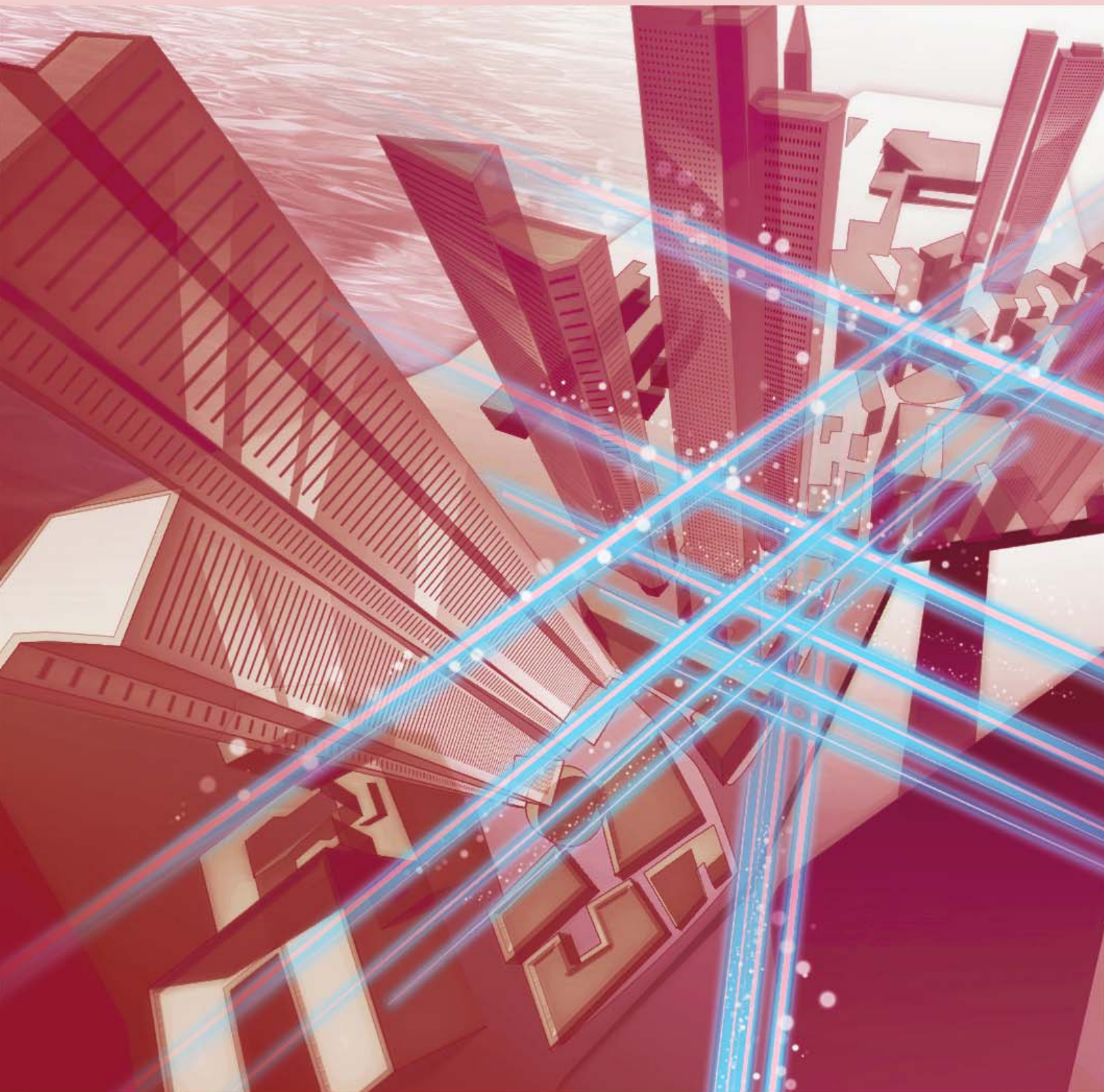


NTT Technical Review

1
2022



January 2022 Vol. 20 No. 1

NTT Technical Review

January 2022 Vol. 20 No. 1

Front-line Researchers

- Toshikazu Hashimoto, Senior Distinguished Researcher, NTT Device Technology Laboratories

Rising Researchers

- Yosuke Todo, Distinguished Researcher, NTT Social Informatics Laboratories

Feature Articles: NTT Research: Open Collaboration to Upgrade Reality

- Opening Up about Our Collaboration Strategy
- Making the Blockchain Ecosystem Secure, Scalable, and Sustainable
- The Future of Problem Solving: The Coherent Ising Machine Approach
- Bio Digital Twin Research Update
- A New Lab Exploring Emergent Matter from Light

Feature Articles: Research and Development of Security in the IOWN Era

- Security as Driving Force of the Future
- Secure Optical Transport Network
- Cryptographic Circuit Technology Consisting of Optical Logic Gates
- Trusted Data Space for Creating Value from Data in a Chain Reaction Manner

Feature Articles: Olympic and Paralympic Games Tokyo 2020 and NTT R&D—Technologies that Colored Tokyo 2020 Games

- Initiatives toward a New Way of Experiencing and Supporting the Torch Relay
- Torch Relay Commemorative Photography × Ultra-realistic Communication Technology Kirari!
- Direction for Supporting Torchbearers × Swarm Communication Control Technology
- Stage Production for Celebration of Torch Relay × Ultra-realistic Communication Technology Kirari!
- Torch Relay Regional Event × Voice-recognition Communication Technology

Feature Articles: Olympic and Paralympic Games Tokyo 2020 and NTT R&D—Technologies that Supported Tokyo 2020 Games

- High-efficiency Wi-Fi Technologies
- Network Security

Global Standardization Activities

- Report on ITU-T SG2 Standardization of Telecommunication Numbering

External Awards/Papers Published in Technical Journals and Conference Proceedings

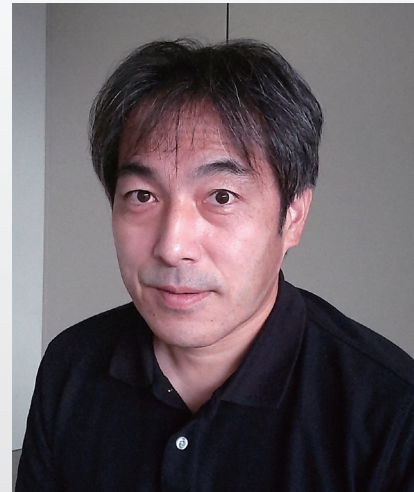
Think about Your Definition of a Good Idea and Believe in Your Idea

Toshikazu Hashimoto
Senior Distinguished Researcher,
NTT Device Technology Laboratories

Abstract

Today, everything is digitalized. In the creative process, however, not only digital thinking but also analog thinking, which captures events as they are, is considered important. Toshikazu Hashimoto, a senior distinguished researcher at NTT Device Technology Laboratories, is researching and developing optical circuits to enable new information processing using the analog characteristics of light. We interviewed him about the progress of his research activities and his attitude as a researcher.

Keywords: optical circuits, planar lightwave circuit, quantum teleportation



Optical circuits for new information processing by manipulating light waves

—Tell us about the research you are currently working on.

I am researching optical circuits that enable a new type of information processing by manipulating light as waves. What I mean by “manipulating light as waves” is to use the analog nature of light. In the case of digital computation, for example, it is necessary to use two values (bits), “1” or “0,” in a sequence such as “010110...” to represent a number. In analog computation, however, it is only necessary to use a single value, for example, “0.10110...” (i.e., the number itself). If we use analog computation skillfully, we may be able to conduct calculations faster, reduce the number of calculation steps, and save the labor involved in calculations. However, as you can easily imagine, when a number is represented by an analog signal such as light intensity, the last digit after the

decimal point would lose its information due to noise. Information processing using analog computation, which is susceptible to noise, is difficult to scale up and has not been applied to computing.

Despite the above-mentioned drawback, for computations to extract properties independent of minor differences, as is the case with artificial intelligence (AI), or computations by using the superposition of many quantum states while suppressing noise in the quantum state, as required with quantum computers, analog computation is more significant because it is possible to execute many calculations at once, albeit at the expense of accuracy, or manipulate quantum states without destroying them. In other words, rather than exceeding the limit of digital-information-processing capacity by using analog computation, we carry out a different type of processing using analog computation for information with different quantity and quality than before. This is the “new” information processing using light waves that I am aiming for. To make such information processing a reality,

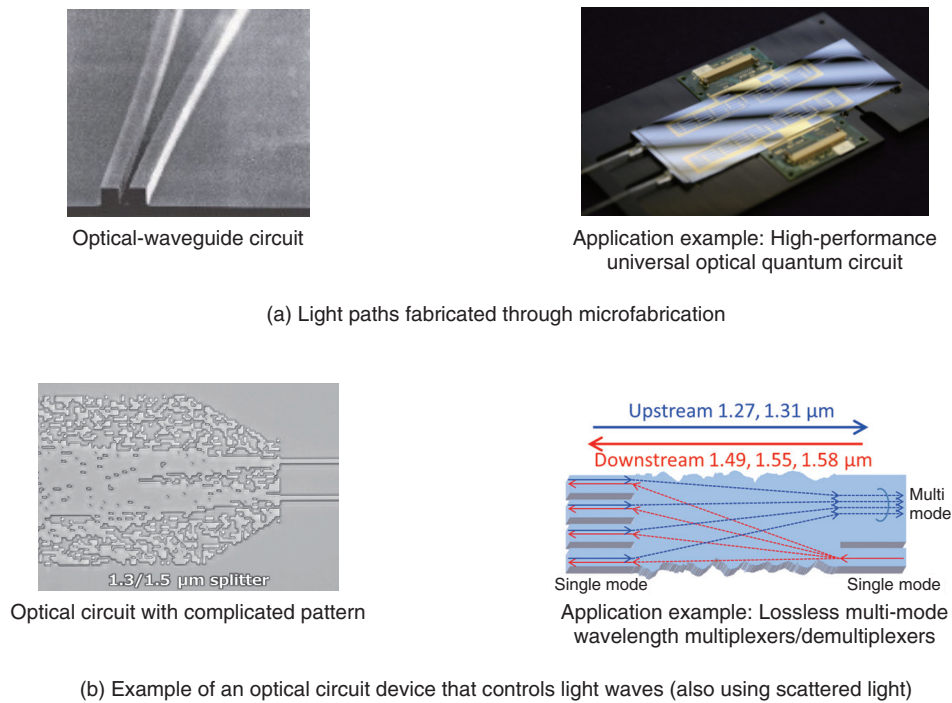


Fig. 1. Newly designed, ultra-low-loss optical device technology.

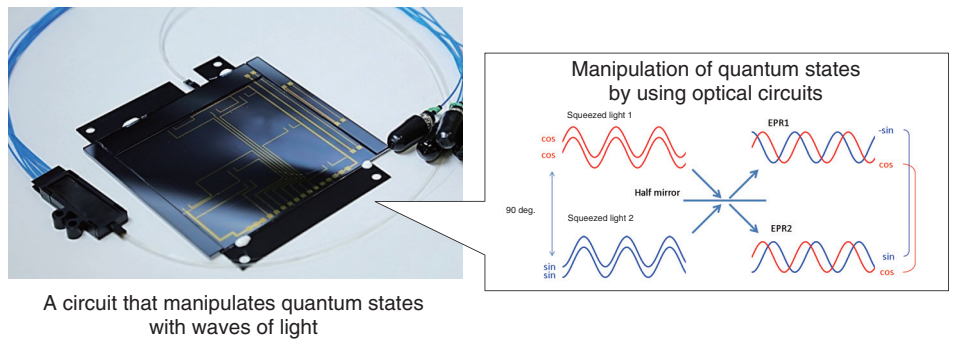
we are proceeding with research and development (R&D) with a focus on the following two technologies.

The first technology is newly designed, ultra-low-loss optical device technology (Fig. 1). It might seem contradictory to what I said earlier, but as noise becomes lower, the calculation performance improves, so the first step is to minimize loss—which constitutes noise—in an optical circuit as much as possible. Therefore, we are working on a new device design that enables significantly reducing the loss and signal processing by capturing the light scattering of the optical circuit that causes the loss. The optical-circuit technology that I am researching targets optical fiber communications, and I have been pursuing low-loss characteristics so that the optical signal does not weaken. However, I am aiming for technology that reduces losses by an order of magnitude and enables large-scale circuits and high-performance optical circuits.

The second technology is light-wave computing technology, which uses light waves for computations (Fig. 2). The challenge is to devise a computational method for exploiting the advantages of light as physical light. We are proposing light-wave information-processing technology using optical device tech-

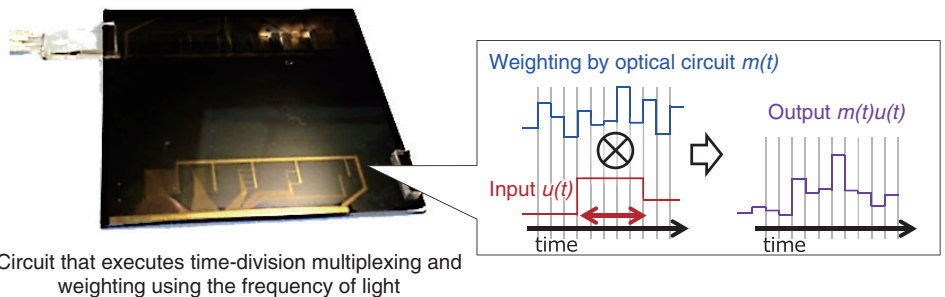
nology. To develop the world's first and highest-performance computing technology using light waves, we are attempting to demonstrate the basic operation of optical information processing using technology based on the light paths (optical waveguides) in current devices.

Of course, lowering the loss of optical circuits also reaches a limit, and electrical control is essential to fully use light waves; accordingly, it is important to create new optical circuit technology by combining the features of both digital and analog computations. One example application of this new type of information-processing technology using light waves is a large-scale, fault-tolerant universal optical quantum computer, which is expected to be developed around 2050. A quantum computer capable of large-scale, universal computation is expected to enable the development of innovative materials and the design of chemical reactions that have been difficult to carry out with conventional supercomputers. It is also expected to contribute to solving global issues such as energy problems. As a participant in one of the Moonshot Research and Development Programs of the Japan Science and Technology Agency, which started in 2020, we are developing optical-circuit device technology for quantum information processing



A circuit that manipulates quantum states with waves of light

(a) Continuum-quantum optical quantum information-processing circuit (quantum teleportation circuit)



Circuit that executes time-division multiplexing and weighting using the frequency of light

(b) Optical-frequency-domain-weighted up-sampling processing circuit

Fig. 2. Example of light-wave computing technology.

to enable a large-scale, fault-tolerant and universal quantum computer that exploits the properties of light as a wave and can operate at room temperature.

—It is fascinating that your research on optical circuit technology could contribute to achieve large-scale quantum computers. Can you tell us about one of your achievements in other applications?

The optical circuit that I am researching is called a planar lightwave circuit (PLC). As a component technology for optical fiber communications, a PLC integrates an optical-waveguide circuit (namely, a path of light) on a silicon substrate. The application of PLC includes optical branch circuits and wavelength multiplexers/duplexers. Developing PLC technology to create optical circuits with even higher performance was the essence of my research. This high-performance optical circuit technology can control light with wavelengths less than half that of the light used for optical fiber communications (visible light). It is therefore being applied not only to optical computation but also to ultra-compact RGB (red, green, and

blue) laser light sources for smart glasses. Semiconductor lasers using the three RGB primary colors are beginning to be used in a variety of situations as single-color lasers; however, to combine them and create an RGB light source, it is important to devise an optical system (optical circuit) technology that uses the characteristics of the laser light by means of interference and other phenomena. Conventionally, the optical system was made up of lenses and mirrors, which are bulky and difficult to assemble. We have therefore applied our visible-light PLC technology for those parts and created the world’s smallest optical system that forms the basis of an ultra-compact light-source module that fits in the temples of smart glasses.

Making sure that the limits of my imagination do not become the limits of my research

—How do you find research themes?

Optical circuit technology—which is the basis of my research—has matured as a device technology for

optical fiber communications, so it can be said that it is difficult to propose new ideas. Therefore, I started to think that what type of light to input into an optical circuit is more important than what type of optical circuit is possible. This way of thinking is the same as I mentioned at the beginning of this interview, namely, it is important to know what kind of information to handle to take advantage of the characteristics of analog computation. By inputting visible light, which has a different wavelength from that used for optical communications, into an optical circuit, we would be able to consider applications such as RGB light sources. Also, by devising ways to put information on optical signals, analog computation with optical circuits becomes possible. We might also be able to create an optical quantum computer by inputting quanta of light (photons) into an optical circuit. I believe that inputting new light into an optical circuit is the source of creating a new optical circuit.

To foster different perspectives, I am paying attention to the trends of deep-tech ventures involved in AI, quantum computers, and so on. Although it is a mixture of good and bad, the ability of such venture companies to quickly commercialize basic technology (such as AI and quantum computers) is remarkable. Collaboration is also important because through collaboration, it will be possible to apply the optical device technology we have developed thus far to completely different fields. I have been greatly stimulated by collaboration with other researchers and companies, which is true joy of research.

—Do you feel that you have any advantage as a researcher working at NTT laboratories? In addition, could you tell us about the attitude that you value in your research activities?

I think that various applications and collaboration are possible only with outstanding optical circuit technology that is difficult for others to imitate. The optical-component technology of the research laboratory to which I belong represents research results accumulated for half a century. With such a foundation, adding a little more value or doing something slightly different will lead to top-notch research results. (Of course, there have been many cases in which our approach has not worked.) We also have a full range of research facilities that are necessary for manufacturing, and such an environment is a huge advantage in regard to advancing device research. To put that another way, I believe that NTT researchers have the mission to develop the technologies that we

have developed thus far and implement them in society. Through such efforts, we will be able to consolidate various technologies and create the direction of technology trends.

Of course, it is not possible to conduct research by only using the advantages of our laboratories; you need to create value on your own accord. One of the most important points that I keep in mind is to make sure that the limits of my imagination do not become the limits of my research. For example, the study of optical circuits deals with the natural phenomenon of “light.” Natural phenomena are far beyond my imagination, and many unexpected things can happen. I think it is important to start your research with the mindset “It would be great if that happened” instead of “This is a natural phenomenon, so anything otherwise cannot happen.” The design method shown in Fig. 1(b) was developed on the basis of this mindset. That is, by using light scattering, we can design optical circuits with desired characteristics. The conventional idea behind optical circuits is to minimize as much scattering as possible because scattering usually results in loss. Instead of adopting that mindset as a starting point, we devised the design method shown in the figure by first thinking about how to create an optical circuit with the desired characteristics. Even if you take this attitude, it does not mean it is always the right way; even so, I think that is okay. I believe that it is okay to make mistakes without hesitation because natural phenomena will correct our wrong ideas after we conduct calculations and experiments. Instead of thinking about what is correct, it is important to think hard about what you wish would happen.

First, let’s consider the definition of a “good idea”

—What are some of the challenges you face as a researcher?

It is normal for research to go wrong and for researchers to struggle, so I tend to think positively and try to persevere. I think that has always been the case. My first research theme was hybrid optical integration of optical waveguides and semiconductor lasers, which is a technology for assembling optical components. Since such integration involved combining multiple optical components, it was necessary that all the components were aligned and fixed properly. At first, it looked like it would be easy to do it in my mind because it was like putting together building blocks; however, it did not go well, and I struggled for

over a month. I researched the cause of the problem, thought about it thoroughly, and corrected it. When I was finally able to assemble all components properly, I let out a shout with tears swelled up, and I would have surprised anyone if they had been around. Although it may have been a minor success, I remember how happy I was to think that I was the first person in the world to know that I have achieved this.

Since having such experiences, I have come to believe that rather than just trying to do what you can do to break free of difficulties, it is better to face those difficulties and think carefully about them. To do that, it is important to be persistent in thinking things through and optimistic in finding the right way forward. If that approach still does not solve the problem, I try not to get stuck by changing my interpretations or assumptions and stay optimistic. For example, I try to find value and meaning in work that I dislike by viewing it from a different perspective. I believe that there is a lot to learn by doing so, and by expanding my work in this way, I will be able to meet more people and come into contact with a wider variety of ideas.

—Would you say a word to future generations of researchers?

I joined NTT and was assigned to a research laboratory, and since then I have been mostly engaged in R&D. Along the way, there were times when I did not know what I wanted to do as a researcher, and sometimes I felt that research was “just a job.” More than 20 years have passed, and sometimes I look back on those early days. I feel that I have come to understand the joy of research a little more by going back to my original intentions and approaching my research from that standpoint. I think it is very effective to go back to your beginning from time to time to look at yourself objectively.

In the past, I have been asked by a young research-

er about my ideas for finding research themes. I think that person was just trying to come up with a new research theme. I answered, “The idea itself is natural, and you will come up with some sort of idea soon,” and I still wonder if that was good advice. Now, I think I would answer, “First, think about the definition of a ‘good idea’.” The definition of a good idea varies from person to person; for example, a good idea may be one that can make money from patents or can be cited in many other studies. My definition of a good idea is one that I like. If you deeply like an idea, you can discuss it with others with passion and can overcome difficulties to make it happen. If you define ideas in this way, I think it is important to think things through in your own way and have your own conviction, even if you cannot prove or explain the idea fully; in other words, believe in your ideas, without worrying about the results or what people around you think.

My message to young researchers would be that if you keep your original intentions in mind and passionately discuss good ideas with others, you will surely enjoy your research.

■ Interviewee profile

Toshikazu Hashimoto received a B.S. and M.S. in physics from Hokkaido University in 1991 and 1993. He joined NTT Photonics Laboratories in 1993 and has been researching hybrid integration of semiconductor lasers and photodiodes on silica-based PLCs and conducting theoretical research and primary experiments on the wavefront-matching method. He is a member of the Institute of Electronics, Information and Communication Engineers and the Physical Society of Japan.

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

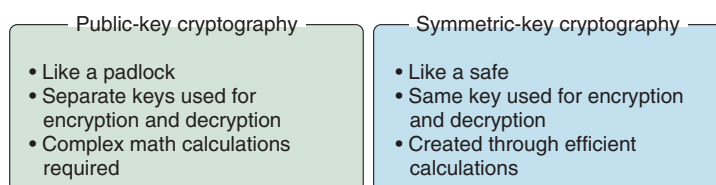


Fig. 1. Public-key cryptography and symmetric-key cryptography.

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 light-weight 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.

Opening Up about Our Collaboration Strategy

Hideaki Ozawa

Abstract

There are several means of conducting scientific research. Corporations have traditionally adopted a proprietary approach. The academic world, by contrast, conducts research in a more open and collaborative manner. This article compares these two approaches in the context of basic and applied research; explains why NTT Research, a private company, has adopted an Open Lab model; and reviews how this is working out in practice.

Keywords: Open Lab, research strategy, research community

1. Proprietary vs. open models

Until a few decades ago, corporations typically conducted research using internal resources alone. One classic example was Bell Telephone Laboratories. Originating from engineering departments within the American Telephone & Telegraph (AT&T) and Western Electric companies, and now known as Nokia Bell Labs, this famous research organization was responsible for many breakthrough technologies, including the electronic transistor. These results, including thousands of patents, were the outcome of basic and applied physics research conducted by Bell Labs' employees. Another example on a smaller scale

is that of a former Bell Labs engineer, Chester Carlson, who patented a dry photocopy technique known as Xerography that he developed in his laboratory. Each technology, the transistor and Xerography, grew into very big businesses in the 20th century.

However, many companies in the U.S. are now focusing on applied research for their products or services, such as autonomous driving, artificial intelligence based on deep neural networking, etc., rather than on basic research. Basic research has tended to be the domain of universities, not corporations, and this remains the case today. This kind of research has the potential for various future products and services, but these beneficial outcomes require very long lead times and the assumption of many types of risks.

In addition to established laboratories in Japan, NTT founded NTT Research in the U.S. with the transformational vision of "Upgrade Reality." NTT believes exploring basic research is also a means to create brand-new business value in the future. In theory, by hiring the right mix of scientists, NTT Research could try to gain a monopoly on any new knowledge acquired in this pursuit, along with the rights of invention. However, the founders of NTT Research chose another path. We realized that many of the challenges facing our current and future generations are extremely complex and closely intertwined. For example, one of the goals of medical care is to enable patients to recover from illness and



maintain their health more easily. Everyone has a different constitution, so we believe it is necessary to provide precise medical care suited to the individual. When we explore precise medical care, we need not only medical and biological knowledge but knowledge related to drug discovery, sensing, big data analytics, treatment materials, etc. To achieve precise medical care, we believe we need to improve upon the accuracy of these technologies.

To gather as much insight, experience, and wisdom as possible, as well as to manage our risk in precision medical care and other research areas, we decided that an Open Lab strategy was the better way to go. This Open Lab approach is more akin to academic and government-sponsored research, rather than corporate research, which on the whole aims for short-term product development. Research universities pursue scientific discovery in the open, with results shared and evaluated by peers. Foundational knowledge is often the common goal. Government-directed research may have more specific goals, but it is also a collective effort for social benefit. The U.S. Defense Advanced Research Project Agency (DARPA), famously responsible for creating the Internet by collaborating with several universities, is a case in point.

The NTT Research executive team and board have taken the lead in establishing the vision “Upgrade Reality,” and setting goals such as a cardiovascular bio digital twin and a quantum computing system based on optical technologies. Our vision and goals are connected to resolving parts of social problems, for instance: precise medical care through the bio digital twin or drug discovery through a new kind of quantum computing. Because our high aspirations are beyond the reach of any single company, we have adopted an Open Lab strategy that faces outward, predominantly through joint research projects with other worldwide research organizations. We contribute our new knowledge, results, and findings in the public as papers or as joint patents with collaborators. We also see ourselves as a venue for discussion, seeking various viewpoints to expand upon the ideas of any individual researcher.

2. Open-source and NTT Research operations

In certain ways, our method resembles that of open-source software development. In that model, an individual or small community first approaches a coding project with a vision and goal. When more developers and users realize the value of the initiative, the com-

munity expands, attracting developers of not only core software but also applications. The knowledge and ideas proposed by community members improves the code, which in turn increases its value.

The Coherent Ising Machine (CIM) research group within our Physics and Informatics Laboratories (PHI Lab) has a comparable record. Starting with just several internal employees, within our first year the CIM group gained eight joint research partners, covering theoretical and hardware research of optical-based quantum computers. In our second year, this has grown to 13 organizations and over 60 members, including collaborators. We are now achieving new breakthroughs as we gain employees and collaborators, including scientists who are researching CIM applications, such as compressed sensing, drug discovery, and artificial/biological brain science.

Like the PHI Lab, our Medical and Informatics Laboratories (MEI Lab) has a clear and visionary lead product—the aforementioned bio digital twin, a virtual replica of individuals in cyberspace. In the initial phase, we are focused on the cardiovascular system. The MEI Lab is also engaged in research on implantable electrodes and remote sensing that can capture many types of vital information from the actual human body. Like the PHI Lab, the MEI Lab can subdivide its research, with collaborators taking on parts of the agenda. The National Cerebral and Cardiovascular Center in Japan and the Technical University of Munich in Germany, for instance, have become key partners.

Measured in terms of contributions to leading academic conferences, our Cryptography and Information Security Laboratories (CIS Lab) has become a world leader in its field. While the CIS Lab has established several joint research agreements, its members also collaborate with peers on a less formal, topical



basis. The cryptography team’s research is more academic and theoretical, whereas the blockchain team’s work is more applied, with implications in law, privacy, and other practical concerns. Theoretical research within cryptography is deepened by discussions between researchers who have the same interest in a target topic. It resembles the kind of small community that initiates an open-source project. Members of an open-source community might write code and documents as their goal. Our CIS Lab researchers write scientific papers.

Across all three labs, we might adjust our strategy if some topics shift from basic research into product development. Regarding basic research, where discoveries should become public assets, the Open Lab strategy is a sound method.

3. Open Lab requirements

To succeed, an Open Lab strategy needs to meet several requirements. Funding is key, as it can clearly

accelerate research activity. However, without a clear vision, strong leadership, and an effective team, funds are likely to be inefficiently distributed. Of all requirements, vision is the most important.

About 40 excellent researchers have gathered around our “Upgrade Reality” vision over the past two years. We hope to improve upon today’s “Reality,” addressing social and industrial problems that face the current and next generations. With a clear vision, the direction of research proceeds in the right manner. However, this is not necessarily without detours, which are often associated with trial and error. Basic research, especially involving multiple laboratories, contains a natural element of surprise. Therefore, we need to allow for some flexibility as well. Because basic research involves unknown facts and brand-new technology, it also carries risk. By subdividing and distributing tasks, the Open Lab strategy helps to manage that risk and increase the likelihood of success.



Hideaki Ozawa

Chief Operations Officer and Chief Technology Officer, NTT Research, Inc.

He received a Ph.D. in engineering from the Graduate School of Science and Technology, Keio University, Kanagawa, in 1992. He joined NTT in 1991. After engaging in research and practical application of multimedia processing technologies at NTT Human Interface Laboratories and Cyber Solution Laboratories, he joined NTT WEST (seconded to Walkerplus, Inc.) in 2000, where he was involved in the provision of local multimedia information. He then joined NTT Resonant Inc. in 2004, where he worked on the development and management of “goo” Internet services including its search engine and the establishment of mobile-search business and became head of the Search Business Division in 2011. After serving concurrently as president of NTT Resonant Technology, Inc. from 2013, he became vice president, head of NTT Media Intelligence Laboratories in 2015 and head of the Global Business Promotion Office at NTT TechnoCross Corporation in 2018. He assumed his current position in June 2019.

Making the Blockchain Ecosystem Secure, Scalable, and Sustainable

Shin'ichiro Matsuo

Abstract

In place of the centralized computation of the Internet's current architecture, blockchain could be used to implement self-resilient or self-operating systems, as it upkeeps states with highly resilient mechanisms by design. Despite blockchain's potential to correct problems associated with the current Internet ecosystem, there are several issues that need addressing within the blockchain ecosystem. These include security; the tradeoff between scalability and decentralization; and sustainability.

Keywords: blockchain ecosystem, smart contract, proof-of-work mechanism

1. Potential and issues regarding the blockchain ecosystem

Whether you are interested in blockchain or not, there are several reasons for engaging with it. Cryptocurrency, smart contracts, and non-fungible tokens (NFTs) rely upon this distributed ledger-based technology, and it could have revolutionary implications for global networking and information technology (IT) companies, and the Internet at large.

The Internet, for instance, was originally designed to achieve global networking without a single point of

failure (SPOF). However, the current problem for the ecosystem over the Internet is that tech giants have in effect become such SPOFs. Hence, there is a continued need for extensible trust without these risky flaws. In place of the centralized computation of the Internet's current architecture, blockchain could be used to implement self-resilient or self-operating systems, as it upkeeps states with highly resilient mechanisms by design.

Despite blockchain's potential to correct problems associated with the current Internet ecosystem, there are several issues that need addressing within the blockchain ecosystem. These include security, broadly understood; the tradeoff between scalability and decentralization; and sustainability.

2. Security and cryptography

Studies conducted on the formalization of blockchain security requirements have largely neglected to consider the entire technology and all its systems. While this does not necessarily imply insecurities, it means we are unable to demonstrate that blockchain does not contain vulnerabilities.

The presence of risk applies not only to blockchain specifications but also to its implementation. The attack in 2016 on a decentralized autonomous organization illustrated the possibility of exploiting vulnerabilities in the Ethereum blockchain code. Because of





the pervasive role that blockchain is expected to play as a social infrastructure tool, the impact of security incidents could increase dramatically. This means there is a need for vulnerability-handling procedures to ensure the quality of code and respond to attacks when they occur.

There also needs to be a standard operating model regarding the use of cryptography. When the IT industry transitioned from secure hash algorithm (SHA)-1 to SHA-2 several years ago, following a reported compromise of SHA-1, the Bitcoin and blockchain engineering community for the most part lacked the experience, mechanisms, and operations to do likewise.

With quantum computing looming as a long-term threat, the digital signature schemes used in blockchain technologies could also become insecure. Efforts to develop post-quantum cryptographic techniques are underway. The U.S. National Institute of Standards and Technology (NIST), for instance, has selected post-quantum finalists covering public-key encryption and digital signatures. Because long-term operations are assumed with blockchain applications, it is important to transition to equally long-term, secure cryptographic techniques. Cryptographic agility, which means a level of flexibility when the underlying cryptography is compromised, should be implemented into blockchain technology, operations, and governance mechanisms.

3. Scalability vs. decentralization

The blockchain ledger is processed according to a specified rule of processing speed. (In the case of Bitcoin, 1-MB block of data is added every 10 minutes.) This upper bound on the maximum number of transactions per unit time effectively puts a limit on scalability, which advancing computing power can-

not overcome.

One solution is to increase the size of the block by changing its specifications. However, this would increase the amount of data stored at all user nodes. This could result in only wealthy individuals or parties having the resources to operate the nodes, which in turn decreases their number. A solution involving fewer nodes would therefore contradict the original “decentralization” philosophy of permission-less blockchain, making such blockchains less secure.

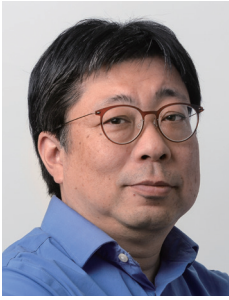
The trade-off between scalability and decentralization is related to design philosophy. Reducing the number of nodes or setting multiple nodes in the same cloud computer (to achieve greater scalability) may destroy one of the prime merits of public blockchain, namely, the removal of centralized operators. It is, therefore, crucial to consider the cost-merit balance of introducing such a semi-decentralized blockchain when we expand its applications.

4. Sustainability

From an environmental perspective, there is concern about whether the proof-of-work (POW) blockchain consensus mechanism used by Bitcoin is sustainable given the tremendous amount of energy consumed in mining these digital assets. The alternative proof-of-stake (POS) mechanism is much more energy-efficient; however, POS faces numerous implementation challenges, including confirmation delays.

From a business perspective, public blockchain systems such as Bitcoin are considered self-resilient because their protocols implement fees for operations through self-issuing crypto assets. A capital growth theory analysis indicates that blockchain systems are usually sustainable, although stakeholders unconstrained by certain standard rules of business (such as those involving taxes, energy costs, or risk of bankruptcy) could undermine a chain’s viability. Similarly, if we were to see a so-called selfish mining attack on the POW mechanism, it could lead to the collapse of a chain, another limit on sustainability. It is also worth mentioning that the use of blockchain by itself, for instance in NFTs or self-executing contracts, does not guarantee outcomes that could be characterized as fair. Achieving fair outcomes calls for appropriate design considerations.

What that also means is that in addition to further analysis, we are likely to need regulations in this field. If we are interested in a new type of public, self-resilient Internet infrastructure mentioned at the start of this article, we may need to upgrade blockchain.



Shin'ichiro Matsuo

Senior Scientist, Head of blockchain research, Cryptography and Information Security Laboratories, NTT Research, Inc.

He is the head of blockchain research at NTT Research. He is also a research professor at Georgetown University, Washington, D.C., USA, and works as a director and blockchain research lead of CyberSMART research center at Georgetown University. He has been engaged in research on cryptography and cryptographic protocols for over 23 years. He was a program chair of Scaling Bitcoin workshop 2019 and program committee member of many blockchain-related academic conferences such as IEEE Security & Privacy on the Blockchain, International Workshop on Cryptocurrencies and Blockchain Technology (CBT), Stanford Blockchain Conference and Crypto Economics and Security Conference. He is also a co-founder of BSafe.network, which is the global and neutral academic research testbed dedicated to blockchain research. As editor and project leader, he oversees two technical reports on the security of blockchain technology at ISO TC307.

The Future of Problem Solving: The Coherent Ising Machine Approach

Yoshihisa Yamamoto

Abstract

Several new computing models tackle combinatorial optimization problems. These include adiabatic quantum computation, also known as quantum annealing, and the coherent Ising machine (CIM). The Physics and Informatics Laboratories at NTT Research launched a CIM initiative, and NTT Basic Research Laboratories built large-scale CIM prototypes. This article reviews the CIM approach, results to date, and future research agenda.

