

Cryptography

Lecture 3: Indistinguishability & Limits of Perfect Secrecy

October 30, 2026

Next Dates

LECTURE (FRI 1:15PM)	
Oct 30th	Lecture 3: Indistinguishability & Limits of Perfect Secrecy
Nov 6th	Lecture 4: Pseudorandom Generators
13th	Lecture 5: Multiple Encryptions
20th	Lecture 6: Pseudorandom Functions
27th	Lecture 7: Operation Modes
Dec 4th	Lecture 8: Message Authentication Codes
11th	Lecture 9: Authenticated Encryption
18th	Lecture 10: Hash functions

LECTURE (FRI 1:15PM)	
Dec 25th	
Jan 1st	
8th	Lecture 11: RSA & Diffie-Hellman assumptions
15th	Lecture 12: Elliptic curves
22nd	Lecture 13: Digital signatures
29th	Lecture 14: Zero-Knowledge Proofs
Feb 5th	Lecture 15: Reserve

Contents

- 1 **Classical cryptography**
(Shift & Vigenère cipher, one-time pad, perfect secrecy)
- 2 **Security definitions & threat models**
(Computational security, CPA & CCA)
- 3 **Private-key cryptography**
(Message authentication, hash functions, primitives, relevant ciphers)
- 4 **Public-key cryptography**
(Assumptions, key management, digital signatures, relevant ciphers)

Perfectly Secret Encryption

Notes

- Use consistent variable naming (messages, keys, ciphertext)
- Drop distribution marker — write $P(m)$ instead of $P_{\mathcal{M}}(m)$

Perfectly Secret Encryption

Notes

- Use consistent variable naming (messages, keys, ciphertext)
- Drop distribution marker — write $P(m)$ instead of $P_{\mathcal{M}}(m)$
- Utilize usual probability notation — $P(m, c)$ for joint probability
- Assume message & key selection is independent

$$P(k, m) = P(k) \cdot P(m)$$

- Then

$$P(c) = \sum_{k \in K, m \in \mathcal{M}} P(k, m) \cdot P[c \leftarrow \text{enc}_k(m)]$$

and in perfectly secret encryption scheme $\mathcal{E}$ for any message $m' \in \mathcal{M}$

$$P(c) = O_{\mathcal{E}}(c, m') = \sum_{k \in K} P(k) \cdot P[c \leftarrow \text{enc}_k(m')]$$

Perfectly Secret Encryption

§2.7 Lemma

Encryption scheme $\mathcal{E}$ is perfectly secret if and only if
in every scenario $(\mathcal{E}, P_M)$ we have $P(m | c) = P(m)$
for all messages $m \in \mathcal{M}$ and possible ciphertexts $c \in \mathcal{C}$ with $P(c) \neq 0$

Perfectly Secret Encryption

§2.7 Lemma

Encryption scheme $\mathcal{E}$ is perfectly secret if and only if in every scenario $(\mathcal{E}, P_M)$ we have $P(m | c) = P(m)$ for all messages $m \in M$ and possible ciphertexts $c \in C$ with $P(c) \neq 0$

Proof (1/2)

($\rightarrow$) Let $P_M: M \rightarrow [0, 1]$, $m, m' \in M$, and $c \in C$ with $P(c) \neq 0$

$$\begin{aligned} P(m | c) &= \frac{P(m, c)}{P(c)} = \frac{\overbrace{\sum_{k \in K} P(k) \cdot P(m) \cdot P[c \leftarrow \text{enc}_k(m)]}^{=P(m, c)}}{\underbrace{O_{\mathcal{E}}(c, m')}_{=P(c)}} \\ &= P(m) \cdot \frac{\sum_{k \in K} P(k) \cdot P[c \leftarrow \text{enc}_k(m)]}{O_{\mathcal{E}}(c, m')} = P(m) \cdot \frac{\cancel{O_{\mathcal{E}}(c, m)}}{\cancel{O_{\mathcal{E}}(c, m')}} \end{aligned}$$

Perfectly Secret Encryption

Proof (2/2)

($\leftarrow$) Let $c \in C$ and $m, m' \in M$. Consider distribution $P_M: M \rightarrow [0, 1]$ such that $P_M(m) = P_M(m') = \frac{1}{2}$ and $P_M(m'') = 0$ otherwise.

