Pursuing Research with the Attitude that "Fortune Is Unpredictable and Changeable" and Building Relationships to Inspire Each Other

Masayuki Abe
Senior Distinguished Researcher,
NTT Secure Platform Laboratories

Overview

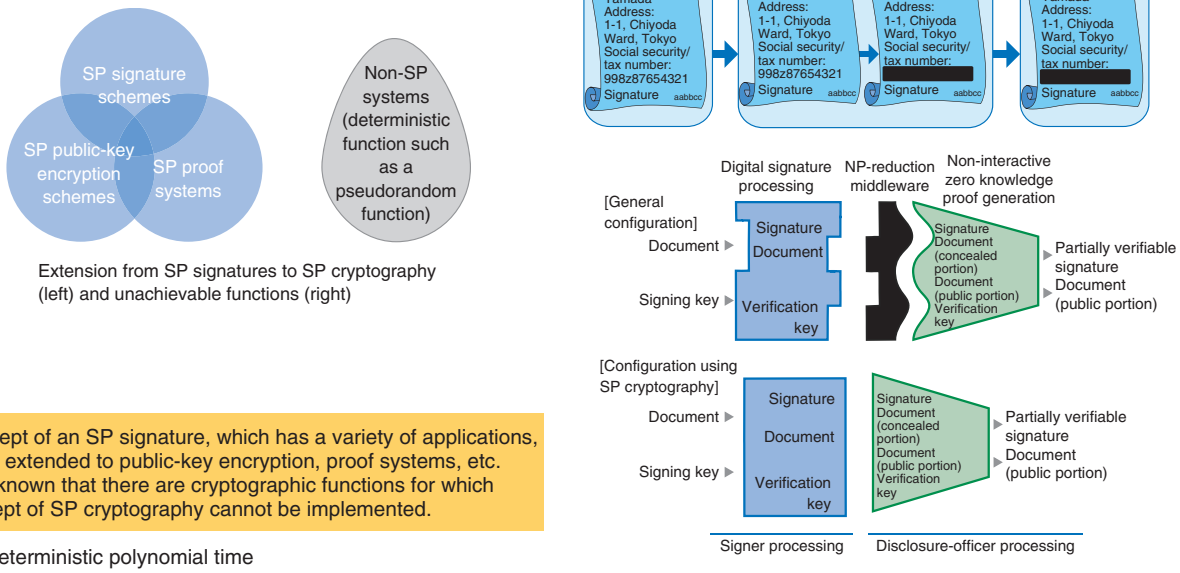
E-commerce transactions using electronic payments and e-government functions, such as online tax filing, continue to expand. Amid this trend, modern cryptography is being actively researched and developed as a technology for guaranteeing the safety of networks and services. Masayuki Abe, a senior distinguished researcher at NTT Secure Platform Laboratories, is known for his pioneering research and creation and implementation of many innovative technologies in cryptography. In 2018, he received the Maejima Hisoka Award, which is presented to individuals for their outstanding achievements in the fields of information communications and broadcasting. We asked him about the current state of his research and the role of a researcher.

Keywords: cryptographic protocol, structure-preserving cryptography, quasi-adaptive non-interactive zero-knowledge proof, smart contract

Clarifying "what can't be done"

—Dr. Abe, please tell us about the research you have been involved in since our last interview.

The main theme that I have been pursuing is the composing of secure cryptographic protocols. The process of safely delivering only the information needed to parties in need of it by encrypting the original information and attaching a digital signature is called a cryptographic protocol, and developing an approach toward a safe and efficient cryptographic protocol is my ultimate objective. A cryptographic protocol is a combination of diverse elements in a multilayer configuration, so the targets of research span a wide range from basic to applied. The basic components of a cryptographic protocol change through tuning in parallel with technological advances. This is truly a matter of technical craftsmanship. However, technology lying above these basic components can handle changes due to technological advances by combining existing technology with new technology because basic components absorb such changes. In such a complex system, I try to develop



Extension from SP signatures to SP cryptography (left) and unachievable functions (right)

The concept of an SP signature, which has a variety of applications, has been extended to public-key encryption, proof systems, etc. It is also known that there are cryptographic functions for which the concept of SP cryptography cannot be implemented.

NP: non-deterministic polynomial time

Fig. 1. SP cryptography.

both comprehensive solutions and solutions to specific problems in a balanced manner.

