§Chap 1. Modern Cryptography Intro.

- Syntax

Gen(·) → sk ⓡ

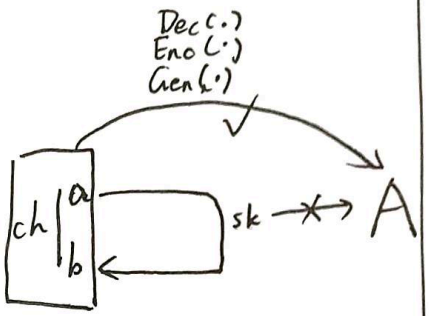
Enc(sk, m) → c ⓡ/ⓓ

Dec(sk, c) → m ⓓ

$\Pi(Gen, Enc, Dec, \mathcal{M})$ ⟨ $\mathcal{M}$ (明文空间) / $\mathcal{K}$ (密钥空间) / $\mathcal{C}$ (密文空间) ⟩

- Ciphertext-only 只偷密文(ch给).
- Known plaintext 有一定量 $\{m_i, Enc(sk, m_i)\}$, 回演 $Enc(sk, m')$
- Chosen-plaintext 可选明文→密文
- Chosen-ciphertext 可选密文→明文.

- Principle.
  - 可用性/正确性 $P[Dec(Enc(sk, m)) = m] = 1$, $sk \leftarrow Gen(1^n)$
  - 机密性 ⟷ Provable security.
  - 完整性 ⟷ MAC (continued ...).
  - ....



- Classic → Modern.
  - (1) Kerckhoffs (柯克霍夫)
    - 性sk不泄, 方案可泄
      - 维护 easy
      - 可扩展.
      - 多方加密有优势.
  - (2) 古典
    - Caesar 加密 (ROT-3 / ROT-13 / ROT-r)
      - $Enc(m_i) \equiv m_i + r \pmod{26}$.
    - Substitution 加密
      - $Enc(m_i) \equiv \pi(m_i)$
      - AI-Kindi 哈姆金
      - ⟷ $\pi(\cdot)$ 词频攻
      - 明文有在意义.

Ciphertext-only.

(不know plaintext).

(3) Modern Principle { Formal Def. [对A能力作约束]
Precise Assumptions. [假设陈述]
Proofs of Security

*一个可行范式 [基于词频极值四看之, → 迭代基于Pattern补全]

§Chap 2. Single-Message Security.

- Perfect Privacy

*idea: sk单纯不泄 → (Msg, sk)不泄. (Shannon 无 "addition" leaks)

A算力无限

$$\forall D, \forall t, c: \; P_{m \leftarrow D}[m = t] = P_{\substack{m \leftarrow D \\ sk \leftarrow Gen(\cdot)}}[m = t \mid Enc(sk, m) = c] \quad \cdots ①$$

↳ Shannon. Eq.

$$\forall m_1, m_2 \in \mathcal{D}: \; P_{sk \leftarrow Gen}[Enc(sk, m_1) = c] = P_{sk \leftarrow Gen}[Enc(sk, m_2) = c]$$

全概率

[Ex] ⟨ ① priori P ≡ posteriori P. [无附加信息] ②
② 不关注明文分布, 密文概率分布相同

注意: ①有对任意 D, 即"词频"的约束

一文与后面无法区分开.

- [Bonus] Perfect IND. → eav-secure.

→ 有一个game表述:

$$\forall \mathcal{A}, i: \; P[\mathcal{A}(Enc(sk, m)) = m_i] \le \frac{1}{2} + negl(n)$$

(△知长为n)

$$\forall \mathcal{A}, f: \{0,1\}^n \to \{0,1\}, \; \exists \mathcal{A}' \; (\text{△知长为n...}): \; P[\mathcal{A}(Enc(sk, m)) = f(m)] \le P[\mathcal{A}'(\cdot) = f(m)]$$

(owes) r

可观察Pattern BF.

• [eg]. One Time Pad [一个 Perfect Privacy 实例].