Perfectly Secret Encryption

Proof (2/2)

($\leftarrow$) Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Consider distribution $P_{\mathcal{M}}: \mathcal{M} \rightarrow [0, 1]$ such that $P_{\mathcal{M}}(m) = P_{\mathcal{M}}(m') = \frac{1}{2}$ and $P_{\mathcal{M}}(m'') = 0$ otherwise. First suppose that $P(c) = 0$. Then

$$P(k) \cdot P[c \leftarrow \text{enc}_k(m)] = 0 = P(k) \cdot P[c \leftarrow \text{enc}_k(m')]$$

for all $k \in K$. Hence $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ as required.

Perfectly Secret Encryption

Proof (2/2)

($\leftarrow$) Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Consider distribution $P_{\mathcal{M}}: \mathcal{M} \rightarrow [0, 1]$ such that $P_{\mathcal{M}}(m) = P_{\mathcal{M}}(m') = \frac{1}{2}$ and $P_{\mathcal{M}}(m'') = 0$ otherwise. First suppose that $P(c) = 0$. Then

$$P(k) \cdot P[c \leftarrow \text{enc}_k(m)] = 0 = P(k) \cdot P[c \leftarrow \text{enc}_k(m')]$$

for all $k \in K$. Hence $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ as required.

Otherwise $P(c) \neq 0$ and we prove that $P(c) = O_{\mathcal{E}}(c, m'')$ for all $m'' \in \{m, m'\}$, which also proves $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$

Perfectly Secret Encryption

Proof (2/2)

($\leftarrow$) Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Consider distribution $P_{\mathcal{M}}: \mathcal{M} \rightarrow [0, 1]$ such that $P_{\mathcal{M}}(m) = P_{\mathcal{M}}(m') = \frac{1}{2}$ and $P_{\mathcal{M}}(m'') = 0$ otherwise. First suppose that $P(c) = 0$. Then

$$P(k) \cdot P[c \leftarrow \text{enc}_k(m)] = 0 = P(k) \cdot P[c \leftarrow \text{enc}_k(m')]$$

for all $k \in K$. Hence $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ as required.

Otherwise $P(c) \neq 0$ and we prove that $P(c) = O_{\mathcal{E}}(c, m'')$ for all $m'' \in \{m, m'\}$, which also proves $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$

$$P(c) = \frac{P(m'', c)}{P(m'' | c)} = \frac{\sum_{k \in K} P(k) \cdot P(m'') \cdot P[c \leftarrow \text{enc}_k(m'')]}{P(m'')}$$



Perfectly Secret Encryption

Proof (2/2)

($\leftarrow$) Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Consider distribution $P_{\mathcal{M}}: \mathcal{M} \rightarrow [0, 1]$ such that $P_{\mathcal{M}}(m) = P_{\mathcal{M}}(m') = \frac{1}{2}$ and $P_{\mathcal{M}}(m'') = 0$ otherwise. First suppose that $P(c) = 0$. Then

$$P(k) \cdot P[c \leftarrow \text{enc}_k(m)] = 0 = P(k) \cdot P[c \leftarrow \text{enc}_k(m')]$$

for all $k \in K$. Hence $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ as required.

Otherwise $P(c) \neq 0$ and we prove that $P(c) = O_{\mathcal{E}}(c, m'')$ for all $m'' \in \{m, m'\}$, which also proves $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$

$$P(c) = \frac{P(m'', c)}{P(m'' | c)} = \frac{\sum_{k \in K} P(k) \cdot \cancel{P(m'')} \cdot P[c \leftarrow \text{enc}_k(m'')]}{\cancel{P(m'')}} \quad \square$$

Perfectly Secret Encryption

Proof (2/2)

($\leftarrow$) Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Consider distribution $P_{\mathcal{M}}: \mathcal{M} \rightarrow [0, 1]$ such that $P_{\mathcal{M}}(m) = P_{\mathcal{M}}(m') = \frac{1}{2}$ and $P_{\mathcal{M}}(m'') = 0$ otherwise. First suppose that $P(c) = 0$. Then

$$P(k) \cdot P[c \leftarrow \text{enc}_k(m)] = 0 = P(k) \cdot P[c \leftarrow \text{enc}_k(m')]$$

for all $k \in K$. Hence $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ as required.

