Private-Key Encryption and Pseudorandomness (Part II)

Yu Zhang

HIT/CST/NIS

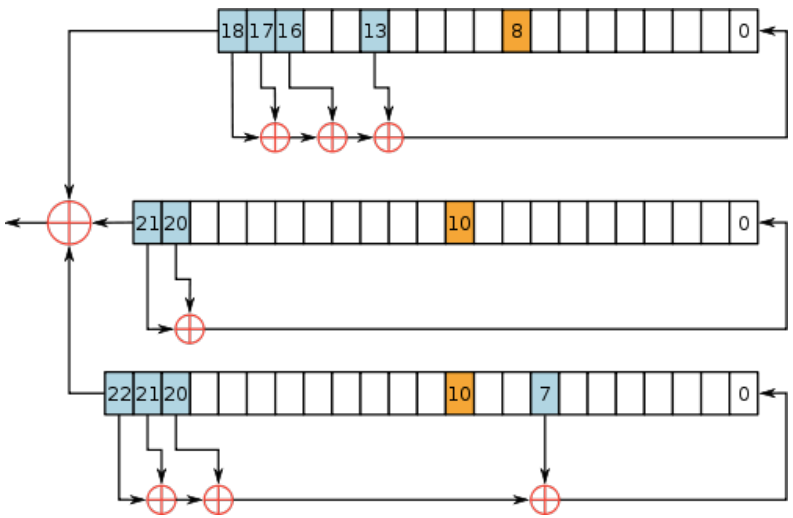
Cryptography, Spring, 2012

Outline

Content

Stream Ciphers

- **Stream cipher**: Encrypting by XORing with pseudorandom stream.
- **State of the art**: No standardized and popular one[1]. Security is questionable, e.g. RC4 in WEP protocol in 802.11, and Linear Feedback Shift Registers (LFSRs).



WARNING

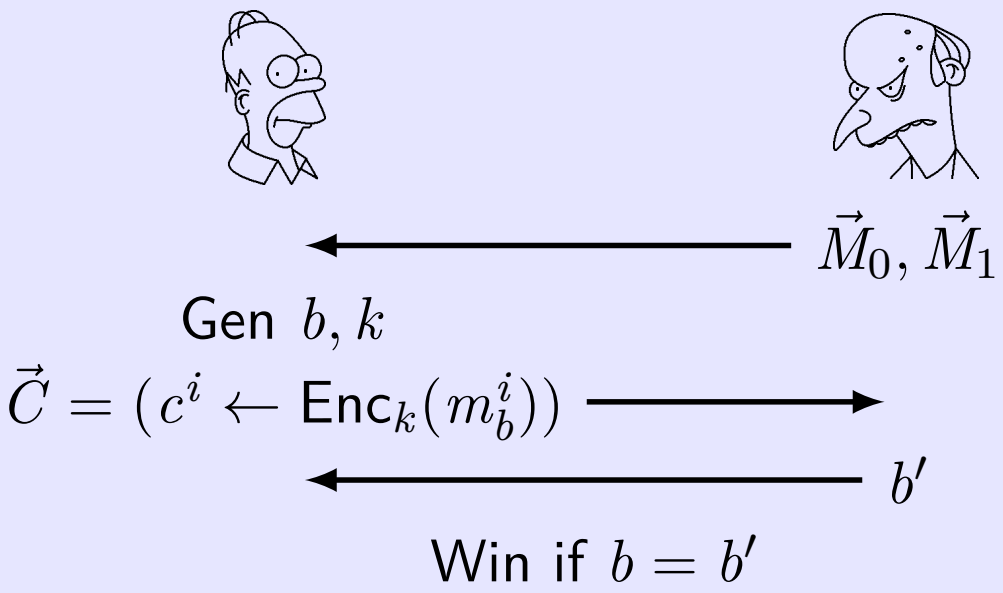
Don't use any stream cipher. If necessary, construct one from a block cipher.

[1] eStream project worked on it. Salsa20/12 is a promising candidate.

Security for Multiple Encryptions

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.



