Taking on Pioneering Research with a Worldview as a Specialist in Cryptographic Theory

Masayuki Abe
Senior Distinguished Researcher,
Research Group Leader, NTT Secure Platform Laboratories

Masayuki Abe, an NTT Senior Distinguished Researcher, has been researching cryptography for over 20 years. He has played an important role in this special field even at an international level having written a number of papers on cryptographic theory and having served as executive committee chairman and program committee member for various international conferences. The origin of this active life is no doubt the personal relationships that he formed during his stays at prominent research laboratories in Switzerland and the United States. We last spoke with him in 2006. We sat down with him again recently to find out more about his research career and current issues, and we asked him to leave a message for young researchers.

Keywords: cryptographic theory, digital signatures, structure-preserving cryptography

Engaged in overseas research activities while pursuing electronic money protocol and other projects

—Dr. Abe, please tell us about the path your research has taken to date.

Well, during my university years, I studied subjects such as radar-screen image processing and speaker recognition, which, needless to say, are unrelated to my current research. Then, in 1992, I began working at NTT Network Information Systems Laboratories in Yokosuka, and it was there that I first took up research in cryptography. That research group was researching both symmetric-key cryptography and public-key cryptography, but I became involved in the latter, and after being taught the basic concepts of public-key cryptography by NTT Fellow Tatsuaki Okamoto, who, by the way, received Japan's Medal with Purple Ribbon in 2012, I became firmly entrenched in this research field.

For the first two years, I was engaged in the design and development of cipher-and-authentication LSIs (large-scale integrated circuits) in cooperation with NTT Communication Science Laboratories. I next took up the research of cryptographic protocols, and thinking that such a protocol should not only be used to conceal a cipher but also to create something interesting, I undertook the development of electronic money. As a form of digital information, electronic

money can be easily copied, and preventing its duplicate use is a major issue. In 1995 and 1996, I was in charge of protocol design for electronic money as well as its software implementation. Then, after almost completing my work on the electronic money protocol, I was given the opportunity to study abroad at the Swiss Federal Institute of Technology (ETH Zurich) as a guest researcher in 1996.

Upon returning to Japan in 1997, I entered the cryptographic theory research group and continued my work on multi-party theory that I had first taken up in Switzerland. It was during this time that I first produced results that were good enough to be accepted by a highly competitive international conference. The words "Do your work with the world in mind" spoken by my group leader soon after entering NTT kept running through my head, and I realized that I wanted to submit work that would be well received by the world at large. From then on, one of my objectives was to submit results worthy of presenting at a leading international conference. Although the risk is great in doing so, a successful paper can generate considerable response, and I have been fortunate in receiving good feedback over the years. I am still following this research style, but I sometimes feel that I've been neglecting involvement with the local research community in Japan.

Next, I became interested in cryptography components in applications such as electronic voting and became involved in the research of advanced digital signatures and advanced ciphers. It was during this time that I became a Distinguished Researcher, a title bestowed by the NTT Distinguished Researcher system. Then, in 2004, I travelled to North America with the idea of enriching my knowledge and working in an environment in which I could concentrate on a single research problem. I spent a year and eight months doing research at the IBM Watson Research Center, a major hub of cryptography research. I continued researching a variety of cryptography components after returning to Japan, and in recent years, I have been researching topics within a single field that I developed called structure-preserving cryptographic systems.

—What did you bring back from your two overseas experiences?

At ETH Zurich, my supervisor was Ueli Maurer, a young, up-and-coming professor at the time but a top authority in the field of cryptography today. He was a very exacting mentor. Of course, learning a lot from a wonderful teacher had a big influence on my later research activities, but so did the interaction and exchanges I had with the students around me. The people in that research group are today very active in the front lines of cryptography research. I was able to make invaluable friendships with many of them, such as Ronald Cramer of the Netherlands, a very well-known researcher in this field.

For my second overseas research trip, I thought that since I had already studied at a European university, it would be advantageous to spend time at a company in North America. Therefore, I chose the IBM Watson Research Center, which had a formidable cryptography research team. Here as well, the connections I was able to make with the people around me were of great benefit. I was able to live in direct contact with a number of prominent researchers, and from them I learned how to approach my research with a sense of urgency and also how to cope with problems. These researchers at the front line of cryptography were indeed larger-than-life people overflowing with energy. They were capable of tackling problems by harnessing their knowledge and applying various techniques in a short period of time. I came away with the impression that research is a very physical activity. The connections I made there had a beneficial effect in various ways on my later activities.

