CPA与CCA安全

哈尔滨工业大学

张宇

2024春

概览

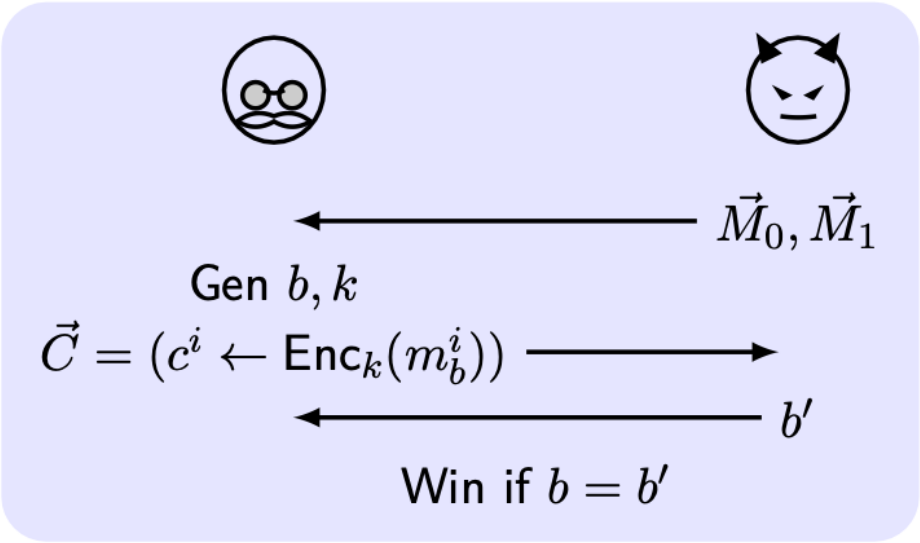
1. 选择明文攻击（CPA）安全
2. 伪随机函数（PRF）
3. 构造CPA安全加密方案
4. 操作模式（Modes of Operation）
5. 选择密文攻击（CCA）安全
6. 填充预言机攻击（Padding Oracle Attack）

多重加密

- 现实中需要多重加密（Multiple Encryptions）：一次加密多个消息或者一个消息的多个片段。在一次一密中，一个密钥不可以用于对多个消息加密。为此，定义多重加密实验：

The multiple-message eavesdropping experiment $\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n)$:

1. $\mathcal{A}$ is given input 1^n, outputs $\vec{M}_0 = (m_0^1, \ldots, m_0^t)$, $\vec{M}_1 = (m_1^1, \ldots, m_1^t)$ with $\forall i, |m_0^i| = |m_1^i|$.
2. $k \leftarrow \mathsf{Gen}(1^n)$, a random bit $b \leftarrow \{0,1\}$ is chosen. Then $c^i \leftarrow \mathsf{Enc}_k(m_b^i)$ and $\vec{C} = (c^1, \ldots, c^t)$ is given to $\mathcal{A}$.
3. $\mathcal{A}$ outputs b'. If $b' = b$, $\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi} = 1$, otherwise 0.



多重加密安全定义

Definition 1

Π has **indistinguishable multiple encryptions in the presence of an eavesdropper** if $\forall$ PPT $\mathcal{A}$, $\exists$ negl such that

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

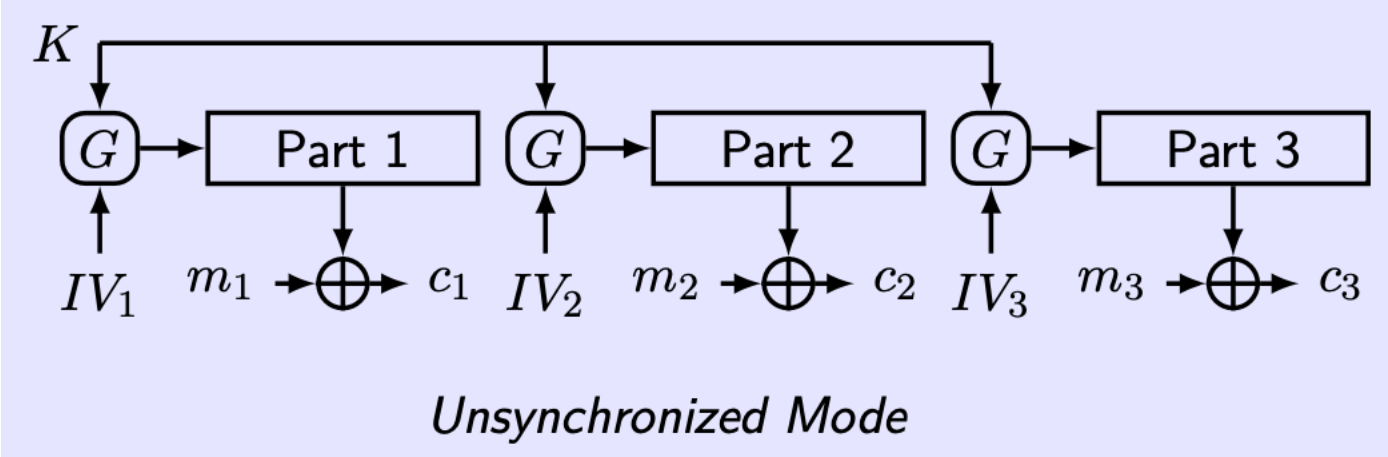
- 根据这个定义，来分析迄今学习的密码学方案是否是多重加密不可区分的？确定性加密过程无法实现多重加密安全。

Generally, if Π's encryption function is deterministic, i.e., a plaintext will be always encrypted into the same ciphertext with the same key, is Π multiple-encryption-secure?

