L4.1: Provable-perfectly-secure secret key encryption - OTP
第4.1讲：可证明完美安全的私钥加密 – 一次一密

Lecturer: Zoe L. JIANG蒋琳

A309
Sept 25, 2018, 15:45-17:30

Most of the slides come from http://drona.csa.iisc.ernet.in/~arpita/Cryptography17.html

Outline

- A secret key encryption construction
- Security proof of the secret key encryption construction
- Limitations of perfect secrecy
- More definitions of Perfect Security and their equivalence

Outline

- **A secret key encryption construction**
- Security proof of the secret key encryption construction
- Limitations of perfect secrecy
- More definitions of Perfect Security and their equivalence

Secret key encryption - construction

Construction 2.8 $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, 1\}^l$

Gen $\xrightarrow{k \in_R \mathcal{K}}$

$m \in \mathcal{M} \rightarrow$ **Enc** (key k): $c := m \oplus k$ $\xrightarrow{c}$

$c \in \mathcal{C} \rightarrow$ **Dec** (key k): $m := c \oplus k$ $\xrightarrow{m}$

Correctness: $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$

One-time pad encryption (OTP)

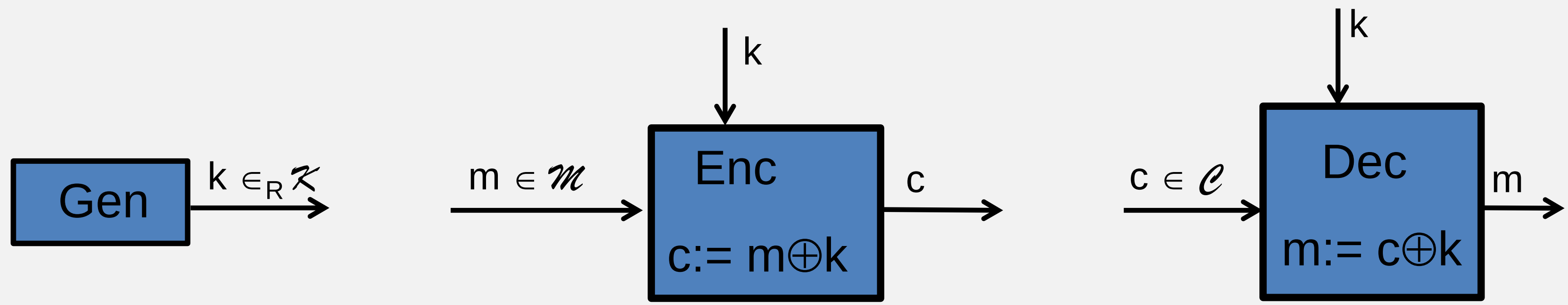
Vernam Cipher [1917]: But Shannon proved its security after formulating perfect security

Outline

- A secret key encryption construction
- **Security proof of the secret key encryption construction**
- Limitations of perfect secrecy
- More definitions of Perfect Security and their equivalence

Perfectly-secure encryption - proof 1/2

Construction 2.8 $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, 1\}^l$



Theorem 2.9 (Security): Vernam Cipher is perfectly-secure

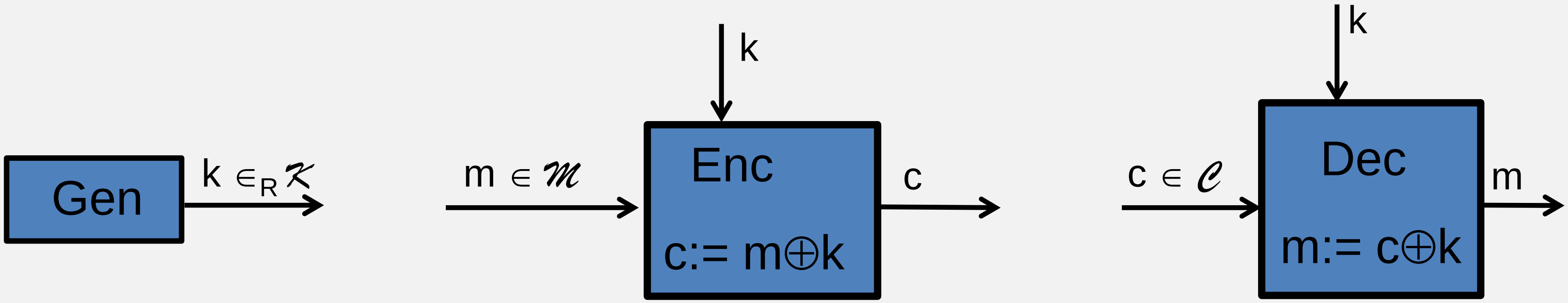
Proof: To prove $\Pr[M = m \mid C = c] = \Pr[M = m]$