Otherwise $P(c) \neq 0$ and we prove that $P(c) = O_{\mathcal{E}}(c, m'')$ for all $m'' \in \{m, m'\}$, which also proves $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$

$$P(c) = \frac{P(m'', c)}{P(m'' | c)} = \frac{\sum_{k \in K} P(k) \cdot \cancel{P(m'')} \cdot P[c \leftarrow \text{enc}_k(m'')]}{\cancel{P(m'')}} = O_{\mathcal{E}}(c, m'')$$



One-Time Pad

§2.8 Example (One-time pad; Vernam 1917)

Let $\ell \in \mathbb{N}$ and $K = M = C = \{0,1\}^\ell$. Length ℓ **one-time pad** is given by

- Key generation $P_K(k) = 2^{-\ell}$ for all $k \in K = \{0,1\}^\ell$
(uniform selection from key space of all keys of length ℓ)

§2.8 Example (One-time pad; Vernam 1917)

Let $\ell \in \mathbb{N}$ and $K = M = C = \{0,1\}^\ell$. Length ℓ **one-time pad** is given by

- Key generation $P_K(k) = 2^{-\ell}$ for all $k \in K = \{0,1\}^\ell$
(uniform selection from key space of all keys of length ℓ)
- Encryption $\text{enc}: K \times M \rightarrow C$ with $K = M = C = \{0,1\}^\ell$

$$\text{enc}_k(m_1, \dots, m_\ell) = (m_1 \oplus k_1, \dots, m_\ell \oplus k_\ell)$$

with $k = (k_1, \dots, k_\ell)$

(bitwise XOR of message & key)

One-Time Pad

§2.8 Example (One-time pad; Vernam 1917)

Let $\ell \in \mathbb{N}$ and $K = M = C = \{0,1\}^\ell$. Length ℓ **one-time pad** is given by

- Key generation $P_K(k) = 2^{-\ell}$ for all $k \in K = \{0,1\}^\ell$
(uniform selection from key space of all keys of length ℓ)
- Encryption $\text{enc}: K \times M \rightarrow C$ with $K = M = C = \{0,1\}^\ell$
$$\text{enc}_k(m_1, \dots, m_\ell) = (m_1 \oplus k_1, \dots, m_\ell \oplus k_\ell)$$

with $k = (k_1, \dots, k_\ell)$ (bitwise XOR of message & key)
- Decryption $\text{dec} = \text{enc}$

Gilbert Sandford Vernam (* 1890; † 1960)

- US engineer at AT&T Bell Labs
- Cipher patented in 1919; used by allies in WW2
- Shannon (also at Bell Labs) proved it unbreakable



One-Time Pad

Illustration

m	1	1	0	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1	0
k	0	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	1	1	1	1	0	0
$enc_k(m)$	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1	1	0	1	1	1	1	0	1	0
k	0	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	1	1	1	1	0	0
$dec_k(m)$	1	1	0	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1	0

One-Time Pad

Illustration

m	1	1	0	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1	0
k	0	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	1	1	1	1	0	0
$enc_k(m)$	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1	1	0	1	1	1	1	0	1	0
k	0	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	1	1	1	1	0	0
$dec_k(m)$	1	1	0	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1	0

Notes

- Correctness of one-time pad obvious $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m$
- Key length = message length (biggest drawback)

§2.9 Theorem

(Length ℓ) One-time pad encryption scheme (§2.8) is perfectly secret

§2.9 Theorem

(Length ℓ) One-time pad encryption scheme (§2.8) is perfectly secret

Proof

Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Since key distribution is uniform, we just prove

$$\sum_{k \in K} \mathbb{P}[c \leftarrow \text{enc}_k(m)] = \sum_{k \in K} \mathbb{P}[c \leftarrow \text{enc}_k(m')]$$

§2.9 Theorem

(Length ℓ) One-time pad encryption scheme (§2.8) is perfectly secret

Proof

Let $c \in \mathcal{C}$ and $m, m' \in \mathcal{M}$. Since key distribution is uniform, we just prove

$$\sum_{k \in K} \mathbb{P}[c \leftarrow \text{enc}_k(m)] = \sum_{k \in K} \mathbb{P}[c \leftarrow \text{enc}_k(m')]$$

$\mathbb{P}[c \leftarrow \text{enc}_k(m)]$ is 1 for $k = m \oplus c$ and 0 otherwise. Hence left-hand side is 1 and with same argument also right-hand side is 1. □

Notes

- XOR removes message bias
(ciphertexts uniformly distributed for any message distribution)
- In general $k \leftarrow U_n$; $m \leftarrow P_M$; $c = k \oplus m$ yields uniformly distributed c
($k \leftarrow U_n$ means draw k from uniform distribution on $\{0, 1\}^n$)

Notes

- XOR removes message bias
(ciphertexts uniformly distributed for any message distribution)
- In general $k \leftarrow U_n; m \leftarrow P_M; c = k \oplus m$ yields uniformly distributed c
($k \leftarrow U_n$ means draw k from uniform distribution on $\{0, 1\}^n$)
- XOR used in modern cryptography for this reason

Question

- Are uniformly distributed ciphertexts needed for perfect secrecy?