For the deterministic encryption, the adversary may generate $m_0^1=m_0^2$ and $m_1^1\neq m_1^2$, and then outputs $b'=0$ if $c^1=c^2$, otherwise $b'=1$.

真实世界案例

- 用于多重加密的密钥（初始向量和密钥对）必须是独立的。否则，前面的攻击就会生效。



Unsynchronized Mode

Attacks on 802.11b WEP

Unsynchronized mode: $\text{Enc}(m_i) := \langle IV_i, G(IV_i \| k) \oplus m_i \rangle$

- Length of IV is 24 bits, repeat IV after $2^{24} \approx$ 16M frames
- On some WiFi cards, IV resets to 0 after power cycle
- $IV_i = IV_{i-1} + 1$. For RC4, recover k after 40,000 frames

选择明文攻击（CPA）案例

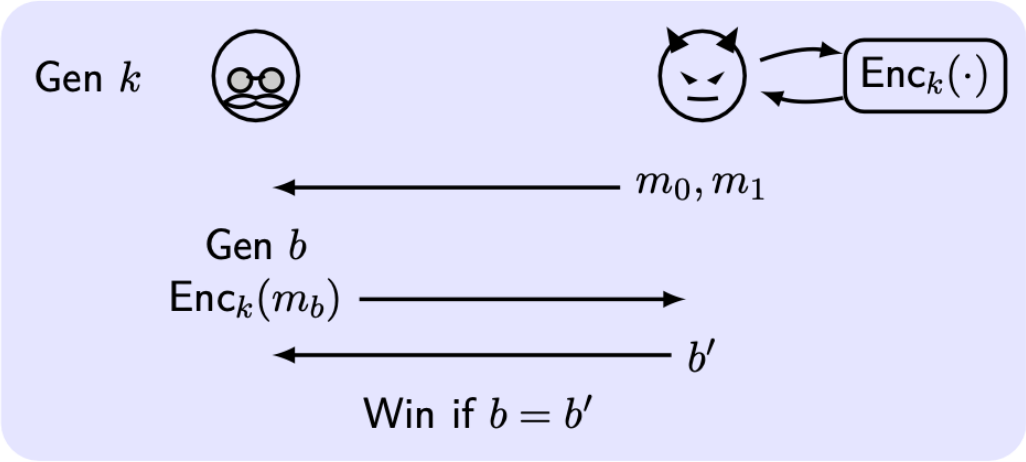
- 多重加密安全其实属于一类更基础的安全概念
- 选择明文攻击（Chosen-Plaintext Attack, CPA）敌手具有获得其所选择明文在同一密钥下对应的密文的能力
- 第二次世界大战中的例子:
  - 美国海军密码分析学家相信密文“AF”表示日语中的“中途岛”;
  - 但美国将军不认为中途岛会遭到攻击;
  - 美国海军密码分析学家发送了一个明文，中途岛淡水供给不足;
  - 日本军队截获的明文，并发送了一段密文，“AF”淡水不足;
  - 美国海军派出三艘航空母舰并且取胜。

CPA不可区分实验

- 敌手对加密函数预言机（Oracle）访问：敌手以任意明文作为输入，可以从预言机得到对应密文。此处，密钥是已经提前生成的，因此才能通过加密函数预研机得到密文，但仍对敌手保密。
- 预言机的一个比喻是一个黑盒，只接收输入并返回输出；访问者不需要了解其内部构造。

The CPA indistinguishability experiment $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$:

1. $k \leftarrow \mathsf{Gen}(1^n)$
2. $\mathcal{A}$ is given input 1^n and **oracle access** $\mathcal{A}^{\mathsf{Enc}_k(\cdot)}$ to $\mathsf{Enc}_k(\cdot)$, outputs m_0, m_1 of the same length
3. $b \leftarrow \{0,1\}$. Then $c \leftarrow \mathsf{Enc}_k(m_b)$ is given to $\mathcal{A}$
4. $\mathcal{A}$ **continues to have oracle access** to $\mathsf{Enc}_k(\cdot)$, outputs b'
5. If $b' = b$, $\mathcal{A}$ succeeded $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi} = 1$, otherwise 0



CPA安全定义

- CPA敌手比多重加密的敌手更“强大”，因为多重加密敌手是可以一次性地获得一组密文，而CPA敌手可以根据已经获得的明文和密文“多次适应性地”再次获得密文。

Definition 2

Π has **indistinguishable encryptions under a CPA (CPA-secure)** if $\forall$ PPT $\mathcal{A}$, $\exists$ negl such that

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)=1\right]\leq\frac{1}{2}+\mathsf{negl}(n).$$

