Cryptography

Lecture 3

Arpita Patra

Quick Recall and Today's Roadmap

>> Construction based on PRG

>> Overview of Proof by reduction

>> Proof of PRG-based SKE

>> Extension of CO-security to CO-MULT-security and the second is stronger than previous

>> Chosen Plaintext Attack (CPA), CPA Security, stronger than previous notions; minimum requirement for any SKE

>> Is it practical?

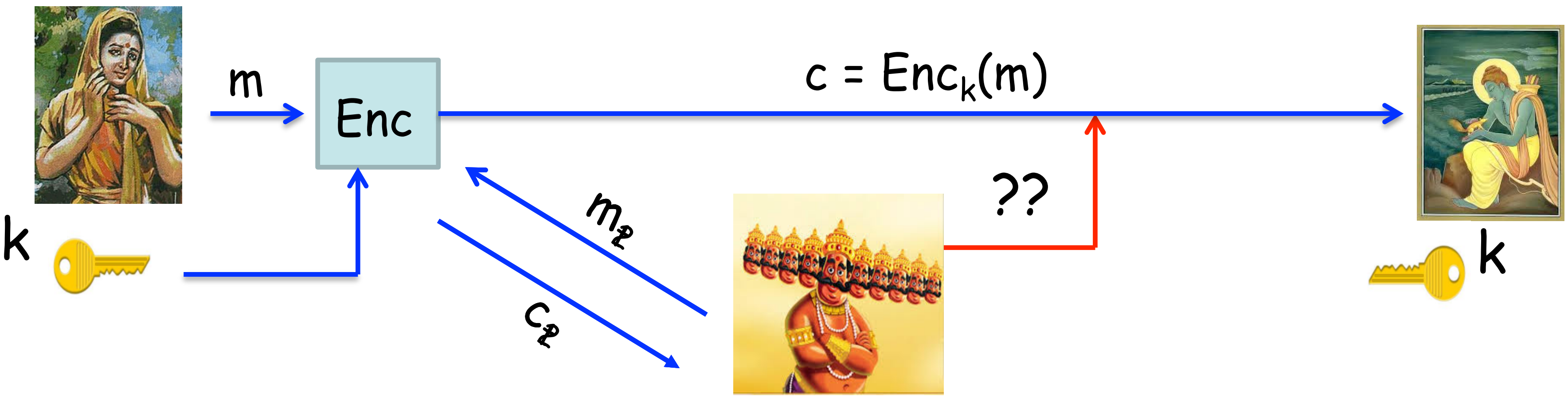
>> A construction for CPA-secure scheme

>> Proof of Security

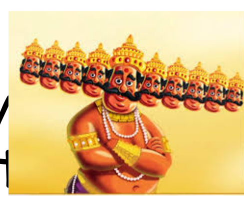
>> Extension to CPA-MULT-security

>> Modes of Operations (very efficient construction used in practice)

Chosen-Plaintext Attacks (CPA) (Single-message Security)



$(m_1, c_1), (m_2, c_2), \ldots, (m_t, c_t)$: $c_i = \mathrm{Enc}_k(m_i)$



>> Adversary ... s ... t encryption of plain-texts (using t... ke...

>> Adv's Goal: to determine the plain-text encrypted in a new cipher-text

CPA

M. Luby: Pseudorandomness and Cryptographic Applications; Princeton University Press, 1996

Mihir Bellare, Anand Desai, E. Jokipii, Phillip Rogaway:
A Concrete Security Treatment of Symmetric Encryption.
FOCS: 394-403, 1997

Is CPA Realistic ?

- How can an attacker influence parties to encrypt messages of its choice (using the same key) ?

- Consider a secure hardware with secret-key embedded

  » Often used in military applications

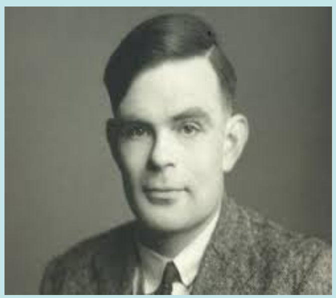
- An insider may have access to the hardware (not the key)

  » Can choose messages of its choice and get their encryptions

CPA shortened WWII by 2-3 Years

- Breaking of German codes by British during WW II

Allied Power



At Bletchley Park

Axis Power

$Enc_k(Loc_1)$ $Enc_k(Loc_2)$

$Enc_k(Loc_3)$

- Trivia: Who played a key role in this cryptanalysis process

CPA Indistinguishability Experiment

$\mathrm{PrivK}^{cpa}_{A,\Pi}(n)$ Π = (Gen, Enc, Dec), $\mathcal{M}$, n

Query: Plain-text

Response: Ciphertext

PPT Attacker A

I can break Π

Let me verify

k

Gen(1^n)

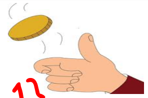
Training Phase:

>> A is given oracle access to $\mathrm{Enc}_k()$

>> A adaptively submits its query (free to submit m_0, m_1) and receives their encryption

CPA Indistinguishability Experiment

$\mathrm{PrivK}^{\mathrm{cpa}}_{A,\Pi}(n)$ $\qquad$ Π = (Gen, Enc, Dec), $\mathcal{M}$, n



$b \leftarrow \{0, 1\}$

Training Phase

PPT Attacker A

I can break Π

$m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

$c \leftarrow \mathrm{Enc}_k(m_b)$

Let me verify

k

Gen(1^n)

Challenge Phase:

>> A submits two equal length challenge plaintexts

>> A is free to submit any message of its choice (including the ones already queried during the training phase)

>> One of the challenge plaintexts is randomly encrypted for A (using fresh randomness)

CPA Indistinguishability Experiment

$\mathrm{PrivK}^{cpa}_{A,\Pi}(n)$ $\qquad$ Π = (Gen, Enc, Dec), $\mathcal{M}$, n

b ← {0, 1}

Training Phase

PPT Attacker A

I can break Π

$m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

$c \leftarrow Enc_k(m_b)$

Query: Plain-text

Response: Ciphertext

Let me verify

k

Gen(1^n)

Post-challenge Training Phase:

>> A is given oracle access to $Enc_k()$

>> A adaptively submits its query (possibly including m_0, m_1) and receives their encryption

CPA Indistinguishability Experiment

$\mathsf{PrivK}^{cpa}_{A,\Pi}(n)$ $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}), \mathcal{M}, n$

$b \leftarrow \{0, 1\}$

Training Phase

PPT Attacker A

I can break Π

$m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

$c \leftarrow \mathsf{Enc}_k(m_b)$

Post-challenge Training

Let me verify

k

$\mathsf{Gen}(1^n)$

$b' \in \{0, 1\}$

Game Output

$b = b'$

1 --- attacker won

$b \neq b'$

0 --- attacker lost

Response Phase:

- A finally submits its guess regarding encrypted challenge plain-text
- A wins the experiment if its guess is correct

CPA Security

$\mathrm{PrivK}^{cpa}_{A,\Pi}(n)$ $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec}), \mathcal{M}, n$

$b \leftarrow \{0, 1\}$

Training Phase

PPT Attacker A

I can break Π

$m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

$c \leftarrow \mathrm{Enc}_k(m_b)$

Post-challenge Training

$b' \in \{0, 1\}$

Let me verify

k

$\mathrm{Gen}(1^n)$

Game Output

$b = b'$

1 --- attacker won

$b \neq b'$

0 --- attacker lost

Π is CPA-secure if for every PPT A, there is a negligible function negl, such that:

$$\Pr\left(\mathrm{PrivK}^{cpa}_{A,\Pi}(n) = 1 \right) \leq \tfrac{1}{2} + \mathrm{negl}(n)$$

Search for Ingredients of CPA-Secure Scheme

- ❑ Encryption procedure cannot be deterministic. Can u find an attack?
- ❑ Encryption procedure MUST be randomized

  >> Need "fresh" randomness for each run of Enc. Results different ciphertexts for the same message

  >> At the same time want to use a "single key".


m → Enc → $c = (x_i, m \oplus y_i)$ →

??

x_1 = 00000…0	$y_1 \in_R \{0,1\}^n$
x_2 = 00000…1	$y_2 \in_R \{0,1\}^n$
…	…
x_{2^n} = 11111… 1	$y_{2^n} \in_R \{0,1\}^n$

$f: \{0,1\}^n \rightarrow \{0, 1\}^n$

y_i

Pad y_i is truly random

>> Instances of OTP

x_1 = 00000…0	$y_1 \in_R \{0,1\}^n$
x_2 = 00000…1	$y_2 \in_R \{0,1\}^n$
…	…
x_{2^n} = 11111… 1	$y_{2^n} \in_R \{0,1\}^n$

$f: \{0,1\}^n \rightarrow \{0, 1\}^n$

>> Problem with the above solution --- size of f is $n2^n$ bits

Ingredient for CPA-secure SKEs

- Need a smarter tool. A short key.
- Pseudorandom Function (PRF)

O. Goldreich, S. Goldwasser and S. Micali. How to Construct Random Functions. JACM, 33(4), 792-807, 1986

Pseudorandom Functions (PRF)

- What is a truly random function (TRF) ?