Definition of Multi-Encryption Security

Definition 1

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

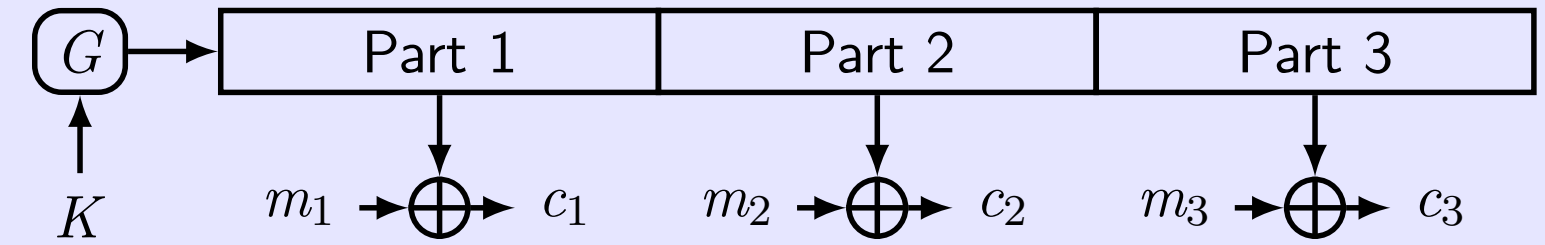
$$\Pr\left[\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

Theorem 2

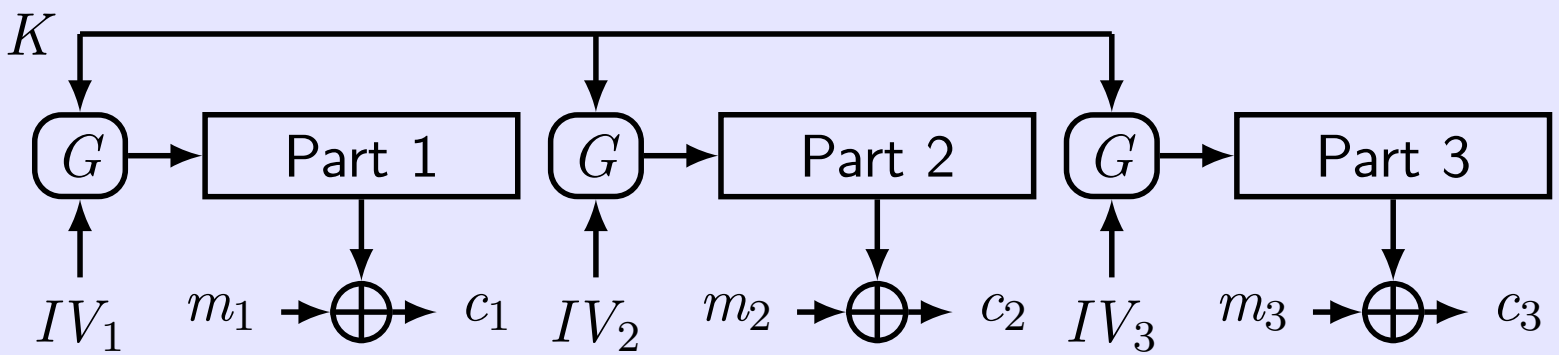
$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *for which* Enc *is a deterministic function of the key and the message. Then* Π *does not have indistinguishable multiple encryptions in the presence of an eavesdropper.*

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

Secure Multiple Encryptions Using a Stream Cipher



Synchronized Mode



Unsynchronized Mode

Unsynchronized mode: $\mathsf{Enc}(m) := \langle IV, G(k, IV) \oplus m \rangle$.
Initial vector IV is chosen *u.a.r.*

Related Keys: Real World Cases

Keys for multiple enc. must be independent.

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.

Content

Chosen-Plaintext Attacks (CPA)

CPA: the adversary has the ability to obtain the encryption of plaintexts of its choice.

