R&D Spirits

Deepening Cryptographic Theory and Advancing Information Security

Masayuki Abe
Distinguished Researcher, Information Security Project
NTT Information Sharing Platform Laboratories

In today's world, in which information of all kinds is being digitized, there is a pressing need for more secure information environments and communication systems. The Information Security Project at NTT Information Sharing Platform Laboratories is actively working on solutions to meet this need. What kinds of problems arise in cryptographic techniques, the basis of information security, and what are some worldwide trends in cryptography research? We put our questions to Masayuki Abe, a distinguished researcher in this project with many achievements in cryptographic theory.

Researching basic theory in cryptographic techniques essential to information security

—Dr. Abe, what kind of research are you currently working on?

Our group is now focused on cryptographic theory as part of information security. In recent years, cryptography has come to be used not only to prevent the interception of messages, but also for a wide range of applications including digital signatures, electronic money, and electronic voting. In such an environment, we can imagine various types of attacks that aim to break down information security, and it is our mission to develop cryptographic theories that are robust against such attacks.

—What specific themes are you involved with?

One recent theme of ours is "hybrid encryption." To put it simply, hybrid encryption is an encryption scheme that combines public-key encryption, which, though highly secure, cannot handle long messages (**Fig. 1**), and private-key encryption, which can handle long messages but is not highly secure. It is consequently a scheme that can handle a large amount of data while having a provable level of security (**Fig. 2**). In this regard, I have been working on a framework called Tag-KEM/DEM based on the KEM/DEM framework (that combines a key encapsulation mechanism and a data encapsulation mechanism) proposed in 2001 by Dr. Victor Shoup of New York University and Dr. Ronald Cramer of Aarhus University. This Tag-KEM/DEM framework makes for more efficient hybrid encryption schemes that are easier to develop.

Another theme that we have been working on is "zero-knowledge proofs." A zero-knowledge proof is a method of convincing a verifier that something is correct without revealing any information. For example, given a padlock, a zero-knowledge proof would prove that it can be opened without showing a key or the act of opening it. There are many levels of zero-knowledge proofs, from computational zero-knowledge proofs that provide no useful information in the proof to complete zero-knowledge proofs that provide no information at all. Of these, the complete zero-knowledge proof has not yet been proven to be secure, but I am proposing a system with provable security based on certain premises.

—What makes these research themes stand out?

The Tag-KEM/DEM framework slightly extends the existing public-key encryption scheme while

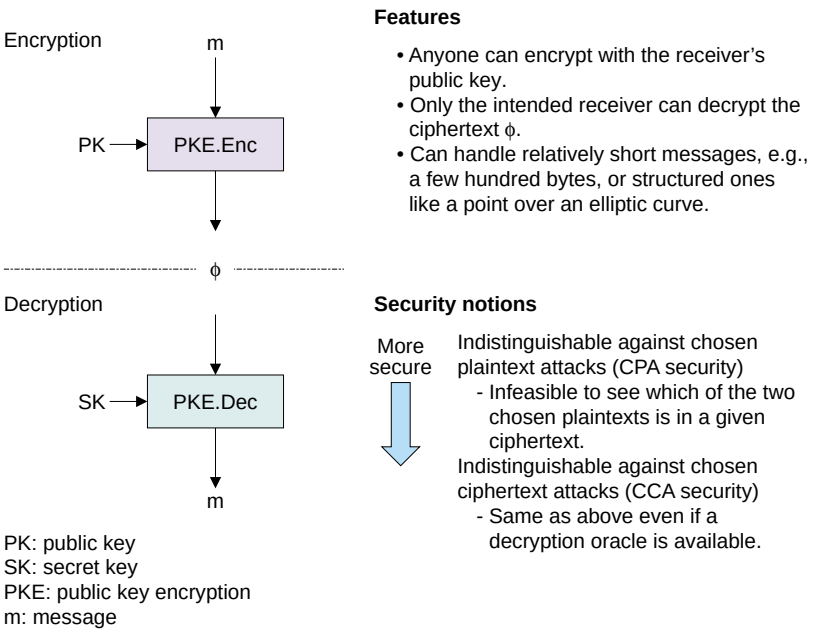


Fig. 1. Public-key cryptosystem.

