CS409 - Chalk and Talk: Equivalence of Definitions for Perfect Security in Encryption Schemes

Aadya Pipersenia (20D170002)

1 Introduction

This report examines the equivalence of four different definitions of perfect security in encryption schemes. We will analyze each definition and demonstrate how they are logically connected, ultimately proving their equivalence.

2 Definitions

2.1 Definition 1: Probability Distribution Equality

An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is perfectly secure if for every probability distribution over $\mathcal{M}$, every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\mathbb{P}[C = c] > 0$:

$$\mathbb{P}[M = m | C = c] = \mathbb{P}[M = m]$$

Description: This definition means that the ciphertext gives no additional information about the underlying message. The probability of any message being the original one remains the same even after the ciphertext is revealed. Thus, learning the ciphertext does not change an adversary's guess about the message.

2.2 Definition 2: Ciphertext Independence

An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is perfectly secure if for every probability distribution over $\mathcal{M}$, for every $m', m'' \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

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

Description: This states that the probability of generating a specific ciphertext is independent of the message being encrypted. Regardless of which message is encrypted, the ciphertext distribution remains the same. This ensures that no information about the original message can be inferred from the ciphertext.

2.3 Definition 3: Adversarial Indistinguishability

Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be an encryption scheme with message space $\mathcal{M}$. The encryption scheme is said to be *perfectly indistinguishable* if for every computationally unbounded adversary Eve, it holds that:

$$\Pr\left[\mathsf{Priv}_{\text{Eve},\Pi} = 1\right] = \frac{1}{2},$$

where $\mathsf{Priv}_{\text{Eve},\Pi}$ is defined by the following indistinguishability experiment:

1. **Setup:** The challenger runs the key generation algorithm to obtain a secret key:

$$k \leftarrow \text{Gen}(1^n).$$

2. **Challenge:** The adversary Eve selects two distinct messages $m_0, m_1 \in \mathcal{M}$. The challenger selects a random bit $b \in \{0, 1\}$ and computes the ciphertext:

$$c_b \leftarrow \text{Enc}_k(m_b).$$

   The ciphertext c_b is sent to the adversary.

3. **Guess:** The adversary outputs a guess $b' \in \{0, 1\}$ as to which message was encrypted, based on the received ciphertext c_b.

4. **Winning Condition:** The adversary wins the game if $b' = b$. That is, the adversary correctly guesses which message was encrypted. The outcome of the game is:

$$\mathsf{Priv}_{\text{Eve},\Pi} = \begin{cases} 1 & \text{if } b' = b, \\ 0 & \text{otherwise.} \end{cases}$$

The encryption scheme Π is said to be perfectly indistinguishable (or perfectly secure) if:

$$\Pr\left[\mathsf{Priv}_{\text{Eve},\Pi} = 1\right] = \frac{1}{2},$$

for any adversary Eve. In other words, the adversary's probability of correctly guessing which message was encrypted is no better than random guessing.

2.4 Definition 4: Shannon's Theorem

An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ such that $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ is perfectly secure if and only if:

- Every $k \in \mathcal{K}$ is chosen with (equal) probability $1/|\mathcal{K}|$ by Gen.
- For every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$, there exists a unique key $k \in \mathcal{K}$ such that $\text{Enc}_k(m) = c$.

Description: This definition ensures that each encryption key is chosen uniformly from the set of possible keys, and that each ciphertext uniquely corresponds to a particular key-message pair. This guarantees that the ciphertext is fully determined by the key and message, and thus the encryption is both uniform and deterministic.

3 Proof of Equivalence

3.1 Definition 1 $\Leftrightarrow$ Definition 2

3.1.1 Definition 1 $\Rightarrow$ Definition 2

Assume Definition 1 holds. By Bayes' rule:

$$\begin{aligned} \mathbb{P}[C = c | M = m] &= \frac{\mathbb{P}[M = m | C = c]\mathbb{P}[C = c]}{\mathbb{P}[M = m]} \\ &= \frac{\mathbb{P}[M = m]\mathbb{P}[C = c]}{\mathbb{P}[M = m]} \quad \text{(by Definition 1)} \\ &= \mathbb{P}[C = c] \end{aligned}$$

This holds for all $m \in \mathcal{M}$, proving Definition 2.

3.1.2 Definition 2 ⇒ Definition 1

Assume Definition 2 holds. Again, using Bayes' rule:

$$\begin{aligned}
\mathbb{P}[M = m|C = c] &= \frac{\mathbb{P}[C = c|M = m]\mathbb{P}[M = m]}{\mathbb{P}[C = c]} \\
&= \frac{\mathbb{P}[C = c|M = m_1]\mathbb{P}[M = m]}{\sum_{m' \in \mathcal{M}} \mathbb{P}[C = c|M = m']\mathbb{P}[M = m']} \quad \text{(by Definition 2)} \\
&= \frac{\mathbb{P}[C = c|M = m_1]\mathbb{P}[M = m]}{\mathbb{P}[C = c|M = m_1] \sum_{m' \in \mathcal{M}} \mathbb{P}[M = m']} \\
&= \mathbb{P}[M = m]
\end{aligned}$$

This proves Definition 1. Thus, **Definition 1 and 2 are equivalent**.

