Cryptography

Lecture 2

Arpita Patra

Summary of Last Class

- Introduction

  >> Zoo/ Mammoth and felt the subject's vastness against our negligible knowledge

  >> Three fundamental principles of Modern Crypto – Formal Definitions, Well-studied Assumptions, Sound Proofs

- Secure Communication in Symmetric Key setting

  >> SKE is the required primitive. Syntax: (Gen, Enc, Dec), M

  >> Definition of SKE: Key components: threat (who?) and break (what?)

  >> Threat: Common:- (bounded with negl success probability; randomized) to all Computational security definitions; will vary attack model: Ciphertext-only (CO) Attck.

  >> Break: No partial info about the message is leaked from the ciphertext irrespective of what external information adv has (except with negl. probability)

  >> the very basic definition of CO-Security both in IND and SIM style that are equivalent

  >> PRG as a tool to build SKE with CO-security. IND-based definition for PRG.

Today's Roadmap

- Construction based on PRG
- Overview of Proof by reduction
- Proof of PRG-based SKE: IND style CO-security
- Extension of CO-security to CO-MULT-security
- PRG-based scheme is insecure; hunt for new scheme (assignment problem)
- Chosen Plaintext Attack (CPA), CPA Security
- Is it practical?
- A construction for CPA-secure scheme

IND: Ciphertext Only Security

Common Feature: Experiment- a game between a challenger and an adversary

Eavesdropping indistinguishability experiment $\text{PrivK}^{co}_{A,\Pi}(n)$ $\Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \mathcal{M}$

Attacker A

I can break Π

Run time: Poly(n)

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

(freedom to choose any pair)

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

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

(Attacker's guess about encrypted message)

Challenger

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

Let me verify

$k \leftarrow \text{Gen}(1^n)$

$b = b'$ → 1 --- attacker won

$\text{PrivK}^{co}_{A,\Pi}(n)$

$b \neq b'$ → 0 --- attacker lost

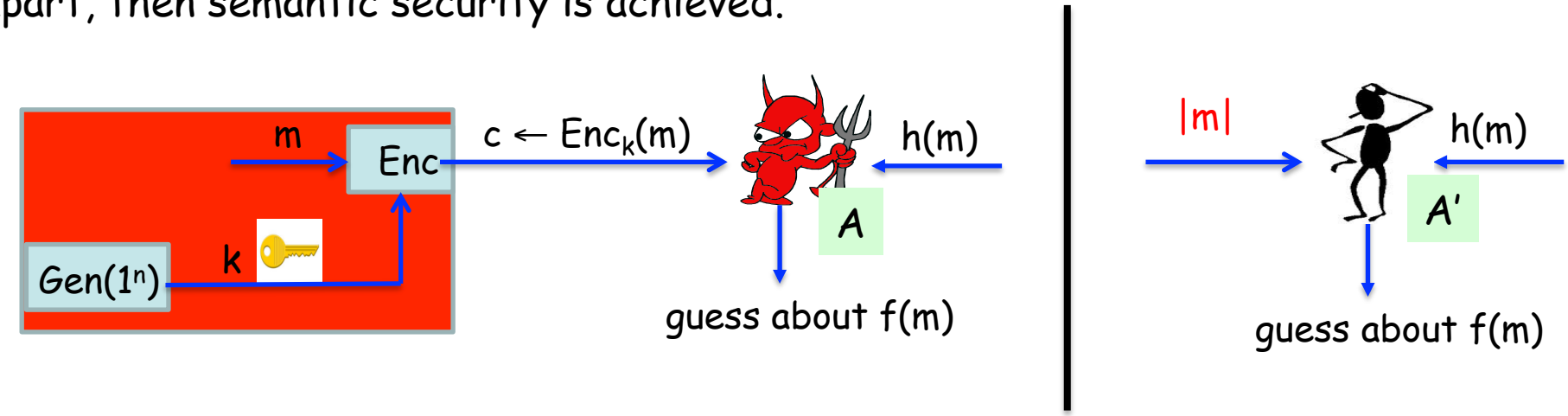
Π has indistinguishable encryptions in the presence of an eavesdropper or is co-secure if for every PPT attacker A, there is a negligible function negl(n) such that

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

Probability is taken over the randomness used by A and the challenger

SEM: Ciphertext Only Security

Two worlds: In one adv gets ciphertext and in another it does not. If the difference between probabilities of guessing f(x) in the both worlds are negligibly apart, then semantic security is achieved.