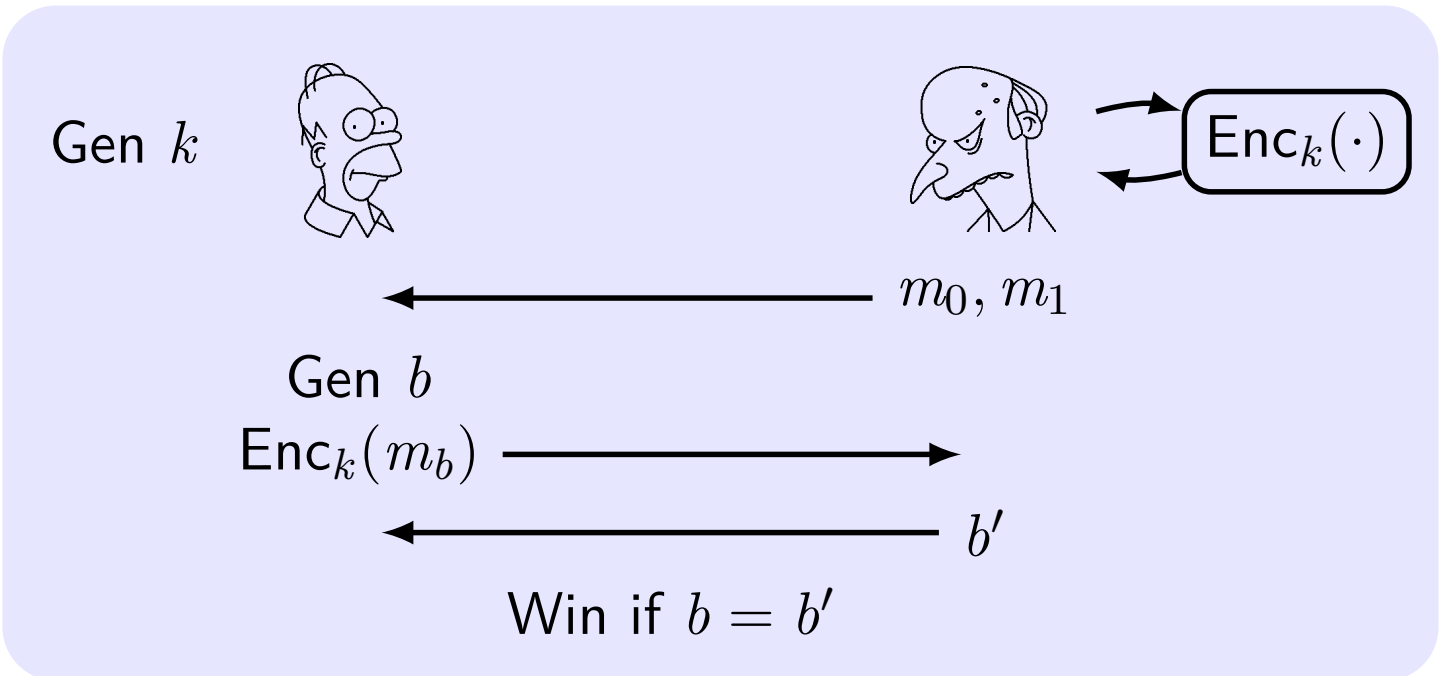
A story in WWII

- Navy cryptanalysts believe the ciphertext "AF" means "Midway island" in Japanese messages.
- But the general did not believe that Midway island would be attacked.
- Navy cryptanalysts sent a plaintext that the freshwater supplies at Midway island were low.
- Japanese intercepted the plaintext and sent a ciphertext that "AF" was low in water.
- The US forces dispatched three aircraft carriers and won.

Security Against CPA

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 Security for Multiple Encryptions

Definition 3

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

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

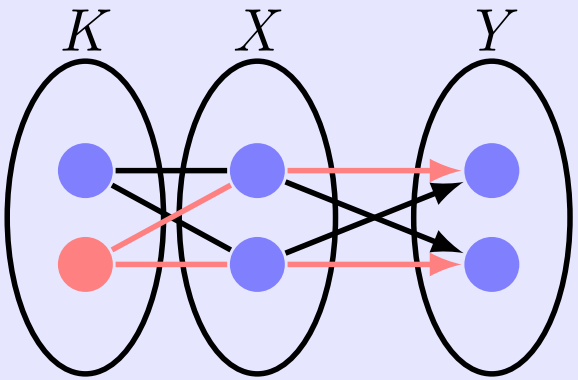
Proposition 4

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

- CPA-secure means Enc is probabilistic.
- **Fixed-length** CPA-secure encryption scheme can be used to construct a **arbitrary-length** CPA-secure one quite easily.