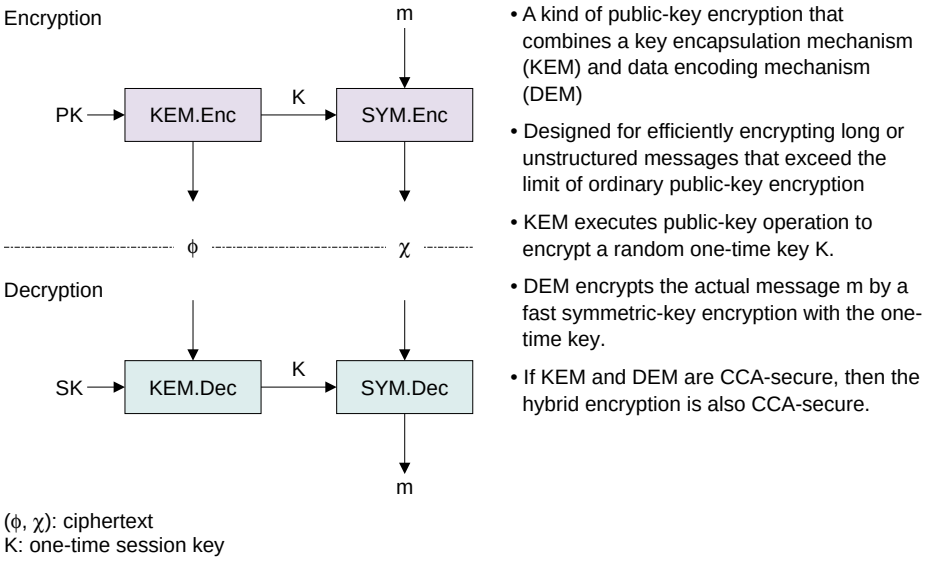
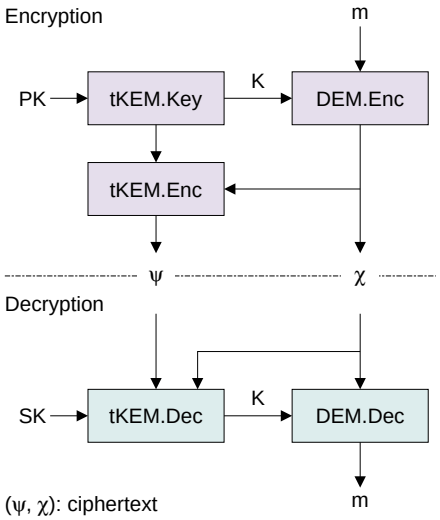


Fig. 2. Hybrid encryption.

adding a function for verifying that the data in question is correct (**Fig. 3**). In this way, despite the fact that private-key encryption is relatively weak, the combination of both types of encryption enables a very strong encryption scheme to be achieved. This framework makes it possible for a developer to focus his or her efforts on only public-key encryption. Tag-KEM/DEM is also modular in nature, which means that schemes based on it are much more efficient than existing schemes. As for zero-knowledge proofs, I believe they have great academic significance. Of course, some people may question the need to work on highly difficult problems such as these now that practical systems of a simpler level are being established. Nevertheless, as long as scheme efficiency is not sacrificed, I believe that security should be as high as possible and that there should be a variety of schemes available as products.



- KEM is extended to tag-KEM, which separates the session-key part (tKEM.Key) from the encryption part (tKEM.Enc).
- The output of the DEM part is given to tKEM.Enc as feedback.
- If tKEM is CCA-secure, then the hybrid encryption is CCA-secure even if DEM is only CPA-secure.
- CPA-secure DEM is very easy to construct, while CCA-secure DEM usually requires extra components such as message authentication codes.
- Tag-KEM can be made of various existing KEMs or PKEs with a small computational cost.