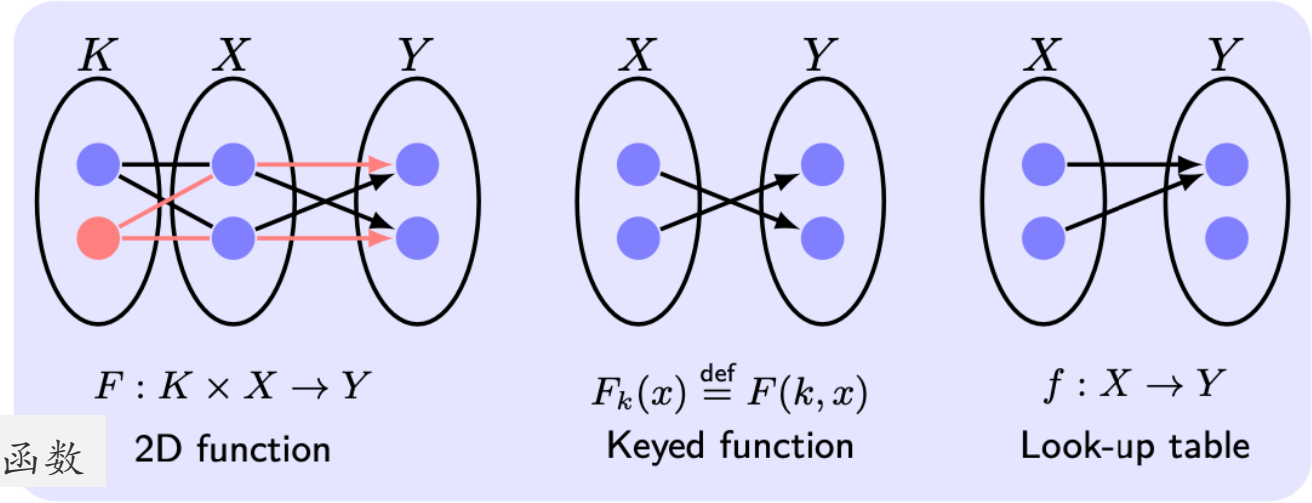
Proposition 3

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

- 多重加密安全意味着CPA安全？（作业）显然是否定的。那么，思考两种安全定义的区别成为解题的关键。

伪随机函数（PRF）

- 为实现CPA安全，PRG提供的随机性不够了，需要新的数学工具为加密提供额外随机性。伪随机函数（Pseudorandom Function, PRF）是对伪PRG的泛化：PRG从一个种子生成一个串，PRF从一个key生成一个函数。



带密钥函数
- **Keyed function** $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$
  $F_k : \{0,1\}^* \to \{0,1\}^*$, $F_k(x) \stackrel{\text{def}}{=} F(k, x)$

查表
- **Look-up table** f: $\{0,1\}^n \to \{0,1\}^n$ with size $= ?$ bits

函数族
- **Function family** Func_n: all functions $\{0,1\}^n \to \{0,1\}^n$.
  $|\text{Func}_n| = 2^{n \cdot 2^n}$

长度不变
- **Length Preserving**: $\ell_{key}(n) = \ell_{in}(n) = \ell_{out}(n)$

PRF定义

- 直觉上，一个PRF生成的带密钥的函数与从函数族中随机选择的真随机函数（查表）之间是不可区分的。
- 一个真随机函数具有指数长度，无法“预先生成”，只能“on-the-fly”（边运行边生成）的使用，引入一个对函数O的确定性的预言机访问（oracle access）D^O。
  - 访问预言机，就是给任意输入，得到该函数的输出。访问预言机的能力不包括了解正在访问的预言机具体内部构造。

Definition 4

An efficient length-preserving, keyed function F is a **pseudorandom function (PRF)** if $\forall$ PPT distinguishers D,

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

where f is chosen *u.a.r* from Func_n.

课堂练习

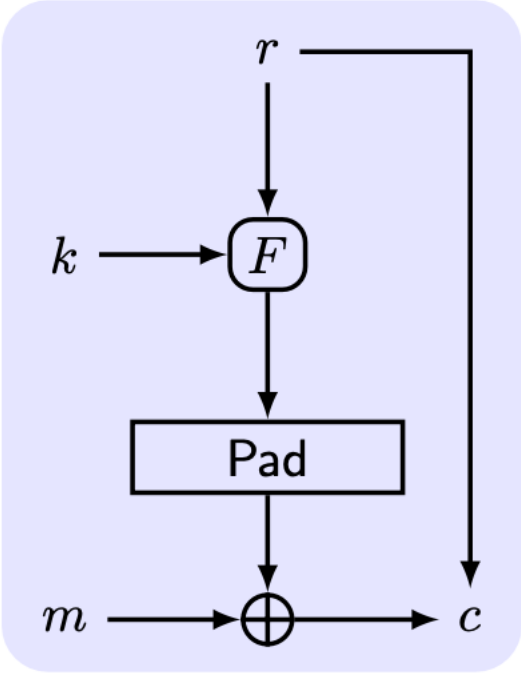
Q: Is the fixed-length OTP a PRF?

Q: Without knowing the key and the oracle access, could anyone learn something about the output from the input with a non-negligible probability?

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. Is G a PRF?

1. $G((k_1, k_2), x) = F(k_1, x) \| F(k_2, x)$
2. $G(k, x) = F(k, x \oplus 1^n)$
3. $G(k,x) = \begin{cases} F(k,x) & \text{when } x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$
4. $G(k,x) = \begin{cases} F(k,x) & \text{when } x \neq 0^n \\ k & \text{otherwise} \end{cases}$
5. $G(k,x) = F(k,x) \bigoplus F(k, x \oplus 1^n)$

构造CPA安全加密方案



Construction 5

- *Fresh random string* r.
- $F_k(r)$: $|k| = |m| = |r| = n$.
- Gen: $k \in \{0,1\}^n$.
- Enc: $s := F_k(r) \oplus m$, $c := \langle r, s \rangle$.
- Dec: $m := F_k(r) \oplus s$.