Definition (§2.5 Perfectly secret)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly secret** if $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ for all messages $m, m' \in \mathcal{M}$ and ciphertexts $c \in \mathcal{C}$

Definition (§2.5 Perfectly secret)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly secret** if $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ for all messages $m, m' \in \mathcal{M}$ and ciphertexts $c \in \mathcal{C}$

Notes

- One-time pad is perfectly secret
- Reveals no information about message from ciphertext (Lemma §2.7)
(length of message already part of scheme)

Definition (§2.5 Perfectly secret)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly secret** if $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ for all messages $m, m' \in \mathcal{M}$ and ciphertexts $c \in \mathcal{C}$

Notes

- One-time pad is perfectly secret
- Reveals no information about message from ciphertext (Lemma §2.7)
(length of message already part of scheme)
- Protocol-based (two-player game) characterization follows
(as preparation for later definitions)
- Stateful algorithms
= algorithms with persistent memory, aware of protocol step

Perfect Indistinguishability

§3.1 Definition (Perfect indistinguishability game)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme and $\mathcal{A}$ stateful probabilistic algorithm. **Adversarial indistinguishability game** $\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})$ is

$\mathcal{A}$ selects messages $m_0, m_1 \in \mathcal{M}$ ①

Perfect Indistinguishability

§3.1 Definition (Perfect indistinguishability game)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme and $\mathcal{A}$ stateful probabilistic algorithm. **Adversarial indistinguishability game** $\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})$ is

- ① $\mathcal{A}$ selects messages $m_0, m_1 \in \mathcal{M}$
- ② $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0, 1\}$
 $c \leftarrow \text{enc}_k(m_b)$ sent to $\mathcal{A}$ (challenge ciphertext)

Perfect Indistinguishability

§3.1 Definition (Perfect indistinguishability game)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme and $\mathcal{A}$ stateful probabilistic algorithm. **Adversarial indistinguishability game** $\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})$ is

- 1 $\mathcal{A}$ selects messages $m_0, m_1 \in \mathcal{M}$
- 2 $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0, 1\}$
 $c \leftarrow \text{enc}_k(m_b)$ sent to $\mathcal{A}$ (challenge ciphertext)
- 3 $\mathcal{A}$ outputs bit $b' \in \{0, 1\}$

Perfect Indistinguishability

§3.1 Definition (Perfect indistinguishability game)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme and $\mathcal{A}$ stateful probabilistic algorithm. **Adversarial indistinguishability game** $\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})$ is

- 1 $\mathcal{A}$ selects messages $m_0, m_1 \in \mathcal{M}$
- 2 $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0, 1\}$
 $c \leftarrow \text{enc}_k(m_b)$ sent to $\mathcal{A}$ (challenge ciphertext)
- 3 $\mathcal{A}$ outputs bit $b' \in \{0, 1\}$
- 4 Return 1 if $b = b'$ ($\mathcal{A}$ wins)
Return 0 otherwise

Perfect Indistinguishability

§3.1 Definition (Perfect indistinguishability game)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme and $\mathcal{A}$ stateful probabilistic algorithm. **Adversarial indistinguishability game** $\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})$ is

- 1 $\mathcal{A}$ selects messages $m_0, m_1 \in \mathcal{M}$
- 2 $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0, 1\}$
 $c \leftarrow \text{enc}_k(m_b)$ sent to $\mathcal{A}$ (challenge ciphertext)
- 3 $\mathcal{A}$ outputs bit $b' \in \{0, 1\}$
- 4 Return 1 if $b = b'$ ($\mathcal{A}$ wins)
Return 0 otherwise

Notes

- 1 Adversary selects messages to be distinguished
- 2 System encrypts randomly selected message with random key
- 3 Adversary predicts which message was encrypted based on ciphertext
- 4 Adversary wins if prediction correct

