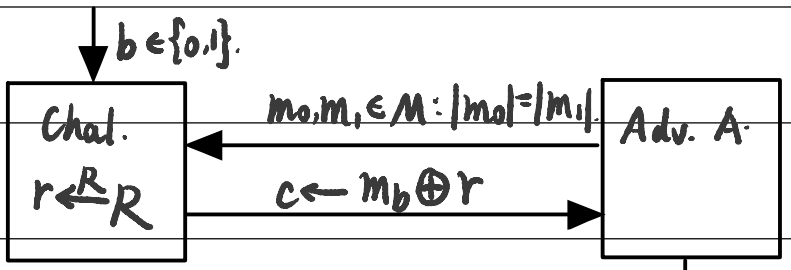
Lem: $\forall$ "eff" sem. sec. adversary A, $\exists$ a "eff" PRG adversary B, s.t.

$$Adv_{SS}[A,E] < 2\,Adv_{PRG}[B,G].$$

pf: for $\forall$ "eff" A, $b \in \{0,1\}$.



def: W_b = [event that $b' = 1$].

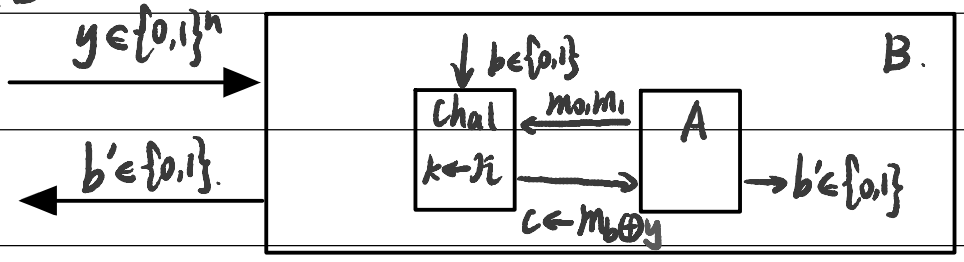


def: R_b = [event that $b'' = 1$].

注意到 R_b 对应 OPT, $\therefore$ 有 $P[R_0] = P[R_1]$

Claim: $\exists$ "eff" PRG adversary B, s.t. $|P[R_b] - P[W_b]| = Adv_{PRG}[B,G]$.

构造 B:



日期: /

then, $Adv_{PRG}[B,G] = \left| P[\underset{r \xleftarrow{R} R}{B(r)=1}] - P[B(G(k))=1] \right|$

$= |P[R_b] - P[W_b]|$

$\therefore Adv_{SS}[A,E] = |P[W_0] - P[W_1]|$

$\leq |P[W_0] - P[R_0]| + |P[R_0] - P[R_1]| + |P[R_1] - P[W_1]|$

$= 2\,Adv_{PRG}[B,G]$. #.

Thm Pf: 由 secure PRG G, $\forall$ "eff" B, $Adv_{PRG}[B,G] < \varepsilon$. ($\varepsilon$ is "neg").

由 Lem, $\forall A, \exists B$, s.t. $Adv_{SS}[A,E] \leq 2Adv_{PRG}[B,G] < 2\varepsilon$.

$\Rightarrow E$ is sem. sec. #.

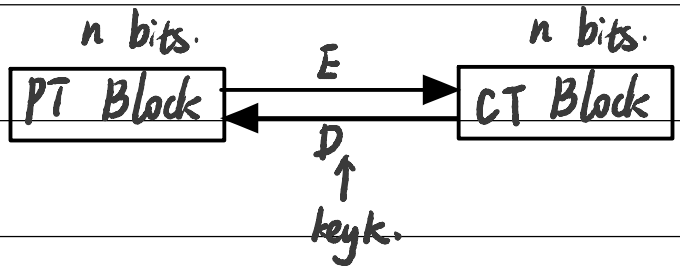
3

Block Cipher

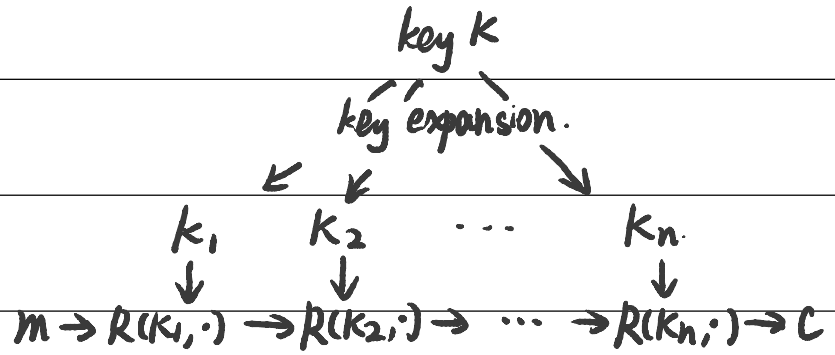
日期: /

§§3: Block Cipher.

§1: General Model:



Block Cipher usually is built by Iteration.



eg. for 3DES (n=48). , for AES-128 (n=10).

§2: PRPs & PRFs.

① Pseudo Random Function (PRF) defined over (K, X, Y):

$$F: K \times X \to Y.$$

such that exists "efficient" alg. to evaluate F(k, x)

② Pseudo Random Permutation (PRP) defined over (K, X):

$$E: K \times X \to X.$$

such that: 1) E is PRF.

2) E is one-to-one 且 ∃ "efficient" inver. alg. D(k, y).

(⇔ E is permutation.)

