Fascinated with Cryptography

Tatsuaki Okamoto
NTT Fellow,
NTT Information Sharing Platform Laboratories

We asked world-renowned cryptography researcher Tatsuaki Okamoto, an NTT Fellow, to explain why cryptography research is important, tell us about his experiences and future research ambitions, and pass on some words of encouragement to young researchers.

Significance of cryptography research

—Dr. Okamoto, could you explain in layman's terms the significance of cryptography research?

Of course. When most people hear the word *cryptography*, the first thing that comes to mind is, I think, a system for keeping something secret or scrambling information. Such an image has been popularized by war movies and spy thrillers. For researchers, however, cryptography has a somewhat broader meaning. The network has come to reach all corners of society, and as a result, crimes like data tampering have the potential to inflict major damage on society. Information security technology is therefore of great importance in guaranteeing personal privacy and the validity of data used in information processing, and the core technology for providing this security is cryptography.

—So the word cryptography can have a variety of meanings, can't it?

That's right. In this regard, I've recently begun using the word *generation* to identify different kinds of cryptography. This is not popular usage, but in my mind, cryptography can be broadly divided into three types: first-generation cryptography, second-generation cryptography, and third-generation cryptography. I am currently researching third-generation cryptography (**Fig. 1**).

First-generation cryptography has been used ever since ancient times, that is, from the time that man first began to write, right up to the present. In this type of cryptography, the key used for encrypting information is the same as the key for decrypting, or recovering, that information. For this reason, this type of cryptography is called *symmetric* cryptography. Second-generation cryptography, on the other hand, was developed more recently in the 1970s, in the same period in which the Internet was born. It features different keys for encryption and decryption, with the encryption key being publicly disclosed, which differs from symmetric cryptography.

Let me explain how second-generation cryptography works. If, for example, I were to publish a key for encrypting information on my personal website, then anybody in the world could use it to encrypt and send information to me. This scheme permits safe and secure data communications because I am the only person who has the key needed for decrypting the encrypted data. This kind of cryptography is called public-key cryptography for the simple reason that the encryption key is public knowledge. At present, first- and second-generation cryptosystems are being used in combination to maintain information security over the Internet. In such a hybrid system, a symmetric key is first encrypted by public-key cryptography and sent from one user to another, and then subsequent exchanges between those users are conducted

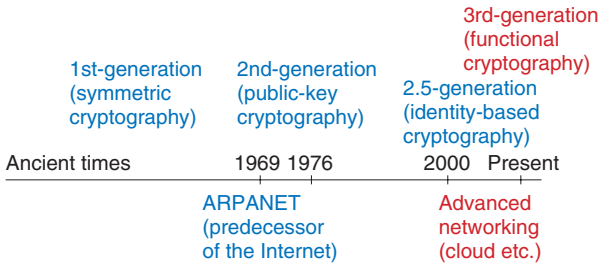

Fig. 1. Cryptography generations.

using that symmetric key for symmetric cryptography, which features fast processing.

Amid this situation, the cloud network has appeared. In cloud computing, the user passes all relevant data to the cloud, which provides the user with services on the basis of that data. This scheme represents a big change in the way that the network is used. However, entrusting the cloud with all kinds of data, from corporate accounting information to customers' personal information, can be extremely risky if there are no guarantees that such information can be maintained securely. Thus, there is a growing need for third-generation cryptography that can provide highly functional cryptosystems to support highly functional networks.

Falling into cryptography research by chance

—Dr. Okamoto, how did you become involved in cryptography research?

Well, this is how it happened. After entering NTT, which was still Nippon Telegraph and Telephone Public Corporation at the time, I became involved in research on computer networks. The project that I began working on began to settle down about four or five years later. It was exactly at this time that an incident occurred at the Hokkaido Bank: a system manager of the online banking system contracted to NTT was found to be making and using counterfeit bank cards. As a result of this unfortunate incident, a cryptography research group was formed in response to orders from the head of NTT's technology systems. This group initially consisted of three members. I was one of those three. That was around 1983. I found cryptography research quite interesting from the start and it didn't take long for me to become totally absorbed in the subject. As it turned out, however, circumstances dictated that I would have to leave cryptography research for a while.

As a result of the Fifth Generation Computer initiative established by the Japanese government in 1982 in the face of a worldwide boom in artificial intelligence (AI) research, an order came down to me in 1985 to take up AI research. I consequently left the cryptography group and joined a natural language processing project called Japanese-English Machine Translation. My research activities in this project lasted about two years. Then, on learning about the birth of a new concept called zero-knowledge proofs in the cryptography field, I asked to return to cryptography research in 1987 and I've been researching cryptography ever since. I remember well how thrilled I was to be able to return to the cryptography group and pursue cryptography research full-time.

