Proof of Equivalence Between Perfect Secrecy and Perfect Indistinguishability

1 Introduction

This document proves that **perfect secrecy** and **perfect indistinguishability** are equivalent properties for a cipher (G, E, D), where G generates a secret key sk, E encrypts a plaintext $m \in M$ into a ciphertext $c \in C$, and D decrypts c back to m. The proof uses Bayes' theorem to show that the two definitions imply each other.

2 Definitions

Let $\mathcal{M}$ and $\mathcal{C}$ be random variables for the plaintext and ciphertext, respectively.

- **Perfect Secrecy**: For all $m \in M$, $c \in C$, and any probability distribution over M,

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

  This means the ciphertext reveals no information about the plaintext.

- **Perfect Indistinguishability**: For any probability distribution over M, for all $m, m' \in M$, and all $c \in C$,

  $$\Pr_{sk}[\mathcal{C} = c | \mathcal{M} = m] = \Pr_{sk}[\mathcal{C} = c | \mathcal{M} = m'].$$

  This means the ciphertext distribution is the same for any pair of plaintexts.

3 Proof

We use Bayes' theorem:

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

where $\Pr[\mathcal{C} = c] = \sum_{m'' \in M} \Pr[\mathcal{C} = c | \mathcal{M} = m''] \cdot \Pr[\mathcal{M} = m'']$.

3.1 Perfect Secrecy Implies Perfect Indistinguishability

Assume perfect secrecy: $\Pr[\mathcal{M} = m | \mathcal{C} = c] = \Pr[\mathcal{M} = m]$.

Apply Bayes' theorem:

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

Multiply both sides by $\Pr[\mathcal{C} = c] / \Pr[\mathcal{M} = m]$ (assuming $\Pr[\mathcal{M} = m] > 0$):

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

Similarly, for any $m' \in M$:

$$\Pr[\mathcal{C} = c | \mathcal{M} = m'] = \Pr[\mathcal{C} = c].$$

Thus:

$$\Pr[\mathcal{C} = c | \mathcal{M} = m] = \Pr[\mathcal{C} = c | \mathcal{M} = m'],$$

satisfying perfect indistinguishability.

3.2 Perfect Indistinguishability Implies Perfect Secrecy

Assume perfect indistinguishability: $\Pr[\mathcal{C} = c|\mathcal{M} = m] = \Pr[\mathcal{C} = c|\mathcal{M} = m'] = f(c)$ for some function $f(c)$, for all $m, m' \in M$.

Compute $\Pr[\mathcal{C} = c]$:

$$\Pr[\mathcal{C} = c] = \sum_{m'' \in M} \Pr[\mathcal{C} = c|\mathcal{M} = m''] \cdot \Pr[\mathcal{M} = m''] = \sum_{m'' \in M} f(c) \cdot \Pr[\mathcal{M} = m''] = f(c).$$

Apply Bayes' theorem:

$$\Pr[\mathcal{M} = m|\mathcal{C} = c] = \frac{\Pr[\mathcal{C} = c|\mathcal{M} = m] \cdot \Pr[\mathcal{M} = m]}{\Pr[\mathcal{C} = c]} = \frac{f(c) \cdot \Pr[\mathcal{M} = m]}{f(c)} = \Pr[\mathcal{M} = m],$$

assuming $\Pr[\mathcal{C} = c] = f(c) \neq 0$. If $\Pr[\mathcal{C} = c] = 0$, then $\Pr[\mathcal{C} = c|\mathcal{M} = m] = 0$, and the posterior is undefined, but such c never occurs.

Thus, perfect indistinguishability implies perfect secrecy.

4 Conclusion

Perfect secrecy and perfect indistinguishability are equivalent, as each implies the other via Bayes' theorem. A cipher with perfect secrecy ensures the ciphertext reveals no information about the plaintext, equivalent to the ciphertext distribution being identical for all plaintexts.