23 Jan 2025

CPA security – Chosen plaintext attack

Various attack models,

More power

① Eavesdropping only – only power is to observe ciphertexts

② Known-plaintext attack -

attacker knows $(m_1, c_1), (m_2, c_2), \dots (m_t, c_t)$

t pairs of messages & ciphertexts are known to the attacker

Goal remains same as previously studied

i.e. Indistinguishability

Adv $\xrightarrow{(m_0^*, m_1^*)}$ challenger

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

$\longleftarrow$ $c = Enc(k, m_b^*)$

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

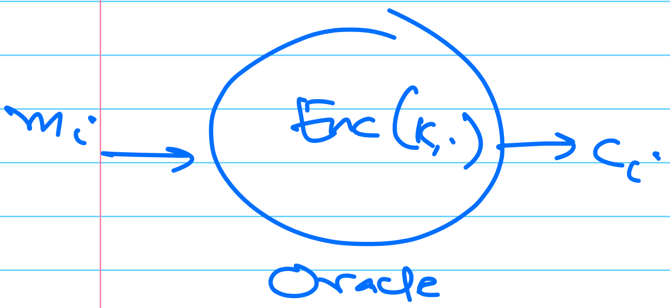
③ Chosen plaintext attack – (CPA)

attacker chooses messages m_i for $i = 1$ to t

receives c_i for these

Same goal as previous

≡ Encryption Oracle is available to the attacker



– $Enc(k, \cdot)$ is to be made available to the attacker

– But NOT the key k.

④ Chosen ciphertext attack (CCA)

CCA attacker = CPA attacker + ...

