

Research on Standardization of Lightweight Symmetric-key Cryptography for IoT and Protection Technology for Its Implementation

Yu Sasaki

Distinguished Researcher, NTT Social Informatics Laboratories



Abstract

We are now in an age where the Internet is not only used for communication between people, but also for connecting various devices. Information circulating on the Internet is diverse. Not only personal and confidential information, but also information emitted by devices is at increased risk of being intercepted and misused for criminal purposes. The field of symmetric-key cryptography prevents third parties from eavesdropping on communications. We spoke with Distinguished Researcher Yu Sasaki, who is researching lightweight cryptography for communication between IoT (Internet of Things) devices.

Keywords: symmetric-key cryptography, standardization, NIST

We aim to encrypt all communications, even those used at the edge of IoT, and create a world in which all devices are protected by encryption

—What kind of research are you conducting?

My research topic has remained the same since I joined the company: symmetric-key cryptography. There are two fields of cryptography: public-key cryptography and symmetric-key cryptography. Symmetric-key cryptography is used to encrypt data communications in everyday life due to its fast computations and low implementation costs. Some symmetric-key cryptographies have been internationally standardized as the de facto standard, but there is a

problem in that the validity of the design is unclear. Therefore, we are incorporating cutting-edge theory and aim to design encryption codes that stand out to everyone as both secure and convenient.

Furthermore, public-key cryptography has not been sufficiently evaluated for security. It may be vulnerable to eavesdropping on communication data if a weakness is exploited and an attack is executed. In order to build a strong fortress to prevent this, it is necessary to anticipate enemy attacks in advance. After joining the company, I spent some time learning a code-breaking technique called an “attack.” Attacks involve trying various attack approaches against publicly available encryption codes to find vulnerabilities and show that they are not secure. Of course, the

attack itself is not the goal, but rather to overcome weaknesses and create a world where all communications are protected.

In the world of public-key cryptography, security can be proven by reducing it to a problem that has been mathematically proven to be difficult to break. But symmetric-key cryptography (my research) is a field that requires a delicate balance to be struck, in which performance must be tuned by a skilled craftsman to ensure security. It requires the expertise of a craftsman to take measures by covering anticipated attacks and past attack patterns and to predict and take measures against attacks with new approaches.

—Tell us about the impact of this research.

One example of the use of symmetric-key cryptography is “lightweight cryptography” used for end-to-end communications such as Internet of Things (IoT). In recent years, smart city projects have become popular, and smart sensors have been in the spotlight. Imagine if all gas meters were equipped with sensors and capable of IP (Internet Protocol) communications, gas companies could collect user data from the sensors, calculate monthly usage and fees, and automatically bill without human intervention. What would happen if that gas meter information was sent in its raw form without encryption? There is a risk that the data could be leaked to malicious individuals who intercept the raw radio waves. The extent of this problem is that a thief may learn that someone is probably not at home because their gas bill has been zero for a while. In addition, if the communications from a chip that links with the GPS (Global Positioning System) to display the distance traveled, time, and route on a map when you go jogging are not encrypted, the user’s address and lifestyle patterns will be leaked. To prevent this, my goal is to encrypt all data that reaches the end user.

Recently, there is a tendency to have a third party evaluate the security of the encryption code that the craftsman has designed, because there is a possibility that they are a bad person and may install a backdoor that allows only them to easily decipher the encrypted communication. We can increase transparency by publicly disclosing all of the encryption specifications, and increase credibility by having impartial third parties, such as academics, evaluate and recognize its safety. Once there is a consensus in the community about the quality of an encryption code, we can standardize it and make our technology available to people all over the world. This is my goal in

research, and I try to design encryption codes with an eye toward its standardization.

Participating in multiple teams in the NIST competition to broaden options for cryptographic design

—Tell us about your research environment.

Basic research is close to computer science. For example, when discussing the future, such as how much it will cost to break current codes when quantum computers are perfected, the quantum computers we envision do not yet exist, so we can only simulate them with paper and pencil. Such cases occur frequently.

One of my research topics is attacks on publicly available encryption codes. When thinking about an attack, I start by understanding the encryption code that someone else has created, so I first read publicly available manuals and specifications. When multiple people are considering an attack, we all gather in a small room, like a university laboratory, and read through the materials and discuss them. After that, when it comes to the verification stage, where we actually determine the vulnerabilities of the encryption code and whether previously known attacks are applicable, we recently created an automatic evaluation tool and examined whether an attack can actually be carried out on a computer server.

I am currently based at the National Institute of Standards and Technology (NIST), located very close to Washington, D.C. in the United States. NIST is the organization that decides on the standard technologies used by the U.S. government. Previously it used to solicit excellent encryption codes from around the world in a competition format, and I was a member of several teams that submitted entries. Roles within the team include multiple tasks such as safety evaluation, component design for encryption codes, and speed measurement. Experts from each field come together to create the encryption code through a division of labor. In the case of lightweight cryptography (my specialty), we also have to consider the issue of the device being used [1] (**Fig. 1**).

