Pursuing Fundamental Theory and Applied Technology of Cryptography That Is Secure in an Environment in Which Quantum Computers Are Widespread

Masayuki Abe
NTT Fellow, NTT Social Informatics Laboratories

Abstract

Security incidents such as data breaches and cyber attacks are being frequently reported. In the event of such an incident, cryptography protects essential information. If the information stolen or leaked was encrypted using a strong cryptography that cannot be decrypted, the information is merely a series of "1"s and "0"s and cannot be tampered with. With the spread of the Internet, cryptographic technologies are widely used in e-commerce such as online shopping and cryptocurrency. Encryption and decryption are done through computer-based computations, but as computer performance improves, they are becoming more complex to ensure robustness.

We talked with NTT Fellow Masayuki Abe of NTT Social Informatics Laboratories, who is researching cryptography, about a new method that uses cryptography for safely buying and selling information, new developments in zero-knowledge proofs, a technique for proving a certain statement is true without revealing additional knowledge, and his thoughts on creating a comfortable community where researchers respect each other.

Keywords: cryptography, zero-knowledge proofs, cryptographic protocol

Cryptographic technology based on fundamental theories that are unshakeable even in the era of quantum computers

—Could you tell us about your current research?

I became an NTT Fellow in 2022, and am researching cryptography under the new structure of the Abe Research Laboratory. Research on cryptography at NTT is roughly categorized into three areas based on periods in chronological order: "present," "near future," and "distant future" (**Fig. 1**). The critical points concerning these categorizations are whether the period is before or after the advent of general-purpose

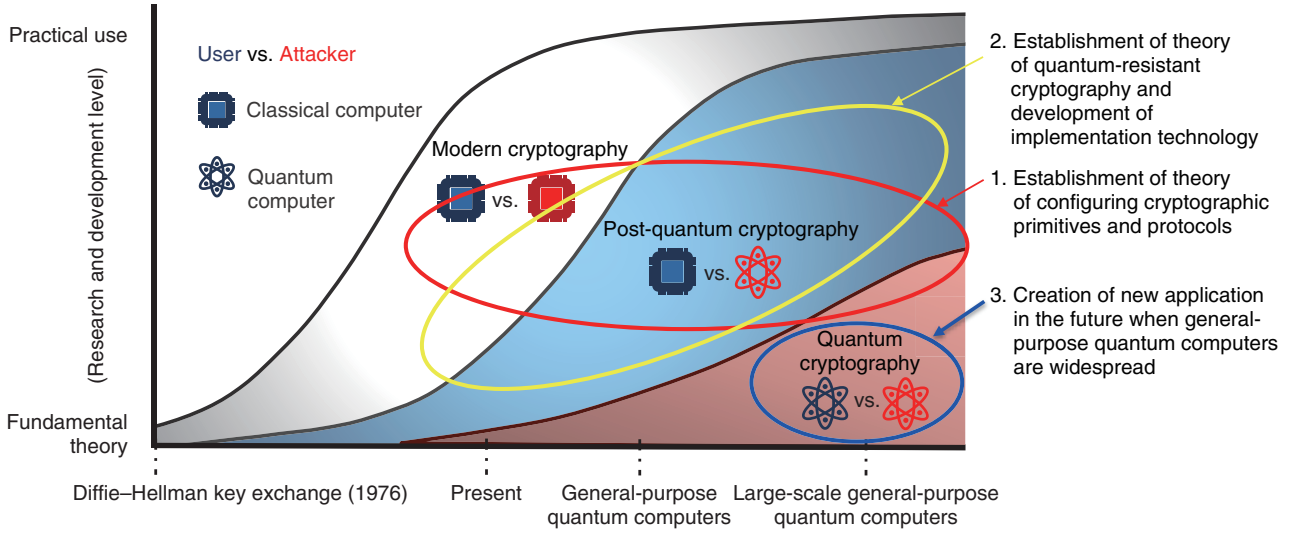


Fig. 1. Current status of NTT's cryptographic research: three research areas.

