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**
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 $2^{-60}$
- Should we be concerned about this?
- With probability $> 2^{-60}$, the sender and receiver will both be struck by lightning in the next year...
- Something that occurs with probability $2^{-60}/\text{sec}$ 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 \( \approx 2^{57} \) keys/year
- Supercomputer \( \approx 2^{80} \) keys/year
- Supercomputer since Big Bang \( \approx 2^{112} \) keys
- Therefore restricting attention to attackers who can try \( 2^{112} \) keys is fine!
- Modern key space: \( 2^{128} \) 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 \( m \in \mathcal{M} \) and vary \( k \in \mathcal{K} \) to get \( PD \) over \( \mathcal{C} \) denoted \( D_m \).

Definition

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

\[
\forall m_0 \neq m_1 \in \mathcal{M} : D_{m_0} = D_{m_1}
\]

i.e. the distributions \( D_{m_0} \) and \( D_{m_1} \) are identical.
Perfect Indistinguishability

**PrivK_{A,\Pi}**

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

1. $A$ outputs $m_0, m_1 \in \mathcal{M}$
2. $k \leftarrow \text{Gen}$, $b \leftarrow \{0, 1\}$, $c \leftarrow \text{Enc}_k(m_b)$ (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

\( \Pi \) is perfectly indistinguishable if for all attackers (algorithms) \( A \), it holds that

\[
\Pr[\text{PrivK}_A, \Pi = 1] = \frac{1}{2}
\]

Note

Easy to succeed with probability \( 1/2 \), just pick randomly \( b \)
Perfect Indistinguishability

Theorem

\[ \Pi \text{ is perfectly indistinguishable} \iff \Pi \text{ is perfectly secret} \]

i.e. perfect indistinguishability is just an alternate definition of perfect secrecy
Perfect Secrecy (recall)

**Definition**

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

\[
\Pr[M = m | C = c] = \Pr[M = m]
\]

i.e. the distribution of \(M\) does not change conditioned on observing the ciphertext
Sufficient and Necessary Condition for PS

Lemma

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

\[
\Pr[C = c | M = m] = \Pr[C = c]
\]
Sufficient and Necessary Condition for PS

Proof.

- \((\iff)\) let \(\Pr[C = c|M = m] = \Pr[C = c]\)
- By Bayes’s rule:

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

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

\[
\Pr[M = m] = \Pr[M = m|C = c]
\]

- \(\iff\) (Gen, Enc, Dec) is PS
Sufficient and Necessary Condition for PS

Proof.

- (⇐) let \((\text{Gen}, \text{Enc}, \text{Dec})\) be PS i.e.

\[
\Pr[M = m | C = c] = \Pr[M = m]
\]

- By Bayes’s rule, analogously:

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

\[
\Pr[M = \overline{m}] = \frac{\Pr[C = c | M = m] \Pr[M = \overline{m}]}{\Pr[C = c]}
\]

- \(\implies \Pr[C = c] = \Pr[C = c | M = m]\)
Perfect Indistinguishability

**Theorem**

\( \Pi \) is perfectly indistinguishable \( \iff \) \( \Pi \) is perfectly secret
Perfect Indistinguishability

Proof.

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

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

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

\[ \Pr[C = c|M = m_0] = \Pr[C = c] \]
\[ \Pr[C = c|M = m_1] = \Pr[C = c] \]

- $\implies \Pr[C = c|M = m_0] = \Pr[C = c|M = m_1]$
- i.e. $\Pi$ is perfectly indistinguishable
Perfect Indistinguishability

Proof.

- $(\iff)$ $\Pi$ is perfectly indistinguishable
- Fix $m_0 \in \mathcal{M}$ and $c \in \mathcal{C}$
- Denote
  \[
  \Pr[C = c|M = m_0] = p
  \]
- Since $\Pi$ is PI, $\forall m \in \mathcal{M}$:
  \[
  \Pr[C = c|M = m] = \Pr[C = c|M = m_0] = p
  \]
Perfect Indistinguishability

Proof.

By the law of total probability:

\[
\Pr[C = c] = \sum_{m \in M} \Pr[C = c | M = m] \Pr[M = m]
\]

\[
= \sum_{m \in M} p \Pr[M = m]
\]

\[
= p \sum_{m \in M} \Pr[M = m]
\]

\[
= p
\]

\[
= \Pr[C = c | M = m_0]
\]

\[
\implies \Pr[C = c] = \Pr[C = c | M = m_0]
\]
Perfect Indistinguishability

Proof.

▶ Since $m_0$ – chosen arbitrary, by the PS Lemma:

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

▶ i.e. $\Pi$ 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.