Since 2001, I have served as program committee member and chairman of many international conferences. The program committee is a forum where members discuss which papers submitted to the conference are to be included in the proceedings. Since space is limited, there are times when even good papers cannot be included, and disputes in this regard occur not infrequently. This committee is an important gathering where one can listen to the true feelings of other committee members on a variety of research results. However, unless you are well connected, you are almost never invited in, and it was even difficult for me when serving as conference chairman to get a seat. On the other hand, once you do get into a program committee, your connections widen, and I have been called upon to give invited lectures and participate in other activities as a result.

Answering the question "What is safe?" to formulate a fundamental theory of cryptography

—Can you tell us about your current research?

My research concerns basic cryptographic theory, and while this may be a bit difficult to understand, my

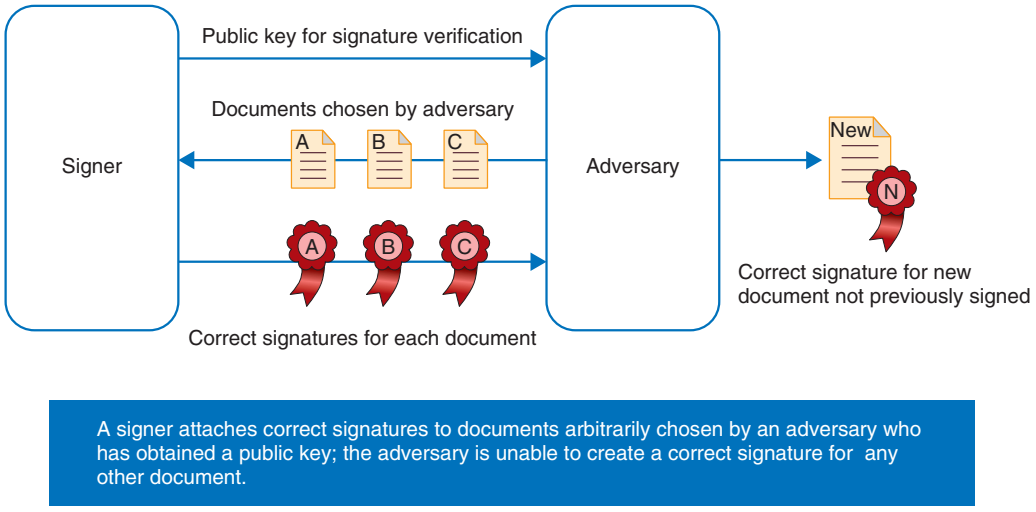


Fig. 1. Existential unforgeability against adaptive chosen message attacks.

aim is to create a foundation for safety in the provision of various types of products and services.

For example, I think about the question "What is safe?" in my research. This is what I would call cryptographic theory—defining the concept of safety from a theoretical and mathematical perspective. Let's imagine that person A sends the message "Tomorrow's plans are cancelled." to person B in encrypted form. Now, if an eavesdropper happens to view that ciphertext but cannot restore it to the original message, I wonder whether or not we can call that encryption safe. If a high degree of safety is desired, it is essential that no part of that message, such as "tomorrow's plans" or "are cancelled," be leaked. Partial information of this type such as what kind of plans were made for tomorrow or what has been cancelled could be very valuable to an eavesdropper. It is also necessary to deal with even more aggressive attacks such as those that send out ciphertexts that generate decryption errors and then analyze the type of error message returned to get hold of internal information.

This view of "safety" also holds true for digital signatures, one of my research themes. For example, if someone would like to forge an IOU with a digital signature saying "Mr. Abe borrowed 1 million yen" but there's nothing to forge such a document from, then can we say that we have a "safe" system? Moreover, if an IOU with a signature stating "Mr. Abe borrowed 100,000 yen" were to exist beforehand, and if "100,000 yen" could be rewritten as "1 million yen," we would certainly have a problem. In short, if an adversary can get hold of signatures for arbitrarily chosen messages but cannot create a signature for any other message, we can call this situation "safe". This kind of safety is referred to as "existential unforgeability against adaptive chosen message attacks," which, with the exception of physical attacks, is considered to be a standard of safety that must be satisfied by a digital signature system (**Fig. 1**). There are also schemes such as blind signatures and group signatures with more advanced functions, but the usage scenario differs for each, and as the usage environment becomes more complicated as the functions become more advanced, it becomes increasingly difficult to accurately express what is "safe" about each system.