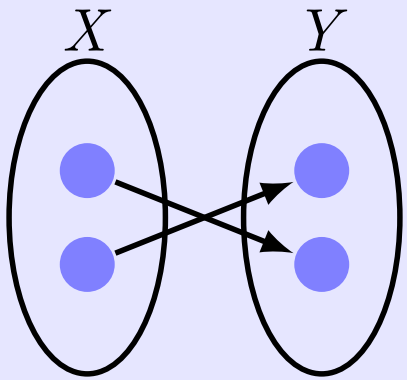
Content

Concepts on Pseudorandom Functions



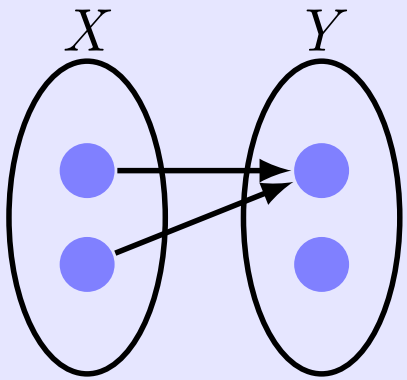
$F : K \times X \to Y$

2D function



$F_k(x) \stackrel{\text{def}}{=} F(k, x)$

Keyed function



$f : X \to Y$

Look-up table

- **Keyed function** $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$.
  $F_k : \{0,1\}^* \to \{0,1\}^*$, $F_k(x) \stackrel{\text{def}}{=} F(k, x)$.
- **Look-up table** f: $\{0,1\}^n \to \{0,1\}^n$ with size $n \cdot 2^n$.
- **Function family** Func_n: all functions $\{0,1\}^n \to \{0,1\}^n$.
  $|\mathsf{Func}_n| = 2^{n \cdot 2^n}$.

Definition of Pseudorandom Function

Intuition: A PRF F generates a function F_k that is indistinguishable for a PPT distinguisher D from truly random selected function f (look-up table) in Func_n.
However, the function has **exponential length**. Give D the deterministic **oracle access** $D^{\mathcal{O}}$ to the functions $\mathcal{O}$.

Definition 5

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

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

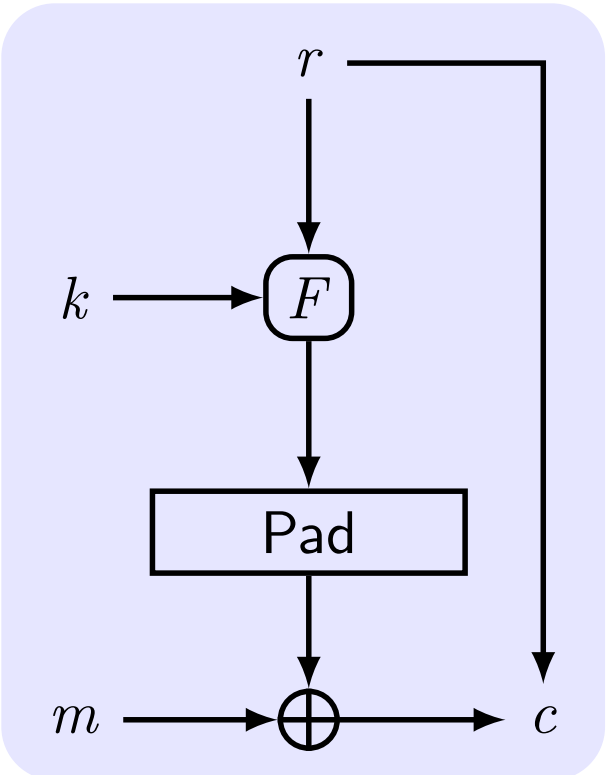
where f is chosen *u.a.r* from Func_n.

PRG vs. PRF:

- Pseudorandomness over a set of strings vs. a set of functions.
- A PRG — an instance of keyed PRF.

Existence: if PRG exists. In practice, block ciphers may be PRF.

CPA-Security from Pseudorandom Function



Construction 6

- *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 7

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

Proof of CPA-Security from PRF

Idea: First, analyze the security in an idealized world where f is used in $\tilde{\Pi}$; next, claim that if Π is insecure when F_k was used then this would imply F_k is not PRF by reduction.

Proof.