3.2 Definition 1 ⇔ Definition 3

3.2.1 Definition 1 ⇒ Definition 3

Assume **Definition 1** holds, i.e., for any message $m \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$, the probability distribution of the message given the ciphertext is the same as the prior distribution:

$$\mathbb{P}[M = m|C = c] = \mathbb{P}[M = m].$$

Now, consider an adversary trying to distinguish between two messages m_1 and m_2 after observing a ciphertext c.

- The adversary receives ciphertext c and must guess whether it corresponds to m_1 or m_2.
- Let p be the adversary's probability of guessing that the ciphertext corresponds to m_1.

Since **Definition 1** states that the probability distribution of the message is unchanged by observing the ciphertext, we know that:

$$\mathbb{P}[M = m_1|C = c] = \mathbb{P}[M = m_1] \quad \text{and} \quad \mathbb{P}[M = m_2|C = c] = \mathbb{P}[M = m_2].$$

If the challenger chooses m_1 and m_2 with equal probability, we have:

$$\mathbb{P}[M = m_1] = \mathbb{P}[M = m_2] = \frac{1}{2}.$$

Thus, after seeing the ciphertext, the adversary gains no additional information about whether the message is m_1 or m_2. The adversary's probability of guessing correctly is:

$$\mathbb{P}[\text{Adversary correct}] = p \cdot \mathbb{P}[M = m_1|C = c] + (1 - p) \cdot \mathbb{P}[M = m_2|C = c].$$

Using **Definition 1**, this simplifies to:

$$\mathbb{P}[\text{Adversary correct}] = p \cdot \mathbb{P}[M = m_1] + (1 - p) \cdot \mathbb{P}[M = m_2].$$

Substituting $\mathbb{P}[M = m_1] = \mathbb{P}[M = m_2] = \frac{1}{2}$:

$$\mathbb{P}[\text{Adversary correct}] = p \cdot \frac{1}{2} + (1 - p) \cdot \frac{1}{2} = \frac{1}{2}.$$

Thus, the adversary has no advantage in distinguishing between m_1 and m_2 after observing the ciphertext, and their probability of guessing correctly remains $\frac{1}{2}$, as required by **Definition 3**.

This proves that **Definition 1** implies **Definition 3**.

3.2.2 Definition 3 ⇒ Definition 1

Now, assume **Definition 3** holds, which means that for any adversary trying to distinguish between two messages m_1 and m_2 after observing a ciphertext c, the adversary's probability of guessing the correct message is $\frac{1}{2}$:

$$\mathbb{P}[\text{Adversary correct}] = \frac{1}{2}.$$

Our goal is to show that this implies **Definition 1**, i.e., for any message m and ciphertext c, we have:

$$\mathbb{P}[M = m|C = c] = \mathbb{P}[M = m].$$

Proof: Consider the same setting as before, where the adversary tries to distinguish between two messages m_1 and m_2. The adversary, given the ciphertext c, guesses that the message is m_1 with some probability p and m_2 with probability $1 - p$.

Since **Definition 3** holds, the adversary gains no advantage from observing the ciphertext c. The probability of correctly guessing the message is $\frac{1}{2}$, regardless of the adversary's strategy. This can be written as:

$$p \cdot \mathbb{P}[M = m_1|C = c] + (1 - p) \cdot \mathbb{P}[M = m_2|C = c] = \frac{1}{2}.$$

Since the adversary's strategy doesn't affect the probability of success, the expression must hold for any p. In particular, it must hold for $p = \frac{1}{2}$, which corresponds to the adversary making a random guess. This gives:

$$\frac{1}{2} \cdot \mathbb{P}[M = m_1|C = c] + \frac{1}{2} \cdot \mathbb{P}[M = m_2|C = c] = \frac{1}{2}.$$

Multiplying both sides by 2, we get:

$$\mathbb{P}[M = m_1|C = c] + \mathbb{P}[M = m_2|C = c] = 1.$$

This equation implies that $\mathbb{P}[M = m_1|C = c]$ and $\mathbb{P}[M = m_2|C = c]$ form a valid probability distribution over m_1 and m_2, given the ciphertext c.

Next, because the adversary's probability of success is exactly $\frac{1}{2}$ and gains no advantage from c, it must be that:

$$\mathbb{P}[M = m_1|C = c] = \mathbb{P}[M = m_1] \quad \text{and} \quad \mathbb{P}[M = m_2|C = c] = \mathbb{P}[M = m_2].$$

More generally, for any message m, the probability $\mathbb{P}[M = m|C = c]$ is independent of c, meaning:

$$\mathbb{P}[M = m|C = c] = \mathbb{P}[M = m].$$

This proves that **Definition 3** implies **Definition 1**. Thus, Definition 1 and 3 are equivalent.
Since **Definition 1 ⇔ Definition 2** and **Definition 1 ⇔ Definition 3**, this implies that all the **Definitions 1, 2 and 3 are equivalent**.