Fig. 3. Hybrid encryption using Tag-KEM/DEM framework.

—What kind of role do you think your research will play in tomorrow's world?

I am mainly involved with basic theory. Even in the case of Tag-KEM/DEM, the fact that I have established a framework does not necessarily mean that it will be readily accepted by the outside world. What I do is no more than present new possibilities to the world at large. It is beyond the scope of my work to consider how to specifically apply this framework. I can say, however, that my framework has the potential to be incorporated wherever there is a need for provable security and efficiency in encryption. In a similar manner, I believe that zero-knowledge proofs could be applied wherever there is a need to persuade someone that a process requiring confidentiality has been performed correctly. Electronic voting is a good example of where this need would arise. In particular, when votes are to be cast for multiple candidates in a one-vote-per-voter system, the theory of zero-knowledge proofs should be especially useful in preserving voter privacy by concealing who voted for whom while proving that each voter correctly cast only one vote for one of the candidates.

—How is your research progressing and what do you see as future issues?

Well, as I am always researching several problems in parallel, I still have a number of problems that I must deal with. Furthermore, as I just touched upon, I really have no idea how the Tag-KEM/DEM framework will develop from here on. For example, if the development team here were to embark on creating something that uses hybrid encryption, I would probably become involved to some extent if Tag-KEM/DEM were to be used.

Keeping aware of a world mixed with competition and cooperation

—What are some worldwide trends in cryptography research?

The International Association for Cryptologic Research (IACR), the nucleus of world cryptography research, currently supports the Crypto, Eurocrypt, and Asiacrypt conferences. Papers accepted by these three conferences tend to have a great impact on the field, and we target these conferences in our research. As for individual research institutions, the Massachusetts Institute of Technology (MIT) and the IBM Watson Research Center in the USA and the Weizmann Institute of Science in Israel are at the forefront of this field. These three institutions engage in many personnel exchanges and it would be no exaggeration to say that they are the current leaders in cryptography studies. In Europe, the École Normale Supérieure (ENS) and France Telecom in France, the Swiss Federal Institute of Technology Zurich (ETH), the National Research Institute for Mathematics and Computer Science in the Netherlands (CWI), and Aarhus University in Denmark are strong. There are also a number of research communities in Asia, and I think it would be fair to say that the strongest of these is our community here at NTT.

—What has been the response to your research in academic societies and elsewhere?

In research dealing with basic theory, the time between publishing a paper and receiving a reaction to it is somewhat long, and our field is no exception. It is not unusual for a paper to become a topic of discussion several years after its publication. To give you an example from a few years back, the research paper on an anonymous communication theory called MIX-net published at Eurocrypt in 1998 is now being referenced by many researchers, giving birth to various forms of derivative research. Now, while I don't expect my theory to generate great commotion and change the world, I am always pleased when researchers in my field take notice and offer their comments.

To give you another example that, while not my own research, has put NTT in the limelight, the Okamoto-Uchiyama encryption system developed by Tatsuaki Okamoto, an NTT R&D Fellow, and Shigenori Uchiyama, currently an associate professor at the Graduate School of Tokyo Metropolitan University, has come to be frequently cited. Likewise, the cipher conversion system developed by Tatsuaki Okamoto and Eiichiro Fujisaki for electronic-money transactions is now being used in various situations.

—Are you involved in any collaborative activities with other research institutions or researchers?

We feel that it is our mission to make scientific and technical contributions that go beyond a corporate or organizational framework, and for this reason, we are actively engaged in collaboration with the outside. For example, the Tag-KEM/DEM framework that I just described was a collaborative effort with Professor Kaoru Kurosawa of Ibaraki University. And talks on collaborating with the IBM Watson Research Center are progressing. On the other hand, unrestrained collaboration is somewhat difficult from a corporate viewpoint, but I want to continue with collaborative activities as much as possible in the years to come.

—How about competition, as opposed to collaboration?