Perfect Indistinguishability



Alice



Eve

Perfect Indistinguishability



Alice

Messages m_0, m_1



Eve

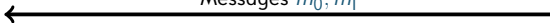
Perfect Indistinguishability



Alice

$k \leftarrow \text{gen}()$
random b

Messages m_0, m_1



Eve

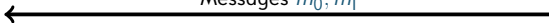
Perfect Indistinguishability



Alice

$k \leftarrow \text{gen}()$
random b
 $c \leftarrow \text{enc}_k(m_b)$

Messages m_0, m_1



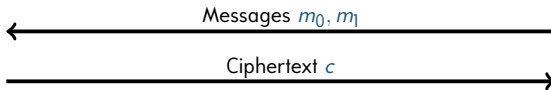
Eve

Perfect Indistinguishability



Alice

$k \leftarrow \text{gen}()$
random b
 $c \leftarrow \text{enc}_k(m_b)$



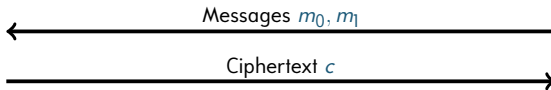
Eve

Perfect Indistinguishability



Alice

$k \leftarrow \text{gen}()$
random b
 $c \leftarrow \text{enc}_k(m_b)$



Eve

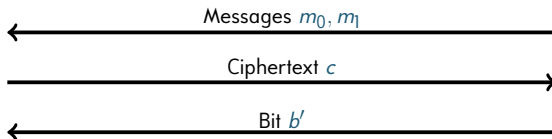
Determines b'

Perfect Indistinguishability



Alice

$k \leftarrow \text{gen}()$
random b
 $c \leftarrow \text{enc}_k(m_b)$



Eve

Determines b'

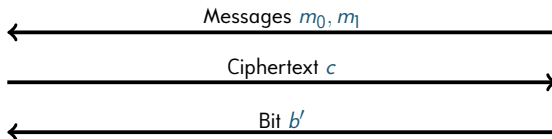
Perfect Indistinguishability



Alice

$k \leftarrow \text{gen}()$
random b
 $c \leftarrow \text{enc}_k(m_b)$

Return $b \stackrel{?}{=} b'$



Eve

Determines b'

Perfect Indistinguishability

Standard function reformulation

Definition (§3.1 Perfect indistinguishability game)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme, $m_0, m_1 \in \mathcal{M}$ messages, and $f: \mathcal{M}^2 \times \mathcal{C} \rightarrow \{0, 1\}$. **Adversarial indistinguishability game**
 $\text{PrivK}^{\text{one}}(\mathcal{E}, m_0, m_1, f)$ is

- ① $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0, 1\}$
 $c \leftarrow \text{enc}_k(m_b)$
- ② $b' \leftarrow f(m_0, m_1, c)$
- ③ Return 1 if $b = b'$ (f wins)
Return 0 otherwise

§3.2 Definition (Perfectly indistinguishable)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly indistinguishable** if for every probabilistic algorithm $\mathcal{A}$

$$\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] = \frac{1}{2}$$

§3.2 Definition (Perfectly indistinguishable)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly indistinguishable** if for every probabilistic algorithm $\mathcal{A}$

$$\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] = \frac{1}{2}$$

Notes

- $\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})]$ = probability that $\mathcal{A}$ wins game
- $\mathcal{A}$ can trivially win 50% of games by returning uniform random bit b'
- Perfectly indistinguishable = $\mathcal{A}$ cannot do better (or worse)

Perfect Indistinguishability

Standard function reformulation

Definition (§3.2 Perfectly indistinguishable)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly indistinguishable** if for all $m_0, m_1 \in \mathcal{M}$ and functions $f: \mathcal{M}^2 \times \mathcal{C} \rightarrow \{0, 1\}$

$$\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, m_0, m_1, f)] = \frac{1}{2}$$

Perfect Indistinguishability

Standard function reformulation

Definition (§3.2 Perfectly indistinguishable)

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is **perfectly indistinguishable** if for all $m_0, m_1 \in \mathcal{M}$ and functions $f: \mathcal{M}^2 \times \mathcal{C} \rightarrow \{0, 1\}$

$$\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, m_0, m_1, f)] = \frac{1}{2}$$

Notes

- We stick to stateful algorithms in following
- Cleaner grouping of selections (avoid quantifiers on m_0, m_1)