  >> Whose output behavior is completely unpredictable

  >> Given an input, it randomly assigns one element from the co-domain as the output

  >> Every element from the co-domain is a possible image with equal probability

- What is a PRF ?

  >> Intuitively a function whose output behavior "looks like" a TRF

  >> As long as the "entity" who observes is computationally bounded

- Given a function f: is it TRF or PRF ?

  >> Randomness/Pseudorandomness tag of a function is meaningful when it is drawn from a distributions of functions.

TRF vs PRF

For simplicity, consider functions from $\{0,1\}^n$ to $\{0,1\}^n$

- $Func_n = \{f_1, f_2, \ldots, f_{2^{n.2^n}}\}$ --- family of all such functions

  A function chosen uniformly at random from the above is a TRF

- $\overline{Func_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$ --- family of keyed functions with key length n

  A function chosen uniformly at random from the above is a PRF

- $|Func_n|$ >>>>>>>>>>> $|\overline{Func_n}|$

- PRFs are keyed functions; given key and input, there is an efficient way of computing a PRF

A possible Definition of PRF in PRG style

- Give F (table) either uniformly sampled from $Func_n$ or from $\overline{Func_n}$ to PPT distinguisher D and ask if it is a TRF or PRF.

  >> Does it work?

  >> No, since the description of the function is of exponential size

  >> Instead we give D oracle access to either a TRF or a PRF and ask "tell us who are you interacting with?"

  >> If D cannot tell apart the "behavior" of the function F_k (for a uniformly random k) from a truly random function f: $\{0,1\}^n \rightarrow \{0,1\}^n$, then we say f is a PRF.

Indistinguishability Game for PRF

$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

$\text{Func}_n = \{f_1, f_2, \ldots, f_{2^{n \cdot 2^n}}\}$

Oracle

PPT distinguisher D

Value of the funct at x_1

x_1

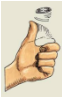
$y_1 = f(x_1)$

$f \in_R \text{Func}_n$

b= 0

Value of the function at x_1 is y_1

$\overline{\text{Func}_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$



b

Indistinguishability Game for PRF

$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

$Func_n = \{f_1, f_2, \ldots, f_{2^{n \cdot 2^n}}\}$

Oracle

PPT distinguisher D

Value of the funct at x_t

x_t

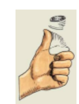
$y_t = f(x_t)$

b= 0

$f \in_R Func_n$

Value of the function at x_t is y_t

$\overline{Func_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$



b

- D can adaptively asks its queries
- D allowed to ask polynomial number of queries

Indistinguishability Game for PRF

$$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$$

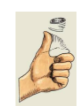
$Func_n = \{f_1, f_2, \ldots, f_{2^{n \cdot 2^n}}\}$

PPT distinguisher D

Value of the funct at x_1

Value of the function at x_1 is y_1

b= 1



b

$k \in_R \{0,1\}^n$

x_1

$y_1 = F_k(x_1)$

F_k

$\overline{Func_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$

Indistinguishability Game for PRF

$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

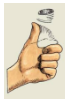
$Func_n = \{f_1, f_2, \ldots, f_{2^{n \cdot 2^n}}\}$

PPT distinguisher D

Value of the funct at x_t

Value of the function at x_t is y_t

b= 1



b

$k \in_R \{0,1\}^n$

x_t

$y_t = F_k(x_t)$

F_k

$\overline{Func_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$

- D can *adaptively* asks its queries
- D allowed to ask polynomial number of queries

Modeling PRF as an Indistinguishability Game

$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

$Func_n = \{f_1, f_2, \dots, f_{2^{n \cdot 2^n}}\}$

?

?

PPT distinguisher D

$(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$

$\overline{Func_n} = \{F_{k_1}, \dots, F_{k_{2^n}}\}$

F is a PRF if for every PPT D there is an negl(n)

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

>> uniformly random k

>> D's randomness

>> uniform choice of f

>> D's randomness

>> D not given k in the above game --- otherwise D can distinguish with high probability

Existence of PRF

- Do PRF exists ?
- OWF → PRG → PRF (Tree Construction) (otheway is also possible; take as an HW)

  >> NT based; Not used in practice

- Several practical PRFs

  >> Block Ciphers, AES, DES

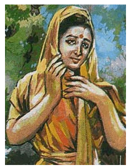
  >> No good distinguishers found till now; believed to be PRF

  >> AES/DES are PRFs: this is an assumption

  >> High practical efficiency compared to provably-secure PRFs

PRF-based CPA-Secure Scheme

Potential solution



Let us agree on a
truly random function

(secret meeting / mechanism)

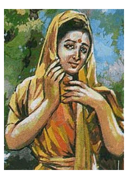
$x_1 = 00000\ldots0$	$y_1 \in_R \{0,1\}^n$
$x_2 = 00000\ldots1$	$y_2 \in_R \{0,1\}^n$
...	...
$x_{2^n} = 11111\ldots 1$	$y_{2^n} \in_R \{0,1\}^n$

Look-up table of a TRF f from $\{0,1\}^n$ to $\{0, 1\}^n$

Fixed-length CPA-Secure Encryption from PRF

Fixed-length encryption

- Let F be a length-preserving PRF (just for simplicity)
  - F: $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$
- Construct a CPA-secure encryption cipher for messages of length n



m,k

$Enc_k(m)$

>> r in $\{0, 1\}^n$

>> $c = (r, m \oplus F_k(r))$

c

c,k

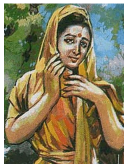
$Dec_k(c = (c0,c1))$

>> $m = c1 \oplus F_k(c0)$

Secret PRF-key k

(key-agreement)

Security Proof



m,k →

$Enc_k(m)$

>> r in $\{0, 1\}^n$

>> $c = (r, m \oplus F_k(r))$

c →

c,k →

$Dec_k(c = (c0,c1))$

>> $m = c1 \oplus F_k(c0)$

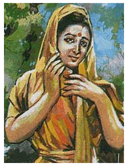
Secret PRF-key k

(key-agreement)

> Theorem. If F_k is a PRF, then Π is a CPA-secure scheme.

Proof: On the board.

Recall Security Proof of PRG-based Scheme



m,k → **$Enc_k(m)$** — $\gg c = m \oplus G(k)$ → c →

→ c,k → **$Dec_k(c)$** — $\gg m = c \oplus G(k)$

Secret PRG-key k

Theorem. If G is a PRG, then Π is a CO-secure scheme.

Proof: Assume Π is not secure

A, p(n): $\Pr\left(\mathrm{PrivK}^{co}_{A,\Pi}(n) = 1\right) > \frac{1}{2} + 1/p(n)$

$=$

$\Pr[D(G(s)) = 1]$

$\Pr\left(\mathrm{PrivK}^{co}_{A,\overline{\Pi}}(n) = 1\right) = \frac{1}{2}$

$=$

$\Pr[D(y) = 1]$

PRS or RS?

$y \in \{0,1\}^{l(n)}$ →

← 1 if $b = b'$

0 otherwise

D

b

Let us run $\mathrm{PrivK}^{co}_{A,\Pi}(n)$

$m_0, m_1 \in_R \mathcal{M}$, $|m_0| = |m_1|$ ←

$c = m_b \oplus y$ →

$b' \in \{0, 1\}$ ←

A

Pseudo Random Permutation (PRP)

$F: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$

$\text{Perm}_n = \{f_1, f_2, \ldots, f_{(2^n)!}\}$

?

?

PPT distinguisher D

$(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$

$\overline{\text{Perm}_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$ Distinct pairs

F is a PRF if for every PPT D there is an negl(n)

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

>> uniformly random k

>> D's randomness

>> uniform choice of f

>> D's randomness

Strong PRP

$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

$Perm_n = \{f_1, f_2, \ldots, f_{(2^n)!}\}$

?

PPT distinguisher D

?

$\overline{Perm_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$ $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$

$(y_1, x_1), (y_2, x_2), \ldots, (y_k, x_k)$

>> Any strong PRP is by default a PRP

>> What about the converse ?