For arbitrary c and m, $\Pr[C = c \mid M = m]$

$$= \Pr[\mathrm{Enc}_K(m) = c]$$
$$= \Pr[m \oplus K = c]$$
$$= \Pr[K = c \oplus m]$$
$$= 1/2^l$$

Perfectly-secure encryption - proof 2/2

Construction 2.8 $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, 1\}^l$



Theorem 2.9 (Security): Vernam Cipher is perfectly-secure

Proof:

$$\Pr[C = c] = \sum_{m \text{ in } M} \Pr[C = c \mid M = m] \Pr[M = m] \quad \text{(irrespective of } \ldots \text{)}$$

$$= 1/2^l \sum_{m \text{ in } M} \Pr[M = m] \quad = 1/2^l$$

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]}$$

$$= \Pr[M = m]$$

Historical Use of Vernam Cipher: Redline between White House & Kremlin during Cold war.

What have we done so far..

- ✓ Formulate a formal definition (threat + break model)
- ○ Identify assumptions needed
- ✓ Prove security of the construction relative to the definition

Outline

- A secret key encryption construction
- Security proof of the secret key encryption construction
- **Limitations of perfect secrecy**
- More definitions of Perfect Security and their equivalence

Vernam Cipher is not all that nice because..

- How long is the key? length is as long as the message

  - For long messages hard to agree on long key
  - What happens the parties cannot predict the message size in advance

- Can we use the key

  = m'

  m'

  ty k

VENONA Project: US & UK decrypted Russian Plaintext exploiting the use of same key to pad many messages

Michael Rabin

"You should never re-use a one-time pad. It's like toilet paper; if you re-use it, things get messy."

Key space must be as large as the message space

Theorem 2.10: If (Gen, Enc, Dec) is a perfectly-secure encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$

Proof: Assume $|\mathcal{K}| < |\mathcal{M}|$

Let c be a ciphertext with Pr[C = c] > 0

$M(c) := \{ m \mid m = Dec_k(c)$ for s

the set of all possible

$|M(c)| \leq |\mathcal{K}| < |\mathcal{M}|$

$\exists\, m \in \mathcal{M}$ s.t. $m \notin M(c)$

Pr [M = m | C = c] = 0 $\neq$ Pr [M = m]

No perfect Security!

Assume for instance un
distribution over M (a
where every message
with non-zero prob is ...e)

OTP is optimal key length-wise and key usability-wise

Show the other limitation is inevitable too!

Outline

- A secret key encryption construction
- Security proof of the secret key encryption construction
- Limitations of perfect secrecy
- **More definitions of Perfect Security and their equivalence**

Perfectly-secure encryption: equivalent definition

Definition 2.3 Perfectly-secure Encryption (Shannon's Definition):

$$\Pr[M = m \mid C = c] = \Pr[M = m], \ \forall\, m \in \mathcal{M}, c \in \mathcal{C}$$

Interpretation: probability o… owing a plain-text remains the same before and af… ext

-Easy to check (i) and (ii).

-No need of any probability calculation unlike original perfect security definition

…em

Theorem 2.11: A sc… th $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$ is perfectly secure if a…

(i) Every key k is c… $|\mathcal{K}|$ by Gen.

(ii) For every m in … C, there is a **unique** key k s.t. $Enc_k(m) = c$.

Perfect secrecy as an indistinguishability game

- Formulated as a challenge-response game between adv. and a challenger

Π = (Gen, Enc, Dec), $\mathcal{M}$

Comp. unbounded attacker

I can break Π

$m_0, m_1 \in \mathcal{M}$ →

(freedom to choose any pair)

← $c \leftarrow Enc_k(m_b)$

$b' \in \{0, 1\}$ →

(Guess about encrypted message)

Hypothetical challenger

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

k ← Gen ←

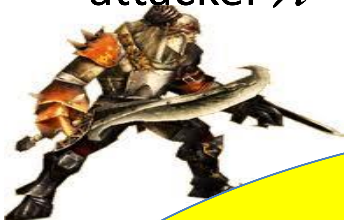
❑ Game output :

- ➢ 1 if b = b' ➔ Attacker won
- ➢ 0 if b ≠ b' ➔ Attacker lost

Perfect secrecy as an indistinguishability game

Comp. unbounded attacker $\mathcal{A}$

Π = (Gen, Enc, Dec), $\mathcal{M}$



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

b $\leftarrow$ {0, 1}

I ca

Gen

- Adversary should learn the underlying message from c only with probability ½
  - No better than guessing m

- Wh

m

k

k

(I know that either m_0 or m_1 will be communicated with equal prob.)