There are many examples of competition. In this field, butting heads in research is not rare. For example, many times researchers that I have had no prior exchange with at all have said to me: "I have been researching the same material as in the paper that you published." Conversely, in my research of zero-knowledge proofs, I was beaten to the punch by a UCLA researcher in an academic-society presentation. In the 1980s, when I first got involved with cryptography research, this field was still quite small with attendance at international conferences being only a few dozen. But today, the biggest conferences have reached a scale of about 400 attendees. The competition between researchers has increased in proportion. Consequently, if researchers do not keep themselves in tune with outside activities, they will not survive in this field. It can be a very harsh world out there!

—In addition to the above, are you involved in any standardization activities or conference committees?

I consider standardization to be another of our important missions, and I am actively involved in several cryptography groups. At present, the Abe-Okamoto digital signature that I proposed is being discussed at ISO (International Organization for Standardization), and it appears that it will become an international standard soon. I am also involved with Asiacrypt and other international conferences, and I have been serving on committees every year for the last several years. Next year, I will be serving as the Program Committee chairman at CT-RSA.

The pleasure of finding and researching unsolved problems

—Dr. Abe, what is the foundation of your technical expertise?

At university, I majored in electrical engineering and did some research in speaker recognition, one area of speech recognition. I was involved, in particular, with the problem of how to have a database cope with changes in a person's voice over time, and I guess you can say that this was one form of security technology. Perhaps it was simply fate that my present research theme would be cryptography.

—What motivated you to enter NTT Laboratories?

While still a student, I was given the opportunity to make a presentation at a certain academic society. By chance, I happened to observe a presentation given by an NTT researcher, and I was very impressed with his energetic and professional style. This was how I first became truly aware of NTT Laboratories. At that time, I was unsure whether to continue with speech-recognition research as a career, and I sometimes thought that I should put myself in a situation where I could pursue R&D with a scope as wide as possible. I therefore thought that NTT Laboratories, which

covers a wide range of themes from pure basic research to end-product development while having extensive R&D facilities, might be just the place to do some very interesting research. Of course, this was just a hastily drawn conclusion typical of a young student, but looking back, I don't think I was mistaken at all.

—Could you tell us about your research career up to now?

I entered NTT Laboratories in 1992 and was first assigned to the design and development of cipher-and-authentication LSIs. At that time, both cryptography and LSIs were an unknown world to me, so I had to study these areas starting from zero while I worked. Somehow, my designs finally took shape. I heard that they were eventually commercialized and used in facsimile machines. My next assignment was the development of a C-language library for use in cryptographic authentication. In this work, I established internal and interface specifications and selected algorithms. Then, in 1995, I became engaged in protocol development and design for electronic money as a cryptography application.

Next, in 1996, after expressing my preferences for some time, I embarked on a one-year stay at the Swiss Federal Institute of Technology in Zurich as a guest researcher. This institute, commonly referred to as ETH, gave me the opportunity to work on "multi-party competition," a theme that I am still involved in. Going to ETH had a big influence on my future direction. After returning to Japan, I began to pour much of my energy into basic theory, particularly on definitions of "secure" and on requirements and conditions for achieving such security. Part of this research resulted in the Abe-Okamoto digital signature and other achievements. Later, on becoming a distinguished researcher in 2003, I journeyed to the IBM Watson Research Center, the Mecca of cryptography research, hoping to make myself better known in the field. Here as well, I was fortunate in obtaining significant results including the completion of the Tag-KEM/DEM framework.

—What is the attraction of research for you?

First and foremost, it is scientifically interesting. Nobel-prize-winner Richard P. Feynman said that research in itself was a great pleasure. That's exactly how I feel about it. Of course, research becomes all the more worthwhile if something that I think of or create on my own turns out to be useful to society. But even if that is not the case, I believe a researcher will always feel motivated as long as problems exist that have yet to be solved. At present, my interest within basic theory is shifting toward unsolved problems of high difficulty. One reason for this lies in my desire to raise my personal hurdle, much like going to the next level of a video game. Today, as cryptography matures as a field of study, techniques for simply encrypting data have already reached a sufficiently practical level. From an application viewpoint, problems of low difficulty are steadily decreasing. It is therefore natural that I turn my attention to unsolved problems of high difficulty. Likewise, requirements from the product side are becoming increasingly severe. For example, on hearing talk about a desire to encrypt the contents of a terabyte-class hard disk all at once, I thought how great a challenge that would be and how I would like to give that problem a try. However, I cannot get involved in everything without a decrease in personal performance, but whatever I do select I would like to solve a problem of high difficulty.

