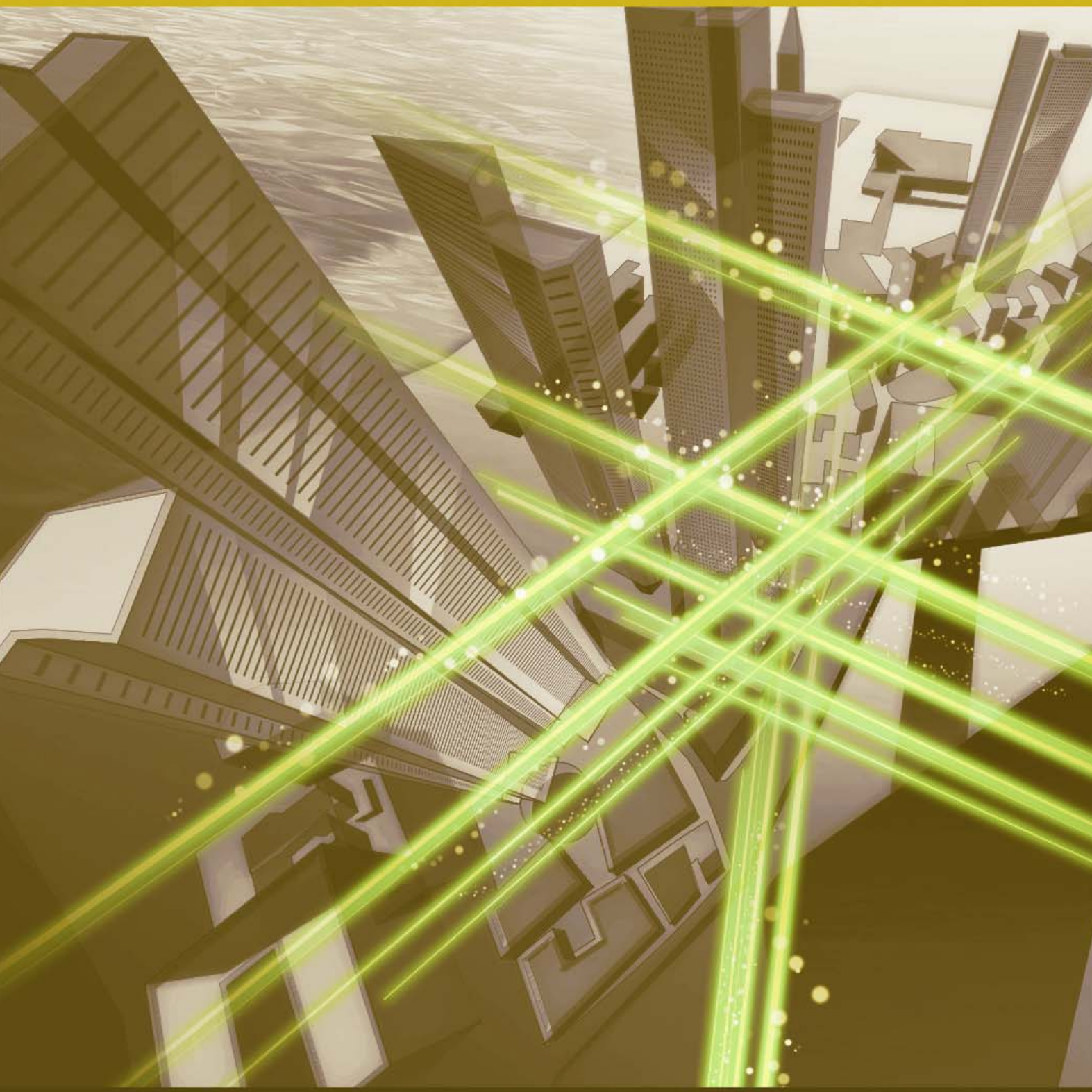
NTT Technical Review

7
2023



July 2023 Vol. 21 No. 7

NTT Technical Review

July 2023 Vol. 21 No. 7

Ongoing Pursuit to Becoming a Company That Is Useful to Society and Close to Our Customers

Riaki Hoshino
Senior Executive Vice President, NTT EAST

Abstract

NTT EAST strives to connect with the communities in which it operates and to build circular communities that can develop sustainably. This initiative has been accompanied by efforts for further strengthening the resilience of telecommunication networks to counter new threats such as escalating natural disasters and increasingly sophisticated cyber-attacks, and improving its crisis-management and mobility capabilities to provide a high-quality and stable telecommunication infrastructure. We asked Riaki Hoshino, senior executive vice president of NTT EAST, about the company's initiatives and his beliefs as a top executive.