日期: /

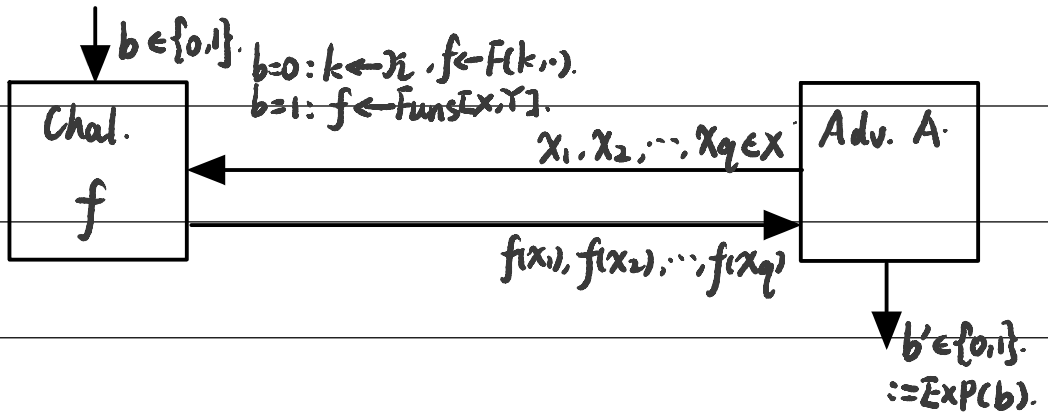
③ Secure PRFs:

1) Intuition: a PRF is secure if:

a random function in Funs[X,Y] is indistinguishable from a random function in S_F.

#f, $\begin{cases} \text{Funs}[X,Y]: \{\text{all functions from } X \text{ to } Y\} \\ S_F = \{F(k,\cdot) \text{ s.t. } k \in \mathcal{K}\} \end{cases}$

2) Def Adv_{PRF}:



def: W_b := Event that $Exp(b)=0$.

$Adv_{PRF}[A,F] = |W_0 - W_1|$.

3) Def: F is a Secure PRF if for all "efficient" A ($<2^{80}$ times):

$Adv_{PRF}[A,F]$ is "negligible".

(Rmk: Adv_{PRP} & secure PRP 's def. 类似).

e.g. for all 2^{80}-time algs. A, $adv_{PRP}[A,AES] < 2^{-40}$.

日期: /

4) Application: (PRF ⇒ PRG).

Let $F: K \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF.

then a secure PRG: $G: K \to \{0,1\}^{nt}$ can be constructed:

$G(k) = F(k,0) || F(k,1) || \cdots || F(k,t)$.

(intuition: 将 $F(k,\cdot)$ 用 true random function $f(\cdot)$ 替代).

5) PRF Switching Lemma:

Any secure PRP is also a secure PRF, if $|X|$ 足够大.

Proof:

lem: let F be a PRP over $[K, X]$, then,

for any q-query adversary A,

$$|Adv_{PRP}[A,F] - Adv_{PRF}[A,F]| < q^2/2|X|.$$

⇒ Suppose $|X|$ is large s.t. $q^2/2|X|$ is "neg".

Then, $Adv_{PRP}[A,F]$ is "neg" ⇒ $Adv_{PRF}[A,F]$ is "neg".

(lem 特征). Hint: 生日悖论.

日期: /

§3: DES & AES.

① DES: key-len = 56 bits. block-len = 64 bits. 16-round.

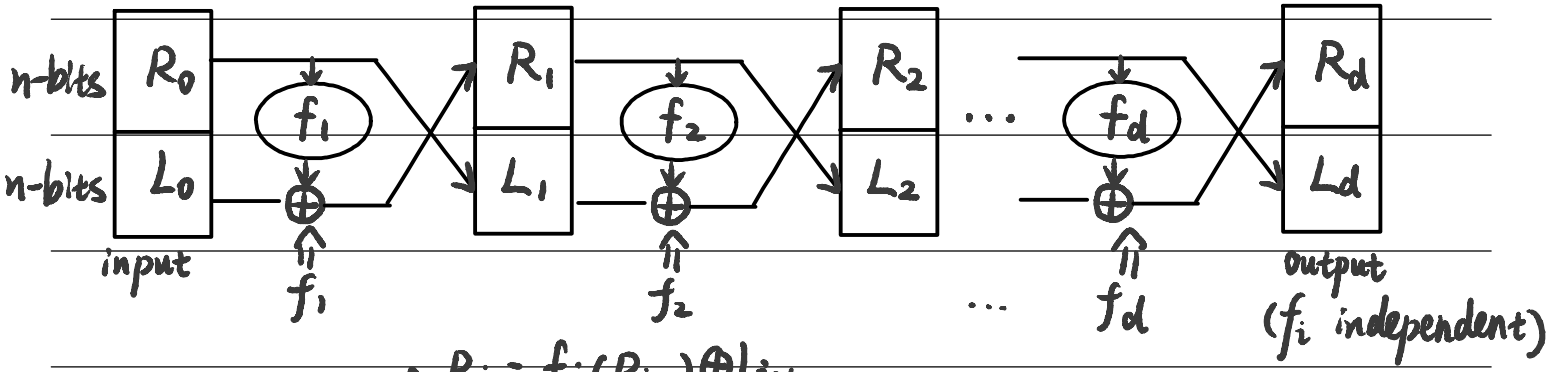
---

core idea: Feistel Network.

Given functions: $f_1, \cdots, f_d : \{0,1\}^n \to \{0,1\}^n$.

Goal: build invertible function $F: \{0,1\}^{2n} \to \{0,1\}^{2n}$.