F is a PRF if for every PPT D there is an negl(n)

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

>> uniformly random k

>> D's randomness

>> uniform choice of f

>> D's randomness

PRF/PRP/SPRP

- Theoretical instantiation of CPA-secure SKE from any PRF/PRP/SPRP.

- Practical instantiation of CPA-secure SKE from only PRP/ Strong PRP

  >> Ex: AES, DES; No distinguisher found so far

  >> Blocks ciphers

  >> Operates on block of message at a time --- hence the name

CPA Security for Multiple Encryptions

$\mathrm{PrivK}^{\text{cpa-mult}}_{A,\Pi}(n)$ $\qquad$ Π = (Gen, Enc, Dec), $\mathcal{M}$, n

$b \leftarrow \{0, 1\}$

Training Phase

PPT Attacker A

$\vec{M_0} = (m_{0,1}, \ldots, m_{0,t})$ $\quad$ $\vec{M_1} = (m_{1,1}, \ldots, m_{1,t})$

(freedom to choose any pair)

$c_1 \leftarrow \mathrm{Enc}_k(m_{b,1}), \ldots, c_t \leftarrow \mathrm{Enc}_k(m_{b,t})$

k

Gen(1^n)

Let me verify

I can break Π

Post-challenge Training

$b' \in \{0, 1\}$

Game Output

$b = b'$: 1 --- attacker won

$b \neq b'$: 0 --- attacker lost

Π is CPA-secure for multiple encryptions if for every PPT A, there is a negligible function negl, such that:

$$\Pr\left(\mathrm{PrivK}^{\text{cpa-mult}}_{A,\Pi}(n) = 1\right) \le \frac{1}{2} + \mathrm{negl}(n)$$

CPA Multiple-message vs Single-message Security

- Experiment $\mathrm{PrivK}^{\mathrm{cpa}}_{A,\Pi}(n)$ is a special case of $\mathrm{PrivK}^{\mathrm{cpa\text{-}mult}}_{A,\Pi}(n)$
  - Se

>> Converse was not true in the case of co-security

>> Ciphers with indistinguishable encryption for single message but no indistinguishable multiple encryptions

- Any ns is also CPA-secu
- What about the c verse ?

Theorem: Any cipher that is CPA-secure is also CPA-secure for multiple encryptions

- Sufficient to prove CPA-security for single encryption; rest is "for free"

CPA-security Guarantee in Practice

- Ensures security against CPA even if multiple messages are encrypted using a single key and communicated

  >> Even if the adversary knows that the encrypted messages belong to one of the two possible "classes"

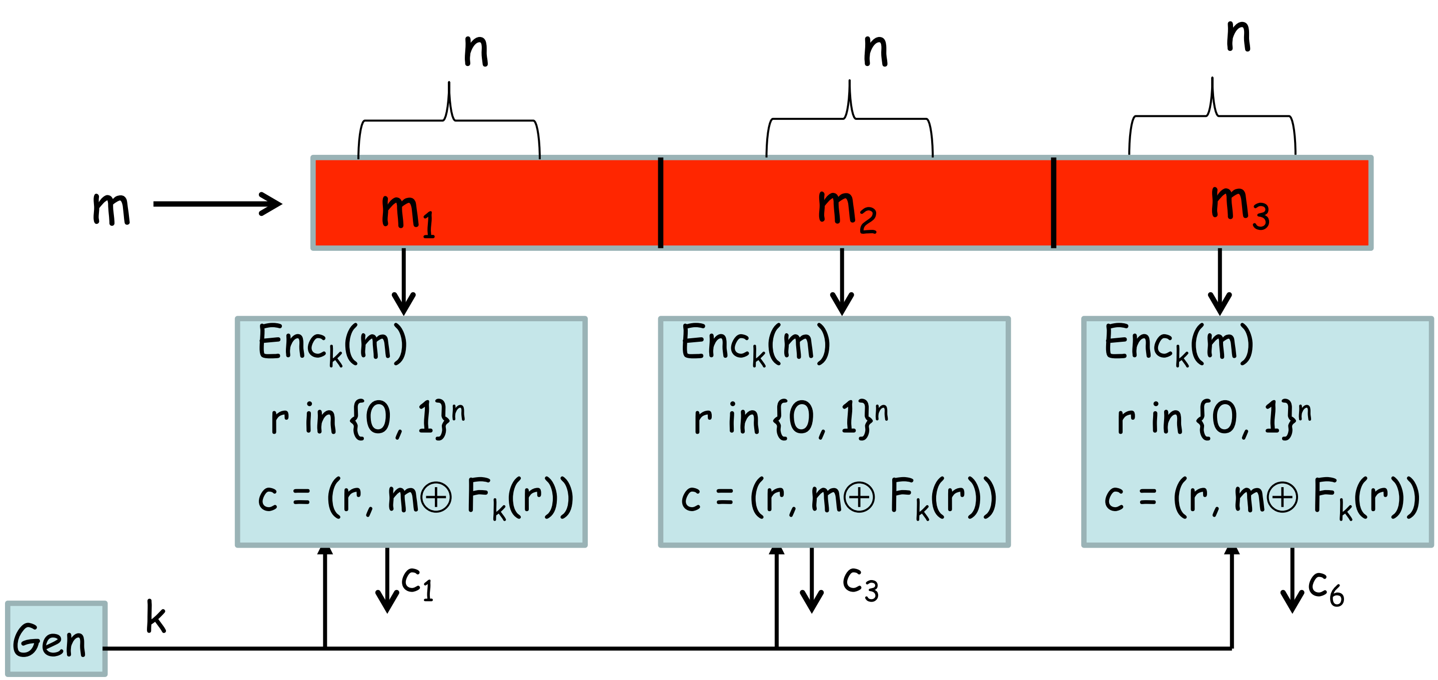
  >> Even if the adversary has seen encryptions of the messages in those classes in the past

- Very good security guarantees

  >> The least we should expect from a cipher

CPA-security for Arbitrary-length Messages (Theoretical Construction)

- Let Π = (Gen, Enc, Dec) be a fixed-length CPA-secure based on PRP/SPRP/PRF. Supports message of length



$c_1c_2 \ldots c_6 \leftarrow Enc_k(m)$

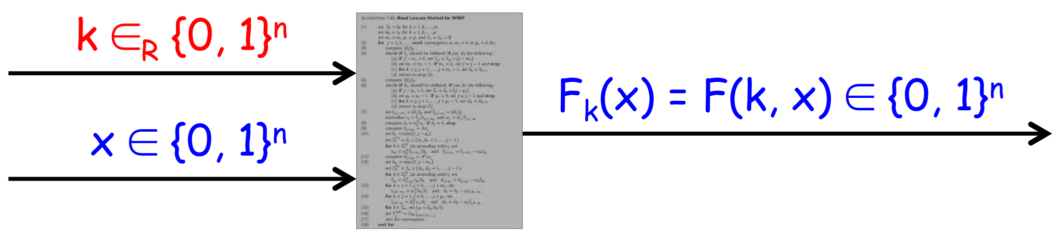
How Good it is?

Assume Message Blocks: k; $|m| = k\ n$

	Theoretical Construction	Finally
Randomness Usage	n / Block = kn	n / Overall = n
Ciphertext Expansion	2n / Block = 2kn	k n + n
Ciphertext Computation Parallelizabl e	Yes	Yes
Randomness Reusability	No	Yes
Minimal Assumption (PRF/PRP/ SPRP)	PRF	PRF
CPA Security	Yes	Yes

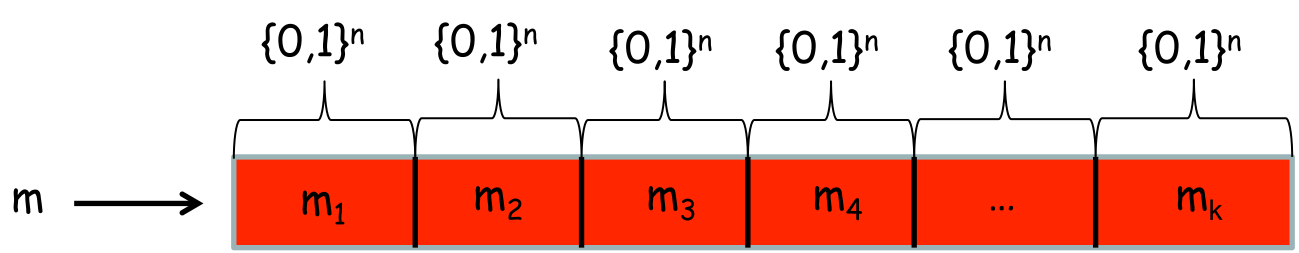
Block-cipher Modes of Operations

- Given
  - A length-preserving block cipher F (may be a PRF/PRP/SPRP) with block length n

