Pioneering a Next-generation Basic Theory and Purpose-specific Cryptography toward the Future of Symmetric-key Cryptography

Yosuke Todo
Distinguished Researcher, NTT Social Informatics Laboratories

Abstract

Cryptography is an essential technology for secure information communications. Types of cryptography include public-key cryptography and symmetric-key cryptography. Here, we're talking to Yosuke Todo, a distinguished researcher who is working on building a basic theory for symmetric-key cryptography and researching purpose-specific cryptography.

Keywords: symmetric-key cryptography, purpose-specific cryptography, tamper resistance

Symmetric-key cryptography: Using a common key for encryption and decryption

—What is symmetric-key cryptography?

In information communications, hiding and protecting your information hinges on encryption. Encryption can be thought of as the "gears," the smallest parts composing the larger system of security. A missing or broken gear can affect the entire system, and may lead directly to safety issues. As such, you could think of cryptography research as pursuing the creation of highly secure, high-performance gears.

Cryptography uses separate keys for encryption and decryption, and within that there is public-key cryptography, which uses a public encryption key, and symmetric-key cryptography, which uses the same key for encryption and decryption (**Fig. 1**).

Public-key cryptography can be compared to a padlock on a shed. Anyone can lock a padlock, but they need a key to open it. Public-key cryptography is a mechanism where there are many distributed "padlocks," but they can only be opened by the person with the corresponding key. To reproduce this digitally, the system is contrived to make use of mathematical problems that are difficult to solve, such as integer factoring, discrete logarithmic problems, and lattice problems. And so, just as with solving these difficult math problems, encryption and decryption require complex computer-based calculations.

On the other hand, symmetric-key cryptography can be compared to a safe in a hotel room. You enter a particular number when you lock it, and then enter the same number again to unlock it. Unlike public-key cryptography, symmetric-key cryptography is

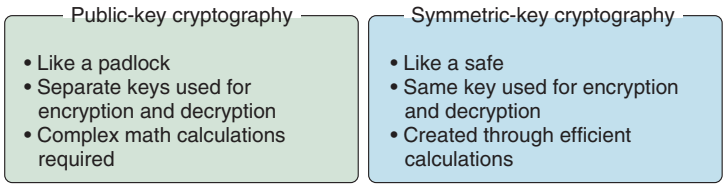

Fig. 1. Public-key cryptography and symmetric-key cryptography.

based on the concept of making efficient calculations based on the environment in which it is used. As a result, symmetric-key cryptography is 100 to 1000 times faster than public-key cryptography, and so is well suited for encrypting large amounts of information.

I work with symmetric-key cryptography, and my current research topics are "A Basic Theory for Next-generation Symmetric-key Cryptography" in the medium to long term, and "Purpose-specific Cryptography and Solutions" in the short, medium, and long term.

—What kind of research is "A Basic Theory for Next-generation Symmetric-key Cryptography"?

Unlike public-key cryptography, symmetric-key cryptography isn't based on difficult mathematical problems, so there are important questions about whether or not the encryption itself is really secure, and how to ensure that security.

For example, the Caesar cipher, used by ancient Roman politician Julius Caesar, could be considered a symmetric-key cipher that shifts each letter of the unencrypted text (the plaintext) a certain number of positions in the alphabet; however, it is very easily attacked. In general, symmetric-key ciphers can be created by anyone, but the drawback is that they can quickly be broken by someone without any special equipment. Nearly half a century has passed since the emergence of cryptographers specializing in symmetric-key cryptography, and nowadays there are many ciphers that are considered difficult to crack. However, even if you can ensure a cipher is secure by testing it with various attacks, you cannot guarantee it will be safe against the attempts of a future cryptographical genius.

The basic theory of symmetric-key cryptography is to discover new methods of attack and analysis, and to explore measures that ensure absolute safety against existing methods of attack and analysis. Of course, it's hard to create truly secure encryption, and in practice it's more like working toward encryption that is absolutely secure against a particular kind of attack, going some way to ensuring overall security.

In a way, this is the defining goal of all cryptographers, and ever since joining the company I have been focusing on an attack method known as "integral cryptanalysis," and studying the complexity of cryptography—phrased more technically, I have been researching the vulnerabilities of attacks that involve accurately estimating algebraic degrees. And to put it simply, it's research that aims to get to grips with the upper bounds of the security of an encryption: knowing that if the encryption is attacked, the security will be lower than a certain level at best. As a result, in 2015 I was the first Japanese person to receive the Best Paper Award at Crypto, the premier international conference in the field of encryption, and in 2020 I became the third ever person to win the award twice. Recently, I have also been working on research where the lower bounds of the security are considered, i.e., where you know that security is higher than a certain level, at least.