Network:

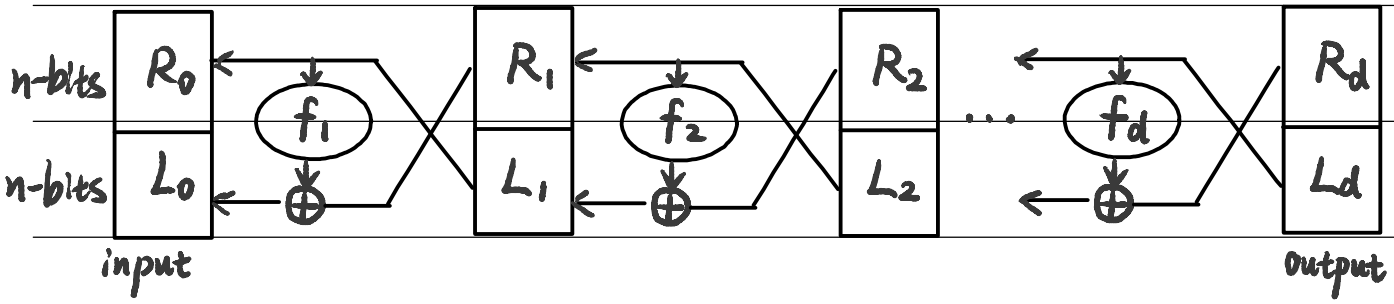


in symbols: $\begin{cases} R_i = f_i(R_{i-1}) \oplus L_{i-1} \\ L_i = R_{i-1} \end{cases}$ $i = 1, \cdots, d$.

Notice! We can easily give its invertion function:

in symbols: $\begin{cases} R_{i-1} = L_i. \\ L_{i-1} = f_i(L_i) \oplus R_i. \end{cases}$

Invertion Network:

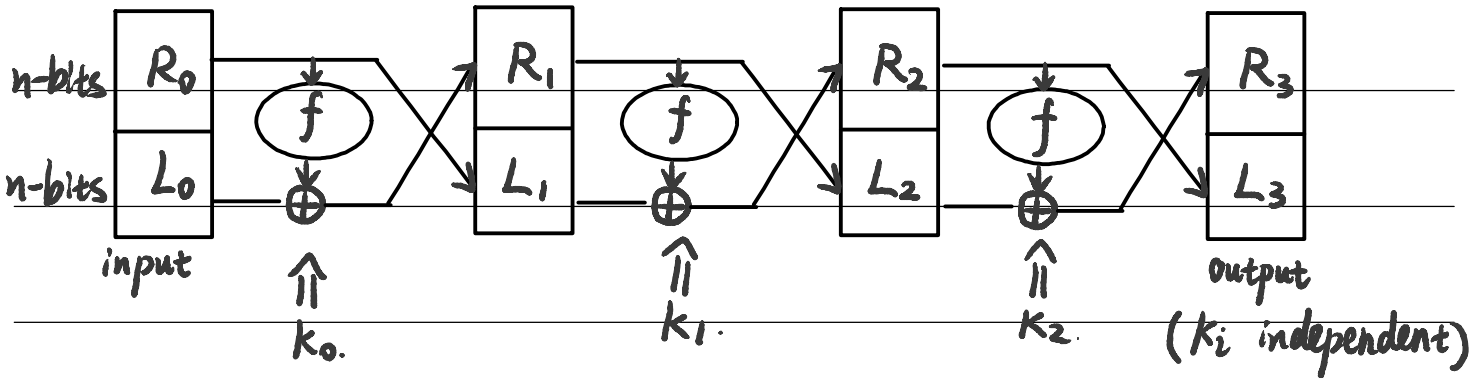


Thm: (Luby-Rackoff). (不证).

日期: /

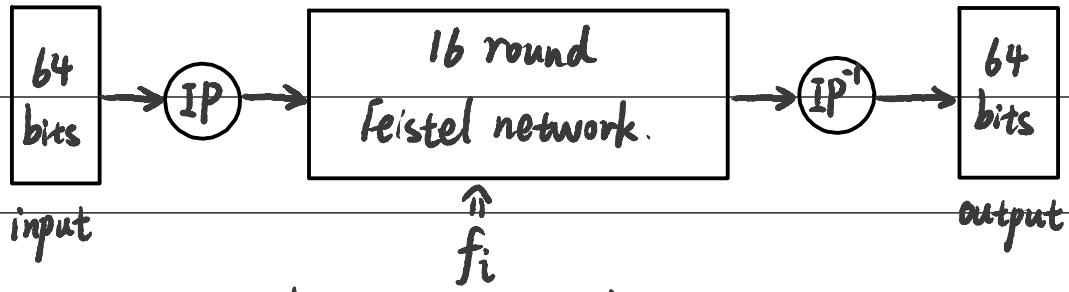
$f: K \times \{0,1\}^n \to \{0,1\}^n$ a secure PRF.

$\Rightarrow$ 3-round Feistel $F: K^3 \times \{0,1\}^{2n} \to \{0,1\}^n$ is a secure PRP.