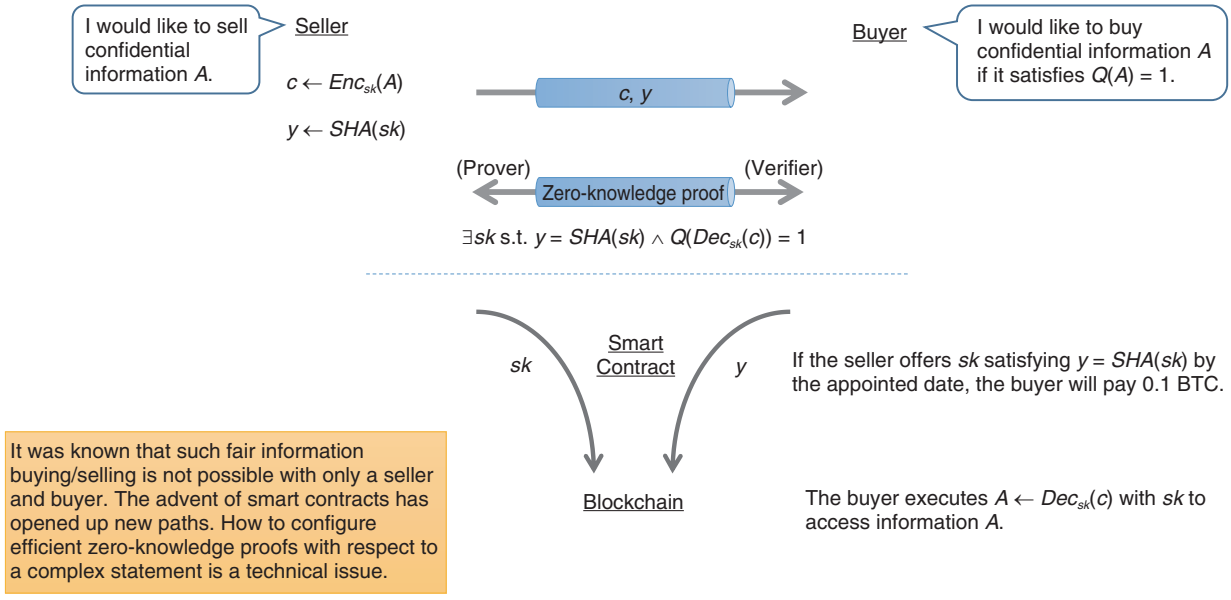
quantum computers or after such computers becoming widely used in society. Under these categorizations, the present is the period before general-purpose quantum computers are invented.

Cryptography aims to protect information from hacking or attacks by malicious individuals or from leaks due to system problems, so it is crucial to know how much computing power malicious individuals have. Improvements in the computing power of classical computers (commonly used computers) can be predicted in line with past improvements. However, quantum computers have powerful computing capabilities that are inconceivable as an extension of classical computers, and new types of attackers will take advantage of these capabilities. Accordingly, cryptography will be utterly different before and after quantum computers are put into practical use. When quantum computers become more widespread, new applications will emerge, and cryptography that can handle them will be needed. Quantum computers will, therefore, be a key factor in cryptography. It is currently unclear whether or when a large-scale general-purpose quantum computer will appear, so we are researching cryptography to prepare for its arrival.

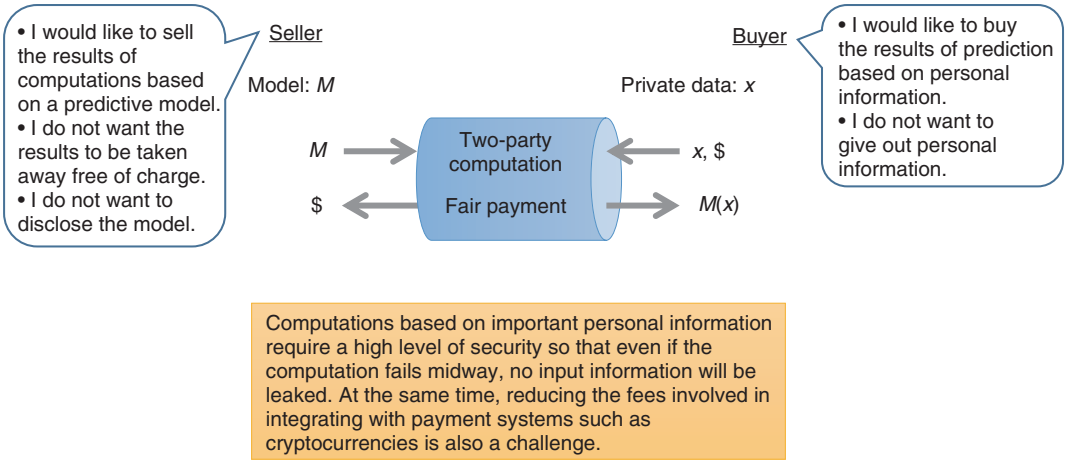
Under these circumstances, the theory of cryptography that has been researched in the world of classical computers will be an unwavering fundamental theory in the future, and the theme of the first area of our research is to continue that research and build a new theory. The second area of our research is to construct cryptography that is secure even after the advent of a general-purpose quantum computer. Being tackled primarily by young researchers, the third area of our research involves imagining what applications will emerge and what the world will be like when quantum computers become as pervasive as smartphones are today and researching the corresponding cryptography.