Making one's presence felt by a steady stream of achievements

—Dr. Abe, how do you see your research developing in the years to come?

For the future, I have two visions: one from an academic viewpoint and the other from a corporate R&D viewpoint. From an academic viewpoint, I would like to undertake unsolved problems in basic theory as I mentioned. From a corporate R&D viewpoint, I would like to introduce innovations in cryptographic applications for future use in business. Here, I would like to search out and develop business applications conducive to cryptographic techniques following in the footsteps of electronic voting, electronic money, and electronic auctioning. I should point out, however, that these business-related pursuits should be done in collaboration mainly with young researchers as opposed to being something that I do on my own. These two directions are not contradictory. Establishing the basics can provide hints of new business models, and conversely, innovations in business can prompt the search for essential basic theory. In this way, these two directions have a mutually beneficial effect on each other.

—What is your ultimate goal as a researcher?

In cryptography research, I would like to make the name "Masayuki Abe" known as that of a researcher. But even in cryptography, there is a wide range of

areas to specialize in from basic theory to application development much like the areas undertaken by mathematicians. As I started out in engineering, I feel that researching frameworks that provide a glimpse of final applications is a perfect activity for me and quite enjoyable at that. Of course, in a position like this, it is not easy to deliver results of a "homerun" level that would create a sensation in the outside world. But I would rather prefer being known as "Dr. Abe of cryptography research" through a steady succession of research hits.

—What is it like working at NTT Laboratories for you personally?

I feel that NTT Laboratories is like a "field" and that I'm like a "crop" being given nutrition by that soil to grow. From time to time, a strong wind may blow, but my roots are firm supported to prevent me from blowing away. Without this field called NTT, I could do nothing.

—Dr. Abe, could you leave us with some advice for young researchers?

I'd be happy to. First of all, I would like you to carry on your research while keeping yourself continuously aware of happenings overseas. You must face the outside world and make your presence known without being afraid to put up a good fight. As I mentioned earlier, the international competition in this field is very severe, and you will miss many chances if you only concentrate on the research environment that you are presently in. You should also keep in mind that overseas evaluation can be a good thing for the research environment in Japan. But to this end, English skill is a must! And I don't mean just the ability to write papers in English, give presentations in English, and read English-language journals like this one. You must also be able to carry on concise discussions in English so that you can become a true member of the global research community.

By the way, when I was a university student my English was very poor, but when I entered NTT, the president at that time said that learning English was only natural for a researcher. And my superiors were always willing to give me help in writing papers in English. I am proud to say that I have been able to produce some results in my research life up to now because of my development in NTT "soil" and because my research targets were zeroed in on overseas. Of course, there are also researchers like Shuji Nakamura, the inventor of the blue laser diode, that achieved results worthy of a Nobel Prize through research activities all within Japan. But to raise your personal evaluation as a researcher, I believe that one effective strategy is to turn your eyes to overseas activities early in your career.

Interviewee profile

■ Career highlights

Masayuki Abe received the B.E. and M.E. degrees in electrical engineering from the Science University of Tokyo, Tokyo, and the Ph.D. degree from the University of Tokyo, Tokyo, in 1990, 1992, and 2002, respectively. He joined in 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, 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 other signature schemes with additional functionality, 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 visiting IBM T. J. Watson Research Center working with the Crypto Group and researched hybrid encryption, zero-knowledge proofs, and universally composable protocols. He has been a Senior Research Scientist since October 2005 and a Distinguished Scientist of NTT Information Sharing Platform Laboratories since January 2006.