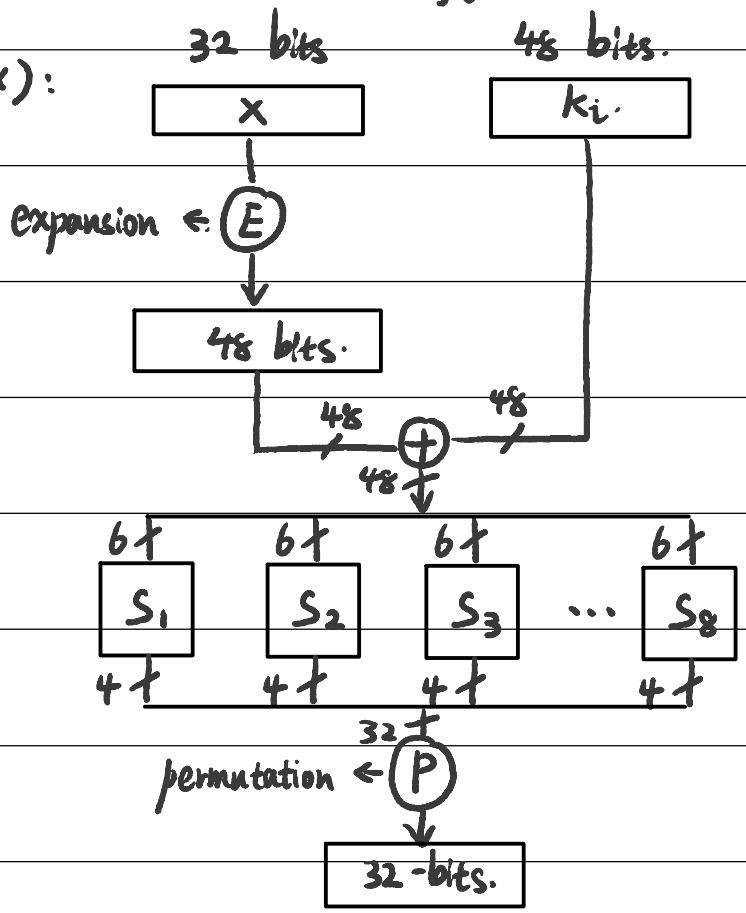


---

1) model: $f_1, \cdots f_{16}: \{0,1\}^{32} \to \{0,1\}^{32}$, $f_i(x) := F(k_i, x)$.



2) $F(k_i, x)$:



其中, S-box 是一个 6-bit: 4-bit 查找表

日期: /

3) Notice! S shouldn't be linear.

Or: all DES do is xors and permutations. then,

∃ fixed matrix. B s.t. $832 = 64 + 16 \times 48$

$$DES(k,m) = \underset{64}{\boxed{B}}_{832} \cdot \begin{bmatrix} m \\ k_1 \\ \vdots \\ k_{16} \end{bmatrix} = \boxed{C} \pmod 2.$$

so then, DES satisfy:

$$DES(k,m_1) \oplus DES(k,m_2) \oplus DES(k,m_3)$$

$$= B \cdot \begin{bmatrix} m_1 \\ k \end{bmatrix} \oplus B \begin{bmatrix} m_2 \\ k \end{bmatrix} \oplus B \cdot \begin{bmatrix} m_3 \\ k \end{bmatrix} = (B \oplus B \oplus B) \cdot \begin{bmatrix} m_1 \oplus m_2 \oplus m_3 \\ k \oplus k \oplus k \end{bmatrix} = B \cdot \begin{bmatrix} m_1 \oplus m_2 \oplus m_3 \\ k \end{bmatrix}$$

$$= DES(k, m_1 \oplus m_2 \oplus m_3).$$

⇒ this can be used to tell DES from truly random functions.

⇒ insecure.

(In fact, 仅需832个输入-输出对即可还原 key $K_1, \cdots, K_{16}$.)

? (猜测: 64即可).

Rmk: even close to linear can lead to insecure.

4) Exhaustive Search Attacks.

1° Goal: given a few input-output pairs $(m_i, c_i = E(k, m_i))$, find key K.

2° Lem: (for given m_i-c_i, key K is (almost) unique.).

1') suppose DES is an ideal cipher

(即 2^{56}个 random invertible funs: $\{0,1\}^{64} \to \{0,1\}^{64}$).

日期: /

Then, $\forall m, c$, there is at most one key K s.t. $C = DES(k, m)$

with prob. $\geq 1 - 2^{-8} \approx 99.5\%$.

Pf: $P[\exists k' \neq k: C = DES(k,m) = DES(k',m)]$

$\leq \sum_{k' \in \mathcal{K} \setminus \{k\}} P[C = DES(k', m)]$

$= \#\mathcal{K} \cdot \frac{1}{2^{64}}$.

$= 2^{-8} \cdot \#$.

2° suppose DES is an ideal cipher (即 2^{56}个 random invertible fun.s)

Then, $\forall (m_1, c_1), (m_2, c_2)$, there is at most one key K

s.t. $C_1 = DES(k, m_1)$ 且 $C_2 = DES(k, m_2)$.

with prob. $\geq 1 - 2^{71}$.

(同理可证).

3° DES challenge.

(use 3 bytes plaintext-ciphertext pairs.).

⇒ Goal: find $k \in \{0,1\}^{56}$, s.t. $DES(k, m_i) = C_i$ for $i = 1, 2, 3$.

⇒ 穷举 2^{56}.

4° Strengthening against ex. search:

Method 1: Triple-DES

let $E: K \times M \to C$ be a block cipher. Define $3E: K^3 \times M \to C$. as:

日期: /

$3E((k_1,k_2,k_3),m) = E(k_1, D(k_2, E(k_3,m)))$.

$\#\mathcal{K}^3 = 2^{168}$. & 理论上的最佳 attack is 2^{118} ($\approx 2^{112} \cdot \log_2 2^{56}$)

Ques. Why not use double DES?