$\Pi = \{ |M| = \{0,1\}^n = K \;\; [\, Gen(\cdot) \xrightarrow{\$} sk. \;\; Enc(sk,m) = sk \oplus m \;\; Dec(sk,m) = sk \oplus c \,] \}$ 从 Perfect 入手

$P[Enc(sk, m_0) = c] = \frac{1}{2^n}$ 均值 (对 $\forall c, D, m_0$),

$sk \xleftarrow{\$} Gen$

Flaw { 依赖 $|K| \geq |M|$ → 设 $m^{-1}(c)$ 表 c 对任意 k 的原象. $|m^{-1}(c)| \leq |K|$ 由 $|K| < |M|$ 故 $\exists |m^{-1}(c)| < |M|$, 存在 m_0

多 Msg 不支持 $c_1 \oplus c_2 = m_1 \oplus m_2$ ↳ 更本质 sk 一致引发可逆性

故对该 c, $P[m \to m_0 \mid Enc \to c] = 0 \neq P[m \to m_0]$

• [Bonus] $|K| = |M| = |C|$, Shannon iff { $k \leftarrow Gen \in K = \frac{1}{|K|}$ (uniform).

$\forall m, c, \exists! \; k \in K, \; Enc(sk, m) = c$. 1

⇓ [Perfect Privacy 不现实 → 可计算安全].

• Computational Security. [attached to $P \overset{?}{=} NP$].

Relax { Δ ~~efficient~~ PPT [相比于多项式可解) poly 不确定 nonpoly 可解

$Adv(\Delta \text{ win}) = negl(n)$ poly or 可忽记 "渐进方法"

(1) Efficient → poly-time Running time. { language independent. composition natural slow-grow

: [M(x) 在 T(|x|) 下停机, $T(|x|) = O(|x|^c) = O(poly(|x|))$.

(2) $negl(n)$ $\forall n > N^*$, P, $f(n) < \frac{1}{P(n)}$. 在多项式规模可忽

- OWF family (one way function)

(1) OWF { easy to compute. $\exists M(P).\ \forall x\in\{0,1\}^*\ M(x)=f(x)$
hard to invert . . . .

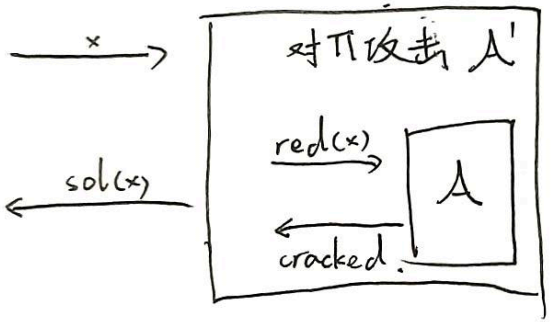
- Worst*: $\exists A$ { $\Pr_{x,r}[A(f(x))=t \mid f(x)=f(t)]=1$ } $\Rightarrow \Pr_x[A(f(x))\in f^{-1}(f(x))]$
- Strong: $\forall A$, $\Pr_{x,r}[A(f(x))=t \mid f(x)=f(t)]\le negl(n)$.
- Weak*: $\forall A$, $\Pr_{x,r}[A(f(x))=t \mid f(x)=f(t)]\le 1-\frac{1}{poly(n)}$.

e.g $f(p,q)=pq$ ✗
e.g $f(x,y)=xy$ ✓ 区分.

(2) hard-core prediction: { $hc\leftarrow M(P)$
$\forall A$, $\Pr_x[A(f(x))=hc(x)]\le \frac{1}{2}+negl(n)$.

- Reduction Methods

求解问题 X



这里要求A作为sub-module其与top-module无法区分

- Computational IND (CIND).

$\{x_n\}\overset{CIND}{\longleftrightarrow}\{y_n\}$.
$\Leftrightarrow \forall A, \left|\Pr_{x\leftarrow\{x_n\}}[A(x)=1]-\Pr_{y\leftarrow\{y_n\}}[A(y)=1]\right|\le negl(n)$

Stream Cipher [升级的 One-time Pad, seed→sk, $|K'|<|M|$.