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

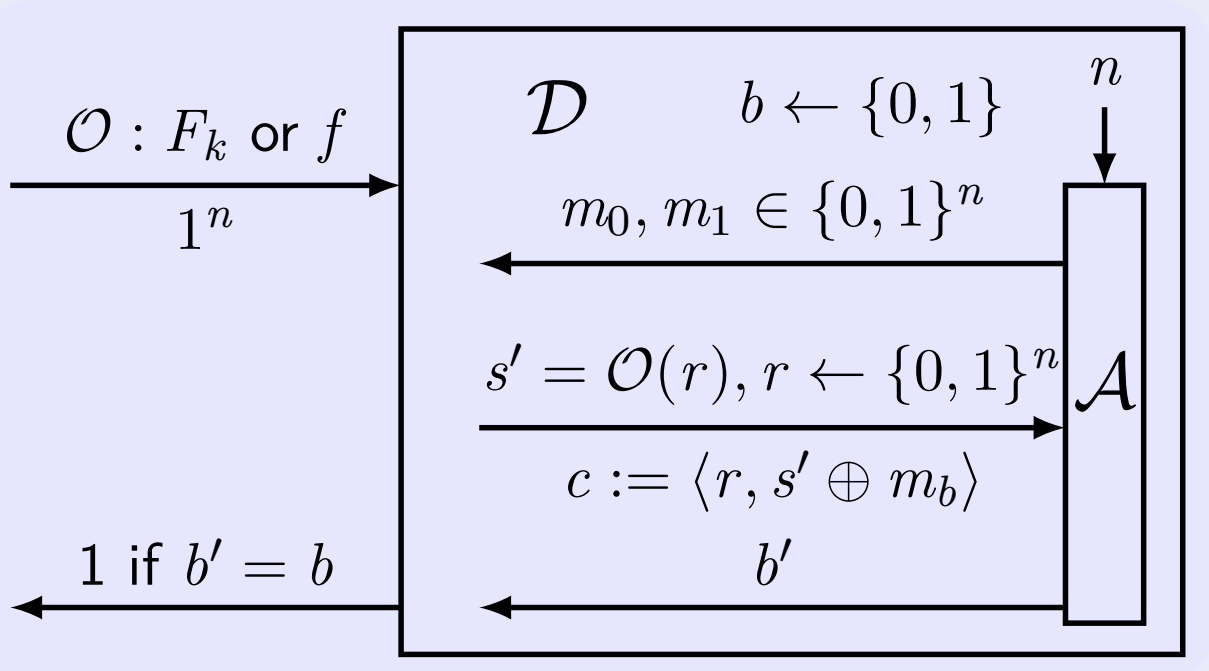
- Repeat: $r_c \in \{r_i\}$ with probability $\frac{q(n)}{2^n}$. $\mathcal{A}$ can know m_b.
- $\overline{\text{Repeat}}$: As OTP, $\Pr[\text{Break}] = \frac{1}{2}$

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

Proof of CPA-Security from PRF (Cont.)

Proof.

(2) Reduce D to $\mathcal{A}$:



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

$\Pr[D^{f(\cdot)}(1^n) = 1] = \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1] = \Pr[\mathsf{Break}] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.

$\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \geq \varepsilon(n) - \frac{q(n)}{2^n}$. $\varepsilon(n)$ is negligible. □

Remarks on CPA-Security from PRF

- 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 8

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

- **Efficiency**: $|c| = 2|m|$.

Pseudorandom Permutations

- **Bijection**: F is one-to-one and onto.
- **Permutation**: A bijective function from a set to itself.
- **Keyed permutation**: $\forall k, F_k(\cdot)$ is permutation.
- F is a bijection $\iff$ F^{-1} is a bijection.

Proposition 9

If F is a pseudorandom permutation then it is a PRF.

Definition 10

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

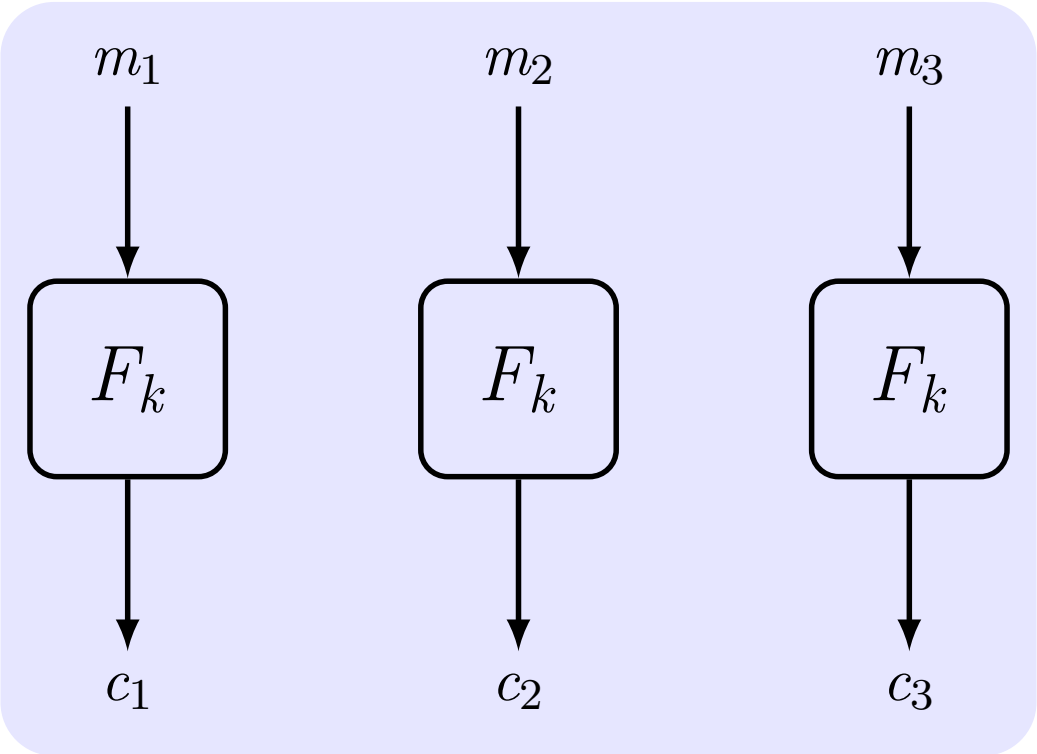
$$\left|\Pr[D^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n)=1]-\Pr[D^{f(\cdot),f^{-1}(\cdot)}(1^n)=1]\right|\leq \mathsf{negl}(n),$$