Keywords: coherent Ising machine, optimization problems, optical parametric oscillator

1. Introduction

The current computing model, composed of processing, communication, and memory units, is more than 70 years old. To overcome the inherent limitations of this model, over the past few decades, physicists, computer scientists, and technology companies have been exploring a range of new approaches. A common goal with these alternative models, which use a mix of analog, digital, classical, and quantum technologies, is to solve extremely difficult computational challenges with reduced energy cost.

Such challenges commonly target non-deterministic polynomial-time (NP)-hard or NP-complete problems. There are several types of NP-hard problems. One type targets combinatorial optimization, i.e., finding an optimal solution from a large set of candidates. One of the earliest described combinatorial optimization problems was determining the minimum total distance in a journey to N number of cities. Calculated by factorials, the number of combinations becomes astronomically high as N increases.

Several new computing models tackle combinatorial optimization problems. These include adiabatic quantum computation, also known as quantum annealing (QA), and a coherent Ising machine (CIM). The Physics and Informatics Laboratories (PHI Lab) of NTT Research launched a CIM initiative, and NTT Basic Research Laboratories built large-scale CIM

prototypes. This article reviews the CIM approach, results to date, and future research agenda.

2. Definition of terms

To understand the CIM approach and why it is a type of quantum/classical hybrid computing, let us define some terms, starting with Ising then turning to coherent. The proper name refers to Ernst Ising, a German physicist linked to a mathematical model created in the 1920s to describe magnetic orders.

The Ising model originally consisted of a one-dimensional set of discrete variables representing N magnetic moments of atomic spins, each of which has two possible states (+1 or -1). Its energy was expressed in terms of the sum of pair-wise (two-body) interaction, Hamiltonian. Solving the model involves finding its ground state, which is the lowest energy state. If a spin-spin coupling configuration is not simple and cannot be described by planar graphs, finding the ground state of an Ising Hamilton falls into the NP-hard category of computational complexity.

The most important active component in a CIM is an optical parametric oscillator (OPO). First demonstrated in 1965, about five years after the invention of the laser, the OPO is a coherent light source. It is distinct from the laser because it produces a quantum state of light (squeezed state). While the Ising model,

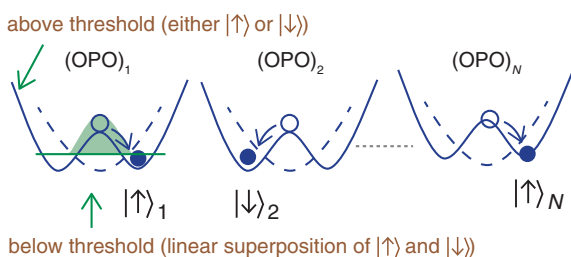
which evolved from a one- or two-dimensional lattice framework, mathematically represents the atomic spins in any complex configuration, the OPO-based CIM creates a universe of artificial spins, which can then be mapped to a real-world combinatorial optimization problem through an $N \times N$ coupling matrix. The solution corresponds to an optimum configuration of spins that minimize their energy function.

This system is doubly coherent in the following sense. When one photon is eliminated from a pump pulse sequence at frequency 2ω , two photons (called a photon-pair or biphoton) are generated simultaneously in a signal pulse sequence at frequency ω . If a CIM consists of two OPOs, a single photon pair exists simultaneously in two OPOs as linear superposition. If the CIM consists of N OPOs, a single photon pair exists simultaneously in N OPOs as linear superposition. Therefore, the elementary excitation of the CIM coherently spreads in an entire machine consisting of N OPOs.

This fact means that each OPO state simultaneously exists in a vacuum state with a zero-photon state with a large probability and two-photon state with a small probability. Because of this coherent superposition nature, each OPO state occupies 0-phase (down spin) and π -phase (up spin) states even if there is one and only one photon pair in an entire machine. Therefore, a prerequisite for quantum computation, linear superposition of two states, is naturally satisfied in a CIM [1].

3. Two CIM types

In practice, there are two types of CIMs: one using an optical delay line (ODL) and the other using measurement feedback (MFB) to introduce the coupling matrices. As mentioned above, the OPO absorbs one photon from the pump field and emits two photons into the signal field simultaneously. As a result of interference among the zero- and two-photon states, the electromagnetic field is stretched into a squeezed



vacuum state or a linear superposition of up- and down-spin states. If the pump amplitude is further increased, the stretched noise is finally split apart into the two states with positive and negative average amplitudes.

That splitting point marks a transition from quantum to classical mechanics. The quantum region below the threshold is represented by a linear superposition of up- and down-spin states and above it, by a classical up or down spin, but not both simultaneously. It is the states of photon pulses that change a CIM from quantum to classical, allowing for reading out final answers with high accuracy [2].

Regarding the MFB-CIM, following the OPO's generation of two photons, an optical beam splitter creates a quantum correlation between the internal and external (measured) fields. The use of homodyne detection, which extracts information encoded as an amplitude of an external signal field, induces state reduction for the internal field [3]. (The measurement of a quantum system induces, via "wave-function collapse", a completely new state.)

In the ODL-CIM, optical mutual coupling creates the quantum correlation (entanglement) among OPOs, while in the MFB-CIM, the original quantum correlation is converted to classical correlation among OPOs via measurement feedback. The difference between the two CIMs, which both involve quantum-to-classical transitions, is that the separation or breaking of symmetry occurs through quantum correlation for the ODL-CIM and classical correlation for the MFB-CIM.

The two machines also have different histories and tradeoffs. The CIM was originally demonstrated using an ODL, but for the past five years, MFB has predominated. While an ODL is more difficult to implement, once set up, it promises higher operational speed and lower energy consumption.

4. CIM performance

How has a CIM performed to date? Two tests, one experimental and the other mathematical, indicate a CIM's unique computational power.

In a 2019 benchmark study between the MFB-CIM and QA [4], the success probability (time to solution) of this CIM outperformed QA by an ever-widening gap as the problem size increased. For a dense Max-Cut problem of $N = 55$, for instance, the MFB-CIM determined a solution seven orders of magnitude faster than did QA from D-Wave, Inc. For a problem size of 100, the differential was estimated as 21

orders of magnitude.

These extremely large differentials derive from design. Whereas the MFB-CIM had all-to-all connections among its 2000 spins, QA was connected only locally. This resulted in a divergence in the number of spin-spin couplings: 4 million (CIM) vs. 8 thousand (QA). Ultimately, the difference can be traced back to the basic hardware platforms. QA consists of localized spins and requires real wiring to connect qubits (the basic unit of quantum information). By contrast, a CIM is based on a de-localized harmonic oscillator field, in which mutual spin coupling can be implemented at any place in the machine.

In a mathematical comparison with an ideal QC machine [5], the MFB-CIM also outperformed it. In this comparison, the ideal QC exhibited no decoherence, no energy dissipation, no gate error, and all-to-all qubit coupling—conditions that are far from being actualized. Even so, the time-to-solution (TTS) for discrete adiabatic quantum computation (dAQC) and the Grover search, an optimum quantum algorithm for unstructured search, fell far behind. The TTS for Grover search and dAQC scaled in accordance with the exponential of problem size n , and the TTS for the MFB-CIM scaled in accordance with the sub-exponential of n , an increasingly small number.

In this case, system design again matters. The unitary QC machines are limited to linear amplitude amplification at best, while a dissipative CIM can increase in this regard exponentially. It can do so because the operating principle of the quantum-to-classical transition enables the stimulated emission of photons above the OPO threshold.

In the latest numerical simulation study [6, 7], the CIM with amplitude error correction feedback can be competitive also against state-of-the-art digital heuristics such as Breakout Local Search (BLS) and Simulated Bifurcation Machine (SBM).

5. Future research agenda

Notwithstanding the strong results from CIM prototypes and mathematical studies, there remains much from a theoretical perspective to understand about how they perform. This situation contrasts with the prevailing scenario in the QC domain, where experimental results lag far behind the theory.

To remedy this knowledge deficit, NTT Research launched an ambitious, long-range collaborative exercise with 14 institutions: Stanford University, California Institute of Technology, The University of

Chicago, Cornell University, Harvard University, University of Michigan, Massachusetts Institute of Technology (MIT), NASA Ames Research Center, University of Notre Dame, Swinburne University of Technology, Tokyo Institute of Technology, The University of Tokyo, University of Waterloo, and IQBit. These joint research projects with 25 principal investigators cover a wide range of topics, including quantum optics and information, neural network and brain science, nonlinear photonics, combinatorial optimization, and machine learning.

To be on the edge of new knowledge can be exhilarating. First, there are pressing, real-world problems that a CIM could solve in areas such as operations and scheduling, drug discovery, wireless communications, finance, integrated circuit design, compressed sensing, and machine learning. Then there is the range of interdisciplinary viewpoints that impinge upon this research, which arguably amount to a new field of study. Neuroscience may be one of the most significant of these areas of knowledge.

Compared with the static nature of the long-standing legacy computing model, the new paradigm, which includes CIMs, is shifting toward more brain-like functionality, a point captured in our PHI Lab slogan: “Quantum Physics meets Brain Science on Optical Platform.”

References

- [1] Y. Yamamoto, T. Leleu, S. Ganguli, and H. Mabuchi, “Coherent Ising Machines—Quantum Optics and Neural Network Perspectives,” *Appl. Phys. Lett.*, Vol. 117, No. 16, 160501, 2020.
- [2] Y. Inui and Y. Yamamoto, “Entanglement and Quantum Discord in Optically Coupled Coherent Ising Machines,” *Phys. Rev. A*, Vol. 102, No. 6, 062419, 2020.
- [3] S. Kako, T. Leleu, Y. Inui, F. Khojatee, S. Reifstein, and Y. Yamamoto, “Coherent Ising Machines with Error Correction Feedback,” *Adv. Quant. Technol.*, Vol. 3, No. 11, 2000045, 2020.
- [4] R. Hamerly, T. Inagaki, P. L. McMahon, D. Venturelli, A. Marandi, T. Onodera, E. Ng, C. Langrock, K. Inaba, T. Honjo, K. Enbutsu, T. Umeki, R. Kasahara, S. Utsunomiya, S. Kako, K. Kawarabayashi, R. L. Byer, M. M. Fejer, H. Mabuchi, D. Englund, E. Rieffel, H. Takesue, and Y. Yamamoto, “Experimental Investigation of Performance Differences between Coherent Ising Machines and a Quantum Annealer,” *Sci. Adv.*, Vol. 5, No. 5, eaau0823, 2019.
- [5] K. Sankar, A. Scherer, S. Kako, S. Reifstein, N. Ghadermarzy, W. B. Krayenhoff, Y. Inui, E. Ng, T. Onodera, P. Ronagh, and Y. Yamamoto, “Benchmark Study of Quantum Algorithms for Combinatorial Optimization: Unitary versus Dissipative,” arXiv:2105.03528, 2021.
- [6] T. Leleu, Y. Yamamoto, P. L. McMahon, and K. Aihara, “Destabilization of Local Minima in Analog Spin Systems by Correction of Amplitude Heterogeneity,” *Phys. Rev. Lett.*, Vol. 122, No. 4, 040607, 2019.
- [7] S. Reifstein, S. Kako, F. Khojatee, T. Leleu, and Y. Yamamoto, “Coherent Ising Machines with Optical Error Correction Circuits,” *Adv. Quant. Technol.*, Vol. 4, No. 9, 2100077, 2021.

**Yoshihisa Yamamoto**

Director, Physics and Informatics Laboratories, NTT Research, Inc.

He received a Ph.D. from the University of Tokyo in 1978 and joined NTT Basic Research Laboratories. He became a professor of applied physics and electrical engineering at Stanford University in 1992. He also became a professor at the National Institute of Informatics (NII) in 2003. He is currently a professor (emeritus) at Stanford University and NII, and an NTT R&D Fellow. He received many distinctions for his work, including the Carl Zeiss Award (1992), Nishina Memorial Prize (1992), IEEE/LEOS Quantum Electronics Award (2000), Medal with Purple Ribbon (2005), Hermann A. Haus Lecturer of MIT (2010), Okawa Prize (2011), and Willis E. Lamb Award (2022). His research focuses on quantum information processing, quantum optics, and mesoscopic physics, especially quantum neural networks and coherent Ising machines.

Bio Digital Twin Research Update

Joe Alexander

Abstract

The mission of the Medical and Health Informatics Laboratories at NTT Research is to make advancements in the medical and health sciences that will improve an individual's overall wellness and health outcomes. Our bio digital twin initiative aims to create digital replicas of patients that physicians can then use to simulate various treatments to enable optimal and patient-specific therapeutics. This article provides recent updates on our projects and team members.

Keywords: bio digital twin, cardiovascular disease

1. Introduction

The mission of the Medical and Health Informatics Laboratories at NTT Research is to make advancements in the medical and health sciences that will improve an individual's overall wellness and health outcomes. Our bio digital twin initiative aims to create digital replicas of patients that physicians can then use to simulate various treatments to enable optimal and patient-specific therapeutics. In the initial phase of this project, we at the MEI Lab are developing a cardiovascular bio digital twin (CV BioDT). We are targeting the cardiovascular system in part because of that system's prominent role in global mortality rates and the relatively high availability of data required for modeling.

Over the past year, the MEI Lab has made significant progress on several fronts. In December 2020,

we signed a research agreement with Japan's National Cerebral and Cardiovascular Center (NCVC) to jointly develop cardiovascular disease-related computational models, implement them on a bio digital twin platform, and develop applications for use by physicians and patients. In the first half of 2021, we made two key hires, Dr. Jon Peterson, newly promoted to a distinguished scientist, and Iris Shelly as a scientist.

2. NCVC joint research

The two-and-a-half-year project with the NCVC is titled "The Development of Human Hemodynamics Mapping and Autonomous Multimodal Therapeutics Systems." It involves research at both organizations. The principal investigator (PI) for the joint research agreement on the NCVC side is Dr. Keita Saku, laboratory chief of NCVC's Department of Cardiovascular Dynamics. I have the PI role on the NTT Research side.

The agreement calls for the NCVC to develop integrated computational models to support multimodal closed-loop interventions for acute myocardial infarction (AMI) and acute heart failure (Acute HF). In parallel, the MEI Lab will be implementing these models into a bio digital twin platform and developing physician- and patient-oriented applications to support physician clinical decision making and patient self-care.

The NCVC is a semi-independent national institution. Its government affiliation is through the Japan



Ministry of Health, Labor and Welfare, the counterpart to the U.S. Department of Health and Human Services. The NCVC focuses on intramural cardiovascular clinical practice and dedicated cardiovascular research. As such, it resembles the National Heart, Lung and Blood Institute (NHLBI) of the U.S. National Institutes of Health. Unlike the NHLBI, however, the NCVC is not a cardiovascular research funding agency.

Near-term goals for the joint project include the development and validation of models representing heart and vascular dynamics, particularly as they relate to AMI and Acute HF. Heart and vascular models that include neural control of circulation, as well as heart energetics, will be fundamental to computational platforms for determining optimal therapies for heart conditions. New models that Dr. Saku is developing in support of the CV BioDT will help determine optimal interventions for AMI and Acute HF across multiple therapeutic modalities such as medications, medical devices, and neuromodulation. The longer-term goal is to achieve patient-specific CV BioDTs to enable patient-specific therapeutics.

The MEI Lab entered this partnership with Dr. Saku and the NCVC because of their internationally recognized expertise in cardiovascular regulation and advanced technologies relating to closed-loop automated therapeutic interventions for conditions such as heart failure and mechanical circulatory support. This exciting project has also benefited from the instrumental support of Dr. Kenji Sunagawa, professor emeritus in the Department of Cardiovascular Medicine at Kyushu University and founder of the Department of Cardiovascular Dynamics at the NCVC Research Institute. Dr. Sunagawa trained both Dr. Saku and myself (in my case, at Johns Hopkins University, Kyushu University and NCVC) and helped orchestrate this agreement. Going forward, he will play a leadership role in this project for the MEI Lab.

By February 2021, the MEI Lab had already conducted two proof-of-concept studies to establish requirements and frame the initial bio digital twin platform architecture. The CV BioDT models developed through this joint research agreement will need to be validated in further studies before subsequent validation in preclinical human studies. These tests will be conducted at NCVC hospitals. During later stages of the CV BioDT validation and rollout, additional organ systems will be added towards the goal of an overall bio digital twin. In a noteworthy development, interfaces with the renal, respiratory, pulmo-



nary and some neural systems are advancing sooner than expected.

3. New staff scientists

In February 2021, it was announced that Dr. Jon Nels Peterson had joined the MEI Lab, then as a senior scientist. Dr. Peterson is a biomedical engineer with both academic and medical device industry experience. He had most recently been principal clinical systems engineer at Micro Systems Engineering, Inc., where he was the lead systems engineer for a family of implantable cardiac monitors. He also previously held research and engineering positions at Boston Scientific CRM and Create, Inc. and was a research assistant professor at the University of Vermont College of Medicine. Dr. Peterson's background as a research scientist and clinical systems engineer, with experience in hardware, firmware, and software subsystems, his talent for mathematical modeling and simulation, and his understanding of physiological control systems, as well as pathophysiological states such as heart failure, all bear directly on the MEI Lab's agenda.

In June 2021, it was announced that Iris Shelly had joined the MEI Lab as a scientist. An applied research engineer with expertise in biomedical signal processing and low-power devices, Shelly was most recently a senior applied research engineer at Micro Systems Engineering, Inc., where she designed, developed, and validated cardiac arrhythmia detection algorithms. She is initially working on model architecture and the interface for the CV BioDT. Her algorithm design experience and attention to detail, honed through years of experience in medical device research and software verification, are vital skills in support of model development for the CV BioDT.

4. Leadership shift

Taken together, the partnerships with the NCVC and new hires represent significant progress for the MEI Lab’s bio digital twin initiative, which I have led since joining NTT Research in 2020. Before closing, I should mention another notable development: my appointment as director of the MEI Lab in July 2021, where I succeeded Dr. Hitonobu Tomoike, who has assumed the position of research professor at the

NTT Basic Research Lab.

In this new position, I will continue to lead the CV BioDT group but now with Dr. Peterson as co-lead. I have also been engaged in harmonizing other MEI Lab projects, namely those involving implantable electrodes and remote sensing, within an overarching strategy that aligns with NTT Research and the broader NTT Group. It is an honor to follow in Dr. Tomoike’s footsteps and continue to advance the MEI Lab’s ambitious “moonshot” goals.



Joe Alexander

Director, Medical and Health Informatics Laboratories, NTT Research, Inc.

After graduating with a degree in chemical engineering from Auburn University, he studied medicine as a fellow of the Medical Scientist Training Program (MSTP) at Johns Hopkins Medical School, where he received both an MD and PhD. His PhD is in biomedical engineering, where he specialized in cardiovascular dynamics, training with Dr. Kenji Sunagawa in the laboratory of the late Dr. Kiichi Sagawa. Immediately afterwards, he completed a fellowship in research cardiology at Albert Einstein College of Medicine before additional training as a Japan Society for Promotion of Science (JSPS) Fellow at Kyushu University. He then took academic faculty positions in biomedical engineering and in medicine at Vanderbilt University while simultaneously completing a residency in internal medicine at Vanderbilt Hospital. During that time, he helped train astronauts such as Dr. Chiaki Mukai for the Neurolab Spacelab Mission. He likewise collaborated with The National Cerebral and Cardiovascular Center as a visiting researcher supported by the Science and Technology Agency of Japan. Following academia, he entered Pharma – first Merck then Pfizer. During his 18 years at Pfizer, he worked in various capacities including roles in R&D, Business Development, and Medical Affairs. In Pharma as in academia, his passion for modeling and simulation was evident throughout his work and extended across therapeutic areas. He is credited with creating several Pharma modeling platforms including The Lyrica Virtual Lab, The Neuropathic and Neuropathic-like Pain Virtual Lab, and The Pulmonary Vascular Disease Virtual Lab. He is a fellow of the American College of Cardiology (FACC) and is very interested in heart failure, pulmonary hypertension, and medical devices.

A New Lab Exploring Emergent Matter from Light

Michael D. Fraser

Abstract

In September 2021, NTT Research unveiled its new smart workspace in Sunnyvale, California, called the NTT OneVision building. It is one of the first office buildings in Silicon Valley built for a post-pandemic vision of the workplace with collaboration-focused spaces, state-of-the-art health monitoring capabilities, and new layouts. The 35,100 square foot office building also contains a new optical laboratory for the NTT Research Physics & Informatics Laboratories (PHI Lab).

The Sunnyvale optical lab supports multiple users and research themes. One specific design focus when planning the new lab was to provide ways to experimentally create and study many-body states of light, a specific example of which is the engineering of a bosonic fractional quantum Hall state using light. This article provides a brief review of our research agenda on quantum many-body states of light and details of the new lab.

Keywords: optical lab, quantum many-body states, fractional quantum Hall effect

1. Research agenda

In traditional condensed matter platforms, the interactions between large ensembles of particles (such as electrons or atoms) lead to the emergence of fascinating new physical phenomena such as superconductivity, superfluidity and the fractional quantum Hall effect. Key to the most exotic of these emergent phases of matter is strong interactions between the constituent particles. While photons (particles of light) do not typically interact, advances in optical materials and hybrid-optical structures can also induce very strong non-linearity between photons. Furthermore, the ability to control photons to very precise, even single photon levels, in addition to more recent discoveries such as topological states of light, make optical platforms extremely exciting for the exploration of fundamentally new states of matter. Pursuing new optical platforms that strategically combine these and other properties, we aim to create and explore new many-body quantum states of light.

In optics, there are many experimental platforms we might use, each of which has distinct features and advantages. Exciton-polaritons (bosonic half-light,

half-matter quasi-particles in a semiconductor micro-cavity), for example, have the advantage of relatively strong interactions, a result of hybridizing cavity photons with interacting electronic excitations. This platform may be fabricated using a variety of materials and structures, also with spatial structuring and even topological phases. Meanwhile, implementation of topological models in a time-multiplexed optical resonator network (a similar geometry to the coherent Ising machine) is a distinct methodology with the unique feature of being able to engineer non-local interactions, which makes this also an exciting platform to study in the context of lattice bosonic quantum Hall effects.

The breadth of photonic-platform exploration is enhanced by strategic partnerships with external institutions, including California Institute of Technology, Massachusetts Institute of Technology, Stanford University and RIKEN – a major scientific research institute in Japan. Of course, much of our work will take place at Sunnyvale. Some of the fundamental problems we are seeking to initially explore in the new optical lab include the following:

1. How can photons be made to interact (very)

strongly – to the level at which strong correlations and new physical phenomena result?

2. How can we induce a large artificial magnetic field for neutral photons, and use this to create topological states of light?
3. What new quantum states of matter and other phenomena might result from highly non-linear, structured photonic systems?

Pursuing our research agenda requires precise optical control, extreme conditions, including low temperatures and large magnetic fields, as well as advances in materials and innovative device design. Our Sunnyvale laboratory is uniquely positioned to approach these challenges, combining in the same space advanced material and device fabrication with ultra-low temperatures, high magnetic fields, and new schemes for optical manipulation and measurement.

2. Optical lab features and capabilities

The main lab area is about 35 feet x 33 feet, with a very high ceiling, which is useful for installing and operating larger equipment, such as our 11-foot-tall dilution fridge. The room is divided into three parts with retractable optical blackout curtains separating the sections. Two sections, which may each be independently and completely blacked out, are host to two distinct experimental research themes, while the other room will always be lit and used for discussions, data analysis, sample preparation, etc.

There were many design requirements incorporating a range of Physics & Informatics Laboratories (PHI Lab) experiments, and it was necessary to make numerous accommodations. The combination of

research projects together had strict requirements, necessitating design of custom HVAC (heating, ventilation, and air conditioning) systems, noise isolation for pumps and compressors, and removal of all magnetic materials from sections of the room. Some of the lab's notable features and capabilities include the following:

- **Precise optical control:** In the context of our experiments, this initially means being able to create and drive optical phenomena on micron or smaller scales with high spatial precision and reproducibility. It will eventually become more stringent, where we will need to have such precise spatial and temporal control at a single photon level of quantum objects.
- **Temperature range:** Certain experiments are being conducted at room temperature, which is one of the advantageous features of optics experiments in general. Other experiments are conducted at significantly using materials and devices cooled to much lower temperatures. We will have two helium refrigerators as part of the lab infrastructure. One is compact and fast to use and operates at around 4 K. This is a sufficiently low temperature to study, iterate new materials and structures in detail, and reveal new physics of these samples. The other refrigerator, known as a dilution fridge, may reach about 5 mK (about 60,000 times colder than room temperature) and is a highly customized apparatus. Such low temperatures are desired because quantum states of matter (many-body states, in particular) are typically revealed only at very low temperatures. Even if a given many-body quantum state can be observed (or engineered to appear) at



higher temperatures, lowering the temperature gives robustness to this quantum state. The fractional quantum Hall effect in its traditional electronic manifestation is paradigmatic of a system requiring and benefitting from both criteria. Both fridges have optical excitation and imaging access with low vibration and high spatial resolutions.

- **Large magnetic field:** A magnetic field can be used to strongly modify the properties and behavior of electronic and magnetic materials. In two-dimensional (2D) electronic materials, a strong magnetic field applied to samples at low temperature quenches the kinetic energy leading to the formation of topological bands and an enhanced importance of interactions, the necessary ingredients to create an electronic fractional quantum Hall effect. We will be studying the emergence of such states in new monolayer optical semiconductors in which optical techniques (not just electronic) can be used for measurement and control. Hybridizing with other monolayer materials may also be used to create new functionality and control.
- **Fabrication tools:** It is atypical for an optics lab to have sample fabrication integrated into a single facility, but in doing so, we hope to be able to rapidly iterate the process of design, fabrication, and measurement of new samples, along with a fast turnaround of testing new materials and incorporating new ideas and refinements into updated sample structures. Whereas traditionally, complex semiconductor structures need to be ‘grown’ in large chemical reactors run by teams of people, newer materials including van der Waals materials may be assembled manually layer-by-layer using a compact but precise set of fabrication tools. In our laboratory, we have an inert atmosphere glove box housing a state-of-the-art 2D material transfer station capable of constructing these structures with atomic level precision in addition to an atomic force microscope for structural characterization. The glove box maintains an oxygen-, water-, and other impurity-free atmosphere (down to the level of parts per billion) for clean sample fabrication.
- **Optical measurement and control:** Part of the design feature set of the laboratory is to be able to fabricate and characterize new materials and structures. Another is the ability to optically pump and measure the dynamics of electronic and optical excitations in these devices. Our

cryogenic capabilities were chosen such that we can measure with sub-micrometer levels of vibration for precise excitation and imaging. We also work with very narrow-linewidth stable laser sources across several wide frequency bands (including ultraviolet, visible, and near-infrared) which will be combined with spatial light modulators to drive structured spatial and temporal dynamics of these excitations.

3. Flexible and focused

As with any new experimental optics laboratory, we needed to make sure the Sunnyvale lab was not too specific to be flexible with the exploratory nature and changing directions of the research projects. We have a well-balanced set of complimentary and cutting-edge equipment and apparatus, the combination of which is unique and offers us the ability to conduct entirely new experiments and work with as-yet unstudied but promising materials, of which only this apparatus is capable.

For the specific themes discussed in this article, the exploration and creation of quantum many-body states in optical platforms is enabled through the development of new techniques, new materials, new theory, and by innovative design of experiments. We are gradually building a toolbox of experimental techniques, materials and device designs that will give us further opportunities to create fundamentally new states of matter with optics.



Michael D. Fraser

Senior Research Scientist, Physics and Informatics Laboratories, NTT Research, Inc.

He received a B.Sc. in physics and physical mathematics and B. Eng. in microelectronics engineering from Griffith University in 2002 and Ph.D. from the Australian National University in 2010. He joined the PHI Lab in 2019, where he focuses on condensed matter physics using optics. He has co-authored numerous papers with PHI Lab Director Yoshihisa Yamamoto, whom he met while a Fulbright Fellow at Stanford University. He concurrently holds a position as a senior visiting scientist at RIKEN, Japan.

Security as Driving Force of the Future

Shinichi Hirata and Katsumi Takahashi

Abstract

This article describes research and development (R&D) of security in the Innovative Optical and Wireless Network (IOWN) era to create a prosperous and enriching society. We seek to change the role of security to activating people and ideas. This new form of security will solve diverse problems related to security motivation in individuals, organizations, and society, convert ideas and computing resources directly into work, and ensure continuous security. We will achieve this through R&D based on the three pillars of theory, data-driven approach, and communication.

Keywords: security, IOWN, R&D

1. Driving force of the future

We have been studying communication and information security continuously for more than 30 years. During this time, the Internet came into being as a means of communicating safely no matter where one may be through cryptography; similarly, the web and cloud came into being as means of safely storing information anywhere through security measures. However, while our daily lives have thus far been protected by such security measures, it cannot be overlooked that there is still much anxiety over security threats; thus, the need for giving full attention to security measures.

The Innovative Optical and Wireless Network (IOWN) era will make life more enriching and satisfying through information and communications technology (ICT) that exceeds the limits of conventional technology. It is our goal to make security the driving force behind this transformation.

There is no debate as to the need for security. The security by design approach is being increasingly adopted, which points to the inherent need for security in achieving healthy individual and social activities. However, keywords, such as *security cost* and *security fatigue*, have appeared, reflecting the common feeling that anything that is needed to ensure healthy activities must be obligatory and trouble-

some. We disagree with this mode of thinking. Simply put, security should bring about a bright future.

It is our intent to change the current belief that security technology is necessary but difficult through research and development (R&D) on the basis of the following viewpoints:

- Security is widely useful for all types of work and lifestyles (*extended*).
- Security can convert ideas and computing resources directly into work (*efficient*).
- Security is ongoing (*continuous*).

In this article, we explain the concept of security R&D in the IOWN era from the viewpoints of extended, efficient, and continuous security and outline the security technologies that we will target (**Fig. 1**). The type of security discussed in this article is information security that, while not intended for maintaining public peace and order, includes peripheral fields such as privacy and ethics.

2. Extended security

It had been generally believed that security is for a particular system to be unbreakable. Since we see security as being useful for all types of work and lifestyles, we would like to drive the evolution of security R&D from the two viewpoints of security targets and security motivation.

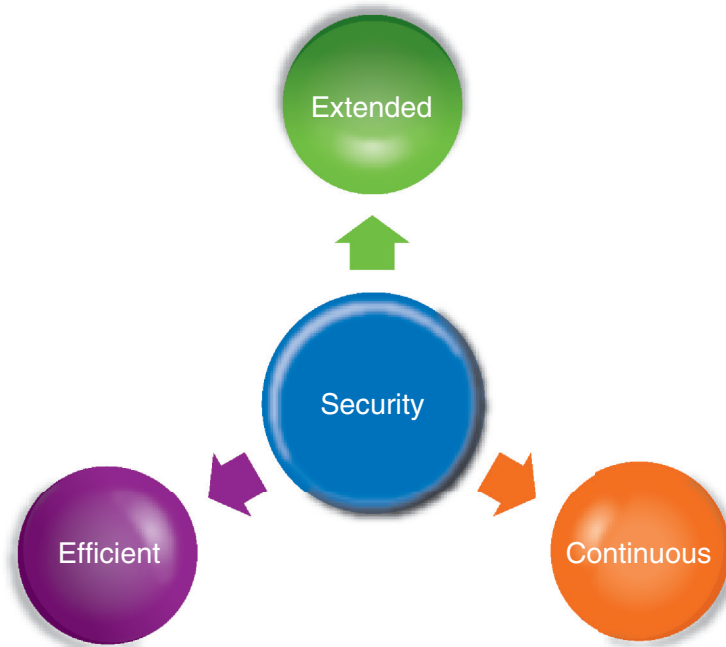


Fig. 1. Concept of security R&D in the IOWN era.

2.1 Extended 1: Security targets

In addition to particular systems (information assets) as targets of protection by security, we would like to include companies and organizations, people, and society.

2.1.1 Information assets

The target of security has been called *information assets*, which means a company's customer information, sales information, technical information, etc. The protection of information assets depends on the form of their records or storage, so the means of storing these information assets will also be a target of protection. Typical formats include files; media, such as paper; disk storage; transmission channels; hardware systems, such as smartphones and computers; and software systems, such as email, databases, and artificial intelligence (AI) services. We can add Internet of Things (IoT) devices such as drones and industrial robots.

2.1.2 Extension to companies and organizations

The targets of security are expected to change greatly in parallel with changes in the activities of companies and organizations. For example, determining the form of information assets will become difficult. Information assets may be placed in storage equipment outside the company or under the management of a separate organization through inter-compa-

ny transactions. In future companies, the data generated by others in a procurement or supply chain may become an information asset of those companies. The introduction of IoT devices, however, will make the form of information assets all the more fluid.

2.1.3 Extension to people

If people were to be regarded as a medium of information assets, they could be called a medium requiring a very high degree of confidentiality. While it is said that facial expressions reflect a person's feelings, it is not the case that customer information could be leaked from facial expressions. People can be easily deceived, and in some cases, they can betray others. Corporations deal with such situations by training their employees and establishing rules and regulations. There is also posting in social networking services (SNSs) as a medium of people's activities not limited to those of corporations. Information security incidents via SNSs include information leaks, copyright infringements, and flaming. However, such incidents are mostly left as a matter of personal responsibility. When it comes to security targeting people, there is a limit as to what safety management that treats people as systems can accomplish.

2.1.4 Extension to society

There is currently no established opinion on whether society can be set as a target of security. Autonomous

car and surveillance-camera systems, for example, are in the process of becoming systemized at a social level. In a smart city, such systems will have basic conventions (policies) with regard to security, so this can be thought of as an extension of a conventional security target, though it depends on the system scale. A specific example is how a pandemic should be dealt with. Measures, such as contact-tracing apps, operate under clear policies, but the rules of behavior behind the operation of many other measures tend to be agreed upon by consensus through voluntary and spontaneous exchanges of information. It is thought that society as a whole operates in this manner. Such rules of behavior are sometimes referred to as ethics or customs, and dealing with them requires a new approach.

2.2 Extended 2: Security motivation

We believe that the reasons (motivation) security is necessary are wide-ranging going beyond preventing information leaks. They also include the existence of incidents, system quality, laws, ethics, customs, and social objectives.

2.2.1 Incidents

The most known motivation for security is preventing information leaks. It is common knowledge that this motivation drives measures for blocking a variety of threats such as unauthorized access, malicious software, and unauthorized entry and exit. However, we believe that it is important not to think of such incidents as infringing upon confidentiality, integrity, and availability. For example, incidents involving privacy (flaming) should also be given attention. Instead of being a matter of information leaking, they have been thought of as a peripheral security problem that arises due to inadequate explanation of information access, purpose of use, etc. or violation of rules. We should also think about whether abnormal AI operations are peripheral security problems. The results of AI operations have not traditionally been considered a security problem. We consider that problems requiring attention should not be treated within the conventional security framework but be extended to include any problems brought about by computers or problems related to privacy, AI, etc.

2.2.2 System quality

In fields such as critical infrastructures, a high level of security is required beforehand in system development. This need produces some of the motivation for security. Yet, there are also systems in which security is just a tacit requirement. In such a case, the level of security required is also tacitly expressed, and pro-

viding for security is simply regarded as a development cost. This is a problem that cannot be ignored. Security is an inherent requirement of a system, so any deviation from that requirement due to a lack of motivation must be fundamentally solved starting with its cause.

2.2.3 Laws

Observing laws and regulations is also a security motivation. In Japan, the Basic Act on Cybersecurity calls for the people of the nation to make security-related efforts. For companies, this means security premised on such laws as the Act on the Protection of Personal Information and Unfair Competition Prevention Act. We believe that it is not simply a matter of scrutinizing the security-related legal system and applying it to R&D but something that must be actively participated in through discussions on what the legal system should be.