$=\{0,1\}^n$
$=\{0,1\}^{n'}$
$<n$

{ $Gen(\cdot)\xrightarrow{\$} sk$
$Enc(sk,m)=G(sk)\oplus m$
$Dec(sk,m)=G(sk)\oplus c$ } sk为种子 要求G与纯随机无法区分

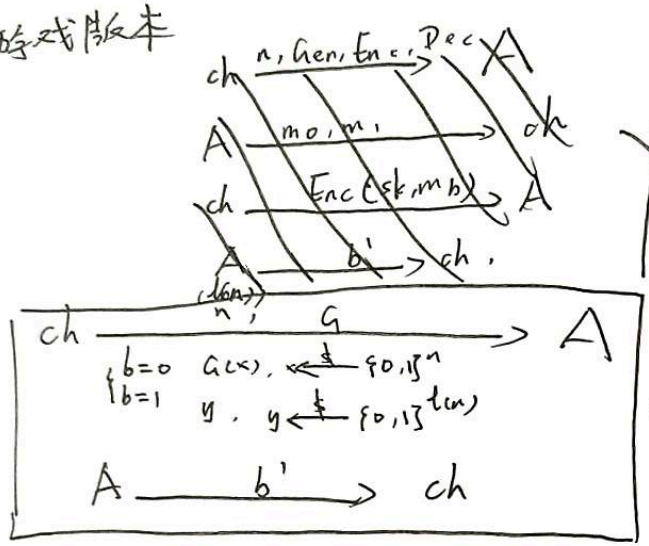
(3)

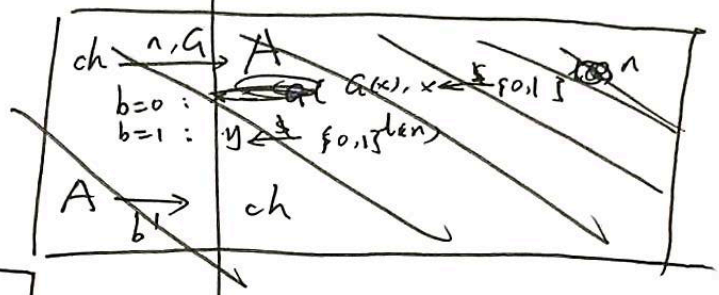
PRG (Pseudo Random Generator).

k真随机，而G(sk)长得像随机，即，

$G:\{0,1\}^n\to\{0,1\}^{l(n)}$. 有 $G(sk_n)$ 与 $\emptyset\ sk\xleftarrow{\$}1^{l(n)}$ CIND.

有一个游戏版本

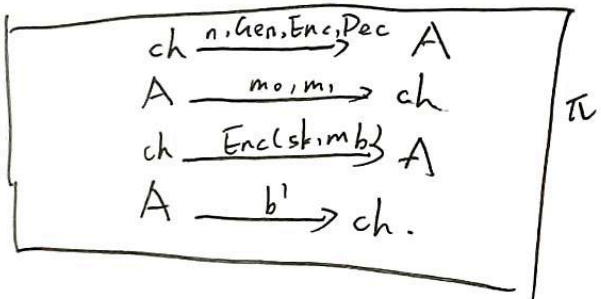




: G is PRG iff

$P[b = b'] \le \frac{1}{2} + negl(n)$.