Since the last interview in 2013, I have been involved in three major research themes. The first is proving that there are unfeasible functions in structure-preserving (SP) cryptography (**Fig. 1**). SP cryptography achieves a high degree of safety by combining multiple cryptographic technologies via a uniform interface. This concept is being widely used, but it has been found that there are cryptographic functions for which this concept cannot be implemented, so I would like to explain and prove this. The second theme is proving non-composability (**Fig. 2**). I would like to prove that when composing an advanced function by combining multiple functions in SP cryptography, using only the interface of a certain function does not make it possible to compose a desired function. Finally, the third theme is studying a system for the safe buying and selling of information using smart contracts from basic research to actual applications (**Fig. 3**).

The idea of SP cryptography came to me around the end of 2009, and 2013 (when the last interview was conducted) was the year that I developed an SP digital signature and came closer to making it a reality. Through joint research conducted with Karlsruhe Institute of Technology (KIT) in Germany, we developed the world's first highly safe and interoperable SP digital signature scheme. We presented this achievement at CRYPTO 2017, a leading conference sponsored by the International Association for Cryptologic Research, held in the United States in August 2017 [1, 2]. Following this, I continued to pursue the arrangement of interfaces for cryptographic functions other than digital signatures and began the development of quasi-adaptive non-interactive zero-knowledge proof (QA-NIZK) systems. Through the development process of QA-NIZK systems, I explored not just combinations of interfaces but also functions and clarified limiting points at which safety could not be guaranteed. In other words, we clarified "what can't be done." This achievement brought us recognition in the field of cryptography and enabled us to create a new research area.

—How important it is to prove limiting points and impossibilities concerning cryptography?

At first glance, it might appear that proving an impossibility is not productive, but knowing what is not possible is very meaningful. In the research on cryptography, changes in computer technology bring

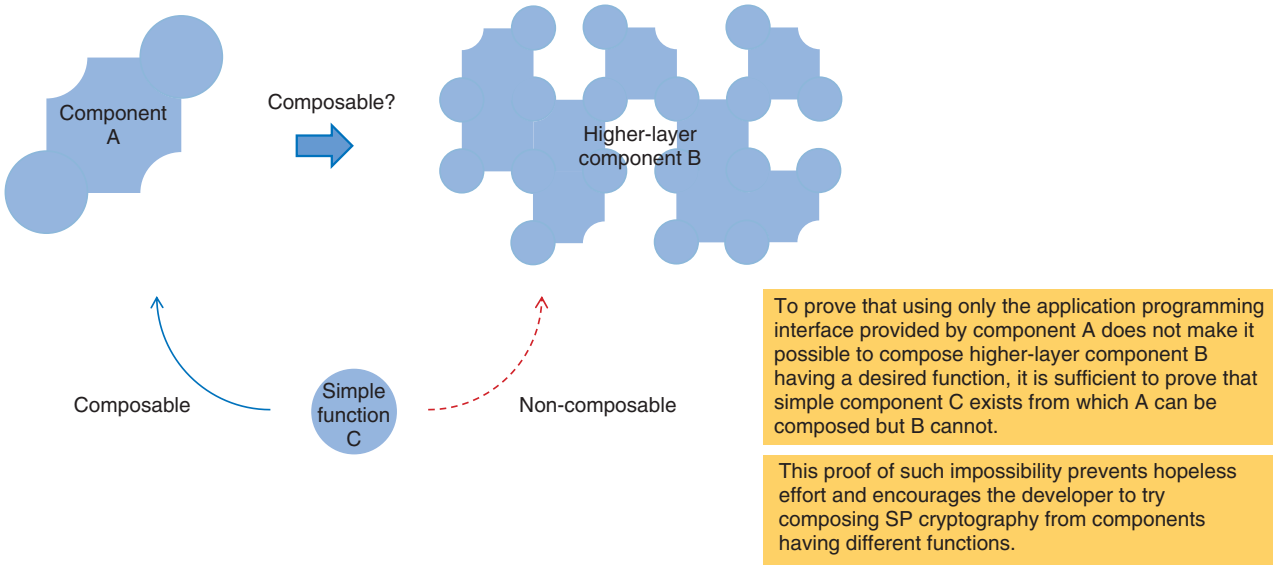


Fig. 2. Proof of non-composability.