I am currently investigating the themes in the first and second areas. In my last interview of this journal (July 2021 issue), I discussed a method that combines zero-knowledge proofs and smart contracts as one of the mechanisms for safely and securely buying and selling information, namely, a buyer purchases (correct) information held by a seller (at the correct price) by using smart contracts on the blockchain (**Fig. 2(a)**). I am now advancing this method one step further and consider that a seller and buyer exchange information, and the buyer buys the result of that exchange. An example is that the seller has a high-precision predictive model (circuit), and the buyer wants the results of predictions made with their information using the seller's model. The seller provides the circuit, and the buyer provides the input information for the computation (prediction). Considering such a case, I am researching a mechanism for safely and securely buying and selling the computation results when both parties want to keep their respective highly confidential model and input information secret (**Fig. 2(b)**).

One method of achieving such a mechanism is to use an intermediary while using the smart contracts



(a) Safe information selling/buying using smart contracts on the blockchain



(b) Secure purchase and sale of computation results

Fig. 2. Information buying/selling.

mentioned above, but doing so would be very costly. Another method is fully homomorphic encryption, which encrypts the buyer's input information and executes the computation with that information on the seller's side. In contrast, the data are still encrypted, and the encrypted computation result is returned to the buyer. The challenge, however, is that the seller's circuit is not encrypted, yet the buyer has no idea whether the result of the seller's computation is correct.

Therefore, I came up with an approach to achieving two-party computation, with encrypted (encoded) information input into an encrypted circuit. The final result of the computation is also output as encrypted information. The correctness of the computational process is guaranteed by the pre-processing between the seller and buyer—independent of their private inputs—to create a circuit. If this pre-processing is correct, it is guaranteed that the actual computations can only be executed correctly. If an error occurs

during the pre-processing, the information between the two parties at that stage is simply computed as random numbers, and the original information is not tampered with or leaked, so the processing can simply be aborted. We are currently using this two-party computation to develop a secure mediation system for computation results. Artificial intelligence-based prediction and other services have become popular, and I expect that selling the results of computations will emerge as a business.

—Besides technology for safely buying and selling information, what other themes are you working on?

Another research theme is cryptographic protocols, which securely combine several components for a particular purpose. I am particularly focusing on composition technology for zero-knowledge proofs. A zero-knowledge proof is a technique for proving that a certain statement is true without revealing additional knowledge beyond the statement itself. For example, the technique enables one party to prove to another party the fact that a particular sheep named Dolly is present in a flock without revealing specific information about where Dolly is in the flock. Therefore, a person who has a public key only needs to inform the other party of the fact that they have the corresponding private key, the public key can be used for authentication through zero-knowledge proofs. The concept of zero-knowledge proofs was developed in 1985 but has recently been recognized as a very effective technique in the blockchain field. With the rapid development of applied technology in the last few years and the entry of startups and other companies, zero-knowledge proofs are now being used in the Web3 and blockchain fields. That being said, not all relevant theories have been created, and as the development of zero-knowledge proofs advances, new areas of research have emerged, so my current theme is to theoretically establish technologies to address these areas.

The point of this theme is how to prove, by zero-knowledge proofs, for example, that a person knows "private key corresponding to the public key" and that "I have more than 1000 bitcoins." In the case of proving the former fact *and* the latter fact, it is only necessary to prove that two individual facts are both true simultaneously; however, in the case of proving the former fact *or* the latter fact, if one party does not want to give the other party information about which fact is true, it is not enough to prove one of them. That is, if these two zero-knowledge-proof systems are not combined effectively, information about which fact is true will be leaked. Consequently, proving the former fact *or* the latter fact cannot be successfully done without an internal composition (zero-knowledge-proof composition).

The study of zero-knowledge-proof composition has rapidly progressed since 1994; however, the method of composing two zero-knowledge-proof systems has been changing in accordance with the properties of each system. In contrast to the traditional, well-known style of zero-knowledge proofs, known as "three round zero-knowledge proofs," a new, more-efficient style of zero-knowledge proofs—which is unsuitable for three round zero-knowledge proofs—has emerged. This progress has made it possible to execute zero-knowledge proofs efficiently with five or more rounds. However, it is interesting that a method of composition that worked well with three rounds becomes vulnerable to so-called "attacks" when the number of rounds reaches five. For example, it becomes possible to create a proof that verifies the statement "(A and B) or (C and D)" even though only A and C are valid, which means the proof becomes incomplete and information will be leaked or security not being properly proven. It has therefore become necessary to develop a method of composition that is compatible with newly emerged zero-knowledge proofs. Given that necessity, I and co-researchers have proposed a method for safely combining multi-round zero-knowledge proofs such as five round and seven round ones. The results of our proposal will be presented at Crypto 2024, the most prestigious conference concerning cryptography, to be held in Santa Barbara, CA, August 18–22, 2024 (as of the time of this interview).