- Perfect secrecy : adversary should not get "any advantage" by seeing c above

Perfect secrecy as an indistinguishability game

Comp. unbounded

Π = (Gen, Enc, Dec), $\mathcal{M}$

I can break Π

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

$c \leftarrow Enc_k(m_b)$

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

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

k Gen

Perfect indistinguishability

❑ Expe

Lemma 2.6 Π = (Gen, Enc, Dec) over $\mathcal{M}$ is perfectly-secure if and only if it is perfectly indistinguishable

Definition 2.5 Π = (Gen, Enc, Dec) over $\mathcal{M}$ is perfectly indistinguishable if for every attacker A

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

Perfectly-secure Encryption : Equivalent Definition

Definition 2.3 Perfectly-secure Encryption (Shannon's Definition):

$$\Pr[M = m \mid C = c] = \Pr[M = m], \forall\, m \in \mathcal{M}, c \in \mathcal{C}$$

Interpretation: probability of knowing a plain-text remains the same before and after seeing the cipher-text

Lemma 2.4 The equivalence holds for any probability distribution over M

Perfectly-secure Encryption (Alternate Definition):

$$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1], \forall\, m_0, m_1 \in \mathcal{M}, c \in \mathcal{C}$$

Interpretation: probability distribution of cipher-text is independent of plain-text

Perfect secrecy: equivalence of definitions

Definition 2.3: For every probability dist over $\mathcal{M}$

$\Pr[M = m \mid C = c] = \Pr[M = m]$

$\forall\, m \in \mathcal{M}, c \in \mathcal{C}$

Lemma 2.4: For every probability dist over $\mathcal{M}$

$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1]$

$\forall\, m_0, m_1 \in \mathcal{M}, c \in \mathcal{C}$

Theorem 2.11: For every probability distribution over $\mathcal{M}$

(i) Every key k is chosen with probability **$1/ |\mathcal{K}|$**

(ii) For every m in M and every c in C, there is a **unique** key k s.t. $Enc_k(m) = c$.

Definition 2.5: For every probability dist over $\mathcal{M}$

$$\Pr\left(PrivK^{coa}_{A,\Pi} = 1 \right) = ½$$

(Perfect Indistinguishability)

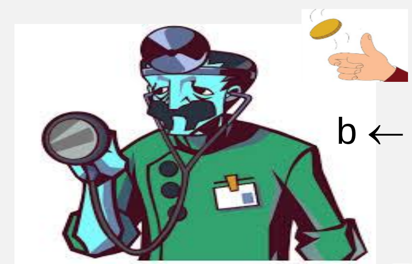
Unbounded Powerful

I can break Π

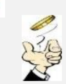
$m_0, m_1 \in \mathcal{M}$

$c \leftarrow Enc_k(m_b)$

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



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



k

Gen

Experiment : $PrivK^{coa}_{A,\Pi}$

Π is perfectly-secure if for every adversary A $\Pr\left(PrivK^{coa}_{A,\Pi} = 1 \right) = ½$

Concluding Perfect Security

CCA

Birth of Computational / Cryptographic Security.

A

A

Remember that at the end of the day crypto is an applied science and we need to construct schemes that has practical relevance. The hurdles in achieving perfect security outweighs the strength of perfect security

A cipl
about
prior i

the

mitations:

e as large as mes

not be reused

elaxations

Unbou

↓

Bounded Powerful /
Polynominally Bounded

Can we overcome the hurdles?

Yes!!

No break allowed

↓

Break is allowed but with 'very small' probability

Perfect Security vs. Computational Security

- Threat is Unbounded Powerful
- No break allowed
- A scheme is secure if

  Pr [M = m | C = c] = Pr [M = m] $\forall$ m, c
- Key as large as the message
- Fresh key for every encryption

- Threat is ‘Computationally Bounded’
- Break is allowed with ‘small’ probability
- A scheme is secure if any computationally bounded adversary succeeds in ‘breaking’ the scheme with at most ‘some very small probability’.
- A small key will do
- Key reuse is permitted.

Is it necessary to relax the threat and break to overcome the limitations?

YES Absolutely!

References

- [1] **Jonathan Katz, Yehuda Lindell**. Chapter 2, Introduction to Modern Cryptography, 2nd Edition, Chapman & Hall/CRC Cryptography and Network Security Series, 2014
- [2] http://drona.csa.iisc.ernet.in/~arpita/Cryptography17.html