2.2.4 Ethics, customs, and social objectives

There are cases in which security would still be felt necessary even if there were no fear of incidents, quality was kept constant, and laws were complied with. This feeling is based on values and fears that people hold within themselves that can be expressed in terms of ethics, customs, and social objectives. We believe their existence should be treated as elements providing some of the motivation for security.

3. Efficient security as a driving force

Unfortunately, security has the possibility of being treated as a business cost, but we would like to change this perception by introducing the concept of security efficiency. Efficiency relates to (1) ideas and (2) computing resources. Maximizing both these aspects will maximize the efficiency of security.

3.1 Efficiency 1: Converting ideas directly into work

We are investigating security that does not hinder the implementation of ideas and supports people in challenging themselves. When implementing an idea, security requirements and methods of achieving them must be determined. Minimizing this process leads to efficiency, and ideally, the security required at the time of system development would be built-in without having to worry about it.

Determining requirements normally consists of analyzing all the elements described above under security motivation, legal compliance assuming the occurrence of incidents, etc. Next, in determining a method for satisfying these requirements, it should be

noted that constructing security measures from scratch is seldom done. The typical approach is to survey available components (in a library) and use the security functions needed.

We are now investigating minimizing and automating both processes. The automation of security is extremely difficult, but the problems involved can be solved through a theoretical approach and the data-driven approach described later. In addition, if *best coupling* of security requirements and implementation methods can be provided through a development environment and user interface, a shortcut to solving these problems should be achieved.

3.2 Efficiency 2: Converting computing resources directly into work

In current web applications, for example, no one is really concerned about the fact that security processing generates overhead and slows down communications and screen displays. However, in the IOWN era in which a massive amount of devices in urban, transport, and other social infrastructures are connected to the network, this cannot be ignored. In the context of carbon-neutral initiatives, security processing that can make full use of computing and communication resources is desirable. For this reason, we are investigating security that can exploit the special features of advanced hardware represented with the All-Photonics Network of IOWN and maximize our experience with information communications.

4. Continuous security

Security must be continuously maintained. Security attacks and defensive measures evolve along with ongoing progress in information processing technology, so our R&D efforts in this area are ongoing to be prepared for that evolution. There is another reason continuity in security R&D is necessary. The core of security technology is theory and data. An example of the former is cryptography and an example of the latter is whitelisting/blacklisting in which theory and data, respectively, must be continually built up. In contrast to the continuity of security technology, the arrival of discontinuous changes in the form of quantum computers is predicted. We are therefore investigating the development of technology based on continuity that can withstand even major changes.

5. Three new pillars of security R&D

To achieve extended, efficient, and continuous

security, we are promoting R&D focused on the following three pillars (Fig. 2).

5.1 Guaranteeing security through theory

Cryptography guarantees the confidentiality of applied data through theory. Given a software module that is theoretically guaranteed to be safe, there is no need to worry about the security of that module. If a system should be constructed by correctly interconnecting only theoretically safe modules, that system can be evaluated as being entirely secure. Increasing the number of theoretically safe modules will clearly contribute to achieving system security. While cryptography is typical of theory that can guarantee security, mathematics, including cryptography, cryptographic protocols, and formal methods, forms the foundation of this theory. Attention is also being given to physics. If quantum information processing becomes possible, we can expect the prevention of new forms of eavesdropping and data alteration to be found not only in communications but in data processing.

5.2 Guaranteeing security by using a data-driven approach

Theoretically guaranteeing the security of all targets is difficult, so it is necessary to guarantee certain items in a data-driven manner. For example, given an infrastructure system consisting of multiple devices, one approach is to record the state of all constituent devices and evaluate risk. This work would be carried out throughout a supply chain and its operations. The records of these states constitute data, and their evaluation is called a data-driven approach. Those parts of an evaluation result that can be used at other times and in other environments can be reformatted and reused. This data-driven approach can be applied to any security target in addition to infrastructure systems. We call such data for conducting re-evaluations *trust data*, which includes both positive and negative evaluations with regard to safety. Using trust data enables a data-driven type of security guarantee. Trust data are not intended to be absolute overall but rather local and fair.

5.3 Communication for a consensus of security level

In addition to the theoretical and data-driven continuous approaches, there is the communication approach in relation to forming agreements that we have come to recognize as being extremely necessary. We noticed that we have to consider how to establish

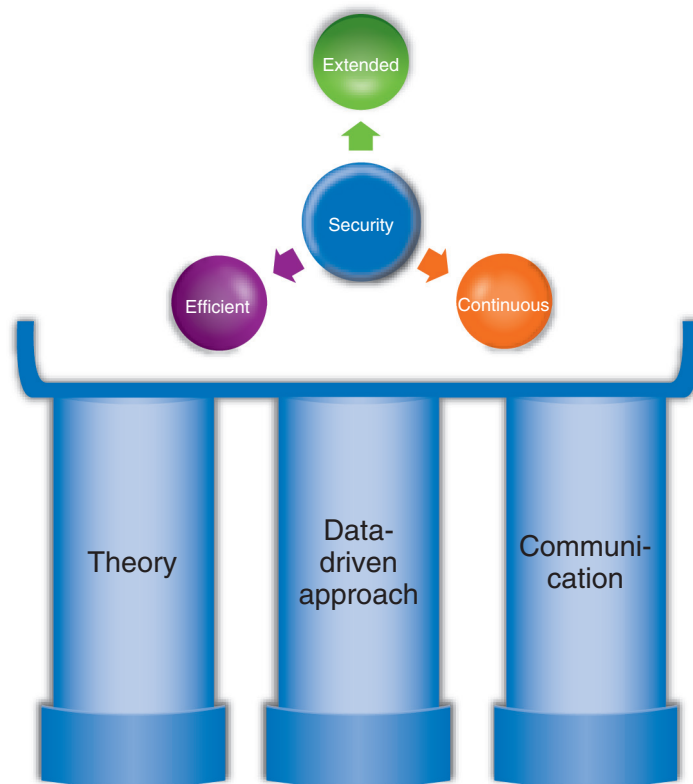


Fig. 2. Three pillars of security R&D.

a security policy, which is a precondition of executing security measures, by considering what is safe to do, and what should be done so that people can live their lives to the fullest without anxiety. To establish a policy that confirms a *security motivation*, we believe that forming agreements through communication between the parties concerned becomes important while extending security in the narrow sense to ethics, customs, and social objectives. We are studying a mechanism for forming agreements on security decisions by concerned parties and a mechanism for evaluating whether operations can actually be carried

out according to the agreed-upon decision.

6. Conclusion

In this article, we reorganized the direction of security R&D in the IOWN era from the viewpoints of extended, efficient, and continuous security and outlined the security technologies that we will target by the three pillars of theory, data-driven approach, and communication. We aim to create a society without anxiety regarding security with high ethical standards and technologies.

**Shinichi Hirata**

Vice President, Head of NTT Social Informatics Laboratories.

He received a B.S. in mathematics from Hokkaido University in 1990. He joined NTT the same year and has been engaged in R&D of cryptography, IC card technology, and authentication systems.

**Katsumi Takahashi**

Executive Research Scientist, Chief Security Scientist, NTT Social Informatics Laboratories.

He received a B.S. in mathematics from Tokyo Institute of Technology in 1988 and Ph.D. in information science and technology from the University of Tokyo in 2006. He joined NTT in 1988 and has studied information processing technologies including security and privacy.

Secure Optical Transport Network

Tetsuya Okuda, Koji Chida, Daisuke Shirai, Sakae Chikara, Tsunekazu Saito, Misato Nakabayashi, Kazuki Yamamura, Yuri Tanaka, Katsuyuki Natsukawa, and Koichi Takasugi

Abstract

The implementation of an optical transport network, especially between datacenters, has been progressing. Similar to the Internet, communications on the optical transport network are protected by public-key cryptography and symmetric-key cryptography, but there are concerns that advances in the research and development of quantum computers will pose a risk to current cryptographic systems, public-key cryptography and key exchange in particular. In response to this problem, researchers at NTT Social Informatics Laboratories and NTT Network Innovation Laboratories are engaged in the research and development of safe key-exchange schemes to counter the cryptographic risks posed by quantum computers. They are also engaged in architecture design and tests with actual equipment with the aim of applying such key-exchange schemes to the optical transport network.

Keywords: optical transport network, quantum key distribution, post-quantum cryptography

1. Background

1.1 What does “transport” mean?

“Transport” is often defined as “carrying” (as in physical distribution) or “transmission” (as in communications). In other words, it generally refers to corporate distribution and transport services and to communication and transmission services. To make it easy to imagine the features of a secure optical transport network as a technology affixed with the label “transport,” we begin our discussion using distribution and transport services as an example (**Fig. 1**).

What are the features of distribution and transport services by truck? Various images may come to mind, such as the carrying of many goods at one time and the prompt delivery of goods after orders are placed. We take up such features from the five viewpoints listed in **Table 1**.

First, in distribution and transport services, large capacity and low delay are features that are most important to customers and that give value to these services. Large capacity means a large number of trucks and low delay means short truck queuing time.

From the viewpoint of running a distribution and transport business, efficient operations are essential, which can be expressed as the optimization of distribution and the economical management of daily operations. Many questions are now being asked about the social impact of services, so concerns about environmental load and safety have also become service features. Environmental load means low levels of exhaust gas/carbon dioxide (CO₂) and safety means correct delivery of goods and few traffic accidents.

What do these features mean in communication and transmission services? Large capacity and low delay are also the features that are the most important to customers and that give value to these services. Using terms from the field of communications, large capacity means high throughput and low delay means low latency. From the viewpoint of running a communication and transmission enterprise, efficient operations are likewise essential, which can be expressed as network efficiency in providing communication and transmission services. Finally, it is also true in the communications industry that the social impact of

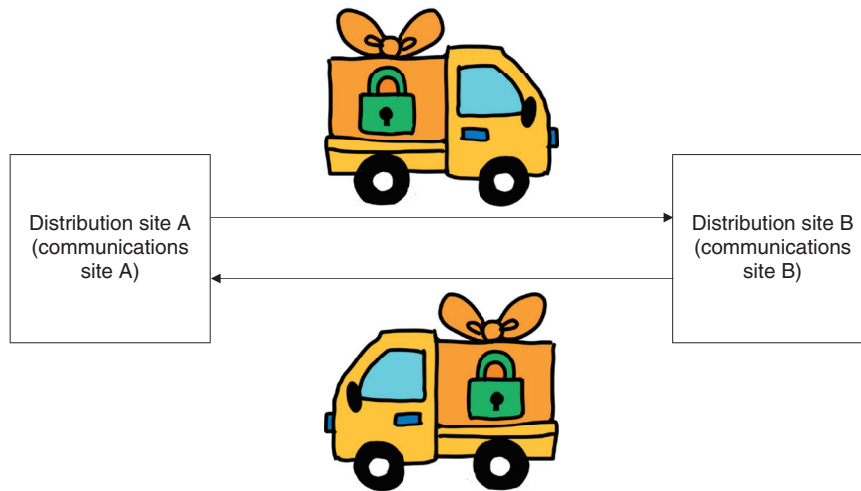


Fig. 1. What does “transport” mean?

Table 1. Comparison of distribution/transport and communication/transmission services.

Service features	Distribution/transport services	Communication/transmission services
Large capacity	Number of trucks	Throughput
Low delay	Truck queuing time	Latency
Efficient operations	Distribution optimization	Communication network optimization
Environmental load	Exhaust gas/CO ₂	Power consumption
Safety	Correct delivery of goods Few traffic accidents	Few communication failures High level of security

services has come under the spotlight, so environmental load and safety have also become of concern. In this industry, environmental load means low power consumption and safety means few network failures and a high level of security.

Among the five viewpoints listed in Table 1, the Innovative Optical and Wireless Network (IOWN) and All-Photonics Network (APN) under research and development at NTT aim for services that take into account the three points of large capacity, low delay, and low environmental load that appeal most to customers [1]. The first step in adding the viewpoint of “safety = security” to IOWN/APN is the secure optical transport network proposed in this article.

1.2 Necessity of an optical transport network

Many people have come to appreciate how their lives have become more convenient thanks to the proliferation of mobile phones and smartphones and the expansion of the large-capacity and low-latency fifth-generation mobile communications system

(5G). Large capacity and low latency are also desirable features in communication and transmission services targeting corporate customers. Customer needs have come to focus on datacenter interconnect services envisioning the need for datacenter disaster recovery as well as on uncompressed video transmission services for remote production to enable simultaneous and parallel work between a video production site in the field and an editing site. Transmitting such large-capacity data with low latency in real time to the extent possible requires the application of optical transport [2]. This article introduces our efforts in adding security to optical transport.

2. Current technologies

2.1 Internet standards

To add security to communication and transmission services, we can expect the application of current technologies used on the Internet to be effective and to mature in terms of evaluating security the longer

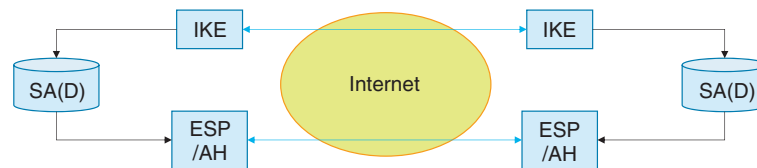


Fig. 2. IPsec architecture.

they stay in use.

On the Internet, Secure Sockets Layer/Transport Layer Security (SSL/TLS) and Security Architecture for Internet Protocol (IPsec) are typical protocols used for configuring safe communication paths (secure channels). SSL/TLS is a standard protocol for configuring a secure channel between a web server and client. IPsec is a standard protocol for configuring secure channels between sites such as between a company's main office and its branch offices. It is a technology used in virtual private network services. The secure optical transport network introduced in this article is a communication and transmission service operating between sites.

2.2 IPsec

IPsec for configuring a secure channel between sites is specified by the Internet Engineering Task Force (IETF), an organization that formulates de facto Internet standards. The IPsec specifications are organized into architecture, encryption, authentication, and key exchange [3].

IPsec's architecture features the following mechanisms: Internet key exchange (IKE) that exchanges keys, encapsulated security payload (ESP) that performs encryption and authentication, authentication header (AH) that performs authentication, and security association database (SAD) that conveys the keys agreed upon in IKE via ESP or AH (Fig. 2). "Authentication" includes message authentication and entity authentication, which test the validity of a message delivered from a communication destination and that of the communication destination, respectively.

Next, we discuss how this IPsec configuration might change in a secure optical transport network.

3. Issues and proposals (I): Possibility of advances in quantum computers

3.1 Possibility of advances in quantum computers

Current communications on the Internet and other networks use key exchange based on public-key cryp-

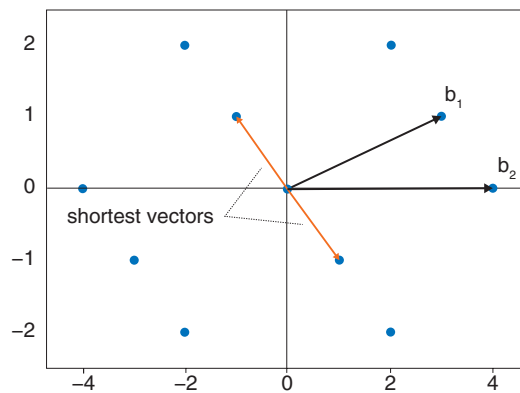
tography, which uses a problem that is difficult to solve mathematically as a basis for ensuring security. For example, the Rivest-Shamir-Adleman (RSA) cryptosystem uses the fact that factoring the product of two large prime numbers takes an extremely long amount of time as a basis for security. However, if a genuine quantum computer having error resilience could be achieved, factoring the product of two large prime numbers could be performed in a relatively short time. If so, the RSA cryptosystem could no longer be called secure. To solve this problem, we have been researching and developing a key-exchange scheme that cannot be broken by a quantum computer.

3.2 Quantum key distribution

Quantum key distribution (QKD) is a mechanism for distributing keys by quantum physics. It shares information on a secret key via quantum states on a quantum channel that can transmit quantum states. The most outstanding feature of QKD is the ability to detect eavesdropping by a third party when sharing the secret key. This originates in a property unique to quantum mechanics that measuring a quantum state changes the state. If a third party is attempting to eavesdrop, that is, to carry out measurements while two parties are sending and receiving a quantum state, the sent quantum state and received quantum state will differ. Consequently, if the two parties should then check with each other on their sent and received states and find that they differ, they would be able to detect that a third party is eavesdropping. Performing this process of sending/receiving quantum states and checking for eavesdropping repeatedly increases accuracy and eventually enables the two parties to share a secret key.

3.3 Post-quantum cryptography-based key distribution

Post-quantum cryptography (PQC) is a public-key-cryptography and key-distribution mechanism in which problems that are mathematically difficult to



Two-dimensional lattice vectors (blue points) generated by basis vectors $\{b_1, b_2\} = \{(3, 1), (4, 0)\}$. The shortest vectors in this lattice are $(1, -1)$ and $(-1, 1)$. The shortest vector problem—a major lattice problem—consists of finding the shortest vectors when given basis vectors $\{b_1, b_2\}$.

Fig. 3. Example of a lattice problem difficult for quantum computers.

solve provide a basis for security. In particular, problems that are assumed to be difficult even for a quantum computer to solve are used as grounds for security. In lattice-based cryptography, for example, it is assumed that finding the lattice points closest to the origin in a given set of lattice points is a difficult problem to solve even for a quantum computer, thereby providing a basis for security.

At NTT, research and development in this area is centered about NTRU, a type of PQC lattice-based cryptography incorporated in technology developed by a team including NTT (Fig. 3).

We generically refer to QKD and PQC-based key distribution (PQKD) as xKD.

4. Issues and proposals (II): Countermeasures against new attackers in architecture design

4.1 Countermeasures against attackers in a zero trust network

Designs that envision attackers in a zero trust network, which, as the name indicates, is a closed network that cannot be trusted [4] have become widespread. In this architecture design, it is necessary to assume attackers on all types of networks including telecommunications carrier networks and intra-site networks. In a telecommunications carrier network, it is assumed that an attacker will be intercepting communications by physically connecting to optical fiber, while in an intra-site network, it is assumed that an

attacker intercepting communications has access rights in that network.

We first consider an attacker attempting to intercept communications by physically connecting to optical fiber in a telecommunications carrier network. A defense can be mounted through *hop-by-hop encryption* such as OTNsec, a protocol that protects Layer 1 (physical layer), and MACsec, a protocol that protects Layer 2 (data link layer). Implementing encryption functions in lower layers in this manner should enable the addition of security without hindering the low-latency feature of IOWN/APN.

Next, to defend against an attacker who is attempting to intercept communications within an intra-site network while having access rights in that network, architecture design for inter-site communications typified by IPsec must be reviewed from the bottom up. In the secure optical transport network, key exchange equivalent to IPsec/IKE described above will correspond to xKD equipment, and encryption equivalent to ESP/AH in IPsec will correspond to an optical transponder or white-box switch. Given the trend toward a disaggregated architecture described later, it must be assumed that separate devices will perform key exchange and transmission and that the key exchange and encryption functions that were integrated in IPsec will take on a separated configuration (Figs. 4, 5, and 6). As a result, key information corresponding to SA(D) in IPsec will circulate in a network external to the device, which means that new measures

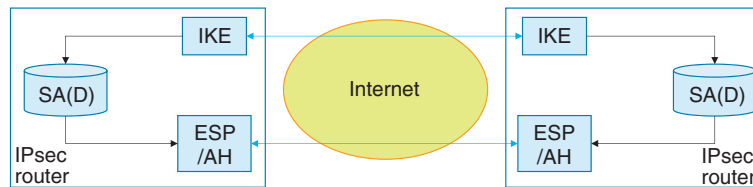


Fig. 4. Ordinary IPsec equipment configuration.

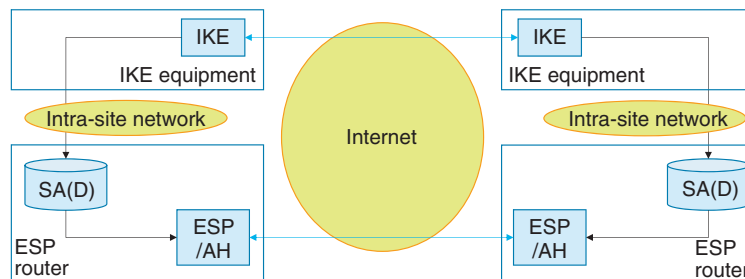


Fig. 5. Configuration with IPsec equipment separated.

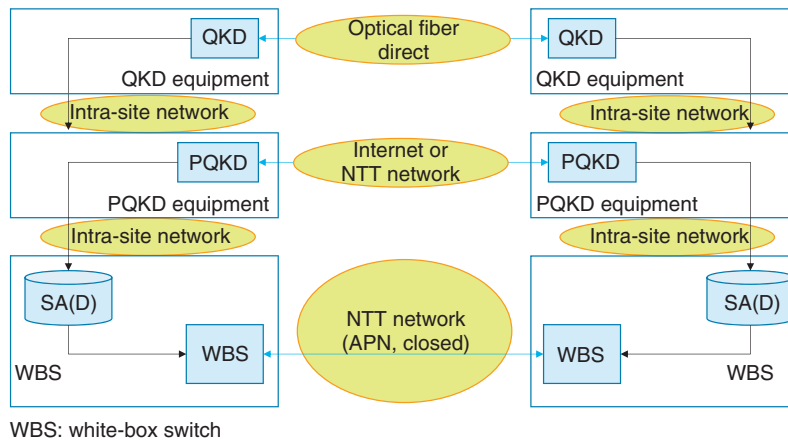


Fig. 6. Configuration with equipment of secure optical transport network separated.

must be studied for protecting communications on any type of network assuming a zero trust network. Specifically, it will be necessary to design a secure method for key distribution from xKD equipment to the optical transponder and a secure method for equipment authentication between xKD equipment and the optical transponder. For details on these studies, the reader is asked to consult a previously published paper [5].

4.2 Necessity of architecture and equipment that can be tested from the outside

In a zero trust network, the ability to test the reliability of architecture, protocol, equipment, etc. from the outside is required. The ability to make updates separately to architecture, protocol, equipment, etc. is also required as a fundamental security measure in anticipation of some type of danger. For architecture design, protocol design, and equipment selection described in this article, we adopted formal verification

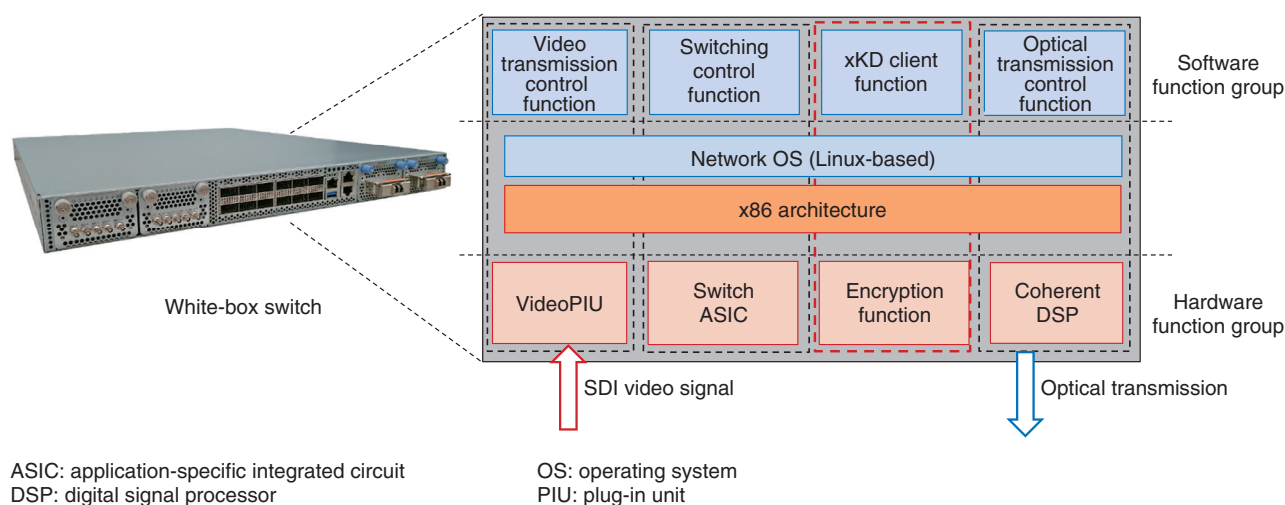


Fig. 7. Disaggregated architecture of white-box switch.

and the white-box switch as technologies for testing reliability from the outside and making updates separately.

4.3 Formal verification

At the time of protocol design including cryptography, there is a need for testing that can mathematically guarantee security as in maintaining the confidentiality of secret information within a protocol and ensuring the integrity of messages. In this regard, formal verification technology has been used for testing the safety of protocols such as SSL/TLS and IPsec that serve as transport layers and for testing the safety of authentication protocol on the 5G standard. Formal verification is a technology that describes a system and the properties that the system must satisfy in a formal language and that tests whether the system is satisfying those properties on the basis of logical reasoning. In formal verification, there are many components that can be automated by computer, so this technology excels in testing results from the outside including checking for reproducibility and in adaptively retesting in the face of protocol updates. For the secure optical transport network introduced in this article, we designed an IPsec-based protocol that combines xKD equipment with an optical transponder and tested its security using the ProVerif formal verification tool [6].

4.4 White-box switch

Transmission equipment for optical-transport purposes had been provided in a form that integrated

optical modules and various functions. In contrast, there is also equipment that adopts technology that enables flexible configuration changes, the addition of new functions, cost reductions, etc. by separating the various functions of the transmission equipment and controlling them by standardized interfaces in a disaggregated architecture. This equipment is called a white-box switch or white-box transponder. In our current research, we have taken a white-box switch and added an xKD client function for obtaining an encryption key from xKD equipment in the software function group in order to set the key and control the encryption function of the hardware function group (Fig. 7). We also added a function for directly inputting an SDI (serial digital interface) signal (video signal) and showed that uncompressed 8K60P video in excess of 40 Gbit/s could be securely transmitted with ultra-low latency using this function. Therefore, we have demonstrated the feasibility of secure optical transport linking xKD equipment and optical transponders.

5. Toward the future

In this article, we introduced a secure optical transport network as an initiative to add security functions to IOWN/APN now being researched and developed at NTT. We also introduced key issues and proposals in relation to this initiative. We consider our efforts to be one step in our ongoing plan to contribute to the provision of safe and secure technologies and services.

References

- [1] Website of NTT R&D, IOWN, <https://www.rd.ntt/e/iown/>
- [2] M. Tomizawa, A. Kaneko, and S. Kimura, "Device Technology Development for Beyond 100G Optical Transport Network," NTT Technical Review, Vol. 14, No. 9, 2016. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201609fa1.html>
- [3] IETF, "Security Architecture for the Internet Protocol," RFC 4301, <https://datatracker.ietf.org/doc/rfc4301/>
IETF, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, <https://datatracker.ietf.org/doc/rfc7296/>
- [4] IETF, "IP Encapsulating Security Payload (ESP)," RFC 4303, <https://datatracker.ietf.org/doc/rfc4303/>
IETF, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," RFC 6071, <https://datatracker.ietf.org/doc/rfc6071/>
- [5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST SP 800-207, Aug. 2020.
- [6] S. Maeda, M. Nakabayashi, and T. Okuda, "Architecture Design and Security Evaluation with Formal Verification for Secure Optical Transport Network," 95th Conference of the Special Interest Group on Computer Security (IPSI-CSEC), Nov. 2021.
- [7] B. Blanchet, "Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif," Foundations of Security Analysis and Design VII, pp. 54–87, Springer, 2013.



Tetsuya Okuda

Research Engineer, NTT Social Informatics Laboratories.

He received a B.S. and M.S. from the University of Tokyo in 2009 and 2011. Since 2011, he has been engaged in research & engineering on security protocol at NTT. He is a member of Information Processing Society of Japan (IPSI). He received the IPSJ/Computer Security Symposium Student Paper Award in 2019.



Koji Chida

Senior Research Engineer, Supervisor, NTT Social Informatics Laboratories.

He received a B.S., M.S., and Dr.Eng. from Waseda University, Tokyo, in 1998, 2000, and 2006. Since 2000, he has been engaged in research on cryptography and privacy-enhancing technologies at NTT. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and IPSJ. He received the IPSJ Best Paper Award in 2012.



Daisuke Shirai

Senior Research Engineer, Supervisor, Frontier Communication Laboratory, NTT Network Innovation Laboratories.

He received a B.E. in electronic engineering, M.E. in computer science, and Ph.D. in media design from Keio University, Kanagawa, in 1999, 2001, and 2014. He pioneered the world's first 4K JPEG 2000 codec system, which enables low latency 4K60p video transmission on a Gigabit network. He has applied his expertise across multiple domains through his study of practical applications in digital audio and video broadcasting technology, image coding, information theory, networking, human-computer interaction, and software architecture. His current research topics include remote video production network, ultra-low latency visual communication and its security over optical transport networks.



Sakae Chikara

Senior Research Engineer, Information Security Technology Research Project, NTT Social Informatics Laboratories.

He received a B.E. and M.E. in electrical and electronic engineering, system of electronic from Tokyo Institute of Technology in 1988 and 1990. He joined NTT Telecommunication Networks Laboratory in 1990 and studied network architecture, network management systems, and distributed computing systems. He also joined the projects of ITS (intelligent transport systems), development of cryptographic systems, and information security systems. His current interests are secure network systems, especially quantum computing systems, post quantum computing systems, and fiber optical network systems. He is a member of IEICE.



Tsunekazu Saito

Senior Research Engineer, NTT Social Informatics Laboratories.

He received a B.S. and M.S. from Waseda University, Tokyo, in 2006 and 2008 and Ph.D. in mathematics from Kyushu University, Fukuoka, in 2011. Since 2011, he has been engaged in research on elliptic curve cryptography and post-quantum cryptography at NTT.



Misato Nakabayashi

Information Security Technology Research Project, NTT Social Informatics Laboratories.

She received an M.Sc. from Tohoku University, Miyagi, in 2019 and joined NTT the same year. Her current research interest is in formal verification.

**Kazuki Yamamura**

Information Security Technology Research Project, NTT Social Informatics Laboratories.

He received an M.S. from Japan Advanced Institute of Science and Technology (JAIST), Ishikawa, in 2021. Since 2021, he has been engaged in research on cryptography at NTT.

**Katsuyuki Natsukawa**

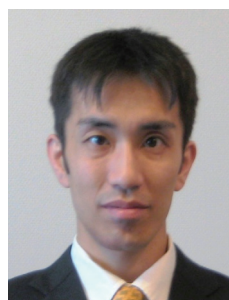
Executive Research Engineer, Supervisor, NTT Social Informatics Laboratories.

He received an M.E. from Nara Institute of Science and Technology in 1996. He joined NTT the same year and is currently conducting R&D on data protection technologies centered on cryptography.

**Yuri Tanaka**

NTT Social Informatics Laboratories.

She received a B.E. and M.E. from Keio University, Kanagawa, in 2019 and 2021. Since joining NTT Secure Platform Laboratories in 2020, she has been engaged in research on quantum security and computing. She is a member of the Physical Society of Japan.

**Koichi Takasugi**

Executive Research Engineer, Director, Head of Frontier Communication Laboratory, NTT Network Innovation Laboratories.

He received a B.E. in computer science from Tokyo Institute of Technology, M.E. from JAIST, and Ph.D. in engineering from Waseda University, Tokyo, in 1995, 1998, and 2004. He was involved in the design and standardization of the Next Generation Network architecture. He has implemented and installed super high-density Wi-Fi systems in several football stadiums. He was also active in the artificial intelligence field, such as diagnosing diabetes by machine learning. He is currently leading research on the network architecture and protocols in optical and wireless transport networks.

Cryptographic Circuit Technology Consisting of Optical Logic Gates

Junko Takahashi, Koji Chida, Kimihiro Yamakoshi, Shota Kita, and Akihiko Shinya

Abstract

With the progress in nanophotonics, miniature optical devices have been fabricated and the research and development of optical logic gates has become active. We are researching cryptographic circuits consisting of optical logic gates for use in data encryption and authentication in optical computing and optical information communications on the All-Photonics Network, a key element of the Innovative Optical and Wireless Network. In this article, we introduce methods of implementing cryptographic circuits using optical logic gates for the Advanced Encryption Standard, which is one of the de facto standard algorithms.

Keywords: All-Photonics Network, optical logic gate, cryptographic circuit

1. Optical computational operations on the All-Photonics Network information-processing platform

Targeting the All-Photonics Network (APN) information-processing platform, a key element of the Innovative Optical and Wireless Network (IOWN), we aim to achieve low-power, high-quality, large-capacity, and low-latency information processing by introducing optical technology from the communications network and communications platform up to terminal devices. While data processing on conventional network equipment and computational operations on terminal devices had been executed on electronic circuits, the use of optical technology in such equipment and devices on the APN information-processing platform should improve processing and operation performance. Optical circuits consisting of optical logic gates to enable logical operations constitute one example of optical technology. It has been shown, for example, that optical circuits can be used for the computational operations required by learning algorithms in the field of deep learning and that low-latency and low-power operations can be achieved [1].

2. Optical cryptographic circuit technology

On the APN information-processing platform, optical circuits will be used to achieve various types of dedicated hardware to improve computing performance. Therefore, optical circuits will also be used to implement dedicated cryptographic hardware required for ensuring the safety of this platform. It is also desirable for the circuits to be designed to suppress delay and power consumption so that cryptographic operations will not result in overall performance bottleneck. Taking this into account, we have been researching optical cryptographic circuits that can execute encryption and authentication operations by optical signals. In this section, we introduce methods for implementing the Advanced Encryption Standard (AES) by optical circuits.

2.1 AES encryption scheme

AES is a block cipher with a 128-bit block length. Key length may be selected from 128, 192, or 256 bits [2]. Here, 128 bits of intermediate values called a “state” are represented by a 4×4 matrix with each element consisting of 8 bits. Repeated application of a round function—the basic structure of encryption—to the state outputs the ciphertext. The round function

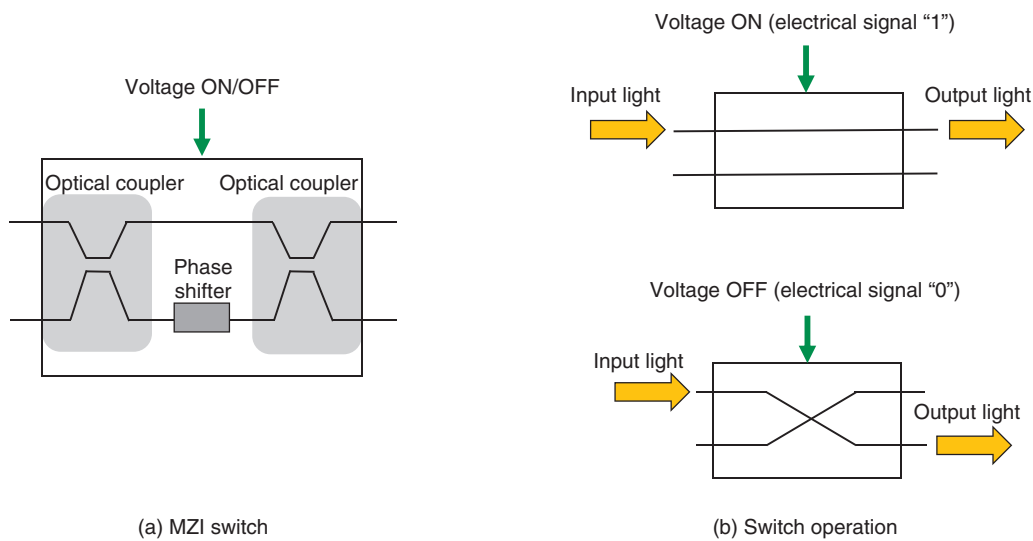


Fig. 1. MZI switch and its operation.

consists of SubBytes, which is a nonlinear operation, ShiftRows and MixColumns, which are linear operations, and AddRoundKey, which combines the state and key. This section focuses on SubBytes and MixColumns as the main operations of AES and introduces methods for achieving these operations by optical circuits.

