Secure Design

고려대학교 (Korea Univ.)

사이버국방학과 · 정보보호대학원 (CIST)

보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

www.kimlab.net

보안성분석평가연구실

Security Analysis aNd Evaluation Lab

sane.korea.ac.kr / www.kimlab.net

Seungjoo Kim
PROFESSOR, KOREA UNIVERSITY
CNN
North Korean government website hacked
Source CNN

연구분야

- Security Engineering
- Recent Security Threat Analysis and Security Evaluation (e.g. CMVP, CC, ISMS)
- All Areas of Security, from Crypto to Hacking, and Policy

김승주 교수 (skim71@korea.ac.kr)

로봇융합관 306호

주요 경력 :

1990.3~1999.2) 성균관대학교 공학 학사 · 석사 · 박사
1998.12~2004.2) KISA 암호기술팀장 및 CC평가1팀장
2004.3~2011.2) 성균관대학교 정보통신공학부 조교수, 부교수
2011.3~현재) 고려대학교 사이버국방학과·정보보호대학원 정교수
Founder / Advisory Director of SECUINSIDE

前) 선관위 디도스 특별검사팀 자문위원
前) SBS 드라마 '유령' 및 영화 '베를린' 자문

現) 한국정보보호학회 이사
現) 대검찰청 디지털수사 자문위원
現) 방송통신위원회 정보통신망침해사고 민관합동조사단 위원
現) 육군사관학교 초빙교수

- '96: Convertible group signatures (AsiaCrypt)
- '97: Proxy signatures, revisited (ICICS): 600회이상 인용
- '06: 국가정보원 암호학술논문공모전 우수상
- '07: 국가정보원장 국가사이버안전업무 유공자 표창
- '12: 고려대학교 석탑강의상
- '13: Smart TV Security (CanSecWest 및 Black Hat): 스마트TV 해킹(도청·도촬) 및 해적방송 송출 시연

주요 연구성과

동아일보
(2011.12.5.)

중앙일보
(2007.7.5.)

중앙일보
(2006.11.9.)

'숫자 6개' 암호는 2초 - '영어+숫자' 는 10초면 해킹

뻥뻥 뚫리는 토종 메신저

성균관대 연구팀 분석
'MSN보다 보안 떨어져'

Messenger
메신저 패스워드 파악에 걸리는 시간

인터넷서 나도는 해킹프로그램만 있으면

증권 '사이버 거래망' 뚫는다

인터넷
증권사 홈트레이딩시스템(HTS)의 개인 정보가 유출되는 과정
해커
사이버 거래 이용자

어떤 증권사의 HTS가 해킹에 취약한가

28개 증권사 중 11곳
ID·비밀번호 등 유출

'거울'앱 속에 당신의 정보 몰래 보는 '눈'이 있다

"일부 안드로이드폰 기본앱 보안결함"

뉴스데스크
심층취재
스마트TV
안방을 엿본다

MBC 뉴스데스크
(2013.5.10.)

Cryptography & Secure Design

Cryptography & Secure Design

- Cryptography has a **firmer** theoretical foundation than other security techniques.
  - So if you study this, you will be able to have an insight to design and analyze other security systems more systematically.

Emphases of Modern Cryptography

- **Modern** cryptography, which is distinguished from classical cryptography by
  - Its emphasis on ( ),
    - If you don't know what it is you are trying to achieve, how can you hope to know when you have achieved it?
  - Precise ( ), and
    - Many cryptographic constructions cannot currently be proven secure in an unconditional sense. Security often relies, instead, on some widely-believed (albeit unproven) assumption. The modern cryptographic approach dictates that any such assumptions must be clearly and unambiguously defined.
  - ( ) of security.
    - This is the essence of modern cryptography, and was responsible for the transformation of cryptography from an art to a science.

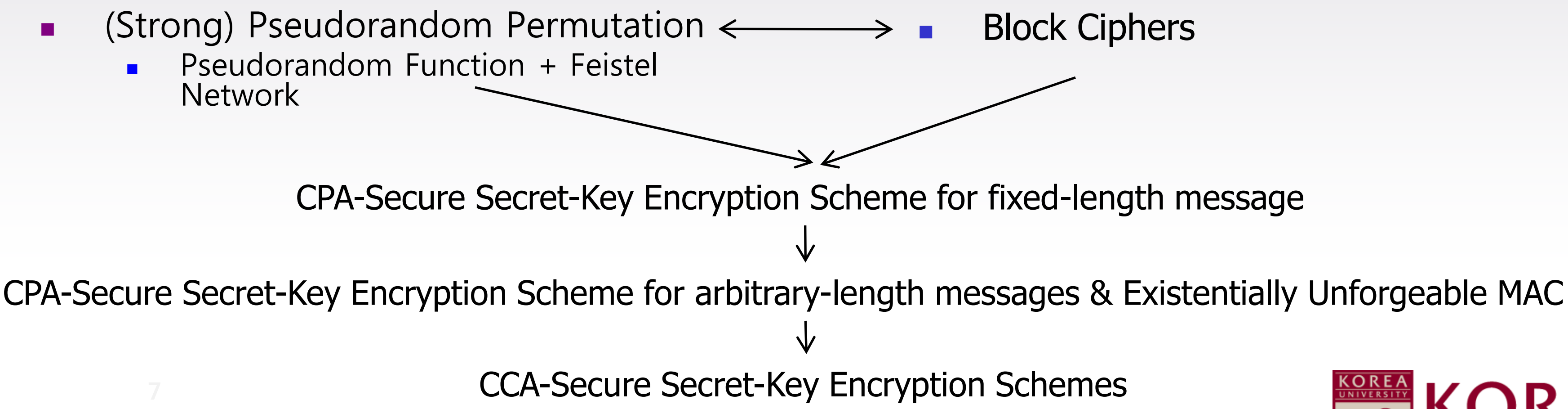
Symmetric Ciphers

The World of Symmetric Ciphers

Theoretical Construction

Practical Construction

- RSA, Discrete Log, Factoring …
- One-Way Function (or One-Way Permutation)
- Hard-Core Predicate
- Pseudorandom Generator with +1 Expansion
- Pseudorandom Generator with Arbitrary Expansion
- Pseudorandom Function



- (Strong) Pseudorandom Permutation ⟷ Block Ciphers
  - Pseudorandom Function + Feistel Network

CPA-Secure Secret-Key Encryption Scheme for fixed-length message

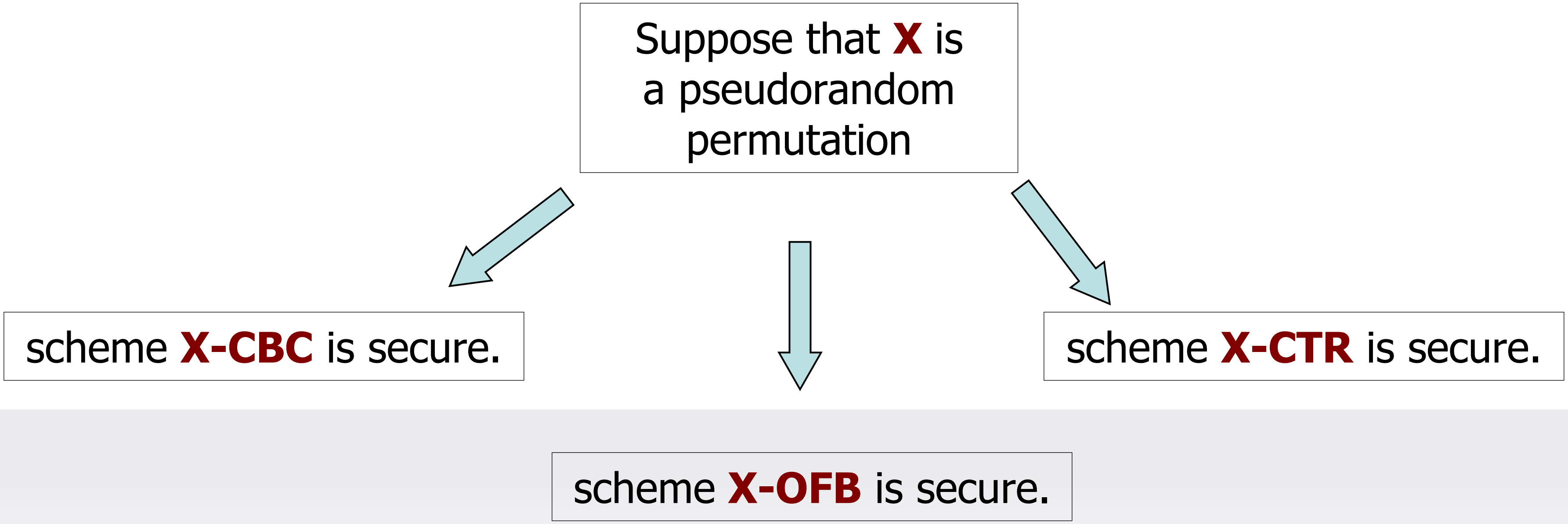
↓

CPA-Secure Secret-Key Encryption Scheme for arbitrary-length messages & Existentially Unforgeable MAC

↓

CCA-Secure Secret-Key Encryption Schemes

Modes of Operation



Suppose that **X** is a pseudorandom permutation

scheme **X-CBC** is secure.

scheme **X-OFB** is secure.

scheme **X-CTR** is secure.

Of course, to get any information about practical relevance of these results one needs to look at the concrete parameters hidden in the “asymptotics”.

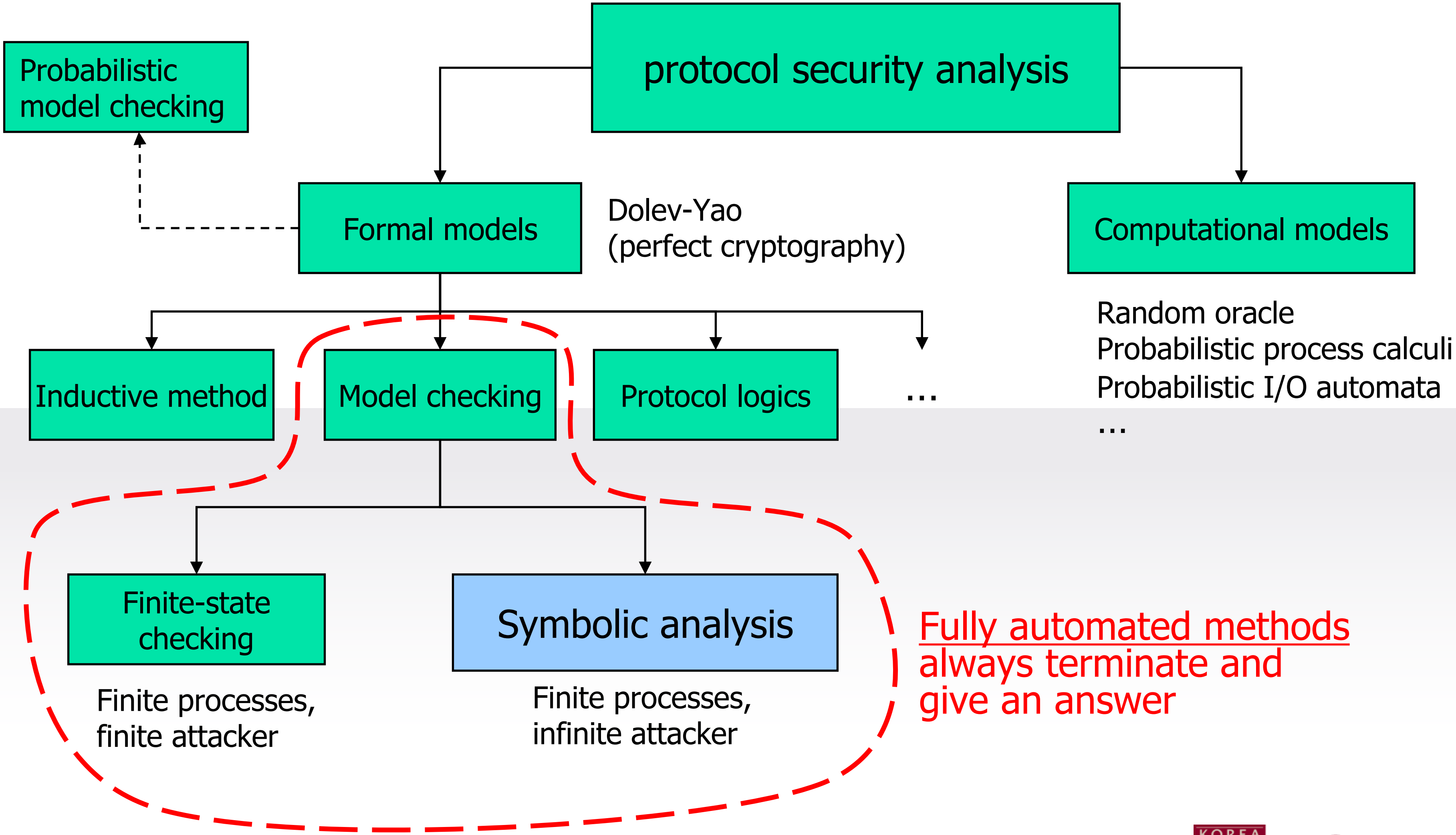
Asymmetric Ciphers

Ideal Properties of a Proof

- The challenge(target) for the adversary should be as (   ) as possible
- The adversary should be as (   ) as possible
- The assumptions should be as (   ) as possible
- Quality of security reduction should be as (   ) as possible

※ Cited from B.Kaliski and J.Jonsson(@ RSA Lab)'s Presentation Material

Protocol Analysis Techniques



Dolev-Yao
(perfect cryptography)

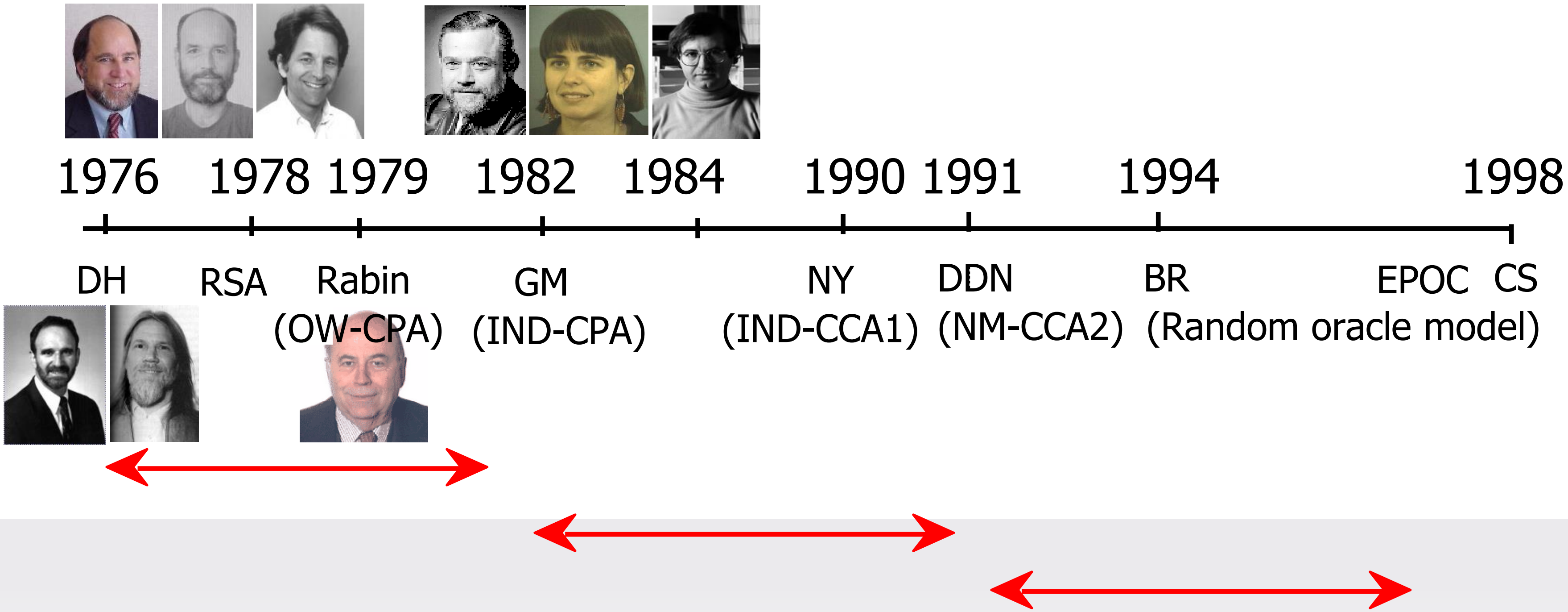
Random oracle
Probabilistic process calculi
Probabilistic I/O automata
...