Π = (Gen, Enc, Dec) is semantically-secure in the presence of a eavesdropper if for every PPT A there exists a A' such that for any Samp and PPT functions f and h:

$$\left| \Pr[A(1^n, c, h(m)) = f(m)] - \Pr[A'(1^n, |m|, h(m)) = f(m)] \right| \leq \text{negl}(n)$$

Probability taken over
>> uniform k,
>> m output by $Samp(1^n)$,
>> the randomness of A and
>> the randomness of Enc

Probability taken over
>> m output by $Samp(1^n)$ and
>> the randomness of A'

PRG Security

U : uniform distribution over $\{0,1\}^{l(n)}$

PPT distinguisher D

A string of length l(n) please

y

How I selected it ?

Challenger

Oracle

A random string of length l(n) plz

$y \in_R \{0,1\}^{l(n)}$

b= 0

b= 1

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

$y := G(s)$

G

G: Probability distribution over $\{G(s): s \in_R \{0,1\}^n\}$

G is a PRG if for every PPT D, there is a negligible function negl

$$\left| \Pr_{r \in_R \{0,1\}^{l(n)}}[D(r) = 1] - \Pr_{s \in_R \{0,1\}^n}[D(G(s)) = 1] \right| \leq negl(n)$$

Probability taken over
>> Random Choice of r
>> the randomness of D

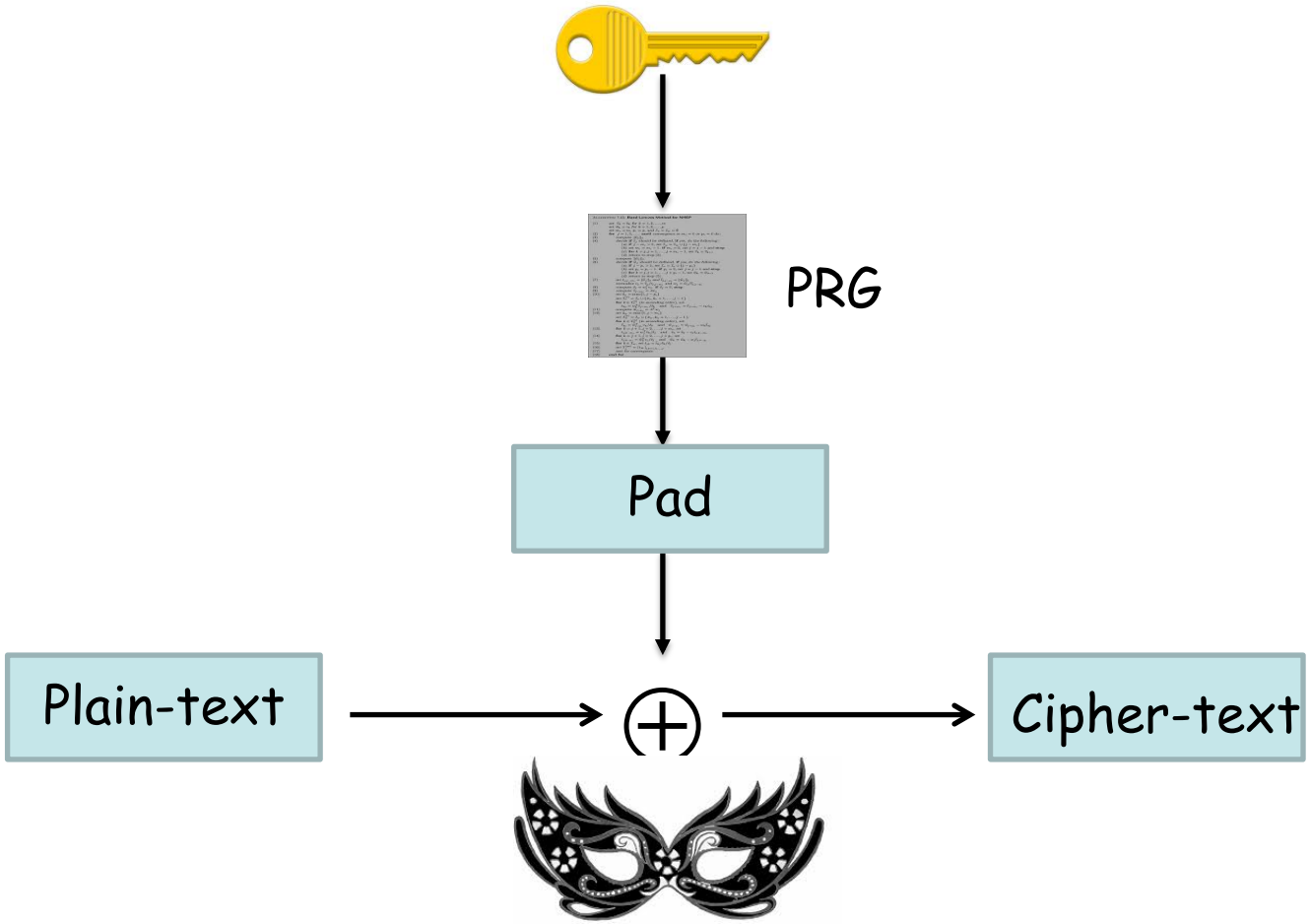
Probability taken over
>> Random Choice of s
>> the randomness of D