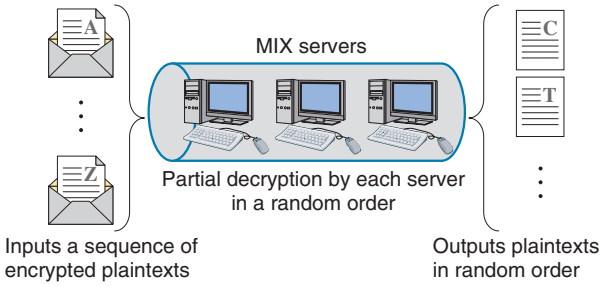
You cannot expect to construct a safe system without clearly defining what "safe" is, and without sufficiently investigating whether that is truly a valid definition. The result of creating such a theoretical foundation is not something that is quickly manifested, but I believe that such foundations contribute to the safety of systems and methods used in society.

—Can you tell us about any specific achievements?

Well, I have published theoretical results as journal papers, but I have also developed various encryption schemes on top of those theoretical foundations. One example is the ECAO (Elliptic Curve Abe-Okamoto) signature, which is a message-recovery type of digital signature scheme in which existential unforgeability comes down to the discrete logarithm problem on an

elliptic curve. This scheme has been adopted by ISO (International Organization for Standardization).

To give a more concrete example, I independently developed a mix-net anonymous communication scheme. This scheme can be used as the core component of an electronic voting system and has already been introduced to regional voting systems in Japan (**Fig. 2**). In this regard, anonymous communication software called Tor has recently appeared as one example of a mix-net application. Tor is a system that protects the privacy of users by preventing their communication paths from being traced. It can be used for whistle-blowing purposes, for example, and its use in the Arab Spring pro-democracy movement in the Middle East was recently in the news. Technology of the Tor kind has both a good and bad side to it, and while it was not a product of my own, this use of research results specifically for such activities reminded me of how socially significant my research field is, as a researcher pursuing safety in terms of privacy.



Encrypted plaintexts from multiple users are received by a set of servers in a multiplex manner. Each server performs some decryption before passing on results to the next server in a random order. A random sequence of plaintexts is eventually output, and anonymity is protected since which user input which plaintext is unknown.

Fig. 2. Achieving transmission anonymity by mix-net.

Structure-preserving signatures that efficiently combine cryptographic components successfully developed in 2010!

—Can you tell us something about structure-preserving cryptographic systems that you are now working on?

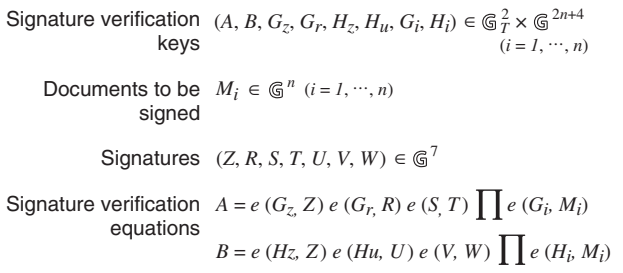
There was a time when fears were growing about privacy infringements by companies. In 1999, there was talk that the Pentium III was equipped with a CPU (central processing unit) serial-number notification function, and that mounting that chip on a personal computer would enable that user to be identified and all user activity, for example, websites visited, to be determined. Then, in 2003, Benetton, the clothing retailer, decided to tag its products with small radio frequency identification (RFID) radio chips to improve product management. This kind of product/customer management raises fears that, in the extreme case, such chips could be scanned at some location to determine who is wearing what item and other types of personal information. Such corporate actions have given rise to boycotts and other forms of protest. Walmart in partnership with Gillette also conducted an RFID-based tag-management experiment and likewise created an uproar among consumers.

As a result of these experiences, the idea that "ignoring customer privacy issues is wrong" began to permeate corporate consciousness. For example, a cryptographic protocol was proposed that would prevent any serial number incorporated in a chip from being disseminated to the outside world and that would only make it possible to verify whether "a genuine chip is mounted." This protocol is currently in the process of being standardized. In other words, the need was felt for a technology that could indicate that something holds true while hiding other details.