Finite processes,
finite attacker

Finite processes,
infinite attacker

Fully automated methods
always terminate and
give an answer

Brief History of Provable Security



1976 1978 1979 1982 1984 1990 1991 1994 1998

DH

RSA

Rabin (OW-CPA)

GM (IND-CPA)

NY (IND-CCA1)

DDN (NM-CCA2)

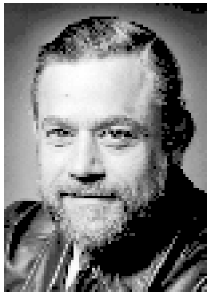
BR (Random oracle model)

EPOC CS

※ Cited from Dr. T.Okamoto's Presentation Material in KISA

Brief History of Provable Security

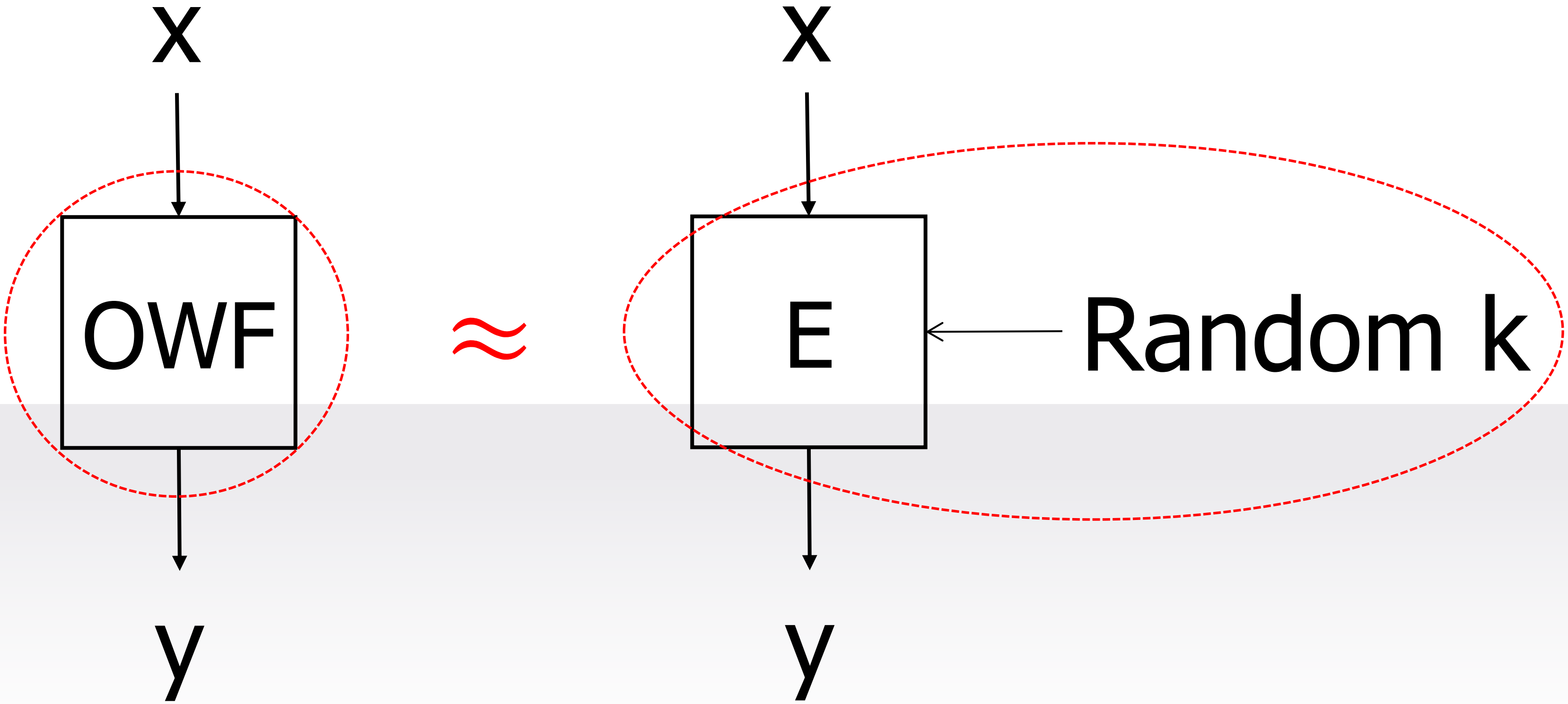
- Blum, Goldwasser & Micali (1982~1988) : Mathematical definitions of security



  - Encryption [Goldwasser, Micali 86]
  - Signatures [Goldwasser, Micali, Rivest 88]

- Now a common requirement to support emerging standards (IEEE P1363, ISO, Cryptrec, NESSIE).

Design Secure Asymmetric Cipher



One-Way Function

❑ **One-Way Function :** A function

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

is called "**one-way** " if there is an efficient algorithm that on input x outputs f(x), whereas **any feasible algorithm** that tries to find a **preimage** of f(x) under f may succeed only with negligible probability.

- **Any Feasible Algorithm :**
  - HW : DTM / NDTM / PTM
  - SW : COA / KPA / CPA / CCA

- **Preimage :**
  - Whole / Partial / Correlated

One-Way Function

- **Preimage (Goal)**
  - **One-Way (OW)** : Hard to invert the encryption function
  - **Semantically Secure (IND)** : Hard to obtain any partial information of a plaintext from the ciphertext
  - **Non-Malleability (NM)** : For any non-trivial relation R, E(M) –> E(R(M)) is hard

One-Way Function

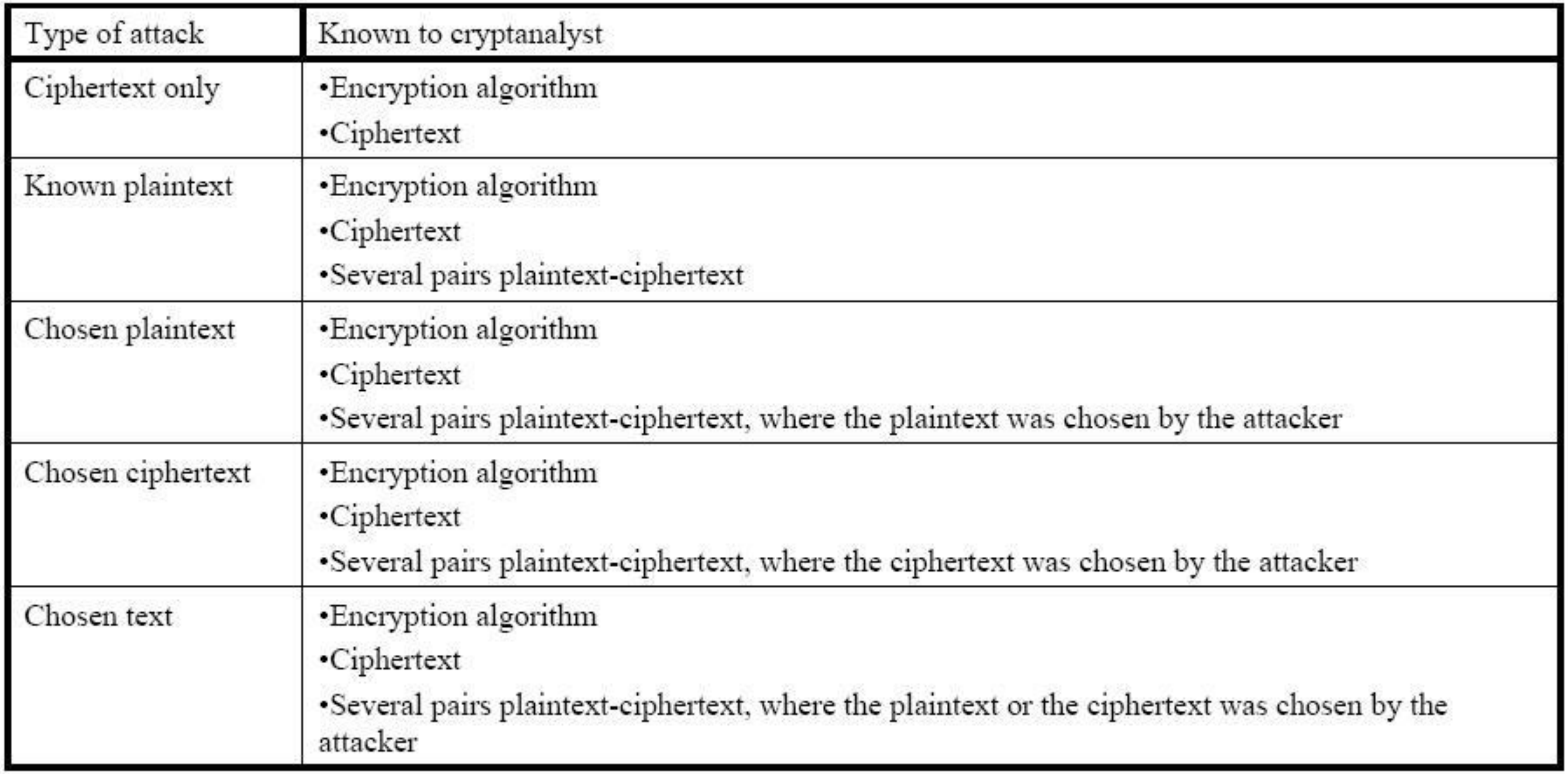
- **Algorithm (HW Attack Method)**
  - FA (Finite Automata)
  - PDA (Pushdown Automata)
  - TM (Turing Machine)
  - PTM (Probabilistic TM)
  - von Neumann Machine

One-Way Function

- **Algorithm (SW Attack Method)**
  - **Passive Attack (CPA)**
    - Ciphertext Only Attack (COA)
    - Chosen Plaintext Attack (CPA)
  - **Active Attack (CCA)**
    - Chosen Ciphertext Attack (CCA)
    - **1990)** Static Chosen-Ciphertext Attack (Lunch time attack, Naor & Yung)
    - **1991)** Adaptive Chosen-Ciphertext Attack (Rackoff & Simon)

One-Way Function

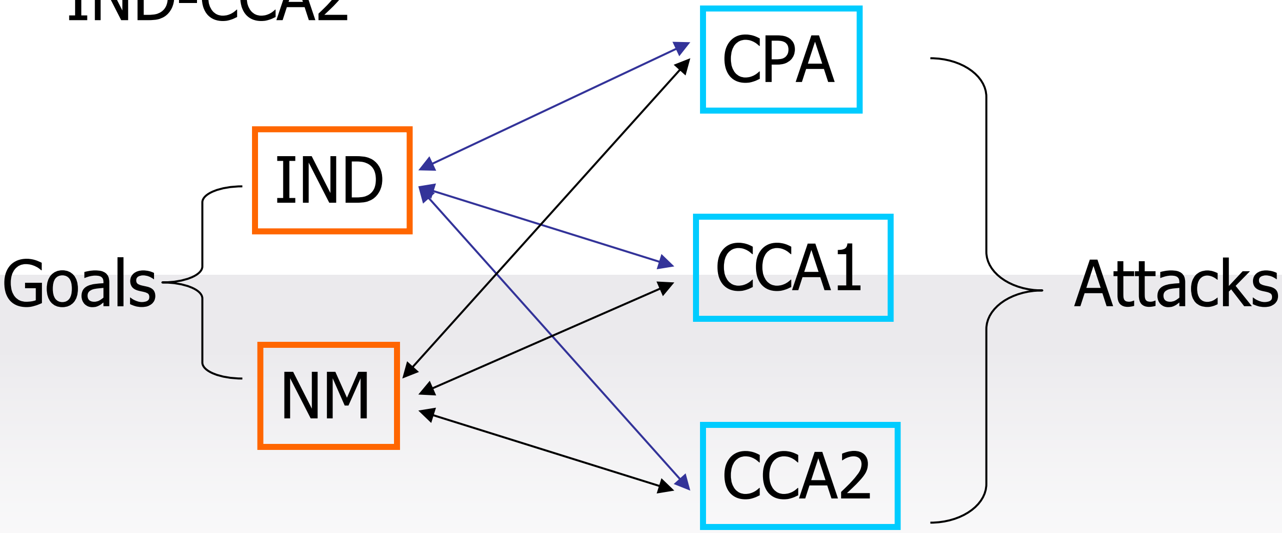
- **Algorithm (SW Attack Method)**



Type of attack	Known to cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext
Known plaintext	•Encryption algorithm •Ciphertext •Several pairs plaintext-ciphertext
Chosen plaintext	•Encryption algorithm •Ciphertext •Several pairs plaintext-ciphertext, where the plaintext was chosen by the attacker
Chosen ciphertext	•Encryption algorithm •Ciphertext •Several pairs plaintext-ciphertext, where the ciphertext was chosen by the attacker
Chosen text	•Encryption algorithm •Ciphertext •Several pairs plaintext-ciphertext, where the plaintext or the ciphertext was chosen by the attacker

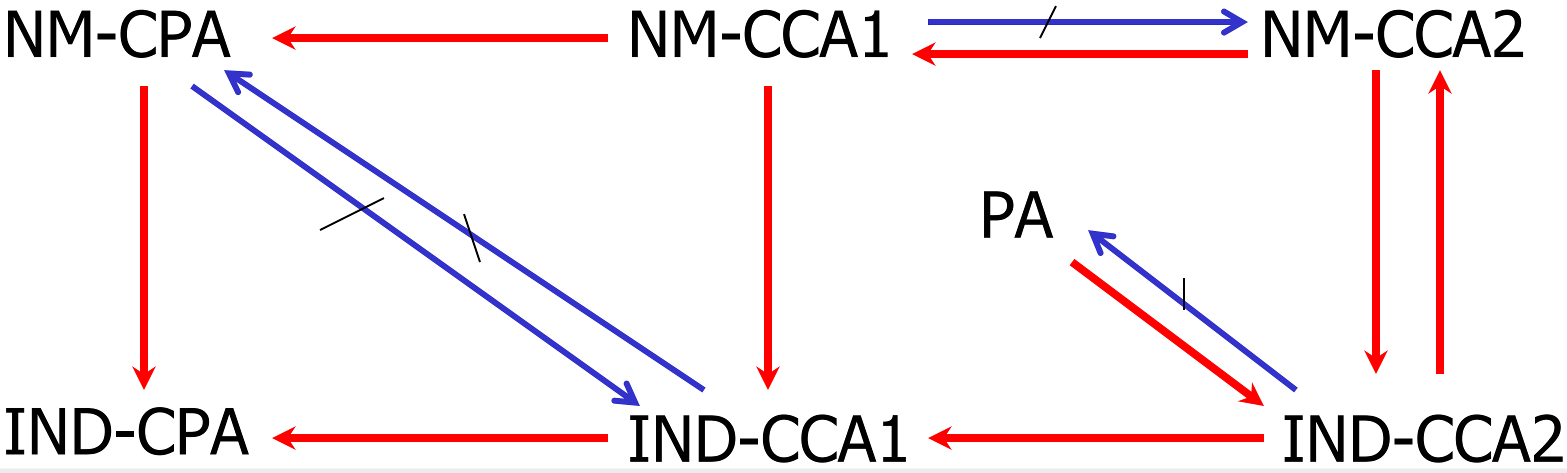
6 Notions of Security

IND-CPA
IND-CCA1
IND-CCA2



NM-CPA
NM-CCA1
NM-CCA2

Relations



NM-CPA

NM-CCA1

NM-CCA2

PA

IND-CPA

IND-CCA1

IND-CCA2

A $\rightarrow$ B: proven that meeting notion A implies meeting B

A $\not\rightarrow$ B: proven that meeting notion A implies **not** meeting B

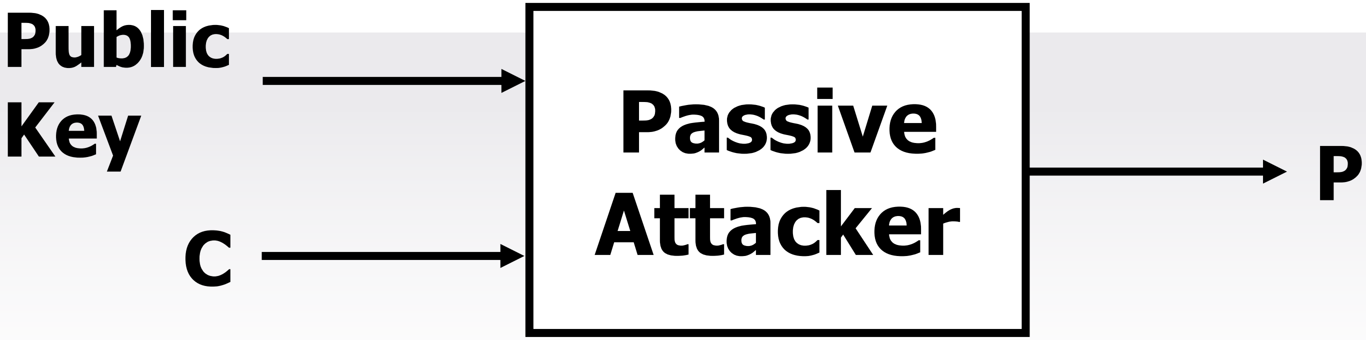
NOTE: A implies B iff there is a path from A to B

One-Wayness (OW-CPA)

Security Goal : One-wayness

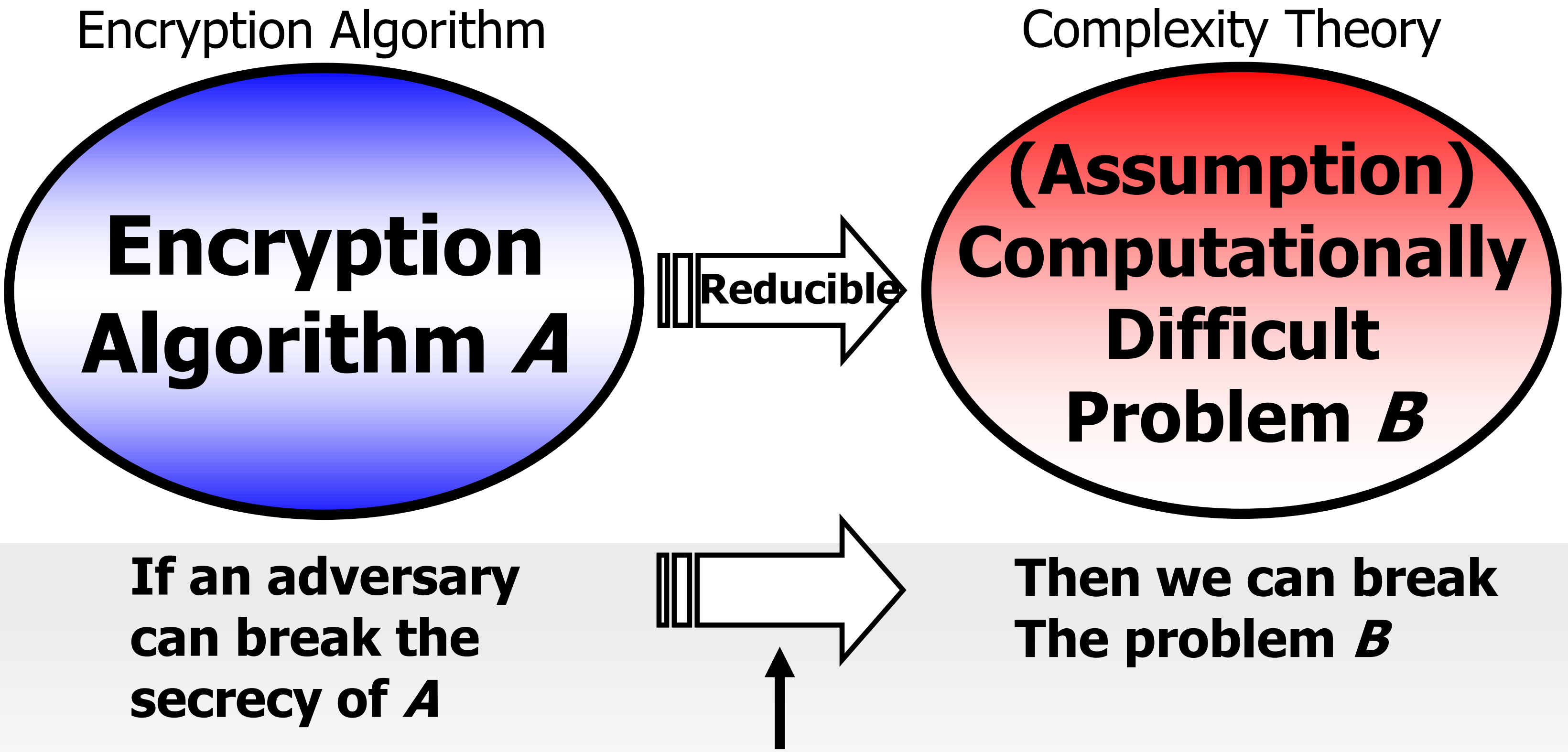
- Easy to compute ciphertext from plaintext but hard to invert.