2.2 Implementing SubBytes by optical logic gates

The SubBytes operation converts each byte to another byte on the basis of a substitution box (S-box) table determined from specifications. The S-box table is an 8-bit input/output nonlinear conversion. Given a set of 8 bits as input, the operation references the table to obtain an 8-bit output value. For example, the S-box output for an input value of 0xf0 would be 0x8c (input/output values are expressed in hexadecimal numbers).

This type of conversion based on a table can be implemented using a Mach-Zehnder interferometer optical switch (MZI switch), which is a type of optical logic gate. As shown in **Fig. 1(a)**, an MZI switch consists of optical couplers and a phase shifter. Applying a voltage to the path embedded in the phase shifter can change the refractive index of the optical waveguide, thus changing the phase difference between the two paths. This enables the MZI switch to operate as a switch that changes the optical pathway. In **Fig. 1(b)**, for example, when inputting light into the upper path and applying a voltage to the path embedded in the phase shifter (corresponding to elec-

trical signal "1"), the optical signal travels straight ahead resulting in output from the upper path. However, when not applying a voltage (corresponding to electrical signal "0"), the optical signal crosses over to the lower path resulting in output from that path.

We devised a method for implementing table conversion that outputs a 1-bit optical signal against 8 input bits. This is accomplished by interconnecting a number of MZI switches in accordance with the number of input bits in table conversion and switching paths (**Fig. 2**). In **Fig. 2**, the method prepares 256 ($= 2^8$) optical signals branched from a single optical source in which each optical signal is set to "light on" (corresponding to an optical signal of bit "1") or "light off" (corresponding to an optical signal of bit "0"). The method then passes light through the MZI switches while selecting paths in accordance with the 8-bit input (x_1, x_2, \dots, x_8) and finally selects and outputs one optical signal. This method achieves table conversion that outputs a 1-bit optical signal against an 8-bit input using MZI switches.

Interconnecting multiple MZI switches, as described above, and appropriately setting the 256 optical signals makes it possible to configure an S-box table. Input to the S-box table is set as MZI input (electrical signals) and output of the S-box table is set as an optical signal. For example, if the least significant bit of each of the 256 values of the S-box table is set as an optical signal, then the least significant bit of the S-box table output with respect to the 8-bit input (x_1, x_2, \dots, x_8) can be obtained. In the same

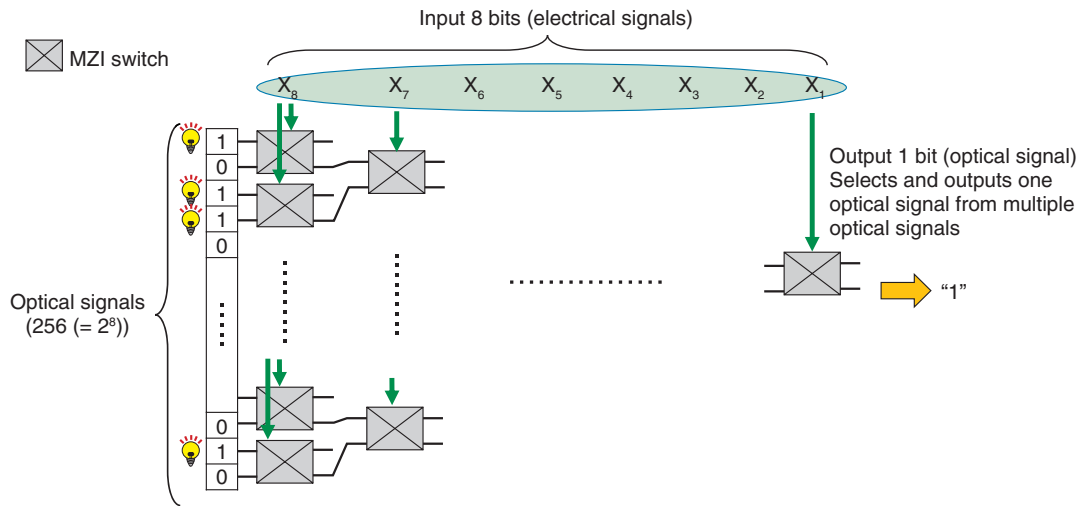


Fig. 2. Method of implementing table conversion using MZI switches.

(a)

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix}$$

(b)

$$Y_1 = \{02\} \cdot X_1 \oplus \{03\} \cdot X_2 \oplus X_3 \oplus X_4 \dots (1)$$

Legend:
 \oplus : Exclusive OR (XOR)
 \cdot : Multiplication

Fig. 3. Configuration of MixColumns in AES.

manner, if the n th bit ($n = 1, \dots, 7$) of each of the 256 values of the S-box table output is set as an optical signal, the n th bit of the S-box table output with respect to the 8-bit input can be obtained.

To obtain 8 bits of S-box table output, the above processing can be repeated 8 times by time division multiplexing or 8 instances of the circuit in Fig. 2 can be implemented in parallel. For optical signals, it is also possible to calculate 8 bits of S-box table output using only one instance of the circuit in Fig. 2 by multiplexing eight wavelengths and deriving the n th bit of the S-box table for each wavelength.

2.3 Implementing MixColumns by optical logic gates

As shown in Fig. 3(a), the MixColumns operation is defined as the multiplication of a fixed matrix and the state (where X and Y indicate 8-bit values). On calculating this matrix equation, each 8-bit output can be expressed using Eq. (1) shown in Fig. 3(b) (only Y_1 is shown in the figure). Furthermore, in carrying out these multiplications, Eq. (1) can be expressed as five 5-bit exclusive OR (XOR) operations (an XOR operation with 5 input bits and 1 output bit) and three 7-bit XOR operations (an XOR operation with 7

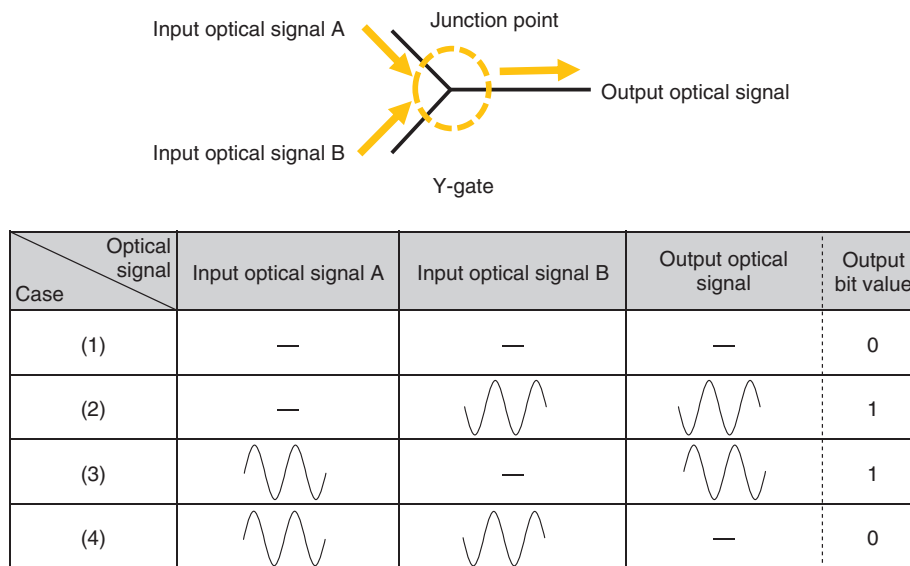


Fig. 4. XOR operation using a Y-gate.

input bits and 1 output bit) [2]. To give an example, we present a method for configuring a 7-bit XOR operation by optical logic gates. A 5-bit XOR operation can be configured in the same manner.

A Y-gate is an optical device that can execute an XOR operation [3]. A Y-gate superposes two input optical signals at a junction point where they meet. An XOR operation or OR operation can be achieved using the property that an optical signal is a “wave” having amplitude and phase, which results in operations approximately 300 times faster than those with electrical logic gates [3].

The principle of an XOR operation by a Y-gate is shown in **Fig. 4**. This Y-gate inputs two optical signals (input optical signal A and input optical signal B) of equivalent amplitude having a phase difference of 180° . In **Fig. 4**, “—” indicates a state in which the amplitude of the input optical signal is 0, that is, a state in which there is no input optical signal. These two optical signals are input into the Y-gate and the magnitude of the output optical signal is determined. In case (4) in **Fig. 4**, for example, the two input optical signals have equivalent amplitude but a phase difference of 180° with the result that the signals cancel each other out, making the amplitude of the output signal 0. Therefore, if we assign bit “0” to the state in which the amplitude is 0 and bit “1” to the state in which the magnitude of the amplitude is essentially the same as that of the input optical signal, an XOR logical operation can be executed, as shown

by the bit values of the output optical signal in the figure. In other words, an XOR operation can be achieved using a Y-gate by limiting the two input optical signals to a phase difference of 180° .

However, while executing a 7-bit XOR operation would involve the connecting of multiple Y-gates, taking the results of XOR operations as the input of the next XOR operation means that the phase difference of the two input optical signals of each Y-gate would not necessarily be 180° . (For example, when executing a 4-bit XOR operation ($a \oplus b \oplus c \oplus d$), the result of the XOR operation between a and b and that between c and d could both be the output of case (2), and those results would then be input to another XOR operation.) There is therefore a need for an operation that can change the phase difference of the two input optical signals to each Y-gate depending on operation results. Such an operation, however, would increase delay and power consumption.

To eliminate this need for converting phase during operations, we devised a method that operates on the input to a Y-gate as optical signals having the same phase and corrects the output result by threshold processing at the end of the operations. This method is outlined in **Fig. 5**. It consists of Y-gate superposition and threshold processing within an optical detector. Y-gate superposition adds up optical-signal amplitudes using a total of 7 Y-gates (since there are 7 input signals, the amplitude of the 8th input is taken to be “0” (light off)). Threshold processing, however, uses

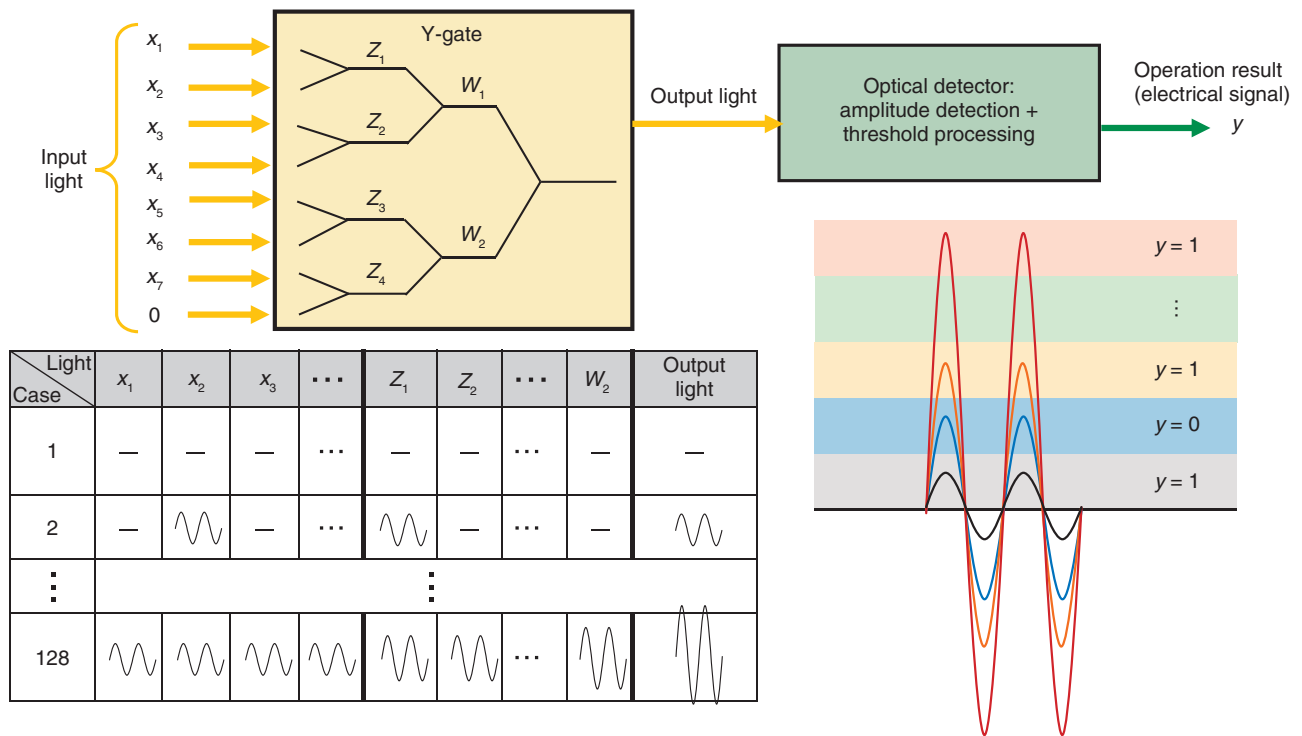


Fig. 5. Method for implementing a 7-bit-input/1-bit-output XOR operation.

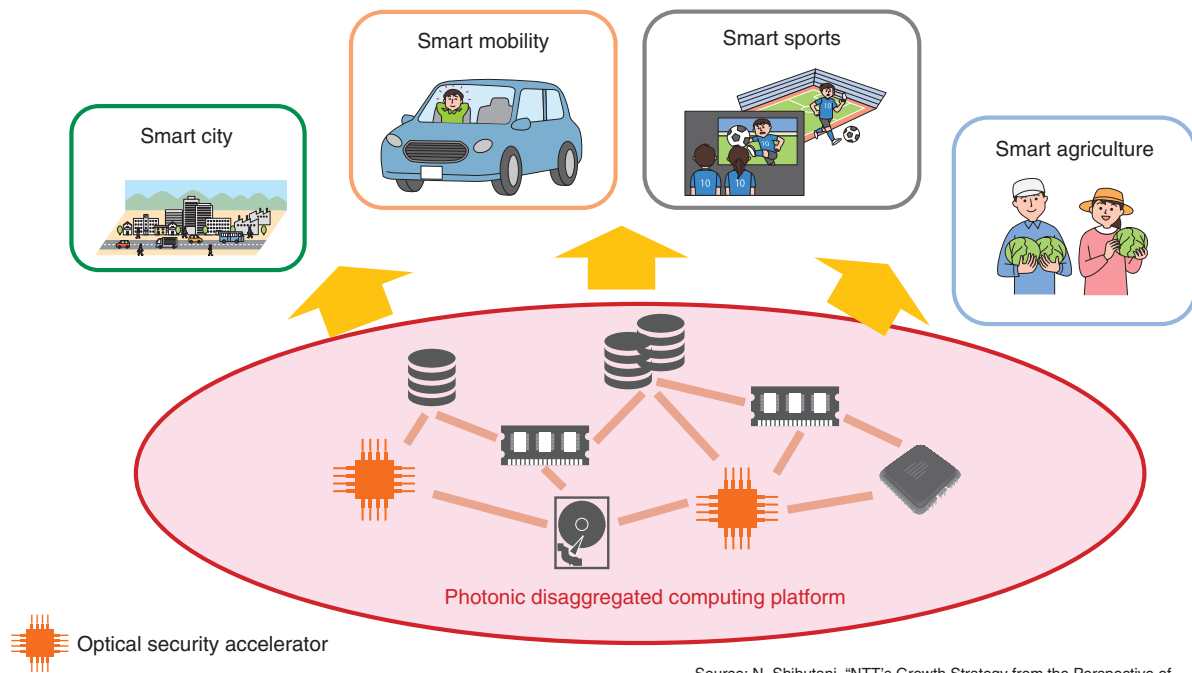
the fact that the greater the number of optical signals with non-zero amplitudes from among the input optical signals ($x_1, x_2, x_3, x_4, x_5, x_6, x_7$), the larger the amplitude of the output optical signal. It detects the magnitude of this amplitude to determine the output bit. On detecting no output signal (light off) or an amplitude that is an even multiple (2, 4, or 6 times as large) of the amplitude of the input signals, the output result is determined to be bit “0”, and on detecting an amplitude that is an odd multiple (1, 3, 5, or 7 times as large) of the amplitude of the input signals, the output result is determined to be bit “1”. This method enables XOR operations without having to convert the phase of input optical signals at every Y-gate operation. It also enables the processing of Y-gate output to be decreased from 7 times (the number of Y-gate outputs) to 1 time (only at the time of threshold processing).

If we let the 7-bit XOR and 5-bit XOR operations calculated from Eq. (1) in Fig. 3(b) correspond to the operation method shown in Fig. 5, one bit of Y_1 can be calculated. As with the SubBytes implementations, the calculation of Y_1 (8 bits) can be implemented by either of three methods: time division multiplexing, using multiple operation circuits, or multi-

plexing wavelengths in one operation circuit.

3. Future developments

We devised methods for implementing AES encryption circuits using optical logic gates. Going forward, ensuring safety on the APN information-processing platform will require an optical security accelerator that implements security technologies by optical circuits for logical operations, authentication, etc. through a variety of encryption schemes. This type of accelerator is considered a constituent of photonic disaggregated computing [4], a type of architecture supporting the APN information-processing platform shown in Fig. 6. The central processing unit, memory, and other types of devices had been confined to servers, but photonic disaggregated computing is a new architecture that can be treated as computers on a rack or a datacenter scale by connecting and distributing those devices over a high-speed optical network. An optical security accelerator will lead to a safe photonic disaggregated computing platform and the provision of safe smart services on that platform. To achieve a low-latency and low-power optical security accelerator, we will continue our



Source: N. Shibutani, "NTT's Growth Strategy from the Perspective of CTO," NTT IR DAY 2020 (2020).

Fig. 6. APN information-processing platform equipped with optical security accelerators.

research on new schemes for implementing encryption and authentication processes by taking advantage of optical characteristics. Therefore, we wish to contribute to the deployment of a safe IOWN.

References

[1] J. Peng, Y. Alkabani, S. Sun, V. J. Sorger, and T. El-Ghazawi, "DNNARA: A Deep Neural Network Accelerator using Residue," Arithmetic and Integrated, ICPP 20: 49th International Conference on

Parallel Processing - ICPP, No. 61, pp. 1–11, (2020).
 [2] National Institute of Standards and Technology (NIST), "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," Federal Information Processing Standards Publication 197, 2001.
 [3] S. Kita, K. Nozaki, K. Takata, A. Shinya, and M. Notomi, "Ultrashort Low-loss Ψ Gates for Linear Optical Logic on Si Photonics Platform," Commun. Phys., Vol. 3, Article number: 33, pp. 1–8, 2020.
 [4] A. Okada, S. Kihara, and Y. Okazaki, "Disaggregated Computing, the Basis of IOWN," NTT Technical Review, Vol. 19, No. 7, pp. 52–57, July 2021.
<https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202107fa7.html>



Junko Takahashi

Senior Researcher, Information Security Technology Research Project, NTT Social Informatics Laboratories.

She received a B.S. and M.S. in physics from Waseda University, Tokyo, in 2004 and 2006, and Ph.D. in engineering from the University of Electro-Communications, Tokyo, in 2012. She joined NTT Information Sharing Platform Laboratories in 2006. She has studied hardware security such as side-channel analysis and automotive security and has been studying security of optical circuits. She is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and Information Processing Society of Japan (IPSJ). She has been a member of technical committee on hardware security in the IEICE and special interest group on system architecture in the IPSJ. She was awarded the 2008 Symposium on Cryptography and Information Security (SCIS) paper prize, and her paper in Journal of Information Processing Vol. 25 was selected as a specially selected paper from the IPSJ in 2017. She also received best paper awards from international conferences such as the International Conference on Information and Communications Security (ICICS) 2020 and International Workshop on Security (IWSEC) 2020.



Koji Chida

Senior Research Engineer, Supervisor, Information Security Technology Research Project, NTT Social Informatics Laboratories.

He received a B.S., M.S., and Dr.Eng. from Waseda University, Tokyo, in 1998, 2000, and 2006. Since 2000, he has been engaged in research on cryptography and privacy-enhancing technologies at NTT. He is a member of IEICE and IPSJ. He received the IPSJ Best Paper Award in 2012.



Kimihiro Yamakoshi

Senior Research Engineer, Information Security Technology Research Project, NTT Social Informatics Laboratories.

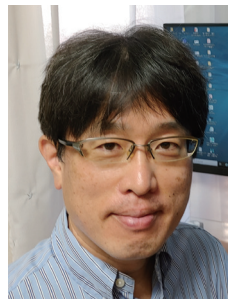
He received a B.E. in physics from Waseda University, Tokyo, in 1988 and M.E. in physics from Tokyo Institute of Technology in 1990. He joined NTT in 1990 and engaged in research and development (R&D) of LSI (large-scale integrated circuit) design and high-speed network switching systems. In 2004, he moved to NTT Cyber Communications Laboratory Group, where he researched IC-card security technology including measures against side-channel attacks. In 2007, he moved to NTT Microsystem Integration Laboratories and engaged in R&D of low-power wireless ubiquitous terminals. He is currently investigating an information security technology for IOWN.



Shota Kita

Senior Researcher, Photonic Nanostructure Research Group of NTT Basic Research Laboratories and NTT Nanophotonics Center.

He received a B.E., M.E., and Ph.D. in engineering from Yokohama National University in 2007, 2009, and 2012. He was a postdoc researcher in Loncar's group at Harvard University, USA, for 3 years. He returned to Japan and joined Notomi's group at NTT Basic Research Laboratories, where he is investigating nanophotonic devices and circuits. His interests are in silicon photonic-based nanofabrication and packaging technologies. He received the Poster Presentation Award at the International Nano-Optoelectronics Workshop (iNOW) 2009 and Young Scientist Presentation Award from the Japan Society of Applied Physics (JSAP) in 2010. He is a member of JSAP, IEICE, and Optical Society (OSA).



Akihiko Shinya

Group Leader, Senior Research Scientist, Supervisor, Photonic Nanostructure Research Group of NTT Basic Research Laboratories and NTT Nanophotonics Center.

He received a B.E., M.E., and Ph.D. in electrical engineering from Tokushima University in 1994, 1996, and 1999. In 1999, he joined NTT Basic Research Laboratories, where he has been engaged in R&D of photonic crystal devices. He is a member of JSAP and the Laser Society of Japan.

Trusted Data Space for Creating Value from Data in a Chain Reaction Manner

Tomoaki Washio, Hiroki Itoh, Koki Mitani, Gembu Morohashi, Kenji Umakoshi, Tetsuya Okuda, Kazuyuki Takaya, Kei Ohmura, and Gen Takahashi

Abstract

The Smart World holds the possibility of maximizing the value of data throughout society by enabling diverse organizations to bring each other data for analysis and create data for new purposes in a chain reaction manner beyond the walls of companies and industries. In reality, however, the use of data among organizations goes no further than the provision of limited data to limited parties, which prevents a value chain from being achieved. This article introduces a new mechanism for data sharing called “trusted data space” as an initiative to solve this problem and describes key technologies for making it a reality.

Keywords: security, data sharing and utilization, data space

1. Smart World enabling data sharing across industries

There has been much activity in the research and development of technology for not only reproducing real-world systems such as manufacturing lines and chemical plants in cyberspace to analyze and predict system operations but also for data sharing and analysis beyond individual organizations, business fields, and industries.

In a smart city, for example, a massive amount of output from sensors, video cameras, etc. installed in physical space can be converted to data so that the movements of people and things can be analyzed in cyberspace in a cross-sectoral fashion. The results of this analysis could then be used as a basis for directing the behavior of people and things in the city, that is, in the physical space. The Smart World that fuses physical space and cyberspace in such an advanced manner is fast approaching.

In the Smart World, data will be continuously generated from a variety of individuals and companies on

a global scale at a level of quality and volume not seen before. There will therefore be a need for a mechanism that can effectively use this massive amount of diverse data. In particular, there is a need for a data marketplace in which everyone can bring each other data for analysis and generate data for new purposes in a chain reaction manner beyond the walls of companies and industries. This would have the effect of uncovering value from each other’s data and maximizing the value of data throughout society. This mechanism is called “trusted data space” (hereafter, data space).

Both providers and users participate in a data space. The data in a data space, while placed under the management of the providers, can be used virtually in the manner of one massive data lake and searched through freely. The providers present terms of data use (period of use, allowed processing, secondary use conditions, etc.), while the users can use the data within the allowed range after agreeing with those terms. This type of mechanism enables data collected for a certain purpose to be used for a new purpose,

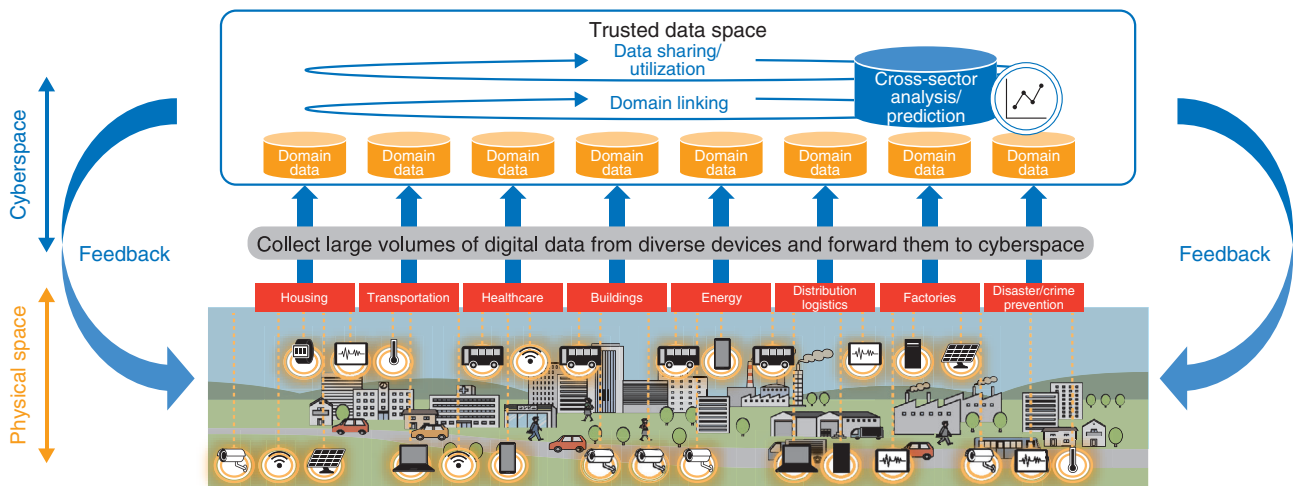


Fig. 1. Smart World and trusted data space.

which points to the possibility of generating data with new value from existing data in a chain reaction manner. For example, marketing data collected through the cooperation of amusement facilities, transportation operators, and eating and drinking establishments for making user recommendations on personal behavior on a certain day could also be used by local governments for various purposes such as disaster and crime prevention, promoting the health of its residents, and urban development. In short, things that could not be achieved by a particular business entity alone would become possible (Fig. 1).

1.1 Issues with cross-organizational use of data

Despite heightened expectations for such a society, the social adoption of data sharing and analysis technology remains at the level of local value discovery. Data collected by an organization is generally used only for the purpose for which the data were collected by the collecting company, while the use of data among organizations stops at the provision of limited data to limited parties, preventing the creation of a value chain. We call this the “data sharing wall.”

Overcoming the data sharing wall requires technology for resolving three types of issues: issues in discovering an appropriate data provider and optimal data, issues in forming an agreement on data use, and issues in sharing and using data on the basis of that agreement (Table 1).

By providing technology for resolving these issues, we should be able to achieve a form of data sharing that creates new value in a chain reaction manner

while also maximizing the value of data throughout society.

2. Trends in data sharing throughout the world

In Europe, data sharing is being revitalized with a focus on the manufacturing industry. Typical of this movement is the Gaia-X [1] project that aims to establish a data-sharing infrastructure for Europe. The Gaia-X vision of supporting data sharing and use on a European scale was announced on October 29, 2019 by the German and French governments. This was followed by the founding of the Gaia-X AISBL non-profit organization for achieving this vision in January 2021. The plan is to construct an infrastructure that can provide a technical mechanism for ensuring interoperability with diverse cloud services while controlling data access based on rules and agreements and protecting data sovereignty*. In Japan, the Data Society Alliance was founded on April 1, 2021 in the wake of this movement with the aim of constructing a platform called DATA-EX [2] to facilitate data linking across diverse fields. A number of projects have been established as data sharing initiatives using Gaia-X with the aim of constructing data-sharing infrastructures composed of companies in a trustworthy relationship such as a supply chain. In Germany, for example, there is Mobility Data Space for achieving Mobility as a Service (MaaS) and

* Data sovereignty: The right of a data provider to determine the range of data disclosure, usage applications, etc.

Table 1. Issues with cross-organizational data sharing.

Issues in discovering appropriate data providers and optimal data	<ul style="list-style-type: none"> • Prevent data giving/receiving among undesirable parties • Enable data users to discover data applicable to their conditions
Issues in forming an agreement	Form an agreement between the data provider and data user on data-processing conditions and process the data on the basis of those conditions
Issues in sharing and using data on the basis of the agreement formed	Enable the data possessed by a provider to be processed and provided to data users without disclosing the data and processing method to the other party

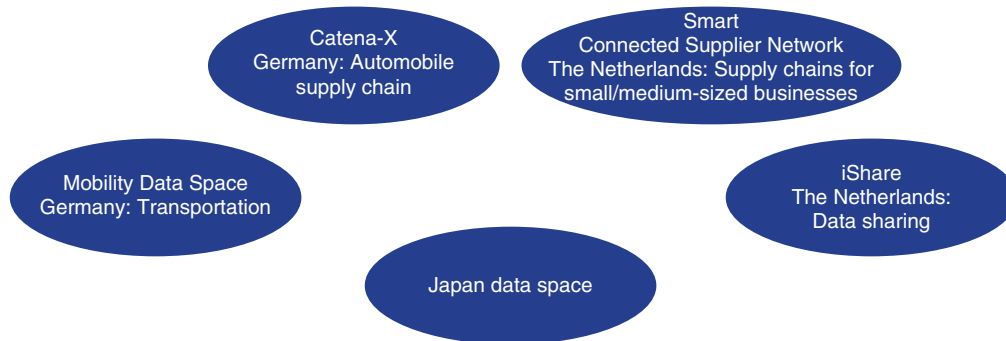


Fig. 2. Data sharing platform beyond industry walls.

Catena-X for achieving an automobile manufacturing supply chain, while in The Netherlands, there is the Smart Connected Supplier Network (SCSN) for small/medium-sized businesses in the manufacturing industry. Catena-X and SCSN plan to build data sharing infrastructures on a scale of 1000 and 3000 companies, respectively, by 2022.

The construction of data-sharing infrastructures across industries has already begun. However, this process is still at the stage of setting up rules centered about Gaia-X; as a result, data sharing has been limited to companies that are already in a trustworthy relationship. In addition, major issues are expected to arise from here on in terms of providing security to protect data from cyber attacks and providing protection of data sovereignty that enables data sharing while protecting the rights of data providers. The questions to be answered are what technologies should be implemented to achieve these goals and how should such a system be constructed as a social infrastructure (Fig. 2).

3. Technology for configuring a data space

The following three mechanisms must be considered to resolve the issues described in Section 1.

- (1) Mechanism for discovering data, applications,

and business partners that can be trusted: Catalog data/applications and business partners and visualize information on their reliability to gauge their appropriateness. Match up with business partners that can be trusted on the basis of this visualized information.

- (2) Mechanism for forming an agreement on data processing conditions: Form an agreement between the data provider and data user on data-processing conditions, disclosure conditions, and processing methods on the basis of cataloged information. Determine whether a certain type of data processing can proceed according to the content of that agreement.
- (3) Mechanism for processing data based on an agreement: The data provider manages the data on its own and virtually shares and integrates the data only when necessary. The data user executes various types of analysis and processing deemed necessary while keeping secret not only the data but the data-processing methods as well.

Current data processing executes risk management on the basis of contracts such as non-disclosure agreements (NDAs) and operation management policies, but there is a need for corroboration based on technology, as in mechanism (3). To execute transactions

with unknown parties with which no business relationship has been established and create value in a chain reaction manner, there is a need for forming an agreement on data-processing conditions, as in mechanism (2). Finally, there is also a need for discovering partners, data, and applications that can be trusted, as in mechanism (1).

We introduce a data-processing mechanism based on an agreement centered about a data space. This mechanism gathers and virtually integrates data dispersed among organizations and individuals in an encrypted state through the use of a virtual data lake and processes that data while they are encrypted by using either of two methods: data sandbox or secure computation. We also introduce our forward-looking work on an agreement-forming mechanism for data-processing conditions.

3.1 Virtual data lake

When sharing one's data with another party, only the minimum required amount of data must be provided, and information protection and management must be executed according to data usage conditions established beforehand. A virtual data lake is achieved through technology that virtually integrates data under different management entities scattered over a wide area while maintaining the governance of each management entity and that transfers only a minimum amount of data on the basis of the requirements of the data user. On top of this, a virtual data lake includes mechanisms for quickly informing the data user that data generation has begun and for allowing the data user to begin using a portion of that data before data generation is fully completed. This makes it possible to use even a large amount of data at an early stage as needed and accelerate data sharing.

For example, a company that is generating data could simultaneously generate and update data management information (metadata such as a data catalog and control policies) and notify the platform of such. The platform, in turn, could appropriately control the sharing of that data by informing approved users of the existence of that data and transmit to them that portion of the data deemed necessary on the basis of data management information. In addition, users would be able to find desirable data with good efficiency by referring to a virtually integrated list of data and begin using those data at an early stage. These mechanisms enable safe and convenient use of data beyond individual organizations.

3.2 Data sandbox technology

Data sandbox technology brings together an organization that possesses data but no analytical technology and that has no desire to share that data with another company and an organization that possesses analytics technology but has no desire to share that technology. Therefore, analysis results can be obtained without these organizations having to share data and analytics technology with each other.

If a data owner and analytics technology owner were to reach an agreement on the use of a data sandbox, a dedicated data sandbox that includes data and analytics technology could then be created on the basis of that agreement. A data sandbox blocks communications with the outside and encrypts internal communications, storage, and memory so that even the data sandbox provider cannot decrypt that content. In short, data can be analyzed without anyone including the data owner, analytics technology owner, and data sandbox provider accessing decrypted data or analytics technology.

The data sandbox saves the results of analysis in a location that can be viewed by the data owner and/or analytics technology owner on the basis of the agreement reached between those two parties. First, the case in which the data owner may view the results of analysis means that the data owner can access analysis results without having to share data with another party and that the analytics technology owner can be compensated for the use of its data analysis technology by the other party without having to share algorithms with another party, all through the use of a data sandbox. Next, the case in which the analytics technology owner may view the results of analysis means that the data owner can be compensated for the use of its data for analysis by the other party without having to share data with another party and that the analytics technology owner can access analysis results using another party's data that it does not possess without having to share analytics technology with another party, all through the use of a data sandbox.

3.3 Secure computation

Secure computation is an advanced encryption technology that can process data while they are encrypted without returning to the original data even once. In 2019, NTT developed secure computation deep learning to provide security and privacy measures for data used in artificial intelligence (AI). This technology executes deep-learning training and prediction while keeping the target data encrypted without returning to the original data even once. Since the

conventional technology had performance issues, this technology became an alternative using processing that was even simpler than that of ordinary (unencrypted) deep learning training and prediction. NTT's secure computation deep learning uses world-class secure computation-processing performance and reproduces the training process using standard optimized processing executed in deep learning as a world's first by secure computation.

In other words, all the steps required for data usage in deep learning, that is, (1) data provision, (2) data storage, (3) training, and (4) prediction, can be executed in an encrypted state. Since data are always kept in an encrypted state without returning to their original form even once, this technology enables users and organizations to provide data with peace of mind compared with conventional technology. This should lead to an increase in the amount and types of data that can be used for training. It is exactly this expansion of data that should enable AI to achieve even more accurate and advanced analysis.

3.4 Agreement-forming mechanism

In the use of data, there are two conditions under which the provider approves of data usage and requirements that the user demands of that data. The content of those conditions and requirements differ depending on the provider and user. The provider may specify as conditions under which parties are permitted to use the data, the purpose of use, the range of use, the period of use, etc. The user, on the other hand, may specify as requirements the target data, purpose of use, desired processing, etc.