Perfect Indistinguishability

Example: Shift cipher $\mathcal{E}$

- Adversary $\mathcal{A}$ selects messages $m_0 = aa$ and $m_1 = ab$
- Adversary $\mathcal{A}$ receives ciphertext $c = c_1c_2$
 - ▶ Returns 0 if $c_1 = c_2$
 - ▶ Returns 1 otherwise

Perfect Indistinguishability

Example: Shift cipher $\mathcal{E}$

- Adversary $\mathcal{A}$ selects messages $m_0 = aa$ and $m_1 = ab$
- Adversary $\mathcal{A}$ receives ciphertext $c = c_1c_2$
 - ▶ Returns 0 if $c_1 = c_2$
 - ▶ Returns 1 otherwise

$$\begin{aligned} & \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] \\ &= \frac{1}{2} \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 0] + \frac{1}{2} \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 1] \end{aligned}$$

Perfect Indistinguishability

Example: Shift cipher $\mathcal{E}$

- Adversary $\mathcal{A}$ selects messages $m_0 = aa$ and $m_1 = ab$
- Adversary $\mathcal{A}$ receives ciphertext $c = c_1c_2$
 - ▶ Returns 0 if $c_1 = c_2$
 - ▶ Returns 1 otherwise

$$\begin{aligned} & \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] \\ &= \frac{1}{2}\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 0] + \frac{1}{2}\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 1] \\ &= \frac{1}{2}\mathbb{P}[c_1 = c_2 \mid b = 0] + \frac{1}{2}\mathbb{P}[c_1 \neq c_2 \mid b = 1] \\ &= \frac{1}{2} + \frac{1}{2} = 1 > \frac{1}{2} \end{aligned}$$

Perfect Indistinguishability

Example: Shift cipher $\mathcal{E}$

- Adversary $\mathcal{A}$ selects messages $m_0 = aa$ and $m_1 = ab$
- Adversary $\mathcal{A}$ receives ciphertext $c = c_1c_2$
 - ▶ Returns 0 if $c_1 = c_2$
 - ▶ Returns 1 otherwise

$$\begin{aligned} & \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] \\ &= \frac{1}{2} \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 0] + \frac{1}{2} \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 1] \\ &= \frac{1}{2} \mathbb{P}[c_1 = c_2 \mid b = 0] + \frac{1}{2} \mathbb{P}[c_1 \neq c_2 \mid b = 1] \\ &= \frac{1}{2} + \frac{1}{2} = 1 > \frac{1}{2} \end{aligned}$$

→ Shift cipher not perfectly indistinguishable

§3.3 Theorem

Encryption scheme is perfectly secret iff it is perfectly indistinguishable

Perfect Indistinguishability

§3.3 Theorem

Encryption scheme is perfectly secret iff it is perfectly indistinguishable

Proof (1/2)

($\rightarrow$) Let $\mathcal{A}$ be prob. algorithm, $r \in R$, and $m_0, m_1 \in \mathcal{M}$ selected messages. Moreover, let $C_b = \{c \in C \mid \mathcal{A}_r(c) = b\}$ for all $b \in \{0, 1\}$. Obviously $C = C_0 \cup C_1$. ($\mathcal{A}_r$ is de-randomized version of $\mathcal{A}$)

Perfect Indistinguishability

§3.3 Theorem

Encryption scheme is perfectly secret iff it is perfectly indistinguishable

Proof (1/2)

($\rightarrow$) Let $\mathcal{A}$ be prob. algorithm, $r \in R$, and $m_0, m_1 \in \mathcal{M}$ selected messages. Moreover, let $C_b = \{c \in C \mid \mathcal{A}_r(c) = b\}$ for all $b \in \{0, 1\}$. Obviously $C = C_0 \cup C_1$. ($\mathcal{A}_r$ is de-randomized version of $\mathcal{A}$)

$$P[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}_r)] = \frac{1}{2}P[\mathcal{A}_r(c) = 0 \mid b = 0] + \frac{1}{2}P[\mathcal{A}_r(c) = 1 \mid b = 1]$$

Perfect Indistinguishability

§3.3 Theorem

Encryption scheme is perfectly secret iff it is perfectly indistinguishable

Proof (1/2)