Theorem 6

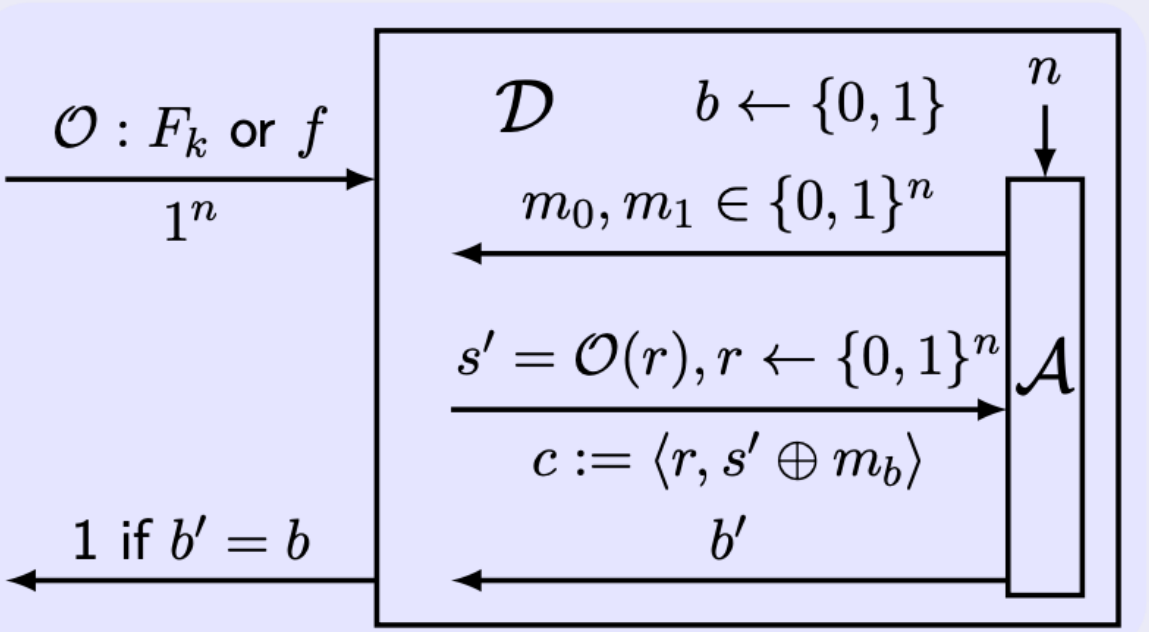
If F *is a PRF, this fixed-length encryption scheme* Π *is CPA-secure.*

CPA安全证明

- 从PRF的区分器算法D规约到加密方案敌手算法A，区分器D作为敌手A的挑战者，敌手A实验成功时区分器D输出1。分两种情况，当输入真随机函数f时，相当于一次一密；当输入伪随机函数F时为加密方案。

Proof.

Reduce D to $\mathcal{A}$:



□

CPA安全证明

- 通过规约将A的不可区分实验成功的概率与D的区分器实验输出1的概率建立等式；分析输入真随机函数预言机时D输出1的概率（即不可区分实验成功概率）是1/2+一个可忽略函数。

Proof.

Analyze $\Pr[\text{Break}]$, Break means $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1$:
$\mathcal{A}$ makes $q(n)$ queries and collects $\{\langle r_i, f(r_i)\rangle\}$, as $c_i = \langle r_i, s_i\rangle$, and $f(r_i) = s_i \oplus m_i$, for $i = 1, \ldots, q(n)$.
The challenge $c = \langle r_c, f(r_c) \oplus m_b\rangle$.

- Repeat: $r_c \in \{r_i\}$ with probability $\frac{q(n)}{2^n}$. $\mathcal{A}$ can know m_b.
- $\overline{\text{Repeat}}$: As OTP, $\Pr[\text{Break}] = \frac{1}{2}$

$$\begin{aligned}\Pr[\text{Break}] &= \Pr[\text{Break} \wedge \text{Repeat}] + \Pr[\text{Break} \wedge \overline{\text{Repeat}}] \\ &\leq \Pr[\text{Repeat}] + \Pr[\text{Break}|\overline{\text{Repeat}}] \\ &\leq \frac{q(n)}{2^n} + \frac{1}{2}.\end{aligned}$$

$\Pr[D^{F_k(\cdot)}(1^n) = 1] = \Pr[\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} + \varepsilon(n)$.
$\Pr[D^{f(\cdot)}(1^n) = 1] = \Pr[\text{PrivK}^{\text{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1] = \Pr[\text{Break}] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.
$\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \geq \varepsilon(n) - \frac{q(n)}{2^n}$. $\varepsilon(n)$ is negligible. □

课堂练习

Q: G is a PRG. Is this scheme CPA-secure?

$\mathrm{Enc}_k(m) = r, G(k\|r) \oplus m$, where r is a fresh random string.

CPA-Security from PRF for Arbitrary-Length Messages

- For arbitrary-length messages, $m = m_1, \ldots, m_\ell$

$$c := \langle r_1, F_k(r_1) \oplus m_1, r_2, F_k(r_2) \oplus m_2, \ldots, r_\ell, F_k(r_\ell) \oplus m_\ell \rangle$$