$\Rightarrow$ $2E((k_1,k_2),m) = E(k_1, E(k_2,m))$. $\#\mathcal{K}^2 = 2^{112}$.

here's a meet-in-the-middle attack.:

Step1: $\Rightarrow$ $E(k_2,m) = D(k_1,c)$.

Step2: build table for $k_2 - E(k_2,c)$., $k_2 \in \{0,1\}^{56}$.

& sort the table. $\Rightarrow 2^{56} \cdot \log_2 2^{56}$.

Step3: for all $k_1 \in \{0,1\}^{56}$, find in table. $\Rightarrow 2^{56} \cdot \log_2 2^{56}$.

Step4: 验证 (k_1,k_2) for (m',c'). (for each test).

$\Rightarrow 2^{63}$. times.

Method2: DESX.

Define EX: $EX((k_1,k_2,k_3),m) = \overset{2^{64}}{k_1} \oplus E(\overset{2^{56}}{k_2}, m \oplus \overset{2^{64}}{k_3})$.

easy attack: $2^{120} = (2^{56} \cdot 2^{64})$.

Rmk. for $k_1 \oplus E(k_2,m)$, $E(k_2, m \oplus k_3)$.

has attack in 2^{56} times.

($k_1 = E(k_2,m) \oplus C$, 可得 2^{56} 个 (k_1,k_2) 对).

日期: /

5) Other attacks:

1° Side channel attacks:

measure time to do E/D. ; measure power to do E/D. ; ...

2° Fault attacks:

In the last round, compute some errors (which exposes the secret key k).

3° Linear Cryptanalysis:

Suppose for random k, m:

$P[m[i_1]\oplus\cdots\oplus m[i_r]\oplus c[j_1]\oplus\cdots\oplus c[j_v] = k[l_1]\oplus\cdots\oplus k[l_u]] = \frac{1}{2}+\varepsilon$. for some ε.

⇒ for DES. $\varepsilon = 2^{-21}$. (因为5th S-box a little linear.).

Thm: given $1/\varepsilon^2$ random m-c pairs. then,

$k[l_1]\oplus\cdots\oplus k[l_u] = MAJ[m[i_1]\oplus\cdots\oplus m[i_r]\oplus c[j_1]\oplus\cdots\oplus c[j_v]]$

with prob. ≥ 97.7%.

Rmk: roughly speaking, can find 14 key "bits"(即关系). in 2^{42}.

剩余 56-14=42 bits 使用 EX.

⇒总共 2^{43} attack times. ($<< 2^{56}$).

4° Quantum Attack:

a Generic Search Problem can be generally 抽象 as:

Let $f: X \to \{0,1\}$ be a function.

日期: /

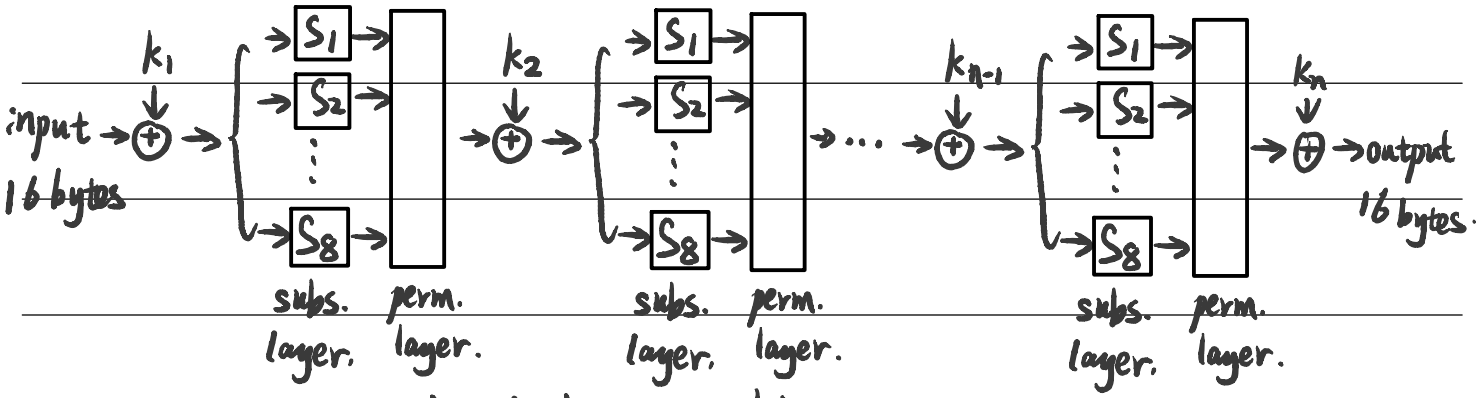
Goal: find $x \in X$, s.t. $f(x)=1$.

on classical computer: best generic alg. time $= O(|X|)$.

on quantum computer: time $= O(|X|^{1/2})$.

② AES.

1) model: key size = 128/192/256 bits. block size = 128 bits.



rmk: everything should be invertible.

- ByteSub: 查找表.
- ShiftRows: 每行递增左移
- MixColumns: 列混淆.

2). Attacks:

最佳 attack: AES-128: 2^{126}.

AES-256: 2^{99} (for related keys).

§4: Block Ciphers from PRGs. (GGM-PRF).

let $G: K \to K^2$ be a secure PRG.