If the target is a personal computer (PC), electricity is supplied from a power source, but in the case of IoT, the chip has a built-in battery, and if the battery dies, the device can no longer be used. There is no memory, no central processing unit that can be implemented at high speed, and usable batteries are limited, so you need to think about what you want in such

NIST's view on lightweight cryptography

- Encryption that can transition from general-purpose PCs to devices with limited resources (RFID tags, sensors, IoT) is needed.
- The weight of a cryptographic algorithm refers to its implementation performance measured using an evaluation method that depends on the target device and implementation environment.
 - Hardware: circuit size, latency, processing speed, power consumption, etc.
 - Software: RAM size, code size, processing speed, etc.
- Because there are many different uses, it is difficult to choose a single encryption code that is superior in all aspects. The optimal trade-off is important.

Examples of problems that cannot be handled by general-purpose cryptography

- There are 16-bit microcontrollers that do not have enough memory to implement AES encryption and decryption.
- The SHA-3 hash function requires a much larger memory. A lightweight version of SHA-3 exists, but it has not yet been standardized.



Key points extracted from Ref. [1].

AES: Advanced Encryption Standard
RAM: random access memory

RFID: radio frequency identification
SHA-3: Secure Hash Algorithm 3

Fig. 1. NIST's view on lightweight cryptography.

a situation and make a selection. However, high-speed computation and low power consumption are contradictory goals, so you cannot achieve both at the same time. Therefore, we must consider the specific application and choose the one that achieves the best balance for that application. That is why I was involved in multiple teams. Each team has different characteristics, such as being good at a certain approach, so I participated in multiple teams to find more options.

We aim to demonstrate the security of the encryption we have created, standardize it, and have it used by many people in the future

—Tell us about the current results of your research and its future prospects.

Cryptography research is similar to mathematics research in that it has an aspect of theoretical research. In that sense, rather than promoting practical applications, we are working to delve into cryptography theory, just like mathematics. In terms of results in this regard, many of our papers have been accepted for publication, and we are gradually being entrusted with more important work by the International Association for Cryptologic Research (IACR), which is our forum and community. Personally, I feel that my work is gradually being recognized, for example, by

being a finalist in the NIST competition.

Our goal as a research institute is to become an authority in research on symmetric-key cryptography. I want people to associate it with NTT and turn to “Sasaki at NTT” for everything related to symmetric-key cryptography. I also hope that many people will use the encryption codes we create. There are two ways to get people to use our encryption codes: we can standardize them so that everyone can use them freely, and we can actually propose using our own encryption codes when creating the product.

Specifically, we designed a lightweight encryption scheme called SKINNY, which was standardized by the International Organization for Standardization (ISO) in 2022. I feel that the scheme I created is gradually being used more. There are two keywords when it comes to using SKINNY: primitives and modes. Primitives refer to the engine design, and modes refer to how the engine is used and what functions are achieved, with SKINNY being the engine part. We had proposed standardizing the mode part, which determines what functions can be achieved using SKINNY. A few months ago, ISO agreed to begin international standardization of this. We are now moving forward with standardizing the modes.

—Tell us how you came to be appointed to NIST.

A long-term overseas posting spanning multiple

years, rather than a one-year study abroad program, may be quite unusual among NTT laboratories. NIST is located in a place where cybersecurity research is very active. Previously, there was no direct connection between NTT and NIST, but five or six years ago, NIST began accepting NTT researchers through its computer security division. My predecessor had been at NIST for about three years, and when his posting was coming to an end, the question of whether there was anyone available to take over was raised. The cryptography researchers at NIST at the time knew of my skills, so they chose me to take over. Because US standard technologies are essentially global standards, I was motivated to learn about the mechanisms of standardization within a U.S. government organization and see what goes on behind the scenes of standardization in order to utilize this experience in my future trajectory. Those three years constituted a very valuable experience.

In recent years, although NIST competitions have been able to ensure transparency, they place a heavy burden on NIST. Therefore, NIST is increasingly taking the lead in deciding standard technologies. Thus, even though anyone in the world can provide their opinions in the form of public comments, the final decision is made by NIST, so it is extremely important to be on the inside when deciding on standardization. Therefore, I would like to extend my posting and stay at NIST for another two years, so that I can keep an eye on the process of deciding on standards.

—Could you tell us about the challenges and difficulties you faced in conducting this research?

I mentioned earlier about the division of labor in our research team. Since I lack the expertise to do it alone, I have to ask experts in each task to help me with each job. This means that human networks are very important, and it can be difficult to find people who share the same passion and sensibilities as you, but cryptographers tend to get along well. When I still had no network and lacked expertise, I took part in overseas research meetings with a bit of trepidation, but suddenly I would start having group discussions with all the participants. As I did this, I gradually learned about the participants' areas of expertise, and by them getting to know me as well, I was able to expand my network. Now, I actively participate in international research meetings and find people with the most advanced skills in the world.

