Introduction to Modern Cryptography

Michele Ciampi

(Slides courtesy of Prof. Jonathan Katz)

Lecture 4, part 2

Perfect Indistinguishability

Perfect Secrecy (PS)

Is the notion too strong?

PS requires that absolutely **no information** about the plaintext is leaked, even to eavesdroppers with **unlimited computational power**

- Has some inherent drawbacks
- Seems **unnecessarily strong**

Computational Secrecy (CS)

A weaker, yet practical notion

- Still fine if a scheme **leaks information** with tiny probability to eavesdroppers with **bounded computational resources**
- i.e. we can **relax perfect secrecy** by
  1. Allowing security to "fail" with tiny probability
  2. Restricting attention to "efficient" attackers

Tiny probability of failure?

- Say security fails with probability $\mathbf{2^{-60}}$
- Should we be concerned about this?
- With probability $> \mathbf{2^{-60}}$, the sender and receiver will both be struck by lightning in the next year...
- Something that occurs with probability $\mathbf{2^{-60}}$/sec is expected to occur once every **100** billion years

Bounded attackers?

- Consider brute-force search of key space; assume one key can be tested per clock cycle
- Desktop computer $\approx \mathbf{2^{57}}$ keys/year
- Supercomputer $\approx \mathbf{2^{80}}$ keys/year
- Supercomputer since Big Bang $\approx \mathbf{2^{112}}$ keys
- Therefore restricting attention to attackers who can try $\mathbf{2^{112}}$ keys is fine!
- Modern key space: $\mathbf{2^{128}}$ keys or more...

An Equivalent Definition of Perfect Secrecy

- We will give an alternate (but equivalent) definition of PS
  - Using a randomized experiment
- That definition has a **natural relaxation** to **computational secrecy**

Perfect Indistinguishability (PI)

Fix message $\boldsymbol{m} \in \boldsymbol{\mathcal{M}}$ and vary $\boldsymbol{k} \in \boldsymbol{\mathcal{K}}$ to get *PD* over $\boldsymbol{\mathcal{C}}$ denoted $\boldsymbol{D_m}$.

Definition

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\boldsymbol{\mathcal{M}}$ satisfies **perfect indistinguishability** if

$$\forall \boldsymbol{m_0} \neq \boldsymbol{m_1} \in \boldsymbol{\mathcal{M}} : \ \boldsymbol{D_{m_0}} = \boldsymbol{D_{m_1}}$$

i.e. the distributions $\boldsymbol{D_{m_0}}$ and $\boldsymbol{D_{m_1}}$ are identical.

Perfect Indistinguishability

$\mathsf{PrivK}_{A,\Pi}$

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\mathcal{M}$, and A an adversary. Define a randomized experiment $\mathsf{PrivK}_{A,\Pi}$:

1. A outputs $m_0, m_1 \in \mathcal{M}$
2. $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0, 1\}$, $c \leftarrow \mathsf{Enc}_k(m_b)$ (challenge)
3. $b' \leftarrow A(c)$
4. Adversary A succeeds if $b = b'$, and we say the experiment evaluates to 1 in this case

Perfect Indistinguishability

$\mathbf{\Pi}$ is **perfectly indistinguishable** if for **all** attackers (algorithms) $\boldsymbol{A}$, it holds that

$$\mathbf{Pr}[\mathsf{PrivK}_{\boldsymbol{A},\mathbf{\Pi}} = \mathbf{1}] = \frac{\mathbf{1}}{\mathbf{2}}$$

Note

Easy to succeed with probability $\mathbf{1/2}$, just pick randomly $\boldsymbol{b}$

Perfect Indistinguishability

Theorem

$\mathbf{\Pi}$ *is perfectly indistinguishable* $\iff$ $\mathbf{\Pi}$ *is perfectly secret*

i.e. perfect indistinguishability is just an alternate definition of perfect secrecy

Perfect Secrecy (recall)

Definition

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\boldsymbol{\mathcal{M}}$ and ciphertext space $\boldsymbol{\mathcal{C}}$ is **perfectly secret** if $\forall PD$ over $\boldsymbol{\mathcal{M}}$, $\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}$, and $\forall \boldsymbol{c} \in \boldsymbol{\mathcal{C}}$ with $\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c}] > \mathbf{0}$, it holds that

$$\mathbf{Pr}[\boldsymbol{M} = \boldsymbol{m} | \boldsymbol{C} = \boldsymbol{c}] = \mathbf{Pr}[\boldsymbol{M} = \boldsymbol{m}]$$

i.e. the distribution of $\boldsymbol{M}$ does not change conditioned on observing the ciphertext

Sufficient and Necessary Condition for PS

Lemma

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with message space* $\boldsymbol{\mathcal{M}}$ *and ciphertext space* $\boldsymbol{\mathcal{C}}$ *is* **perfectly secret** *if and only if* $\forall PD$ *over* $\boldsymbol{\mathcal{M}}$, $\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}$, *and* $\forall \boldsymbol{c} \in \boldsymbol{\mathcal{C}}$ *, it holds that*

$$\mathbf{Pr}[C = \boldsymbol{c} | M = \boldsymbol{m}] = \mathbf{Pr}[C = \boldsymbol{c}]$$

Sufficient and Necessary Condition for PS

Proof.