To enable data usage in a form that both sides agree upon, there is a need for a mechanism that can com-

pare data conditions and requirements of data usage between the provider and user then form an agreement.

It has been common for a provider and user to express provision conditions and usage conditions, respectively, in the form of policies, which would then be checked manually by each other to form an agreement. In the future, however, we can consider an approach in which the content of a user request for data usage is compared with those policies at the time of that request to automatically determine whether the agreement is being satisfied. If differences exist between requirements and conditions, the ability to dynamically adjust those requirements and conditions between the provider and user would enable more flexible agreement formation. This kind of approach must also be targeted for future study to promote the use of data among companies and organizations.

4. Toward the future

The creation of a data space should accelerate the sharing of data beyond corporate and industry walls, which has been difficult, and enable data sharing that creates new value in a chain reaction manner. To make the data space a reality, we plan to research and develop key technologies while accelerating the testing of those technologies with partners.

References

- [1] Gaia-X, <https://www.gaia-x.eu/>
- [2] DATA-EX, <https://data-society-alliance.org/about/vision-mission/#top>



Tomoaki Washio

Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

He received a B.E. and M.E. in systems and information engineering from Hokkaido University in 2000 and 2002. Since joining NTT in 2002, he has been engaged in research and development (R&D) of authentication systems and secure data sharing technologies.



Hiroki Itoh

Senior Research Engineer, Social Innovation Research Project, NTT Social Informatics Laboratories.

He received a B.S. from Tokyo University of Science in 2002, M.E. from Tokyo Institute of Technology in 2004, and M.S. in management of technology from Tokyo University of Science in 2009. He is engaged in leading practical application of research outcomes from NTT Social Informatics Laboratories.



Koki Mitani

Senior Research Engineer, NTT Social Informatics Laboratories.

He received a B.E. in information and computer science and M.Sc. in engineering in science for open and environmental systems from Keio University, Kanagawa, in 2003 and 2005. In 2005 he joined NTT. From 2011 to 2015, he was a product manager of global network services in NTT Europe Ltd. and NTT Communications Corporation. He returned to NTT in 2015, where he currently leads open and collaborative innovation for building global infrastructure for data sharing across businesses at NTT Social Informatics Laboratories.



Kazuyuki Takaya

Senior Research Engineer, Supervisor of Data Sharing Infrastructure Project, NTT Software Innovation Center.

He received an M.E. from Waseda University, Tokyo, and joined NTT in 2000. He is engaged in R&D of technologies and platforms for data sharing.



Gembu Morohashi

Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

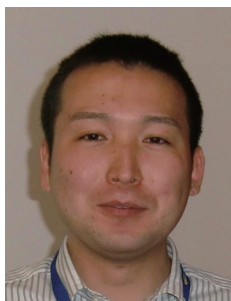
He received a B.S., M.S., and Ph.D. from the University of Electro-Communications, Tokyo, in 2001, 2003 and 2009. He began working at NTT in 2003, and his main research interests are cryptography and information security.



Kei Ohmura

Senior Research Engineer, Data Sharing Infrastructure Project, NTT Software Innovation Center.

He received an M.E. from Waseda University, Tokyo, in 2009. Since joining NTT the same year, he has been engaged in developing platforms for cloud, Internet of Things, and AI leveraging open source software.



Kenji Umakoshi

Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

He received an M.E. from Waseda University, Tokyo, in 2009. He joined NTT in 2009 and has been researching and developing in areas such as ubiquitous/Internet of Things computing, smart room/factory, and data sharing platform. He also worked as a product manager of a cloud service in NTT Communications Corporation from 2014 to 2016.



Gen Takahashi

Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

He received a Master of Media and Governance from Keio University, Tokyo, in 2005 and joined NTT in 2006. His research interests include information security and cryptographic engineering.



Tetsuya Okuda

Research Engineer, NTT Social Informatics Laboratories.

He received a B.S. and M.S. from the University of Tokyo in 2009 and 2011. Since 2011, he has been engaged in R&D on security protocol at NTT. He is a member of the Information Processing Society of Japan (IPSJ) and received the IPSJ/Computer Security Symposium Student Paper Award in 2019.

Initiatives toward a New Way of Experiencing and Supporting the Torch Relay

Shingo Kinoshita

Keywords: Olympic and Paralympic Games, Torch Relay, ultra-realistic communication technology Kirari!

1. Tokyo 2020 Olympic Torch Relay

The Tokyo 2020 Olympic Torch Relay, which started in Fukushima Prefecture on March 25, 2021, was supported by 10,515 torchbearers over 121 days through all 47 prefectures in Japan. The purpose of the Torch Relay is to embody the Olympic ideals of peace, unity, and fraternity by connecting the entire host country with the torch, which is the symbol of the Olympic Games, and build momentum for the upcoming Games throughout the country.

NTT believes in the purpose of the Torch Relay and initiated various support activities to help spread this light of hope throughout Japan. We were involved in four activities: (i) supporting the torchbearers, (ii) supporting celebration events, (iii) supporting expanded versions of the celebration events, and (iv) hosting regional torch-relay events.

- (i) The first activity (torchbearer support) involved recruiting and recommending torchbearers and providing various types of support for the selected torchbearers and cheering them on during the relay run.
- (ii) The second activity (celebration events), which was held at the points where the torchbearers finished each day, involved cheering on the torchbearers from a stage and holding exhibitions such as a commemorative photography of a Torch Relay torch.
- (iii) The third activity (expanded celebration events) involved expanded versions of the second activity and large-scale events such as live performances and exhibitions. We origi-

nally planned to hold such events with an audience of 5000 people in Osaka on April 13 and in Yokohama on June 30.

- (iv) The fourth activity (NTT event) involved designating business sites as the Torch Relay route and holding events through which neighbors, students, employees working on site, and others could experience the Torch Relay together. NTT research and development (R&D) laboratories organized one such event at the NTT Yokosuka R&D Center, which invited elementary and high-school students from around the neighborhood.

Due to the spread of novel coronavirus (COVID-19), the Torch Relay was postponed for one year. After the postponement, it was still affected by the pandemic in various ways. At the beginning of the Torch Relay, many torchbearers ran on public roads; however, as the pandemic worsened, more and more local governments decided to take the Torch Relay off public roads, eleven prefectures took it off public roads altogether and nine prefectures took it off certain public roads. Accordingly, most of the celebration events were restricted or even cancelled. The expanded celebration event scheduled to be held in Osaka was streamed online instead of being attended on site by the general public. The expanded celebration event scheduled to be held in Yokohama was also streamed online and closed to the general public, and only torchbearers and their families and friends were allowed to watch on site. A number of regional torch-relay events—as well as events organized by NTT—were also cancelled.



Fig. 1. Virtual torch kiss experience with Kei Nishikori using Kirari!.

Unfortunately, the festive momentum that was initially expected did not fully develop; regardless, NTT continued its support because it felt the need to use the power of communication to protect communication between people and spread the light of hope throughout Japan.

2. A new form of experiencing and supporting the Torch Relay by NTT R&D

NTT R&D has been researching and developing communication technologies and experimentally applying them to various fields to explore new forms of entertainment and art that connect people and enable amplification and sharing of emotions through communication. We have been engaged in ultra-realistic stage production and live transmission of *kabuki*, music concerts, fashion shows, sports, and other events by using our ultra-realistic communication technology called Kirari!, spatial-image production based on moving display bots using robot- and video-communication control technology, and other art exhibitions.

For the Tokyo 2020 Olympic Torch Relay, we used these communication technologies and expertise to help make the Torch Relay more exciting. Using the latest communication technologies, such as Kirari! and the communication control technology called “Swarm,” we could support the above-mentioned

events.

3. Commemorative photo of the Torch Relay torch

At the celebration and the expanded celebration events, we hosted a booth at which visitors could take commemorative photos of the Torch Relay torch by using communication technology. The best user experience for visitors was to actually hold the torch in their hands, appreciate its beauty and weight, and feel as if they were torchbearers. We further enhanced that experience by applying communication technology in the following exhibits.

The first was the Virtual Torch Kiss, Torch Relay Commemorative Photo Corner: Kirari! Version. In this experience, the participant was able to share a “virtual torch kiss” with the professional tennis player Kei Nishikori displayed as a holographic image (**Fig. 1**).

The second was the Torch Relay Commemorative Photo Corner: Optical Illusion Version. In this experience, projecting light triggered optical illusions that created a mysterious “trick space” in which the still pictures on panels appeared to move.

The third was the Torch Relay Commemorative Photo Corner: Kabuki Version. This was an interactive-experience exhibit that combined NTT’s communication technologies. When participants held a

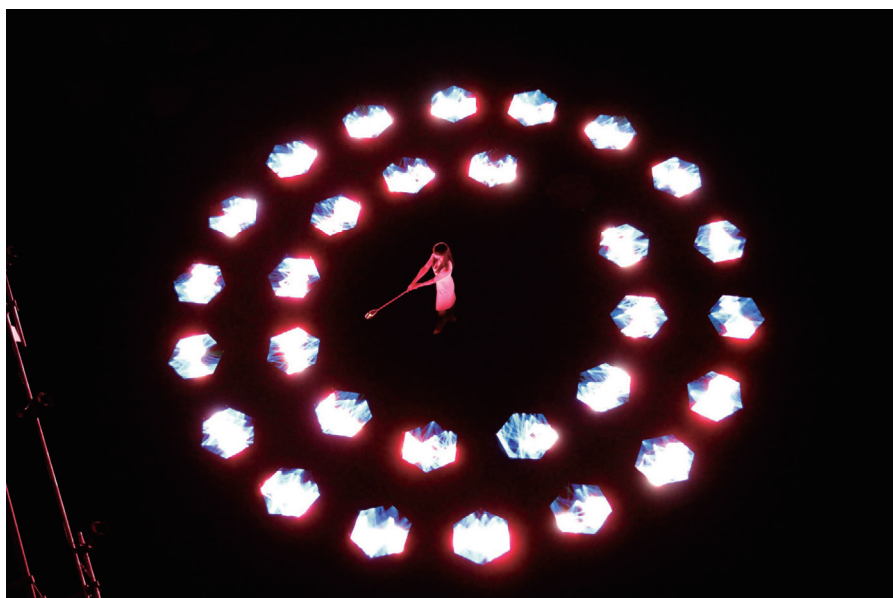


Fig. 2. Spatial production to cheer on the torchbearers via display bots.

kabuki mask in front of their faces for a few seconds, their faces appeared on a monitor in *kabuki* makeup and they could have a commemorative photo taken while holding up a torch.

4. Spatial production to support torchbearers

Communication technology was used to coordinate countless moving displays (display bots) and create a space from which to cheer on the torchbearers while the road surface was being decorated with images (Fig. 2). The magical expressions created by the multiple display bots by approaching or moving away from each other, displaying images individually or as a group, and so on gave the feeling that they were a swarm of living creatures. This spatial production was the result of joint research by NTT and Ars Electronica, a world-renowned media art research institute.

5. Stage production for celebrating the Torch Relay

Kirari! was used for a stage production called “GENERATIONS from EXILE TRIBE” in the expanded celebration events held in Osaka and Yokohama. We attempted to overcome and improve the circumstances that made it difficult to bring people together due to the COVID-19 pandemic through the

power of communication.

The first part of this production was “remote collaboration” (Fig. 3). It had become difficult for artists to get together due to the COVID-19 pandemic. Artists from different locations tried to create a group dance in tune with the song “Choo Choo TRAIN” by EXILE. Images of artists dancing separately were instantly cropped by Kirari! to create a composite image that gave the impression that the artists were dancing together in the same place.

The second part of the production was “remote live viewing” (Fig. 4). This viewing experience created the impression of the artist being teleported in front of the viewer even though the viewer could not go to the live venue due to the pandemic.

The third part of the production was “remote fan interaction” (Fig. 5). Due to the pandemic, it had become difficult for artists to interact with their fans. Therefore, we created an experience that made the fans feel like they were standing next to the artist while sharing the same space.

6. Regional torch-relay events

We had initially planned to invite local elementary school students to the NTT Yokosuka R&D Center to participate in the torch-relay event. As a new means of cheering during the pandemic, each student made a device for “paper-cup communication” that would



Fig. 3. Stage production using Kirari! (remote collaboration).



Fig. 4. Stage production using Kirari! (remote live viewing).

let them cheer while preventing droplets spraying from their mouths when they shouted (**Fig. 6**). This event was cancelled because of the increase in COVID-19 cases; nevertheless, to give the students (who were looking forward to the event) memories of the Torch Relay, we went to the school and held a

cheering event using paper cups, holding a torch commemorative photo shoot by the students, and presenting a technical lecture by researchers, all of which the students enjoyed.



Fig. 5. Stage production using Kirari! (remote fan interaction).



Fig. 6. Cheering on the torchbearers by using paper-cup communication devices made by the students.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

**Shingo Kinoshita**

Vice President, Head of NTT Human Informatics Laboratories.

He received a B.E. from Osaka University in 1991 and M.Sc. with Distinction in technology management from University College London, UK, in 2007. He joined NTT in 1991 and was a senior manager of the R&D planning section of the NTT holding company from 2012 to 2015. He is currently a visiting professor at the Art Science Department, Osaka University of Arts, and visiting executive researcher at Dentsu Lab Tokyo. He has served as a member of the Japan Science and Technology Agency (JST) JST-Mirai Program Steering Committee, member of the All Japan Confederation of Creativity (ACC) TOKYO CREATIVITY AWARDS 2021 Judging Committee, and member of the Broadband Wireless Forum Steering Committee. He has been engaged in R&D of a media-processing technology, user interface/user experience, communication protocols, information security, machine learning, service design, and technology management. Until recently, he had been in charge of NTT's Tokyo2020 initiatives, including sports-watching video technology, inclusive design for social issues, and promoting the use of ICT in *kabuki*, entertainment, and media arts such as live music.

He has been in his current position since 2021, where he manages R&D on information and communication processing of humans based on human-centered principles.

Torch Relay Commemorative Photography × Ultra-realistic Communication Technology Kirari!

Yoshiyuki Mihara, Masami Nagata, Keisuke Hasegawa, Taiji Nakamura, Junji Watanabe, Tatsuya Matsui, Hideaki Iwamoto, and Shingo Kinoshita

Keywords: Olympic and Paralympic Games, Torch Relay, ultra-realistic communication technology Kirari!

1. Overview

To foster the momentum of the Olympic Games Tokyo 2020, we wanted as many people as possible to experience the Olympic Torch Relay. We therefore created three experiential exhibits that enabled participants to take commemorative photos with a torch as a personal experience of the Olympic Torch Relay. The first exhibit was the Virtual Torch Kiss, Torch Relay Commemorative Photo Corner: Kirari! Version, where participants could carry an actual torch and virtually experience a torch kiss using the Kirari! ultra-realistic communication technology. Kirari!, which conventionally needs to be set up in a laboratory and include large devices, was packaged into a truck, making it possible to hold the exhibit anywhere around the country. The second exhibit was the Torch Relay Commemorative Photo Corner: Optical Illusion Version. By projecting a special light that elicits phantasmagoric optical illusion onto a still image, we created the mysterious effect of making a supposedly unmoving image of a flame appear to move. Unlike shooting in front of a regular panel, it was possible to provide a more dynamic experience despite using still images. The third exhibit was the Torch Relay Commemorative Photo Corner: Kabuki Version. This exhibit combined *kabuki*, which has a long history in Japan, and the Olympic Torch Relay, which connected the regions of Japan, by enabling participants

to take a commemorative photo with a torch while having *kabuki* makeup virtually applied to their faces.

2. Torch Relay Commemorative Photo Corner: Kirari! Version

We modified a truck that enabled participants to do a virtual torch kiss with the professional tennis player Kei Nishikori, who was holographically projected using Kirari! inside the truck (**Fig. 1**). The holographic display was based on a two-dimensional (2D) aerial image display [1]. We set up the display on the floor of the truck and mounted a transparent screen at a 45-degree angle from the display. The image of Kei Nishikori shown on the display was reflected and transmitted to the transparent screen, making it appear as if he were standing on the stage.

Setting up the stage for this purpose usually requires time for installing truss parts and setting the transparent screen diagonally. For this celebration event, since we had to move and install the transparent screen on the truck every day, we implemented a structure that made it easy to store and install the transparent screen. Thus, we were able to complete the stage setup, which would usually take a day, in only about two hours. Because also we had to travel throughout the country for 121 days, we needed to display the exhibit in a bright environment during the day, depending on the actual venue and the time of



Fig. 1. Kirari! truck exterior view.



Fig. 2. Torch Relay Commemorative Photo Corner: Kirari! Version experience.

the event. Therefore, we used a light-emitting diode (LED) panel instead of a projector to improve the brightness of the original image and enhance outdoor visibility. We installed these pieces of equipment on the loading deck of a 10-ton truck.

2.1 Flow of experience

Participants first climbed onto the stage on the truck's loading deck from the rear entrance of the vehicle and received a torch from the staff. We also

installed a lift to enable wheelchair users to experience the exhibit.

Once the participant bearing the torch was in the proper position, a holographic image of Kei Nishikori appeared on the stage in such a way that the virtual Kei Nishikori and real-life participant appear to be standing side-by-side (Fig. 2). We prepared two patterns for displaying the holographic image of Kei Nishikori: one where he was standing up and one where he was kneeling. This made it possible for

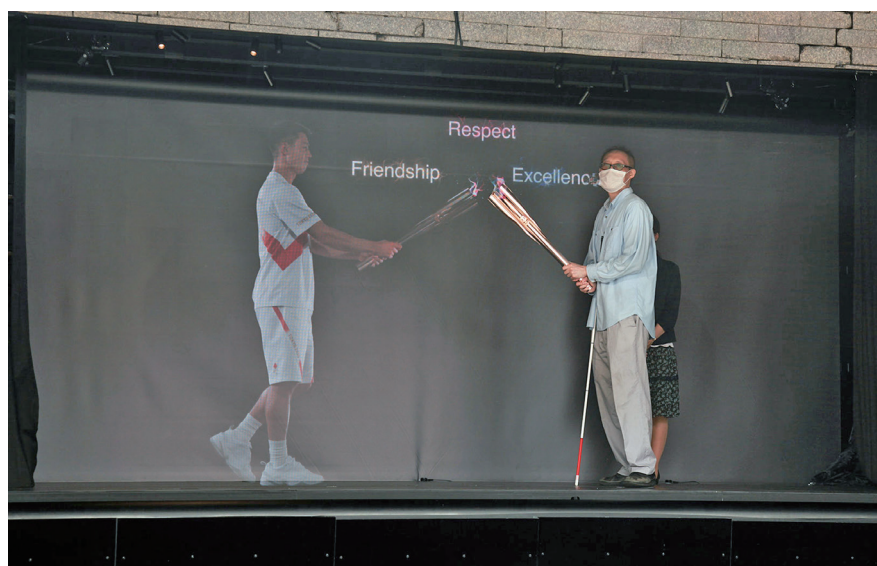


Fig. 3. Visually impaired person trying the virtual torch kiss experience.

participants to make a torch kiss regardless of their height.

Since participants could not see Kei Nishikori directly on the transparent screen, we prepared a separate monitor through which the participants could view the movement of Kei Nishikori's torch as they moved their torch toward his torch and do a virtual torch kiss. The torch carried by the participant was equipped with an infrared sensor to detect its position. As the participant's torch approached Kei Nishikori's, its tip lit up with an image of the Olympic flame.

The experience was captured using a camera installed off stage, and the video was instantly uploaded to an Internet server. We provided a means for issuing a 2D code of the video's URL (uniform resource locator) to the participant after the experience so that they could immediately view the recorded video on their smartphone and post it on social networking services (SNS).

2.2 Results

The novel coronavirus (COVID-19) continued to spread during the Olympic Torch Relay period, and many municipalities canceled local torch relay celebration events, so the number of exhibitions was less than originally planned. We were able to hold the torch commemorative photo corner using the Kirari! truck at 34 venues in 25 prefectures, enabling a total of 4498 people to experience the exhibit. Many peo-

ple were surprised at the realness of the life-size holographic image of Kei Nishikori appearing on stage, with many participants saying that they were able to gain a realistic experience of being an Olympic torchbearer.

To improve the realness of the Torch Relay experience, we added a function to simulate the tactile sensation of the fire being lit. This allowed people with visual impairments to also enjoy the experience (Fig. 3). Since the torch kiss experience with Kei Nishikori's holographic image was visual based, visually impaired individuals had no way of knowing when and how it was done. Therefore, by adding a function that vibrated the torch simultaneously with the torch kiss, we were able to deliver a haptic experience for the passing of the flame from Kei Nishikori's torch to the participant's.

This was done by attaching a small vibration device, which can be switched on and off by an external infrared signal, to the torch, and having a staff member turn the vibration on and off in accordance with the timing of the torch kiss for visually impaired individuals. We also designed the vibration to make it easier for visually impaired individuals to sense flames. This experience was provided only at one venue (Yokohama, June 30, 2021). A visually impaired person who experienced it commented that "Although the vibration was weak immediately after being lit, it gradually became stronger as I raised the torch above me, so I was impressed by the effort put



Fig. 4. Torch Relay Commemorative Photo Corner: Optical Illusion Version experience.

into making it possible to feel even the changing intensity of the fire.”

3. Torch Relay Commemorative Photo Corner: Optical Illusion Version

In this exhibit, a special light was projected onto a panel showing an image of Kei Nishikori bearing a torch to trigger the illusion that the flames on the panel and the flurry of cherry blossoms in the background are moving (Fig. 4). Position matching was important for this exhibit because light was applied on the feature points on the panel. To accurately carry out alignment at each venue, we accurately projected the light to a specific location on the panel by linking the projector with the camera. This made it possible for the local staff to easily set up the exhibit.

A total of 5616 people in 3373 groups experienced this exhibit. All participants were surprised at the movement of still images that were not supposed to move.

4. Torch Relay Commemorative Photo Corner: Kabuki Version

NTT began its initiatives to create new experiences by combining traditional culture with information and communication technology (ICT) in 2016. As part of these initiatives, we have been focusing on

kumadori, the distinctive *kabuki* style of makeup, and created the unusual experience of having your chosen *kumadori* mask virtually adhere to your face using ICT. Packaging this experience exhibit in a container, we have traveled to Fukushima and Kumamoto prefectures to provide a fun experience through ICT. Building on these initiatives, we provided the Torch Relay Commemorative Photo Corner: Kabuki Version as an experience with the theme of “connecting,” as exemplified by the Olympic Torch Relay that connected the regions (Fig. 5).

4.1 Flow of experience

First, participants chose their preferred mask from among the many painted with *kumadori* makeup (Fig. 6). We also projected the same special light used in the optical illusion version to make it appear that the *kumadori* masks hanging on the wall were casually changing their expressions. Once the participant stood in front of the monitor and placed their chosen mask on their face, the system automatically recognized the *kumadori* mask and overlaid it on the face of the participant. The *kumadori* mask had augmented reality (AR) features, i.e., it followed the person’s facial expressions and movements in all directions on the monitor in real time while the mask remained attached to the person’s face. The background in the monitor was also rendered to match the selected *kumadori* mask. We also prepared a background



Fig. 5. Torch Relay Commemorative Photo Corner: Kabuki Version booth.



Fig. 6. Selection of *kumadori* mask.

specifically inspired by the Olympic Torch Relay (Fig. 7). With their chosen mask attached to their faces, participants could pose any way they wanted while carrying the torch. Going to the next room, participants then found their faces being projected onto a gigantic 1.2-meter-high, three-dimensional

(3D) face, to give them an element of surprise (Fig. 8). Photos of the experience were later posted on SNS and made available for download.

4.2 Results

This experience was intended to be offered at the



Fig. 7. Torch Relay Commemorative Photo Corner: Kabuki Version experience.



Fig. 8. A gigantic 3D face with a height of 1.2 m.

Olympic Torch Relay expanded celebration events at two locations, namely, the Expo '70 Commemorative Park in Osaka and the Yokohama Red Brick Warehouse Square in Yokohama. However, due to the spread of COVID-19, it was only held at the Yokohama Red Brick Warehouse Square. A total of 82

people, including Olympic torchbearers and other people involved, experienced the exhibit. Participants laughed once they saw their chosen *kumadori* masks attached to their faces upon holding the masks up, and many got into character as *kabuki* actors while taking commemorative photos with the torch in hand.

5. Summary

Due to the spread of COVID-19, the number of people who experienced the exhibits was less than planned. Nevertheless, we were able to deliver surprises and smiles to the participants at the venues where we could provide the experiences. We believe that these interactions with the advanced technologies of our laboratories, which are not normally accessible to the public, enabled many people to experience firsthand NTT's innovativeness.

Going forward, we will continue to work on creating new experiences using ICT and connect people with each other.

Acknowledgments

We would like to express our gratitude to the members of the Tokyo Organising Committee of the Olympic and Paralympic Games and the representatives of the local governments who were involved in the operations. We also would like to thank the members who handled the operation of the Kirari! truck at the celebration venues.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

Reference

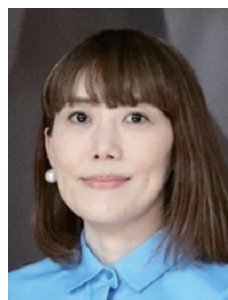
- [1] S. Uchida, E. Ashikaga, M. Imoto, M. Wagatsuma, and K. Hidaka, "Concept of Immersive Telepresence Technology 'Kirari!'," Proc. of the Media Computing Conference 2015, p. 39, 2015 (in Japanese).



Yoshiyuki Mihara

Senior Research Engineer, NTT Human Informatics Laboratories.

He received a B.Sc. and M.Sc. from Tokyo Institute of Technology in 2004 and 2006. He also received a Ph.D. from Kyoto University in 2017. Since joining NTT in 2006, he has been engaged in research and development (R&D) of a home network management service. The home network management protocols he designed have been standardized by Universal Plug and Play (UPnP) Forum, International Telecommunication Union Telecommunication Sector (ITU-T), and Japan's Telecommunication Technology Committee (TTC). He is currently promoting the key protocols with a view to launching a home network management service.



Masami Nagata

Manager, NTT 2020 Public Relations Strategic Business Development Division.

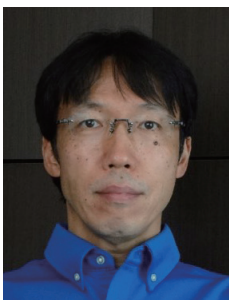
She joined NTT DOCOMO in 2002 and has been engaged in marketing. She is currently responsible for asset activation of the Tokyo 2020 Olympic Torch Relay as the Presenting Partner.



Keisuke Hasegawa

Engineer, NTT Human Informatics Laboratories.

He received a B.E. and M.E. in informatics from Kyoto University in 2012 and 2014. He joined NTT WEST in 2014 and engaged in the maintenance of network facilities. Since joining NTT Service Evolution Laboratories in 2016, he has been engaged in research of media processing for the ultra-realistic communication technology Kirari!. He is a member of the Institute of Image Information and Television Engineers (ITE).



Taiji Nakamura

Senior Research Engineer, 2020 Epoch-Making Project, NTT Human Informatics Laboratories.

He joined NTT DATA Communications Systems (now NTT DATA) in 1991. He has over 20 years' experience in information systems planning and development in the national public sector.



Junji Watanabe

Senior Distinguished Research Scientist, NTT Communication Science Laboratories.

He received a Ph.D. in information science and technology from the University of Tokyo in 2005. His research is focused on cognitive science and haptic communication devices with applied perception. His academic work has been published in scientific journals in the field of psychology and interface technologies. He has also presented his work at technology showcases and art festivals such as SIGGRAPH and Ars Electronica. His current research interest is how technologies are designed to achieve the wellbeing of society.



Tatsuya Matsui

Senior Research Engineer, NTT Information Network Laboratory Group.

He received a B.Sc. and M.Sc. from Tokyo Institute of Technology in 1993 and 1995. Since joining NTT in 1995, he has been engaged in R&D of the cyber security, digital library, MICE (meetings, incentives, conventions, exhibitions) application, interactive exhibition "Henshin Kabuki." He is currently working to improve the working style of researchers at NTT labs.



Hideaki Iwamoto

Research Engineer, NTT Human Informatics Laboratories.

He received a B.E. and M.E. in information engineering from Kyushu Institute of Technology, Fukuoka, in 1991 and 1993. He joined NTT Information and Communication Systems Laboratories the same year and engaged in R&D on information retrieval and natural language communication. He is currently researching and developing innovative user interface/user experience design and its showcasing.



Shingo Kinoshita

Vice President, Head of NTT Human Informatics Laboratories.

He received a B.E. from Osaka University in 1991 and M.Sc. with Distinction in technology management from University College London, UK, in 2007. He joined NTT in 1991 and was a senior manager of the R&D planning section of the NTT holding company from 2012 to 2015. He is currently a visiting professor at the Art Science Department, Osaka University of Arts, and visiting executive researcher at Dentsu Lab Tokyo. He has served as a member of the Japan Science and Technology Agency (JST) JST-Mirai Program Steering Committee, member of the All Japan Confederation of Creativity (ACC) TOKYO CREATIVITY AWARDS 2021 Judging Committee, and member of the Broadband Wireless Forum Steering Committee. He has been engaged in R&D of a media-processing technology, user interface/user experience, communication protocols, information security, machine learning, service design, and technology management. Until recently, he had been in charge of NTT's Tokyo2020 initiatives, including sports-watching video technology, inclusive design for social issues, and promoting the use of ICT in *kabuki*, entertainment, and media arts such as live music.

He has been in his current position since 2021, where he manages R&D on information and communication processing of humans based on human-centered principles.

Direction for Supporting Torchbearers × Swarm Communication Control Technology

Masafumi Suzuki, Hiroshi Chigira, Hitoshi Yamaguchi, Takuya Indou, and Shingo Kinoshita

Abstract

In connection with the Tokyo 2020 Olympic Torch Relay, NTT held NTT Presents Tokyo 2020 Olympic Torch Relay Celebration events in Yokohama and Osaka and presented a torchbearer-support program that welcomes torchbearers exchanging torch kisses using spatial-expression technology with robots. In this article, we introduce the control technologies used for the display bots that enabled the torchbearer-support program.

Keywords: Olympic Torch Relay, supporting torchbearers, spatial expression using robots

1. Overview

NTT is working to create new experiences by combining art and technology, and one of the results of our research in this area is “Art of Swarms,” a spatial-expression technology using display bots. Spatial expression refers to the creation of an organically changing visual space through the coordinated above-ground movements of a swarm of robots equipped with multiple displays. Unlike projection through the entire floor surface, display bots, which have physical mass, move as a swarm to create a visual space that enables an unconventional and tangible visual experience.

NTT introduced the concept of spatial expression at the 2018 NTT R&D Forum. Since then, we have expanded the scale and examined the theatrical effects of using display bots, including through demonstrations at the world’s largest art festival in Linz, Austria in 2018 and exhibits at the Sports Viewing Re-Imagined Exhibition in July 2019. At the Sports Viewing Re-Imagined Exhibition, we presented a collaboration of a swarm of more than 30 display bots with prominent artists Akiko Nakayama [1] and Ei Wada [2]. We also used a swarm of display bots for

sports expression, which received high praise from many people who watched the exhibit.

Using the knowledge gained from these demonstration experiments, we applied Art of Swarms to the Tokyo 2020 Olympic Torch Relay. We wanted many people to have a more dramatic experience of the Torch Relay and enable them to witness the possibilities of the fusion of NTT’s communication technologies with art. We directed a festival to welcome the torchbearers arriving at the venue during the NTT Presents Tokyo 2020 Olympic Torch Relay Celebration events (Figs. 1 and 2).

1.1 NTT Presents Tokyo 2020 Olympic Torch Relay Celebration

- Osaka: April 13, 2021, in front of the Tower of the Sun Plaza at the Expo ’70 Commemorative Park
- Yokohama: June 30, 2021, at the Red Brick Warehouse Event Square

We originally planned for many local people to watch these two events. However, due to the spread of the novel coronavirus (COVID-19), onsite viewing through general admission was canceled; thus, we presented the event online.

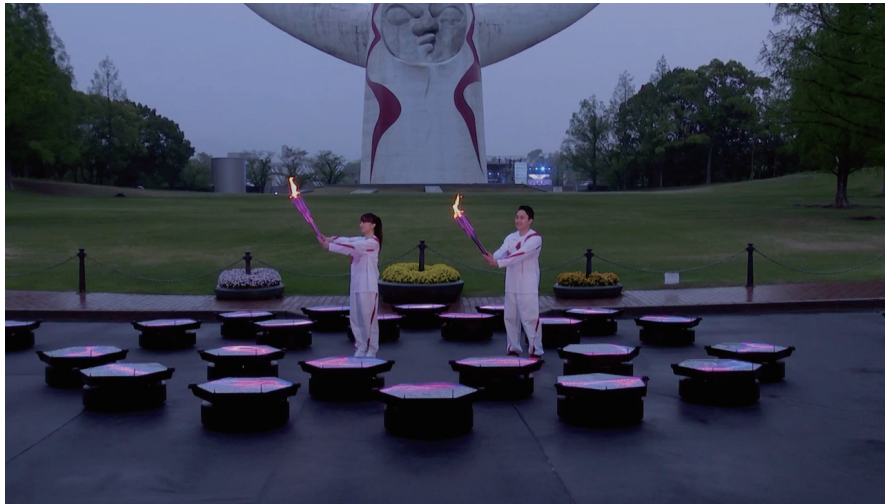


Fig. 1. Torch kiss scene at the Osaka event.



Fig. 2. Torch kiss scene at the Yokohama event.

We collaborated with Ars Electronica, a world-class media art research institute, to create dramatic scenes for the stage presentation. The original plan was for members of Ars Electronica to come to Japan to take part in local operations with members of NTT. However, they could not travel due to COVID-19, so instead they provided support online from Austria.

2. System configuration and technologies used

Display bots are robots that move on the ground and equipped with hexagonal displays (**Fig. 3**). They are composed of a display component at the top and a driving function component at the bottom, each operating independently. This configuration enables the robots to move in any direction while keeping the display surface in a fixed direction, thereby increasing

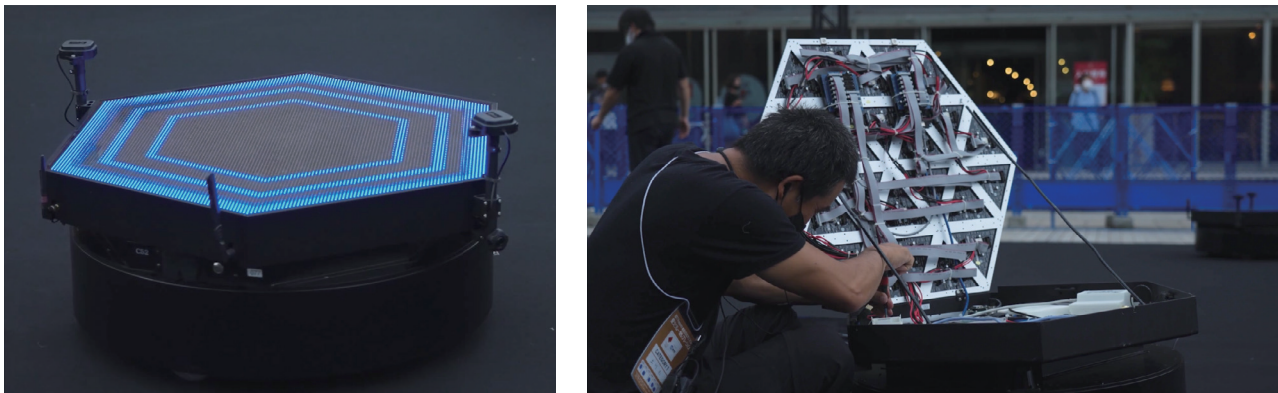


Fig. 3. Display bots.