Also, just like cybersecurity, trends in cryptography research change very quickly, and if you don't keep

your ears open, trends can flip in the blink of an eye. Until around 2015, there was little talk of applying quantum computers to symmetric-key cryptography, but a few years later research into the topic began in earnest. And now, of course, research is also being conducted into the application of artificial intelligence (AI) to cryptography. Although many people are trying to design encryption codes with AI, it is not yet possible to leave the design and decryption of codes entirely to AI. However, AI-related papers and research are very popular, and even in these areas, we can see trends flip.

—What makes this research fascinating?

I think of symmetric-key cryptography as a kind of battle of wits. Public-key cryptography is a field where everything can be discussed mathematically, but symmetric-key cryptography is a field that requires a lot of craftsmanship, and it's fun to compete on these skills. On a more casual note, I've been a puzzle creator for a long time. I've always loved creating sophisticated Sudoku or crossword puzzles and pitting my wits against others, so I'm fascinated by the fact that a single idea can either create something good or, conversely, turn something bad. For example, in an attack, if everyone thinks it is safe but I am able to find a weakness and report it to the appropriate authorities, I feel a sense of accomplishment.

Also, it's always a joy to see the moment when you complete a cryptographic design and it is recognized as a good one. There were some fun, almost game-like moments when it was standardized by ISO and when it advanced from the first round to the second round to the finals in the NIST competition.

—Do you have a message for young researchers, students, and business partners?

When I was in Japan, I had the opportunity to conduct joint research with students, and on those occasions, I told them how fun it can be to become a researcher. There are many ways to enjoy it. I personally find it fun to be able to work across borders, so even though we have different values and lifestyles, as is the case now at NIST, it's interesting to be able to talk about mathematical expressions and calculations. Even just going on a business trip is fine, but such intercultural experiences are very enjoyable and educational, so I recommend doing international research.

Those who want to do basic research have no choice but to live off their research ideas. The world of symmetric-key cryptography (my research) is like a battle of wits, but sometimes it's frustrating when we can't come up with a solution. But in my experience, it's not often that I can't come up with anything, and the more I struggle, the more useful ideas and results I can come up with.

I also feel that NTT is a very good research institute. There are many people doing research at universities and other institutions, but I see that they are struggling with university operations and funding. At least for now, NTT recognizes the value of my research in cryptography and supports what I want to do. Of course, I work in concert with the company and do what is necessary for the company, but the company also lets me boldly pursue what I want to do.

Furthermore, the group I'm in recognizes the importance of basic research and allows me to study abroad in a joint research program at a university of my choice, where I can learn new skills and gain experience. In 2015, I studied abroad at Nanyang Technological University in Singapore for one year.

In terms of interpersonal relationships, each individual is a professional with a proven track record, so we respect each other. On the other hand, this also means that our research topics are different from those of our colleagues in the same group, but this is not an obstacle. Rather, we maintain a certain distance and respect each other, creating a good atmosphere. A characteristic of NTT researchers is that they are all serious about science and technology while also enjoying the work, so I would recommend NTT to anyone who wants to do research, as it provides a good research environment.

I am currently a visiting researcher at NIST, but I will be returning to Japan in two years. We are

already seeing some concrete plans, but going forward, I would like to propose using the encryption codes that I designed in Japanese products and protocols.

I would love to talk to business partners and design the best possible solution to meet their needs, so I would like to continue to exchange ideas.

Reference

- [1] M. Sönmez Turan, "Update on the NIST Lightweight Cryptography Standardization Process," 2019. <https://csrc.nist.gov/CSRC/media/Presentations/nist-lwc-standardization/images-media/session1-turan-update-on-nist-lwc-standardization.pdf>

■ Interviewee profile

Yu Sasaki completed his master's degree in information and communication engineering at the Graduate School of Electro-Communications, University of Electro-Communications, Tokyo, in 2007. He joined Nippon Telegraph and Telephone Corporation in the same year. In 2010, he completed his doctoral degree in information and communication engineering at the Graduate School of Electro-Communications, University of Electro-Communications and obtained a Ph.D. in engineering. He was appointed as a senior research fellow at Nanyang Technological University (NTU), Singapore, from 2015 to 2016. He has been appointed as an overseas visiting researcher at the National Institute of Standards and Technology (NIST) in the United States from 2022 to the present. He is engaged in research into the design and security analysis of secure symmetric-key cryptography to create a world where communications around the world are protected by encryption. He received the Test of Time Award from the International Association for Cryptologic Research (IACR) in 2023 and the 75th Institute of Electronics, Information and Communication Engineers' Best Paper Award in 2019.