Existence of PRG

- Do PRG exists ?
- OWF + hardcore bit → PRG
  - Provably secure

- Several practical PRGs (Stream Ciphers)
  - No good distinguishers found till now
  - High practical efficiency compared to provably-secure PRGs

Secure Communication using PRG



- Sender and receiver share a (short) PRG key
  - ➢ Pseudo-random pad instead of a truly random pad

SKE from PRG

- Let G be a PRG with expansion factor $l(n)$
- We design a cipher for encrypting messages of length $l(n)$

  The scheme is fixed-length encryption

>> Gen:

- Input: security parameter n
- Output: key $k \in_R \{0,1\}^n$

>> Enc:

- Input: secret key k; plain-text $m \in \{0,1\}^{l(n)}$
- Output: cipher-text $c := G(k) \oplus m$ ⟶ Deterministic encryption

>> Dec:

- Input: secret key k; cipher-text $c \in \{0,1\}^{l(n)}$
- Output: plain-text $m := G(k) \oplus c$

Proof by Reduction

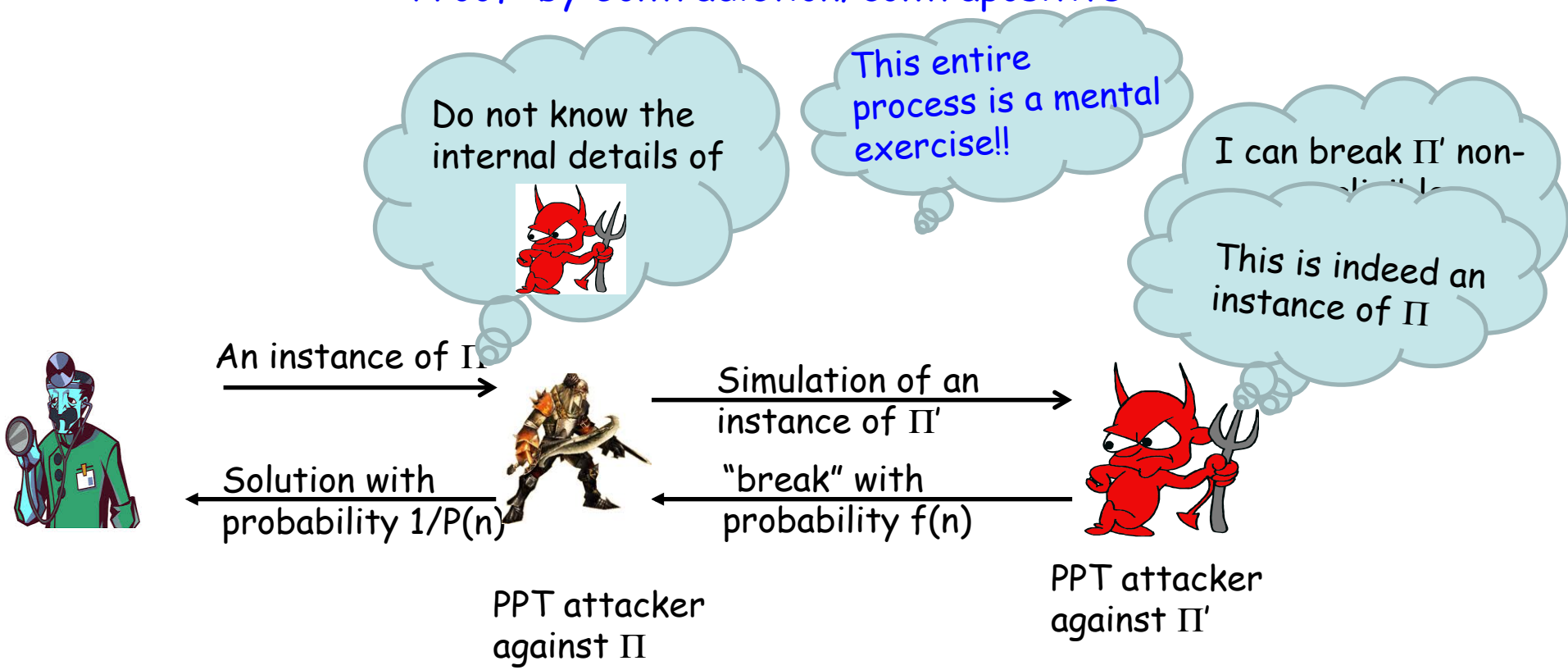
Case1: If Π is secure then Π' is secure

Case2: If A holds then Π is secure

Case3: If A1 holds then A2 holds

Case4: If Π is secure then A holds

Proof by Contradiction/contrapositive



The probability that PPT attacker for Π breaks security is f(n)/P(n)