3.3 Definition 4 ⇔ Definition 1

3.3.1 Definition 4 ⇒ Definition 1

Assume that the encryption scheme satisfies the given conditions, and we show that it is perfectly secret.

1. **Condition 1** implies that every key $k \in \mathcal{K}$ is chosen uniformly with probability $1/|\mathcal{K}|$. Therefore, the probability of any particular key being chosen is uniformly distributed.

2. **Condition 2** implies that for every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$, there is a unique key $k \in \mathcal{K}$ such that $\text{Enc}_k(m) = c$. This means any ciphertext c could have been generated from any message m using some key k.

3. Fix an arbitrary ciphertext $c \in \mathcal{C}$ and message $m \in \mathcal{M}$. Let k be the unique key (from Condition 2) such that $\text{Enc}_k(m) = c$. The probability that c is the encryption of m is:

$$\Pr[C = c \mid M = m] = \Pr[K = k] = \frac{1}{|\mathcal{K}|}.$$

4. The probability of any ciphertext $c \in \mathcal{C}$ is then:

$$\Pr[C = c] = \sum_{m \in \mathcal{M}} \Pr[\text{Enc}_K(m) = c] \cdot \Pr[M = m] = \frac{1}{|\mathcal{K}|}.$$

   This holds for any distribution over $\mathcal{M}$.

5. Now, for any $m \in \mathcal{M}$ with $\Pr[M = m] \neq 0$ and any $c \in \mathcal{C}$, we have:

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} = \frac{\frac{1}{|\mathcal{K}|} \cdot \Pr[M = m]}{\frac{1}{|\mathcal{K}|}} = \Pr[M = m].$$

Thus, the scheme satisfies the definition of perfect secrecy: $\Pr[M = m \mid C = c] = \Pr[M = m]$ for any $m \in \mathcal{M}$ and $c \in \mathcal{C}$, **Definition 1**. Therefore, if the encryption scheme satisfies the two conditions, it is perfectly secret. This means Definition 4 implies Definition 1.

Definition 1 $\Rightarrow$ Definition 4

Now, assume the encryption scheme is perfectly secret, which means for any message $m \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$, we have:

$$P(M = m \mid C = c) = P(M = m).$$

We will show that conditions 1 and 2 must hold.

1. Fix an arbitrary ciphertext $c \in \mathcal{C}$. Since the scheme is perfectly secret, for any message $m \in \mathcal{M}$, the ciphertext c must be a possible encryption of m. In other words, there must exist at least one key $k \in \mathcal{K}$ such that $\text{Enc}_k(m) = c$. If no such key existed, $P(C = c \mid M = m) = 0$, which would violate perfect secrecy because $P(M = m \mid C = c) = 0$ would imply $P(M = m) = 0$, which contradicts the assumption that $P(M = m) > 0$.

2. Let $\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}$, and for each $m_i \in \mathcal{M}$, define the set of keys $\mathcal{K}_i \subseteq \mathcal{K}$ such that $\text{Enc}_k(m_i) = c$ if and only if $k \in \mathcal{K}_i$. Since perfect secrecy implies that for every $m \in \mathcal{M}$, each ciphertext $c \in \mathcal{C}$ is equally likely to occur, we have:

$$P(C = c \mid M = m_i) = P(C = c \mid M = m_j) \quad \forall m_i, m_j \in \mathcal{M}.$$

   This means the number of keys that map any message m_i to the ciphertext c must be the same across all messages. Thus, $|\mathcal{K}_i| = |\mathcal{K}_j|$ for all i, j.

3. For perfect secrecy to hold, $\mathcal{K}_i \cap \mathcal{K}_j = \emptyset$ for $i \neq j$, since two different plaintexts cannot map to the same ciphertext under the same key, or else the decryption would be ambiguous, violating correctness. This implies that $\{\mathcal{K}_i\}$ is a partition of the key space $\mathcal{K}$.

4. Since $|\mathcal{K}| = |\mathcal{M}|$, each set $\mathcal{K}_i$ contains exactly one key $k_i \in \mathcal{K}$. Thus, for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$, there is a unique key $k \in \mathcal{K}$ such that $\text{Enc}_k(m) = c$. This satisfies Condition 2.

5. To satisfy perfect secrecy, the probability distribution over the keys must be uniform. If the keys were not uniformly distributed, some ciphertexts would be more likely than others, and perfect secrecy would be violated. Hence, for any $k \in \mathcal{K}$, the probability that k is chosen must be:
$$P(K = k) = \frac{1}{|\mathcal{K}|}.$$
This satisfies Condition 1.

Thus, perfect secrecy implies both Condition 1 and 2 of the Definition 4. Therefore, Definition 1 implies Definition 4. This proves the **equivalence** of **Definition 1 and 4**.

4 Conclusion

This proves the equivalence of all the definitions of Perfect Security. By proving the logical connections between these definitions, we have established that they all describe the same fundamental concept of perfect security.