**Perfect Secrecy**

Suppose there is an adversary who is capable of learning the probability distribution of the message and the encryption scheme, as well as intercepting the ciphertext, but not the key used to encrypt the message, i.e., launching a ciphertext-only attack. Then, an encryption scheme is perfect secrecy when the adversary’s observing the ciphertext has no effect on his learning the plaintext.

The textbook *Introduction to Modern Cryptography* gives the definition of perfect secrecy as the following (Katz 27):

An encryption scheme (Gen, Enc, Dec) with message space *M* is perfectly secret if for every probability distribution for *M*, every message *m* ∈ *M*, and every ciphertext *c* ∈ *C* for which Pr[*C* = *c*] > 0:

Pr[*M* = *m* | *C* = *c*] = Pr[*M* = *m*].

(Eq. 1)

The formula above has an equivalent form. That is, for any *m*, *m’* ∈ *M*, and every *c* ∈ *C*:

Pr[Enc*K*(*m*) = *c*] = Pr[Enc*K*(*m’*) = *c*].

(Eq. 2)

The textbook also provides a lemma (Katz 28):

An encryption scheme (Gen, Enc, Dec) with message space *M* is perfectly secret if and only if Eq. 2 holds for every *m*, *m’* ∈ *M* and every *c* ∈ *C*.

(Lemma 1)

In plain words, Lemma 1 says that for any *m*, *m’* ∈ *M*, the probability distributions of the ciphertext are the same, thus implying nothing about the plaintext.

**Shannon’s Theorem**

The textbook defines Shannon’s Theorem as (Katz 35):

Let (Gen, Enc, Dec) be an encryption scheme with message space *M*, for which |*M*| = |*K*| = |*C*|. The scheme is perfectly secret if and only if:

1. Every key *k* ∈ *K* is chosen with (equal) probability 1/|*K*| by Gen.

2. For every *m* ∈ *M* and every *c* ∈ *C*, there is a unique key *k* ∈ *K* such that Enc*k*(*m*) outputs *c*.

Since it is an “if and only if” relation, we first start with the proof of the sufficiency of the conditions, i.e., if the two conditions are satisfied, then the encryption scheme is perfectly secret.

Given condition 2, we have

Pr[*C* = *c* | *M* = *m*] = Pr[Enc*k*(*m*) = *c*].

Since every key is unique and is chosen with equal probability 1/|*K*| as in condition 1, we have

Pr[*C* = *c* | *M* = *m*] = Pr[Enc*k*(*m*) = *c*] = 1/|*K*|.

Therefore, given the property |*M*| = |*K*| = |*C*|, by Bayes’ Theorem,

.

According to the definition of perfect secrecy and Eq. 1, the encryption scheme is perfectly secret.

Next we deal with the necessity of the conditions, i.e., given that the encryption scheme is perfectly secret, then the two conditions should be satisfied.

For any *c* ∈ *C*, there exists *m* such that Pr[Enc*K*(*m*) = *c*] ≠ 0. Then, Lemma 1 gives that for any *m*, *m’* ∈ *M*,

Pr[Enc*K*(*m*) = *c*] = Pr[Enc*K*(*m’*) = *c*] ≠ 0.

Let *Ki* ∈ *K* denote the nonempty set for *mi* that Enc*Ki*(*mi*) = *c*. When *mi* ≠ *mj*, *Ki* and *Kj* must be disjoint, otherwise the same key for different messages will give the same ciphertext. And since |*K*| = |*M*|, for any *mi* ∈ *M* we have

|*Ki*| = 1,

and there stands condition 2, the existence and uniqueness of the key which gives Enc*k*(*m*) = *c*. Again based on Lemma 1, we shall have

Pr[*K* = *ki*] = Pr[Enc*K*(*mi*) = *c*] = Pr[Enc*K*(*mj*) = *c*] = Pr[*K* = *kj*]

for any *mi*, *mj* ∈ *M*, making “every key *k* ∈ *K* is chosen with equal probability 1/|*K*|”, as in condition 1. Q.E.D.

**References**

Katz, Jonathan, and Yehuda Lindell. *Introduction to Modern Cryptography*. 3rd ed., CRC Press, 2021, pp. 27-36.