--- Non-negligible

Security of the PRG-based SKE

Theorem: If G is a PRG, then Π is a fixed-length CO-secure SKE.

Proof: On the white broad.

Security for Multiple Encryptions

- Till now we considered an eavesdropper monitoring a single ciphertext
- Desirable (in practice):
  - Several messages encrypted using a single key
  - A PPT eavesdropper observes all the ciphertexts
  - Not captured in previous SEM/IND CO-security definition.
- Require a new definition
  - Semantic Paradigm: No PPT eavesdropper can non-negligibly compute any polynomial function of the underlying plain-texts by looking at the ciphertexts
  - IND Paradigm: Even though Adv knows the two sets of ciphertexts encrypted in the ciphertext, he cannot decide which set is encrypted.

Multiple-message Ciphertext Only Security

$\text{PrivK}^{\text{co-mult}}_{A,\Pi}(n)$ $\quad \Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \mathcal{M}$

Attacker A

I can break Π

Run time: Poly(n)

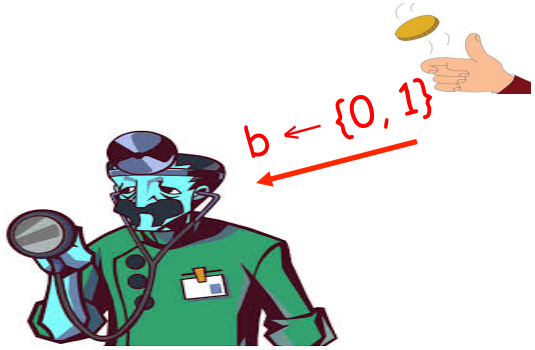
$\vec{M_0} = (m_{0,1}, \ldots, m_{0,t})$ $\quad \vec{M_1} = (m_{1,1}, \ldots, m_{1,t})$

(freedom to choose any pair)

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

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

(Attacker's guess about encrypted vector)



Game Output

$b = b'$ → 1 --- attacker won

$b \neq b'$ → 0 --- attacker lost

Π has indistinguishable multiple encryptions in the presence of an eavesdropper or is CO-MULT-secure if for every PPT attacker A taking part in the above experiment, the probability that A wins the experiment is at most negligibly better than $\frac{1}{2}$

i.e. $\Pr\left[\text{PrivK}^{\text{co-mult}}_{A,\Pi}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n)$

Relation between Multiple-message and Single-message Security

- Experiment $\text{PrivK}^{co}_{A,\Pi}(n)$ is a special case of $\text{PrivK}^{co\text{-}mult}_{A,\Pi}(n)$
  - $\text{PrivK}^{co}_{A,\Pi}(n)$ is the same as $\text{PrivK}^{co\text{-}mult}_{A,\Pi}(n)$ with $|\vec{M}_0| = |\vec{M}_1| = 1$
- Any cipher which has indistinguishable multiple encryptions has also indistinguishable encryptions
- What about the converse ?
  - Not necessarily

Multiple-message Security is Stronger than Single-message Security

Attacker A

$\vec{M}_0$ = (hello, hello) $\vec{M}_0$ = (hello, world)

c_1 := hello ⊕ k c_2 := hello ⊕ k If b = 0

c_1 := hello ⊕ k c_2 := world ⊕ k If b = 1

$$\Pr\left[\text{PrivK}^{\text{co-mult}}_{A,\text{OTP}}(n) = 1\right] = 1$$

b′ = 0 if $c_1 = c_2$

b′ = 1 if $c_1 \neq c_2$

- Why the above attack i… …
  - OTP is deter… …using same key yields the same ciphertext
  - The above … …y cipher whose Enc algorithm is deterministic

Way to bypass the negative result: Statefullness

Thm: If Π is a cipher whose Enc algorithm is a deterministic function of the key and the plain-text then Π cannot have indistinguishable multiple encryptions in the presence of an eavesdropper

Time to Go for Randomization of Encryption

Thank You!