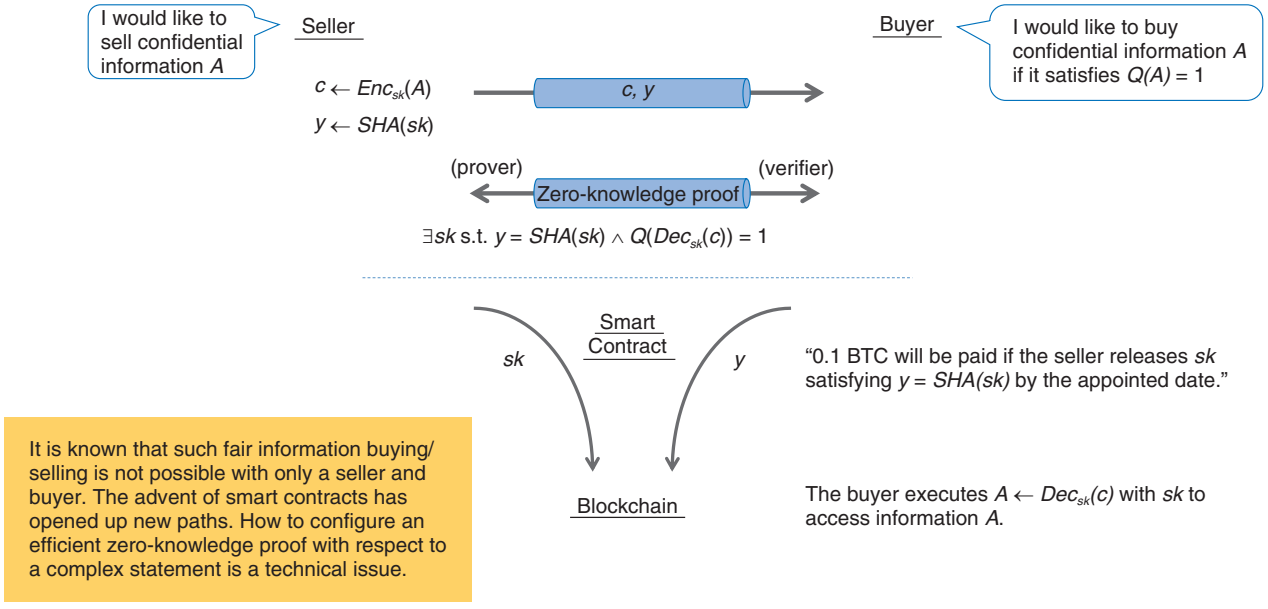


Fig. 3. Safe information buying/selling using blockchain-based smart contracts.

about changes in the level of attackers, which means changes in the concept of safety. Simply put, to ensure that the safety of the foundation of computers does not impact the technologies built on top of it, it is necessary to understand the limiting point of that impact. Proving an impossibility is an action that tells us "road closed from here on" and teaches us the nature of what is impossible. It is therefore extremely meaningful research that can lead to new methods of constructing cryptographic protocols.

I first began to use such a research approach (proving limiting points and impossibilities) for exploring the language extension of non-interactive proof systems. A non-interactive proof system is a technology

that completes a proof by simply sending information in a one-way manner. It is a cryptographic technology different from digital signatures, but I also pursued the limitations of this technology. As an example of non-interactive proof systems, we can take the case of verifying an individual's age. This can be accomplished, of course, by asking the individual in question to present a medium (such as a driver's license or passport) on which personal information including birthdate has been inscribed. However, if the individual does not want birthdate or other personal information to be referenced, this problem can be solved if it was possible to present only one's age. The technology that makes this possible is zero-knowledge proofs in a field of cryptography called proof systems. Non-interactive proof systems have good affinity with SP cryptography, and they have been used in combination. I considered that using them in combination could prove an even greater set of facts. For example, I began to investigate an extension to proof systems that would enable the proving of a composite situation such as being 20 years or older, possessing a driver's license, and working for a company with 2000 or more employees. However, I understood this to be difficult, and I'm currently trying to clarify whether it's simply difficult or just impossible.