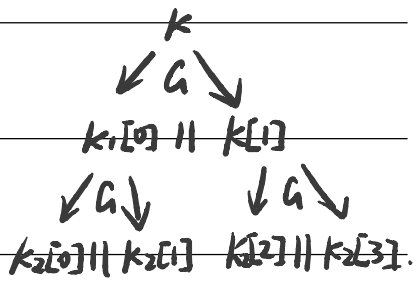
日期: /

Define PRF: $K \times \{0,1\}^n \to K$ as:

$F(k, x) = G(F(k, x_0 \cdots x_{n-2}))[x_{n-1}]$.

for $x = x_0 x_1 \cdots x_{n-1} \in \{0,1\}^n$.

eg. $n=2$.



Rmk: we can use a secure PRG to build a secure PRP.

⇒ plug GGM PRF into Feistenel network.

(but efficiency is not good.).

§5. Using Block Ciphers. (Ideal Models).

① An Incorrect use: Electronic Code Book (ECB):

PT: $\overbrace{m_1, m_2, \cdots}^{\text{blocks}}$

$\Downarrow E(k, \cdot)$

CT: $c_1, c_2, \cdots$

Problem: if $m_{i,1} = m_{i2}$, then $c_{i,1} = c_{i2}$

Prop: ECB is not Semantically Secure:

Pf: for example, choose $m_0 =$ "$\overbrace{\text{Hello World}}^{\text{2 blocks}}$", $m_1 =$ "Hello Hello".

then $Adv_{SS}[A, ECB] = 1$.

Secure Constructions are follow:

② One-time key:

deterministic counter mode:

日期: /

Suppose F is a secure PRF,

def: $E_{DETCTR}(k,m) =$

	m[0]	m[1]	...	m[L]
⊕	F(k,0)	F(k,1)	...	F(k,L)
	c[0]	c[1]	...	c[L]

(Notice! only require PRF, ⇒ Salsa20 is OK.(可以采用3DES, AES等).

Thm: for any L>0, if F is a secure PRF over (K, X, X), then

E_{DETCTR} is S.S. cipher over (K, X^L, X^L).

Lem: for ∀ "eff" adversary A for E_{DETCTR}.

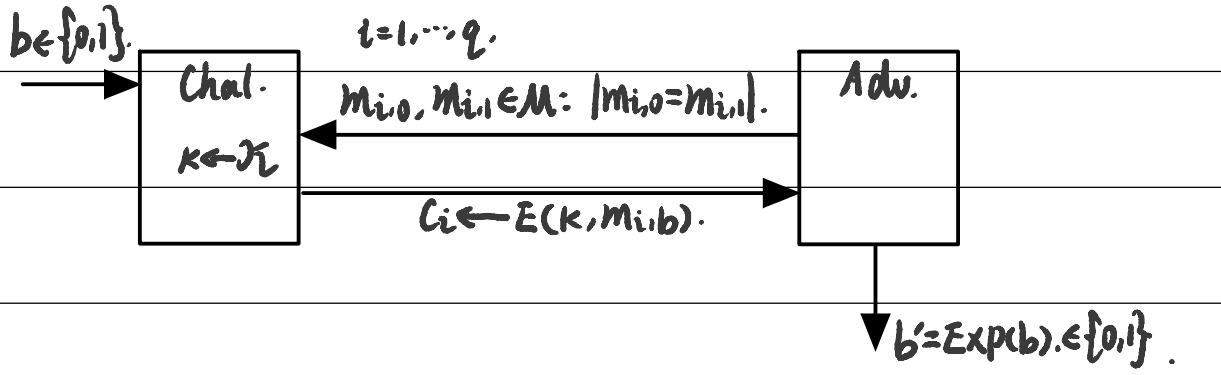
there exists an "eff" PRF adversary B for F.

S.t. $Adv_{SS}[A, E_{DETCTR}] = 2 \cdot Adv_{S.S}[B, F]$.

待证(替换法)

③ Semantic Security for many-time key.

E defined over $(\mathcal{K}, \mathcal{M}, \mathcal{L})$. For b=0,1, define EXP(b) as:



(Notice! Adversary can use CPA (chosen-plaintext attack):

日期: /

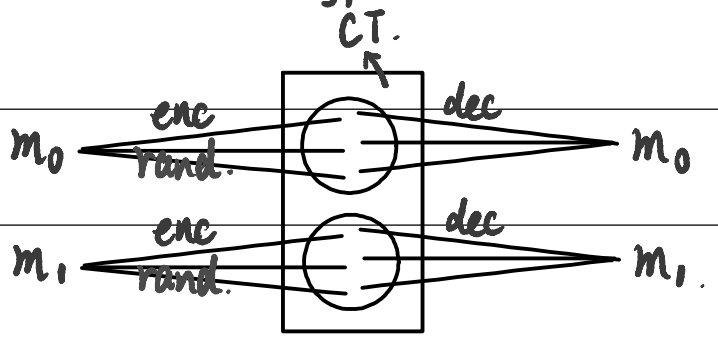
if adv. wants $c=E(k,m)$, it can use $m_{j,0}=m_{j,1}=m$, for some j.).

Def: E is sem. sec. under CPA if for all "eff" A:

$Adv_{CPA}[A,E] = |P[EXP(0)=1] - P[EXP(1)=1]|$ is "neg".

④ Many-time key.

1) Randomized Encryption.