($\rightarrow$) Let $\mathcal{A}$ be prob. algorithm, $r \in R$, and $m_0, m_1 \in \mathcal{M}$ selected messages. Moreover, let $C_b = \{c \in C \mid \mathcal{A}_r(c) = b\}$ for all $b \in \{0, 1\}$. Obviously $C = C_0 \cup C_1$. ($\mathcal{A}_r$ is de-randomized version of $\mathcal{A}$)

$$\begin{aligned} P[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}_r)] &= \frac{1}{2}P[\mathcal{A}_r(c) = 0 \mid b = 0] + \frac{1}{2}P[\mathcal{A}_r(c) = 1 \mid b = 1] \\ &= \frac{1}{2} \left(\sum_{c \in C_0} O_{\mathcal{E}}(c, m_0) \right) + \frac{1}{2} \left(\sum_{c \in C_1} O_{\mathcal{E}}(c, m_1) \right) \\ &= \frac{1}{2} \sum_{c \in C} O_{\mathcal{E}}(c, m_0) = \frac{1}{2} \end{aligned}$$

Perfect Indistinguishability

Proof (2/2)

($\leftarrow$) Suppose that $\mathcal{E}$ is not perfectly secret. Then there exist messages $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$ such that $O_{\mathcal{E}}(c, m_0) \neq O_{\mathcal{E}}(c, m_1)$.

Perfect Indistinguishability

Proof (2/2)

($\leftarrow$) Suppose that $\mathcal{E}$ is not perfectly secret. Then there exist messages $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$ such that $O_{\mathcal{E}}(c, m_0) \neq O_{\mathcal{E}}(c, m_1)$. Consider adversary $\mathcal{A}$ that selects messages m_0, m_1 and then receives ciphertext $c' \in \mathcal{C}$. If $c = c'$, then $\mathcal{A}$ returns $b' = 0$. Otherwise it returns uniform random bit b' .

Perfect Indistinguishability

Proof (2/2)

($\leftarrow$) Suppose that $\mathcal{E}$ is not perfectly secret. Then there exist messages $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$ such that $O_{\mathcal{E}}(c, m_0) \neq O_{\mathcal{E}}(c, m_1)$. Consider adversary $\mathcal{A}$ that selects messages m_0, m_1 and then receives ciphertext $c' \in \mathcal{C}$. If $c = c'$, then $\mathcal{A}$ returns $b' = 0$. Otherwise it returns uniform random bit b' .

$$\mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] = \frac{1}{2}\mathbb{P}[b' = 0 \mid b = 0] + \frac{1}{2}\mathbb{P}[b' = 1 \mid b = 1]$$



Perfect Indistinguishability

Proof (2/2)

($\leftarrow$) Suppose that $\mathcal{E}$ is not perfectly secret. Then there exist messages $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$ such that $O_{\mathcal{E}}(c, m_0) \neq O_{\mathcal{E}}(c, m_1)$. Consider adversary $\mathcal{A}$ that selects messages m_0, m_1 and then receives ciphertext $c' \in \mathcal{C}$. If $c = c'$, then $\mathcal{A}$ returns $b' = 0$. Otherwise it returns uniform random bit b' .

$$\begin{aligned} \mathbb{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] &= \frac{1}{2}\mathbb{P}[b' = 0 \mid b = 0] + \frac{1}{2}\mathbb{P}[b' = 1 \mid b = 1] \\ &= \frac{1}{2}\left(\frac{1}{2}\mathbb{P}[c' \neq c \mid b = 0] + \mathbb{P}[c' = c \mid b = 0]\right) + \frac{1}{4}\mathbb{P}[c' \neq c \mid b = 1] \end{aligned}$$



Perfect Indistinguishability

Proof (2/2)

($\leftarrow$) Suppose that $\mathcal{E}$ is not perfectly secret. Then there exist messages $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$ such that $O_{\mathcal{E}}(c, m_0) \neq O_{\mathcal{E}}(c, m_1)$. Consider adversary $\mathcal{A}$ that selects messages m_0, m_1 and then receives ciphertext $c' \in \mathcal{C}$. If $c = c'$, then $\mathcal{A}$ returns $b' = 0$. Otherwise it returns uniform random bit b' .