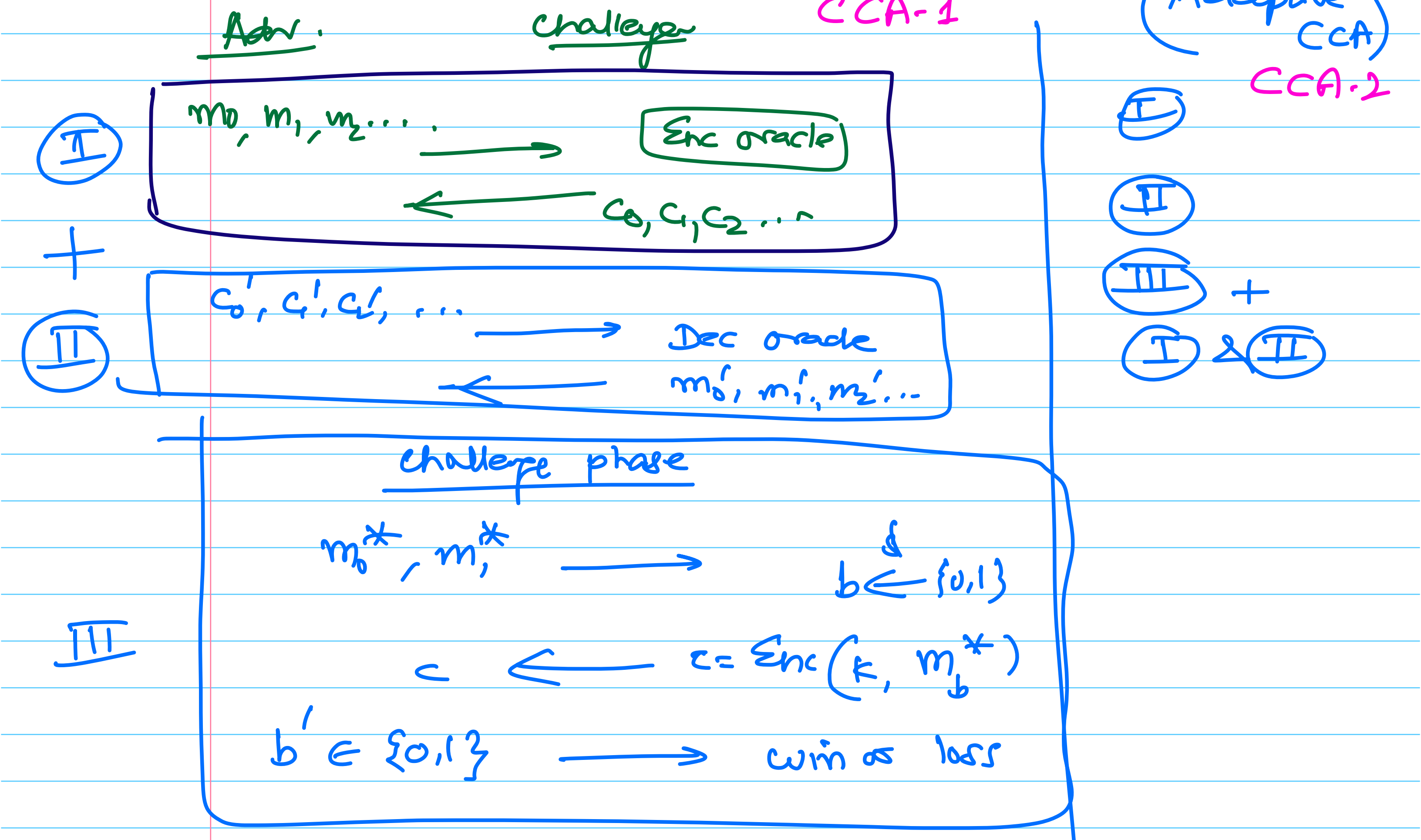
↓ Chosen ciphertexts can be decrypted

≡ Decryption oracle is available to the attacker

Restriction: can't ask for decryption of the challenge ciphertext

CCA (Non-adaptive CCA) CCA-1

(Adaptive CCA) CCA-2



Adv. Challenger

I $m_0, m_1, m_2 \ldots$ → Enc oracle

← $c_0, c_1, c_2 \ldots$

+

II $c_0', c_1', c_2', \ldots$ → Dec oracle

← $m_0', m_1', m_2' \ldots$

III challenge phase

m_0^*, m_1^* → $b \overset{\$}{\leftarrow} \{0,1\}$

c ← $c = Enc(k, m_b^*)$

$b' \in \{0,1\}$ → win or loss

CCA-2: I, II, III + I & II

Ultimate goal for encryption = CCA-2 Secure Encryption schemes

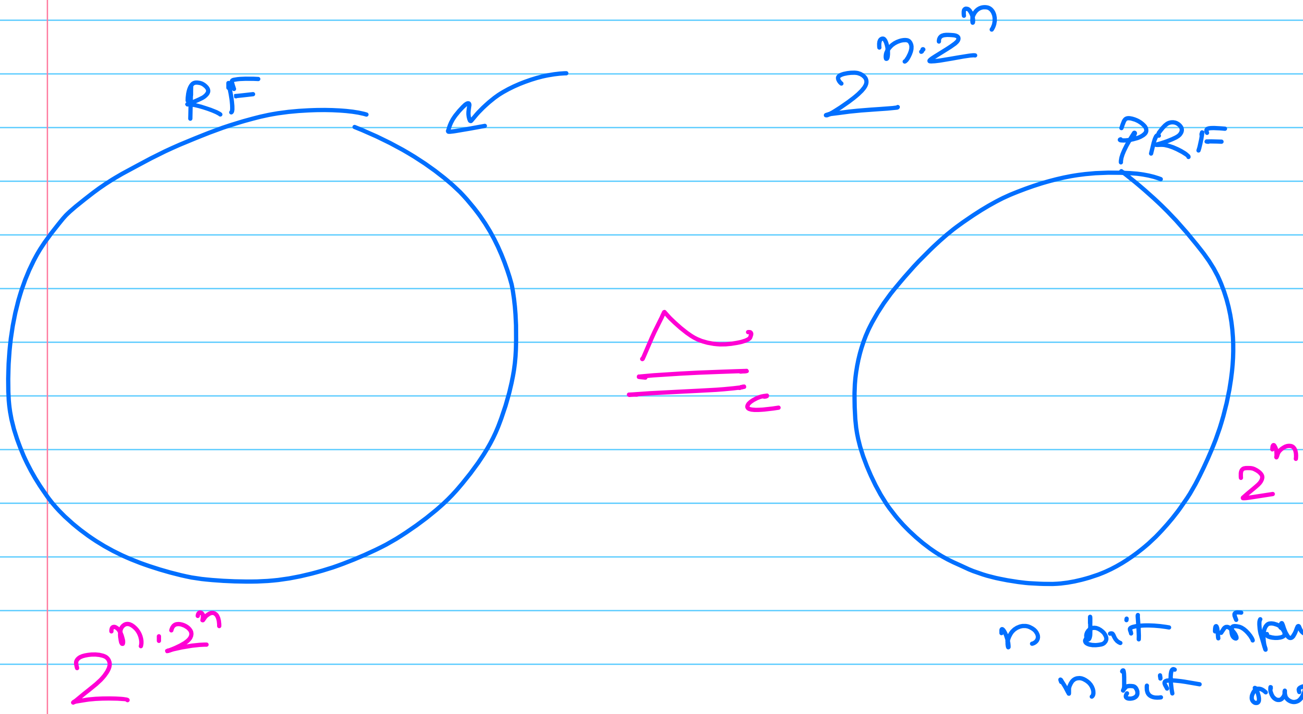
CPA secure Encryption :

- From previous class
  - Deterministic Encryption can't be CPA secure

PRF : Pseudo-Random function

Consider functions from $\{0,1\}^n \rightarrow \{0,1\}^n$
n-bit to n-bit function.

Que. How many such functions exist ?



n bit input to
n bit output
+ additional parameter
= key k ($\in$ n bits)

Keyed functions.

$F(k, \text{input}) \rightarrow \text{output}$

If key is fixed

$F_k(\cdot) \rightarrow$ deterministic

RF Computation in simulation -

$T[\,] = \{ \quad \}$ empty table

- user asks query i
- Challenger checks if $T[i]$ = empty or not

if empty then answer (n-bit random string)

also add $T[i]$ = ...

consistency in repeated queries

if not empty then answer $T[i]$

PRF Computation

- key k is chosen at random & fixed
- user asks query i

Challeger ansoers $F(k, i)$

Encryption algorithm using PRF

Enc: $k \leftarrow$ randomly generate

m to be encrypted $\in \{0,1\}^n$

with PRF $F(-,-)$

- randomly generate $r \in \{0,1\}^n$
- Compute $F(k, r)$

ciphertext $= (r, F(k,r) \oplus m)$

e.g. m being asked for encryption twice

first time ciphertext $= (r_1, f(k, r_1) \oplus m) = (c_1, c_2)$

second time $= (r_2, f(k, r_2) \oplus m) = (c_1', c_2')$

This scheme is CPA secure because of PRF property

This scheme is NOT CCA secure

- ask for encryption of m_1

$(r_1, f(k, r_1) \oplus m_1)$

$\underline{m_0^*}, \underline{m_1^*}$ → one of them is encrypted

$\boxed{\text{lsb of } (m_0^*) \neq \text{lsb } (m_1^*)}$

output we get is (c_1, c_2)

ask for decryption of

$(c_1, c_2 \oplus 1)$

$\boxed{\text{No class tomorrow}}$ — Recording will be made