Cryptology 18th August 2015

Lecture 4: Perfect Secrecy: Several Equivalent Formulations

Instructor: Goutam Paul *Scribe: Arka Rai Choudhuri*

1 Notation

We shall be using the following notation for this lecture,

$\mathcal{M}$	−The set of all possible messages
$\mathcal{C}$	−The set of all possible ciphertexts
$\mathcal{K}$	−The set of all possible keys
$m \in \mathcal{M}$	−A specific message over $\mathcal{M}$
$c \in \mathcal{C}$	−A specific message over $\mathcal{C}$
$k \in \mathcal{K}$	−A specific message over $\mathcal{K}$
M, K, C	−Random variables over $\mathcal{M}, \mathcal{K}$ and $\mathcal{C}$ respectively
$\mathsf{enc}_k(m) = c$	−Encryption of m with the key k to give ciphertext c
$\xleftarrow{\$}$	−chosen uniformly at random

2 Perfect Secrecy

Definition 2.1 *An encryption scheme* (Enc, Dec) *over a message space* $\mathcal{M}$ *is* **perfectly secure** *if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$ *and every ciphertext* $c \in \mathcal{C}$ *for which* $\Pr[C = c] > 0$*:*

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

The following theorem gives an equivalent formulation of 2.1.

Theorem 2.2 *An encryption scheme* (Enc, Dec) *over a message space* $\mathcal{M}$ *is* **perfectly secure** *if and only if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$ *and every ciphertext* $c \in \mathcal{C}$*:*

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

Proof. Firstly, suppose for every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$,

$$\Pr[C = c \mid M = m] \;=\; \Pr[C = c] \tag{1}$$

By Bayes' theorem,

$$\Pr[C = c \mid M = m] \;=\; \frac{\Pr[M = m \mid C = c] \cdot \Pr[C = c]}{\Pr[M = m]} \tag{2}$$

From (3) and (2), we get

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

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

For the other way, we assume perfect secrecy, and hence, for every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$,

$$\Pr[M = m \mid C = c] = \Pr[M = m] \tag{3}$$

again, by Bayes' theorem, and similar to the above proof, we get

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

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

Hence, proved in both directions. □

3 Perfect Indistinguishability

We fix a message m and vary the key over the key space $\mathcal{K}$, to get get a distribution of ciphertexts. This is represented either as $\mathsf{enc}_K(m)$ or D_m.

Definition 3.1 *An encryption scheme* (Enc, Dec) *over a message space* $\mathcal{M}$ *is said to have the property of* **perfect indistinguishability** *if* $\forall\ m_0 \neq m_1 \in \mathcal{M}$, D_{m_0} *and* D_{m_1} *are identical.*

This is just another way of saying that the ciphertext contains no information about the plaintext.

Theorem 3.2 *An encryption scheme* (Enc, Dec) *over a message space* $\mathcal{M}$ *is* **perfectly secure** *if and only if it has* **perfect indistinguishability**.

Proof. (I) Perfect secrecy ⇒ perfect indistinguishability
We know by Theorem 2.2,

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

The above equation implies,

$$\Pr[C = c \mid M = m_0] = \Pr[C = c] \tag{4}$$
$$\Pr[C = c \mid M = m_1] = \Pr[C = c] \tag{5}$$

From the above two equations, we get

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

Since the choice of m_0, m_1 were arbitrary, this trivially implies that D_{m_0} and D_{m_1} are indistinguishabile. This implies perfect indistinguishability.
(II) Perfect indistinguishability $\Rightarrow$ perfect secrecy
Fix $m_0 \in \mathcal{M}$ and $c \in \mathcal{C}$. Let $\Pr[C = c \mid M = m_0] = p$. Since $\Pr[C = c \mid M = m] = \Pr[C = c \mid M = m_0] = p$ for all m because of perfect indistinguishability, we have

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

Since m_0 was arbitrary, we have shown $\Pr[C = c] = \Pr[C = c \mid M = m]$ for all $c \in \mathcal{C}$ and $m \in \mathcal{M}$. $\therefore$ from Theorem 2.2, this implies perfect secrecy. □