Toward practical application of third-generation cryptography

—Please tell us more about third-generation cryptography.

Third-generation cryptography, or functional cryptography, is somewhat new: it has been around for only a few years. As in second-generation cryptography, the encryption key used for third-generation cryptography is made public, but in contrast, the encryption key and the decryption key are each determined by a certain parameter (**Fig. 2**). In this sense, third-generation cryptography can be regarded as an extension of second-generation cryptography. Specifically, a certain parameter x is used to encrypt plain text into cipher text, and a decryption key having a certain parameter v is used to decrypt that cipher text. Correct decryption can be performed only when parameters x and v satisfy a sophisticated logical relationship. This is the main principle of third-generation cryptography.

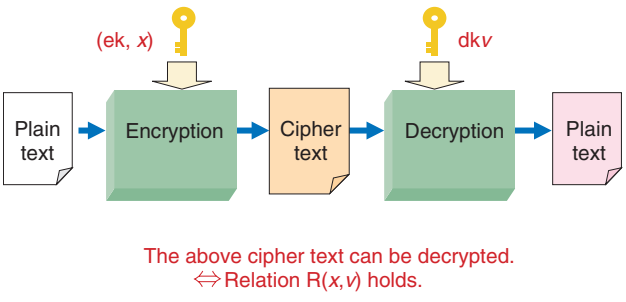

Fig. 2. Third-generation cryptography (functional cryptography).

—What kind of services do you envision?

Let's consider a content delivery service as an example. When applying third-generation cryptography to such a service, the first thing to do would be to classify the content to be delivered using certain attributes. These could be, for example, animation as the genre, 3000 yen as the price, and under-18 as the target users. The next thing to do would be to encrypt the content using a parameter. Now then, who would be able to decrypt the content? It would be anyone possessing a decryption key that incorporates a conditional statement in the form of "If the content has these attributes, it can be decrypted." Thus, from the user's standpoint, there is content that can be decrypted and content that cannot be decrypted according to the key that the user possesses. With such a scheme, we can consider a business model in which decryption keys are sold at a price that corresponds to their decryption capability. For example, decryption keys with relatively mild restrictions, that is, keys that can decrypt just about any type of content, would naturally be priced high. On the other hand, keys with many restrictions, such as one that can be used to decrypt only animation priced at 3000 yen targeted for under-18 users, could be priced lower. We can therefore envision a mechanism in which a user purchases a decryption key beforehand and uses that key to decrypt and use encrypted content stored in the cloud according to the conditions stipulated by that key.

The advantage of this type of cryptography is that the information-providing side only has to place encrypted content in the cloud. Then, if that data were to be stolen, there would be no need to worry about unauthorized viewing of that content. In addition, complex access control does not have to be performed in a centralized form on the cloud side using database management functions. Instead, third-generation cryptography can provide this control in an autonomously distributed manner through relationships among parameters (attributes, conditional statements, etc.) between the user side and the information-providing side. Third-generation cryptography makes possible extremely advanced and detailed control functions.

—When do you expect third-generation cryptography to become practical?

Since the concept of third-generation cryptography has been around for only a few years, we are now conducting research with practical applications slated for five to ten years down the road. I believe that the research that we are conducting is at the forefront of worldwide third-generation cryptography. We are researching this cryptographic system in collaboration with Katsuyuki Takashima of Mitsubishi Electric Corporation, and I have a strong feeling that great results will be forthcoming. I want this research to keep expanding in the years to come.

Individual pursuits

—Other than cryptography research, are there other kinds of problems that you would like to pursue?

Well, there are actually various challenges that I would like to take up. Among the seven Millennium Prize Problems in mathematics declared in 2000, one of them, the P versus NP problem, has a deep relationship with cryptography. The objective is to prove either P=NP, P≠NP or the formal independence: either result would have a big impact on the foundations of cryptography. I understand that it is extremely difficult to find any solution to this problem, but I would love to be able to make some sort of contribution toward its solution.

—Dr. Okamoto, could you leave us with a message for young researchers?

I often tell young researchers that researchers should have good taste. Originally, research had a tendency to be uncertain about the future. In the art world, *taste* refers to a person's sense of beauty, but in research, it is the researcher's sense of where research is headed: to a rich and fruitful place or a dry and barren land. It is vitally important that researchers cultivate taste in this sense.

Tatsuaki Okamoto
NTT Fellow, Okamoto Research Laboratory, NTT Information Sharing Platform Laboratories.
He received the B.Eng., M.Eng., and Dr.Eng. degrees from the University of Tokyo in 1976, 1978, and 1988, respectively. He is currently engaged in research on cryptography and information security. He is also a guest professor of Kyoto University.