My research objective is to construct an efficient cryptographic protocol that can prove the correctness of something while preserving privacy in this manner. As part of this effort, I have been working on the micro-problem of how to combine cryptographic components to achieve "safety." First, in 2008, I attempted to achieve an advanced type of digital signature called a "blind signature" that would combine a digital signature with a tool for convincing another party of something, which is called a non-interactive zero-knowledge proof. However, the interfaces of these two components were completely different, which created a problem. Specifically, an efficient digital signature has a mathematical structure expressed by group elements, while a non-interactive zero-knowledge proof accepts input expressed by a logic circuit to maintain maximum versatility. I therefore saw the need for middleware that could make the input and output of these two components compatible. Theoretically speaking, middleware could combine these components well, but it could also be a source of program bugs while delaying development

work. With this in mind, I arrived at the idea of creating cryptographic components having compatible input/output to maintain a "group structure."

At first, I ran into problems, as I was not able to create a digital signature having structure-preserving characteristics. One aspect of cryptography is guaranteeing safety by outputting input information in a form different from its original form in such a way that the original form cannot be restored. As a result, it was very difficult to satisfy the constraint that the input and output have the same form while also achieving safety. Nevertheless, by applying a trial-and-error process and building up empirical rules much like solving a puzzle, I at long last made the first step in achieving a structure-preserving scheme in 2010 (**Fig. 3**).



By treating public keys, documents, and signatures as group elements on an elliptic curve, only group operations and pairing operations need to be performed to verify signature correctness. These characteristics make for efficient non-interactive zero-knowledge proofs.

Fig. 3. Structure-preserving signature scheme.

—What are your future ambitions?

When new worldviews or methodologies are proposed, many problems arise that need solving. There are also many things that cannot be accomplished by such methodologies that need to be pursued. At present, I am working on various new problems that seem to be arising one after another in that way. I often find myself thinking, "I want to enhance this paradigm," and that generally takes two to three years. Additionally, I would like to continue my research in efficiently creating cryptographic protocols that can protect privacy.

Playing with his children and listening to jazz piano as his great pleasures

—What do you do for rest and relaxation?

When I am engrossed in my work, I cannot get the research out of my head. However, once my concentration is broken, it's difficult to return to a zone of deep thinking. Thus, during times of concentration, it would be a shame to stop while commuting. For me, thinking is not a stressful activity. Stress for me is not getting a good reception for a paper that I have written to convey a scheme's benefits and safety. At most major international conferences related to cryptography, the paper selection rate is about 20%. I myself have lost out two times. I get especially stressed when my paper is not understood even after submitting it repeatedly. Of course, I am very pleased when a paper of mine is accepted, and I'm in a great mood for a while after that. For twenty years, I have advocated the approach of working with the world in mind, and while I have experienced some very trying times, I have colleagues that have persevered through tough times in the same way.

My greatest pleasure is taking my children to a pool in a neighborhood park and spending time with them on weekends. Since I will not be able to do this once they get older, I want to play with them as much as possible at this time.

In addition, during my stay in the United States, I wanted to do something that I could not do in Japan, so I bought a vacuum-tube audio system at an auction and listened to jazz piano to my heart's content in my room. Later, I found that I could not do without this audio system even on returning to Japan and my small apartment, and now I often listen to music using headphones. I especially like the pianist Marian McPartland.

Don't shut yourself off from the outside world—current technology may last only 10 years but personal relationships can last a lifetime

—Dr. Abe, please leave us with a message for young researchers.

When I look at young researchers, there is much to be admired and to be amazed at—they are truly industrious and serious about their work.

So I can't say that I have any advice in particular, but based on personal experience, I would like to point out that new technology comes around about

every five years and that a certain type of technology may last for only five to ten years before becoming obsolete. That is a natural cycle. Personal relationships, however, can be maintained for 20 years and longer, and the benefits they provide can change with the passage of time. I would therefore encourage young researchers to create opportunities for themselves to talk with all kinds of people all the time. In other words, do not close yourself off in your research laboratory and limit your relationships to the same set of colleagues. If you talk about your ideas to ten people, some of them may become quite captivated about your work, which will more than make up for your efforts. And if you get an opportunity to do research overseas, by all means take it!

Interviewee profile

■ Career highlights

Masayuki Abe received the B.E. and M.E. degrees in electrical engineering from the Science University of Tokyo and the Ph.D. degree from the University of Tokyo in 1990, 1992, and 2002, respectively. 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 multi-party computation, supervised by Professor Ueli Maurer. From 1997 to 2004 he was in 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 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 has been a Senior Distinguished Researcher and Research Group Leader of NTT Secure Platform Laboratories since July 2013.