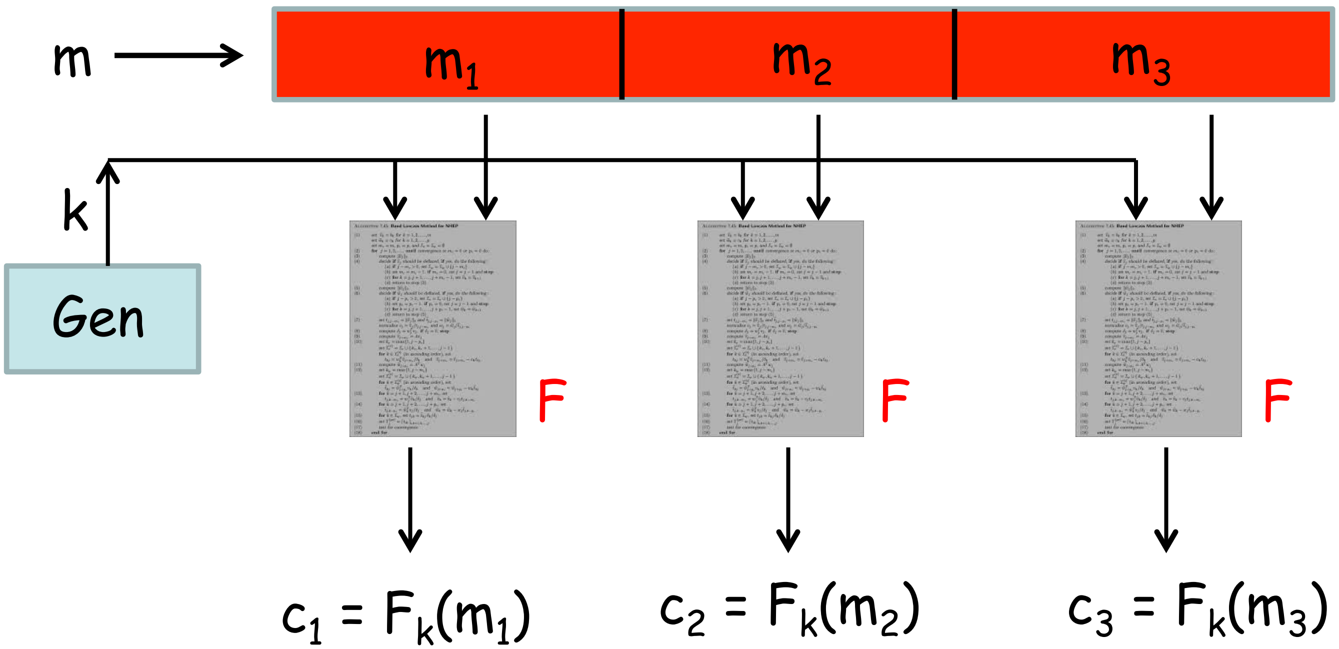


Keyed Algorithm F

- Goal
  - To encrypt a message $m = m_1 m_2 \ldots m_k$ using F with ciphertext length as small as possible and with randomness as less as possible.
  - Without loss of generality --- each $m_i \in \{0,1\}^n$



Electronic Code Book (ECB) Mode



- Encryption: compute $c_i = F_k(m_i)$ – No randomness used at all ! $|c| = |m|$
- Decryption: compute $m_i = F_k^{-1}(c_i)$ >> Assumes F_k is SPRP.
- Parallelizable!
- CPA Security ?

  >> Deterministic Encryption

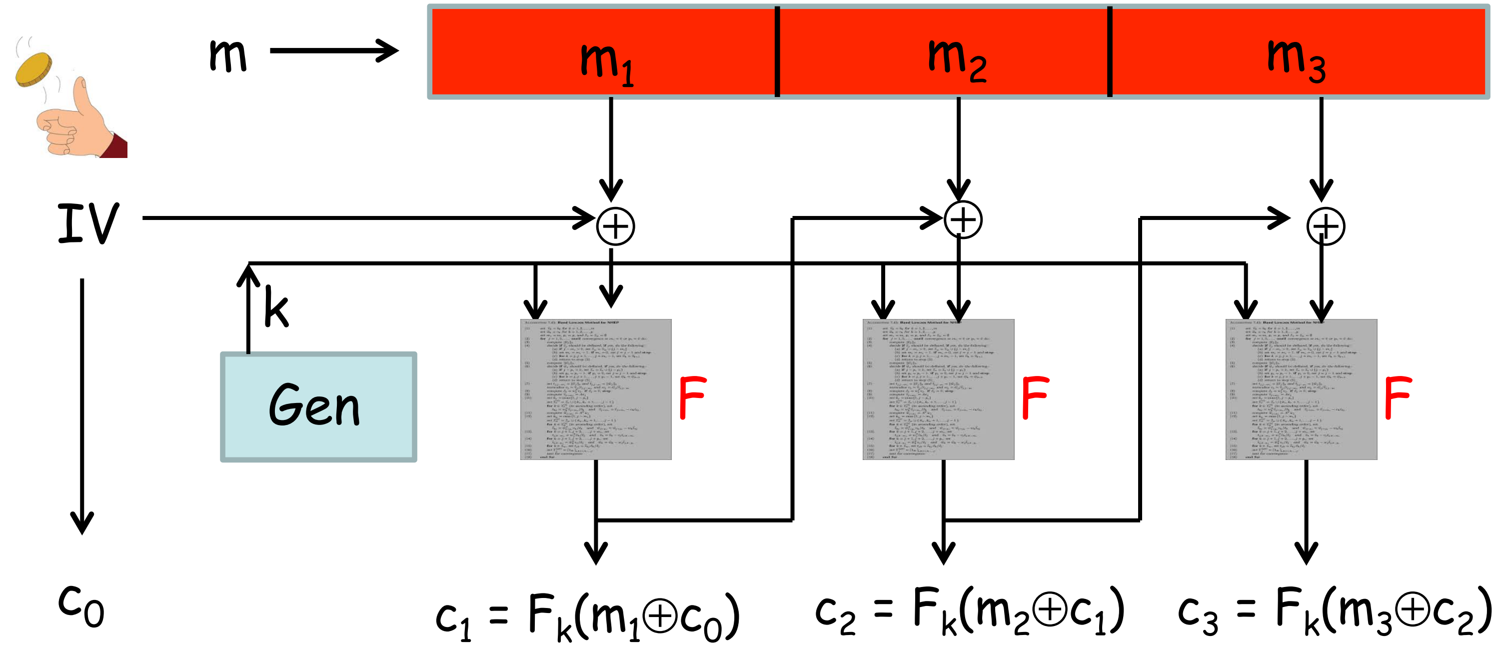
  >> No. not even CO security for multi message

Current Picture

Assume Message Blocks: k; $|m| = k\,n$

	Theoretical Construction	ECB Mode
Randomness Usage	n / Block = kn	No randomness
Ciphertext Expansion	2n / Block = 2kn	k n
Ciphertext Computation Parallizable	Yes	Yes
Randomness Reusability	No	---
Minimal Assumption (PRF/PRP/SPRP)	PRF	SPRP
CPA Security	Yes	NO

Cipher Block Chaining (CBC) Mode



Encryption $c_i = F_k(m_i \oplus c_{i-1})$, for $i = 1, \ldots, k$ $\quad Enc_k(m_1\, m_2 \ldots m_l) = (c_0\, c_1 \ldots c_l)$

Decryption: $m_i = F_k^{-1}(c_i) \oplus c_{i-1}$, for $i = 1, \ldots, l$ $\quad$ >> Assumes F_k is SPRP.