Attacker Model :



Security Proof : Relative complexity by reduction

One-Wayness (OW-CPA)



Encryption Algorithm

Complexity Theory

Encryption Algorithm *A*

Reducible

(Assumption) Computationally Difficult Problem *B*

If an adversary can break the secrecy of *A*

Then we can break The problem *B*

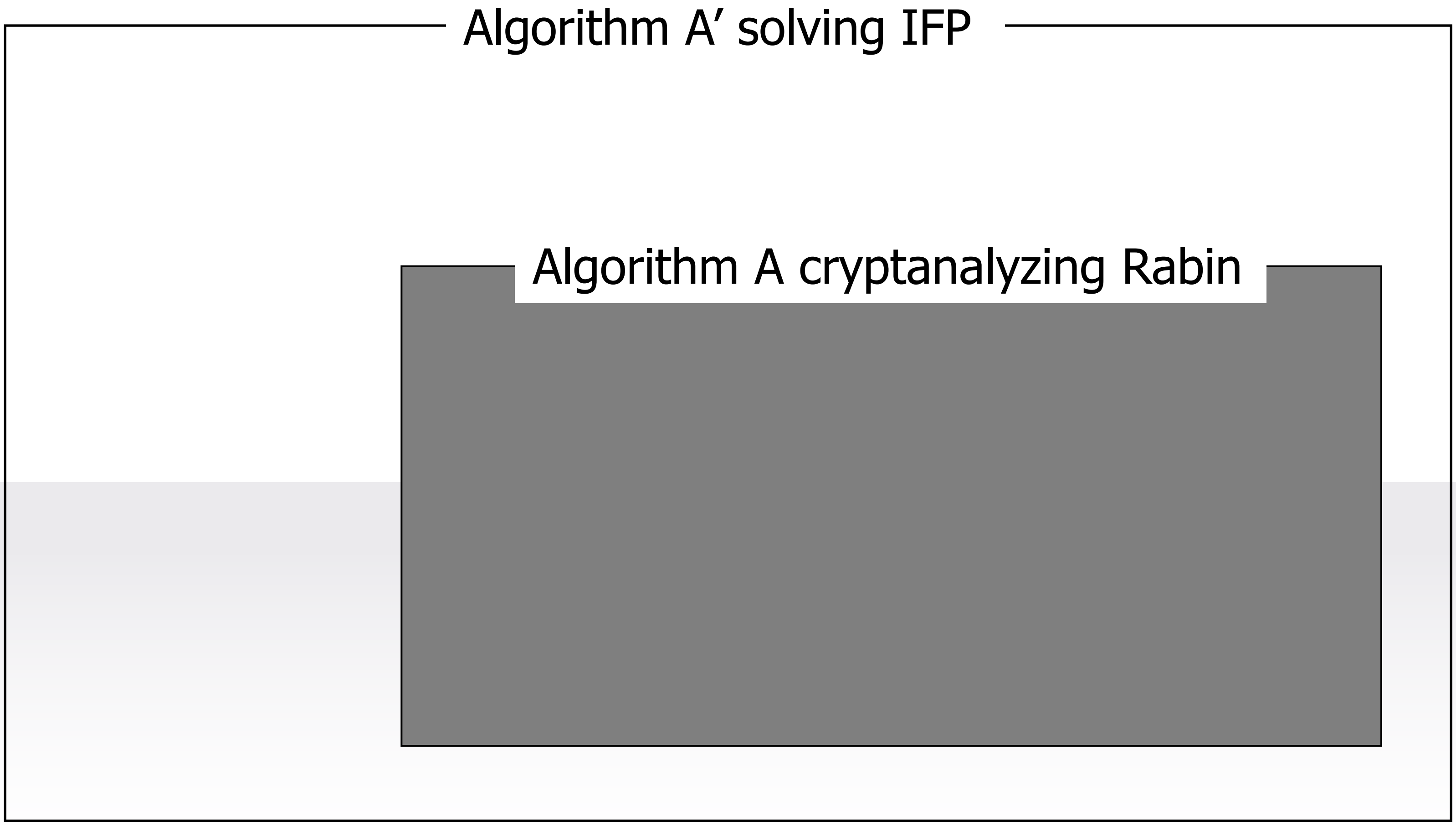
Contradicting Assumption

※ ***Partial information problem*** **:** Leak partial information if the plaintext comes from small plaintext space!

OW-CPA Example : Rabin Scheme

- **Private Key :** $p = q = 3 \pmod 4$
- **Public Key :** $n = pq$
- **Encryption :** $C = M^2 \pmod n$
- **Decryption :**
  - $m_1 = C^{(p+1)/4} \pmod p$, $m_2 = (p - C^{(p+1)/4}) \pmod p$, $m_3 = C^{(q+1)/4} \pmod q$, $m4 = (q - C^{(q+1)/4}) \pmod p$.
  - $a = q(q^{-1} \bmod p)$, $p = p(p^{-1} \bmod q)$.
  - $M_1 = (am_1+bm_3) \bmod n$, $M_2 = (am_1+bm_4) \bmod n$, $M_3 = (am_2+bm_3) \bmod n$, $M_4 = (am_2+bm_4) \bmod n$.
  - M is one of $\{M_1, M_2, M_3, M_4\}$

Proof Sketch of Rabin Scheme



Algorithm A’ solving IFP

Algorithm A cryptanalyzing Rabin

Let A be an adversary that breaks the Rabin scheme. Then A can be used to solve IFP. If so, we say solving IFP reduces to breaking the Rabin scheme.

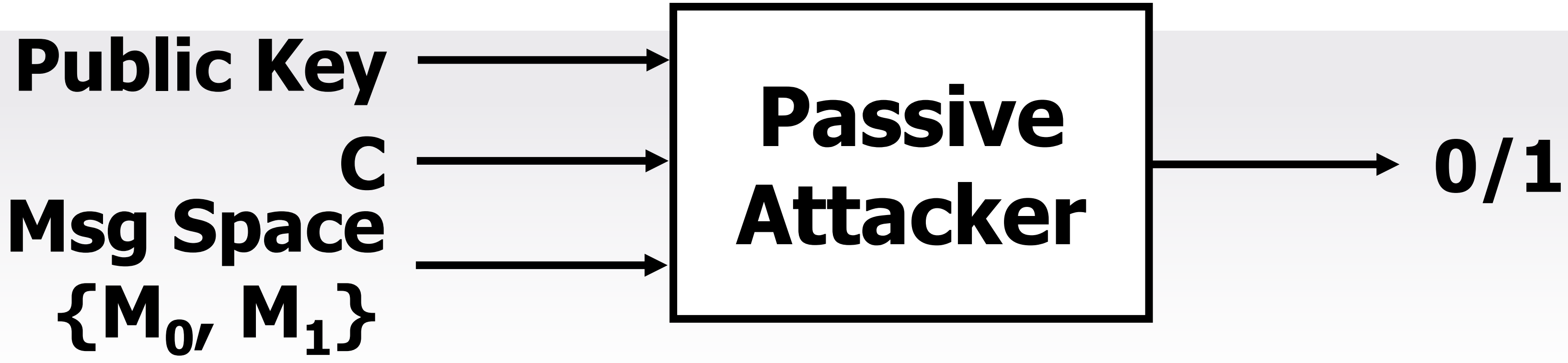
–> Conclusion: If IFP untractable then Rabin scheme is unbreakable!

Polynomial Security (IND-CPA)

Security Goal : Polynomial Security

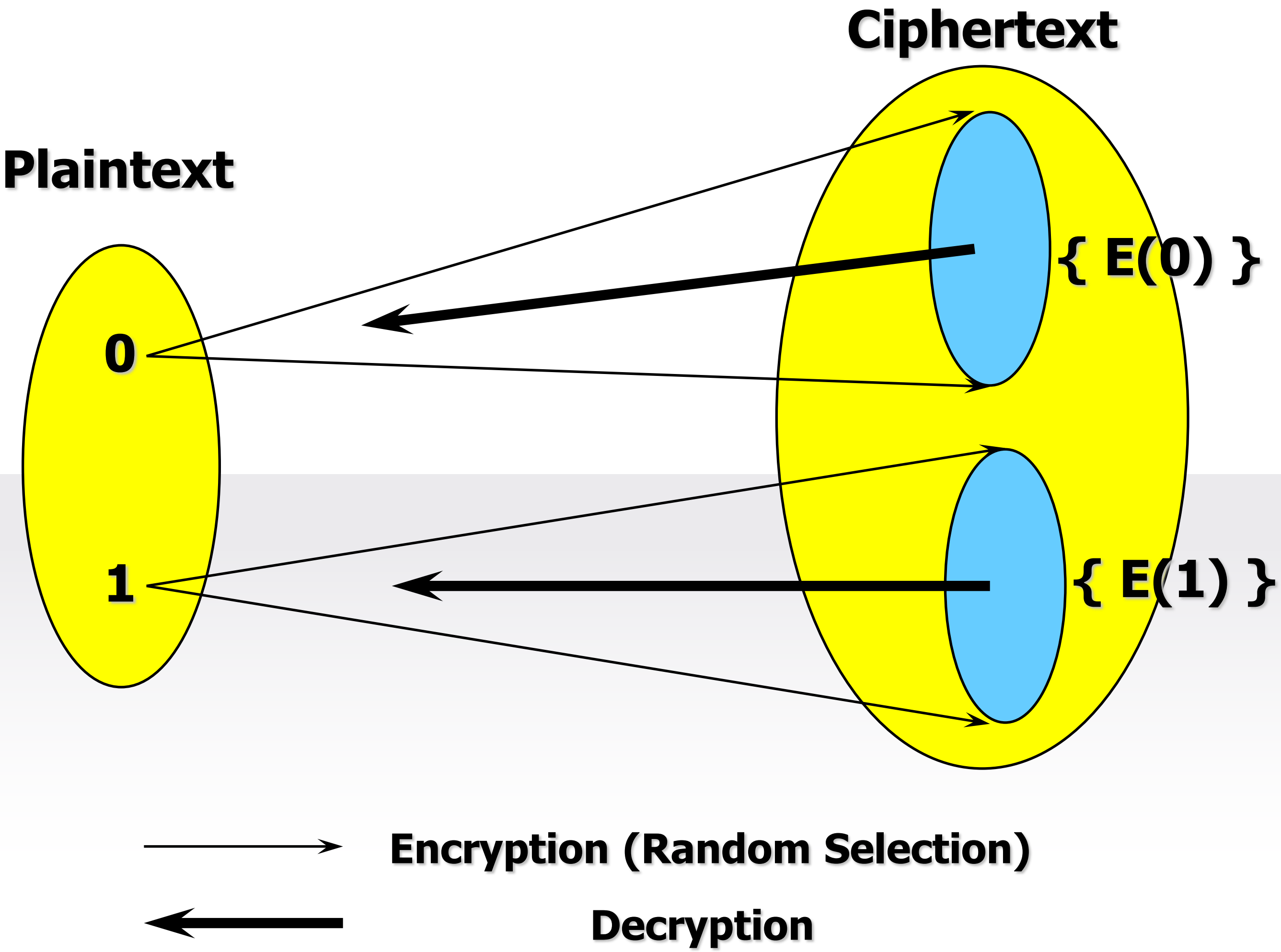
– Cannot distinguish 2 ciphertexts (Indistinguishability)

Attacker Model :



→ **Encryption Alg. :** ***must be probabilistic!***

Probabilistic Encryption



Ciphertext

Plaintext

0

1

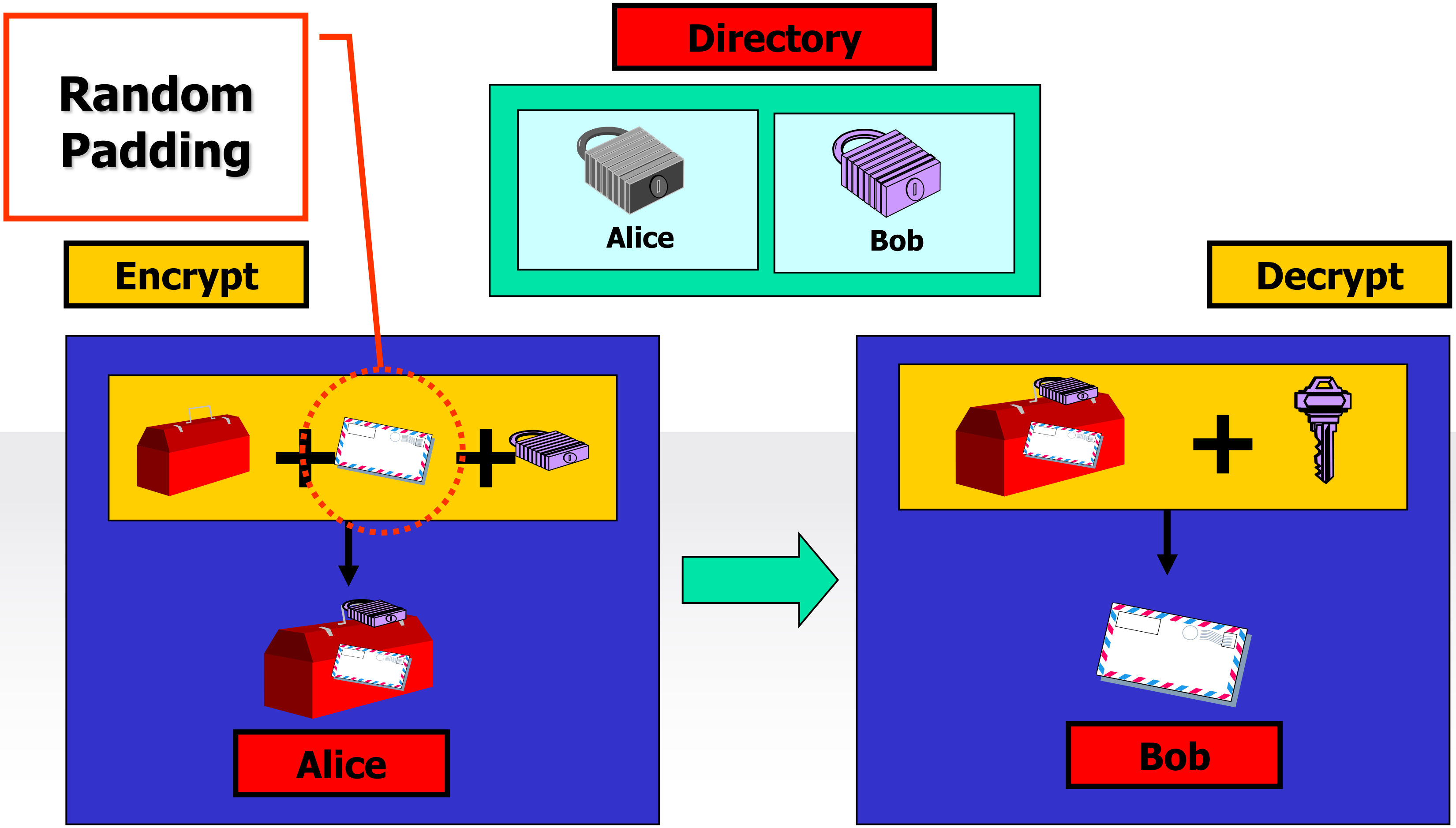
{ E(0) }

{ E(1) }

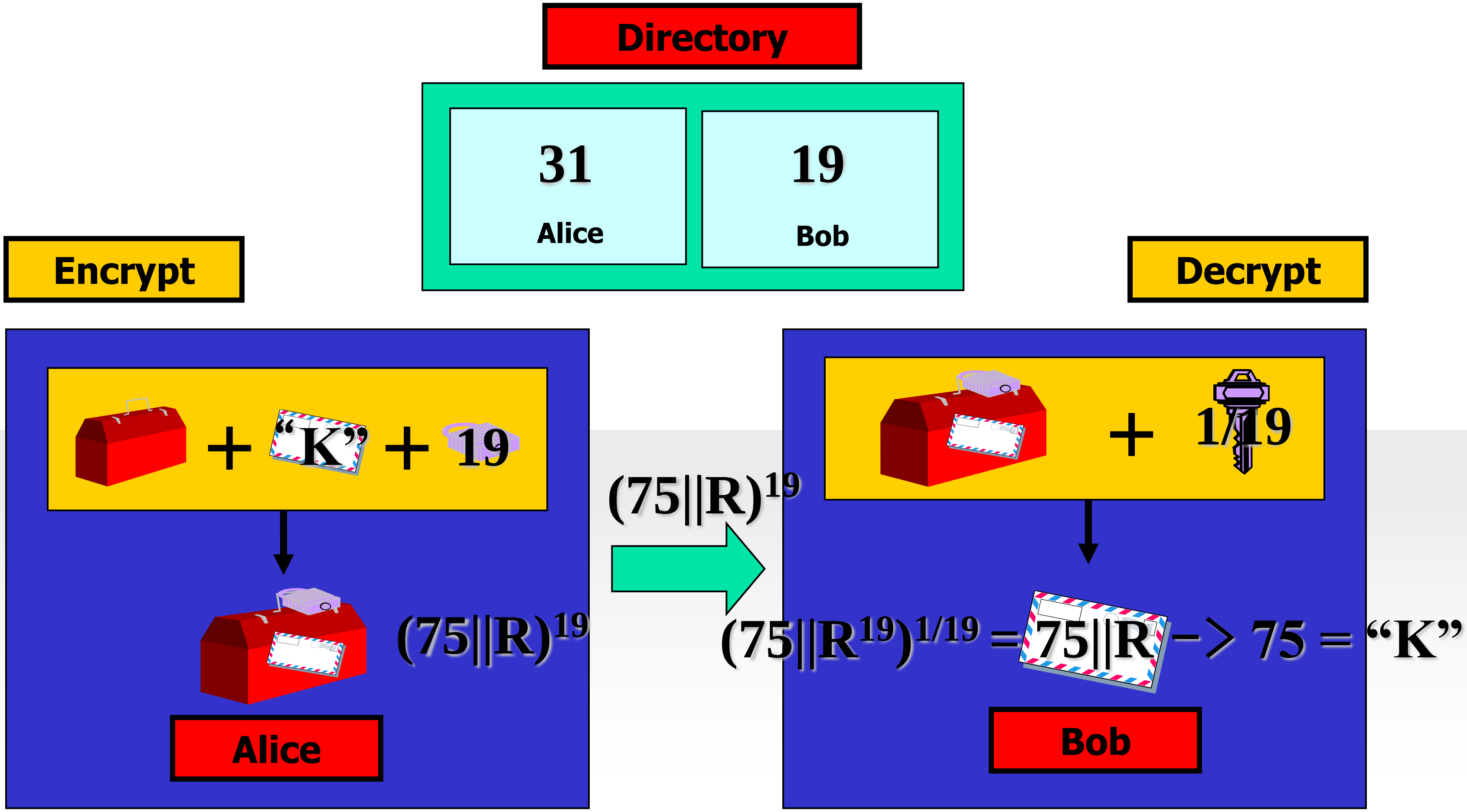
Encryption (Random Selection)

Decryption

Probabilistic Encryption



Probabilistic Encryption



Directory

31 Alice

19 Bob

Encrypt

+ "K" + 19

$(75||R)^{19}$

Alice

Decrypt

+ 1/19

$(75||R)^{19}$

$(75||R^{19})^{1/19} = 75||R \rightarrow 75 = $ "K"

Bob

Semantic Security

- Semantic Security (= Polynomial Security) is a (   ) of Shannon's "**perfect secrecy**".