Corollary 7

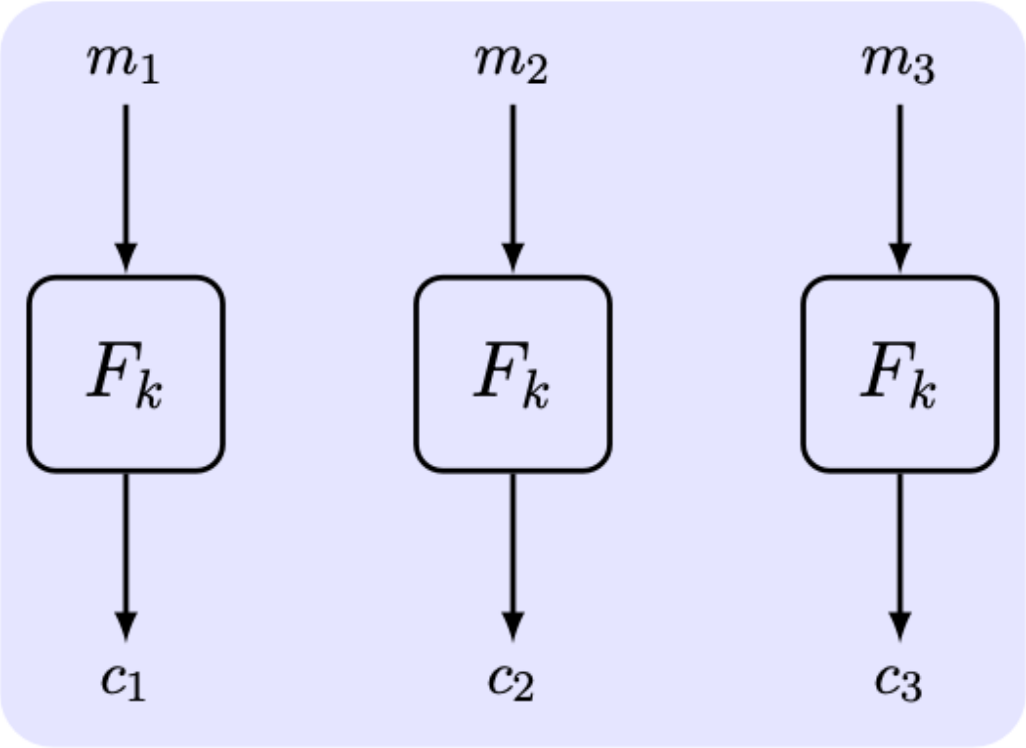
If F is a PRF, then Π is CPA-secure for arbitrary-length messages.

- What is the shortcoming of this scheme?

操作模式（Modes of Operation）

- 将一个消息分成若干等长的块（分组，block），每个块以相似方式处理
- 操作模式是使用PRP或PRF来加密任意长度消息的方法
- 操作模式是从PRP或PRF来构造一个PRG的方法

Electronic Code Book (ECB) Mode



- Q: is it indistinguishable in the presence of an eavesdropper?
- Q: can F be any PRF?

伪随机排列（PRP）

- 双射 Bijection: F 是一到一的（一个输入对应一个唯一输出）且满射（覆盖输出集中每个元素）；
- 排列 Permutation: 一个从一个集合到自身的双射函数；
- 带密钥的排列 Keyed permutation: 是排列，类似带密钥的函数；

Definition 8

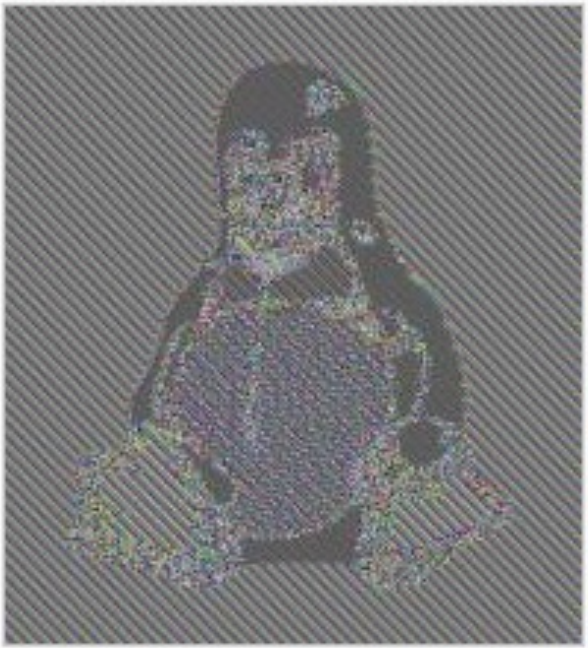
An efficient, keyed permutation F is a **strong pseudorandom permutation (PRP)** if $\forall$ PPT distinguishers D,

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

where f is chosen *u.a.r* from the set of permutations on n-bit strings.