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

Block Cipher and Modes of Operation

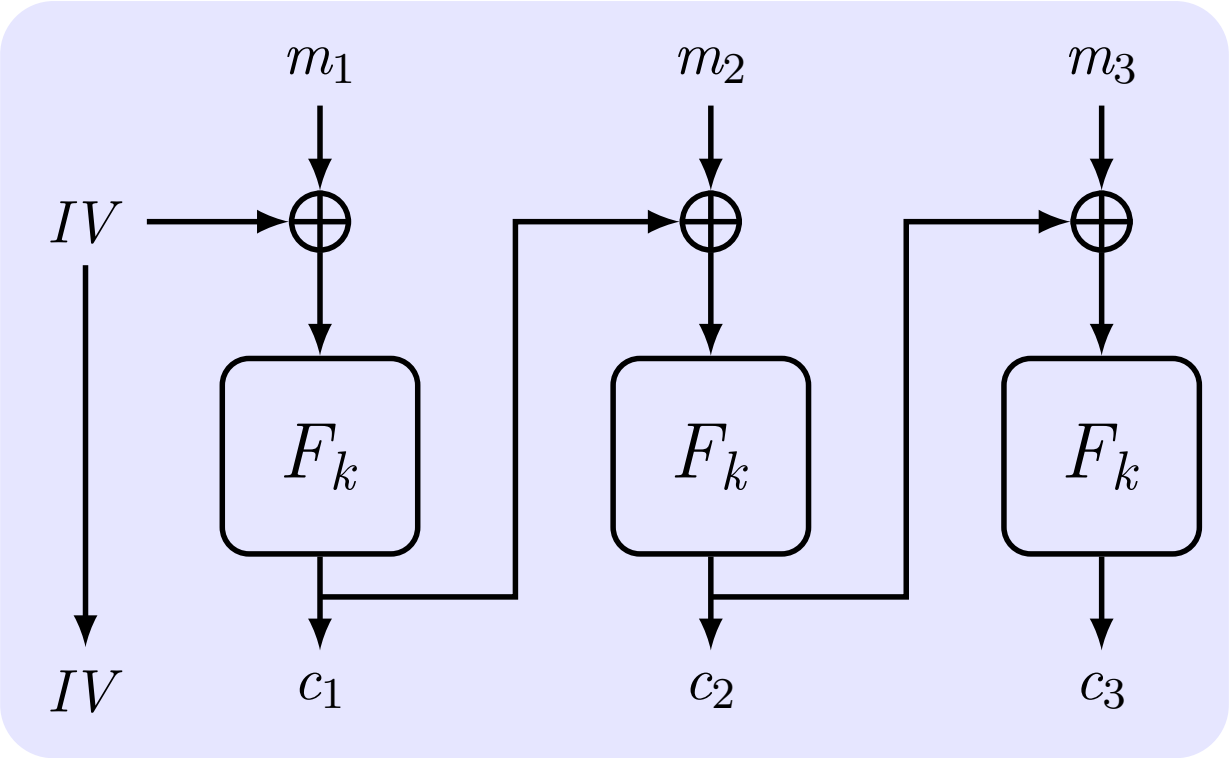
- **Block cipher**: A practical (strong) PRP.
  - Not encryption scheme, but a building block of encryption scheme.
  - Block cipher itself is not CPA-secure.
- **Modes of Operation**: A way of encrypting arbitrary-length messages using a block cipher/PRP.

