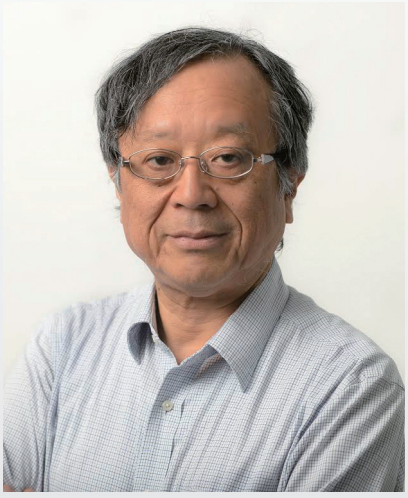
Aiming to Be the World's Top Cryptography Laboratory

Tatsuaki Okamoto
NTT Fellow, Director, Cryptography & Information Security Laboratories, NTT Research, Inc.



Overview

Information and communication technology is used in all types of business activities, and expectations concerning security and reliability of cryptography—which is key to information security measures—are increasing. We asked Dr. Tatsuaki Okamoto, an NTT Fellow who spearheads the Cryptography and Information Security Laboratories (CIS Labs) of NTT Research, Inc., employing top scientists in cryptography and blockchains, about the progress of CIS Labs and his attitude toward being a distinguished researcher.

Keywords: cryptography, blockchain, attribute-based encryption

Forming a dream team in cryptography research that can be done only in the USA

—Please tell us what you are currently doing.

As the director of the Cryptography and Information Security Laboratories (CIS Labs) of NTT Research, Inc., I work mainly in management. The last time I appeared in this column, I was talking as a researcher; this time, I'm talking from a management perspective. That is, regarding themes such as cryptography and blockchain we are working on at CIS Labs and what kind of research institute NTT Research is.

Although NTT Research was launched in July 2019, we had been preparing long before that. Since we were starting from scratch, I was particularly focused on gathering people and building an organizational system during the six months before the opening of NTT Research. Prior to the launch, in 2018, when I was asked to work there in my research field of cryptography, I wanted to do something that could not be done in Japan and could only be done in the USA. First of all, we needed to recruit human resources, and the Bay Area attracts many well-known and outstanding people from around the world. Taking advantage of this, our goal is to establish the world's top cryptographic laboratory by gathering people who are active in cryptography to create a "dream team."

—What was your plan for forming a dream team?

What we should focus on in this research field is an important strategic issue. I chose core cryptography and blockchain as research themes and decided to promote them at a respective ratio of 7:3. Starting around the end of 2018 with a focus on those themes,

we began to recruit researchers, and as of February 2020, ten people have joined. In cryptography, we have six prominent researchers, led by Dr. Brent Waters, and in blockchain, we have four outstanding researchers, led by Dr. Shinichiro Matsuo, who is also researching at Georgetown University. However, there are many places to work such as startups and venture companies regarding blockchain. People are inevitably attracted to those places, and few want to do basic research. As a result, we have some difficulty in securing human resources in that field.

Although the laboratories have opened, our recruitment activities are ongoing. A new top researcher in cryptography joined us in March 2020. Taking a long-term perspective, we plan to hire more human resources. Many outstanding researchers are not in a situation where they can immediately join us when we invite them. For example, if they work at a university, they cannot retire immediately and enter our laboratories, even if they want to. In consideration of the circumstances of each researcher, we are making arrangements for researchers working at universities to be affiliated with CIS Labs concurrently. Then, as soon as their situation allows, they can pivot towards our laboratory.

We are in an era in which we can work remotely from anywhere in the world; even so, our colleagues are gradually settling here in the Bay Area. NTT Research will reach its first year of operation in the summer of 2020 and it is evolving considerably. We are making steady progress toward achieving my plan.

Take on big strategic challenges

—What are your goals in cryptography research?