Blockwise Parallel Computation ? $\quad$ >> NO

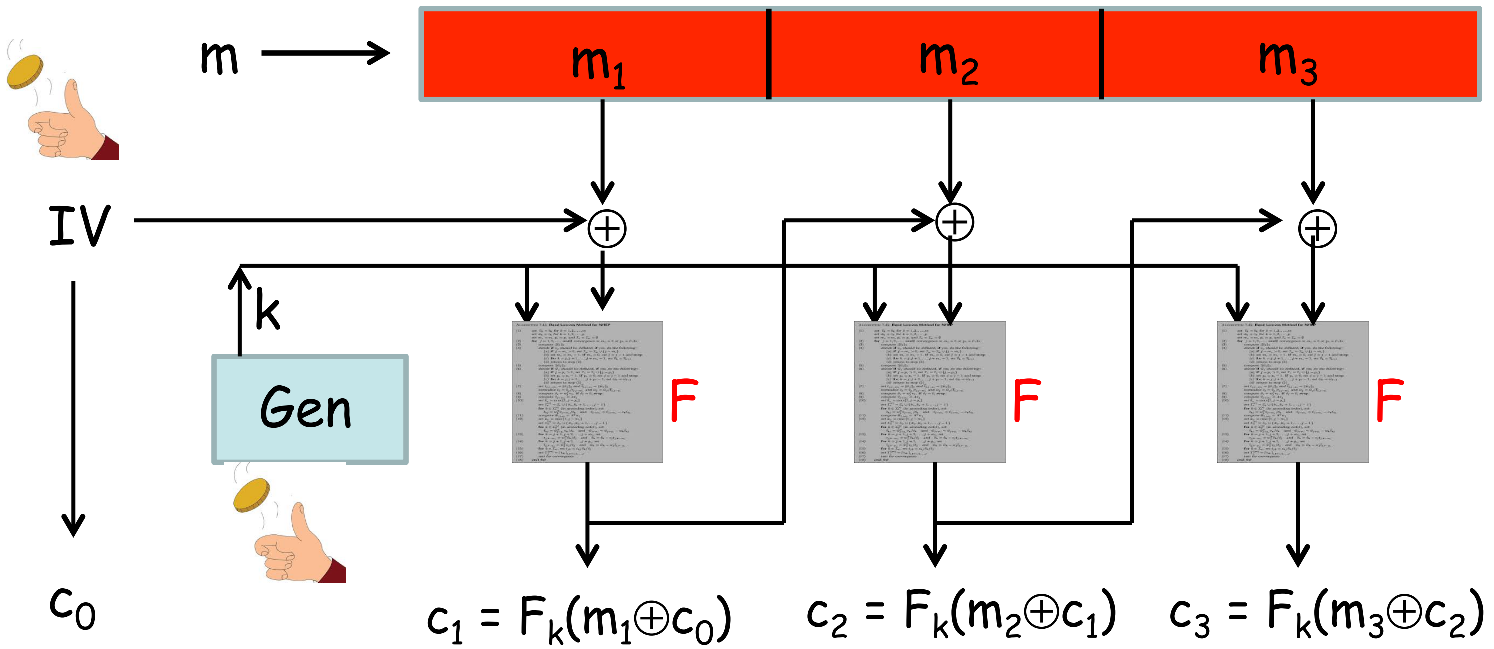
CPA Security ? $\quad$ >> Randomized Encryption. Provides CPA security. HW

Current Picture

Assume Message Blocks: k; $|m| = k\ n$

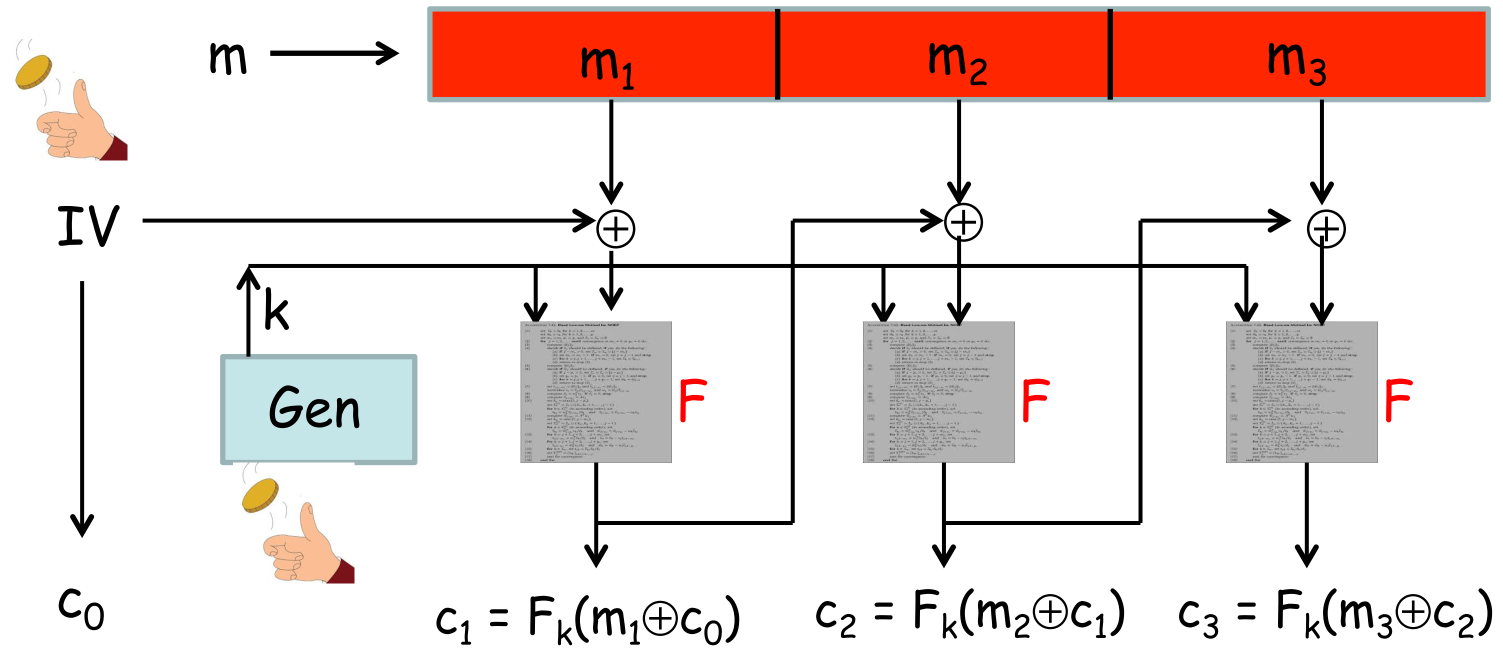
	Theoretical Construction	ECB Mode	CBC Mode
Randomness Usage	n / Block = kn	No randomness	n
Ciphertext Expansion	2n / Block = 2kn	k n	k n + n
Ciphertext Computation Parallizable	Yes	Yes	NO
Randomness Reusability	No	---	---
Minimal Assumption (PRF/PRP/SPRP)	PRF	SPRP	SPRP
CPA Security	Yes	NO	YES

IV Misuse in CBC Mode



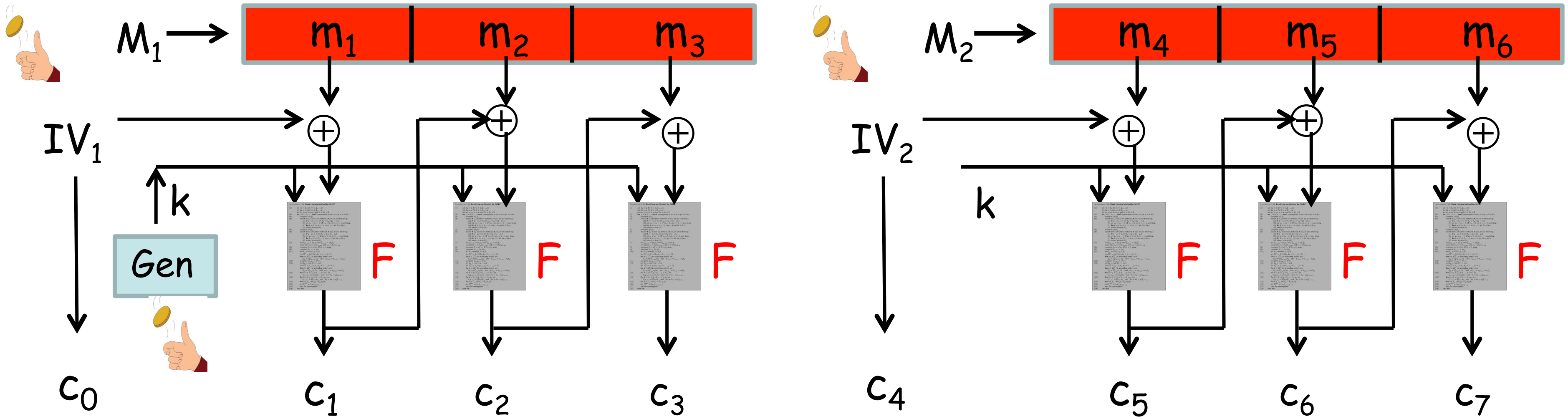
- Choosing distinct IV enough ? Can save randomness
- Unfortunately this version of CBC mode is not cpa-secure-- Assignment

IV misuse in CBC Mode



- Can the last ciphertext of previous block act as the IV for next encryption ?
  - Bandwidth and randomness saving