Semantic Security

- Semantic Security (= Polynomial Security) is a (   ) of Shannon's "perfect secrecy".

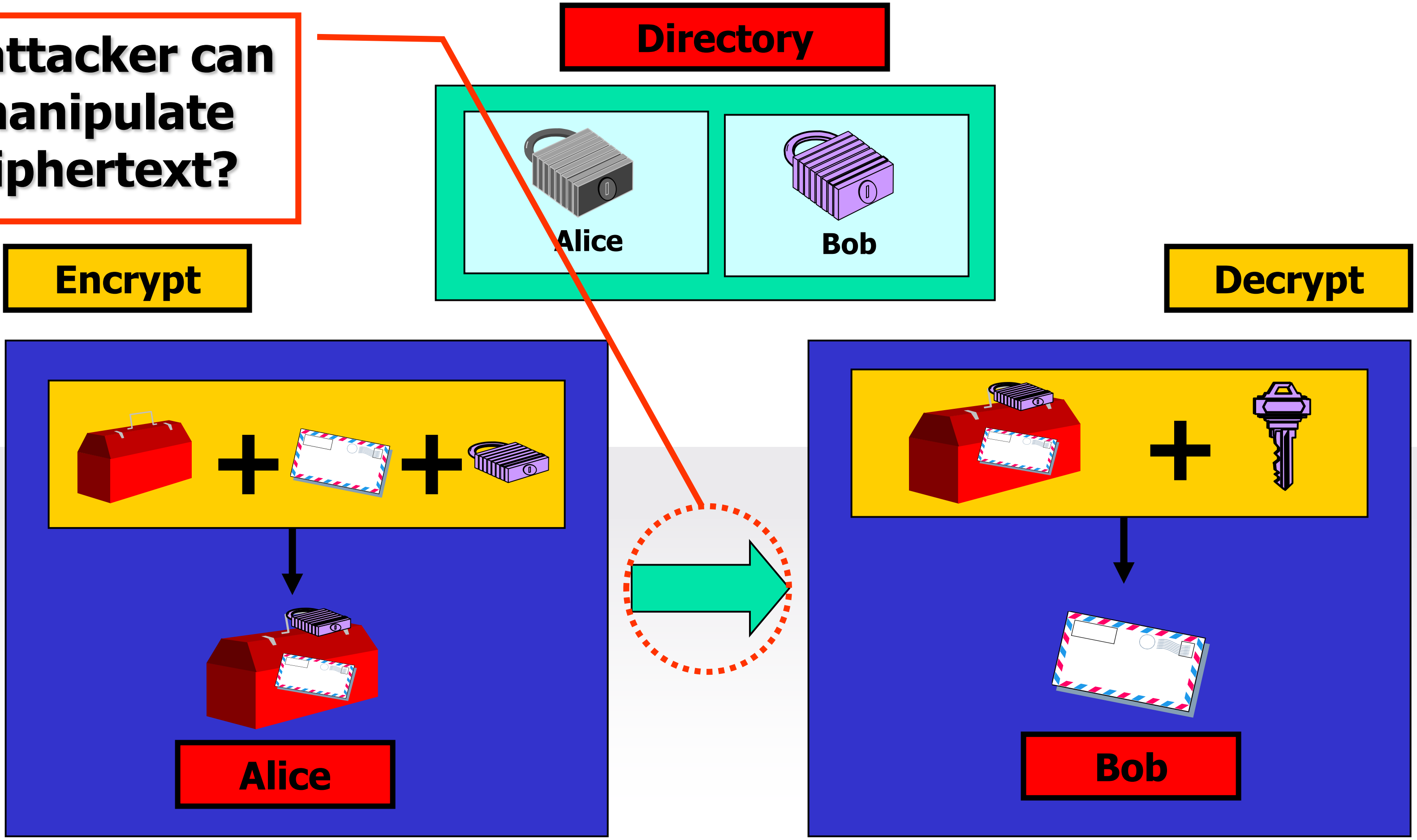
How to define this goal formally?

How to Make Semantic Secure Cipher?

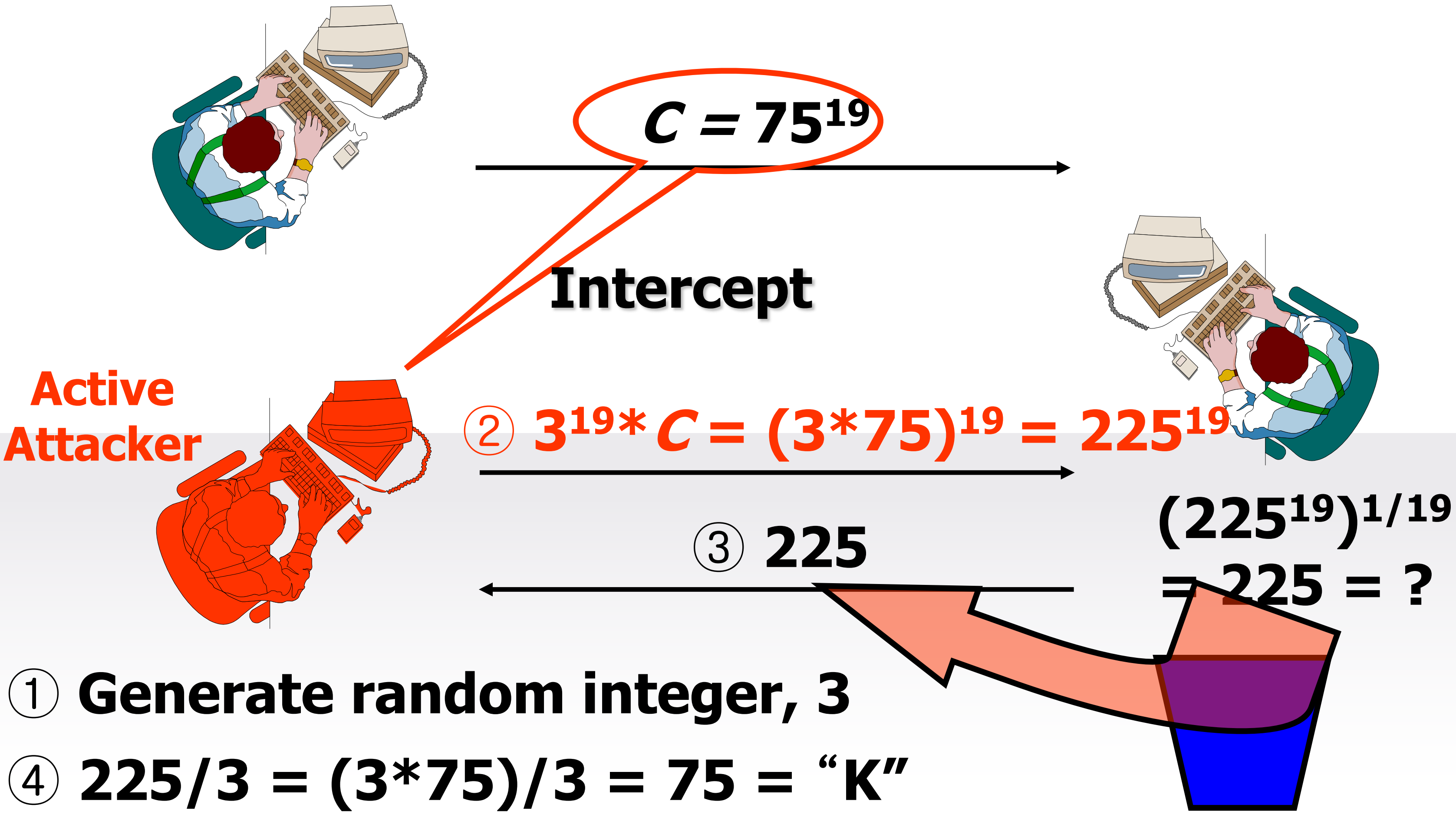
How to make it?

Chosen Ciphertext Attack

If attacker can manipulate Ciphertext?



Chosen Ciphertext Attack



$C = 75^{19}$

Intercept

Active Attacker

② $3^{19} * C = (3*75)^{19} = 225^{19}$

③ 225

$(225^{19})^{1/19}$

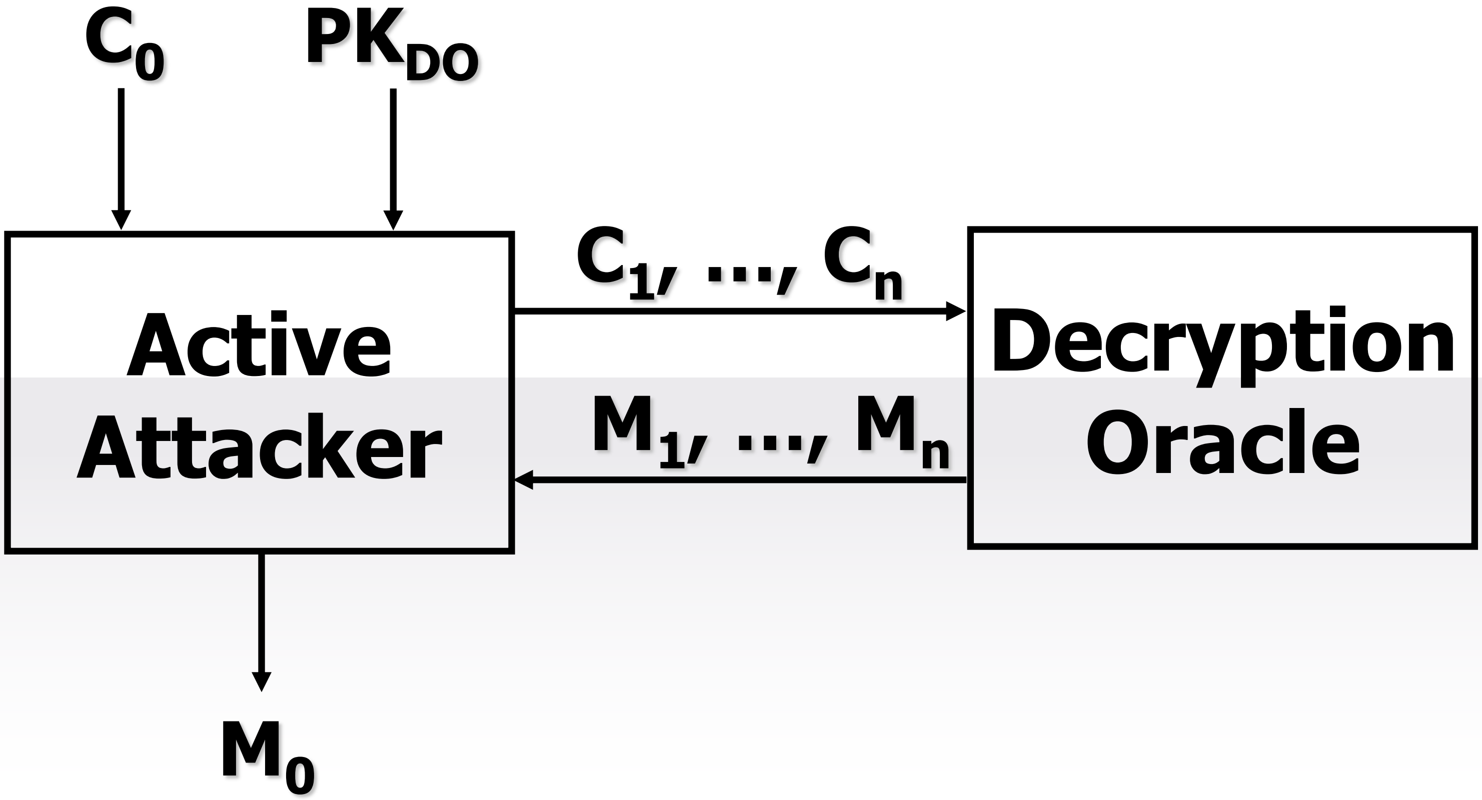
$= 225 = ?$

① Generate random integer, 3

④ 225/3 = (3*75)/3 = 75 = “K”

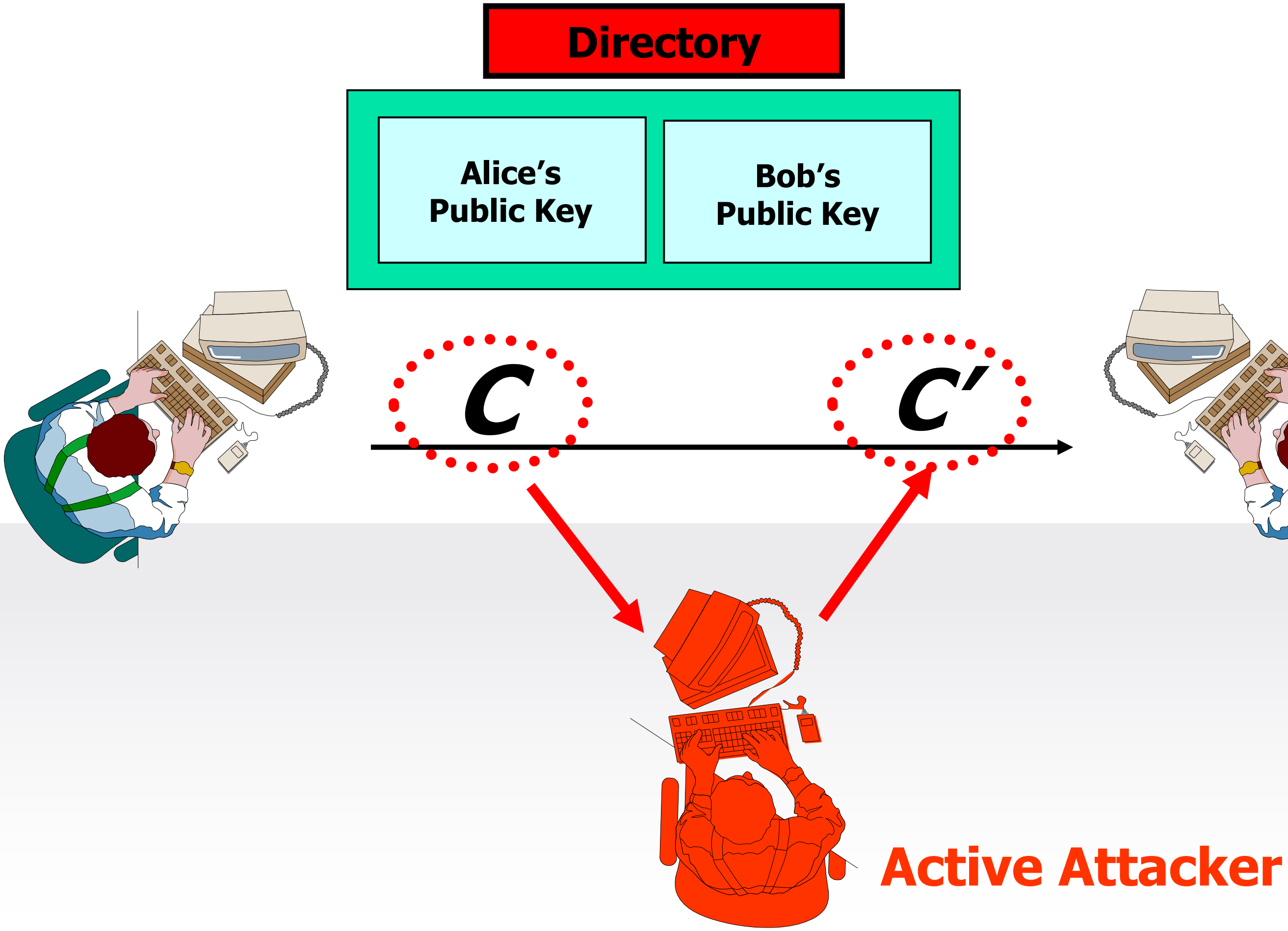
Chosen Ciphertext Attack

- After queries to *DO*
- Before queries to *DO*



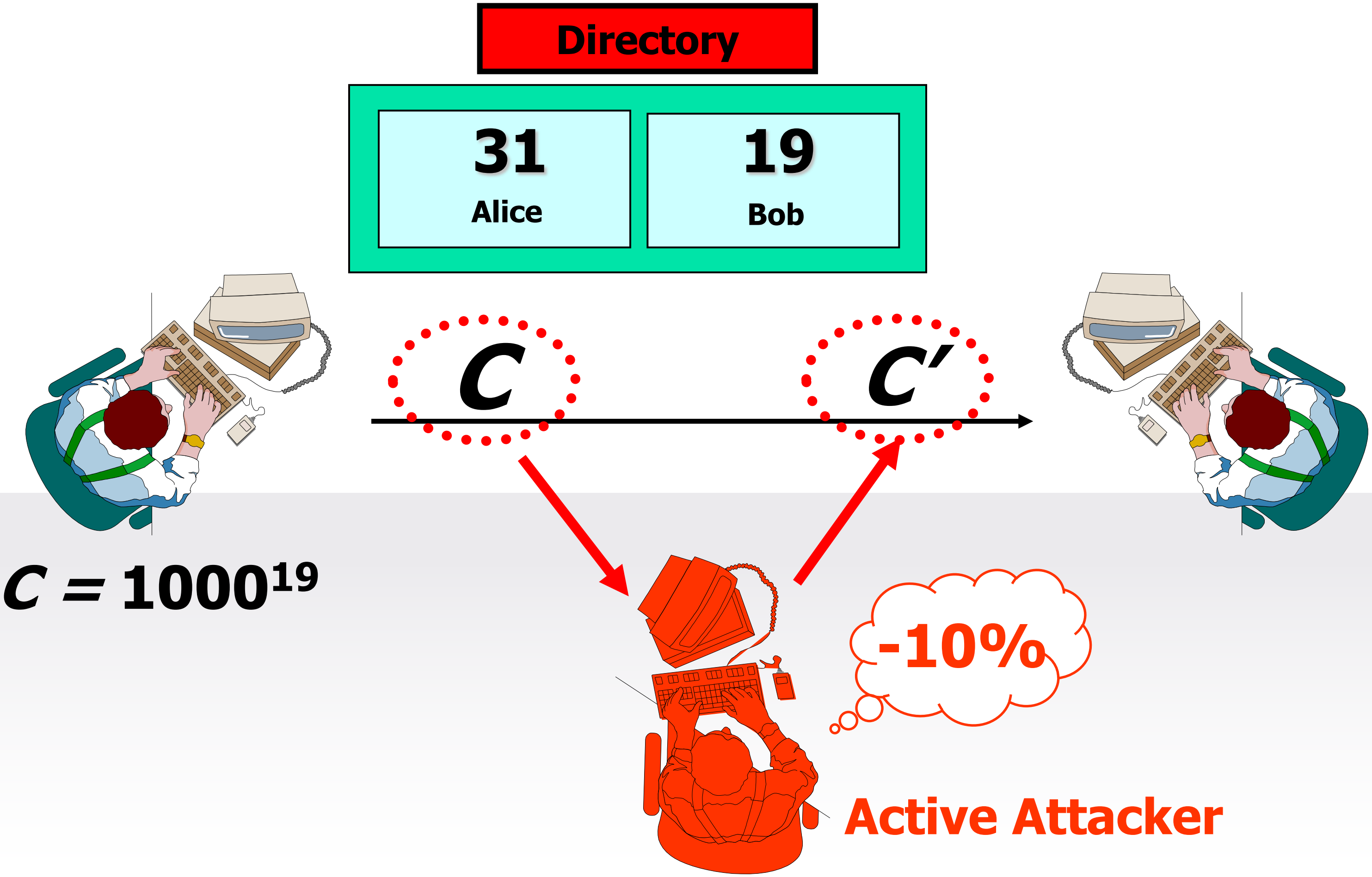
※ RULE : $C_0 \neq C_1, \dots\dots, C_n$