The conventional encryption method is based on the concept of putting something that would be troublesome if seen by other people into a kind of 'safe' (encryption), sending it in this manner, then removing it from the safe on the receiver side by using a key (decryption). However, if you try to delete spam mail from the encrypted mail you want to receive, for example, it is necessary to detect and delete the spam mail on the server when it is on its way to you. For that reason, the server decrypts the encrypted email (opens the lock with the key), checks the content of the email, detects and deletes any spam mail, and re-encrypts the email (i.e., puts the messages back in the safe and locks it). In other words, the server (a third party) has a duplicate key for the safe, so in that sense, the role of encryption between the sender and receiver is lost. To put that the other way around, the security of such encryption systems faces various restrictions (including usage).

In contrast to the conventional method described above, the concept known as attribute-based encryption (ABE), or more generally, functional encryption, was pioneered by CIS Labs' Dr. Waters about 15 years ago (**Fig. 1**). As a result, in the above-described example, only the information necessary for detecting and deleting spam mail can be extracted from the encrypted email, without decrypting the encrypted data on the server, and it is possible to detect and delete the spam mail based on that information.

As this new concept of cryptography emerges, to develop highly functional cryptography that has been proven secure under standard assumptions, we are conducting research on (i) methods of conversion from weaker security to desirable security; (ii) design of various cryptographic protocols and security proofs; and (iii) encryption methods based on the learning with errors (LWE) assumption.

I'll now introduce some of our efforts. The chosen-ciphertext security (indistinguishability under chosen-ciphertext attack: IND-CCA) is a class of the strongest security for ciphers with a higher level of security than that of chosen-plaintext security (indistinguishability under chosen-plaintext attack: IND-CPA), which is easier to achieve. For ABE, we recently showed that any IND-CPA-secure ABE can be converted to an IND-CCA-secure ABE by using a new method called hinting pseudorandom generator (PRG). As a result of this finding, we aim to (i) create a faster and more compact hinting PRG by using number-theory techniques and (ii) establish an IND-CCA conversion method that can be applied to general functional cryptography and re-randomized cryptography (**Fig. 2**).

The LWE assumption has been widely accepted as a strong assumption in cryptography in relation to, for example, quantum-resistant security and the worst-case lattice problem, and has seeded many methods for creating new cryptographic functions. Accordingly, we have a new ambitious goal of constructing cryptosystems based on the LWE assumption. We first consider a new concept, that is, obfuscating a pseudo-random function (PRF), and its application. We then show how to build witness encryption from the LWE assumption. As an intermediate step between those two steps, we are constructing a 'restricted PRF,' and in that process, we are trying to find new methods (and their limitations) for