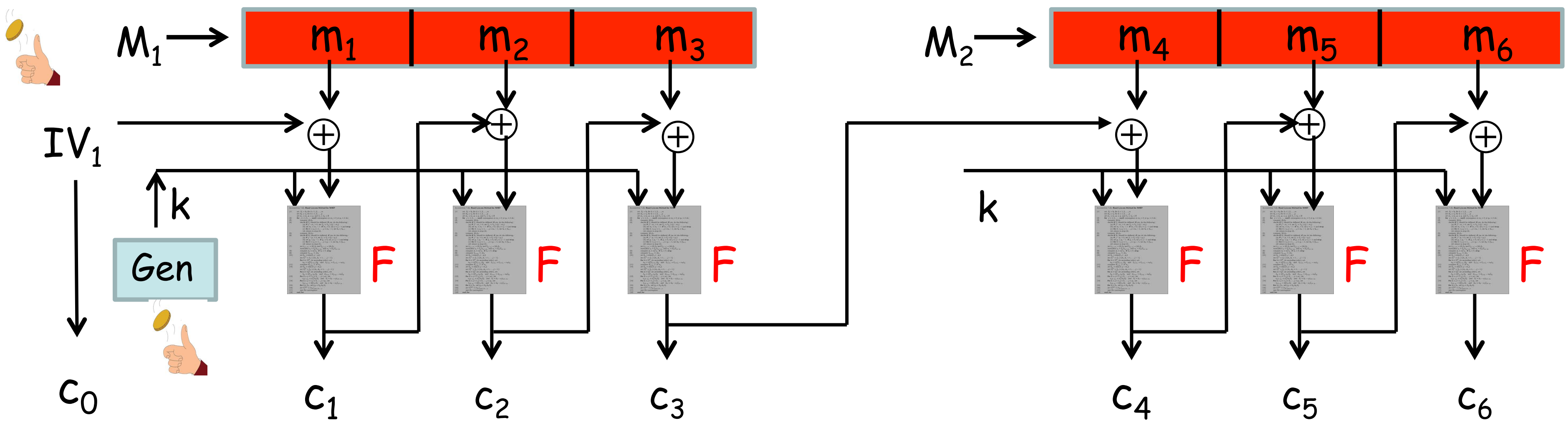
IV misuse in CBC Mode



Ideal way of encrypting two messages via CBC mode

- Can the last ciphertext of previous block act as the IV for next encryption ?
  - Bandwidth and randomness saving

IV misuse in CBC Mode- Chained CBC



Chained CBC mode

- Can the … act as th…
  - >> B…

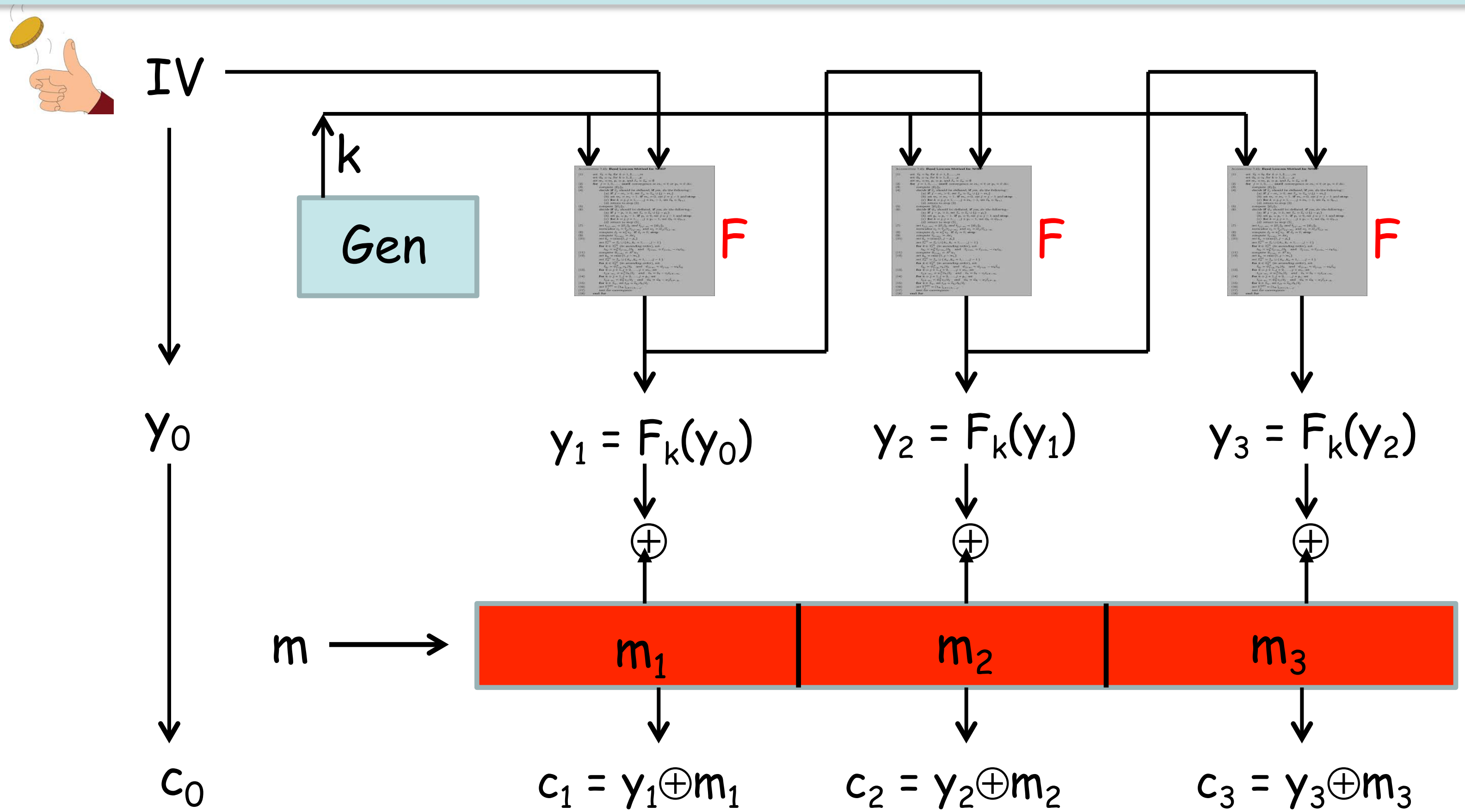
BEAST attack on SSL/TSL

- Chained CBC m…e — …used in SSL 3.0 and TL…
  - >> Stateful variant of CBC

No modifications to crypto schemes even if the modifications look benign

- CPA security?
  - >> It is "equivalent" to encrypting a single large message … $M_1 \,||\, M_2$ via CBC mode
  - >> Yet Not CPA-secure

