Research of Cryptographic Protocols for Secure Communications in the Quantum Computer Era

Takashi Yamakawa
Distinguished Researcher, NTT Social Informatics Laboratories

Abstract

The development of quantum computers has been progressing rapidly in recent years based on principles fundamentally different from those of conventional computers. It is known that they can be used to break many of the encryption schemes that are now in actual use. To counter this threat, there is a need for "post-quantum cryptography" that cannot be broken even by quantum computers. In this interview, we asked NTT Distinguished Researcher Takashi Yamakawa to tell about his research in solving such social issues using cryptography.

Keywords: post-quantum cryptography, zero-knowledge proof, secure computation

Providing secure communications in preparation for the coming era of quantum computers

—Dr. Yamakawa, please explain to us the meaning of post-quantum cryptography.

Post-quantum cryptography means "cryptography that is secure against the threats of high-performance quantum computers." The research and development (R&D) of quantum computers has been progressing rapidly in recent years, and the possibility exists that quantum computers will become widely used in the near future. Security in current cryptographic schemes is based on the difficulty of prime factorization, but quantum computers feature the ability of factoring prime numbers to an extent not possible by classical computers. Consequently, if quantum computers should become commonly used in society, it is predicted that existing cryptographic schemes will be broken in several minutes leading to social disorder. It is therefore essential that all ciphers now in use be replaced with post-quantum cryptography before general-purpose quantum computers come into use to ensure secure information communications in the future. In fact, the National Institute of Standards and Technology (NIST) in the United States embarked on a standardization project for post-quantum cryptography in 2017, and because the demand for information security systems that can withstand quantum computing is increasing, I also began research in post-quantum cryptography.

My first undertaking after entering NTT was the research of quantum-secure public-key cryptography. In public-key cryptography, the example of the padlock is often used in reply to the question, "What is cryptography in the first place?" A padlock can be

Classical cryptography vs. post-quantum cryptography

	Classical cryptography	Post-quantum cryptography
Attack by classical computer	✔	✔
Attack by quantum computer	?	✔

Fig. 1. Relationship between classical cryptography and post-quantum cryptography.

used by anyone to lock (encrypt) a box (data), but to open the box, a key (decryption) is needed. So when sending someone a box (data), secure communications can be achieved by preparing a padlock, placing data in the locked (encrypted) box, and sending the box. This cryptographic system is called public-key cryptography. Specifically, in my research, I proposed a general technique for transforming a cryptographic system having weak security, or chosen-plaintext-attack security, into one having strong security, or chosen-ciphertext attack security. This technique was later adopted in a key-exchange, public-key-cryptography system called NTRU, which became a finalist as a candidate algorithm in the post-quantum cryptography standardization competition organized by NIST.

—At present, what are you specifically researching in post-quantum cryptography?

In the field of post-quantum cryptography, I'm now researching "zero-knowledge proof" and "secure computation." First, zero-knowledge proof, in brief, is a cryptographic protocol (a communication protocol using cryptography) for "proving that a certain statement is true without providing any additional knowledge other than the truth of that statement." This would correspond, for example, to saying, "I would like to prove that the correct answer to this puzzle exists." Of course, simply disclosing the answer would prove that "the answer exists," but this would reveal "knowledge" in the form of that answer. In short, technology that makes it possible to prove that an answer to a puzzle exists without conveying "knowledge" about that fact is called zero-knowledge proof.

Basically speaking, conventional cryptography only considers attackers using classical computers with respect to the security of zero-knowledge proofs, but whether they are secure if an attacker is using a quantum computer is unclear, so this is why I am researching post-quantum zero-knowledge proofs (**Fig. 1**). In this research, I have so far obtained negative results and positive results. As a negative result, I proved that a quantum-secure zero-knowledge-proof method that satisfies the same advantageous properties as classically secure methods "does not exist." This finding reflects a fundamental difference between classically secure zero-knowledge proofs and quantum-secure zero-knowledge proofs, a surprising result. As a positive result, I proved that making an appropriate transformation of a classically secure method as I mentioned above would directly result in a quantum-secure method as long as the definition of a zero-knowledge proof were to be relaxed within a range that presents no problems in actual use. This research could be applied, for example, to an anonymous authentication protocol as in proving that "I carry proper identification without having to reveal my identity."