4 Adverserial indistinguishability

We define a game $\mathcal{G}^{\text{dist}}_{\mathcal{A},\mathsf{enc}}$ as mentioned in [**?**].
Eavesdropping indistinguishability experiment (game) $\mathcal{G}^{\mathbf{dist}}_{\mathcal{A},\mathsf{enc}}$

1. *The adversary $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.*
2. *A random key k is generated at random from $\mathcal{K}$, and a random bit $b \xleftarrow{\$} \{0,1\}$ is chose. (These are chose by the challenger entity that is running the experiment with $\mathcal{A}$.) Then, a ciphertext $\mathsf{enc}_k(m_b)$ is computed and given to $\mathcal{A}$.*
3. *$\mathcal{A}$ outputs a bit $b' \in \{0,1\}$.*
4. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\mathcal{G}^{dist}_{\mathcal{A},\mathsf{enc}} = 1$ if the output is 1 and in this case we say $\mathcal{A}$ succeeded.*

One should think of $\mathcal{A}$ as trying to guess the value of b that is chosen in the experiment, and $\mathcal{A}$ succeeds when its guess b' is correct.
It should be noted that the key is chosen and does not depend on the messages it receives from the attacker $\mathcal{A}$.
Probability that the adversary $\mathcal{A}$ win,

$$\begin{aligned}
&= \Pr[\mathcal{G}^{\text{dist}}_{\mathcal{A},\mathsf{enc}} = 1] \\
&= \Pr[b = b']
\end{aligned}$$

Definition 4.1 *An encryption scheme* (Enc, Dec) *over a message space $\mathcal{M}$ is said to have* **adversarial indistinguishability** *if*

$$Pr[\mathcal{G}^{dist}_{\mathcal{A},\mathsf{enc}} = 1] = \frac{1}{2}$$

Theorem 4.2 *An encryption scheme* (Enc, Dec) *over a message space* $\mathcal{M}$ *has* **perfect secrecy** *if and only if it has* **adversarial indistinguishability**.

Proof. (I) Perfect secrecy ⇒ adversarial indistinguishability
Note: we make the assumption that the adversary will always guess the same for the same ciphertext, i.e. the adversary is deterministic.

$$\begin{aligned}\Pr[\mathcal{G}^{\text{dist}}_{\mathcal{A},\mathsf{enc}} = 1] &= \Pr[b = b'] \\ &= \Pr[b' = b \mid M = m_0]\Pr[M = m_0] + \Pr[b' = b \mid M = m_1]\Pr[M = m_1]\end{aligned}$$

Essentially what the adversary does is try to partition the ciphertext space $\mathcal{C}$ into two subsets $\mathcal{C}_0, \mathcal{C}_1$ such that $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1$ and $\mathcal{C}_0 \cap \mathcal{C}_1 = \phi$. If the attacker gets $c \in \mathcal{C}_0$, it outputs 0, else if $c \in \mathcal{C}_1$ it outputs 1.

$$\begin{aligned}&\therefore \Pr[b' = b \mid M = m_0]\Pr[M = m_0] + \Pr[b' = b \mid M = m_1]\Pr[M = m_1] \\ &= \Pr[c \in \mathcal{C}_0] \cdot \frac{1}{2} + \Pr[c \in \mathcal{C}_0] \cdot \frac{1}{2} \\ &= \frac{1}{2}\left(\Pr[c \in \mathcal{C}_0] + \Pr[c \in \mathcal{C}_0]\right) \\ &= \frac{1}{2}\end{aligned}$$