Non-Malleability



m' is unknown, but related in some known way to m

Non-Malleability



Directory

31 Alice

19 Bob

C

C'

-10%

Active Attacker

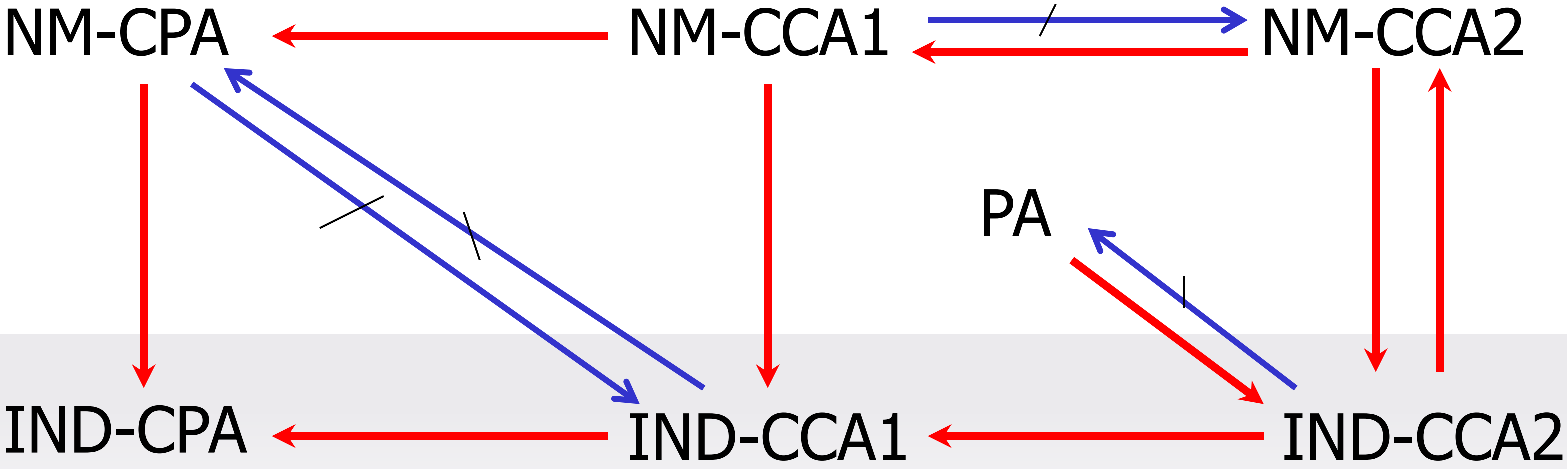
① $C = 1000^{19}$

② $C' = C * (0.9)^{19} = (1000 * 0.9)^{19} = 900^{19}$

How to Make Non-Malleable Cipher?

How to make it?

How to Make Non-Malleable Cipher?



NM-CPA

NM-CCA1

NM-CCA2

PA

IND-CPA

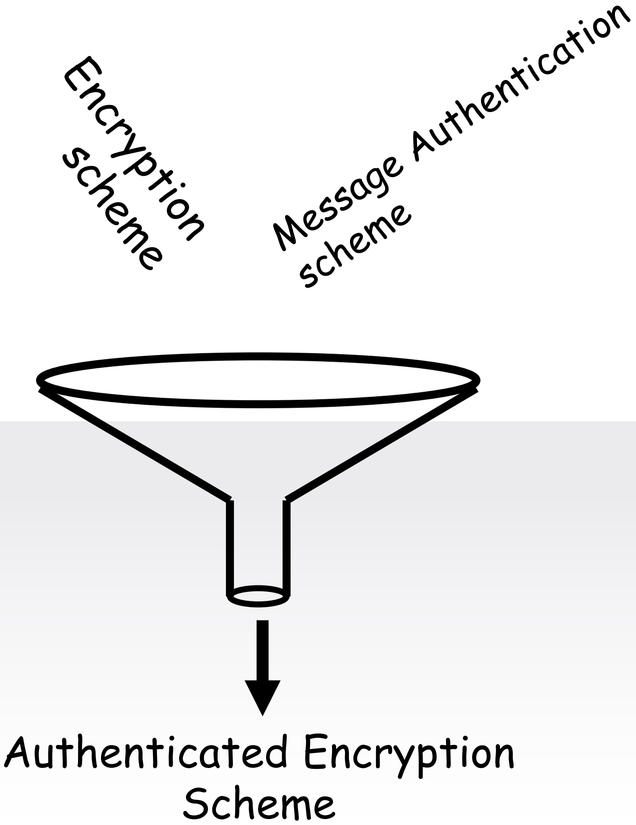
IND-CCA1

IND-CCA2

How to Make Non-Malleable Cipher?

- Authenticated Encryption
- Plaintext Awareness

Authenticated Encryption



Encryption scheme

Message Authentication scheme

Authenticated Encryption Scheme

Relevance to Internet Security

- Many popular Internet protocols rely on authenticated encryption schemes for privacy and authenticity.
  - Examples: SSL, TLS, SSH, IPSEC, …

- Many applications on the Internet require both privacy and authenticity.
  - Examples: online banking, online retail, online auctions, instant messaging, remote login, secure file transfer, …

Generic Composition Methods

- **Encrypt-and-MAC**
  - $\bar{E}_{Ke,Km}(M) = E_{Ke}(M) \,||\, T_{Km}(M)$
- **MAC-then-Encrypt**
  - $\bar{E}_{Ke,Km}(M) = E_{Ke}(M \,||\, T_{Km}(M))$
- **Encrypt-then-MAC**
  - $\bar{E}_{Ke,Km} = E_{Ke}(M) \,||\, T_{Km}(E_{Ke}(M))$

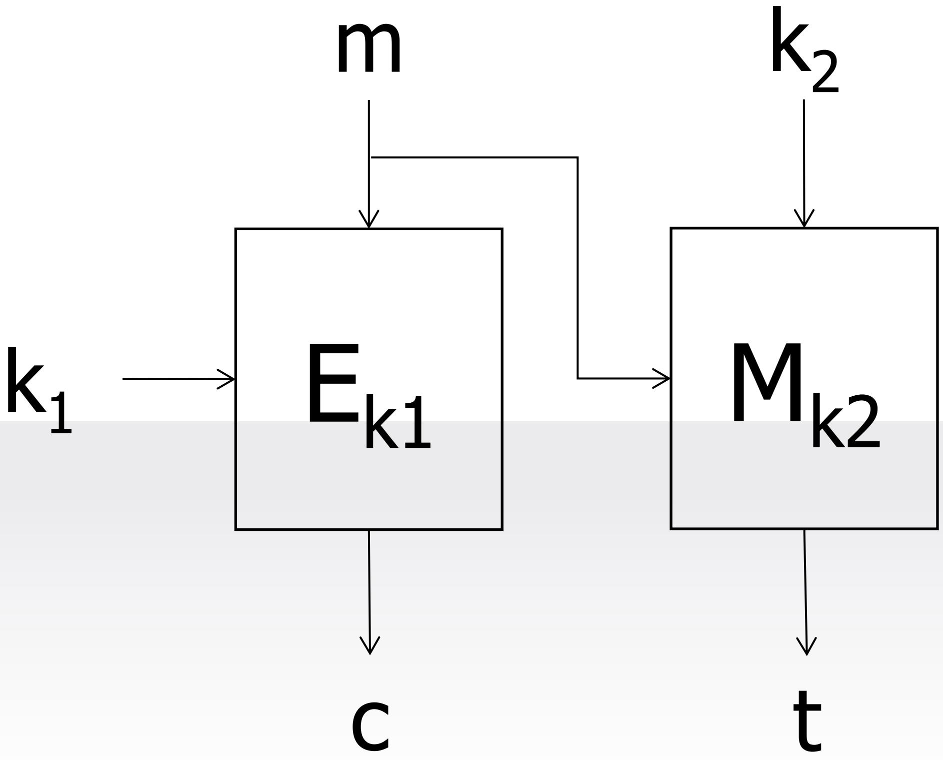
Generic Composition Results

- **Question:**
  - Assuming the base encryption scheme is secure (IND-CPA) and the base MAC scheme is secure (UF-CMA),
  - is the composed scheme CCA-secure?

Generic Composition Results

Composition Method	Security
1) Encrypt-and-MAC $E_{Ke,Km}(M) = E_{Ke}(M)\|\|T_{Km}(M)$	
2) MAC-then-Encrypt $E_{Ke,Km}(M) = E_{Ke}(M\|\|T_{Km}(M))$	
3) Encrypt-then-MAC $E_{Ke,Km}(M) = E_{Ke}(M)\|\|T_{Km}(E_{Ke}(M))$	

Encrypt-then-MAC



Plaintext Awarenes

- PA is merely a (   ) rather than a (   ).
- A scheme with IND-CPA security is plaintext aware (PA) if an adversary cannot produce a valid ciphertext without knowing the corresponding plaintext.
  - The adversary has access to an encryption oracle and random oracles but no decryption oracle.
- PA implies IND-CCA2 security.
  - Decryption queries give no information since the adversary already "knows" the plaintext.

※ Cited from B.Kaliski and J.Jonsson(@ RSA Lab)'s Presentation Material

PA & Random Oracle Model

- Sometimes it is helpful to consider models where some tools (primitives) used by cryptographic schemes such as,
  - Hash functions
  - Block ciphers
  - Finite groups

  are considered to be ideal, that is, the adversary can only use (attack) them in a certain way.
- Idealized Security Models:
  - Hash function -> Random oracle
  - Block ciphers -> Ideal cipher
  - Finite groups -> Generic group
- Standard model: no idealized primitives (sort of)

PA & Random Oracle Model

- A paradigm for designing efficient provably secure protocols (M.Bellare and P.Rogaway, 1993)

- In cryptography, a RO is an oracle (a theoretical black box) that responds to every query with a (truly) random response chosen uniformly from its output domain, except that for any specific query, it responds the same way every time it receives that query.

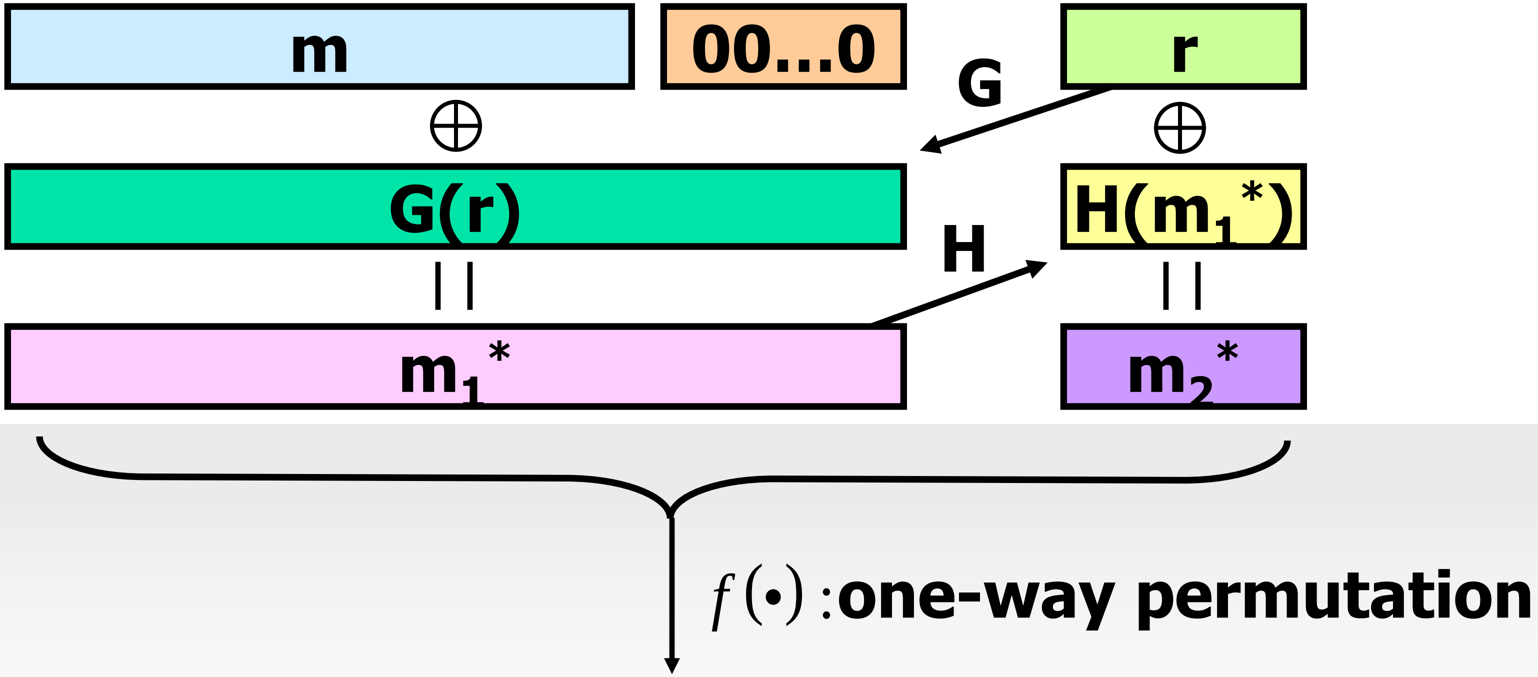
PA & Random Oracle Model

- PA makes sense only in the ROM!
  - The RO is used in the definition of plaintext awareness to give the extractor a "window" into the internal state of the adversary (as revealed through its queries). If the external RO is replaced by an internal algorithm, then this window is closed.
  - In the standard model, the adversary can encrypt a plaintext and then "forget" it.

OAEP

- Optimal Asymmetric Encryption Padding
- The main drawback of the previous scheme is that ciphertexts are longer than a single element of Z_N*, even when short messages are encrypted.
- The encoding function OAEP is designed so that the only way to find an element in the image of OAEP is to choose m and r and then explicitly compute OAEP(m,r).
- OAEP is essentially a (   ).

RSA-OAEP



$f(\cdot)$:**one-way permutation**

$$C = f(OAEP(m,r)) = (m_1^*||m_2^*)^e \bmod N$$

OAEP++

- A new padding scheme OAEP++ was proposed by Jonsson (2002).
  - The one-time pad on the OAEP (xor between random and output of H) is replaced by a strong block cipher (ideal cipher model).

- Ideal Cipher Model
  - Consider block cipher E as a family of perfectly random and independent permutations.

Limits of Provable Security

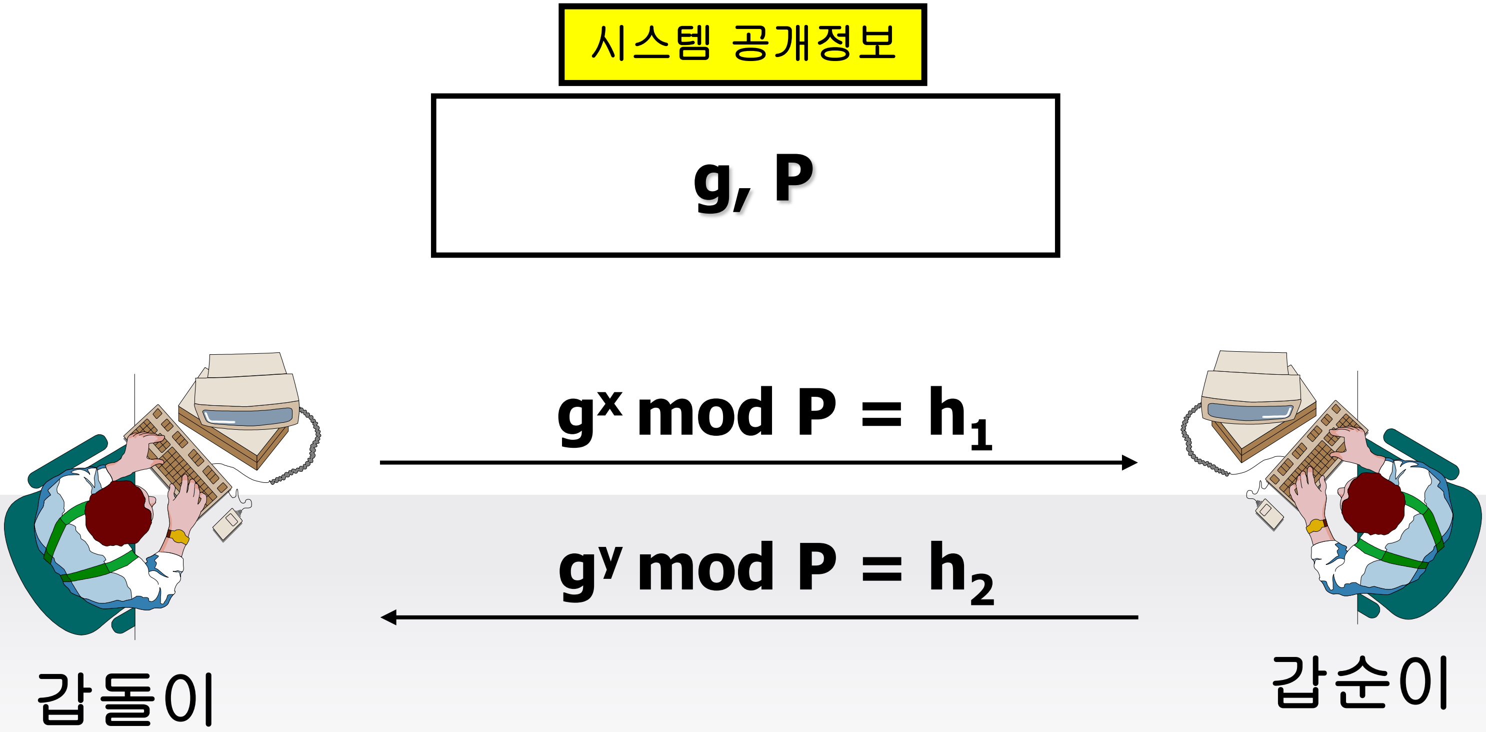
- Provable security does not yield proofs
  - Proofs are relative (to computational assumptions) and to the definition of the scheme’s goal
  - Proofs often done in ideal models (Random Oracle Model, Ideal Cipher Model, Generic Group Model) with debatable meaning.
  - Definitions and proofs need time for acceptance.