In the research of cryptography, thinking about safety tailored to individual requirements is necessary. One part of this work is to determine to what point protection can be provided by cryptographic theory and to clearly identify the "protect surface." A researcher studies the meaning of safety and the use of a cryptographic technology every time such new technology has emerged. For example, a smart contract facilitates the automated execution of a contract by applying the technology of non-interactive proofs to support blockchains. In the beginning, this technology was not very efficient, and its safety could not be clearly shown. I first attempted to address these technical issues in application systems and in the field of blockchains together with a postdoc (a person working at a research organization for a fixed term after obtaining a doctor's degree) from Europe, and we were able to propose a method for the safe selling and buying of digital information. There is still much to be studied in this area, and I would like to continue my research on this technology.

Linking up with people leads to achieving research results

—Is there anything that you keep in mind to enrich your research activities?

At one time, the research field of cryptographic protocols was made up of a relatively small community of researchers, and research targets were limited. However, concepts of information security have become widely acknowledged and the range of its research has broadened, so I sometimes could not fully follow discussions in neighboring fields in adjacent sessions at academic conferences.

What helps me in such situations is to broaden my perspectives and interact with coauthors of past papers or with friends and acquaintances. It is very difficult to collect information and accomplish research on one's own, but one can acquire new information by communicating with people one knows.

My research of smart contracts that I mentioned above is a good example of this practice. What started me off in this research was a conversation with a postdoc who went on to achieve good results in this field and become a fellow researcher. As a result of that interaction, I went on to pursue smart contracts in earnest and write impactful papers. I first encountered him at an academic conference held in Spain. At that time, he was still a student, but he gave a presentation on a research theme that I had worked on in the past. I thought it was a very interesting presentation, and I called out to him saying "Good presentation!" and talked with him for a while. No more came of this chat at that time, but several years later, he contacted me saying "I'm going to complete graduate school soon and would like to do some research under you." That was the beginning of our research collaboration. I think that this collaboration would have never happened without that one face-to-face conversation.

This experience taught me that networking with people is of great value to researchers, and I have since placed much importance on relationships with friends and acquaintances. I make an effort to go out and meet a variety of people whenever an opportunity arises, such as a conference, and connect such interaction to research. I have been doing this for quite some time, so I now have many friends and acquaintances who are in authoritative positions, which has given me the opportunity to make connections with some of their students. In this way, I have been able to form good connections from which new research activities are born. I take great delight in the fact that

linking up with people leads to achieving research results.

—Such fulfilling connections certainly have a great impact on research. What types of researchers do people tend to gather around?

People naturally gravitate towards researchers who have extensive knowledge about topics one doesn't know about. Of course, it's important to be such a knowledgeable person, but since research activities include relationships between people "living under the same roof," it is even better to connect with people with whom you can get along.

Young researchers may connect with each other in a more systematic manner, but I want to place priority on connecting with the human side of research. This is because research, for me, is a part of life, and most of my life has been made up of research activities. There is no way that I would like to detach myself from something that I feel to be so important.

Basically, research requires output, so input becomes important in creating that output. Where that input comes from, such as human relationships or leisure activities, depends on the person, but I obtain input from my worldwide connections with people. I have been very fortunate in being in an environment in which I can leverage these relationships to enrich my research activities.

However, the COVID-19 pandemic of 2020 prevented me from building such personal connections. The Great East Japan Earthquake of 2011 interrupted my linking up with people in the same way. At that time, postdocs who had planned on joining my research group were hesitant about coming to Japan because of this disaster. I was able to gradually eliminate their fears by convincing them that Japan was safe, but this worldwide COVID-19 outbreak has presented a different set of problems. This time, we too cannot venture overseas, and it's difficult for overseas researchers to come to Japan. There are researchers of foreign nationalities living in Japan, but there are very few researchers who would like to try to come to Japan at this time. Although we can connect remotely with people we already know and can make new acquaintances through their introductions, it's unfortunate that unexpected encounters cannot spontaneously occur.

Words of encouragement to young researchers provides encouragement for oneself too

—As a pioneer in the field of cryptography, how do you view the development of this field?

The field of cryptography has matured thanks to an accumulation of achievements since 1970. Many young researchers have entered this field and pursued wide-ranging research, which has broadened this field. I believe that the process in which a technology matures is not simply an accumulation of core components but also the ongoing formation of a broad base, much like the shape formed by picking up a bed sheet with one's fingers. The searching out of all sorts of possibilities by many researchers broadens this field in the lateral direction while pursuing cutting-edge research extends the field in the vertical direction. The fact that this shape does not collapse reflects the maturity of this research field.