对比eva

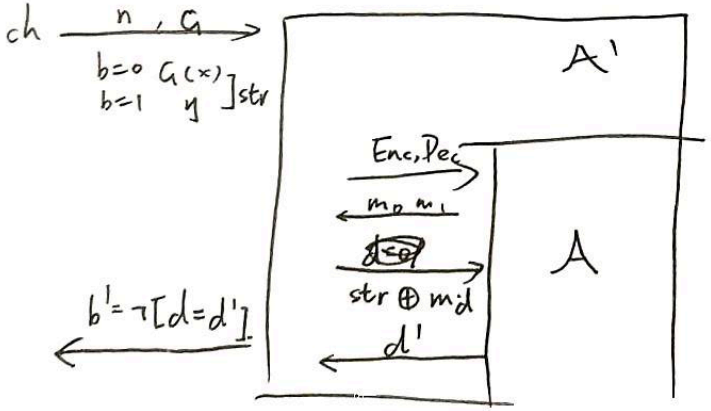


π is eva secure iff

$P(b=b'] \le \frac{1}{2} + negl(n)$.

(1)[Theorem]. $\pi = (Gen, Enc, Dec)$ be a Stream Cipher,

π eva-secure $\iff$ G is PRG,



$P[A \text{ win}] = \frac{1}{2} + \varepsilon$.

$P[A' \text{ win}] = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot (\frac{1}{2} + \varepsilon)$

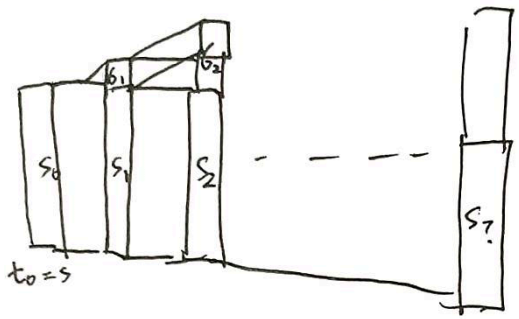
$= \frac{1}{2} + \frac{\varepsilon}{2}$.

这里是 game prove game

也可从代换出发

(2) [Theorem] PRG可扩.

$G: \{0,1\}^n \to \{0,1\}^{n+1}$, 则有 $\hat{G}: \{0,1\}^n \to \{0,1\}^{p(n)}$.



$t_0 = s$

$t_1 = G(t_0) = s_1 + b_1$

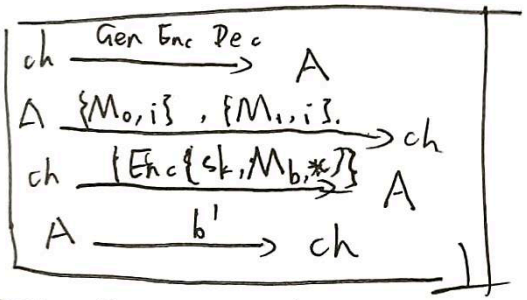
$t_2 = G(s_1) | b_1 = s_2 + b_2$

⋮

$t_k = G(s_{k-1}) | b_{k-1} = s_k + b_k$.

多书上两版 → 本样的 没差

{Gamei 可CIND可传递 代数 } 均可证.



• MMS:

§ Chap 3. Multi-Message Security.

π is Multi-Msg-Secure iff

$P(b=b') = \frac{1}{2}$.

(1) ~~Cipher text~~ Stream Cipher not MMS:

可构造 $M_{0,*}$ 列全同, $M_{1,i}$ 列全不同 (未用田性质!).

通用攻击!

(2)

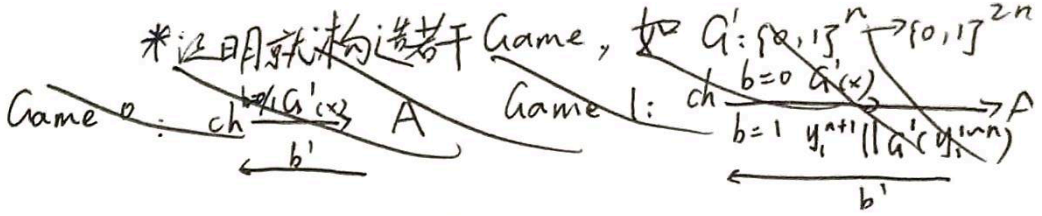
• PRFs. Pseudo-Random Functions.