Next, secure computation is a cryptographic protocol for calculating, for example, statistical quantities from multiple sets of data each possessed by a different party without disclosing that data among those parties. As in the case of zero-knowledge proofs, conventional research in secure computation basically considered only classical attacks, but whether it was quantum-secure was still unclear, which is why I took up this research. In terms of specific research, I have configured a quantum-secure method satisfying the same advantageous properties as the classically secure method and a method having a slightly relaxed version of security.

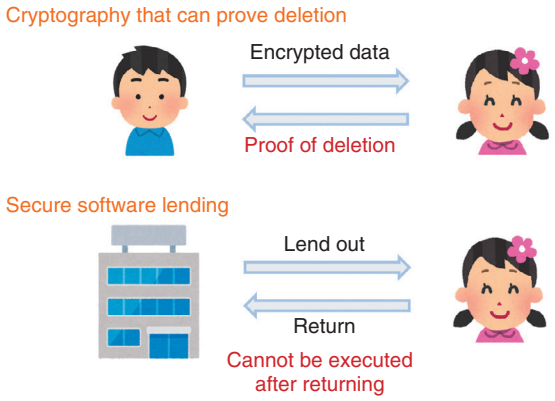

Fig. 2. Solving social problems through research of new cryptographic functionality using quantum computers.

—What other research are you conducting as a fusion of quantum computing and cryptography?

I am also engaged in the research of new cryptographic functionality using quantum computers. Classical cryptographic protocols suffer from an unavoidable problem in that they are all expressed in terms of digital data. For example, once data gets into someone's hand, it can be copied any number of times, and in addition, there is no technology for verifying that certain data has been deleted from the standpoint of another person. Realistically speaking, however, there is a much demand in society in the area of communications for preventing certain data from being copied and for guaranteeing that certain data has indeed been deleted. With this in mind, I am researching cryptographic protocols using quantum computers with the aim of achieving such functionality by cryptographic techniques (**Fig. 2**).

To be more specific, I am looking to achieve cryptographic functionality by making good use of the "no-cloning theorem" in quantum mechanics that states that it is impossible to copy a given quantum state. This is substantially different from classical digital data that can be copied any number of times, so I have researched a cryptographic method that can prove that certain ciphertext has been deleted using that theorem. I am also studying a cryptographic protocol for lending out software in a secure manner. This means, in short, a function that enables software to be executed during the period that it is being lent out but prevents it from being executed after being returned. This type of protocol had already been proposed, but in my research, I successfully achieved a function having a level of security that is even more reliable.

This new cryptographic functionality using quantum computers constitutes new technology, and it is still at a stage in which basic theory has room to mature. In fact, we are now in a proof-of-concept stage, but given that there is a real need in society for programs that cannot be copied and for proofs of data deletion, I think that many useful applications of these technologies will be appearing in the real world sometime in the future.

I am also researching the verification of quantum computers using cryptography. Although great strides are now being made in the development of quantum computers, it will take some time before they come into common use, so until then, general users who want to use a quantum computer will have to do so via the cloud from a classical computer. At that time, it will be necessary to verify the validity of those quantum computations to guarantee that the cloud is returning valid computational results. To give you a better idea of this research, let's let a quantum computer solve a puzzle for which the correct answer emerges only when the calculations are done correctly. Since this puzzle is generated on the user's side, the user already knows the answer, so if the quantum computer issues the correct answer, this tells the user that those quantum calculations are correct. Conversely, if the answer is incorrect, the user knows that the quantum computer did not perform the calculations correctly. To achieve this in reality, it will be necessary to skillfully embed cryptographic tools in quantum computations.

Additionally, it will be necessary, even in the quantum-computer R&D stage prior to such a function, to verify whether a quantum computer that is truly

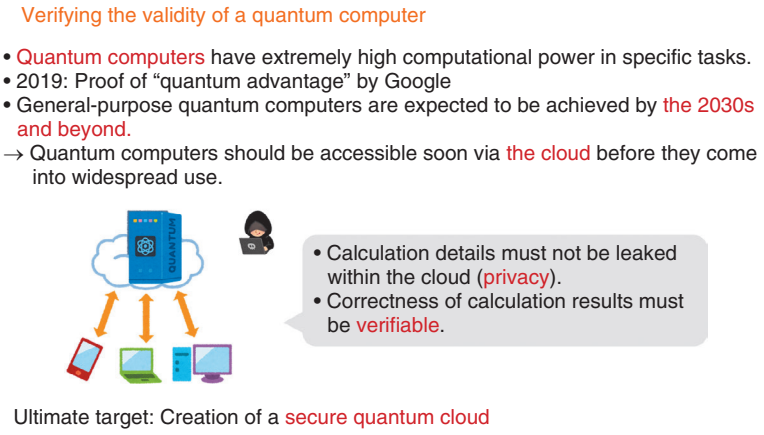

Fig. 3. Verifying the validity of a quantum computer using cryptography.