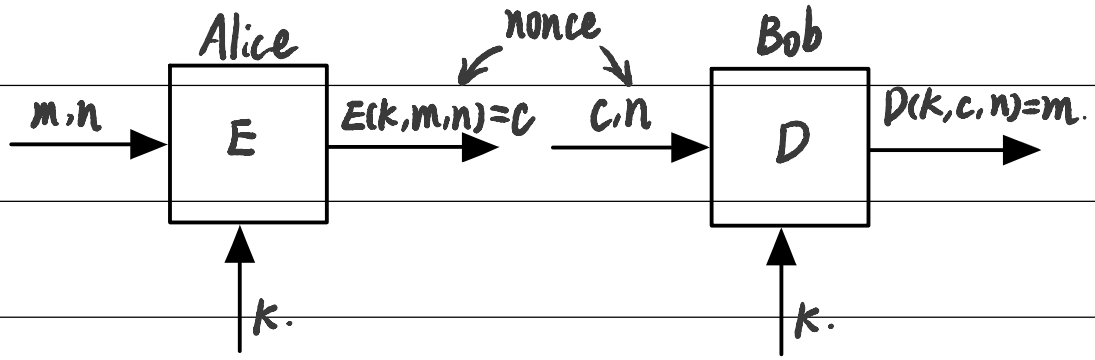


[roughly speaking:
CT-size = PT-size + "#rand. bits".]

* encrypting same msg. twice gives different ciphertexts.
* the "circles" shouldn't be crossed.

⇒ one cyphertext must be correspond to one plaintext. (反过来不是).

2) Nonce-based Encryption.



* nonce n: S.t. (k,n) pair never used more than once.

*way to choose nonce:

日期: /

- counter. (优势. no need to 包含 nonce in packs.).

- random nonce. ($n \leftarrow \mathcal{N}$).

Rmk: for nonce-based cipher E's sem. sec. under CPA,

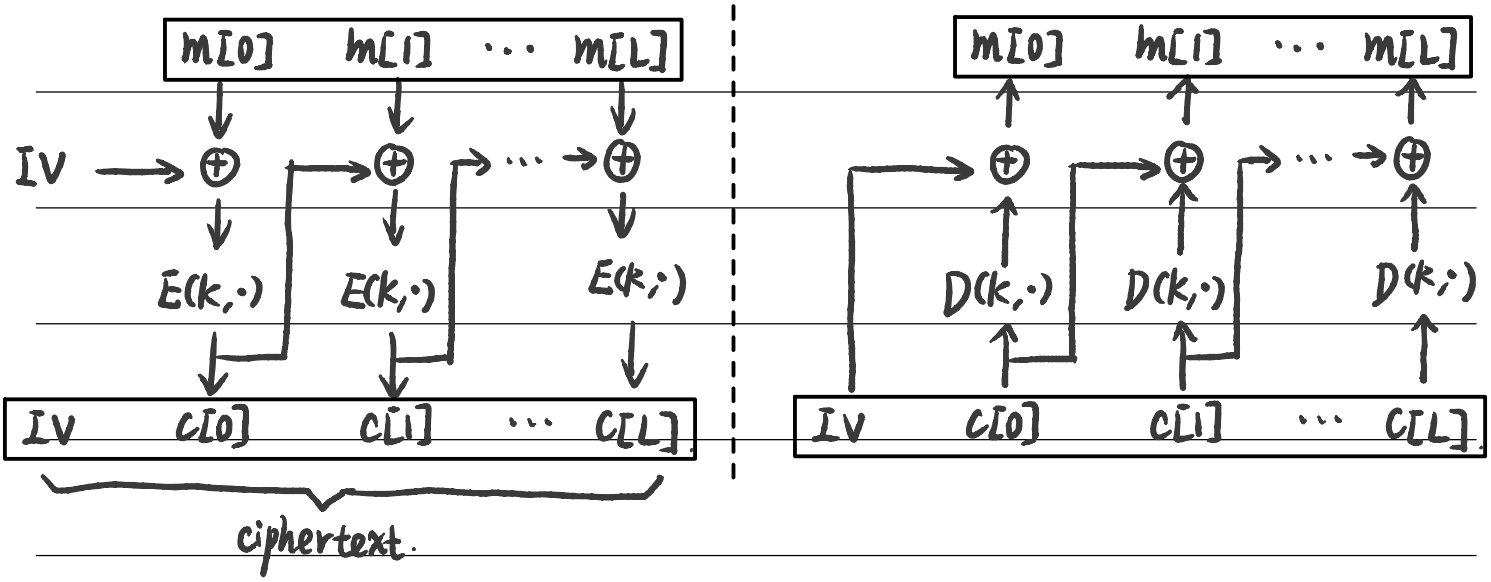
allow adversary choose nonce n_i.

but all nonces $\{n_1, \cdots, n_q\}$ must be distint.

§6. Concrete Construction.

(cipher block chaining)

① CBC with random IV. (choose random $IV \leftarrow X$)



In symbols: $c[0] = E(k, IV \oplus m[0])$ $\Rightarrow$ $m[0] = IV \oplus D(k, c[0])$.

$c[i] = E(k, c[i-1] \oplus m[i])$. $m[i] = c[i-1] \oplus D(k, c[i])$.

Thm (CPA analysis):

for any $L > 0$, if E is a secure PRP over (K, X), then

E_{CBC} is S.S. cipher under CPA over (K, X^L, X^{L+1}).

日期: /

Lem: for a q-query adv. A attacking E_{CBC},

∃ PRP adv. B s.t.

$$Adv_{CPA}[A, E_{CBC}] \le 2 \cdot Adv_{PRP}[B, E] + 2 \cdot q^2 L^2 / |X|.$$

Pf:

(Rmk: ⇒ CBC is secure ⇔ $q^2L^2 << |X|$).