Limits of Provable Security

- Still, provable security
  - Provides some form of guarantee that the scheme is not flawed
  - Motivates us to spell out (clarify) definitions and models formally, a process that, in itself, may help us to better understand the problem!
  - Gives well-defined reductions from which we can distill practical implications of the result (exact security)

Key Management

Diffie-Hellman Key Exchange



시스템 공개정보

g, P

$g^x \bmod P = h_1$

$g^y \bmod P = h_2$

갑돌이

갑순이

$K = h_2^x = (g^y)^x = g^{xy} \pmod{P}$

$K = h_1^y = (g^x)^y = g^{xy} \pmod{P}$

Definition of Security

Indistinguishable !

K

Completely random key

K

수동적 공격자

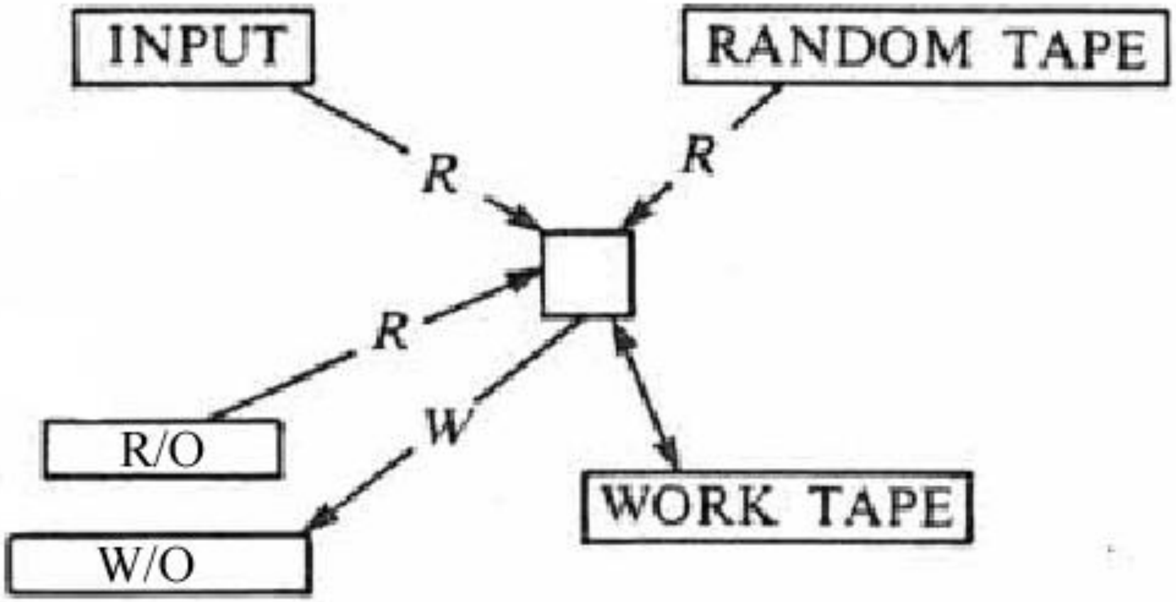
- ***This is much stronger than simply requiring that the adversary be unable to compute K exactly.***
  - *Can compute K –> Can distinguish K*

2-Party Protocols

※ Cited from Vitaly Shmatikov’s Presentation Material

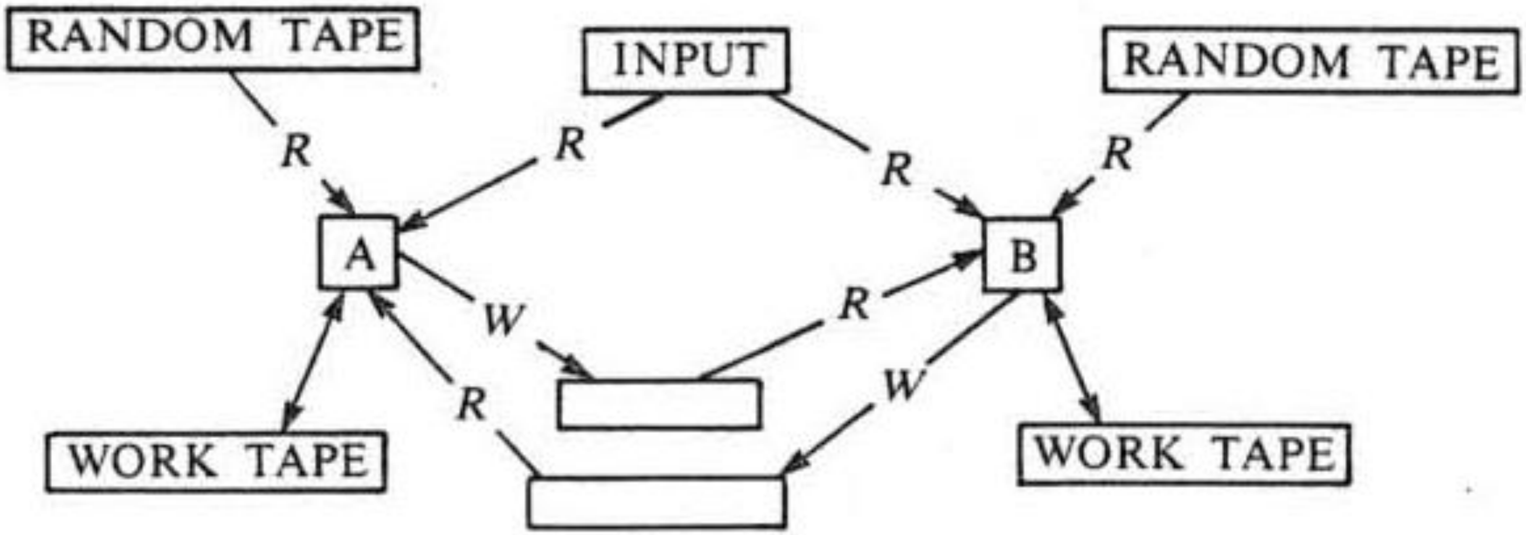
Interactive Protocol

- Interactive Turing Machine



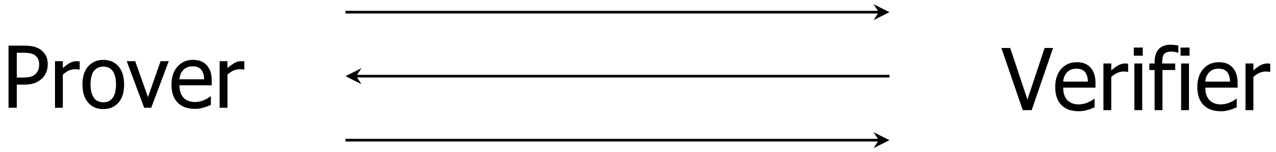
Interactive Protocol

- Interactive Turing Machines



Zero-Knowledge Proofs

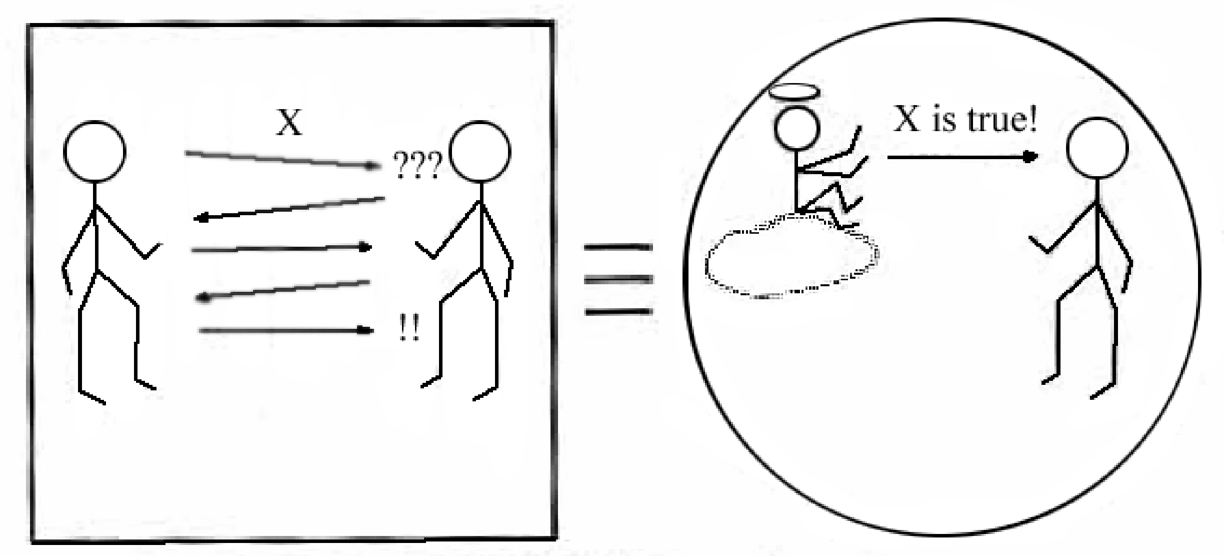
- An interactive proof system involves a prover and a verifier



(Interactive proofs)

Zero-Knowledge Proofs

- **Idea:** the prover proves a statement to the verifier without revealing anything except the fact that the statement is true
  - **Zero-Knowledge Proof of Knowledge (ZKPK):** prover convinces verifier that he knows a secret without revealing the secret



Properties of ZKPK

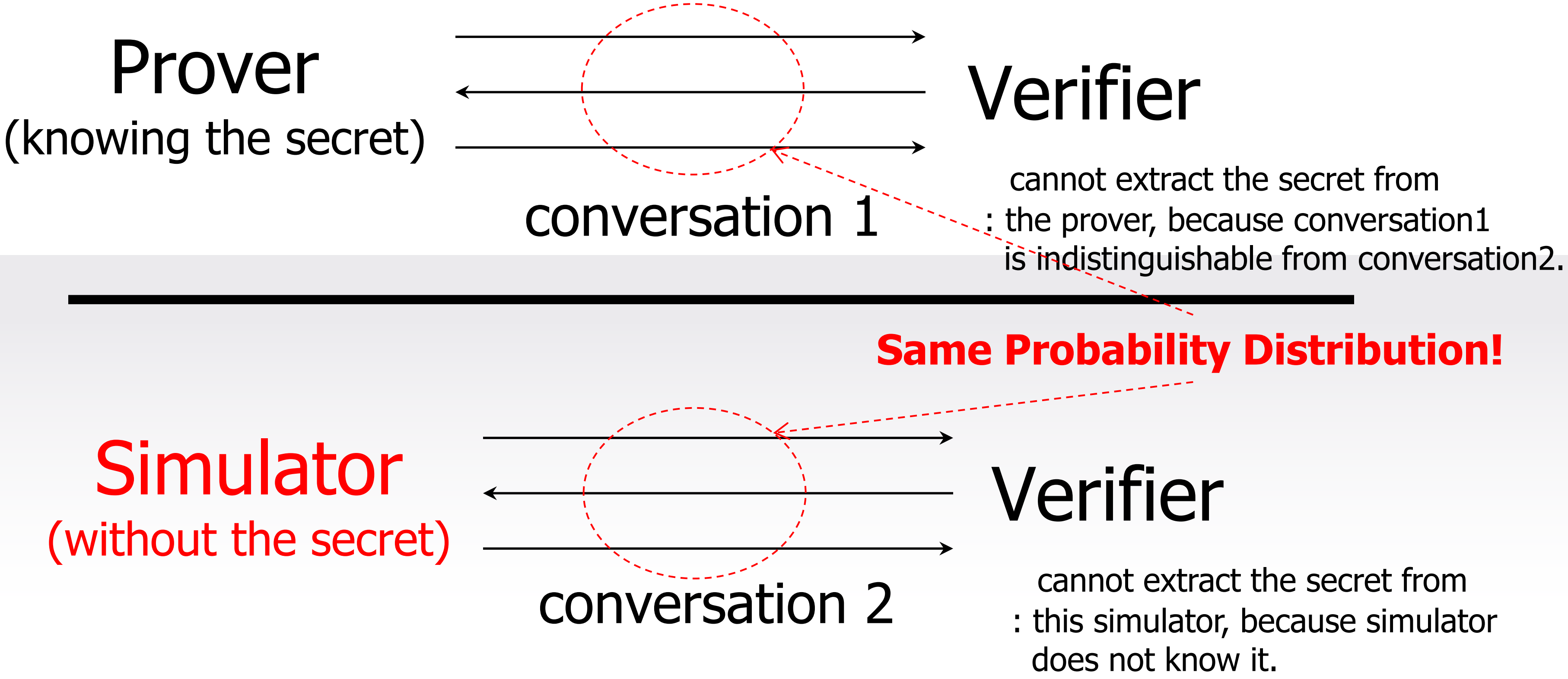
- **Completeness**
  - If both prover and verifier are honest, protocol succeeds with overwhelming probability
- **Soundness**
  - No one who does not know the secret can convince the verifier with nonnegligible probability
    - Intuition: the protocol should not enable prover to prove a false statement
- **Zero-Knowledge**
  - The proof does not leak any information

Zero-Knowledge Property

- The proof does not leak any information
- There exists a **simulator** that, taking what the verifier knows before the protocol starts, produces a fake “transcript” of protocol messages that is **indistinguishable** from actual protocol messages
  - Because all messages can be simulated from verifier’s initial knowledge, verifier does not learn anything that he didn’t know before
  - **Indistinguishability:** perfect, statistical, or computational
- Honest-verifier ZK only considers verifiers that follow the protocol

Zero-Knowledge Property

- Zero knowledge proofs are simulatable (conversation distributions are **indistinguishable**)



Prover

(knowing the secret)

conversation 1

Verifier

cannot extract the secret from
: the prover, because conversation1
is indistinguishable from conversation2.

Same Probability Distribution!

Simulator

(without the secret)

conversation 2

Verifier

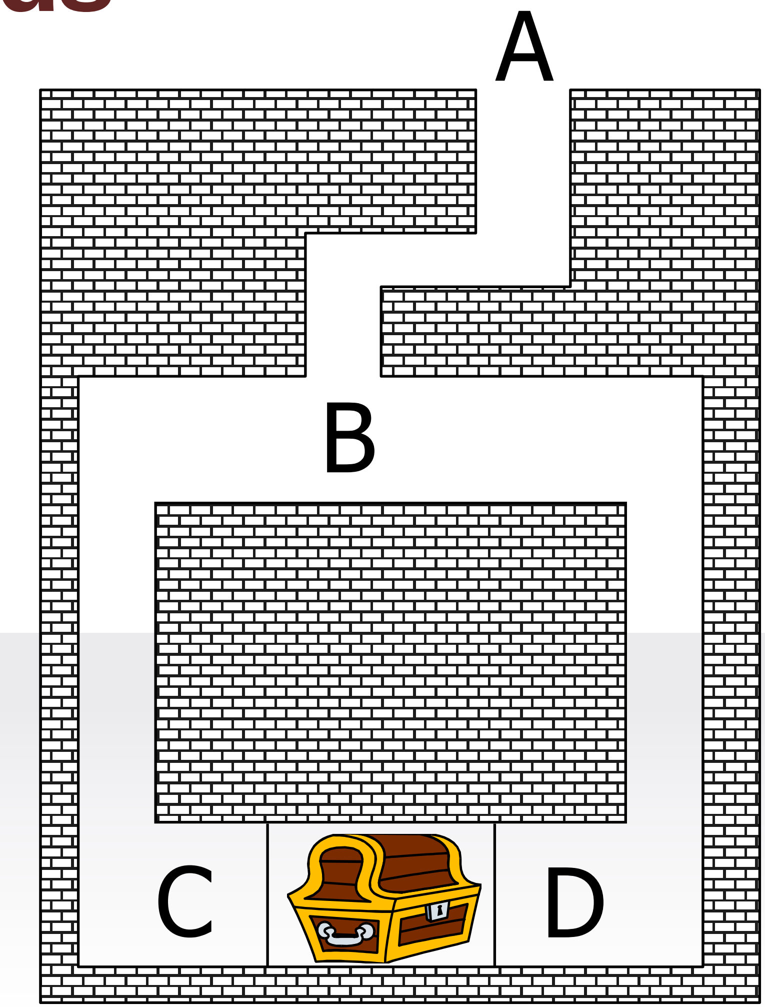
cannot extract the secret from
: this simulator, because simulator
does not know it.

Zero-Knowledge Property

- No one who does not know the secret can convince the verifier with nonnegligible probability.
- Let A be any prover who convinces the verifier …
- … there must exist a **knowledge extractor** algorithm that, given A, extracts the secret from A.
  - **Intuition:** if there existed some prover A who manages to convince the verifier that he knows the secret without actually knowing it, then no algorithm could possibly extract the secret from this A.