ECB模式缺陷

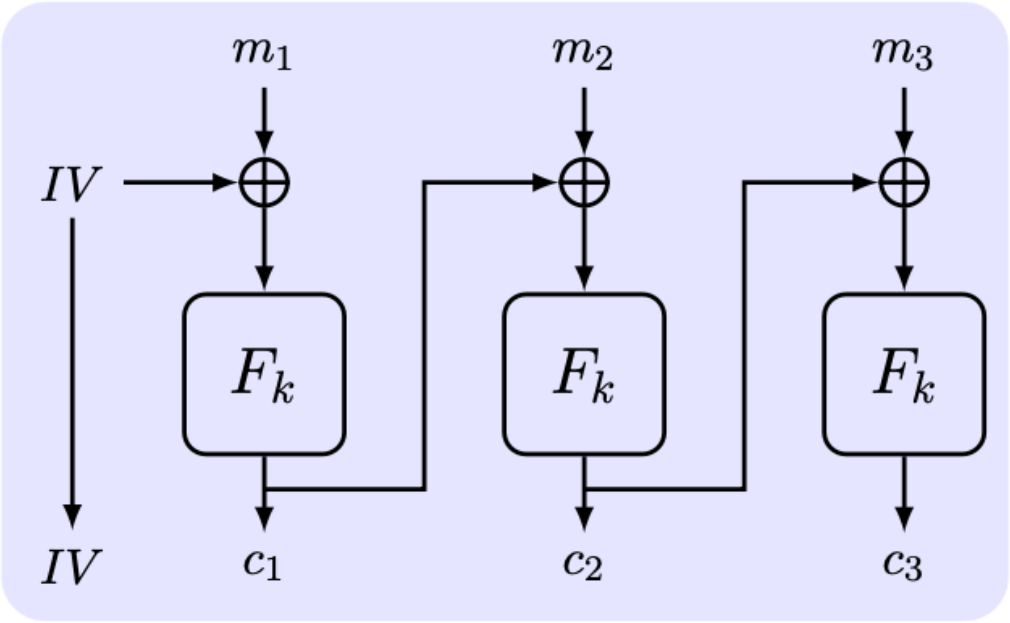
Original image



Encrypted using ECB mode

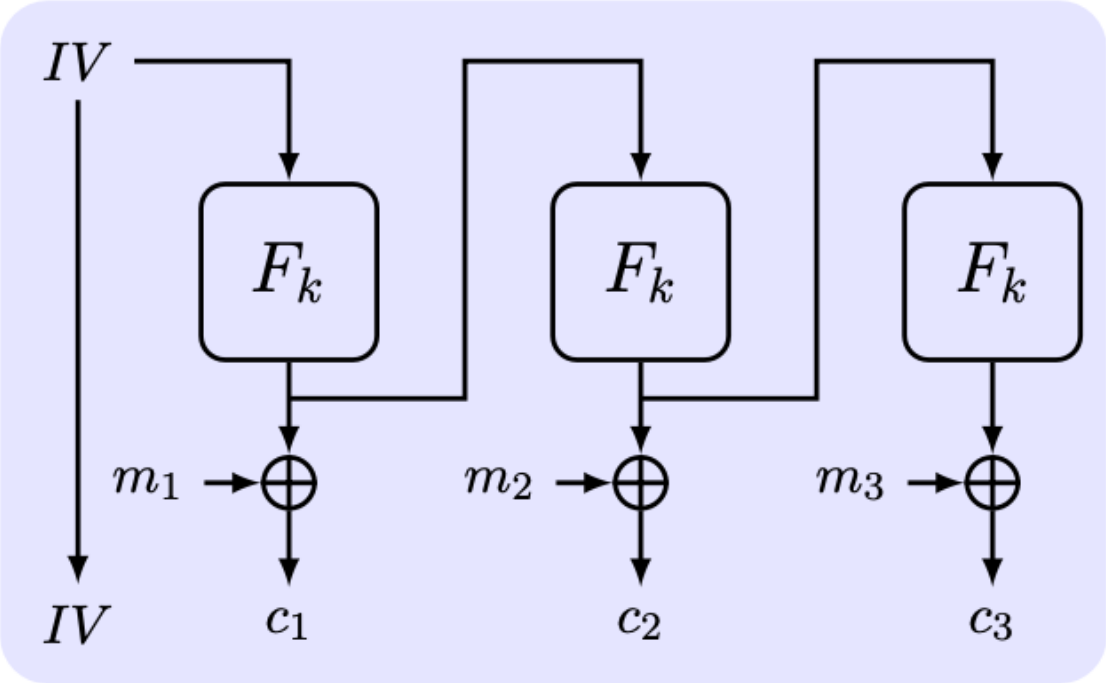
Modes other than ECB result in pseudo-randomness

Cipher Block Chaining (CBC) 密文链



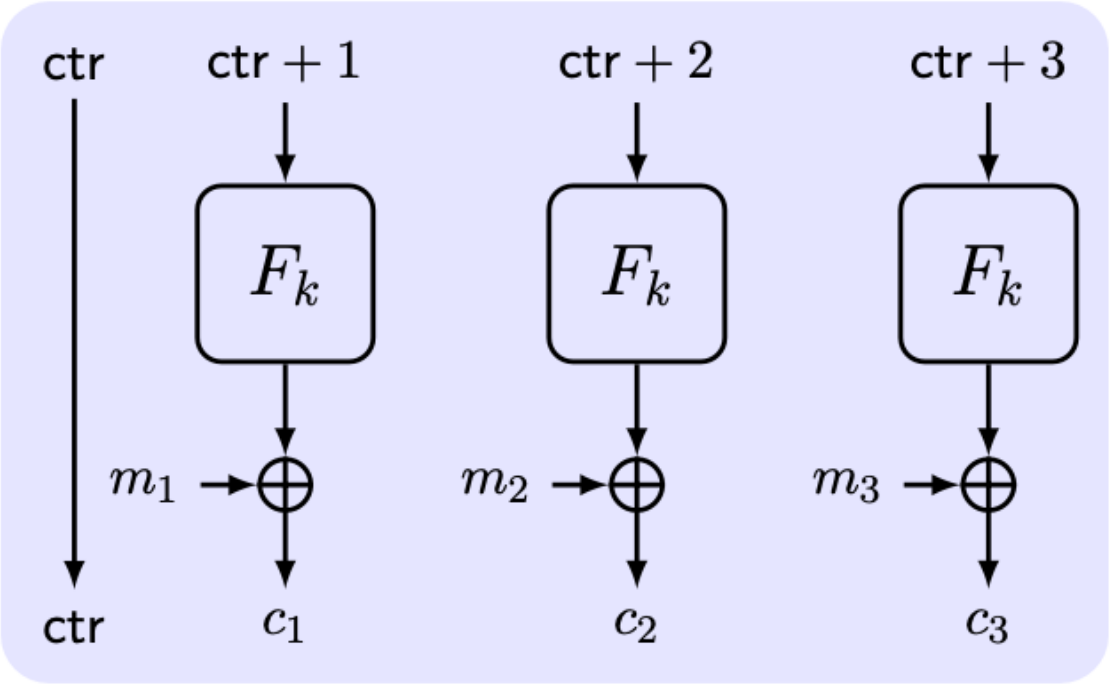
- IV: initial vector, a fresh random string.
- Q: is it CPA-secure? what if IV is always 0?
- Q: is the encryption parallelizable, i.e., outputting c_2 before getting c_1?
- Q: can F be any PRF?