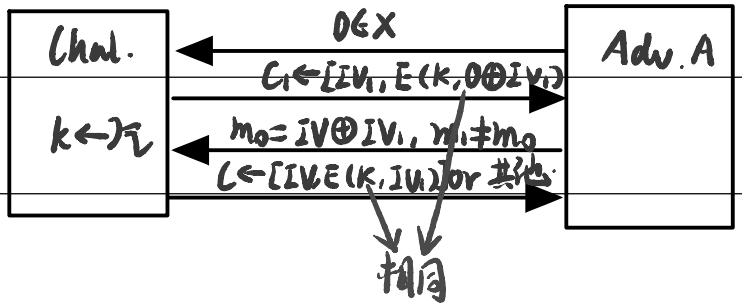
⇒ max 加密 blocks under CPA.

eg. suppose want $Adv_{CPA}[A, E_{CBC}] \le 1/2^{32}$:

* E=AES-128. $|X| = 2^{128}$ ⇒ $qL < 2^{48}$ ⇒ after 2^{48} AES blocks, must change key.
* E=3DES. $|X| = 2^{64}$ ⇒ $qL < 2^{16}$.

Notice! If IV is predictable, then CBC with random IV is not S.S. under CPA.

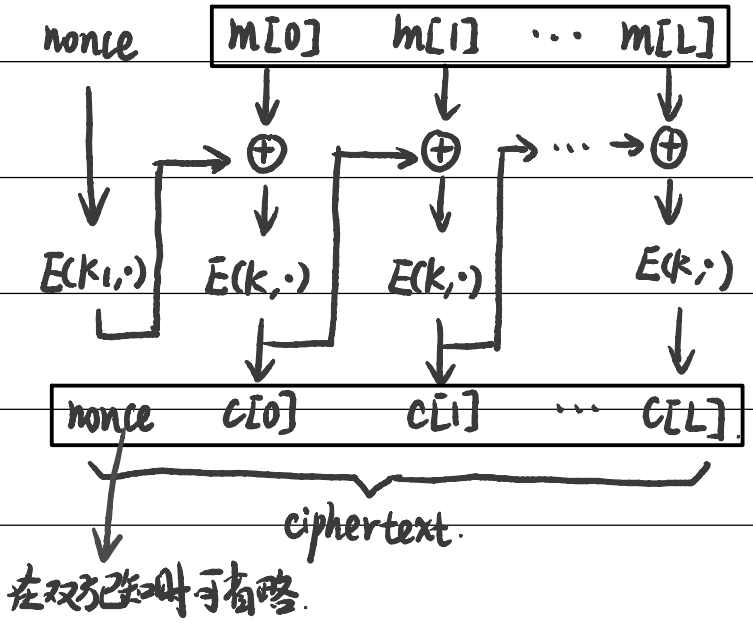
eg. suppose 由 IV_1 predict IV.



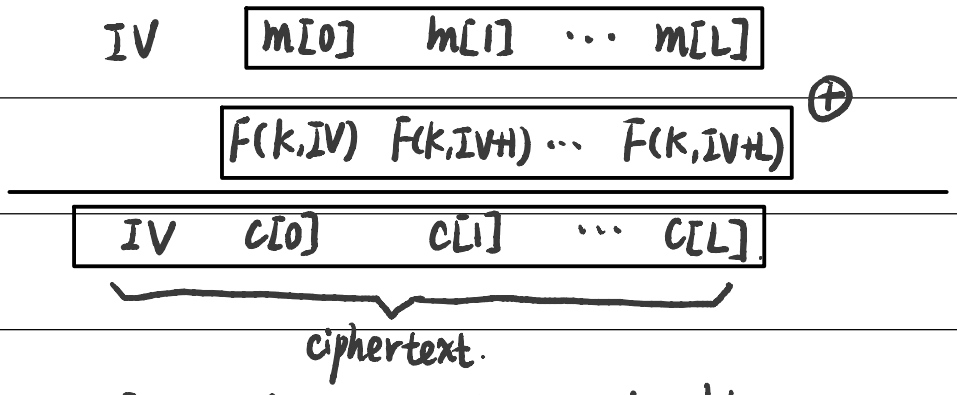
$Adv_{CPA}[A, CBC] = 1$.

日期: /

② nonce-based CBC. ($IV \leftarrow E(K_1, nonce)$).



③ rand. ctr-mode. (PRF is enough).



(Rmk: IV is also required unpredictable)

Thm (CPA analysis):

for any $L>0$, if E is a secure PRF over (K, X, X), then

E_{CTR} is S.S. cipher under CPA over (K, X^L, X^{L+1}).

Lem: for a q-query adv. A attacking F ,

∃ PRP adv. B s.t.

日期: /

$Adv_{CPA}[A, E_{CTR}] \le 2 \cdot Adv_{PRF}[B, F] + 2 \cdot q^2 L / |X|$.

Pf:

(Rmk: $\Rightarrow$ CBC is secure $\Leftrightarrow q^2 L^2 << |X|$

better than CBC mode.

④ Summary:

Comparison: CBC vs CTR.

CBC	CTR
PRP	PRF
串行	并行
$q^2 L^2 << \|X\|$.	$q^2 L << \|X\|$.
need dummy padding block.	No.

$\Rightarrow$ CTR 优于 CBC. (各方面)

↓ can be solved by "ciphertext stealing".

Summary:

one-time key	many-time key (CPA)	CPA & integrity.
stream cipher. & DET CTR-mode.	rand CBC. & nonce-based CBC. & rand CTR-mode	later

4

Message Integrity

日期: /

§§4. Message Integrity.