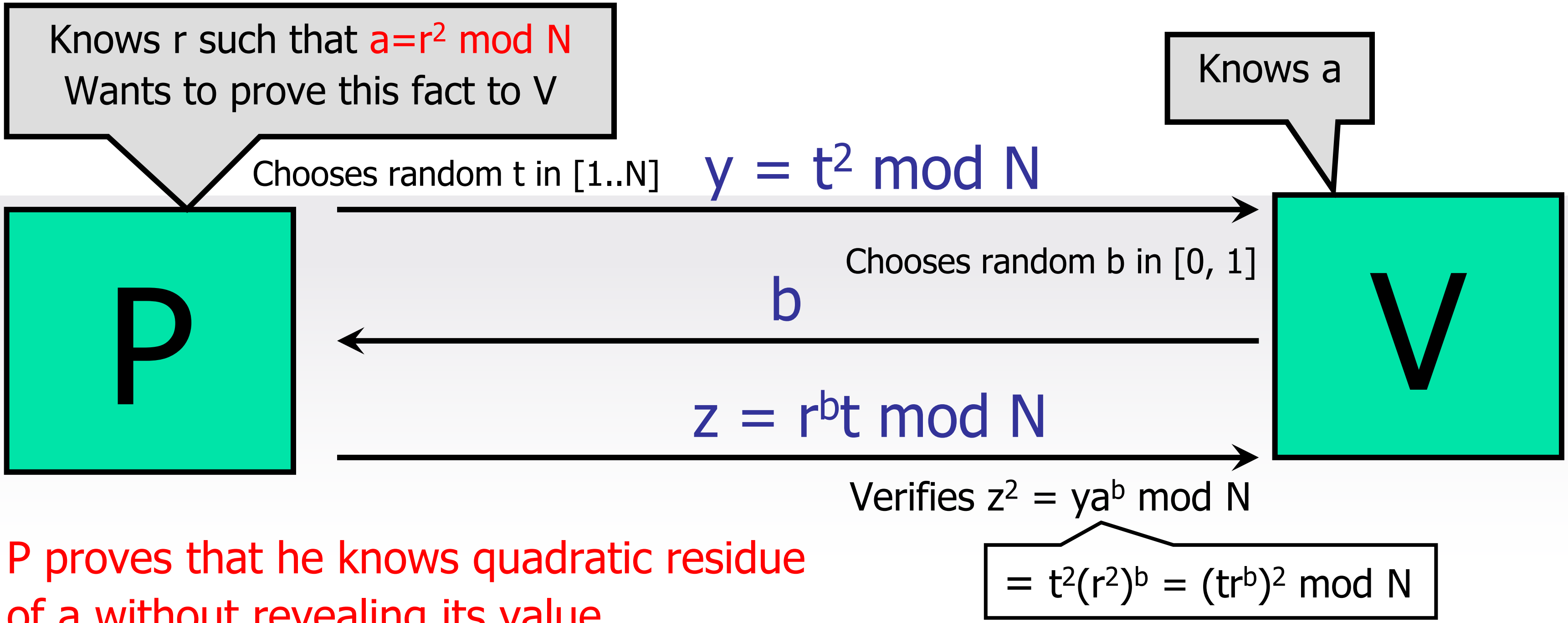
Zero-Knowledge for Kids

1. V stands at A.
2. P walks to C or D.
3. V walks to B.
4. V asks P to come L or R.
5. P follows the request.
6. Repeat 1 ~ 5, n times.



ZKIP for QRP

- System parameters
  - N



Knows r such that $a=r^2 \bmod N$
Wants to prove this fact to V

Knows a

P

V

Chooses random t in [1..N]

$y = t^2 \bmod N$

Chooses random b in [0, 1]

b

$z = r^b t \bmod N$

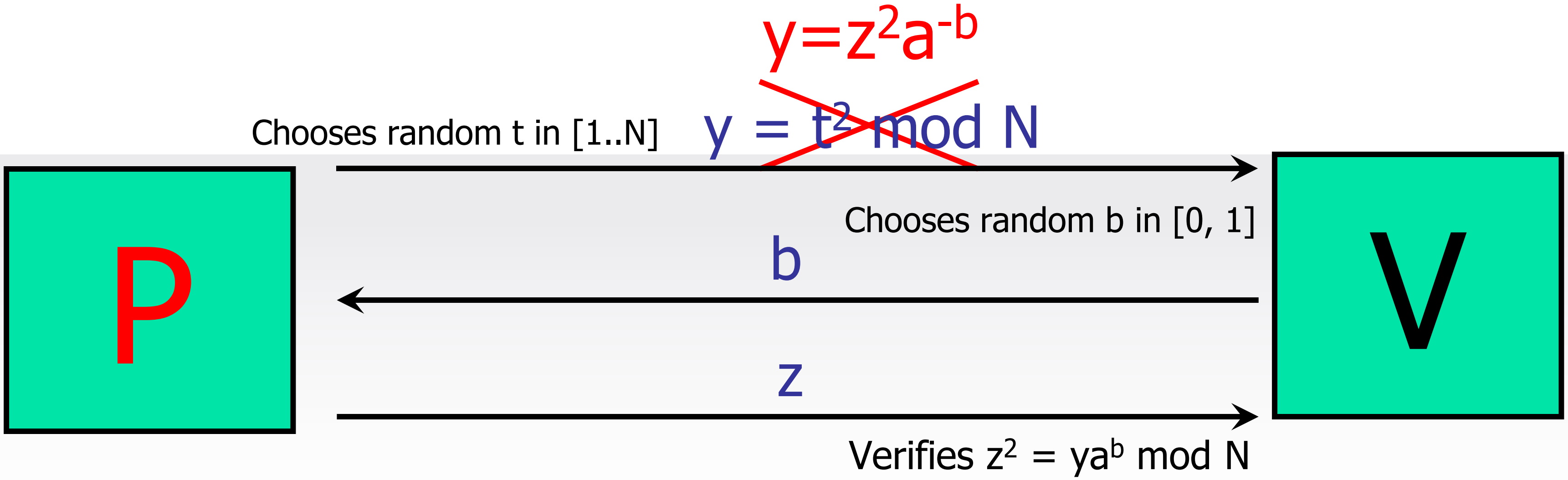
Verifies $z^2 = ya^b \bmod N$

$= t^2(r^2)^b = (tr^b)^2 \bmod N$

P proves that he knows quadratic residue of a without revealing its value

Cheating against ZKIP for QRP

- Prover can cheat if he can guess b in advance
  - Guess b, set $y=z^2a^{-b}$ for random z in 1st message
  - What is the probability of guessing b?

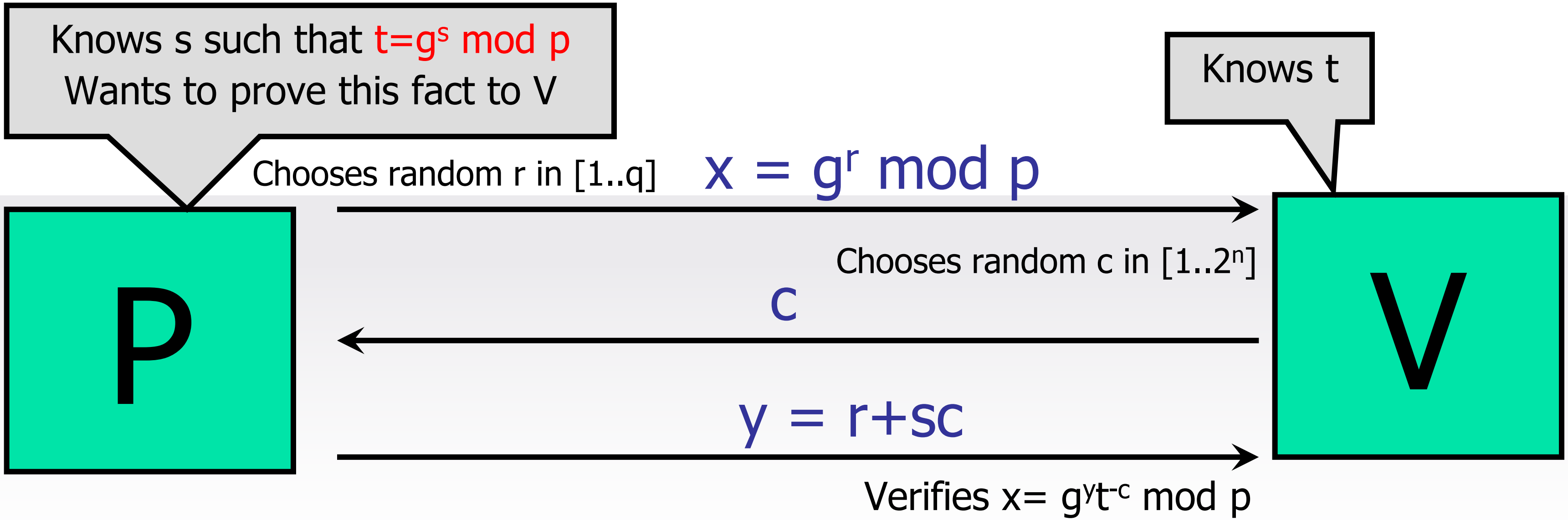


$y=z^2a^{-b}$
Chooses random t in [1..N]
~~$y = t^2 \bmod N$~~
P
V
Chooses random b in [0, 1]
b
z
Verifies $z^2 = ya^b \bmod N$

P proves that he “knows” quadratic residue of a even though he does not know r

Schnorr’s Id Protocol (ZKIP for DLP)

- System parameters
  - Prime p and q such that q divides p-1
  - g is a generator of an order-q subgroup of Z_p^*



Knows s such that $t=g^s \bmod p$
Wants to prove this fact to V

Knows t

P

V

Chooses random r in [1..q] $x = g^r \bmod p$

Chooses random c in $[1..2^n]$

c

$y = r+sc$

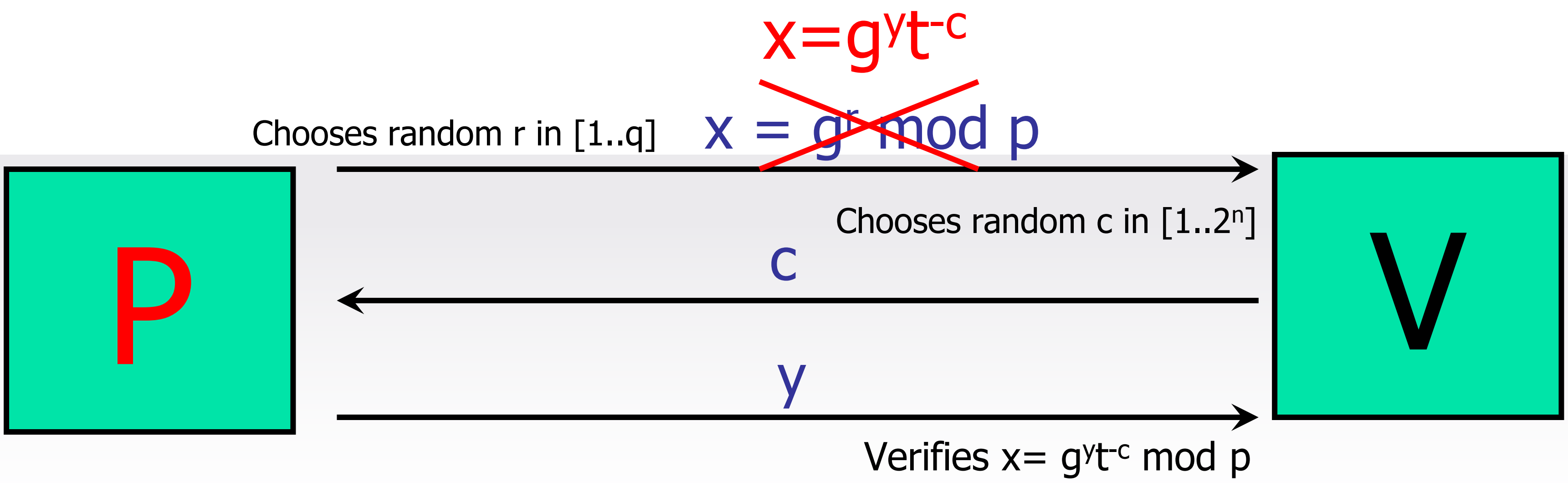
Verifies $x= g^y t^{-c} \bmod p$

$= g^{r+sc}(g^s)^{-c} \bmod p = g^r \bmod p$

P proves that he knows discrete log of t without revealing its value

Cheating against Schnorr's Id Protocol

- Prover can cheat if he can guess c in advance
  - Guess c, set $x=g^y t^{-c}$ for random y in 1st message
  - What is the probability of guessing c?

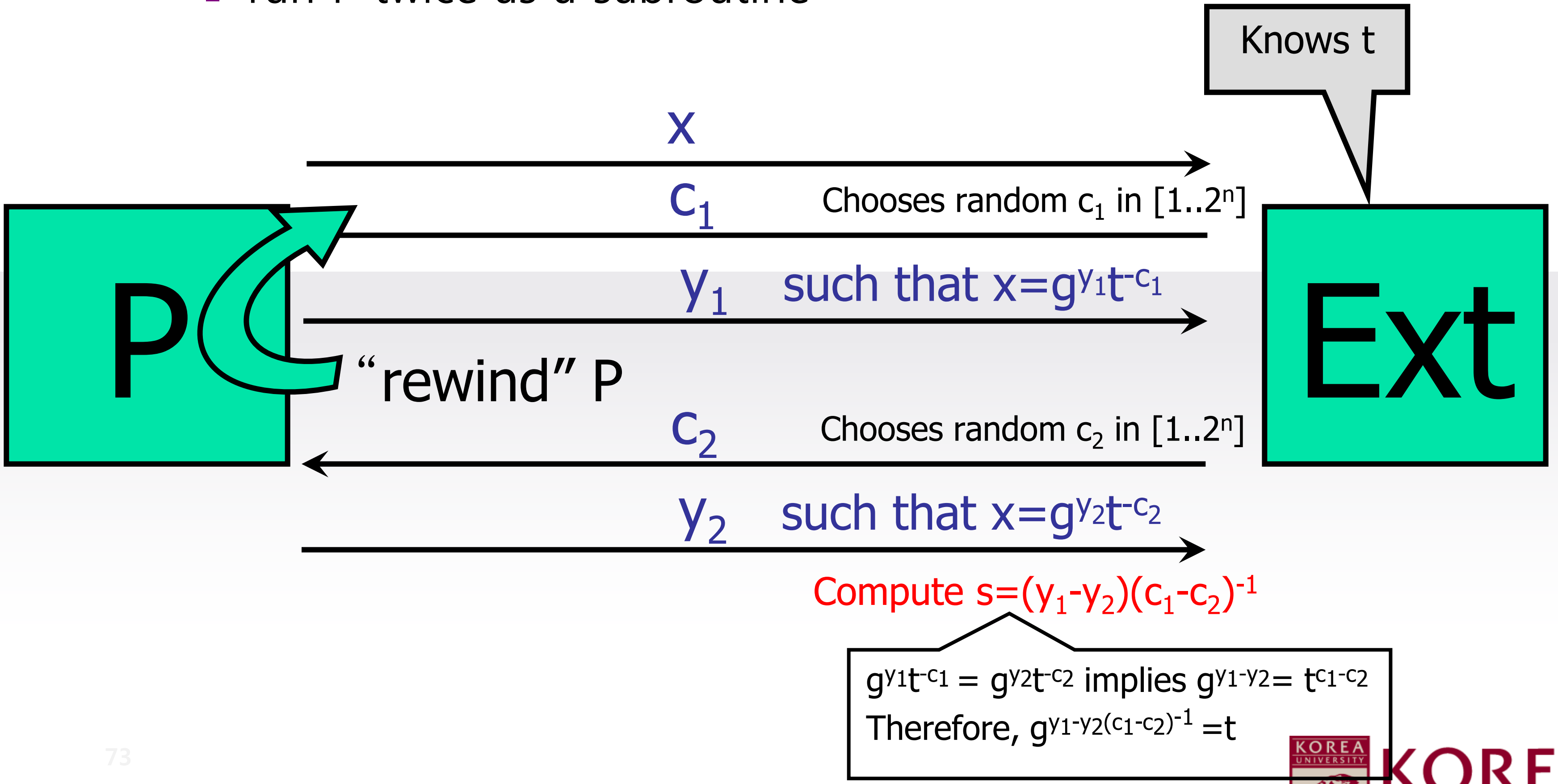


$x=g^y t^{-c}$
Chooses random r in [1..q]
~~$x = g^r \bmod p$~~
Chooses random c in $[1..2^n]$
c
y
Verifies $x= g^y t^{-c} \bmod p$
P
V

P proves that he "knows" discrete log of t even though he does not know s

But Schnorr’s Id Protocol Is Sound

- Prover can cheat if he can guess c in advance
  - Given P who successfully passes the protocol, extract s such that $t=g^s \bmod p$
    - run P twice as a subroutine



Knows t

P

Ext

x

c_1 Chooses random c_1 in $[1..2^n]$

y_1 such that $x=g^{y_1}t^{-c_1}$

“rewind” P

c_2 Chooses random c_2 in $[1..2^n]$

y_2 such that $x=g^{y_2}t^{-c_2}$

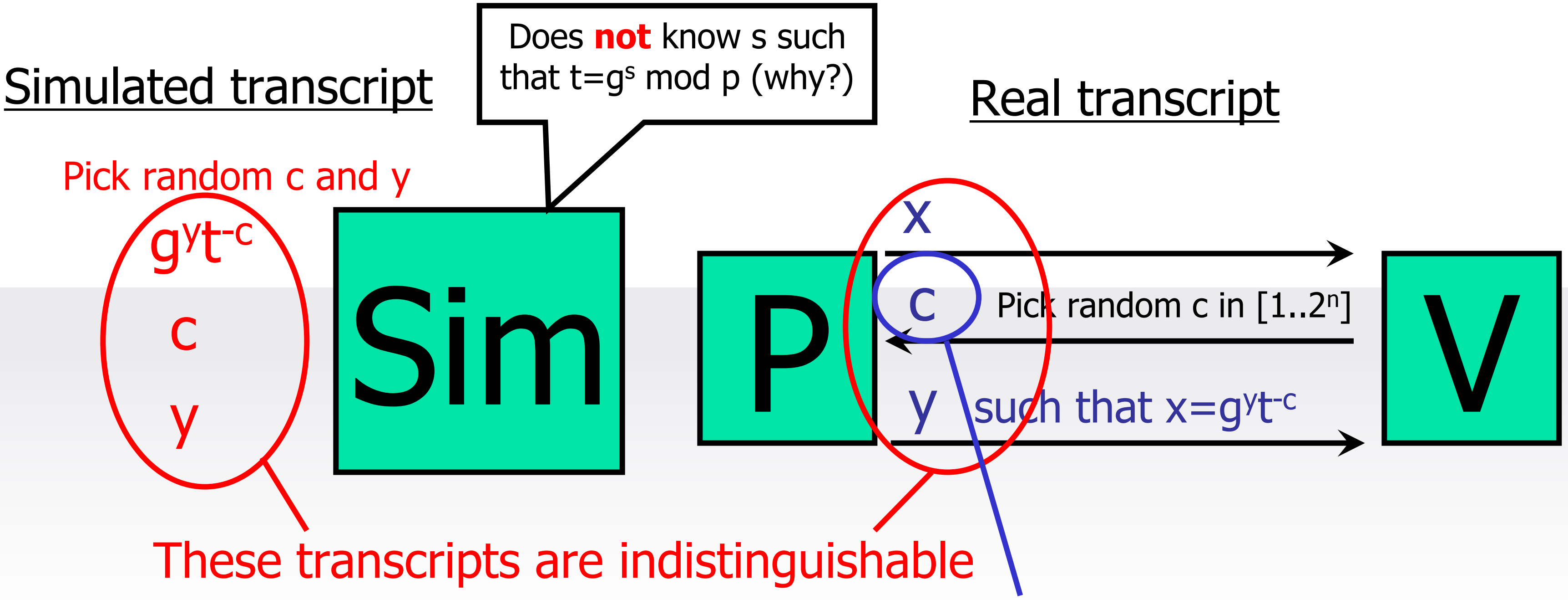
Compute $s=(y_1-y_2)(c_1-c_2)^{-1}$

$g^{y_1}t^{-c_1} = g^{y_2}t^{-c_2}$ implies $g^{y_1-y_2}= t^{c_1-c_2}$

Therefore, $g^{y_1-y_2(c_1-c_2)^{-1}} =t$

Schnorr's Id Protocol Is HVZK

- Simulator produces a transcript which is indistinguishable from the real transcript



Simulated transcript

Does **not** know s such that $t=g^s \bmod p$ (why?)