Output Feedback (OFB) 输出反馈



- Q: is it CPA-secure?
- Q: is the encryption parallelizable?
- Q: can F be any PRF?

Counter (CTR) 计数器



- ctr is an IV
- Q: is it CPA-secure?
- Q: is the encryption parallelizable?
- Q: can F be any PRF?

真实世界案例

If IV is predictable, then CBC mode is not CPA-secure.
Q: Why? (homework)

Bug in SSL/TLS 1.0

IV for record $\#i$ is last CT block of record $\#(i-1)$.

API in OpenSSL

```
void AES_cbc_encrypt (
    const unsigned char *in,
    unsigned char       *out,
    size_t              length,
    const AES_KEY       *key,
    unsigned char       *ivec,     User supplies IV
    AES_ENCRYPT or AES_DECRYPT);
```

非确定性加密总结

- 有三种通用的实现CPA安全的非确定性加密方法：
- 随机化的：r随机生成，如构造5；需要更多熵，长密文
- 有状态的：r为计数器，如CTR模式；需要通信双方同步计数器
- 基于Nonce的：r只用一次；需要保证只用一次，长密文

选择密文攻击（CCA）

- 在现实世界中，敌手可以通过影响被解密的内容来实施CCA（Chosen-Ciphertext Attack，选择密文攻击）。如果通信没有认证，那么敌手可以以通信参与方的身份来发送特定密文。后面学习一个CCA攻击Padding Oracle攻击。

The CCA indistinguishability experiment $\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$:

1. $k \leftarrow \mathsf{Gen}(1^n)$.
2. $\mathcal{A}$ is given input 1^n and oracle access $\mathcal{A}^{\mathsf{Enc}_k(\cdot)}$ and $\mathcal{A}^{\mathsf{Dec}_k(\cdot)}$, outputs m_0, m_1 of the same length.
3. $b \leftarrow \{0,1\}$. $c \leftarrow \mathsf{Enc}_k(m_b)$ is given to $\mathcal{A}$.
4. $\mathcal{A}$ continues to have oracle access **except for** c, outputs b'.
5. If $b' = b$, $\mathcal{A}$ succeeded $\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi} = 1$, otherwise 0.

Definition 11

Π has **indistinguishable encryptions under a CCA (CCA-secure)** if $\forall$ PPT $\mathcal{A}$, $\exists$ negl such that

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

CCA安全意味着密文不可锻造

- -CCA安全性意味着“non-malleability”（不可锻造性，即改变但不毁坏），不能修改密文来获得新的有效密文，进而通过解密修改后的密文得到相关的明文。
- 之前的方案中没有CCA安全的，因为都不是不可锻造。

CCA against Construction 5

$\mathcal{A}$ gives m_0, m_1 and gets $c = \langle r, F_k(r) \oplus m_b \rangle$, and then queries c' which is the same with c except that a single bit is flipped. The $m' = c' \oplus F_k(r)$ should be the same with m_b except ____?

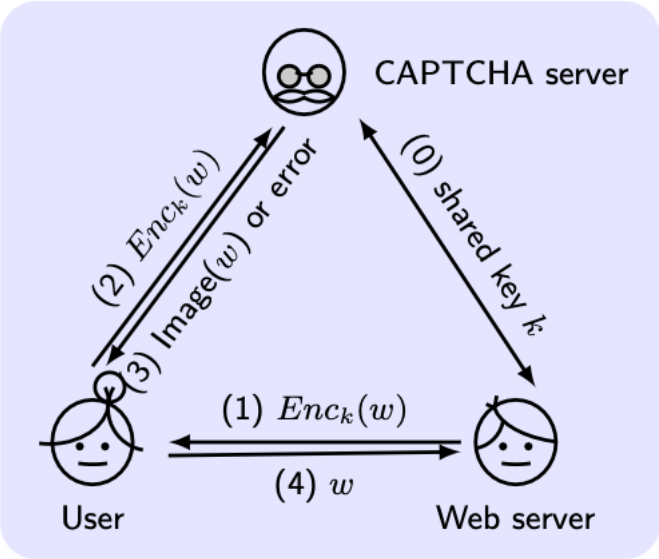
Q: Show that the above modes (CBC, OFB and CTR) are also not CCA-secure. (homework)