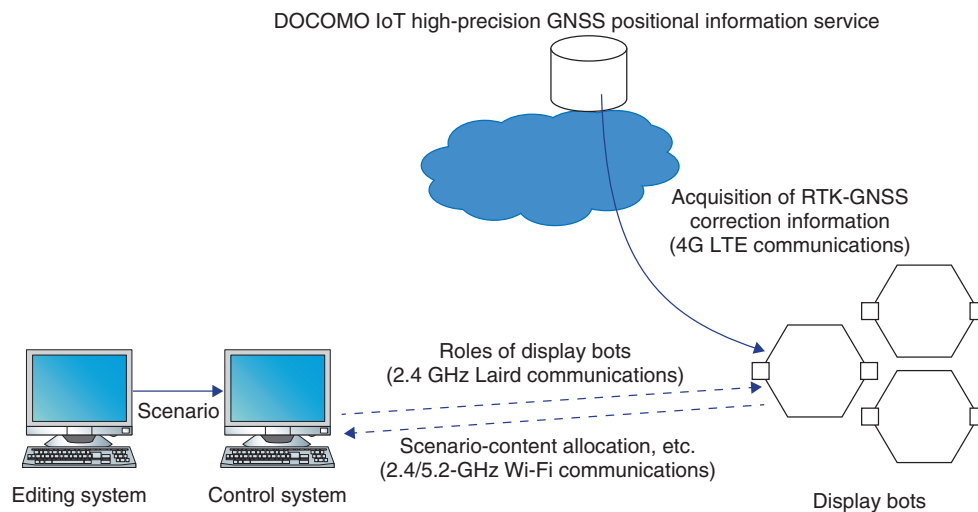


Fig. 4. Overview of system configuration.

the breadth of the spatial-image expression. In addition to the display, the top part includes devices for communicating, positioning, and controlling the movement of the display bot. The bottom part includes the driving mechanism and battery.

Figure 4 shows an overview of the entire system, including the display bots. The editing system is used for generating scenarios in which movements of multiple display bots and video-content assignments are programmed on the basis of the desired final image expression for the entire space. The control system then delivers and executes the specific scenarios and video content to the display bots. This enables display bots to move organically as a swarm.

The position of each display bot must be measured

accurately to enable coordinated movements while they move close to each other at a distance of around 10 centimeters. We had used motion capture with infrared cameras and reflective markers for positioning during previous demonstration experiments since they were conducted indoors. The same method, however, could not be applied since the torch relay event was going to be held outdoors. Although Global Positioning System (GPS) is commonly used for outdoor environments, the normal positioning accuracy of GPS exceeds a few meters, making it impossible to apply it as is. We therefore adopted a high-precision positioning system called real-time kinematic global navigation satellite system (RTK-GNSS). However, RTK-GNSS had not been widely

used, and using it for simultaneous control of 60 robots had never been attempted. RTK-GNSS enables high accuracy (error of a few centimeters) even outdoors by using correction information generated in real time from observation data at different locations called base stations in addition to the positional information obtained from regular GPS antennas. For this project, we applied NTT DOCOMO's "DOCOMO IoT high-precision GNSS positional information service" [3] to RTK-GNSS, a first-of-its kind initiative. Using RTK-GNSS enables accurate location information to be obtained, but it does not enable measurement of the exact direction. If the exact direction could not be determined, the direction of each display bot's display would be different from one other, and the entire image would become corrupt. We therefore installed two antennas diagonally on the display bot and obtained the direction information using the differential information from the two antennas.

We used proprietary standard Laird communications (2.4 GHz) and Wi-Fi communications (2.4/5.2 GHz) for communication between the display bots and control system and fourth-generation (4G) Long-Term Evolution (LTE) communications via mobile routers for communication with the DOCOMO IoT high-precision GNSS positional information service.

Before the display bots start moving, the scenarios are communicated simultaneously to each bot via radio signals from the control system upon the operator's command. Each display bot then begins to move in accordance with the transmitted scenarios. The bots move in accordance with the programmed scenario, but they can also be controlled in real time by the operator, such as to stop display bots simultaneously or decrease their speed, since they always operate in concert with the control system.

3. Testing

Testing with 100 display bots requires a space that is large enough to store, charge, and operate them and that is relatively free from obstructions to enable reception of the satellite signals for RTK-GNSS. We therefore conducted tests at the NTT Tsukuba R&D Center (Tsukuba City, Ibaraki Prefecture), which meets these requirements. After the decision to postpone the Tokyo 2020 Games, at the time of test resumption, the plan was to hold the event in collaboration with members from Ars Electronica. However, COVID-19 infections did not subside as we had expected, increasing the likelihood that they could not come on the day of the event. We therefore

promptly changed our policies as follows (Figs. 5 and 6).

- Control and preparations for actual event and tests at Tsukuba was carried out by only Japanese members mainly from NTT.
- Ars Electronica members did not come to Japan but supported the operations online.

As a result, NTT members had to deal with many unfamiliar tasks, such as handling hardware issues, troubleshooting and analyzing problems, and other tasks that were originally supposed to be handled by members of Ars Electronica. Many hours were therefore spent on remote correspondence with members in Austria. Due to the time difference with Austria, there were many time constraints; thus, it was necessary to efficiently carry out testing, problem analysis, and response.

4. Live performance

We held the first live event in front of the Tower of the Sun Plaza at the Expo '70 Commemorative Park on April 13, 2021. The final torch kiss with the last torchbearer of the day would have been welcomed through a spatial-expression show by a swarm of display bots, with the Tower of the Sun, the symbol of the Expo '70 Commemorative Park, in the background.

Around April 7, when we traveled to Osaka for the preparations, the number of new COVID-19 infections in Osaka Prefecture began to increase sharply, and the declaration of the third state of emergency became imminent. Eventually, on April 7, an announcement was made that the Torch Relay along public roads would be canceled and held at the Expo '70 Commemorative Park. Although we were able to avoid having the event on April 13 canceled, it was held with no spectators. In addition, the Osaka prefectural government requested us to avoid presenting in front of the Tower of the Sun, which was illuminated in red after sunset during the state of emergency. To comply with this request, we needed to start the event before sunset. However, since the display bots create the magical spatial expression by moving as a swarm of images in the dark, holding the event before sunset meant that the presentation would lose much of its charm. Also, given that many display-bot hardware failures had occurred since we arrived in Osaka and that GPS reception in the field was poor and positioning failed during preliminary rehearsals, to be safe, we decided to carry out the live performance in Osaka with 48 display bots in a stationary state. During the day of the event, while it was raining

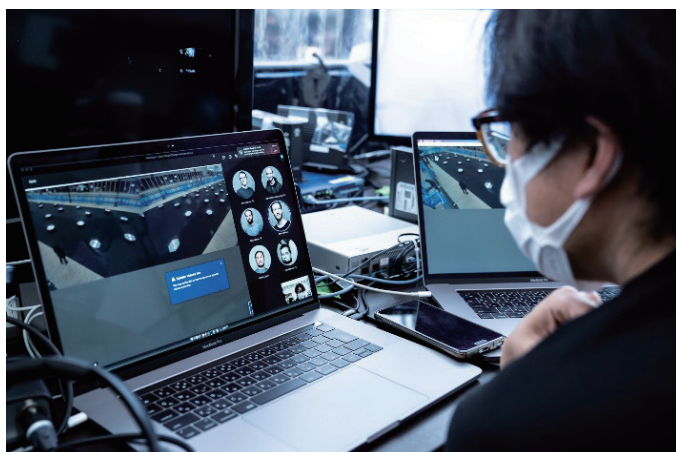


Fig. 5. Remote collaboration with members of Ars Electronica.



Fig. 6. Testing at NTT Tsukuba R&D Center.

heavily, the stationary display bots welcomed the torchbearers and rendered a coordinated display of lights along with the torch kiss.

After the completion of the Osaka event, we were faced with two major issues to be resolved in preparation for the Yokohama event scheduled on June 30. The first issue was the repair of the broken display bots. More than half of the bots had some sort of problem, so we needed to quickly carry out troubleshooting and repair to ensure that as many display bots as possible were operational before the next event. For the repair of the display bots, we determined which ones had to be returned to Austria for repair and which ones could be repaired in Japan. Considering all possible factors, including the number of units necessary for the entire production, number of days required for repair, and number of days required for testing, we created a repair plan and changed it in accordance with the daily situation. As a result, we were able to secure 48 operational display bots before the live event.

The second issue was the stabilization of their positioning. The location of GPS satellites on the day of the event and the surrounding environment had a significant impact on positioning. Even if we conducted prior testing in the same location and obtained good results, there was no assurance that we could obtain the same results during the actual event. We therefore used two methods to increase the reliability of positioning.

The first was improving the antenna-installation method. From our experience in Osaka, we found that raising the position of the antenna could lead to more

stable positioning. However, installing the antennas too high leads to many issues, such as difficulty in fixing the antenna in place or an unsightly appearance, so it was necessary to find a height that balances functionality with aesthetics. After various tests, we determined that the optimum height was around 15 cm from the surface of the display. The second was achieving failsafe positioning. We needed to ensure that positioning would continue even if the RTK-GNSS positioning fails. To achieve this, we used an odometer to estimate the position and direction using the amount of rotation, etc. of the wheel of the display bots.

The second event was held at Yokohama Red Brick Warehouse on June 30, 2021. Due to the COVID-19 situation, like in Osaka, onsite viewing through general admission was canceled, and the event was conducted exclusively through online streaming. From rehearsals to the live performance, the display bots did not fail, and their positioning was stable and almost never failed. In the area between Buildings No. 1 and No. 2 of the Red Brick Warehouse, the display-bot program showcased a magical display of lights through coordinated movements of 48 display bots as the last torch kiss of the day was exchanged and the final torchbearer was sent off to ignite the cauldron (Fig. 7).

5. Summary

Onsite viewing through general admission was canceled for both the Osaka and Yokohama events, preventing the general public from experiencing the

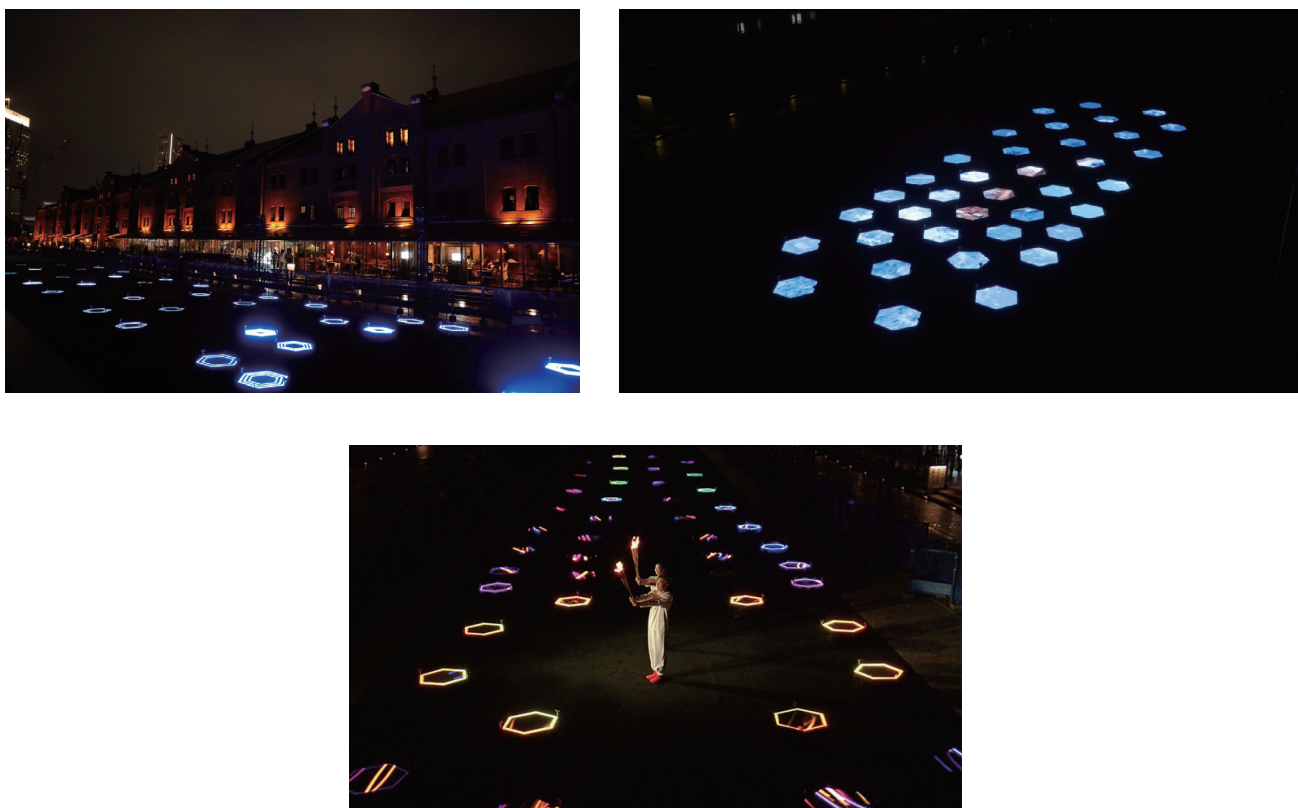


Fig. 7. Direction support for the Torch Relay in Yokohama.

display-bot presentation in person. Nevertheless, we consider it a major achievement to have enabled many people to enjoy via online streaming the presentation of lights and movements by the swarm of display bots around the torchbearers and for the show to be featured in various media events, including the opening ceremony presentation, as an iconic scene of the Tokyo 2020 Olympic Torch Relay.

Going forward, we will continue to study further possibilities of the fusion of art and technology.

Acknowledgments

The implementation of the display-bot torchbearer-support program was made possible with the cooperation of many people. We would like to express our

sincere gratitude to the people of Osaka and Kanagawa Prefectures for supporting the events, members of Dentsu and Dentsu Live, members of Ars Electronica, and many others who were involved in the preliminary rehearsals, tests, as well as during the live performance.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

References

- [1] Akiko Nakayama, <http://akiko.co.jp/akikoweb/>
- [2] Ei Wada, <https://eiwada.com>
- [3] DOCOMO IoT high-precision GNSS positional information service (in Japanese), https://www.nttdocomo.co.jp/biz/service/highprecision_gnss_positioning/



Masafumi Suzuki

Research Engineer, NTT Human Informatics Laboratories.

He received an M.E. in engineering from Ritsumeikan University, Kyoto, in 2011. After joining NTT in 2011, he engaged in research on cloud services using carrier network functions. He developed a number of proof-of-concept systems at NTT Service Integration Laboratories, NTT Cyber Solution Laboratories, and NTT Service Evolution Laboratories. In 2015, he joined the 2020 Epoch-Making Project. He has been involved in the development of systems to promote NTT's cutting-edge technology for the Tokyo 2020 Games.



Hiroshi Chigira

Senior Research Engineer, NTT Human Informatics Laboratories.

He received a B.E. and M.E. in engineering from Waseda University, Tokyo, in 2007 and 2009, and joined NTT in 2009. Since then he has been engaged in research on human-computer interaction and developed vital sensing hardware at NTT Cyber Solution Laboratories and NTT Service Evolution Laboratories. In 2016, he joined the 2020 Epoch-Making Project, where he has been engaged in several creative research projects combining NTT's cutting-edge technologies, design, and art to celebrate Tokyo 2020 Games.



Hitoshi Yamaguchi

Senior Research Engineer, NTT Human Informatics Laboratories.

He received a B.E. in physics from Keio University, Kanagawa, and M.E. in applied physics from Tokyo Institute of Technology in 1997 and 1999, and joined NTT in 1999. Since then he has been engaged in the development of network node systems at NTT Network Service Systems Laboratories, and the development of smart-phone applications at NTT DOCOMO.



Takuya Indou

Senior Research Engineer, Supervisor, NTT Human Informatics Laboratories.

He received a B.S. in physics from Kyoto University in 1993. In the same year, he joined NTT. His research interests include media processing and human-computer interaction. He is a member of the Information Processing Society of Japan (IPSI), and the Association for Computing Machinery (ACM).



Shingo Kinoshita

Vice President, Head of NTT Human Informatics Laboratories.

He received a B.E. from Osaka University in 1991 and M.Sc. with Distinction in technology management from University College London, UK, in 2007. He joined NTT in 1991 and was a senior manager of the R&D planning section of the NTT holding company from 2012 to 2015. He is currently a visiting professor at the Art Science Department, Osaka University of Arts, and visiting executive researcher at Dentsu Lab Tokyo. He has served as a member of the Japan Science and Technology Agency (JST) JST-Mirai Program Steering Committee, member of the All Japan Confederation of Creativity (ACC) TOKYO CREATIVITY AWARDS 2021 Judging Committee, and member of the Broadband Wireless Forum Steering Committee. He has been engaged in R&D of a media-processing technology, user interface/user experience, communication protocols, information security, machine learning, service design, and technology management. Until recently, he had been in charge of NTT's Tokyo2020 initiatives, including sports-watching video technology, inclusive design for social issues, and promoting the use of ICT in *kabuki*, entertainment, and media arts such as live music.

He has been in his current position since 2021, where he manages R&D on information and communication processing of humans based on human-centered principles.

Stage Production for Celebration of Torch Relay × Ultra-realistic Communication Technology Kirari!

Taiji Nakamura, Keisuke Hasegawa, Yoshiyuki Mihara, Takashi Miyatake, and Shingo Kinoshita

Keywords: ultra-realistic communication technology Kirari!, Torch Relay, live performance

1. Overview

The Tokyo 2020 Olympic Torch Relay, which started in Fukushima Prefecture on March 25, 2021, was carried by 10,515 runners over 121 days through all 47 prefectures in Japan. The Torch Relay usually involves the torchbearers running on public roads and a celebration event at the final point of the relay at the end of each day. At the celebration event, the final torchbearer of the day lights the Olympic flame in its cauldron, local residents and sponsors perform songs and dances on stage, and people can have their photos taken with an Olympic torch at the Olympic Torch Relay Commemorative Photo Corner and enjoy other exhibits to add to the excitement of the Torch Relay.

As an extended version of the celebration event, “NTT Presents Tokyo 2020 Olympic Torch Relay Celebration - CONNECTING WITH HOPE” was staged by NTT in Osaka on April 13 and in Yokohama on June 30. In addition to the torch being carried by the final torchbearer of the day, GENERATIONS from EXILE TRIBE performed live, junior-high-school students, EXILE ÜSA, and EXILE TETSUYA performed “Rising Sun -2020-,” and calligraphy artist Soun Takeda performed using calligraphy. Initially, we planned to invite a general audience of about 5000 people; however, due to the spread of the novel coronavirus (COVID-19), general audience viewing at both venues were canceled and switched to online streaming instead.

NTT research and development (R&D) laboratories have been conducting demonstration experiments of

ultra-realistic live broadcasts and stage productions of *kabuki*, live music, fashion shows, sports events, and other events by using our ultra-realistic communication technology Kirari! (Fig. 1).

On the basis of the results of those demonstration experiments, for the live performance by GENERATIONS from EXILE TRIBE in the extended celebration event, we created three new stage productions by using Kirari!, i.e., “remote performance,” “remote viewing,” and “remote fan collaboration.”

2. Details of stage productions

2.1 Remote performance

During the COVID-19 pandemic, it has become increasingly difficult for artists to get together, especially if they are far apart. The purpose of the remote performance in such an environment is to harness the power of communication to create an experience that makes remote artists feel as if they are performing in the same place. For this remote-performance stage production, we created a group dance in tune with the song “Choo Choo TRAIN” by artists in remote locations.

Normally, artists at distant venues would collaborate with each other; however, in this case, to simulate the experience, we used two locations on the stage as remote locations and a transparent screen above the stage as a virtual shared space. As shown in Fig. 2, points (1) and (2) on the stage are the remote locations, and the transparent screen (3) is a shared space above those locations. The images of the artists dancing

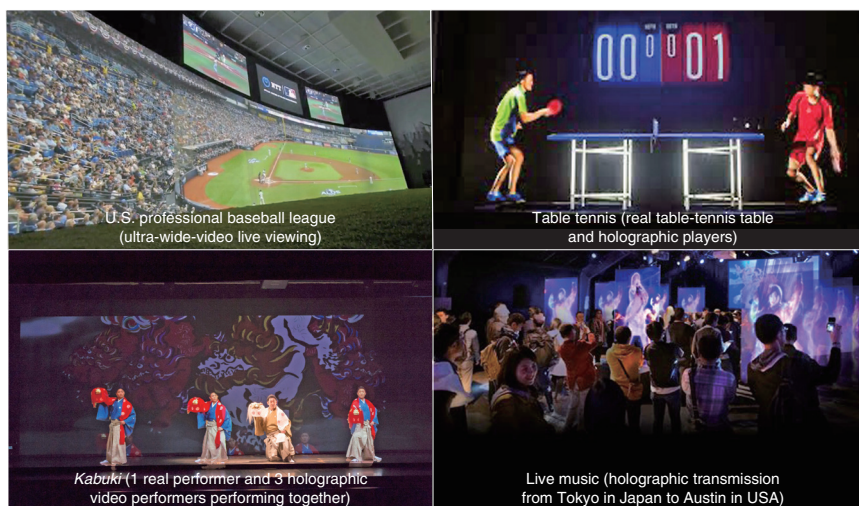


Fig. 1. Demonstration experiments using Kirari!.

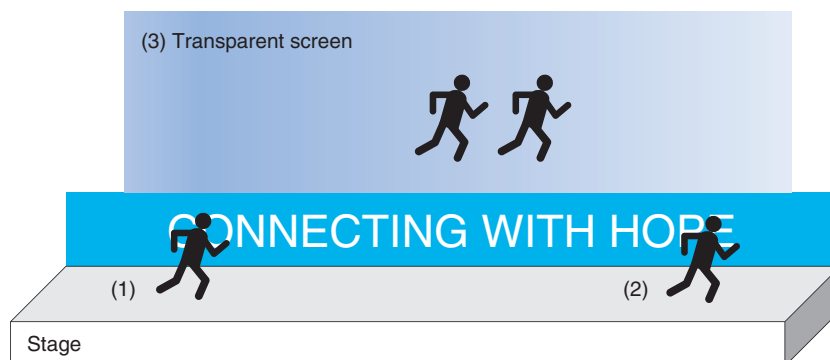


Fig. 2. Stage production.

at points (1) or (2) were transferred to the transparent screen. At that time, the background images were cut out by Kirari! and only each artist's image was transmitted. The images projected on the transparent screen appeared to be three-dimensional, and that appearance created an experience in which the viewer feels that the artists are actually dancing there. Five artists dance in turn, so, each time, the number of artists on the transparent screen increased (**Fig. 3(a)**); finally, when all artists have finished dancing, the images of the five artists merged into one as if they were dancing in circular motions at the same location (**Fig. 3(b)**). It is also possible to extract and transmit the images of all the artists dancing at the same time in real time.

2.2 Remote viewing

During the pandemic, it has also become difficult for fans to attend live-music concerts, especially for fans in provincial areas wanting to go to concerts in big cities. The purpose of this remote viewing was to harness the power of communication in such an environment to create an experience through which the artist appears to be performing right in front of you.

Our challenge was to transmit the video of the artists on the main stage to another remote stage with the fans present. Normally, we would have streamed the images to a remote site far away; however, for the purpose of simulating the experience, as shown in **Fig. 4**, we transmitted the data to a Kirari! truck set up at a remote location in Yokohama. The Kirari! truck housed a transparent screen similar to the one



(a) Remote performance (performer in lower right is the real image, and the performers in center stage are virtual images)



(b) Remote performance

Fig. 3. Group dance in tune with the song “Choo Choo TRAIN” via Kirari!.

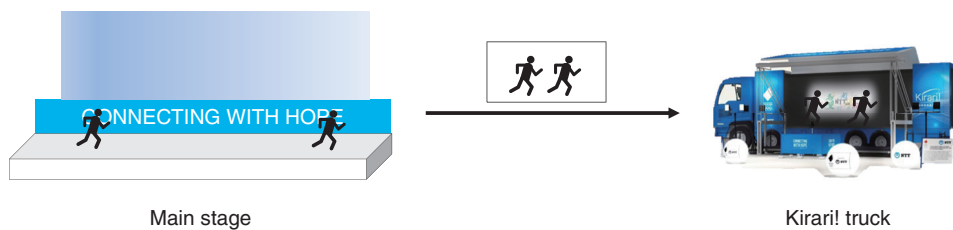


Fig. 4. Configuration of remote viewing.

forming the main stage and, as shown in **Fig. 5**, the artists transferred by Kirari! were displayed on the screen in a holographic manner to create an experience in which the artists appear to have come to perform right in front of the fans.

2.3 Remote fan collaboration

It has been difficult for fans and artists to interact with each other during the pandemic. Even if the fans could go to a venue, the experience of shaking hands with a celebrity like before has become impossible. The purpose of remote fan collaboration was to harness the power of communication in such an environment to create an experience in which the artist appears to come and perform with the fans.

We faced two challenges for this production. One was to transfer the artist on the main stage and the other was to transfer the fans at the venue next to the artist on the stage. For the first challenge, the images of the artist on the stage were extracted using Kirari! and superimposed next to the images of the fans displayed on a monitor on the stage. As shown in **Fig. 6**,

this process gave the fans in the audience the virtual feeling of being next to the artist. For the other challenge, the images of the artist extracted using Kirari! were transferred to the remotely located Kirari! truck in a manner that created the feeling that the artist had been transferred next to the fans in the truck.

3. Technology

We now explain one of the technologies that make up Kirari!, “real-time extraction of objects with arbitrary background” technology [1]. This technology can extract a specific object from a video without the need to use a green background. NTT developed “KIRIE” [2] in 2018, which systemizes object extraction using this technology, and used it for the above-described stage productions.

With KIRIE, the object is extracted by switching between two methods: one using only background subtraction and the other combining background subtraction and machine learning. With background subtraction, an image without an object is acquired in

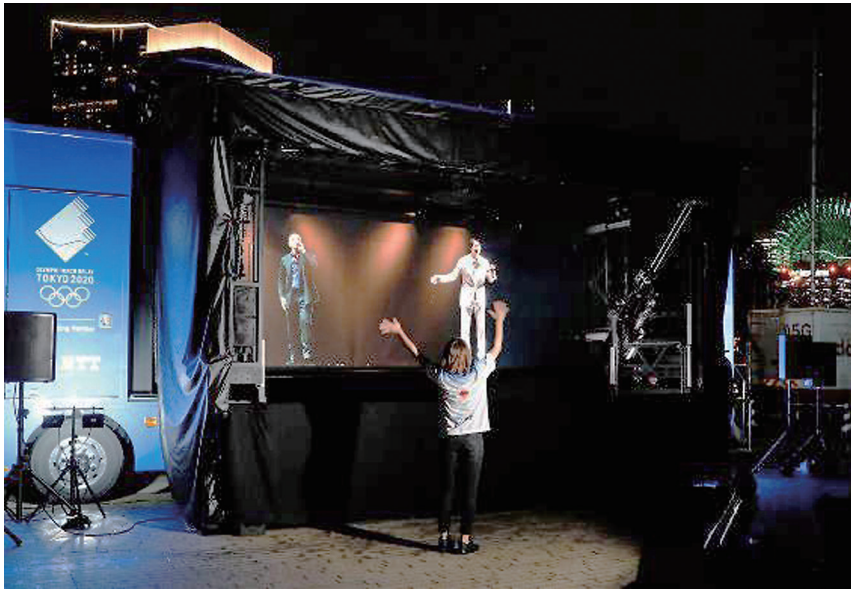


Fig. 5. Appearance of remote viewing.



(a) The performers are transferred next to the fans in the audience so they can all dance together



(b) The performer interacts with fans on the Kirari! truck

Fig. 6. Appearance of remote fan collaboration.

advance as a background, and the area in which the object is to appear is identified by taking the difference between the background and image being captured.

Using machine learning, in addition to the above-mentioned background image, multiple images showing the object and background at the same time are taken. By learning the combination of background color and color of the object to be extracted as training data, it is possible to determine what area corresponds to the object.

The method that only uses background subtraction has the advantage of not requiring prior training; however, it is not easy to extract objects in colors close to the background color. Another disadvantage is that if the background changes even slightly, the extraction accuracy will decrease. In contrast, the method of combining background subtraction and machine learning has advantages such as being able to extract images even when the colors of the background and object are similar and being able to handle changes in the background. However, it requires prior

training.

For the above-mentioned stage productions, when the performers could participate in the rehearsal the day before and the color of the costume they would wear on the day was decided, we aimed for more-accurate object extraction by using the method of combining background subtraction and machine learning. When the performers could not attend the rehearsal on the previous day, however, we used the method that only uses background subtraction to extract the objects.

4. Results

The extended versions of the Torch Relay celebration, which were streamed online, were viewed by many people, with 100,000 views on YouTube Live with a maximum of 12,000 simultaneous connections. We also received a large amount of positive feedback on social networking sites, where over 90% of the responses were positive.

Using the above-mentioned technologies for the remote-performance, remote-viewing, and remote-fan-collaboration productions, we could extract objects with high accuracy.

Even under the condition that the color of the background tends to change, such as when it was raining during the previous day's rehearsal but sunny on the next day's rehearsal, we could extract the object by combining background subtraction and machine learning with an accuracy acceptable for viewing. In some cases, the arrangement of the production suddenly changed on the day, and performers different from those targeted in the previous day's rehearsal became the extraction target; nevertheless, the method using only background subtraction still produced generally acceptable extraction results. The average processing delay of KIRIE was 166 ms, which indicates that we achieved real-time object extraction with low latency and high accuracy.

5. Concluding remarks

For the extended celebration events of the Tokyo 2020 Olympic Torch Relay, we conducted three stage productions, remote performance, remote viewing, and remote fan collaboration using Kirari!. Although the public viewing was cancelled due to the spread of COVID-19, we could still demonstrate to tens of thousands of viewers the possibility of new remote entertainment during the pandemic through online streaming and received positive feedback from the majority of those viewers. Taking the above-described challenges as a first step, NTT R&D will continue to research and develop technologies toward the creation of a new form of live entertainment suitable for the "new normal" era.

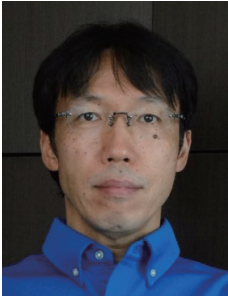
Acknowledgments

We thank the Tokyo Organising Committee of the Olympic and Paralympic Games, Osaka Prefecture, Suita City, Kanagawa Prefecture, Yokohama City, and our partner companies for their cooperation in promoting this project. We also thank GENERATIONS from EXILE TRIBE and all the performers who graced the stage of the extended celebration.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

References

- [1] H. Kakinuma, J. Nagao, H. Miyashita, Y. Tonomura, H. Nagata, and K. Hidaka, "Real-time Extraction of Objects from Any Background Using Machine Learning," *NTT Technical Review*, Vol. 16, No. 12, pp. 12–18, 2018.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201812fa2.html>
- [2] J. Nagao, H. Miyashita, T. Sano, K. Hasegawa, and T. Isaka, "Kirari! for Arena: Real-time Remote Reproduction of 4-directional Views with Depth Perception," *Journal of the Imaging Society of Japan*, Vol. 58, No. 3, pp. 306–315, 2019 (in Japanese).



Taiji Nakamura

Senior Research Engineer, 2020 Epoch-Making Project, NTT Human Informatics Laboratories.

He joined NTT DATA Communications Systems (now NTT DATA) in 1991. He has over 20 years' experience in information systems planning and development in the national public sector.



Takashi Miyatake

Senior Research Engineer, Supervisor, NTT Human Informatics Laboratories.

He received an M.E. in engineering from Kobe University in 1995. In the same year, he joined NTT and engaged in research on image processing and human interface. He also worked as a system engineer at NTT Communications and other companies. He is currently engaged in research on the ultra-realistic communication technology Kirari!.



Keisuke Hasegawa

Engineer, NTT Human Informatics Laboratories.

He received a B.E. and M.E. in informatics from Kyoto University in 2012 and 2014. He joined NTT WEST in 2014 and engaged in the maintenance of network facilities. Since joining NTT Service Evolution Laboratories in 2016, he has been engaged in research of media processing for the ultra-realistic communication technology Kirari!. He is a member of the Institute of Image Information and Television Engineers (ITE).

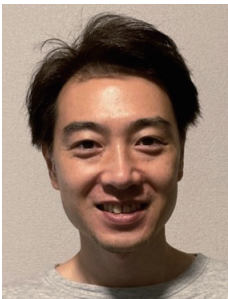


Shingo Kinoshita

Vice President, Head of NTT Human Informatics Laboratories.

He received a B.E. from Osaka University in 1991 and M.Sc. with Distinction in technology management from University College London, UK, in 2007. He joined NTT in 1991 and was a senior manager of the R&D planning section of the NTT holding company from 2012 to 2015. He is currently a visiting professor at the Art Science Department, Osaka University of Arts, and visiting executive researcher at Dentsu Lab Tokyo. He has served as a member of the Japan Science and Technology Agency (JST) JST-Mirai Program Steering Committee, member of the All Japan Confederation of Creativity (ACC) TOKYO CREATIVITY AWARDS 2021 Judging Committee, and member of the Broadband Wireless Forum Steering Committee. He has been engaged in R&D of a media-processing technology, user interface/user experience, communication protocols, information security, machine learning, service design, and technology management. Until recently, he had been in charge of NTT's Tokyo2020 initiatives, including sports-watching video technology, inclusive design for social issues, and promoting the use of ICT in *kabuki*, entertainment, and media arts such as live music.

He has been in his current position since 2021, where he manages R&D on information and communication processing of humans based on human-centered principles.



Yoshiyuki Mihara

Senior Research Engineer, NTT Human Informatics Laboratories.

He received a B.Sc. and M.Sc. from Tokyo Institute of Technology in 2004 and 2006. He also received a Ph.D. from Kyoto University in 2017. Since joining NTT in 2006, he has been engaged in R&D of a home network management service. The home network management protocols he designed have been standardized by Universal Plug and Play (UPnP) Forum, International Telecommunication Union Telecommunication Sector (ITU-T), and Japan's Telecommunication Technology Committee (TTC). He is currently promoting the key protocols with a view to launching a home network management service.

Torch Relay Regional Event × Voice-recognition Communication Technology

Yusuke Ichikawa and Yuki Yoshida

Abstract

To celebrate the Tokyo 2020 Olympic Torch Relay, NTT held a hands-on event that enabled children from local elementary schools to cheer on the Torch Relay. During this event, we created a new cheering experience by developing a cheering-production system together with the elementary-school students that visualizes the cheers of the children as text using voice-recognition communication technology and sends the text cheers to the runners. This article introduces the event and cheering-production system.

Keywords: Torch Relay, voice-recognition communication technology, experience design

1. Overview

The NTT Yokosuka R&D Center was selected as one stop on the route of the Tokyo 2020 Olympic Torch Relay, which traveled the length and breadth of Japan. An event to welcome the torch to the center was managed by NTT. NTT research and development (R&D) laboratories recruited a wide range of staff from across several laboratories to plan and organize the event. A total of 18 people from 9 laboratories worked together as a study team to organize the event. The team decided to welcome the torch to the NTT Yokosuka R&D Center by inviting local residents to participate—with whom we have had many exchanges in the past.

The concept of the Tokyo 2020 Olympic Torch Relay was “Hope Lights Our Way.” Established in 1972 in Yokosuka, Japan, the NTT Yokosuka R&D Center has long been involved in exchanges with local residents through technology. Combining this background with the concept of the Torch Relay, we decided on the theme of “Connecting ages, connecting communities, and connecting technologies” for the event.

In accordance with that theme, we selected senior researchers as initial torchbearers who would pass the torch to young researchers who would in turn pass it

to local students. In addition, elementary-school students from nearby schools (Awata and Iwato Elementary Schools in Yokosuka City) were invited as spectators to cheer on the Torch Relay. The entire Torch Relay, including the spectators, was designed to connect ages and communities. Students from Kanagawa Prefectural Yokosuka High School, which had been interacting with the NTT Yokosuka R&D Center through programs such as “Super Science High School,” were also selected as local student torchbearers.

