

# Notes on Information Theoretic Security

Ninghui Li

## 1 Information theoretic security

A cryptosystem is *information-theoretically secure* if its security derives purely from information theory. That is, it is secure even when the adversary has unbounded computing power. No brute-force attack, in fact, no attack except for stealing the key, can break the security.

For ciphers, where one cares about confidentiality, being information-theoretically secure is also known as having *perfect secrecy*: an encryption algorithm has perfect secrecy if a ciphertext produced using it provides no information about the plaintext without knowledge of the key.

Information-theoretic security can be applied in contexts other than encryption, to properties other than confidentiality. For example, one can define information-theoretically secure authenticity (in message authentication code schemes), information-theoretically binding (in cryptographic commitment schemes), and so on. Here we are only concerned with perfect secrecy.

A cipher provides perfect secrecy if and only if for **any** probability distribution from which the plaintext is drawn, and for **any** plaintext-ciphertext pair  $(M_0, C_0)$ , we have

$$\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \Pr[\text{PT} = M_0].$$

That is, after observing the ciphertext is  $C_0$ , the posterior probability that the plaintext is  $M_0$  remains the same as the prior probability that the plaintext is  $M_0$ .

An example of an information-theoretically secure cryptosystem is the one-time pad.

## 2 One-Time Pad

### The One-Time Pad encryption

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$ , where  $\mathcal{M}$  is the plaintext (message) space,  $\mathcal{C}$  is the ciphertext space,  $\mathcal{K}$  is the key space, they are all  $n$ -bit binary strings.
- $\mathbb{K} = K \leftarrow \mathcal{K}$  (meaning that  $K$  is drawn uniformly random from  $\mathcal{K}$ , in other words, each key in  $\mathcal{K}$  is drawn with equal probability).
- $\mathbb{E}_K[M] = \mathbb{E}[K, M] = K \oplus M$ .
- $\mathbb{D}_K[C] = \mathbb{D}[K, C] = K \oplus C$ .

### One-Time Pad has Perfect Secrecy

**Proof.** For any probability distribution from which the plaintext is drawn, for any plaintext-ciphertext pair  $(M_0, C_0)$ , we need to show that  $\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \Pr[\text{PT} = M_0]$ .

$$\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \frac{\Pr[\text{PT} = M_0, \text{CT} = C_0]}{\Pr[\text{CT} = C_0]} = \frac{\Pr[\text{PT} = M_0] \Pr[\text{CT} = C_0 \mid \text{PT} = M_0]}{\sum_{M \in \mathcal{M}} (\Pr[\text{PT} = M] \Pr[\text{CT} = C_0 \mid \text{PT} = M])}$$

Since that the encryption key is drawn uniformly random from the key space, and there is only one key that encrypts any given plaintext into any given cipher text (the key is given by the XOR of the plaintext and the ciphertext),

$$\Pr[\text{CT} = C_0 \mid \text{PT} = M_0] = \frac{\# \text{ of keys in } \mathcal{K} \text{ that encrypts } M_0 \text{ into } C_0}{\# \text{ of total keys in } \mathcal{K}} = \frac{1}{2^n}$$

Similarly, for every  $M \in \mathcal{M}$ ,  $\Pr[\text{CT} = C_0 \mid \text{PT} = M] = \frac{1}{2^n}$ .

Therefore, continuing the first equation, we have

$$\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \frac{\Pr[\text{PT} = M_0] \frac{1}{2^n}}{\sum_{M \in \mathcal{M}} (\Pr[\text{PT} = M] \frac{1}{2^n})} = \frac{\Pr[\text{PT} = M_0]}{\sum_{M \in \mathcal{M}} (\Pr[\text{PT} = M])} = \frac{\Pr[\text{PT} = M_0]}{1}$$

■

### 3 A Crypto System that does not have perfect secrecy

Consider a crypto system in which  $\mathcal{M} = \{a, b, c\}$ ,  $\mathcal{K} = \{K_1, K_2, K_3\}$  and  $\mathcal{C} = \{1, 2, 3, 4\}$ . The keys are chosen uniformly randomly; in other words,  $\Pr[\text{Key} = K_1] = \Pr[\text{Key} = K_2] = \Pr[\text{Key} = K_3] = 1/3$ , and the encryption matrix is as follows:

	$a$	$b$	$c$
$K_1$	1	2	3
$K_2$	2	3	4
$K_3$	3	4	1

This does not have perfect secrecy because observing that the ciphertext is 1, one knows that the plaintext cannot be  $b$ .

That is, for any distribution of plaintext in which  $\Pr[\text{PT} = b] \neq 0$ , we have  $\Pr[\text{PT} = b \mid \text{CT} = 1] = 0$ , and thus  $\Pr[\text{PT} = b \mid \text{CT} = 1] \neq \Pr[\text{PT} = b]$ .