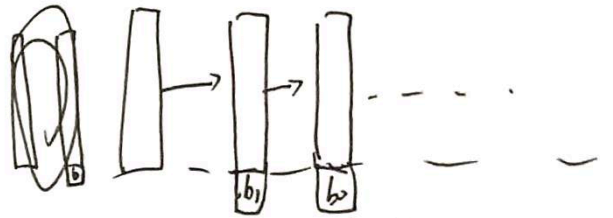
~~$F_{sk} = \{F_I(sk, \cdot)\}$~~

$\mathcal{F}_I = \{F_i\}_{i \in I}$.

$\mathcal{F} = F(\{0,1\}^n, \{0,1\}^n)$ 即全集 $|F(\cdot)| = n^{2^n}$

*证明就构造若干 Game, 如 $G': \{0,1\}^n \to \{0,1\}^{2n}$





Game k: ch b=0 G'(x)

Game 0: ch $b_1 \cdots b_{2n}$ A

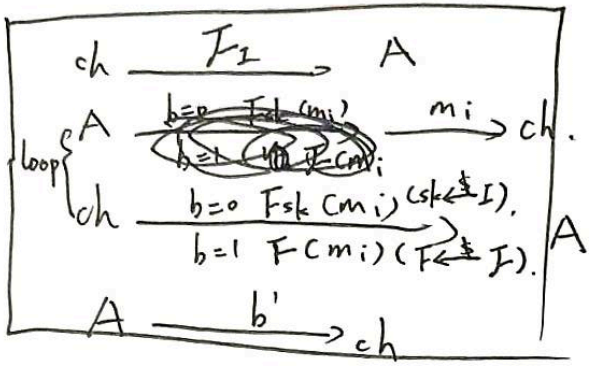
Game 1: ch $b_1 \cdots b_{2n-1}\ y_1$ A

⋮

Game 2n: ch $y_{2n} \cdots y_1$ A

则 Game i 与 Game i+1 可被某 RPG 之类 ~~区分~~ 不可区分 ...

F_I 为 PRFs 当且仅当 $P[b=b'] \le \frac{1}{2} + negl(n)$

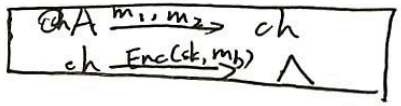


(1) IND-CPA Indistinguishable chosen-plaintext-attacks).

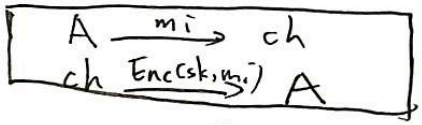
分三阶段

Init Phase

Challange Phase



Phase 2

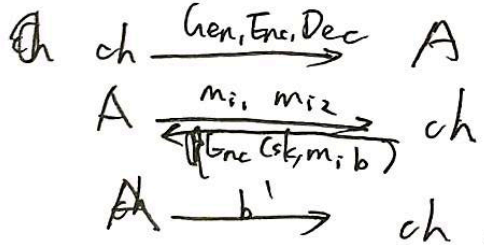


A $\xrightarrow{b'}$ ch

π is IND-CPA 当且仅当

$P[b=b'] \le \frac{1}{2} + negl(n)$.

(2) CPA2 构造，用 challange phase 填充 Init Phase



△ CPA2 ⟶ MMF 显然（不想说了）

CPA → MMT

CPA ⟹ CPA 2

具体 Game'o

问 (m_{10}, m_{11}) ---- (m_{i0}, m_{i1})

全答 0 的 $(0, 0, \dots, 0)$

Game1

问 (m_{10}, m_{11}) ----

除第1个全答0的 $(1, 0 \dots 0)$

Game i

除前 i 个全答 b=0 的 $(1 \dots 1, 0 \dots)$

则 Game i 与 Game i+1 同为一个 CPA 下的事.