On the basis of the theme of connecting communities and technologies, this event aimed to provide an opportunity for elementary-school students to experience the communication technology of the NTT Yokosuka R&D Center through cheering. The aim of the event was to provide a new experience of cheering for the Torch Relay. We developed a cheering-production system using voice-recognition communication technology that enables the cheers of elementary-school students to be visualized and transmitted to the torchbearers. To expose the students to such technology, we introduced a paper-cup microphone that they could make themselves using commercially available paper cups, magnets, and coils and use as an input device for the cheering-production system. Before the event, we asked the students to make their



Fig. 1. The cheering-experience event at Iwato Elementary School.

own paper-cup microphones. By making the microphones themselves, the students had a chance to learn the principles of communication by which sound is transmitted by a magnet and coil.

In March 2020, in the midst of these preparations, it was decided to postpone the Torch Relay and the Olympic and Paralympic Games for one year due to the spread of the novel coronavirus (COVID-19). Nevertheless, members of the study team organizing the event continued to prepare to welcome the torch to the NTT Yokosuka R&D Center. In March 2021, the Torch Relay started as scheduled; however, two weeks before our event, due to continuing spread of COVID-19 infections, the Kanagawa prefectural government decided to take the Torch Relay off public roads in the prefecture. Consequently, the Torch Relay event at the NTT Yokosuka R&D Center was cancelled. Although it was decided to cancel the event, all the members of the study team had one goal in mind, to create memories for the elementary-school students who had participated in making their paper-cup microphones. With that goal in mind, we worked together and immediately started planning an alternative event. Since we could not hold a group-type event at the NTT Yokosuka R&D Center, we decided to take the cheering-production system to the Awata and Iwato elementary schools and hold a similar Torch Relay cheering-experience event on those premises. The paper-cup microphones, which was an idea of the members of the study team, has the advantages of not only preventing oral droplets from spreading but also amplifying voices without the need for shouting. From that viewpoint, we were con-

vinced that we could hold the event safely even in the midst of the pandemic. When we consulted with the elementary schools about our plan, they readily agreed to hold the event in the gymnasium at Awata Elementary School and in the audiovisual room at Iwato Elementary School. The participants were sixth graders. The event was simultaneously held at both schools on June 29, which was the date the Torch Relay was originally scheduled to be held (Fig. 1). The total number of participants was 107, including 61 from Awata Elementary School and 46 from Iwato Elementary School.

2. Cheering-production system

The cheering-production system visualized the voices of the students through paper-cup microphones by using voice-recognition communication technology. The configuration of the system is shown in Fig. 2. To obtain the sound of a student's voice, each student's paper-cup microphone was connected to his/her smartphone. The voice collected by the paper-cup microphone was sent to the voice-recognition communication network through the smartphone ((1) in Fig. 2). Through the voice-recognition communication network, the speech content was converted into characters and output during the communication. The speech content output from the voice-recognition communication network was displayed on a projector at the event venue that can also be seen by the torchbearers ((2) in Fig. 2). We improved the recognition accuracy by limiting the recognition to two specific cheering words, “*ganbare!*” (“Go for

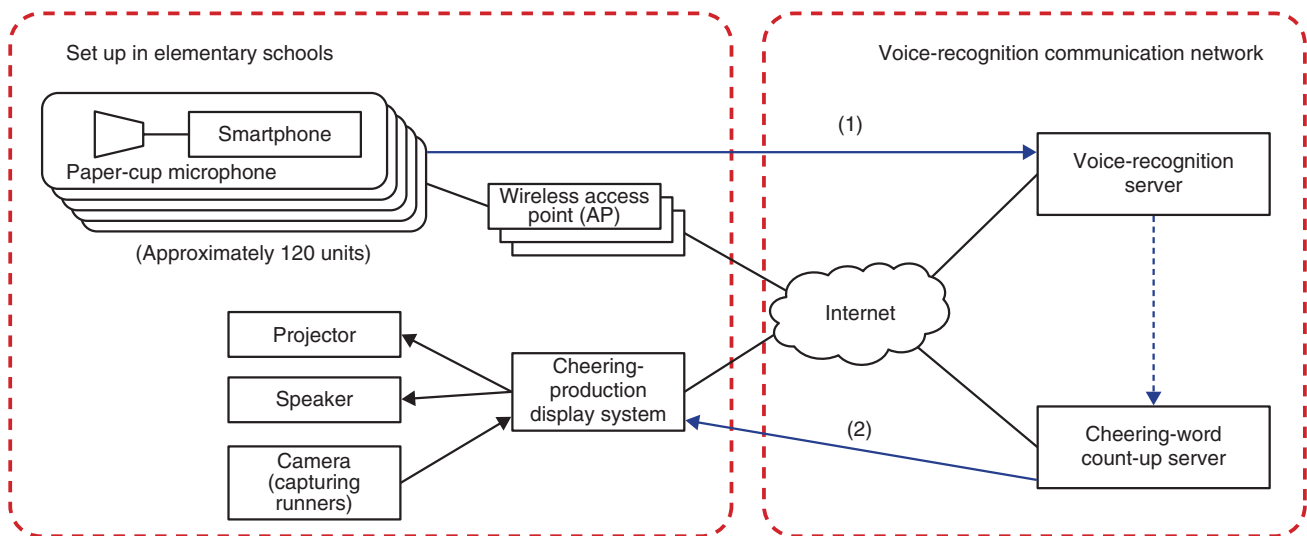


Fig. 2. Overview of cheering-production-system configuration.

it!", "Come on", etc.) and "*faito!*" (lit. "fight!"). The number of times each cheering word was uttered was also counted, and from the results of the counting, the image projected by the projector at the venue and the cheers collected with the paper-cup microphones and output to the loudspeakers were visualized and transmitted to the torchbearers (Fig. 3).

3. Technology

3.1 Voice-recognition communication technology

The signal-to-noise ratio of the speech collected with paper-cup microphones is low, and the frequency of the band required for speech drops. Therefore, the failure to recognize phonemes (sound units such as the vowels /a/, /i/, /u/, /e/, and /o/) posed a challenge to implementing the cheering-production system. Therefore, we developed a learning model and tuned it to the characteristics of a paper-cup microphone. For this event, it was important to recognize the specified cheering word without omission. Therefore, we were able to improve the cheering experience by limiting the number of words to be recognized and tuning the model by prioritizing reproduction rate (sensitivity) over relevance rate (accuracy).

We asked the elementary-school students to make their own paper-cup microphones for transmitting their cheers to the voice-recognition communication network. The creation of the paper-cup microphones was part of the technology-education program that was implemented in the children's science class held

at the NTT Yokosuka R&D Center Open House in 2012.

For this cheering-experience event, all students had to complete their paper-cup microphones within the time allotted by the school, i.e., two periods of 120 minutes. With that allocated time in mind, the study-team members repeated trials, identified steps that would take time, and devised ways such as omitting work steps requiring scissors and prepared an all-you-need kit. All the students completed their microphones within the allocated time. A scene from the day of the event is shown in Fig. 4.

On the day of the event, the procedure was as follows. On completing their paper-cup microphones, each student, in order of finishing, connected the microphone to their smartphone and recorded their voice on the smartphone. Their recorded voices were then played back from the speaker, and the operation of the cheering-production system was checked. The students were able to enjoy learning about the mechanism of voice communication, for example, when their voice was actually played back from the speaker, we heard them exclaim "Ooh!" and "Aah!"

4. Results

During the cheering-experience event, teachers from the school ran with torches around classrooms and gymnasiums, and when each torch-bearing teacher reached the next teacher, they conducted a simulated "torch kiss" by touching the tips of their



Fig. 3. Example of displayed cheering words and number of times the words were uttered (The center of the screen is a composite display of an actual runner's image.).

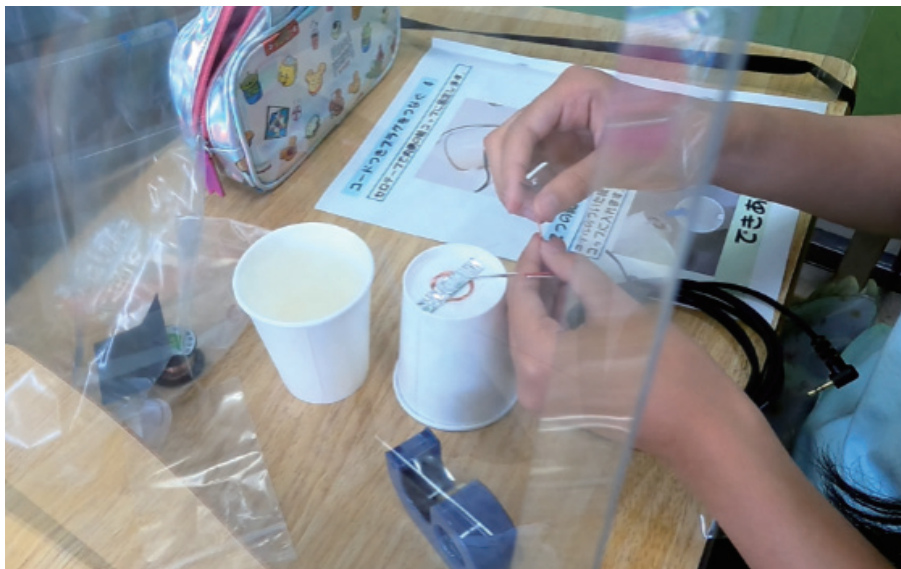


Fig. 4. A snapshot of a student making a paper-cup microphone.

torches. The simulated Torch Relay lasted about 15 minutes, during which the students continued cheering while desperately trying to keep their voices down to prevent droplet infection. Although the cheers were not loud, they were amplified by the paper-cup microphones and became louder, and the two cheering words were counted about 9000 times and displayed while the torchbearers were running. After the event, all of the participating students wrote their impressions (in a completely free format) with comments such as, “I was so happy when I could make a sound with the paper-cup microphone,” “I could speak with a normal voice even though my voice came from a microphone,” and “It was amazing to cheer with the paper-cup microphone just like with a real microphone.” We were amazed to see that the

cheering experience was not only fun but also led to an interest in technology. We heard the students' interest in the fundamentals of technology with comments such as “I want to know why it is the way it is.”

This event was evaluated as having value in terms of not only regional exchange but also education. The school principals said, “I think it was good for learning that various communication technologies are being researched at local facilities” (Principal Kaneko, Awata Elementary School) and “It was very significant in regard to career education to be exposed to NTT's research and technology” (Principal Haraguchi, Iwato Elementary School).

5. Concluding remarks

The planned regional event of the Torch Relay in the form of inviting elementary-school students to the NTT Yokosuka R&D Center was not possible. However, from making paper-cup microphones to actual cheering, the elementary-school students actively experienced a simulated relay, and we believe that we were able to reach our goal set out in our original theme of “Connecting ages, connecting communities, and connecting technologies.” We believe that the exposure to the Torch Relay helped build momentum for the Tokyo 2020 Games. To be a research institute that continues to develop together with the community, we will continue to connect with the local community through technology.

Acknowledgments

We thank the teachers and students of Awata Elementary School and Iwato Elementary School in Yokosuka City for understanding the value of this event and participating in it. We also thank the Kanagawa Prefectural Sports Bureau, Yokosuka City Policy Promotion Department, Kanagawa Prefectural Police Security Department, and Kanagawa Prefectural Yokosuka High School for their cooperation in the preparation of the Torch Relay.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).



Yusuke Ichikawa

Senior Research Engineer, Cyber-World Laboratory, NTT Human Informatics Laboratories.

He received a B.E. and M.E. in measurement engineering from Keio University, Kanagawa, in 1995 and 1997, and Ph.D. in informatics from Shizuoka University in 2020. He joined NTT Multimedia Network Laboratories in 1997. Since 1998, he has been researching and developing recommendation systems. He is a senior member of the Information Processing Society of Japan (IPSJ) and received the 2005 and 2019 IPSJ Yamashita SIG Research Award.



Yuki Yoshida

Research Engineer, NTT Human Informatics Laboratories.

She received a B.Sc. and M.Sc. from the University of Tsukuba. She joined NTT and engaged in R&D of human interface. In 2019, she joined the 2020 Epoch-Making Project, where she has been engaged in service promotion to celebrate the Tokyo 2020 Games.

High-efficiency Wi-Fi Technologies

*Toshiro Nakahira, Motoharu Sasaki,
Masayoshi Nabeshima, Tomoaki Ogawa,
Takatsune Moriyama, Ken Hiraga, Kento Yoshizawa,
and Ikutaro Ogushi*

Abstract

NTT undertook the technical development and implementation of high-efficiency Wi-Fi technologies to provide spectators and related personnel a stress-free wireless communications environment at the Japan National Stadium and other venues of the Olympic and Paralympic Games Tokyo 2020. These technologies are expected to lead to new sports-viewing styles using the network of a venue and a variety of new services using a flexible network at events such as meetings, incentives, conferences, and exhibitions (commonly referred to as MICE).

Keywords: high-efficiency Wi-Fi, wireless resource control technology, wireless quality visualization technology

1. Introduction

Everyone's lifestyle has been changing along with the widespread use of smartphones and social networking services (SNSs), and the way in which people participate in events such as when attending sports matches or live concerts has likewise been changing. For example, it has become common for spectators at a venue to take photos or video of an exciting scene using their cameras or smartphones and immediately post such images simultaneously on SNSs or upload them to a cloud environment. In a similar manner, it was envisioned that many spectators at venues of the Olympic and Paralympic Games Tokyo 2020 would be simultaneously using the networks of these venues.

The Japan National Stadium, the main venue of the Tokyo 2020 Games, required a stress-free communications environment for spectators appropriately linked to a variety of systems to become a world-class stadium as the new hub for sports in Japan. To this end, specialists having high technical competence through extensive experience in constructing Internet Protocol (IP) networks, Wi-Fi* systems, etc. were recruited from NTT Group companies to set up an

information-and-communication-technology environment on a world-class level. These specialists used their diverse experience and expertise in constructing and operating Wi-Fi systems at large-scale stadiums to achieve an optimal arrangement of access points (APs) tailored to the construction and shape of the Japan National Stadium. This arrangement featured an AP for every 70 seats and provided coverage of areas where people would tend to gather such as concourses, vendor stalls, and ticket counters. The end result was a total of approximately 1300 APs, making for a high-density, world-class Wi-Fi system. To achieve such a high-density configuration, optimal channel settings to avoid radio-wave interference and tuning performed at the final stage of construction were important. Therefore, it was decided to use the high-efficiency Wi-Fi technologies being developed by NTT laboratories to create a stable and high-quality Wi-Fi environment. This provided smooth connections to the Internet enabling everyone in the stadium to share their feelings or impressions on SNSs or elsewhere.

* "Wi-Fi" is a registered trademark of Wi-Fi Alliance.

- (a) AP wireless control: Dynamic control of AP operating frequency band (920 MHz, 2.4 GHz, 5 GHz) and wireless parameters
 (b) Terminal connection control: Dynamic control of terminal wireless-connection destination from the AP side between multiple APs and frequencies

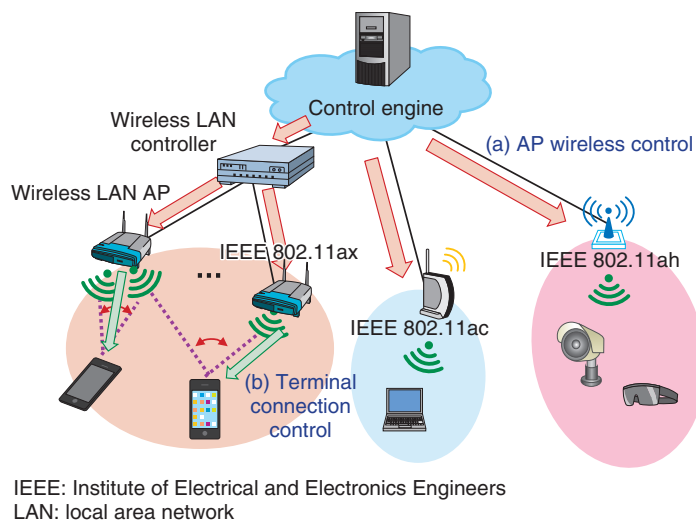


Fig. 1. Wireless resource control technology.

2. Introduction to high-efficiency Wi-Fi technologies

The following introduces high-efficiency Wi-Fi technologies for achieving a stable and high-quality Wi-Fi environment.

2.1 Wireless resource control technology

The wireless resource control technology derives an optimal combination of Wi-Fi parameters such as the operating frequency channel, bandwidth, and transmission power of each AP depending on the radio-interference conditions among multiple APs (**Fig. 1**) [1]. It derives, in particular, an optimal channel combination that avoids interference between APs through iterative optimization processing using a genetic algorithm. Carrying out this processing dynamically enables the parameters of each AP to be controlled in accordance with changes in the environment.

2.2 Wireless quality visualization technology

The wireless quality visualization technology estimates the degree of congestion under peripheral wireless conditions by listening to and analyzing control signals radiated in an area through the use of monitoring devices (boxes) installed at locations near APs or

users (terminals) [2]. This technology makes it possible to estimate the positions of transmitting/receiving terminals, issue alerts in the event of a sudden increase in traffic, and provide an operator with user-velocity information needed to clarify the cause of network instability (**Fig. 2**).

3. Demonstrations at venues

The opening event for the new Japan National Stadium was held in December 2019 immediately after completion of the structure. Filled to capacity with 64,000 spectators, the stadium hosted a program that included relay races by famous athletes and live performances by popular artists. During these activities, there were moments when images and video taken by spectators were simultaneously posted to SNSs or emailed throughout the world. Through this event, it was shown that 64,000 spectators could simultaneously make SNS postings without problems as an extension of their everyday life and that the communications infrastructure of the Japan National Stadium could provide stable and high-quality connections.

This opening event provided an ideal opportunity to determine changes in the wireless environment and shifts in traffic for an actual high-density gathering of

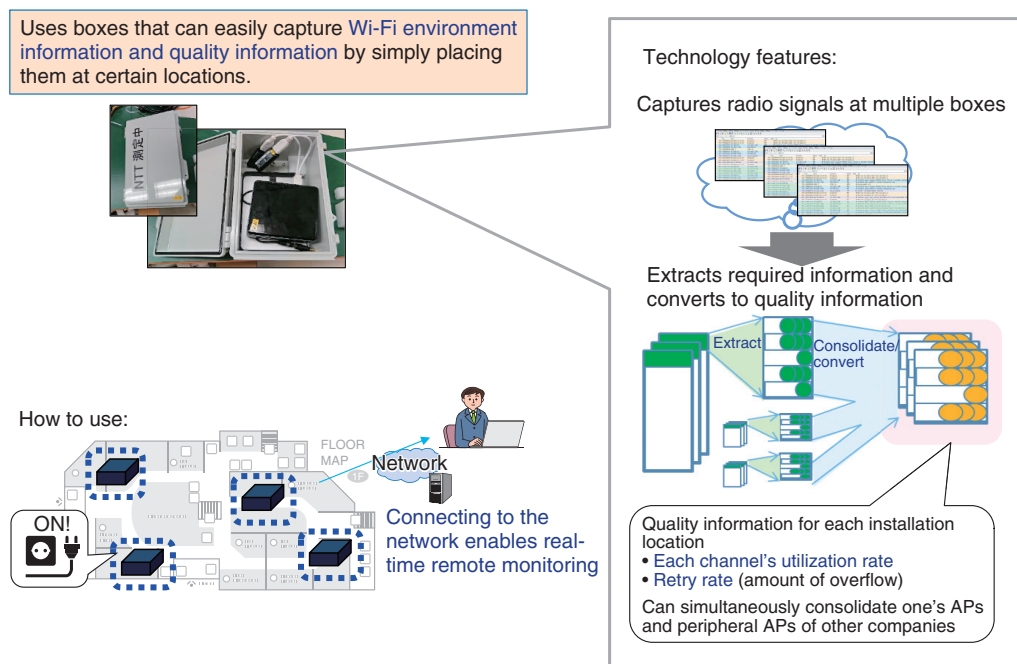


Fig. 2. Wireless quality visualization technology.

spectators. With the wireless quality visualization technology, the analysis of wireless-environment data that were collected widely and continuously confirmed that traffic could be accommodated without problem during peak traffic occurrences even from the viewpoint of data communications (Fig. 3). Analysis based on data collected using this technology clarified the effects of human-body shielding with respect to receiving radio waves in an environment closely packed with spectators (Fig. 4). It has been reported that the shielding and attenuation of radio waves by human bodies in a crowd of spectators in an environment such as the Japan National Stadium can affect wireless communications, but the magnitude of that effect has not been quantitatively clarified. These analysis results provided beneficial data for detailed designs of Wi-Fi parameters using the wireless resource control technology.

This opening event was the first large-scale event in the world to use the 5.2-GHz band, which had not been approved for outdoor use prior to the event. Japan, however, was a prime promoter of worldwide system revisions with respect to this band and achieved a revision of radio regulations allowing its outdoor use in November 2019 just in time for the opening event. As a result of this achievement, NTT received the 31st Radio Achievement Award of the

Minister of Internal Affairs and Communications from the Association of Radio Industries and Businesses.

With a view to the Olympic and Paralympic Games Tokyo 2020, there was a need for dividing channels into those for spectator use and those for management use at the same stadium. The aim was to ensure a stable level of communications quality for people related to the Tokyo 2020 Games and actual sports events even during the occurrence of large volumes of traffic generated by as many as 60,000 spectators. From the analysis results of the opening event, a test calculation of traffic volumes was conducted beforehand, and it was found that insufficient capacity would occur at an event on the scale of the Olympic Games if the number of available channels was limited [3] (Fig. 5). NTT's high-efficiency Wi-Fi technologies can dynamically derive an optimal combination of Wi-Fi parameters even with such a limited number of resources. The effectiveness of these technologies was recognized, and it was decided to provide them at the Japan National Stadium. Unfortunately, it was decided to hold the Tokyo 2020 Games without spectators, so Wi-Fi for spectators was switched off and these technologies were not used at the Japan National Stadium. However, they were used in the free Wi-Fi environment at the Tokyo

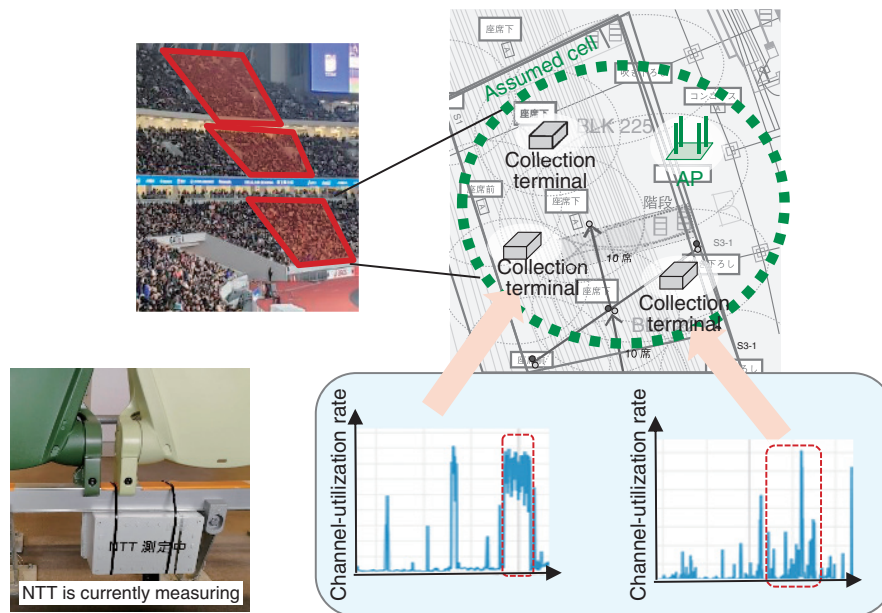


Fig. 3. Collection of wireless-environment information at opening event of Japan National Stadium using wireless quality visualization technology.

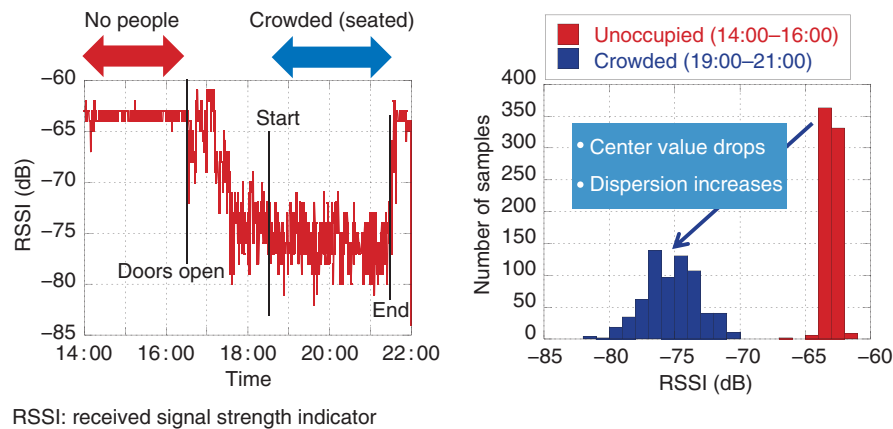


Fig. 4. Example of loss in receiving radio waves due to human-body shielding in a crowd of people.

Big Sight Aomi Exhibition Halls that became the showcase venue for sponsors of the Tokyo 2020 Games. It contributed to the provision of a stress-free wireless environment at this location.

4. Toward the future

At NTT, we have been researching and developing high-efficiency Wi-Fi technologies to optimize the network within a venue and provide stable through-

put with an eye to creating new viewing styles and new types of events. For example, these technologies will enable the flexible allocation of communication resources in accordance with network demand per unit area and the provision of flexible networks that can improve throughput at particular locations such as premium seating and press galleries.

These wireless technologies have been given the group name Cradio[®] [4], which we will continue to research and develop toward the implementation of

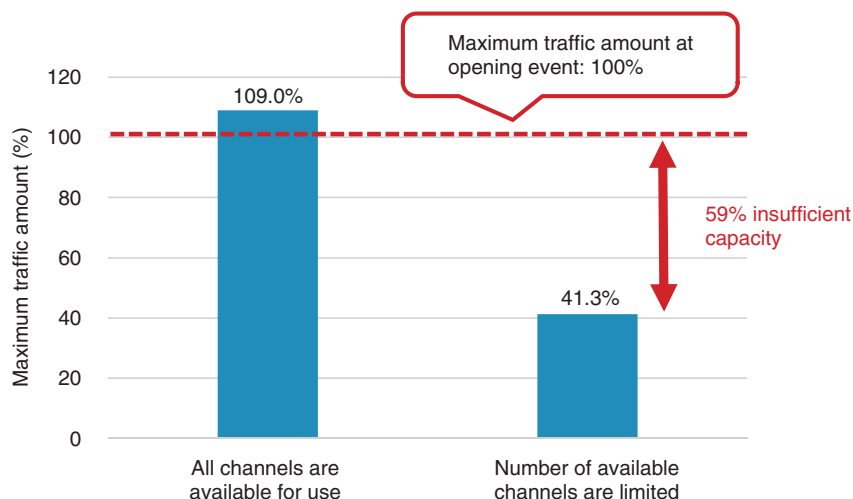


Fig. 5. Example of calculating throughput when available channels are limited.

the Innovative Optical and Wireless Network (IOWN) vision promoted by NTT.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

References

[1] NTT Access Network Service Systems Laboratories, “Technology for Efficiently Providing Optimal Wireless LANs,” ANSL R&D Times, Vol. 116, Aug. 2020 (in Japanese), <https://www.rd.ntt/as/times/116/04/top.html>

[2] NTT Access Network Service Systems Laboratories, “Development of Wireless Communication Environment Information Platform,” ANSL R&D Times, Vol. 111, Dec. 2019 (in Japanese), <https://www.rd.ntt/as/times/111/02/top.html>

[3] M. Sasaki, T. Nakahira, K. Wakao, and T. Moriyama, “Human Blockage Loss Characteristics of 5 GHz Wi-Fi Band in a Crowded Stadium,” IEEE Antennas and Wireless Propagation Letters, Vol. 20, No. 6, pp. 988–992, June 2021. doi: 10.1109/LAWP.2021.3069004

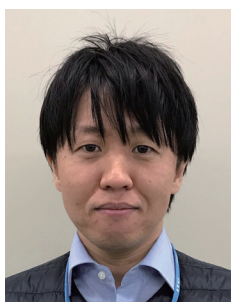
[4] M. Sasaki, T. Nakahira, T. Moriyama, T. Ogawa, Y. Asai, and Y. Takatori, “Multi-radio Proactive Control Technology (Cradio®): A Natural Communication Environment where Users Do Not Need to Be Aware of the Wireless Network,” NTT Technical Review, Vol. 19, No. 8, pp. 37–45, Aug. 2021. <https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202108ra1.html>



Toshiro Nakahira

Research Engineer, Wireless Access Systems Project, NTT Access Network Service Systems Laboratories.

He received a Bachelor of Maritime Safety from Japan Coast Guard Academy in 2009 and M.I. in informatics from Kyoto University in 2012. In 2012, he joined NTT Network Innovation Laboratories. He is now working at NTT Access Network Service Systems Laboratories. He received the Best Research Award of the fourth basic course workshop of the Institute of Electronics, Information and Communication Engineers (IEICE) Communication Quality in 2017 and the Young Engineer Award from IEICE in 2019. His recent research interests include natural area design and dynamic control techniques using multiple wireless access. He is a member of IEICE.



Motoharu Sasaki

Senior Research Engineer, Wireless Access Systems Project, NTT Access Network Service Systems Laboratories.

He received a B.E. in engineering and an M.E. and Ph.D. in information science and electrical engineering from Kyushu University, Fukuoka, in 2007, 2009, and 2015. In 2009, he joined NTT Access Network Service Systems Laboratories. He has been engaged in research on propagation modeling for various wireless communication systems; propagation modeling of interference between mobile terminals for spectrum sharing wireless access systems, propagation modeling in very high-frequency bands for emergency wireless systems, and propagation modeling in high frequency bands for 5G. He received the Young Researcher's Award and the Best Paper Award from IEICE in 2013 and 2014, respectively. He received the Best Paper Award at the International Symposium on Antennas and Propagation (ISAP) in 2016 and the Young Engineer Award from the Institute of Electrical and Electronics Engineers (IEEE) Antennas and Propagation Society Japan chapter in 2016. He also received the Young Researcher Award and the Excellent Paper Award from IEICE Technical Committee on Antennas and Propagation in 2012 and 2018, respectively. He is a member of IEEE.



Masayoshi Nabeshima

Research Engineer, Wireless Access Systems Project, NTT Access Network Service Systems Laboratories.

He received a B.E. and M.E. in electrical communication engineering from Waseda University, Tokyo, in 1992 and 1994. He joined NTT in 1994. His research interests include traffic analytics and visualization for wireless networks.



Tomoaki Ogawa

Senior Research Engineer, Supervisor, NTT Access Network Service Systems Laboratories.

He received a B.E. and M.E. from Keio University, Kanagawa, in 1996 and 1998. He joined NTT Wireless System Laboratories in 1998, where he has been engaged in the research and development of indoor location systems. His recent interest focuses on development of 6G wireless network technologies. He is a member of IEICE.



Takatsune Moriyama

Senior Research Engineer, Supervisor, NTT Access Network Service Systems Laboratories.

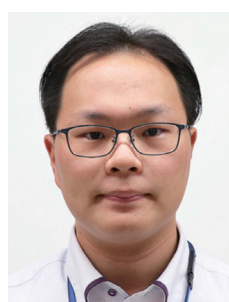
He received a B.E. and M.E. from Muroran Institute of Technology, Hokkaido, in 1991 and 1993. He joined NTT in 1993. From 1999 to June 2019, he worked at NTT Communications, where he was in charge of network service development and operation for corporate customers. He has been in his current position since July 2019.



Ken Hiraga

Senior Research Engineer, NTT Network Innovation Laboratories.

He received a B.E., M.E., and Ph.D. in electronics and information engineering from Hokkaido University in 2003, 2005, and 2013. Since 2005, he has been engaged in research and standardization on high-speed wireless systems at NTT. From 2018 to 2021, he was with NTT Broadband Platform Inc., where he designed radio coverage areas of commercial wireless local area networks. He is a member of IEEE and IEICE.



Kento Yoshizawa

Engineer, NTT Broadband Platform, Inc.

He received a B.E. and M.E. from Yokohama National University, Kanagawa, in 2014 and 2016. He joined NTT Network Innovation Laboratories in 2016. His research interests are high-reliable radio access system, large-capacity wireless backhaul, and overlapping and power saving technique for low power wide area radio systems. Since 2021, he has been affiliated with the wireless technology department in NTT Broadband Platform and engaged in the quality control of radio and development for radio access network system.



Ikutaro Ogushi

Senior Manager, NTT Broadband Platform, Inc.

He received a B.E. and M.E. in electrical engineering from Osaka University in 2000 and 2002. In 2002, he joined NTT Access Network Service Systems Laboratories. His research interests include research and development of an optical fiber line testing system for submarine cables and optical fiber distribution system for use in central offices. He is a member of IEICE. He has been in his current position since July 2019.

Network Security

Takashi Mishina, Akiko Matsuhashi, Takemi Nisase, and Hidehiro Shito

Abstract

Events that attract worldwide attention, such as the Olympic and Paralympic Games and international exhibitions, have become easy targets for cyber attacks, and it is no longer rare to hear of reports of damage from such attacks. The Olympic and Paralympic Games Tokyo 2020 was held in 2021 after a one-year delay due to the novel coronavirus (COVID-19), and NTT, as a Gold Partner (Telecommunications Services), had the responsibility of managing the network infrastructure supporting the Tokyo 2020 Games, thus dealing with the threat of cyber attacks. This article describes how NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team) of NTT Social Informatics Laboratories faced cyber attacks as the representative computer security incident response team of the NTT Group.

Keywords: information security, cyber attack, CSIRT

1. Olympic and Paralympic Games and cyber attacks

The Olympic and Paralympic Games is an international event with a long history. It attracts worldwide attention, therefore, it can become a target of many parties with a variety of malicious intentions. The event can be misused as a site for advancing political agendas, swindling money, or generating a loss of confidence in the host nation by inducing failure. The *modus operandi* of attackers having such malicious intentions have begun to spread to cyberspace beyond physical activities. In past Olympic and Paralympic Games, a variety of attacks having the potential of impacting their operations and management have been confirmed. These include disruptive acts caused by denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, the breaching of systems belonging to organizations related to the Games, and targeted attacks toward malware infections. To obtain results at a single international event, attackers have been watching for opportunities and refining their techniques. Organizations related to the Olympic and Paralympic Games must therefore implement extensive and reliable systems to protect the Games from such advanced attacks. As a Gold Partner (Telecom-

munications Services) of the Olympic and Paralympic Games Tokyo 2020, NTT had the important responsibility of managing the network infrastructure supporting the Tokyo 2020 Games, thus having to deal with the threat of cyber attacks. This article introduces the activities of NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team) of NTT Social Informatics Laboratories at the Olympic and Paralympic Games Tokyo 2020.