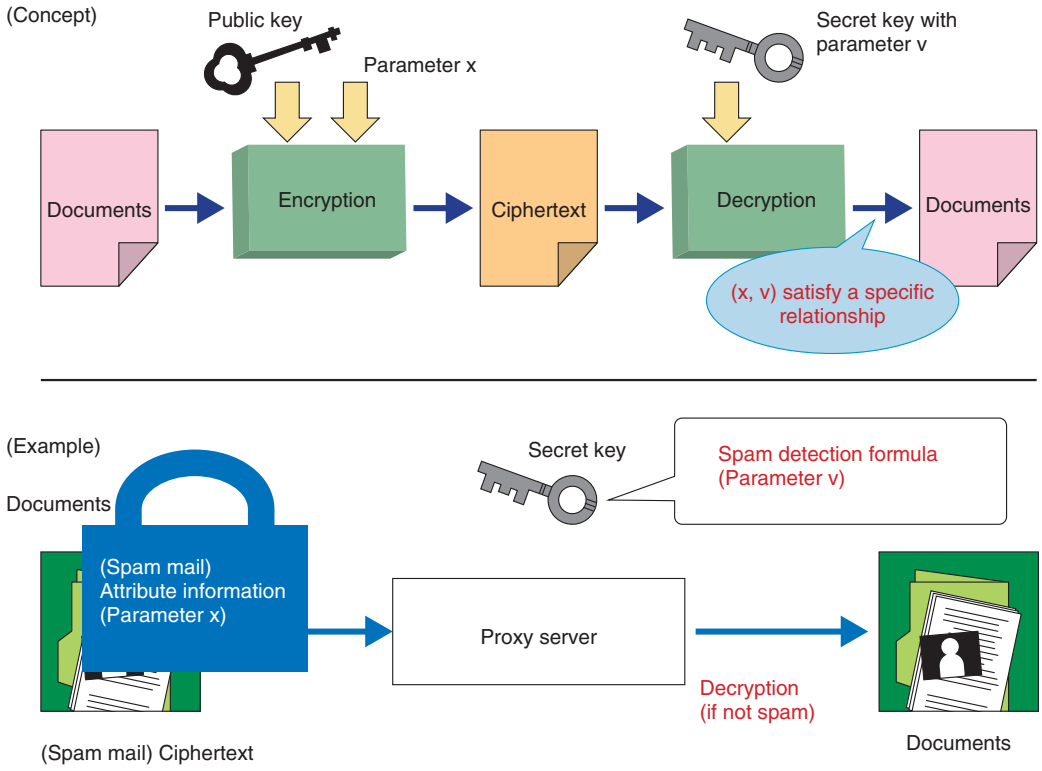


Fig. 1. Attribute-based encryption (functional encryption).

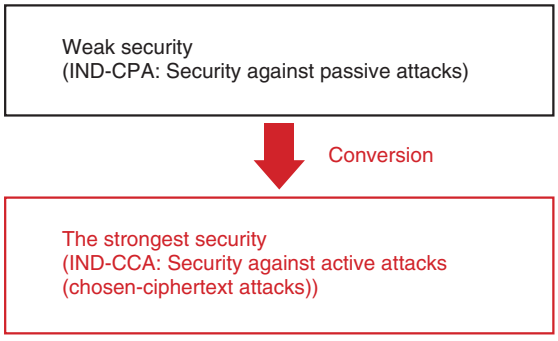


Fig. 2. Converting weak security into desirable security.

achieving adaptive security with LWE-based ABE.

—What about in the blockchain field?

We are focusing on fundamental research to achieve a major goal of research and development (R&D) on blockchain, namely, create an environment in which anyone can freely develop applications that use programmable and shared ledgers (**Fig. 3**).

Bitcoin and blockchain have become hot topics, so it may seem that the time of their widespread adoption is coming soon. However, achieving the above goals is a huge challenge and requires long-term basic and theoretical R&D. To meet that challenge, we are researching (i) secure and more-scalable distributed consensus algorithms, (ii) creation of a secure programming environment for programmable ledgers, and (iii) implementation of privacy protection when information is processed on the blockchain.

Because theoretical research on blockchain requires exquisite combinations of research fields, it is necessary to form a team of researchers with different specialties. Moreover, research on blockchain must be conducted strategically. As I mentioned before, it is difficult to secure outstanding researchers because they tend to flow towards ventures and startups. My team has just started up, so we need to strengthen our human resources. Although my team is composed of researchers with expertise in security of cryptographic protocols, software engineering, formal verification, game theory, and economics, I plan to recruit more researchers with different specialties.

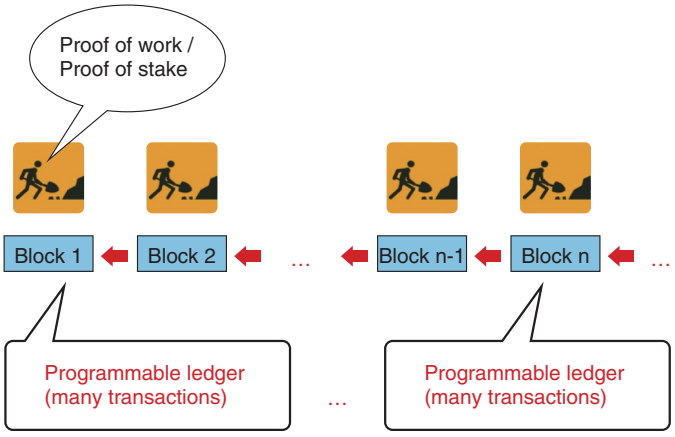


Fig. 3. Programmable public ledger by blockchain.

The only way to be recognized is to achieve results as a researcher

—Where do you look when identifying talented people? In other words, could you tell us how to impress you from the applicant's viewpoint?