By applying our method to the areas where conventional zero-knowledge proofs are used, it should be much easier to use zero-knowledge proofs. I believe that our method will contribute not only to the Web3 and blockchain fields but also to broader fields that require efficient zero-knowledge proofs.

To create a comfortable community where researchers respect each other

—What do you keep in mind as a researcher?

I have always wanted to contribute to NTT's research and development through cryptographic research, but becoming an NTT Fellow has given me a broader perspective and a stronger desire to nurture the successors and younger generations in the

cryptography community as a whole. Research and development can blossom precisely because it has theoretical seeds, but if you admire the flower and eat the fruit, it will end there. It is therefore necessary to train successors and younger generations. At the same time, the soil (fundamentals and theory) that supports the flower (application) must be constantly supplied with nourishment, so I want to work hard to make the soil strong while finding enjoyment in doing that. Since applied fields are fast-paced and results will not last forever, I strive daily to use fundamentals to produce results one after another.

I currently have two positions: the director of the Abe Research Laboratory and a researcher. As a laboratory director, since the members of my lab are outstanding, independent researchers, I am aware that my job is to respect their independence and create an environment in which they can do what they want to do. I grew as a researcher watching the example of my seniors, but the research styles and lifestyles of today's researchers differ from those of researchers in the past, so I ask myself whether I can be a good role model for my fellow researchers. My style is not everything, and we are equals as researchers regardless of age, so I try to set an example to young researchers as one model.

Connecting and discussing ideas with a wide variety of people at international conferences is a direct opportunity for collaboration, so I want to maintain this style. Nothing is more satisfying than having people want to conduct research with me after seeing the discussions and presentations I gave at conferences.

—Do you have a message for younger researchers?

Terms, such as Millennials and Generation Z, are used to lump together behavioral and lifestyle characteristics on the basis of year of birth and generation. The world of researchers has also seen significant change in the research environment. Research styles, lifestyles, and ways of thinking of young researchers, mid-career researchers, and their superiors differ, and those of mid-career researchers and their superiors have also changed compared to when they were young researchers. Ways of thinking also vary from individual to individual.

When such members form a research community or team, each member tends to impose their way of doing things, and because it takes time to understand each other, disagreements tend to occur. The community or team will never feel comfortable. I believe a sense of comfort is important to grow as a community and team and achieve results. To create a comfortable environment, it is best to take the time to understand each other, and the first step to that is to be relaxed and respect each other regardless of age, position, etc. Each generation has different problems, and each is searching for a way of life and direction to go amid those problems. Your experienced colleagues can offer advice or provide examples that are based on their experiences, so please do not hesitate to talk to us if you need assistance.

During the COVID-19 pandemic, I found researching challenging because I could not meet people in person. However, now that the various restrictions have been lifted and the research environment has improved significantly, face-to-face communication has become more active. I'm happy about this situation, and I want to seize this opportunity to engage in more face-to-face communication—necessary to make the community more comfortable—while preserving the benefits of remote work. Let's continue to research together in a comfortable community.

■ **Interviewee profile**

Masayuki Abe received a Ph.D. from the University of Tokyo in 2002. He joined NTT Network Information Systems Laboratories in 1992. He engaged in developing fast algorithms for cryptographic functions and their software/hardware implementation as well as the development of a software cryptographic library. From 1996 to 1997, he was a guest researcher at ETH Zurich, where he studied cryptography, specifically multi-party computation, supervised by Professor Ueli Maurer. From 1997 to 2004, he was with NTT Information Sharing Platform Laboratories (now NTT Social Informatics Laboratories), where he worked on the design and analysis of cryptographic primitives and protocols, including electronic voting, a key escrow system, blinding signatures for digital cash systems, message recovery, and publicly variable encryption schemes. He also engaged in efficient multi-party computation based on cryptographic assumptions and zero-knowledge proofs in multi-party computation. From 2004 to 2006, he was a visiting researcher at IBM T. J. Watson Research Center, NY, USA, working with the Crypto Group, where he researched hybrid encryption, zero-knowledge proofs, and universally composable protocols.

He served as a program chair for the 7th Cryptographers' Track at the RSA Conference on Topics in Cryptology in 2007, Aisa CCS'08: the 2008 ACM Symposium on Information, Computer and Communications Security, and ASIACRYPT 2010: the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security. His research interests include digital signatures, zero-knowledge proofs, and design of efficient cryptographic protocols.