INTRODUCTION

Chair: Atsuko MIYAJI

1. Cryptography

The cryptography is one of information science, whose purpose is to achieve **confidentiality**, **integrity**, and **availability**. Confidentiality is to protect privacy from an outside. Integrity is to guarantee the data consistency through the process for sending, receiving, compressing, or decompressing data, etc. Availability is to let any data be available even after the process for sending, receiving, compressing, or decompressing data, etc. in the case of necessity. The cryptography has to achieve efficiency and security as well as these properties, which is the hardest part of cryptology. Thus, we often use some assumptions such as the computational difficulty to overcome this problem. A problem is called the **computationally secure** when it cannot be solved by the polynomial-time adversary. On the other hand, a problem is called the **unconditional security** when it cannot be solved by any adversary.

In order to achieve properties of cryptology, the **information theory** was introduced in 1949. The information theory focuses on the unconditional security by sacrificing the efficiency. On the other hand, both the **computational theory** and the **number theory** are introduced to achieve these properties of cryptology. They can realize the efficiency by assuming the computational security. The most important invention, which uses both the computational and the number theory, was the **public key cryptosystem**. After the concept of public key cryptosystem was proposed by Diffie and Hellman in 1976, the cryptology has dramatically changed to be widely and practically used.

In summary, the cryptology has absorbed various fields such as the information theory, the number theory, and the computational theory and has been developed. In a sense, the cryptology is, so called, the synthetic science.

2. Why the cryptology has been dramatically changed by the public key cryptosystem?

Before explaining the public key cryptosystem in detail, let me explain the **secret key cryptosystem**, which had been only a typical cryptosystem before the public key cryptosystem was proposed and has been still a key technology of cryptology together with the public key cryptosystem. In the secret key cryptosystem, an encryption key is equal to a decryption key. So, an encryption (decryption) key should be kept secretly. This is why an encryption (decryption) key is called a secret key and the cryptosystem itself is called the secret key cryptosystem. In the secret key cryptosystem, each sender should use each different key to communicate a receiver. Therefore, a receiver has to keep N keys secretly to communicate N senders. To make matter worse, both entities of a receiver and a sender need to share a key secretly before starting a secure communication. How can we share a key secretly through the open internet? So, the secret-key cryptosystem has serious drawbacks of key management and agreement.

On the other hand, the public key cryptosystem resolves problems of key management and agreement in the secret key cryptosystem. In the public key cryptosystem, an encryption key is not equal to a decryption key. So, an encryption key can be published and, thus, is called a public key. On the other hand, a decryption key should be kept secretly and, thus, is called a secret key. In the public key cryptosystem, for N senders, 1 key is enough to decrypt. That is, in the public key cryptosystem, a user can communicate with anyone by just keeping 1 secret key without any secret communication beforehand. Thus, the public key cryptosystem has a big advantage over the secret key cryptosystem in key management and agreement.

3. Principle of public key cryptosystem

Let us explain the principle of the public-key cryptosystem. The principle of public key cryptosystem consists of the computational theory and the number theory. We have seen that a public key is different from a secret key. However, if a secret key can be easily solved from its corresponding public key, then the system is vulnerable. Therefore, we have to set the problem of finding a secret key from

a public key to be difficult. On the other hand, both decryption and encryption should be efficiently implemented. Thus, the public key cryptosystem has to satisfy such an asymmetric relation. Up to now, four problems have come into practical use, the **integer factorization** (**IF**), the **discrete logarithm problem over a finite field** (**DLP**), and the **elliptic curve discrete logarithm problem** (**ECDLP**), where an elliptic curve is a non-degenerate cubic curve. These are all difficult problems in the number theory.

4. One application based on a public-key cryptosystem

SSL (**Secure Socket Layer**) is widely used through Internet when we have to keep a transaction secret such as an electronic shopping. In a typical web browser, an icon in the form of a key at the bottom indicates our use of SSL. Let me pick out SSL to explain how a public key cryptosystem is used. The form of a key indicates that a server has prepared a public key on its web server beforehand. In the beginning of SSL, the handshake protocol is done between a client and a server. Then, a client takes the public key through internet, encrypts a random number K by the public key, and sends a ciphertext to the server, where K will be used for data encryption later. Then, the server decrypts the ciphertext by its own secret key to obtain K. Then, both a client and a server can share the key K. After they succeed to share a key, the secure communication by a secret key cryptosystem with K will start. A noteworthy advantage of SSL is that the client does not have to provide her/his own public key.

6. Comparison between IF, DLP, and ECDLP

We have already seen the security of the public-key cryptosystem is based on something difficult problems in the number theory, which are typically IF, DLP, and ECDLP. Here let us compare between IF, DLP, and

ECDLP from the point of view of the strongest attack. The key size is determined in such a way that it assures the security against the strongest attack, while the efficiency mainly depends on the key size. Both DLP and IF are solved in the sub-exponential time $O(\exp\{(\log\log p * \log p)^{1/2}\})$ for the key size p, where p corresponds to a finite field with p elements F_p in DLP. On the other hand, some ECDLP is solved only in the exhausted algorithm $O(p^{1/2})$ for the key size p, where p

corresponds to an elliptic curve E/F_p. So, ECDLP with the key size of 160 bits has almost the same security level as IF or DLP with the key size of 1024 bits and, thus, ECDLP is more efficient than DLP and IF with the same security level.

7. A new primitive using a pairing and its related open problems

Here we show another mathematical tool of a **pairing** over an elliptic curve briefly, which was introduced to cryptology in 1991. An elliptic curve over a finite field is a finite abelian group, on which the Weil or Tate pairing is defined. They are pairings that satisfy bilinearity and non-degeneracy. A pairing is called a cryptographic pairing if a pairing satisfies the computability as well as bilinearity and non-degeneracy. The pairings connect ECDLP and DLP and have solved some problems of cryptology by using a powerful tool of bilinearity so far. Thus, pairings, one of important features of elliptic curves has begun to attract an attention.

However, it is not easy to find an elliptic curve that has a cryptographic pairing. Theoretically, there exists a pairing with bilinearity and non-degeneracy, however, it does not necessarily satisfy the computability. In fact, it is known that the computation time of pairing is greater than the logarithm of the key size p of elliptic curve E/F_p. This is why it is not easy to find an elliptic curve with a cryptographic pairing. Up to now, only three algorithms of Miyaji-Nakabayashi-Takano (MNT), Barreto-Naehrig (BN), and Freeman have been proposed. So we need another efficient algorithm to find an elliptic curve with a cryptographic pairing. This is one of the open problems related on the cryptographic pairing.

9. Conclusion

The cryptology has been widely used as a necessary technology to achieve an electronic market, an electronic government, etc. The cryptology is a synthetic science and has dramatically changed by introducing various fields such as the information theory, the computational theory, and the number theory. We believe, from now on, cryptology will solve open problems by introducing various fields.