Keywords: circular communities, digital transformation, regional revitalization

NTT EAST: A social innovation company supporting the future of regional communities

—It has been almost a year since you were appointed senior executive vice president. What has the year been like?

It's been a year in which I'm convinced that we still have much to do, and it has renewed my determination to channel the passion of our employees into energy for action and challenge ourselves to meet the needs of our customers.

Since the reorganization of Nippon Telegraph and Telephone Corporation in 1999, I have been with NTT EAST with the exception of a brief stint at the holding company, NTT Corporation. As a senior executive vice president of NTT EAST, I have taken a fresh look at the ability of the company, its technological capabilities, and the passion of its employees for contributing to society, and realized that the ability of the company and the range of expectations that our customers put on us are far greater than I had imagined.

NTT EAST's service area includes both the Tokyo metropolitan area and the surrounding rural areas. Each region faces unique challenges—for example, the Tokyo metropolitan area is dealing with a large number of residents, while in contrast, the surrounding rural areas are faced with declining populations. Against this background, NTT EAST has launched initiatives designed to improve the telecommunication infrastructure and implement disaster countermeasures, and we've also been exploring new possibilities in the fields of culture and agriculture. As a result of these initiatives, we have received numerous comments and inquiries from customers, such as "We want our employees to fully understand the significance of digital transformation (DX), and we want to use DX to solve problems. Could you help us do that?" Over the past year, as I have listened to the

needs of our customers, I have become convinced that our mission, which was initially to connect telecommunications, should further expand to connect people and to play a role in connecting and developing communities for the next generation.

—So you want to connect people and communities. Would you tell us specifically what direction NTT EAST is aiming for?

Generally speaking, the main managerial objective of a company has been to maximize profits; however, recently, companies are also expected to make further contributions to society. NTT EAST aims to become a "social innovation company that supports the future of regional communities" in a manner that creates sustainable new value and solves problems. With that aim in mind, we are striving to "rediscover value in communities" and "build circular communities" by "implementing empathetic DX consulting" and "strengthening our field-engineering capabilities."

Unlike the conventional approach, namely, analyzing customer's problems, making proposals to address the problems, and implementing the proposals, empathetic DX consulting involves coming face-to-face with customers in a community, getting closer to the community, and pondering solutions to problems together in an empathetic manner. We then try to solve problems by implementing a solution with them through trial and error. In this manner, we can refine a management style that is unique to NTT EAST as a community-based company.

Regarding strengthening our field-engineering capabilities, we intend to expand and strengthen our comprehensive engineering capabilities on the basis of our technical capabilities cultivated in the information and telecommunication field to create real value in the actual field. This is essential when it comes to fostering industries, passing on culture to the next generation, and creating the eco-friendly towns that are necessary for creating value in communities.

Aiming to accelerate regional revitalization, we

will create new value by making use of local assets and attractions such as culture, cuisine, and nature. In January 2023, with the aim of creating a society in which regional communities can develop sustainably and feel dreams and hopes, we established the Regional Circular Future Lab, which is engaged in creating value and building a circular society in communities. If I had to describe these initiatives in a few words, I would say we are "getting closer to our customers."

Creating a decentralized network society with IOWN and the REIWA project

—You will be able to apply the knowledge you have cultivated in addressing local issues, such as the expansion of optical broadband services and digital solutions, right?

When I envision the future of Japan, I think we should take advantage of our strengths in telecommunication networks. For example, I want us to not only emphasize efficiency by concentrating the population in urban areas but also achieve both diversity and efficiency by dispersing it to different regions. The Innovative Optical and Wireless Network (IOWN) being advocated by the NTT Group and the REIWA project promoted by NTT EAST will be keys to achieving this goal.

IOWN uses photonics-based technology to address issues such as the significant increase in data volume, power consumption, and communication delays due to the expansion of the Internet of Things (IoT) and the diversification of services. As a key element of IOWN, we are conducting various research and development activities to implement the All-Photonics Network (APN). Compared to conventional

electronics-based communication networks, the APN will have a 125-times-higher transmission capacity, 1/200 end-to-end delay, and 100-times-higher power efficiency. In March 2023, we launched APN IOWN1.0 as our first APN service. APN IOWN1.0 can be used in scenarios that require ultralow latency, such as remote ensembles, remote lessons, e-sports, remote production, remote operation of equipment such as experimental measurement equipment, and close coordination between datacenters. We are constantly working with customers to create new usage scenarios.