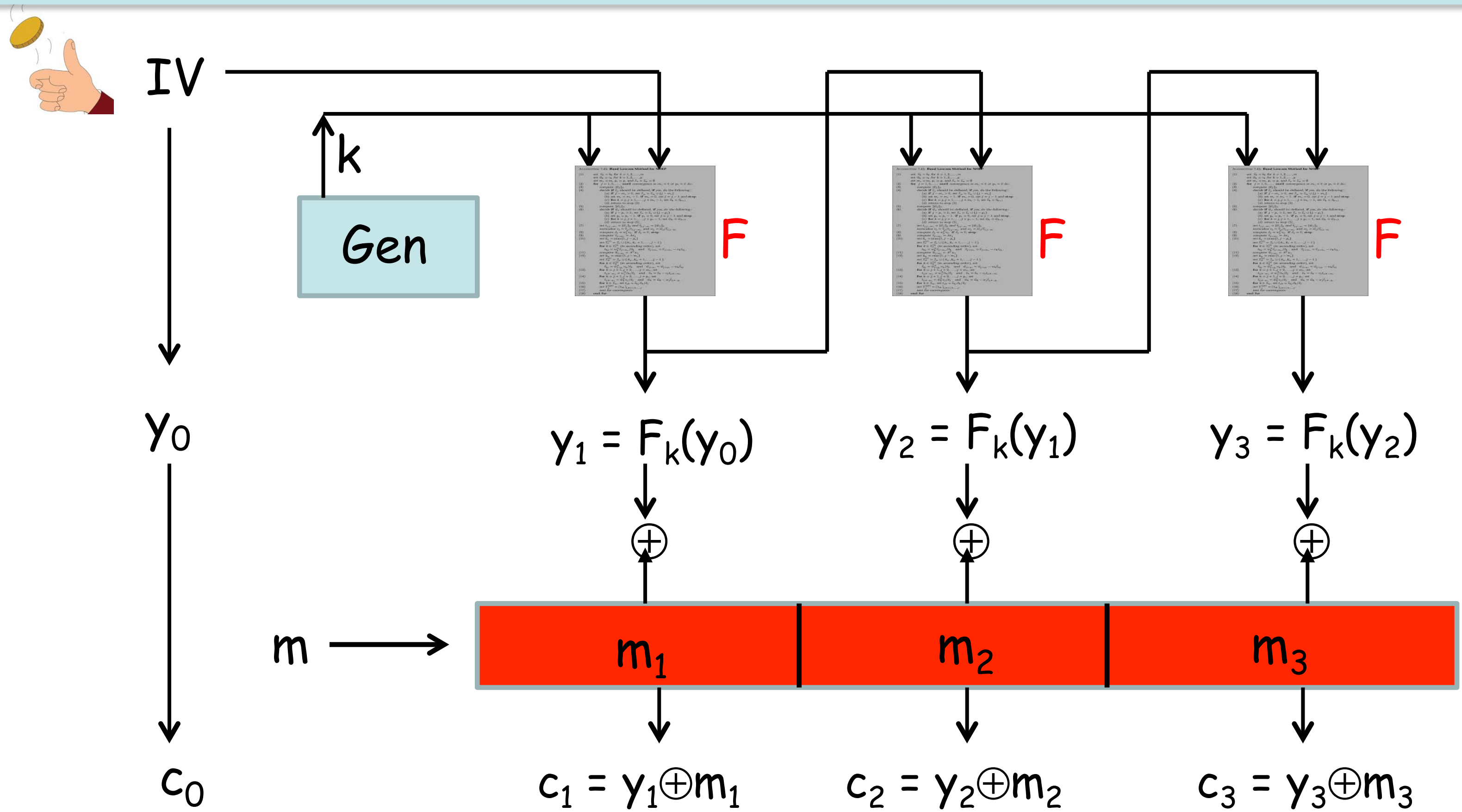
Output Feedback (OFB) Mode



Encryption: $Enc_k(m_1\ m_2\ \ldots\ m_l) = (c_0\ c_1 \ldots\ c_l)$

- First generate a pseudorandom stream of pad (independent of m)
- Use the pseudorandom stream for masking m

Output Feedback (OFB) Mode



Encryption: $Enc_k(m_1\ m_2\ \ldots\ m_l) = (c_0\ c_1 \ldots\ c_l)$

Decryption: $m_i = F(y_{i-1}) \oplus c_i$ PRF Enough !

Not parallalizable but pre-computable

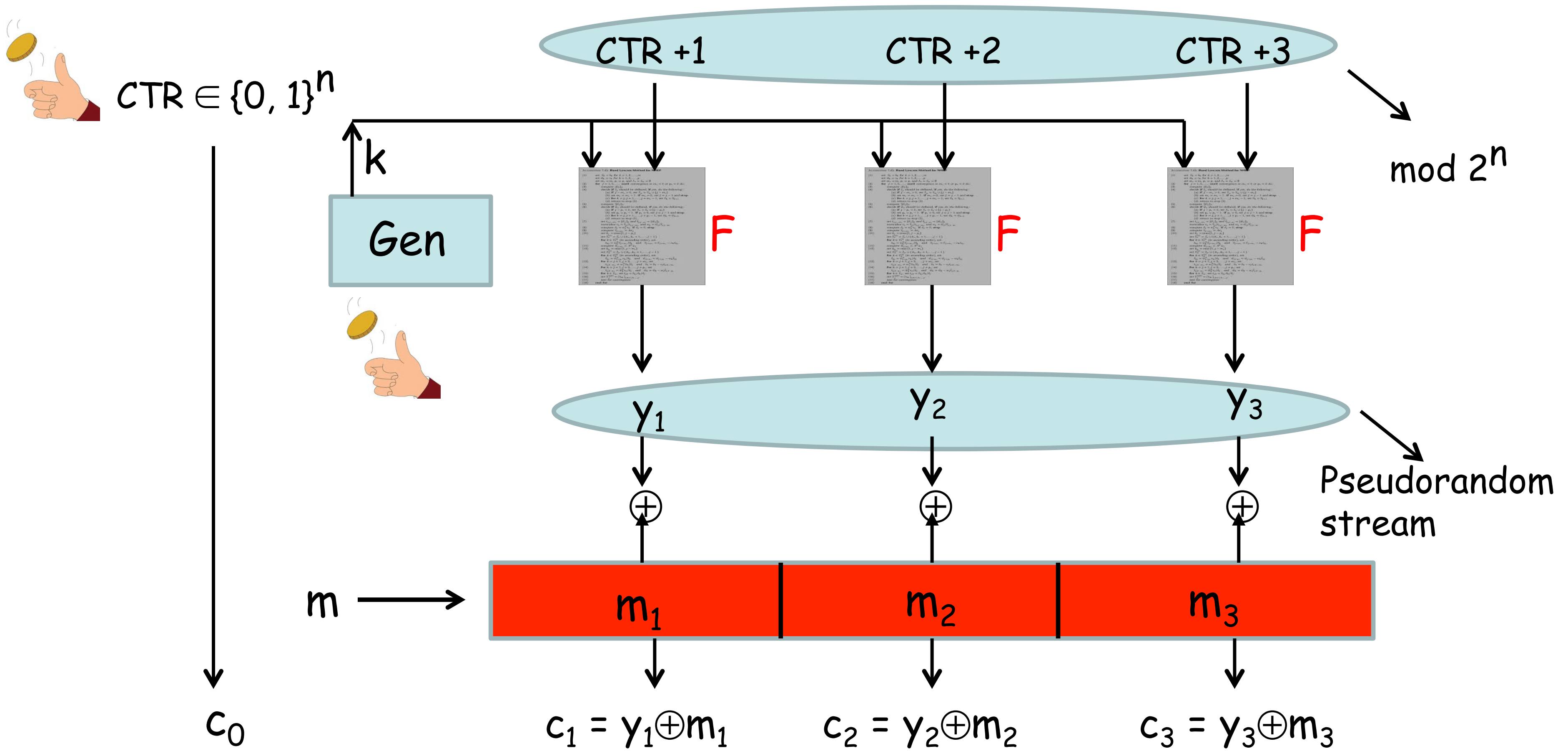
CPA-secure! The chained version too!

Current Picture

Assume Message Blocks: k; |m| = k n

	Theoretical Construction	ECB Mode	CBC Mode	OFB Mode
Randomness Usage	n / Block = kn	No randomness	n	n
Ciphertext Expansion	2n / Block = 2kn	k n	k n + n	k n + n
Ciphertext Computation Parallizable	Yes	Yes	NO	NO (But pre-computable)
Randomness Reusability	No	---	---	YES
Minimal Assumption (PRF/PRP/SPRP)	PRF	SPRP	SPRP	PRF
CPA Security	Yes	NO	YES	YES