I don't think researchers need to impress us by any means other than their achievements. In academic societies in which professional researchers in certain fields gather, outstanding researchers evaluate each other. For example, Dr. Waters of the cryptography team is a world-leading researcher, and he knows a lot of excellent researchers in all aspects of the field, including key figures and young researchers. Current team members were also recommended by him. Although some researchers have heard rumors about us and promoted themselves during the six months since our establishment, we basically do not take on self-recommended people; instead, we hire people who have outstanding achievements and abilities in certain research fields. Dr. Matsuo of our blockchain team is also familiar with talented people in that field, and we welcome researchers on his recommendation. Even in the case of young student researchers about to receive a doctorate, their research achievements have something that shines differently from those of others, so we can find them. In other words, I don't think there is any other way to attract us other than achieving results as a researcher.

—What are you aware of when searching for research issues or themes?

I'd like to make the most-important issues in my field of study into research themes. Those issues should determine the direction of the research field as well as interest me. When involved in discussions while collaborating in research with various people, we may discover new themes together. At such times, even if someone rates a topic as interesting, I don't necessarily want to make it a research theme if I don't find it important. However, there are many different cases, and topics that did not seem so important at first consideration can later become central themes. Although selecting themes can be difficult, basically, a good researcher has a good sense, so I think that you can often select themes based on that sense. As I said in my interview ten years ago, in a nutshell, these themes are the tastes of the researchers. In the case of the arts, taste is like an aesthetic sense, and what we are waiting for in our research is a kind of intuition that determines whether we are in a fruitful place or the wilderness.

No matter where you are, aim for something original, not an imitation

—What is your vision for the future?

As a team, we aim to be a world-class group of researchers recognized by both ourselves and others. I think we are pretty close to the top, but I want to make sure we are. I want us to receive accolades such as a major award that proves the achievements of

each researcher. Since cryptography is a field of computer science, it is not subject to the Nobel Prize. Therefore, one of our goals is to win the Turing Award, which has been declared the Nobel Prize of computer science. I want us to win this award to build our reputation to make it clear that NTT Research is a research institute with globally prestigious award-winning researchers.

As an individual, I'm working on something as my lifework. The world is complicated. For example, life forms are very complex. It is also known that the universe has evolved from a simple form immediately after the Big Bang to its present complex form. In regard to things that are said to be complicated in this world, I want to take a unified perspective as a kind of science. Although the research field of complexity science has been around more than 30 years, as an extension of that field, I want to put out something that is theoretically exact. I'm 67 years old. I don't think that my management job can go on for much longer, but I want to continue working as a researcher for a little longer.

—Please say a few words to our young researchers.

Working outside of Japan, I have the image that Japan is shrinking slightly. In the 1980s, Japan experienced an economic bubble, so "Japan as number one" was often heard; however, Japan today has less presence in the world. Companies like the GAFA (Google, Apple, Facebook, and Amazon) in the information technology (IT) industry spend more than 10 times more on R&D than NTT. Under such circumstances, if Japanese companies simply repeat the way of doing things that has been successful in the past, it may not be possible for them to make their presence felt much globally. Currently, even the most successful IT companies in Japan have little presence around the world. Therefore, how can we make our presence felt? We are just running around in small circles if we just focus our activities in Japan, so we are taking the initiative through global endeavors at NTT Research. It is important to create something original, not an imitation. I feel that Japanese venture companies often imitate others. You have to have the spirit to create something unique. In this era, since we are all online, you ought to be able to do what can be done in Silicon Valley or Tokyo (or in any region of Japan). I want you to turn your perspective toward the world and create original ideas with the spirit that this is second to none.

■ **Interviewee profile**
Tatsuaki Okamoto
Director, Cryptography & Information Security Laboratories, NTT Research, Inc.

He received a B.E., M.E., and Ph.D. from the University of Tokyo in 1976, 1978, and 1988. He has been working for NTT since 1978 and is an NTT Fellow. He has been a director of NTT Research in USA since 2019 and engaged in research on cryptography and information security. He served as president of the Japan Society for Industrial and Applied Mathematics (JSIAM), director of International Association of Cryptology Research (IACR), and a program chair of many international conferences. He received the best and life-time achievement awards from the Institute of Electronics, Information and Communication Engineers (IEICE), the distinguished lecturer award from the IACR, the Purple Ribbon Award from the Japanese government, the RSA Conference Award, and the Asahi Prize.