From the first to the second, the $\frac{1}{2}$ comes from the fact that $\Pr[M = m_0] = \Pr[M = m_1] = \frac{1}{2}$. The last equality follows from the fact that $\mathcal{C}_0$ and $\mathcal{C}_1$ are mutually exclusive and exhaustive. Hence perfect secrecy implies adversarial indistinguishability.
(II) Adverserial indistinguishability ⇒ perfect secrecy
We prove the contrapositive of the above statement.
Not perfect secrecy ⇒ Not adverserial indistinguishability
By not perfect secrecy, we mean

$$\exists\ m_0', m_1' \in \mathcal{M}, c' \in \mathcal{C}, \text{such that}$$
$$\Pr[C = c' | M = m_0'] \neq \Pr[C = c' | M = m_1']$$

$$\Pr[\mathcal{G}^{\text{dist}}_{\mathcal{A},\mathsf{enc}} = 1] = \Pr[b = b'] = \Pr[b = b' \mid M = m_0']\Pr[M = m_0'] + \Pr[b = b' \mid M = m_1']\Pr[M = m_1'] \tag{6}$$

$$= \frac{1}{2}\left(\Pr[b = b' \mid M = m_0'] + \Pr[b = b' \mid M = m_1']\right) \tag{7}$$

For positive results, we don't care about what the adversary does, but for the negative result we show that there exists at least one adversary for which the probability of success is away from half.
Since there will exist at least one pair m_0' and m_1', that adversary will pick these to work with and hence we can write the above equations.
Construction of adversary
$\mathcal{A}$ chooses m_0', m_1' and gives it to the challenger. If it receives $C = c'$, output $b' = 0$ else

output $b' \xleftarrow{\$} \{0,1\}$
The randomness is to ensure that we can separate out the case when $C = c'$.

$$\begin{aligned}\Pr[b = b' \mid M = m_0'] &= \Pr[C = c' \mid M = m_0']\Pr[b = b' \mid M = m_0', C = c'] \\ &+\Pr[C \neq c' \mid M = m_0']\Pr[b = b' \mid M = m_0', C \neq c'] \\ &= \Pr[C = c' \mid M = m_0'] \cdot 1 + \Pr[C \neq c' \mid M = m_0'] \cdot \frac{1}{2}\end{aligned}$$

$\Pr[b = b' \mid M = m_0', C = c'] = 1$ since $b = 0$, and also $b' = 0$ because $C = c'$ (by definition). Substituting into (7), we get

$$= \frac{1}{2}\left(\Pr[C = c' \mid M = m_0'] + \frac{1}{2} \cdot \Pr[C \neq c' \mid M = m_0'] + \Pr[b = b' \mid M = m_1']\right) \quad (8)$$

Now,

$$\begin{aligned}\Pr[b = b \mid M = m_1'] &= \Pr[C = c' \mid M = m_1']\Pr[b = b' \mid M = m_1', C = c'] \\ &+\Pr[C \neq c' \mid M = m_1']\Pr[b = b' \mid M = m_1', C \neq c'] \\ &= \Pr[C = c' \mid M = m_1'] \cdot 0 + \Pr[C \neq c' \mid M = m_1'] \cdot \frac{1}{2}\end{aligned}$$

The reasoning follows similar to the equation done earlier. We substitute this into (8).

$$\begin{aligned}
&= \frac{1}{2}\left(\Pr[C = c' \mid M = m_0'] + \frac{1}{2} \cdot \Pr[C \neq c' \mid M = m_0'] + \frac{1}{2}\Pr[C \neq c' \mid M = m_1']\right) \\
&= \frac{1}{2}\left(\Pr[C = c' \mid M = m_0'] + \frac{1}{2} \cdot (1 - \Pr[C = c' \mid M = m_0']) + \frac{1}{2}\Pr[C \neq c' \mid M = m_1']\right) \\
&= \frac{1}{4} + \frac{1}{4}\left(\Pr[C = c' \mid M = m_0'] + \Pr[C \neq c' \mid M = m_1']\right) \\
&\neq \frac{1}{4} + \frac{1}{4}\left(\Pr[C = c' \mid M = m_1'] + \Pr[C \neq c' \mid M = m_1']\right) \\
&= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}
\end{aligned}$$

The inequality comes from the fact of *not perfect secrecy* that we have assumed.

$$\therefore \Pr[\mathcal{G}^{\text{dist}}_{\mathcal{A},\mathsf{enc}} = 1] \neq \frac{1}{2}$$

And hence, it does not have adversarial indistinguishability.

□