CPA ⟺ CPA2 ⟶ MMF

有 IND-CPA 我们可以逐位加密，

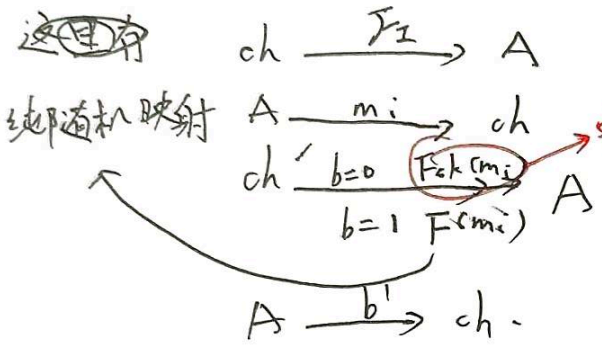
位与位之间不泄露！！！

(3) PRFs. ~~(为了实现IND-CPA)~~ ⟶ CPA

$Gen(1^*) \to I$, $1^* \xrightarrow{\$} r$.

$Enc(sk, m, r) = (r, F_{sk}(r) \oplus m)$

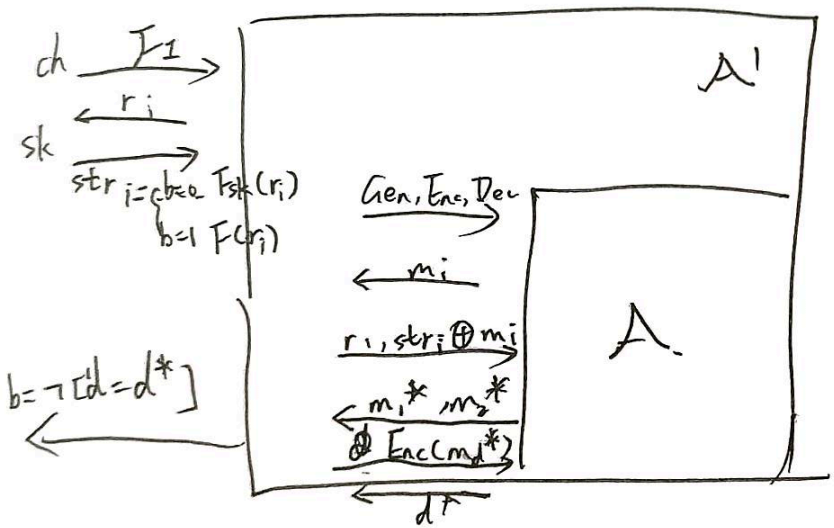
$Dec(sk, c_1, c_2) = c_2 \oplus F_{sk}(c_1)$.



要求 $m_i = m_j$ 有 $F_{sk}(m_i) = F_{sk}(m_j)$

或 r本质有 r_m 后代

同样 reduction.