—What kind of research is "Purpose-specific Cryptography and Solutions"?

We compared encryption to gears earlier, and gears are generally manufactured without the creators knowing where the gears are going to be used. We're therefore trying to create gears that are as safe and high-performance as possible. However, of course there will be special gears out there that are only used for certain products.

And like these gears, the same approach can be used in creating custom-made ciphers to suit specific applications, which is the topic of my research on "Purpose-specific Cryptography and Solutions." In recent times, Internet of Things devices and smart cards are increasingly handling sensitive data such as personal information, and so more devices require

encryption. In response to this, I am working on lightweight encryption that can be implemented on devices with less computing power than personal computers.

Designing purpose-specific, custom-made ciphers

—In what fields can you use symmetric-key cryptography research?

My research into "A Basic Theory for Next-generation Symmetric-key Cryptography" will potentially create a generic standard cipher; It will combine research from the perspective of the attacker, understanding the upper bounds of the security of an encryption, and research from the perspective of the designer, understanding the lower bounds of the encryption's security, and ensuring high security of at least a certain level. The foundation of today's encryption was developed 40 years ago, so if a new generic standard cipher is built, it could become the foundation for the next generation of encryption, increase security, and find applications in all sorts of fields.

One type of purpose-specific cryptography is ultra-low-energy encryption, which is expected to be useful in the medical field. For example, consider a medical device, implanted in a person, that collects and transmits a variety of vital data to a medical institution. Such sensitive vital data should, of course, be encrypted to prevent plagiarism and tampering. However, it is quite the ordeal to have surgeries every time the device's battery is depleted. So the device needs to run for a long time on a small battery, and the encryption also needs to consume as little energy as possible.

Previous approaches to cryptography have been quite all-purpose, balancing all elements and improving overall performance. However, if you make a compromise in one area you can ramp up the performance in another to suit the application, and this is what I aim to do with purpose-specific cryptography. In addition, various types of encryption may be possible depending on the application. For example, minimizing the circuit size using small sensors, or minimizing the communication latency between the central processing unit and the memory.

I think it would be interesting to ask organizations that deal with confidential data and personal information about how their data are used, and then create new, specific encryption methods to meet those needs.

—What are your plans for future research?

First, we are aiming for ultimate tamper resistance. Current cryptographic safety studies assume that the plaintext and ciphers will be seen by third parties, but that the intermediate stage, during the actual encryption process, will not be seen. However, there have been instances of a type of attack called a "side-channel attack," which figures out encryption keys using information such as the power consumption of hardware and electromagnetic wave leakage. It can be even more serious in the case of software, with instances of reverse engineering being used to extract the algorithms in the encrypted portion of an app downloaded to a smartphone. The strength to withstand these attacks on the encryption process is called "tamper resistance."

Given that the encryption process itself is being exposed, we are now focusing on research areas such as "white box cryptography" and "gray box cryptography" that, while they may not currently be 100% secure, are safe in the event of an encryption algorithm being leaked.

—What is special about your current research environment?

NTT's strength is that it has many talented people. When I joined the company ten years ago, I didn't know about symmetric-key cryptography, how to write papers, or how to conduct research, but I received a lot of guidance from my senior colleagues. We do have to create new research fields ourselves, but when you're just getting to grips with the basics of research, you have the advantage that you can increase the speed and quality of your learning by following the paths skillfully carved out by your

senior colleagues, rather than by studying alone.

I also think it's valuable to have several distinguished researchers in the same laboratory working on the common field of encryption. I think that having multiple distinguished researchers working in the same area will create diversity in research, which will in turn lead to the creation of new technologies. Above all, young researchers who are under the guidance of distinguished researchers will also be promoted if they get important results, which I think will be encouraging for them.

■ **Interviewee profile**

Yosuke Todo joined NTT in 2012 as a master's graduate, and worked for NTT Secure Platform Laboratories. He received the Crypto Best Paper Award in 2015, completed a Ph.D. at Kobe University in 2017, was a visiting researcher at Ruhr-University Bochum from July 2019 to October 2020, and received the Crypto Best Paper Award in 2020. He has been a distinguished researcher at NTT Secure Platform Laboratories since April 2021, and is currently a distinguished researcher at NTT Social Informatics Laboratories.