Unconditional security

Speaker: Junji SHIKATA

1. Introduction

I focus on the topics on unconditional (or information-theoretic) cryptography. Informally, *unconditional security* means the security which is guaranteed against the adversary having unlimited (i.e. infinite) computational resources, while computational security is the one against the computationally limited adversary (i.e. polynomial-time adversary). Therefore, unconditional security is regarded as the ultimate one, though it usually has drawbacks in efficiency such as requirement of long keys. In this talk, I briefly explain two fundamental cryptographic systems: unconditionally secure cryptosystems (encryption schemes) and authentication-codes. The former provides *confidentiality* (or *privacy*): keeping information secret from the adversary. The latter achieves *integrity* (or *authenticity*): preventing information from being altered or substituted by the adversary. Also, I talk about further advanced topics on unconditionally secure schemes for various models.

2. Cryptosystems with Unconditional Security

In 1949, C. Shannon first published the paper which dealt with information-theoretic cryptography in terms of systematic and theoretical aspects. In this talk, I briefly explain the unconditionally secure cryptosystem with perfect secrecy which was shown by Shannon.

The cryptosystem (encryption scheme) is a cryptographic technique to provide confidentiality. Let us consider a model of the cryptosystem where there are three entities, a sender (or a transmitter), a receiver and an adversary (opponent). Suppose that the sender and the receiver share a secret key. The sender encodes a plaintext into a ciphertext by using the key, and then transmits it to the receiver in

an insecure channel to which the adversary can have perfect read-only access. On receiving the ciphertext, the receiver recovers the plaintext by using the key. In this model, *perfect secrecy* is the strongest security notion which means that the adversary having unlimited computational power cannot obtain any information on the underlying plaintext after observing the target ciphertext. As construction of the cryptosystem with perfect secrecy, Vernam's one-time pad cipher is well-known.

3. Authentication with Unconditional Security

The authentication-code (A-code) is a cryptographic technique to provide integrity. Historically, the A-code was invented by E. Gilbert, F. J. MacWilliams, and N. J. A. Sloane in 1974, and the theory of authentication was developed by G. J. Simmons in the early part of the 1980's.

Let us consider a model of the authentication-code where there are three entities, a sender (or a transmitter), a receiver and an adversary (opponent) with unlimited computational power. Suppose that the sender and the receiver share a secret key. The sender encodes a source state into an authenticated message by using the key, and transmits it to the receiver in an insecure channel to which the adversary can have perfect read-and-write access. On receiving the authenticated message, the receiver checks its validity by using the key. If it is valid, the receiver accepts it and regards it being legally sent from the sender. Otherwise, the receiver rejects it. In this model, the adversary can insert an authenticated message into the channel, and/or can substitute an observed authenticated message with another one. These two attacks are called *impersonation* attack and *substitution* attack, respectively. By performing these attacks, the goal of the adversary is that the authenticated message inserted and/or substituted by him/her is accepted by the receiver. The authentication-code is secure if the success probability of the above two attacks by the adversary is negligible.

4. Further Topics on Unconditional Security

I further talk about two advanced topics on unconditional security.

The first topic is about various authentication systems (other than A-codes in the previous section) including multi-receiver authentication-codes (MRA) and signature schemes. We note that these authentication systems can provide long-term security (i.e. long-term integrity), though computationally secure schemes may not guarantee long-term security. This is because there is possibility of appearance of faster computers such as quantum computers in the future which can efficiently solve computationally intractable problems (e.g. integer factoring problem). Therefore, unconditionally secure authentication systems would be useful for applications in which long-term integrity is strongly required. The applications may include official documents, court records, important contracts and copyright protection.

The second topic is about various models to achieve unconditional security. The cryptosystems and authentication systems in Sections 2 and 3 implicitly assume that the sender and the receiver can share a secret key in a secure manner, and that is often discussed in Trusted Initializer Model (TI model) where there is a trusted authority, called *TI*, which distributes each user's secret key in the initial phase. Also, there are other attempts at constructing unconditionally secure schemes along with different models such as Noisy Channel Model, Bounded Storage Model (BSM) and Quantum Channel Model. Cryptographic schemes along with these models reply on physical assumptions rather than the existence of TI.