In the field of cryptography, there was a time when new ideas were announced at a fervent pace, but today, the broad base of this field means that new ideas must be discussed after giving sufficient consideration to peripheral areas. Moreover, papers of about 10 pages in length would have been accepted in the past, but papers of 30 to 40 pages in length have become the norm, making it all the more difficult to complete a paper. At the same time, the development of cryptography into a broad-based field such that one does not know what neighboring researchers are working on means that each researcher has worked their utmost to succeed, thereby raising the possibility of becoming the one and only in one's field of study, which can be very gratifying.

Yet, in any research field, a technical revolution in basic components increases the possibility of having to reset research up to that point. For example, the crossbar switch in communication networks was replaced with the digital switch, which was replaced with the router. Therefore, past technologies have been replaced with technologies based on completely different concepts. Similarly, fields that are close to the basic components of cryptography have been evolving. Computers, which have a close relationship with cryptography, are now on the verge of entering the quantum computer era after making great progress from the era of vacuum tubes. The time has come to construct cryptographic protocols that can deal with quantum computers, which will break down cryptography based on conventional mathematics. To keep up with this development, researchers have to be

adept at completely new technologies. On the other hand, cryptographic protocols that I am pursuing are well positioned for use in application fields, so I think I can make use of my knowledge to date.

—Dr. Abe, what do you think is the role of a researcher and what advice would you give your junior researchers?

Much like organisms in the natural world, researchers have completely different personalities with each having meaning and a role to play in an ecosystem that they called a research community. If the characteristics of researchers were to be uniform, I don't think there would be anyone to be inspired by and I don't think that anything original would be developed. In other words, stimuli (expertness, achievements, etc.) among fellow researchers influence each other and ignite something (research) that each researcher has been working on.

I would like all young researchers not to forget to give things time. When giving and taking knowledge, there is no need to repay a debt immediately, to think with a short-term, narrow field of vision, or to make decisions hastily. There is a proverb that I like, "fortune is unpredictable and changeable," which I think can be interpreted in various ways. I take it to mean, "think with a long-term view." I think it's best to make decisions by adopting long-term and broad perspectives.

To be honest, having to reset the knowledge that one has accumulated due to technical innovations and the coming of a generational change can be quite distressing. One part of the work of an NTT senior distinguished researcher is to train the next-generation of researchers and give them opportunities, and I'm quite pleased to see young researchers continuously putting out results and building relationships. A senior distinguished researcher is also expected to be an active researcher, so I need to keep up with the results presented by young researchers. When I observe the activities of young researchers, I sometimes worry, "Will I really be able to keep up with them?" But even without going head-to-head with young researchers to prove myself, I feel that I can overcome my concerns and remain active as long as the research that I am working on matches well with current needs and interests. I believe that the words that I use to encourage young researchers encourage me as well! Going forward, I have no intention of resting on my laurels—I want to keep challenging myself.

References

[1] NTT press release, "NTT, NICT and Karlsruhe Institute of Technology Design Highly Secure and Interoperable Digital Signature Scheme—Progress in Simplifying Design of Secure and Scalable Cryptographic Applications," July 27, 2017. https://group.ntt/en/newsrelease/2017/07/27/170727a.html

[2] M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo, and J. Pan, "Compact Structure-preserving Signatures with Almost Tight Security," Advances in Cryptology – CRYPTO 2017, pp. 548–580, LNCS, Vol. 10402, Springer, 2017.

■ **Interviewee profile**
Masayuki Abe

Senior Distinguished Researcher, NTT Secure Platform Laboratories.

He received a Ph.D. from the University of Tokyo in 2002. He joined NTT Network Information Systems Laboratories in 1992 and engaged in the development of fast algorithms for cryptographic functions and their software/hardware implementation and the development of a software cryptographic library. From 1996 to 1997 he was a guest researcher at ETH Zurich, where he studied cryptography, especially multiparty computation, supervised by Professor Ueli Maurer. From 1997 to 2004 he was with NTT Information Sharing Platform Laboratories (now NTT Secure Platform 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 multiparty 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, ACM Symposium on Information, Computer and Communications Security in 2008, and the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security in 2010. His research interests include digital signatures, public-key encryption, and efficient instantiation of cryptographic protocols.