operating correctly has been created. In this regard, I have proposed a method for verifying the validity of quantum computations at very high speeds (**Fig. 3**), so we are making progress in this research. Furthermore, in protocol for verifying the validity of the statement "I have a quantum computer," I have proposed an entirely new method that uses only a function that behaves randomly called a hash function as a cryptographic tool. This method is fundamentally different from conventional methods.

Solving an abundance of problems and contributing to future research and human development

—What are some difficult challenges in your current research?

Classical cryptography is backed by basic results accumulated over many years, but quantum cryptography that I am researching is a field of research that has just begun. It is still in an entirely undeveloped state, and as a result, there are many unsolved problems dealing with very basic aspects of the theory. To give you an example, it is known that many cryptographic functions in classical cryptography have the property expressed as "calculations are easy to do but determining the original input from the results of those calculations is difficult," which is equivalent to a one-way function. It is still not known, however, whether the same holds in quantum cryptography. Recently, in 2019, a leading information and technology company published a paper claiming that quantum computers can solve problems faster than classical computers (quantum advantage). However, the method it describes is not "verifiable" in terms of cryptography and the assertion that quantum computers truly do exceed classical computers is not convincing from the standpoint of a third party. Even if speaking in generalities, the lack of a basic theory here can impede the configuration of more complex and high-performance ciphers. For this reason, we should research a method that can validate quantum advantage in terms of cryptography and work to solve fundamental problems.

—Please tell us about your research goals and vision going forward.

In my research, I believe it to be highly important to solve problems thought to be highly difficult to the point of greatly surprising researchers around the world. When attempting to solve truly difficult problems, many such attempts will end in failure. On the

other hand, by setting high goals, it is not uncommon to obtain a variety of interesting research results as a by-product, so I feel that it is vitally important to take on research with high goals in mind. My goal in research from here on is not so much to aim for applications in the near future but rather to contribute to future R&D through research of basic theory. Specifically, I would like to produce results that are still having an impact several tens of years or even hundreds of years from now by solving basic unsolved problems in quantum cryptography. I believe that these research results will deepen humankind's understanding of "computation" and lead to a more prosperous and enriched society making extensive use of quantum computers.

—Dr. Yamakawa, please leave us with a message for other researchers and students.

In the world of cryptography, the name "NTT" is known throughout the world, and at international conferences and other events, just mentioning NTT is enough to convey its credentials, which has the advantage of substituting as a business card. In addition, NTT brings together invited professors and superb postdoctoral researchers and research interns, which enables researchers to form international relationships and connections. Whatever field you are working in, this can be a great boost to advancing your own research. Abe Research Laboratory that I belong to within NTT Social Informatics Laboratories specializes in basic research in cryptography, and I am grateful that it recognizes the importance of basic theoretical research and allows us to continue this research. I believe it to be one of the most excellent research institutions in the world, of which there are few. In addition, I feel it is exactly such basic research that becomes the source of NTT's future competitiveness, and with this in mind, I will continue in my day-to-day research efforts.

Finally, I would like to thank all of my fellow researchers for their ongoing support of my research and their helpful discussions. I believe that new ideas are born through daily discussions with a variety of people. I look forward to advancing my research together with anyone having an interest in my research topics.

■ Interviewee profile

Takashi Yamakawa studied cryptography at the Graduate School of Frontier Sciences, The University of Tokyo and received his Ph.D. in 2017. He entered NTT in the same year. He has been a distinguished researcher at NTT Social Informatics Laboratories since 2022 conducting research in the combined field of quantum computing and cryptography. He was a visiting scholar at Princeton University from 2020 to 2021 performing joint research with Mark Zhandry, a leading scientist in this field. His papers have been accepted for presentation at Eurocrypt and CRYPTO sponsored by the International Association for Cryptologic Research (IACR), FOCS sponsored by IEEE, and other conferences.