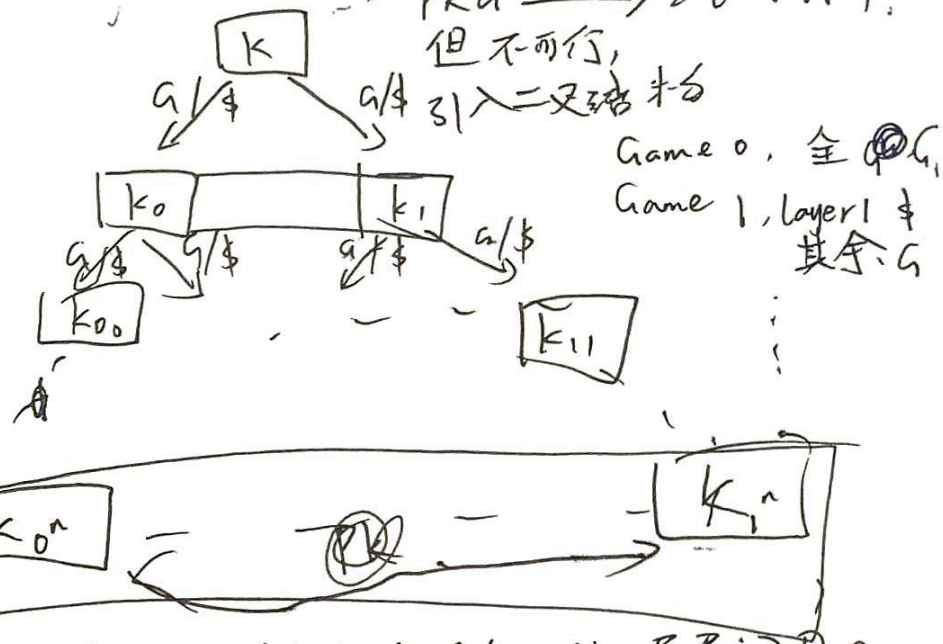


(4) PRG ⟶ PRFs

先可拉到 PRG ⟶ 2^n长字符串.

但不可行,

引入二叉结构



Game 0, 全 G_1

Game 1, layer 1 $

其余 G

这就生成的PRFs.

Game在tree上构造, 每次多一位, 层层调用 G_1,

易发现 G_1 次数指数级,

但由于 PRFs 间还是有限, 点数不超 nq 个, 可裁剪.

(5) PRFs ⟶ 良PRG.

良 $PRG(\overbrace{11\cdots1}^{n}) = PRF_m(1) \| \cdots \| PRF_m(|n|)$

m为n位.

§Chap 4 Authentication

· PRPs.

$\forall A, P[A(P/P^{-1}_{sk}(1^n)=1] - P[A(\pi/\pi^{-1}(1^n))=1] \le \frac{1}{2} + negl(n)$

或游戏

ch $\xrightarrow{P_I}$ A

A $\xrightarrow{m_i}$ (P/P^{-1}) ch, → 软空无扩

ch $\xrightarrow[b=1\ y_i]{b=0\ P_k/P_k^{-1}(\oplus, m_i)}$ A

$P[b=b'] \le \frac{1}{2} + negl(n)$

A $\xrightarrow{b'}$ ch.

只用记住 OWF $\Leftrightarrow$ PRG $\Leftrightarrow$ PRFs $\Leftrightarrow$ PRPs

weak $\Leftrightarrow$ strong

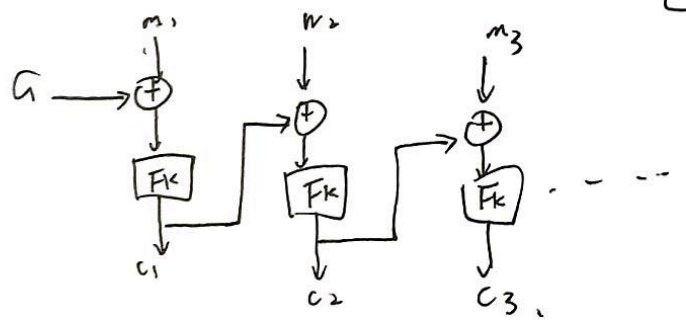
· CBC model

分组密码 { ECB 电子密码本
CBC 密码分组链接 ☆
OFB 输出反馈
CTR 计数器

$Enc(m, sk, r) = (r, F_{sk} \oplus m)$

对比 CBC 与 Stream Cipher ⇓ 结论

$\Rightarrow Enc(sk, m_1 || \cdots m_t, r) = (r, F_{sk}(r) \oplus m_1, F_{sk}(c_1) \oplus m_2 \cdots F_{sk}(c_{t-1}) \oplus m_t)$



PRFs ⇒ CBC is CPA-SND

· MAC: Message Authentication (

(1) Syntax $Gen(1^n) \to sk$

$MAC(sk, m) \to T$ 签

$verify(sk, T, m) \to$ [MAC(sk, m,) = T)

ch $\xrightarrow{Gen, MAC, Verify}$ A

A $\xrightarrow{m_i}$ ch

ch $\xrightarrow{MAC_{sk}(m_i)}$ A

(m^*, T^*)

伪造签名(新) 即 $i, m_i = m^*$

$P[verify(m^*, T^*, sk) = 1] \le negl(n)$

☆ 可不确定也可确定