$$\begin{aligned} \text{P}[\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})] &= \frac{1}{2}\text{P}[b' = 0 \mid b = 0] + \frac{1}{2}\text{P}[b' = 1 \mid b = 1] \\ &= \frac{1}{2} \left(\frac{1}{2}\text{P}[c' \neq c \mid b = 0] + \text{P}[c' = c \mid b = 0] \right) + \frac{1}{4}\text{P}[c' \neq c \mid b = 1] \\ &= \frac{1}{4} \left(1 - O_{\mathcal{E}}(c, m_0) \right) + \frac{1}{2} O_{\mathcal{E}}(c, m_0) + \frac{1}{4} \left(1 - O_{\mathcal{E}}(c, m_1) \right) \\ &= \frac{1}{4} \left(2 + \underbrace{O_{\mathcal{E}}(c, m_0) - O_{\mathcal{E}}(c, m_1)}_{\neq 0} \right) \neq \frac{1}{2} \end{aligned}$$

□

§3.4 Theorem

If $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly secret, then $|K| \geq |M|$

§3.4 Theorem

If $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly secret, then $|K| \geq |M|$

Proof

By contraposition: Let $|K| < |M|$ and thus K is finite. Clearly, $|K| \geq 1$, so take $k \in \text{ran}(\text{gen})$. Similarly, take $r \in R$ and $m \in M$ arbitrarily. Let $c = \text{enc}(r, k, m)$, so $P(k) \cdot P[c \leftarrow \text{enc}_k(m)] \neq 0$.

Limits of Perfect Secrecy

§3.4 Theorem

If $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly secret, then $|K| \geq |M|$

Proof

By contraposition: Let $|K| < |M|$ and thus K is finite. Clearly, $|K| \geq 1$, so take $k \in \text{ran}(\text{gen})$. Similarly, take $r \in R$ and $m \in M$ arbitrarily. Let $c = \text{enc}(r, k, m)$, so $P(k) \cdot P[c \leftarrow \text{enc}_k(m)] \neq 0$. Select $M' \subseteq M$ of size $|K| + 1$ arbitrarily such that $m \in M'$. Consider scenario $(\mathcal{E}, P_M)$ with uniform distribution on M' . Then $P(k) \cdot P(m) \cdot P[c \leftarrow \text{enc}_k(m)] \neq 0$ and hence $P(c) \neq 0$.

Limits of Perfect Secrecy

§3.4 Theorem

If $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly secret, then $|K| \geq |M|$

Proof

By contraposition: Let $|K| < |M|$ and thus K is finite. Clearly, $|K| \geq 1$, so take $k \in \text{ran}(\text{gen})$. Similarly, take $r \in R$ and $m \in M$ arbitrarily. Let $c = \text{enc}(r, k, m)$, so $P(k) \cdot P[c \leftarrow \text{enc}_k(m)] \neq 0$. Select $M' \subseteq M$ of size $|K| + 1$ arbitrarily such that $m \in M'$. Consider scenario $(\mathcal{E}, P_M)$ with uniform distribution on M' . Then $P(k) \cdot P(m) \cdot P[c \leftarrow \text{enc}_k(m)] \neq 0$ and hence $P(c) \neq 0$. Let $M'' = \{\text{dec}_{k'}(c) \mid k' \in K\}$. Obviously $|M''| \leq |K| < |M'|$. Hence there exists $m' \in M' \setminus M''$.

$$P(m' \mid c) = 0 \neq \frac{1}{|K| + 1} = P(m')$$

so $\mathcal{E}$ is not perfectly secret by Lemma §2.7. □

Limits of Perfect Secrecy

Consequences

- Perfect secrecy requires at least as many keys as there are messages
($\rightarrow$ perfect secrecy impractical)
- One-time pad achieves optimal $|K| = |M|$

Questions

- Can keys be reused?
(Is one-time pad still perfectly secret
if multiple messages are encrypted with the same key?)
- Are there other optimal perfectly secret encryption schemes?

§3.5 Theorem (Shannon's theorem)

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ encryption scheme with $|K| = |M| = |C| = \ell \in \mathbb{N}$.
Then $\mathcal{E}$ is perfectly secret iff

- $P_K(k) = \ell^{-1}$ for every $k \in K$ (uniform key distribution)
- For every $m \in M$ and $c \in C$ there exists unique $k \in K$ such that $P[c \leftarrow \text{enc}_k(m)] \neq 0$
(det. encryption and $\text{enc}(\cdot, m): K \rightarrow C$ bijective for every $m \in M$)

Claude Elwood Shannon (* 1916; † 2001)

- US mathematician & electrical engineer
- Father of information theory
- Alfred-Nobel-laureate (1939), but not Nobel-laureate (different Alfred)



© Konrad Jacobs

Summary

- Perfect indistinguishability
- Limits of perfect secrecy