2. NTT-CERT activities at Olympic and Paralympic Games Tokyo 2020

NTT-CERT, a research group operating within NTT Social Informatics Laboratories, acts as the representative computer security incident response team (CSIRT) of the NTT Group (**Fig. 1**). NTT-CERT activities, which do not include the operation of equipment, have two major objectives: (i) collect information and share that information seamlessly with NTT Group companies to prevent cyber attacks from occurring, and (ii) provide support to minimize the damage caused by actual incidents and prevent their reoccurrence. NTT-CERT also feeds back the knowledge gained from such activities to research

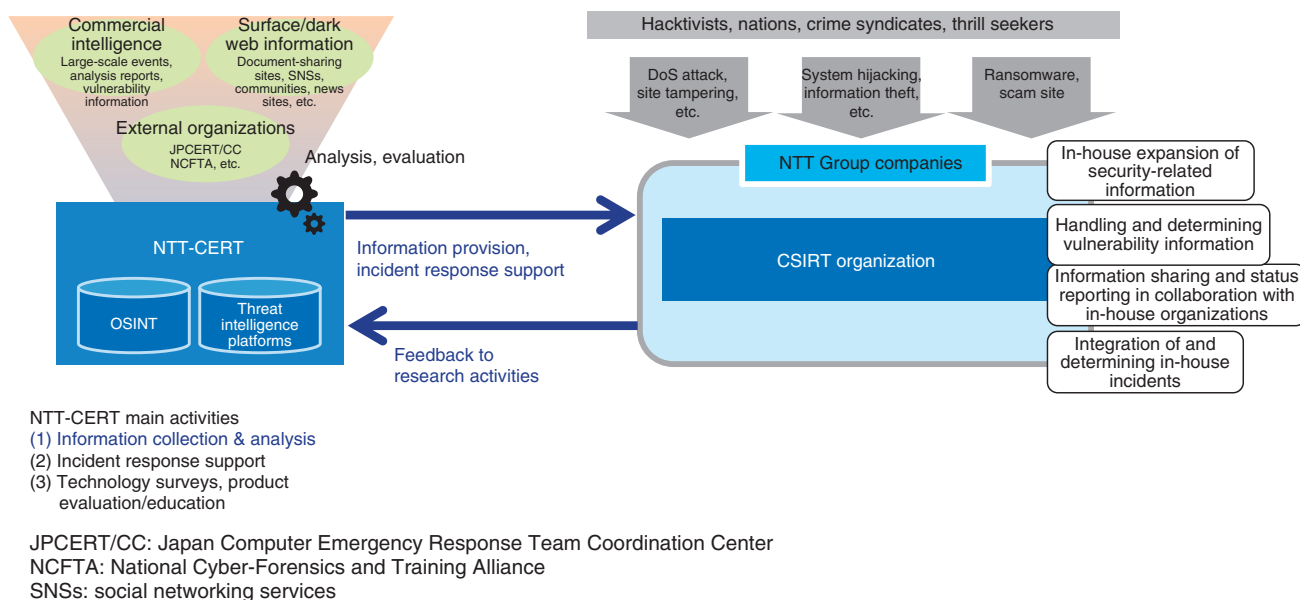


Fig. 1. Role of NTT-CERT.

activities and promotes research toward more advanced and robust security technologies.

As described above, the NTT Group had the responsibility of creating and maintaining a safe and secure network infrastructure in support of the Tokyo 2020 Games. Therefore, it was essential that NTT-CERT functions be enhanced to protect the NTT Group and network infrastructure from a diverse array of attackers from around the world. As an organization related to the Tokyo 2020 Games, we drafted a policy of preventing the possibility of a cyber attack before it occurs, and if an incident should occur, of minimizing any damage and impact on the Tokyo 2020 Games. We focused our efforts on enhancing our information collection and analysis functions.

Since NTT-CERT possesses no network facilities that it directly operates, the target of its information collection is mainly external open source intelligence (OSINT). However, collecting such a large volume of randomly arranged OSINT information would be nearly impossible no matter how many people are assigned to the task. We decided to prioritize the type of threat analysis to be conducted for the Tokyo 2020 Games and the information that should be collected. We analyzed cyber attacks that would seem likely to occur at the Tokyo 2020 Games by analyzing threats from the following four viewpoints: 1) What kind of attacker or organization using 2) what type of attack technique and having 3) what purpose would mount

an attack on 4) what attack target? On the basis of these four viewpoints, it became possible to organize information in terms of what attack target should be prioritized and protected by NTT-CERT and what information on attack techniques should be prioritized and detected, and on the whole, to classify with good efficiency the information that should be prioritized and collected. It was first necessary to list and analyze as many cyber attacks as possible that could occur at the Tokyo 2020 Games.

With this in mind, we began by collecting information on cyber attacks that occurred in the past. Ranging from the Olympic Games London 2012, during which full-fledged cyber attacks occurred, to the Olympic Winter Games PyeongChang 2018, during which targeted attacks were confirmed, we analyzed both Japanese and overseas news articles on past Olympic Games, reports issued by security vendors, etc. To obtain a comprehensive understanding of attacks that should be expected, we broadened our survey range to attacks that targeted personnel related to the Olympic Games and spectators and prepared a list of damages that occurred and damages that could be assumed. To carry out the threat analysis described above, we classified these data into “attacker,” “purpose,” “technique,” and “target.”

After using that list to determine “attacker,” “purpose,” and “technique” for which an attack could be detected from outside sources, NTT-CERT prioritized

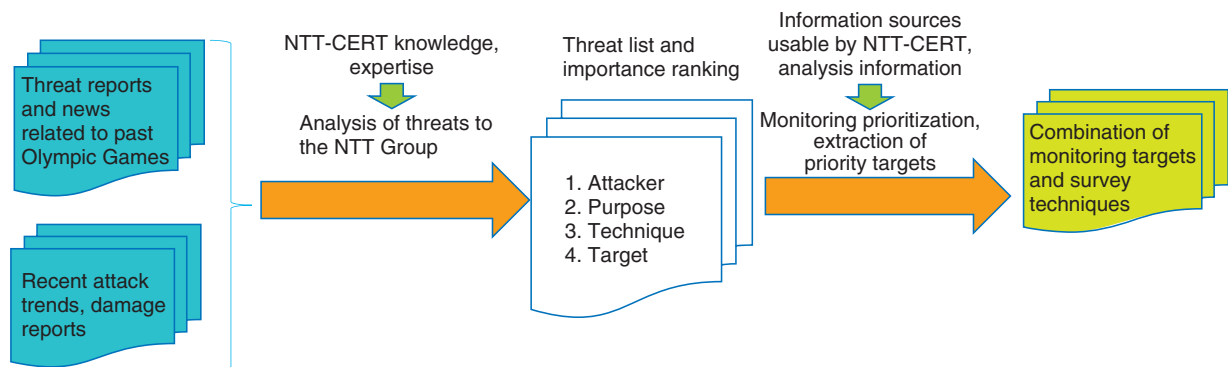


Fig. 2. Analysis toward enhanced monitoring.

the information that should be collected from the viewpoint of “target.” Specifically, attacks for which the NTT Group would be the direct attack target were set as top priority followed by attacks on personnel related to the Tokyo 2020 Games that could have an impact on the NTT Group and attacks on spectators in that order. “Technique” and “purpose” were prioritized on the basis of what NTT-CERT could detect from OSINT information. For example, while the threat level of a targeted mail attack targeting the NTT Group was high, it would be difficult to directly detect the receiving of such mail at NTT-CERT, so devoting resources there would be inefficient. We therefore studied how the NTT Group could be protected from such threats on the basis of information that could be detected from the outside. We considered, for example, detecting phishing sites having domains similar to those of NTT that might act as an inducement, determining whether stolen information is being sold on the dark web, and checking for the existence of hacktivists (persons engaged in hacking activities to advance their social or political agendas) who warn of politically oriented attacks. In short, we investigated a variety of attacks that could be detected from NTT-CERT’s position (**Fig. 2**).

After prioritizing the information that should be collected, the next step was to enhance the range and volume of information collection. Until recently, NTT-CERT’s main target of information collection had been the surface web as well as dark web information from intelligence vendors with survey languages being Japanese and English. However, as described above, it was considered insufficient to detect as much information as possible on information for sale on the dark web or on hacktivists’ agendas, so we used machine translation to add two survey

languages for which there were many past cases. Dark web surveys developed by NTT-CERT were also launched. Though we had been conducting surveys of domains similar to those of the NTT Group, we decided to simultaneously conduct surveys of domains similar to those of the Olympic and Paralympic Games Tokyo 2020 that were predicted to increase while the Tokyo 2020 Games were being held (including the preparatory period) and collected information on phishing sites in detected domains. These activities can be regarded as surveys that introduced new tools and applied accumulated knowledge as functional enhancements making use of research results in the automation of CSIRT functions.

No matter how much a single company’s functions can be enhanced through such efforts, there is a limit to how much information a company can collect. Therefore, NTT-CERT proactively shared information in collaboration with a variety of communities that it had thus far fostered. It participated, for example, in the Japan Cybersecurity Information Sharing Platform (JISP), an information-sharing tool of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), and the information sharing platform for the Olympic and Paralympic Games Tokyo 2020 set up by the ICT Information Sharing and Analysis Center (ICT-ISAC). These activities created a state in which NTT-CERT could access unreleased or original information. Collaboration with NTT Security’s Global Threat Intelligence Center also created a state of detailed information sharing from overseas sites with respect to cyber attacks on the Tokyo 2020 Games. This information obtained through such external collaborations was distributed to NTT Group companies along with additional surveys and analysis results from NTT-CERT. These efforts

Table 1. Monitoring results: Information sources and examples of detection results.

Information source	Information source details	Examples of detection results
Public organizations	JPCERT/CC, IPA, etc.	Vulnerability information, general attack information, etc.
SNSs	Twitter, blogs, message board	Posts encouraging attacks on Tokyo 2020 Games personnel, information on discovered phishing sites, etc.
News sites	Newspaper companies, broadcast stations, information technology-related news sites	News on fake sites posing as deliverers of Tokyo 2020 Games videos, news on cyber attacks on past Olympic Games-related organizations, articles on malware pretending to be Tokyo 2020 Games-related, etc.
Dark web	Hacker forums, black-market trading sites, etc.	Information on credential selling/buying thought to be Tokyo 2020 Games-related.
Fake site information	Domain abuse, Google search results, etc.	Information on new domains that can be mistaken as Tokyo 2020 Games-related (some of which are confirmed to be phishing sites)
Other	Manually prepared reports, vendor reports, etc.	Analysis information on assumed attackers, malware, etc.

could be seen as boosting the role of NTT-CERT as a hub between external organizations and the NTT Group.

To prepare for the discovery of information on vulnerabilities that could impact the network infrastructure and operating systems, NTT-CERT strengthened its vulnerability-information collection system as well as its test system for cases in which attack code came to be released.

Preparations for the activities described above were made right up to the beginning of the Tokyo 2020 Games, and cyber exercises were finally held within the NTT Group in anticipation of attacks. In these exercises, NTT-CERT was in charge of creating attack scenarios in which information on attacks presumed to have occurred or actually detected was to be shared within the NTT Group. Each company was to check their contact system and response procedure for any problems and confirm whether appropriate measures could be taken. Thus, the NTT Group worked together in its preparations for the opening of the Olympic and Paralympic Games Tokyo 2020.

3. Results of activities for the Olympic and Paralympic Games Tokyo 2020

As a result of the functional enhancements taken for the Tokyo 2020 Games, NTT-CERT collected and analyzed information from a variety of sources and passed on information for review to each company in the NTT Group (**Table 1**). In this information for review, NTT-CERT shared detection details that if ignored could allow an attack to gain a foothold, e.g., warnings of attacks due to growing geopolitical tensions in Southeast Asia and information on the buying and selling of credential information thought to

be related to the Tokyo 2020 Games, although no small-scale DDoS attacks or damage actually occurred. By repeatedly providing information in this manner, we were able to prevent major damage from being done and provide each company in the NTT Group with a feeling of security. It was reported after the Tokyo 2020 Games that Japan's National Police Agency had declared that "No Acts of Terrorism or Cyber Attacks Occurred during the Olympic and Paralympic Games" [1], which agreed with our detection results.

4. Comparison with past Olympic Games

The largest difference between the Tokyo 2020 Games and past Olympic Games is that most of the venues held events with no spectators due to the novel coronavirus (COVID-19) pandemic. It was probably for this reason that no sites selling fake tickets or cyber attacks on the venue admission system as seen in past Olympic Games were observed, and sites selling fake goods were likewise hardly seen. While DDoS attacks carried out by hacktivists as in past Olympic Games are regarded to be dangerous, there has recently been a drop in the frequency of such attacks that push a political agenda. There were also very few organizations in Japan that were greatly opposed to the Tokyo 2020 Games. We consider that this is why no DDoS attacks of this kind occurred.

In summary, the enhancing of NTT-CERT functions and nurturing of collaborations enabled the detection of information not previously available and, while small in scale, the sharing of information on a number of attacks that had the potential of gaining a foothold. The network infrastructure supporting the Tokyo 2020 Games suffered no incidents due to cyber

attacks and the closing ceremony was reached without problem. We feel that all of these results testify to the significance of our activities in protecting the Tokyo 2020 Games.

5. Future outlook

We consider that the threat analysis we conducted for the first time on cyber attacks against the Tokyo 2020 Games was effective. We feel that this threat analysis, which included related parties on the outside while considering the impact on the NTT Group and our ability to detect information and threats not previously detectable, should enable us to conduct flexible surveys on future large-scale events that the NTT Group will participate in as a provider of a network infrastructure. As an effort to strengthen NTT-CERT functions, we expanded our survey range by

increasing our survey languages and dark-web surveys, analyzing the actors involved in attacks, etc. Now that the Tokyo 2020 Games are over, we should be able to collect information of even higher quality by applying these achievements to our survey range in normal situations. Once this knowledge becomes formalized, it is our intention to distribute it to NTT Group companies to help improve the security of the entire NTT Group.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

Reference

- [1] The Sankei Shimbun news, Sept. 9, 2021 (in Japanese).
<https://www.sankei.com/article/20210909-KOK2GCDO3JK2LPIBAJOBHBRW6Y/>



Takashi Mishina

Research Engineer, Social Innovation Research Project, NTT Social Informatics Laboratories.

He joined NTT EAST in 2011 and engaged in network design, network operation, and system construction. He is currently with NTT Social Informatics Laboratories, where he is in charge of research and development (R&D) of information-leakage detection using intelligence services.



Takemi Nisase

Vice Director, Social Innovation Research Project, NTT Social Informatics Laboratories.

He joined NTT in 1987 and engaged in the R&D of an asynchronous transfer mode network service, OCN service, Next Generation Network service, etc. He joined NTT Security Platform Laboratories, where he was in charge of handling security incidents. He is currently with NTT Social Informatics Laboratories, where he is in charge of security incident response support and research on risk-analysis techniques.



Akiko Matsuhashi

Senior Research Engineer, Social Innovation Research Project, NTT Social Informatics Laboratories.

She joined NTT Communications in 2003 and engaged in the maintenance of web servers. In 2016, she joined NTT Security Platform Laboratories, where she was in charge of handling security incidents. She was also a member of the Tokyo Organising Committee of the Olympic and Paralympic Games from 2019 to 2021. She is currently with NTT Social Informatics Laboratories and engaged in NTT-CERT activities.



Hidehiro Shito

Director, Social Innovation Research Project, NTT Social Informatics Laboratories.

He received a B.E. and M.E. in mechanical and system engineering from Yamanashi University in 1994 and 1996. He joined NTT in 1997. After several years of experience in R&D, operation, and construction of communications infrastructure, he began his career as a member of CSIRTs at NTT EAST and NTT DATA. He joined NTT laboratories in 2018, and his current position is a director of NTT-CERT, the representative CSIRT of the NTT Group.

Report on ITU-T SG2 Standardization of Telecommunication Numbering

Koji Isshiki

Abstract

The Working Party (WP) 1 of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Study Group 2 has been engaged in the allocation and management of international telecommunication numbering, naming, addressing, and identification resources. Due to the recent migration to Internet Protocol networks and the rapid development and globalization of Internet-of-Things services and over-the-top services, the issues have been diversified. Since the problems of fraud by spoofing by telecommunication number misuse have increased, it has become an urgent topic for discussion. In the WP2, they discuss the issues concerning network management.

This article mainly reports on the telecommunication numbering and identifications studied in WP1, subjected by the World Telecommunication Standardization Assembly Resolutions.

Keywords: telecommunication numbering, IoT numbering, number spoofing

1. WTSA Resolutions on telecommunication numbering and identification

World Telecommunication Standardization Assembly (WTSA) is the primary meeting of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), and its output, WTSA Resolutions, give direction of the activities of ITU-T. Resolution 2 defines the responsibilities and obligations of each Study Group (SG) and the other Resolutions are materialized further and mapped to the studies in each SG. The following are the WTSA Resolutions relevant to telecommunication numbering and identifications discussed in SG2 Working Party (WP) 1 [1].

Extraction of WTSA Resolutions relevant to telecommunication numbering and identifications

- Resolution 20: Procedures for allocation and management of international telecommunication numbering, naming, addressing, and identification resources
- Resolution 29: Alternative calling procedures on

- international telecommunication networks
- Resolution 49: ENUM*
- Resolution 60: Responding to the challenges concerning the evolution of the identification/numbering system and its convergence with Internet Protocol (IP)-based systems/networks
- Resolution 61: Countering and combating misappropriation and misuse of international telecommunication numbering resources
- Resolution 64: IP address allocation and facilitating the transition to and deployment of IPv6
- Resolution 65: Calling party number delivery, calling line identification, and origin identification information
- Resolution 70: Telecommunication/information and communication technology accessibility for persons with disabilities
- Resolution 88: International mobile roaming
- Resolution 91: Enhancing access to an electronic repository of information on numbering plans

* ENUM: E.164 Number Mapping; the framework of mapping of IP address and telecommunication number.

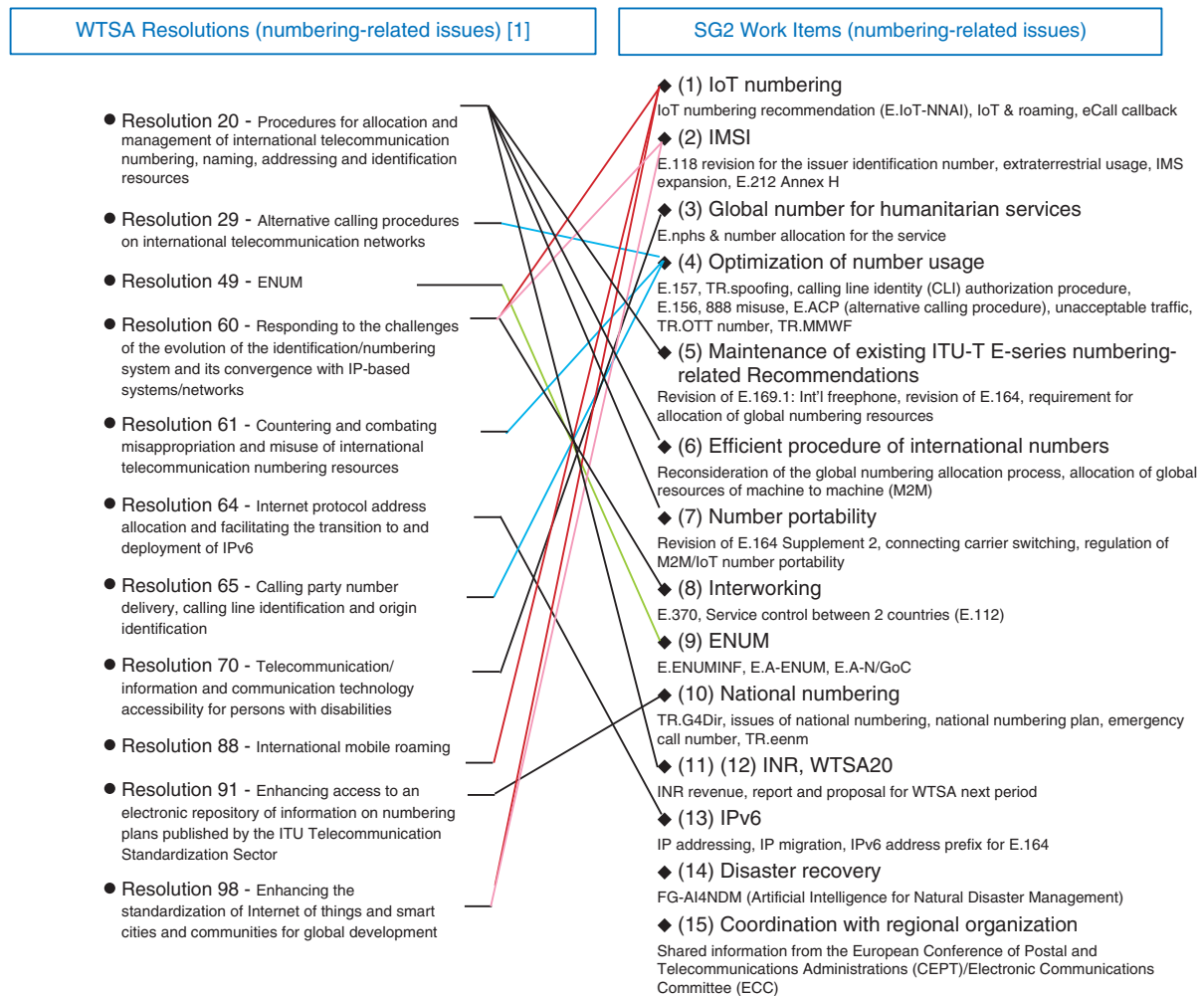


Fig. 1. Mapping of SG2 studies and WTSA Resolutions.

published by the ITU-T

- Resolution 98: Enhancing the standardization of Internet of Things (IoT) and smart cities and communities for global development

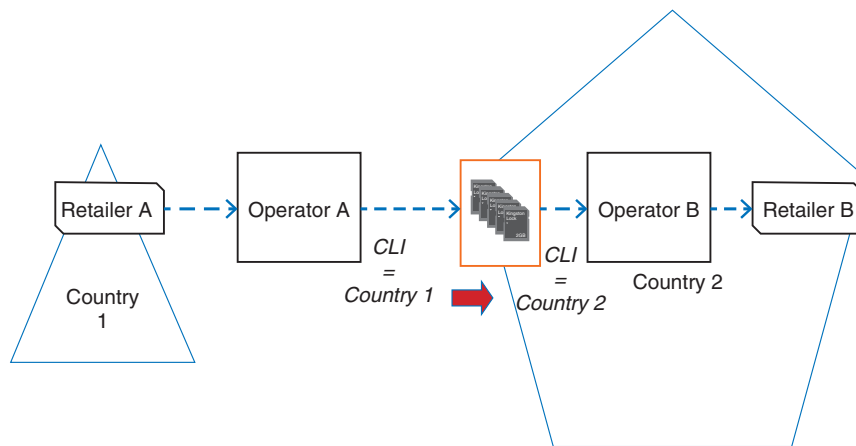
2. Issues under study in SG2 WP1

Issues with telecommunication numbers and identifications under study in ITU-T SG2 WP1 are diversifying and categorized into items (1) to (15) listed in the next subsection. **Figure 1** shows the subdivision of these individual issues and their relation to the WTSA Resolutions. The issues concerning (1) the allocation of international numbers for IoT and (4) the status of optimizing the use of numbers that are actively discussed are introduced in Section 3. Section 4 presents a list of the recommendations, includ-

ing some drafts, based on the studies of the issues.

Categorization of the studies in SG2

(1) Allocation of IoT international numbers, (2) Allocation of international mobile subscriber identity (IMSI) for mobile subscriber identification, (3) Global number for humanitarian services, (4) Optimization of number usage, (5) Maintenance of existing ITU-T E-series numbering-related Recommendations, (6) Efficient procedure of international numbers, (7) Number portability, (8) International interworking, (9) ENUM, (10) Issues with national numbering, (11) Revenue from International Numbering Resources (INR), (12) Input to WTSA20, (13) IPv6, (14) Disaster recovery, (15) Coordination with regional organization.



Note: Example of falsification of international call charges
The calling number (CLI): Country 1 is replaced with Country 2 by SIM box etc. between the origination country (Country 1) and termination country (Country 2).

Fig. 2. Example of number spoofing during an international call (referred from TR.spoofting).

3. Active issues

Even though the issues are diversifying due to the recent migration to IP networks and the rapid development and globalization of IoT and over-the-top (OTT) services, the items actively discussed most for standardization are the studies on the proper use of telecommunication numbers. The issues with IoT numbering have also been high priority for discussion. The status of the two studies are introduced on the basis of the results from the 9th meeting held from May 31 to June 11, 2021.

3.1 Optimization of number usage

The items being actively discussed most for standardization are the studies on the proper use of telecommunication numbers.

3.1.1 Approval of the revised recommendation (E.157): International calling party number delivery

Since the background has enhanced to include the services on the Internet and OTT, which are beyond the current basis of public switched telephone networks and public land mobile networks, the discussion regarding the revised E.157: International calling party number delivery in the meeting has diversified due to the opinions regarding scope, level of details, degree of obligation, etc. The editor of the UK then elaborated to coordinate the group and brought the solution with agreement to edit the recommenda-

tion, i.e., removing the section of preventing individual cases of spoofing to the separate technical report based on the general principles.

3.1.2 Consent of TR.spoofting

As mentioned in 3.1.1, countering spoofing is a new item separated from E.157 describing the methods of preventing individual cases of spoofing. It covers the mechanism of number spoofing caused by SIM (subscriber identification module) boxes etc., internationally carried out by OTT operators, and STIR/SHAKEN (Secure Telephony Identity Revisited/Signature-based Handling of Asserted Information Using Tokens), which is being introduced in the United States as a countermeasure against number spoofing, including comparison with blockchain technology etc. **Figure 2** shows an example of number spoofing in international communications.

3.1.3 Discussion on creation of technical report on Wangiri

Sudan proposed a new Work Item to create a technical report on methodologies to mitigate Wangiri fraud (i.e., a callback scam). The proposal was approved to create a new Work Item of TR.MMWF (methodologies to mitigate Wangiri fraud). Interactive voice response facility, using artificial intelligence technology, number blocking, and sharing of blacklists are being introduced for the technological method to mitigate Wangiri and number administration.

3.1.4 Discussion on OTT

As a fraudulent case associated with the use of

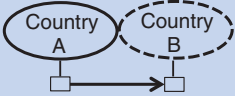
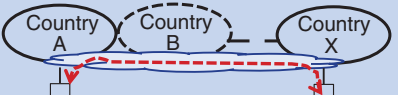
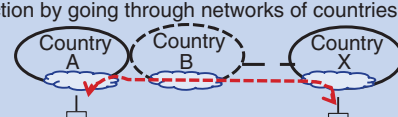
	Geographic number	Non-geographic number
Allocation	ITU to National Regulatory	Directly from ITU to service providers
Structure	Country code + national number (Ex. Japan 81+ national number)	1. International network number (ex. 883 (international network number) + subscriber number) 2. International service number ➔The direction to apply for IoT numbering (ex. 878 (UPT number) + subscriber number)
Network structure & routing image	 <ul style="list-style-type: none"> • For temporary international roaming • Permanent use in other countries is out of scope (extra-terrestrial use) 	  <p>1. International network number Connection with a network through countries</p> <p>2. International service number Connection by going through networks of countries</p>

Fig. 3. International numbers for IoT services.

E.164 numbers for OTT services that are deployed on the Internet, the UAE proposed to start studying countermeasures for cases in which mobile numbers and fixed numbers are used to authenticate and launch apps such as WhatsApp. It was agreed to contact the OTT application provider through the ITU Telecommunication Standardization Bureau (TSB) regarding this issue. In addition, the United States proposed to encourage WhatsApp to participate in future discussions on this matter.

3.2 Standardization of allocation of IoT international numbers

3.2.1 Background of studies on IoT numbering recommendation: E.IoT-NNAI (naming numbering addressing and identifiers)

This issue started with the UK editor as one of the major issues for this study period for the study to assign appropriate international numbers in response to the rapid increase in global IoT services.

Initially, the eCall service, which is standardizing emergency calls within Europe, is specified as a use case, and it was decided to be used as part of the international service number (E.164-number for global services) applied to universal personal telecommunication (UPT) services. It is regarded that the 878 number allocated for the global mobility services as

UPT services will be appropriate usage for IoT since the usage of the number is currently still low. However, the roaming of the existing national mobile number (E.164-number for geographic areas) and international network numbers (E.164-number for networks), such as 883, have been applied for currently deployed eCall and other various global IoT services, while the studies of IoT numbers continue. Such difference in number usage also needs discussion. **Figure 3** illustrates the IoT international numbers.

3.2.2 Draft recommendation of E.IoT-NNAI at the 9th meeting

At the 9th meeting, the following contributions were input, and the discussion will continue on the basis of the draft reflecting the inputs.

- NTT proposed Annex-A in the draft recommendation describing the number portability of IoT services. The proposal was agreed, and the studies of carrier switching of service providers will start with this draft for the next meeting.
- Malta proposed to include that the IoT number 878 should not be used for existing voice and short messaging services in the E.IoT-NNAI Recommendation, and it was decided to proceed with further studies.
- Russia proposed a list of issues such as definition

Table 1. ITU-T SG2 Recommendations and relevant WTSA Resolutions.

Recommendation number	Recommendation title	Relevant WTSA Resolutions
E.112	Arrangements to be made for controlling the telephone services between two countries	Resolution 60
E.118	The international telecommunications charge card	Resolution 60, 98
E.157	International calling party number delivery	Resolution 29, 61, 65
E.164.1	Criteria and procedures for the reservation, assignment, and reclamation of E.164 country codes and associated identification codes	Resolution 20
E.370	Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks	Resolution 60
TR.disab	Specification of an international numbering resource for use in the provisioning of services for persons with disabilities and persons with specific needs	Resolution 70
E.nphs	Application of E.164 numbering plan for humanitarian services	Resolution 70
E.dit	Deemed impermissible traffic	Resolution 29, 61, 65
E.IOT-NNAI	IoT naming numbering addressing and identifiers	Resolution 60, 98
E.164 Sup.2	Number portability	Resolution 20
TR.EENM	Guidelines for effective and efficient national numbering resources administration	Resolution 91
TR.Spoofing	Countering spoofing	Resolution 29, 61, 65
TR.MMWF	Methodologies to mitigate Wangiri fraud	Resolution 61
TR.OTTnum	Current use of E.164 numbers as identifiers for OTTs	Resolution 61, 65
E.ACP	Alternative calling procedures	Resolution 29
E.ENUMINF	Differentiating between ENUM and infrastructure ENUM	Resolution 49
TR ERIN	Guidance for the Director TSB as stated in Resolution 91 (Hammamet 2016) "Enhancing access to an electronic repository of information on numbering plans published by the ITU Telecommunication Standardization Sector"	Resolution 91
TR.INCCBS	Implementation of network colour codes in the border sites	Resolution 61
TR.DOTT	Definitions for telecom and telecom interconnection	Resolution 60
E.A-ENUM	Principles and procedures for the administration of E.164 country codes for registration into the domain name system	Resolution 49
E.A-N/GoC	Administrative procedures for ENUM for E.164 country codes and associated identification codes (ICs) for networks and group identification codes (GICs) for groups of countries	Resolution 49

of terms, regulation of each field of IoT numberings, number portability, and global/domestic role of number management, and it was decided to proceed with further examination.

4. Recommendation of the output of the studies

Table 1 lists the recommendations that will be the output of the examination of various issues introduced in Section 2. The WTSA Resolutions associated with each recommendation are also listed.

5. Conclusion

Along with the development of telecommunication

services and changes in network formats, the roles of numbers and identifiers are changing, and SG2 has a variety of activities from short-term issues that require immediate response to medium- to long-term issues. While observing these trends, we will continue to engage actively in activities such as standardization activities related to numbers and identifiers with discussions at the TTC (Telecommunication Technology Committee) Numbering Planning Expert Committee in Japan.

Reference

- [1] WTSA Resolutions of ITU-T, <https://www.itu.int/pub/T-RES>

**Koji Isshiki**

Professional Staff, Network Innovation Business Headquarters, NTT Advanced Technology Corporation.

He joined NTT Advanced Technology Corporation in 2001 after he had engaged in the research and development of voice and data switching systems at research section, business section, and international business section in NTT. Since then he has been engaged in the investigation and standardization of telecommunication numbers and related technologies by attending ITU-T SG2, Internet Engineering Task Force, European Telecommunications Standards Institute (ETSI), Third Generation Partnership Project (3GPP), and CEPT ECC Working Group Numbering and Networks, and by visiting number NRAs (national regulatory authorities) in the US and European countries every year.

External Awards

EuroUSEC 2021 Best Paper Award

Winners: Tenga Matsuura, Waseda University; Ayako A. Hasegawa, Mitsuaki Akiyama, NTT Social Informatics Laboratories; Tatsuya Mori, Waseda University/NICT/RIKEN AIP

Date: October 11, 2021

Organization: The European Symposium on Usable Security (EuroUSEC)

For “Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods.”

Published as: T. Matsuura, A. A. Hasegawa, M. Akiyama, and T. Mori, “Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods,” EuroUSEC 2021, Oct. 2021.

Outstanding Reviewer Award (Top 10%)

Winner: Shiro Kumano, NTT Communication Science Laboratories

Date: October 27, 2021

Organization: The 23rd ACM International Conference on Multimodal Interaction (ICMI 2021)

CSS2021 Best Paper Award

Winners: Kazuki Nomoto, Waseda University; Mitsuaki Akiyama, NTT Social Informatics Laboratories; Masashi Eto, Ministry of Internal Affairs and Communications; Atsuo Inomata, Osaka University; Tatsuya Mori, Waseda University/NICT

Date: October 28, 2021

Organization: Information Processing Society of Japan (IPSJ)

For “Understanding the Risks of Re-identification Attack on the Contact Tracing Frameworks and Its Countermeasures.”

Published as: K. Nomoto, M. Akiyama, M. Eto, A. Inomata, and T. Mori, “Understanding the Risks of Re-identification Attack on the Contact Tracing Frameworks and Its Countermeasures,” Computer Security Symposium (CSS) 2021, Oct. 2021.

CSS2021 Outstanding Paper Award / MWS2021 Outstanding Paper Award

Winners: Toshinori Usui, NTT Social Informatics Laboratories/

Institute of Industrial Science, The University of Tokyo; Tomonori Ikuse, Yuhei Kawakoya, Makoto Iwamura, NTT Social Informatics Laboratories; Kanta Matsuura, Institute of Industrial Science, The University of Tokyo

Date: October 28, 2021

Organization: IPSJ

For “Automatically Appending Execution Stall/Stop Prevention to Vanilla Script Engines.”

Published as: T. Usui, T. Ikuse, Y. Kawakoya, M. Iwamura, and K. Matsuura, “Automatically Appending Execution Stall/Stop Prevention to Vanilla Script Engines,” CSS2021, Oct. 2021.

CSS2021 Encouragement Award

Winners: Shu Aakabane, Kanagawa Institute of Technology; Yuhei Kawakoya, Makoto Iwamura, NTT Social Informatics Laboratories; Takeshi Okamoto, Kanagawa Institute of Technology

Date: October 28, 2021

Organization: IPSJ

For “Identifying Library Function Names Based on Function Dependencies and Linking Ordering in IoT Malware.”

Published as: S. Aakabane, Y. Kawakoya, M. Iwamura, and T. Okamoto, “Identifying Library Function Names Based on Function Dependencies and Linking Ordering in IoT Malware,” CSS2021, Oct. 2021.

CSS2021 Encouragement Award

Winners: Toshiki Shibahara, Takayuki Miura, Masanobu Kii, Atsunori Ichikawa, NTT Social Informatics Laboratories

Date: October 28, 2021

Organization: IPSJ

For “Privacy Risk of Differentially Private Bayesian Neural Network.”

Published as: T. Shibahara, T. Miura, M. Kii, and A. Ichikawa, “Privacy Risk of Differentially Private Bayesian Neural Network,” CSS2021, Oct. 2021.

Papers Published in Technical Journals and Conference Proceedings

Computational Self-testing for Entangled Magic States

A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, and S. Tani
arXiv:2111.02700, November 2021.

In the seminal paper [Metger and Vidick, Quantum ’21], they proposed a computational self-testing protocol for Bell states in a single quantum device. Their protocol relies on the fact that the target

states are stabilizer states, and hence it is highly non-trivial to reveal whether the other class of quantum states, *non-stabilizer states*, can be self-tested within their framework. Among non-stabilizer states, magic states are indispensable resources for universal quantum computation. In this letter, we show that a magic state for the *CCZ* gate can be self-tested while that for the *T* gate cannot. Our result is appli-

cable to a proof of quantumness, where we can classically verify whether a quantum device generates a quantum state having non-zero magic.