Electronic Code Book (ECB) Mode



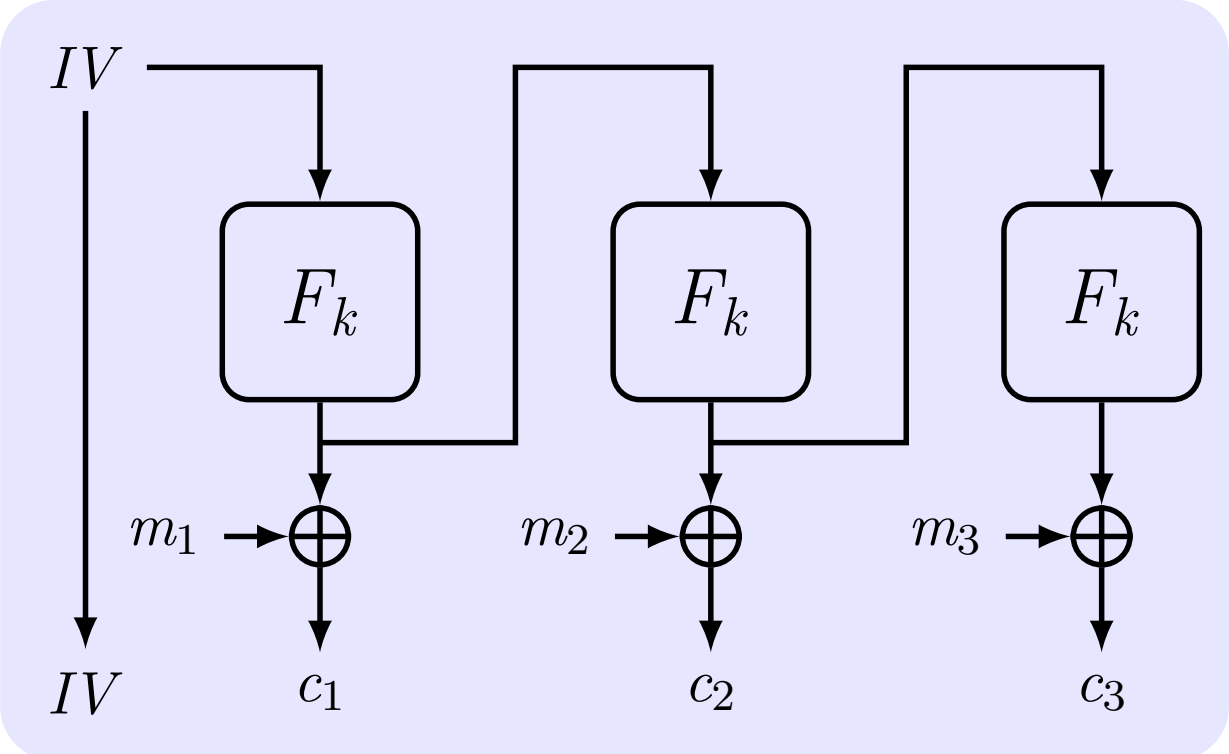
- **Weakness**: not indistinguishable in the presence of an eavesdropper.

Cipher Block Chaining (CBC) Mode



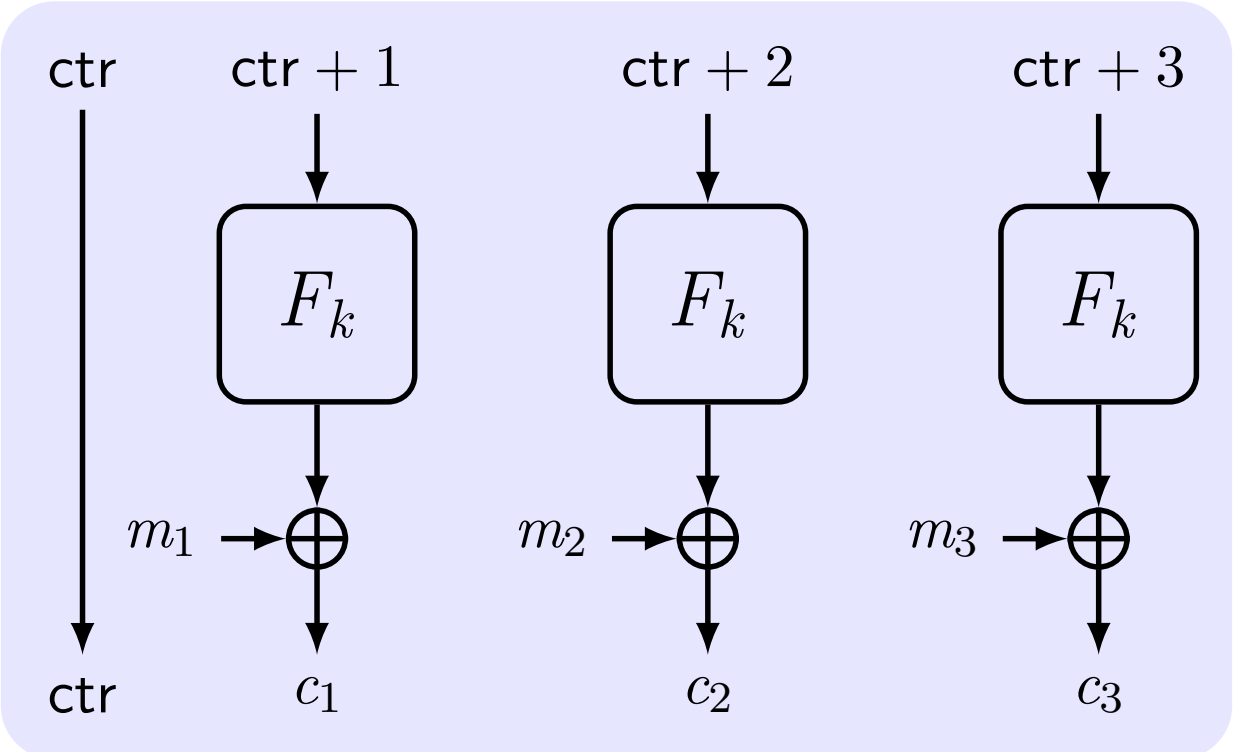
- **Strength**: CPA-secure.
- **Weakness**: not parallelizable.