Real transcript

Pick random c and y

$g^y t^{-c}$

c

y

Sim

P

x

c

Pick random c in $[1..2^n]$

y such that $x=g^y t^{-c}$

V

These transcripts are indistinguishable

Schnorr's ID protocol is honest-verifier zero-knowledge

… but only if c in the real protocol is indeed random (verifier must run the protocol honestly)

Digital Signatures

Security Goal & Attack Model

- Target
  - **Total Break :** Find private key
  - **Selective Forgery :** Signature on selected message
  - **Existential Forgery :** Signature on some message

Security Goal & Attack Model

- Attack
  - Key-Only Attack
  - Known Message Attack
  - Chosen Message Attack

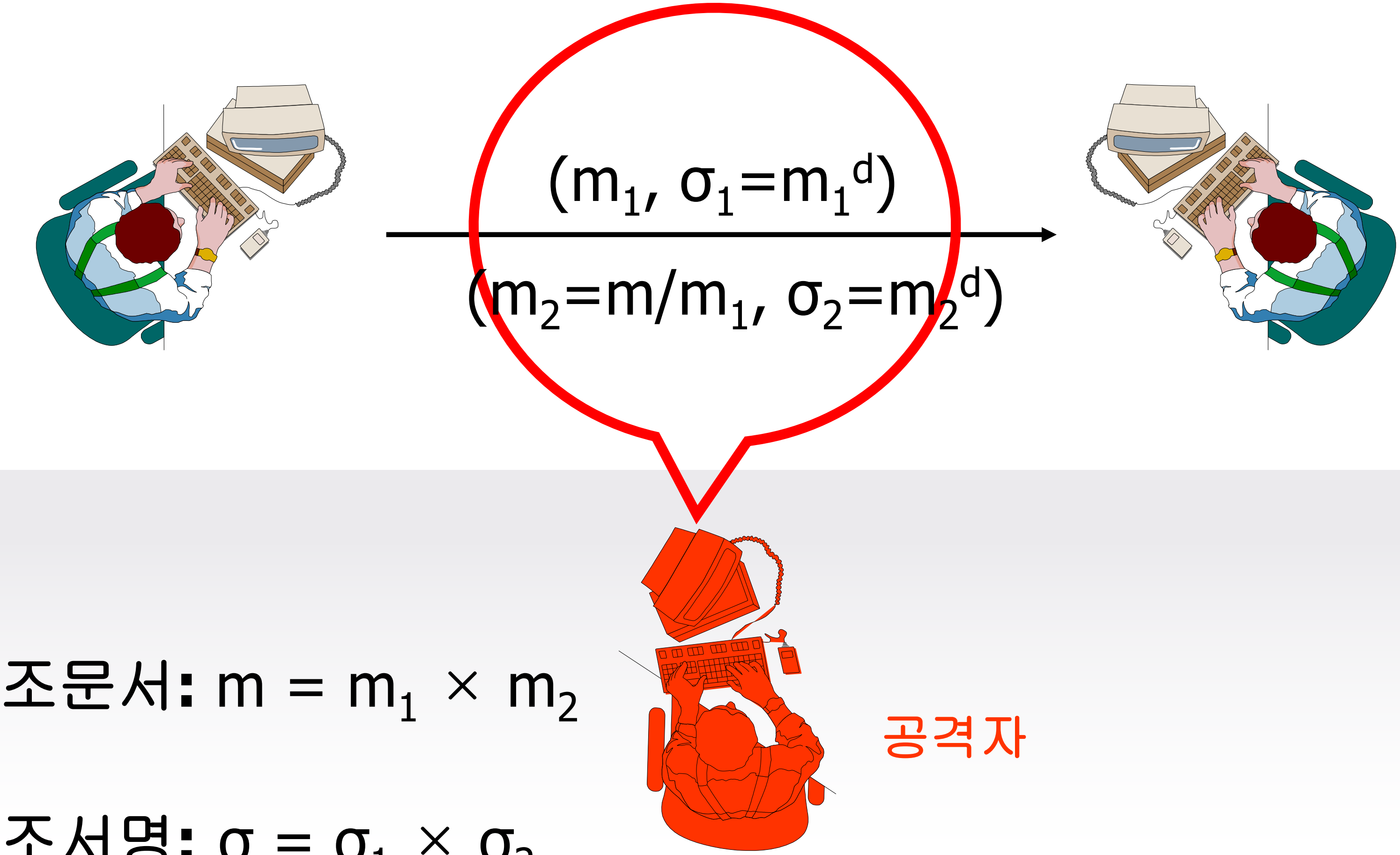
Existential Forgery - KOA

공격자

위조문서: $m = \sigma^e$

위조서명: Random σ

Selective Forgery - CMA

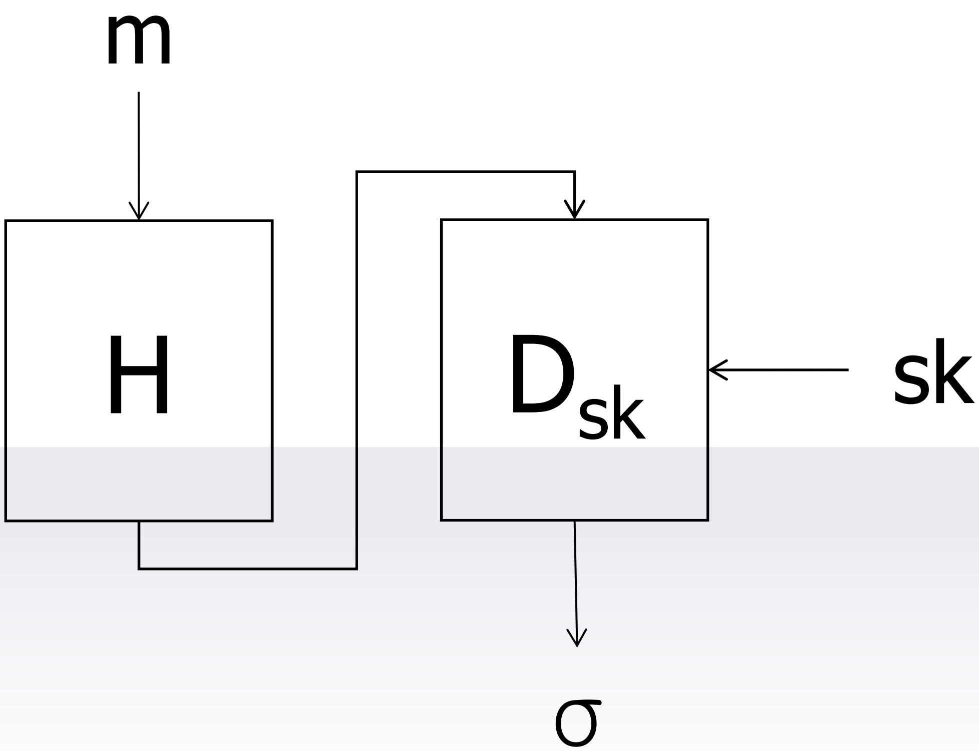


$(m_1, \sigma_1=m_1^d)$

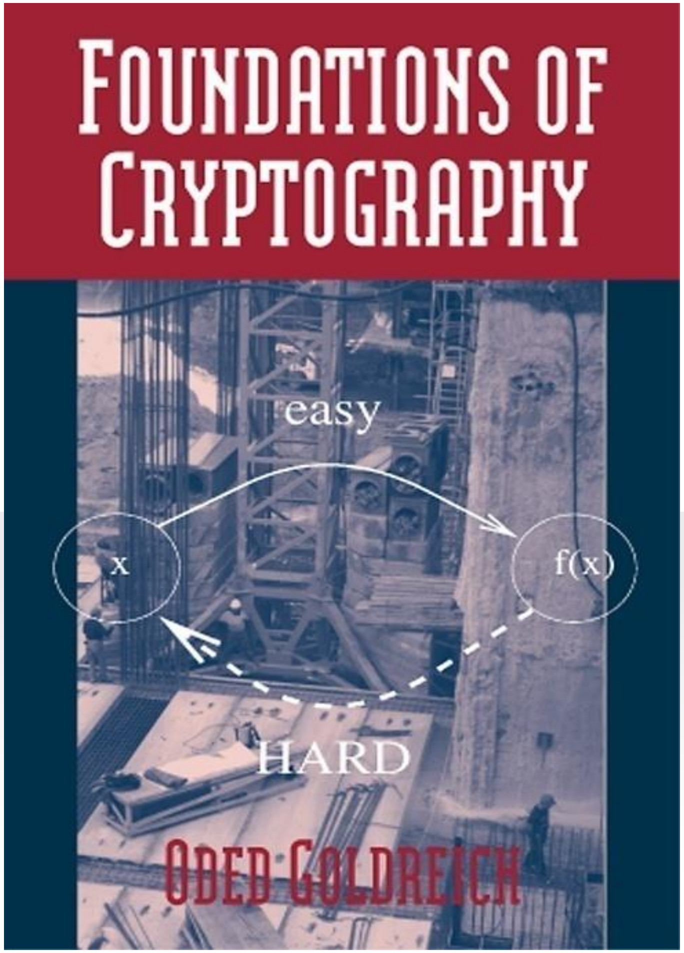
$(m_2=m/m_1, \sigma_2=m_2^d)$

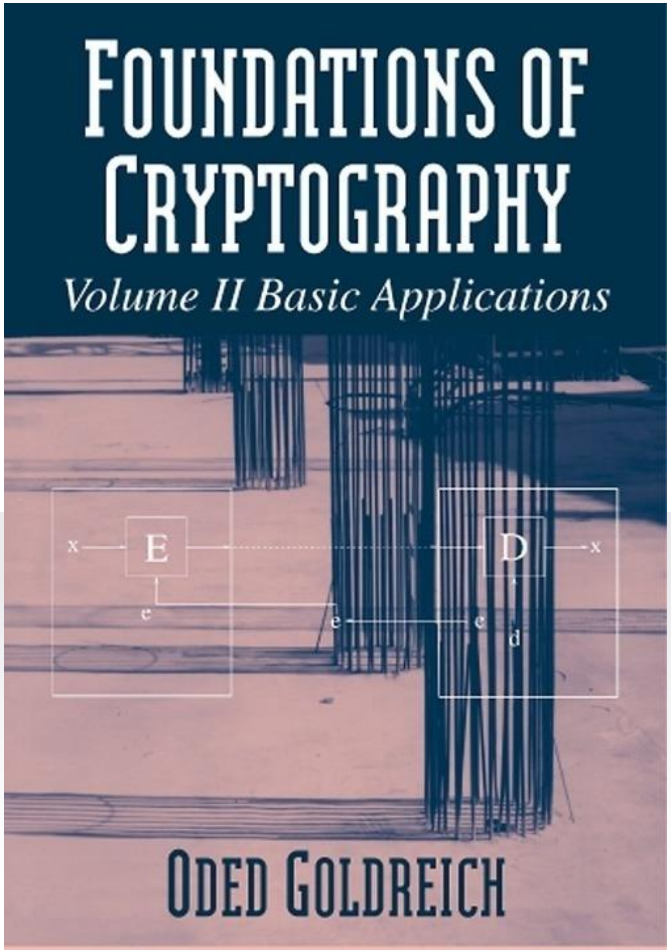
$$\begin{cases} \text{위조문서: } m = m_1 \times m_2 \\ \text{위조서명: } \sigma = \sigma_1 \times \sigma_2 \end{cases}$$

Hash-and-Sign Paradigm

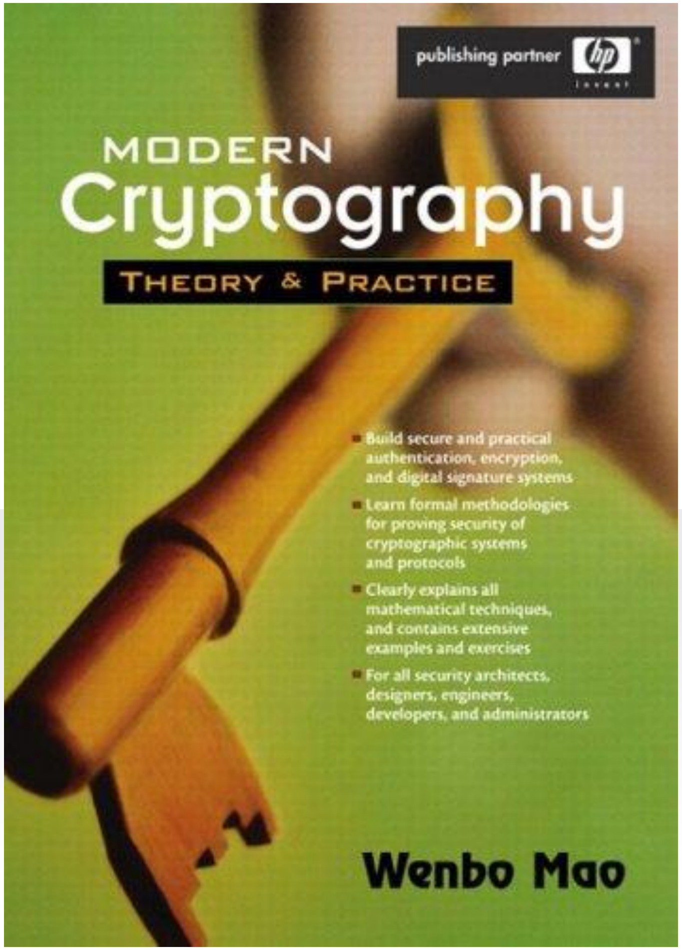


To Learn More





To Learn More

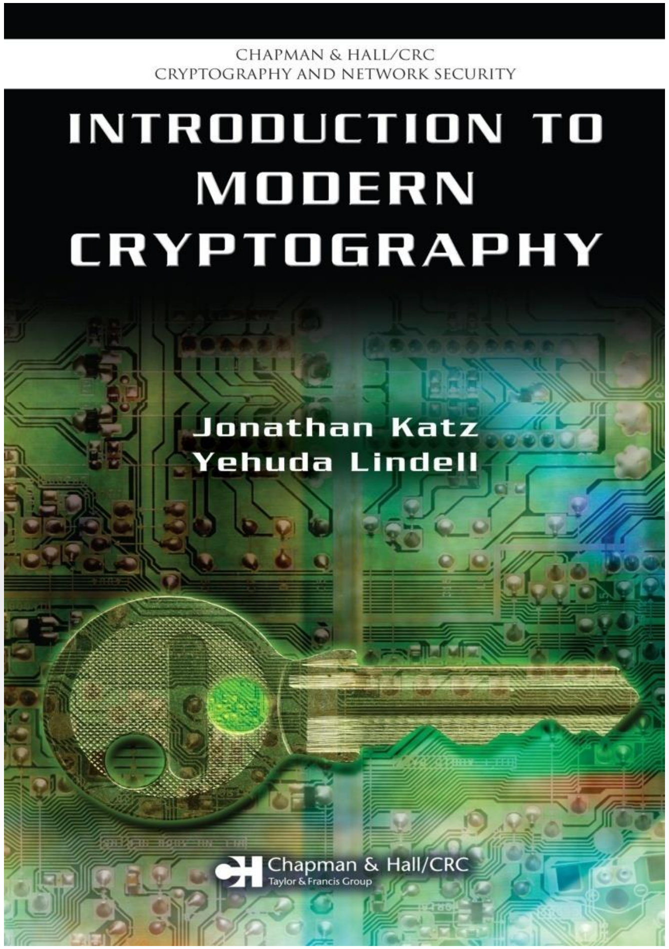


publishing partner hp invent

MODERN
Cryptography
THEORY & PRACTICE

- Build secure and practical authentication, encryption, and digital signature systems
- Learn formal methodologies for proving security of cryptographic systems and protocols
- Clearly explains all mathematical techniques, and contains extensive examples and exercises
- For all security architects, designers, engineers, developers, and administrators

Wenbo Mao



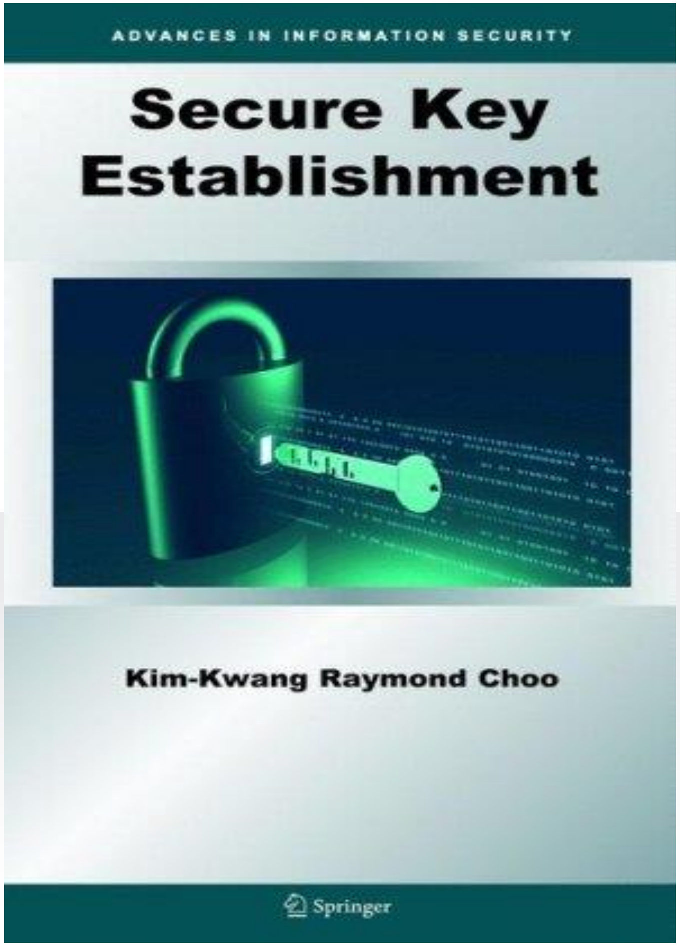
CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY

INTRODUCTION TO MODERN CRYPTOGRAPHY

Jonathan Katz
Yehuda Lindell

Chapman & Hall/CRC
Taylor & Francis Group

To Learn More



ADVANCES IN INFORMATION SECURITY

Secure Key Establishment

Kim-Kwang Raymond Choo

Springer

Secure Design

고려대학교 (Korea Univ.)

사이버국방학과 · 정보보호대학원 (CIST)

보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

(FB) www.fb.com/skim71 (Twitter) @skim71

고려대학교 정보보호대학원 KOREA UNIVERSITY