- ($\implies$) let $\mathbf{Pr}[C = c | M = m] = \mathbf{Pr}[C = c]$
- By Bayes's rule:

$$\mathbf{Pr}[C = c | M = m] = \frac{\mathbf{Pr}[M = m | C = c] \, \mathbf{Pr}[C = c]}{\mathbf{Pr}[M = m]}$$

$$\cancel{\mathbf{Pr}[C = c]} = \frac{\mathbf{Pr}[M = m | C = c] \, \cancel{\mathbf{Pr}[C = c]}}{\mathbf{Pr}[M = m]}$$

$$\mathbf{Pr}[M = m] = \mathbf{Pr}[M = m | C = c]$$

- $\implies$ $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is PS

Sufficient and Necessary Condition for PS

Proof.

- ($\Longleftarrow$) let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be PS i.e.

$$\mathbf{Pr}[M = m | C = c] = \mathbf{Pr}[M = m]$$

- By Bayes's rule, analogously:

$$\mathbf{Pr}[M = m | C = c] = \frac{\mathbf{Pr}[C = c | M = m]\,\mathbf{Pr}[M = m]}{\mathbf{Pr}[C = c]}$$

$$\cancel{\mathbf{Pr}[M = m]} = \frac{\mathbf{Pr}[C = c | M = m]\,\cancel{\mathbf{Pr}[M = m]}}{\mathbf{Pr}[C = c]}$$

- $\Longrightarrow \mathbf{Pr}[C = c] = \mathbf{Pr}[C = c | M = m]$

$\square$

Perfect Indistinguishability

Theorem

$\mathbf{\Pi}$ *is perfectly indistinguishable* $\iff$ $\mathbf{\Pi}$ *is perfectly secret*

Perfect Indistinguishability

Proof.

- $(\implies)$ $\mathbf{\Pi}$ is perfectly secret
- By the PS Lemma:

$$\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}, \boldsymbol{c} \in \boldsymbol{\mathcal{C}}: \ \mathbf{Pr}[C = \boldsymbol{c} | M = \boldsymbol{m}] = \mathbf{Pr}[C = \boldsymbol{c}]$$

- Therefore $\forall \boldsymbol{m_0} \neq \boldsymbol{m_1} \in \boldsymbol{\mathcal{M}}$:

$$\mathbf{Pr}[C = \boldsymbol{c} | M = \boldsymbol{m_0}] = \mathbf{Pr}[C = \boldsymbol{c}]$$
$$\mathbf{Pr}[C = \boldsymbol{c} | M = \boldsymbol{m_1}] = \mathbf{Pr}[C = \boldsymbol{c}]$$

- $\implies \mathbf{Pr}[C = \boldsymbol{c} | M = \boldsymbol{m_0}] = \mathbf{Pr}[C = \boldsymbol{c} | M = \boldsymbol{m_1}]$
- i.e. $\mathbf{\Pi}$ is perfectly indistinguishable

Perfect Indistinguishability

Proof.

- **($\Longleftarrow$) $\boldsymbol{\Pi}$** is perfectly indistinguishable
- Fix $\boldsymbol{m_0} \in \boldsymbol{\mathcal{M}}$ and $\boldsymbol{c} \in \boldsymbol{\mathcal{C}}$
- Denote

$$\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c} | \boldsymbol{M} = \boldsymbol{m_0}] = \boldsymbol{p}$$

- Since $\boldsymbol{\Pi}$ is PI, $\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}$:

$$\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c} | \boldsymbol{M} = \boldsymbol{m}] = \mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c} | \boldsymbol{M} = \boldsymbol{m_0}] = \boldsymbol{p}$$

Perfect Indistinguishability

Proof.

- By the law of total probability:

$$\begin{aligned}\mathbf{Pr}[C = c] &= \sum_{m \in \mathcal{M}} \mathbf{Pr}[C = c | M = m]\, \mathbf{Pr}[M = m] \\ &= \sum_{m \in \mathcal{M}} p\, \mathbf{Pr}[M = m] \\ &= p \sum_{m \in \mathcal{M}} \mathbf{Pr}[M = m] \\ &= p \\ &= \mathbf{Pr}[C = c | M = m_0]\end{aligned}$$

- $\implies \mathbf{Pr}[C = c] = \mathbf{Pr}[C = c | M = m_0]$

Perfect Indistinguishability

Proof.

- Since $\boldsymbol{m_0}$ – chosen arbitrary, by the PS Lemma:

$$\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}, \boldsymbol{c} \in \boldsymbol{\mathcal{C}}: \ \mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c} | \boldsymbol{M} = \boldsymbol{m}] = \mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c}]$$

- i.e. $\mathbf{\Pi}$ is perfectly secret

□

So far

- Introduced perfect secrecy (PS)
- Introduced OTP and proved that it satisfies PS
- Described the two limitations of the OTP
- Introduced perfect indistinguishability (PI)
- Proved that PI is equivalent to PS
- Next lecture: relax PI to computational secrecy (CS)
  - a weaker, yet practical notion of security

End

References: From the last paragraph of Pag. 30 until Pag. 32.