Output Feedback (OFB) Mode



- **Strength**: CPA-secure, pre-processing the stream, PRF-compatible.
- **Weakness**: not parallelizable.

Counter (CTR) Mode



- **Strength**: CPA-secure, pre-processing the stream, PRF-compatible, parallelizable, random access.

CTR Mode Is CPA-secure

Theorem 11

If F is a PRF, then randomized CTR mode is CPA-secure.

Proof.

The message length and the number of query are $q(n)$.
Overlap: the sequence for the challenge overlaps the sequences for the queries from the adversary.
ctr^*: ctr in the challenge. ctr_i: ctr in the queries, $i = 1, \ldots, q(n)$.
Overlap: $\mathsf{ctr}_i - q(n) < \mathsf{ctr}^* < \mathsf{ctr}_i + q(n)$.

$$\Pr[\text{Overlap}] \leq \frac{2q(n) - 1}{2^n} \cdot q(n)$$

□

Proof of CPA-secure CTR Mode (Cont.)

Proof.

See proof of theorem **??**. (1) Analyze Break : $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1$.

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

(2) Reduce D to $\mathcal{A}$

$$\Pr[D^{f(\cdot),f^{-1}(\cdot)}(1^n) = 1] = \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1] \leq \frac{2q(n)^2}{2^n} + \frac{1}{2}$$

$$\Pr[D^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n) = 1] = \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \varepsilon(n)$$

If F is PRP, $\varepsilon(n)$ is negligible.

IV Should Not Be Predictable

If IV is predictable, then CBC/OFB/CTR mode is not CPA-secure.

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,
    AES_ENCRYPT or AES_DECRYPT);
```

User supplies IV

Input `ivec` should be random, otherwise it is not secure.

Remarks on Block Ciphers

- **Block length** should be sufficiently large.
- **Message tampering** is not with message confidentiality.
- **Padding**: TLS: For $n > 0$, n byte pad is $n, n, \ldots, n$. If no pad needed, add a dummy block.
- **Stream ciphers vs. block ciphers**:
  - Steam ciphers are faster but have lower security.
  - It is possible to use block ciphers in "stream-cipher mode".

Performance: Crypto++ 5.6, AMD Opetron 2.2GHz

	Block/key size	Speed MB/sec
RC4		126
Salsa20/12		643
Sosemanuk		727
3DES	64/168	13
AES-128	128/128	109

Content

Security Against CCA

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 12

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

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

Remarks on CCA-security

- In real world, the adversary might conduct CCA by influencing what gets decrypted.
  - If the communication is not authenticated, then an adversary may send certain ciphertexts on behalf of the honest party.
- None of the above scheme is CCA-secure: If one bit of CT is flipped, so does one bit of PT.
- CCA-security implies "**non-malleability**":
  If the adversary tries to modify a given ciphertext, either an illegal ciphertext or one that encrypts a plaintext having no relation to the original one.

Summary

- Asymptotic approach, proof of reduction, indistinguishable.
- PRG, PRF, PRP, stream cipher, block cipher.
- Security/construction against eavesdropping/CPA.
- EBC, CBC, OFB, CTR.