由此，可以总结出CCA下敌手的常用策略：

- 修改挑战密文c为c'，并查询解密预言机得到m'
- 根据关系，由m'来猜测被加密明文m_b

填充预言机攻击（Padding Oracle Attack）

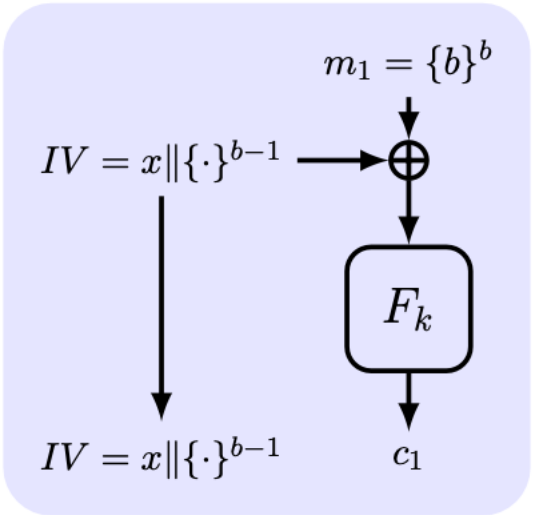
- CAPTCHA服务商为Web网站提供验证用户是否为人类的服务。为此，一个CAPTCHA服务器与Web服务器间事先共享一个密钥k，服务工作原理如下：
  1. 当Web服务器验证用户是否为人类时，生成一个消息w并以k加密，向用户发送一个密文$Enc_k(w)$；
  2. 用户将密文$Enc_k(w)$转发给CAPTCHA服务器；（可实施填充预言机攻击）
  3. CAPTCHA服务器用密钥k将密文解密，根据解密结果返回给用户信息：一个由w生成的图像，或者坏填充错误；
  4. 用户根据图像获得 w 并将 w 发送给Web服务器。
- 在第2步，当恶意用户可以利用CAPTCHA服务器会返回给用户坏填充错误这一漏洞，来实施填充错误攻击。



填充预言机攻击原理

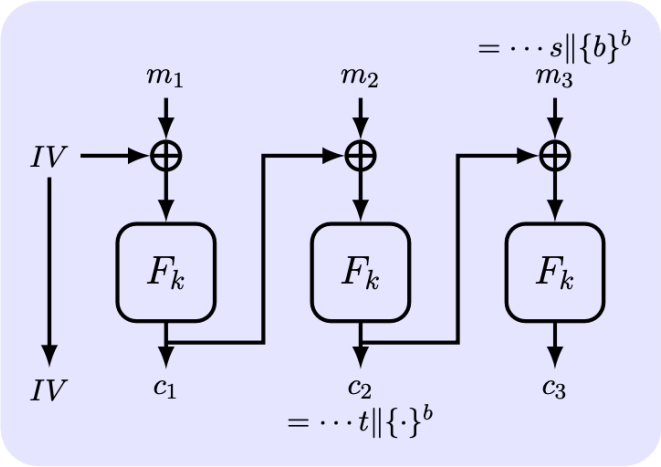
- 在PKCS #5 padding（填充）标准中，为了将一个消息的长度“填充”到块长度的整数倍，在最后一个块中填充b个字节的b；必要时，添加一个哑块（dummy block，不包含消息的一个填充块）。存在一种攻击手段：当填充错误时，解密服务器返回一个“坏填充错误”，这相当于提供了一个解密预言机，最终可以获得整个明文；
- 具体攻击原理：
  - 更改密文（包含IV部分）并发送给解密服务器；
  - 一旦触发了“坏填充错误”，则说明对密文的更改导致了填充部分内容的更改；否则，对密文的更改导致了原明文部分的更改；
  - 通过仔细修改密文来控制填充部分，从而获得消息长度和内容。

填充预言机攻击获得消息长度



- 攻击的第一步判断消息是否为空：在单个块的CBC中，通过更改IV的首个字节，攻击者能够获知是否m是否为空。因为如果m是空的话，更改IV首个字节将更改解密出的填充内容，解密服务器就会返回坏填充错误（1比特信息），具体分析如下：
  - 如果m是空的，那么明文会添加一个哑块$\{b\}^b$；
  - PRP的输入为$IV \oplus \{b\}^b$；设IV的首个字节为x，则PRP的输入为$(x \oplus b) \| (\{\cdot\}^{b-1} \oplus \{b\}^{b-1})$；
  - 将IV的首个字节从x改成y变为 $y \| (\{\cdot\}^{b-1})$，不改变c_1解密得到的PRP的输入不会变，而解密出的明文会改变为 $(x \oplus y \oplus b) \| \{b\}^{b-1}$；
  - 上述明文首个字节一定不是b，这是填充格式错误，会触发服务器返回错误；
  - 如果上面的尝试没有触发错误，那么说明消息非空；下一步，发现消息长度是否为1字节，方法与上一步一样，区别在于只改变IV的第2个字节；如此继续，获得消息的长度；（作业）

填充预言机攻击获得明文内容



- 一旦获得消息的长度，也就知道了填充的长度b，采用下面的方法来获得消息的最后一个字节内容，进而获得整个消息；
- 更改密文中倒数第二块，来获得消息的最后一个字节s；
- 明文的最后一个块 $m_{last} = \cdots s \| \{b\}^b$，密文的倒数第二个块 $c_{last-1} = \cdots t \| \{\cdot\}^b$；
- 最后一块的PRP输入为$c_{last-1} \oplus m_{last} = \cdots (s \oplus t) \| (\{b\}^b \oplus \{\cdot\}^b)$；
- 敌手更改 c_{last-1} 为 $c'_{last-1} = \cdots u \| (\{\cdot\}^b \oplus \{b\}^b \oplus \{b+1\}^b)$；其中，$u$是敌手猜测的某个字节；
- 解密获得最后一块明文$m'_{last} = c_{last-1} \oplus m_{last} \oplus c'_{last-1} = \cdots (s \oplus t \oplus u) \| \{b+1\}^b$；
- 如果没有返回坏填充错误，那么意味着填充了$b+1$个字节的$b+1$，所以 $s \oplus t \oplus u = (b+1)$，而 $s = t \oplus u \oplus (b+1)$。

本节小结

- 对的加密攻击不只窃听，还包括CPA, CCA (padding-oracle attack)
- 安全依赖于与为随机性相关的密码学原语：PRG, PRF, PRP
- 变长消息通过操作模式加密: EBC, CBC, OFB, CTR
- CCA安全不仅仅包含机密性，还包含密文不可锻造性