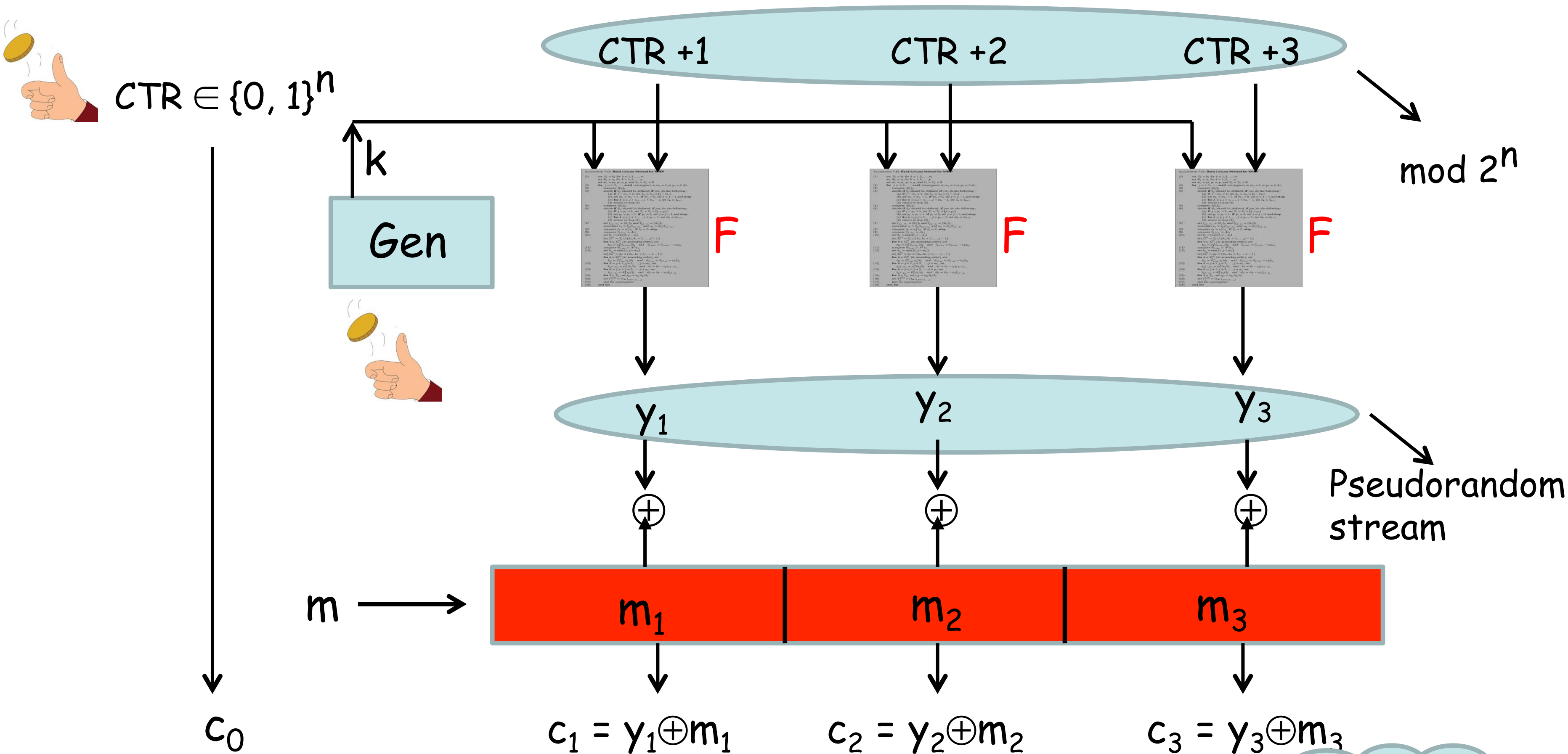
Counter (CTR) Mode



Encryption: $Enc_k(m_1\ m_2\ \ldots\ m_l) = (c_0\ c_1\ldots\ c_l)$

- Same idea as in OFB modes : pseudorandom stream followed by masking
  - However everything can be now parallelized

Counter (CTR) Mode



- Encryption: E
- Encryption /
- Can decrypt c
- Chained/Statefull variant is CPA-secure

Chalk &Talk Session 2 Topic:

CPA-security of CTR Mode

Highly attractive features

Current Picture

Assume Message Blocks: k; $|m| = k\ n$

	Theoretical Construction	ECB Mode	CBC Mode	OFB Mode	CTR Mode
Randomness Usage	n / Block = kn	No randomness	n	n	n
Ciphertext Expansion	2n / Block = 2kn	k n	k n + n	k n + n	k n + n
Ciphertext Computation Parallizable	Yes	Yes	NO	NO (But pre-computable)	YES
Randomness Reusability	No	---	---	YES	YES
Minimal Assumption (PRF/PRP/ SPRP)	PRF	SPRP	SPRP	PRF	PRF
CPA Security	Yes	NO	YES	YES	YES

Some Practical Issues

- Block length in practice
  - CBC, OFB, CTR mode uses a random IV as the starting point
  - For randomizing the encryption process
    - Ensures that each invocation of F is on a "fresh" input (w.h.p)
    - If two invocations of F are on the same input --- security issues
  - Ideal size of IV ? --- depends on block length supported by F
- Say the block length supported by F is l

Birthday paradox

  - In CTR mode, IV will be a uniform string of l bits
  - After $2^{l/2}$ encryptions, IV will repeat with a constant probability
  - If l is too short, then impractical security (even if F is a SPRP)
  - DES with $l = 64$ --- IV repetition after $2^{32} \approx 4, 300, 000, 000$ encryptions
    - Approximately 32 GB of plaintexts --- may not be too large for all applications

Some Practical Issues

- IV misuse
  - Assumption made: a uniform IV selected as the starting point
  - What if the assumption goes wrong (say due to poor randomness generation, incorrect implementation, etc) ?
  - Problems if IV is repeated
    - In the CTR and OFB modes, the same pseudorandom stream will be generated
      - Two messages XORed with the same stream --- serious security breach
    - In the CBC mode, the effect is not that serious
      - After few blocks, inputs to F will "diverge" (blocks of m are also part of the input)
- Solution against IV misuse
  - Use CBC mode
  - Or stateful OFB / CTR mode

Conclusion

- We discussed the notion of CPA
  - A very important class of (passive) attack
  - Minimum requirement from any cipher : CPA-security
- CPA-secure cipher requires stronger primitive than PRG
  - Solution: pseudorandom function (PRF)
- Fixed-length CPA-secure cipher using PRF
  - Arbitrary length CPA-secure encryption: divide into blocks and encrypt each block by fixed-length encryption --- theoretical (inefficient)
  - Practical solution (modes of operation of block ciphers)

Thank You!

Distribution for a TRF

- For simplicity, consider functions from $\{0,1\}^n$ to $\{0,1\}^n$

  >> How many such functions ? --- $2^{n.\,2^n}$

  >> $Func_n = \{f_1, f_2, \ldots, f_{2^{n.\,2^n}}\}$ --- family of all such functions

- f is a TRF $\{0,1\}^n$ to $\{0,1\}^n$ if picked uniformly at random from $Func_n$

  >> Picking a f from $Func_n \approx$

  >> Each row of the look-up table of f randomly selected from $\{0,1\}^n$

$x_1 = 00000\ldots0$	$y_1 \in_R \{0,1\}^n$
$x_2 = 00000\ldots1$	$y_2 \in_R \{0,1\}^n$
…	…
$x_{2^n} = 11111\ldots 1$	$y_{2^n} \in_R \{0,1\}^n$

>> Prob. that a random look-up table is of f = $\frac{1}{2^n} \times \frac{1}{2^n} \times \ldots \times \frac{1}{2^n}$

Distributions for a PRF

- $Func_n = \{f_1, f_2, \ldots, f_{2^{n \cdot 2^n}}\}$
- $\overline{Func_n} = \{F_{k_1}, \ldots, F_{k_{2^n}}\}$
- $|Func_n|$ >>>>>>>>>>> $|\overline{Func_n}|$
- Each function corresponds to a n-length key uniformly distributed over $\{0,1\}^n$

  >> The key facilitates efficient evaluation of the function

- PRFs are keyed functions

Insecurity of ECB Mode: A practical Example

- Think of some practical situation where encrypting using ECB mode is indeed dangerous
  - Suppose you want to encrypt a black and white image using ECB mode
  - Say a group of pixels in the image corresponds to one block of F

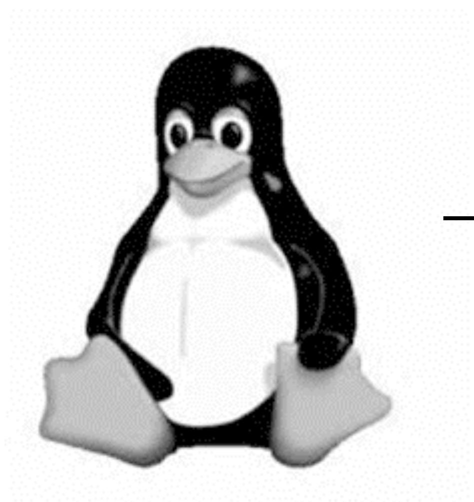
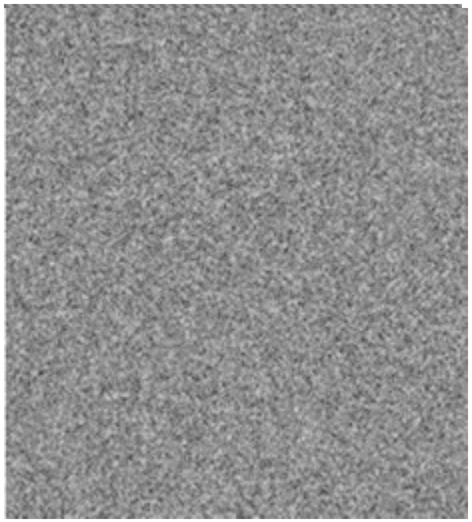


Image to be encrypted

Secure mode
ECB mode



Encrypted image (via a secure mode)

- Source: Wikipedia with imaged derived from Larry Ewing using GIMP

Block-cipher Modes of Operations : Some Practical Issues

- Message transmission errors (non-adversarial)
  - Dropped packets, changed bits, etc
  - Different modes of operations have different effect
  - Standard solutions --- error-correction, re-transmission
- Message transmission errors (adversarial)
  - What if the adversary "changes" ciphertext contents ?
  - Issue of message integrity / authentication
    - Will be discussed in detail later