Under the REIWA project, we have begun offering a cloud service called "Regional Edge Cloud," which utilizes about 1,000 telecommunication central offices (of the approximately 3,000 located in the 17 prefectures in NTT EAST's service area) as datacenters and uses them as regional edge-computing points with the aim of creating new value. We are building a cloud-based information and communication technology (ICT) infrastructure by leveraging all of our assets to connect regional edge-computing points over a wide area via a network, and we are providing various functions in a shared service model through a video-analysis artificial intelligence platform, IoT platform, "Regional Revitalization Cloud," and data lake.

With the aim of making this ICT infrastructure more widely available, we have set up "Smart Innovation Labs" in Tokyo, Hokkaido, and Miyagi as test environments, in which people from industry, academia, and the government are working together to create new services and businesses.

In this way, we hope to support society through initiatives that circulate energy and human resources by utilizing our telecommunication technology, assets, and expertise for the benefit of regional communities.

—I have heard that NTT EAST is undertaking various other changes and challenges.

We are refining our existing businesses and taking on the challenge of creating new business. Examples of specific initiatives include (i) efforts to promote efficiency while improving facilities and service quality in the telecommunications field and (ii) the launch of a software business. To meet the social demand for more convenient and stable services, we are steadily migrating the public switched telephone network (PSTN) to Internet protocol (IP) networks, and upgrading network functions and renewing facilities to connect with IOWN while obtaining third-party assessment. We are proactively using DX technology in network construction and operations, thus reducing labor for work coordination and achieving automation of operations. These efforts have not only significantly curtailed work hours but also contributed greatly to improving reliability by reducing human involvement to eliminate human errors. We are also promoting customer self-service by using web technology and implementing operations utilizing remote environments, and these efforts are improving customer satisfaction and efficiency while strengthening our emergency-response capabilities in the event of natural disasters by securing different means of operations.

The purpose of the launch of our software business

is to develop new business in the non-telecommunications field. By undertaking system development in-house, we aim to accumulate our own software-development technology and nurture DX-related human resources by promoting DX. Naturally, we also aim to reduce system-development costs. During these efforts, we have focused on low-code development, which does not require advanced or specialized skills, and launched the In-house Software Development Promotion Project in April 2022. We also implemented offshore low-code development. At present, we have already achieved promising results concerning the renewal of internal business systems and the development of new ones, and we are preparing for future business development. We have also set up a private cloud that uses virtualization and a hybrid environment with a public cloud as an infrastructure to be used for software development inside and outside the company.

If we keep challenges within the limits of what we can do, our growth will remain within those limits

—What is important to you in your work?

The two main things are the attitude to challenge myself and the desire to achieve goals. Simply dealing with what is in front of me will not lead to the next step. I ask myself what I want to gain from this job and how I can make the most of it. I ask the same questions of our employees and learn from their stories. Hearing the passion of our employees gives me so much energy. I then try to convey that passion to others. I believe it is my responsibility as senior executive vice president to keep that positive energy circulating.

Ever since I first joined the company and was engaged in the maintenance of telecommunication equipment in the field, I have experienced the passion of the field in many different workplace environments. During the recovery efforts after the Great East Japan Earthquake, I realized the importance of giving instructions to employees who were desperately working hard, even though the future was uncertain, so that they could better see what lies ahead. Through these many experiences, I have realized the importance of setting goals for things that should be done rather than things that can be done, clearly communicating what must be done and why changes are necessary, and clarifying the goals to be achieved.

Taking on challenges can sometimes be scary. Even so, if we keep challenges within the limits of what we can do, our growth will remain within those limits. If the challenge involves risk, I believe it is possible to bring out the latent ability of our employees by showing them the risk and leading them to change. It is important as top management to set higher goals that will motivate employees to take on challenges.

—It gives us hope that we will be able to demonstrate abilities that we never thought we had. Finally, please say a few words to researchers, engineers, customers, and partners.

Sometimes the workload we give our employees is heavier—or lighter—than we thought it would be. The influence of the employee's personality and their surrounding environment may be unpredictable when the work is allocated. For example, an employee may behave in unexpected ways when the workload is too heavy, or when there is (or is not) adequate support available. The situation inevitably varies depending on the individual. Accordingly, I believe that instead of just handing over the work and being done with it, the job of the top management is to monitor people's situations and improve their work environment as necessary. As with any other endeavor, it is important to pursue work persistently and not to neglect the adjustment to the environment.

When we take on challenges as a social innovation company, there are certain issues that cannot be handled with our current technology. I therefore want to bring together the strengths of our research laboratories and group companies to create a sustainable society. We are committed to being a company that is useful to society and close to our customers, and we're counting on those at our laboratories and group companies for their help with this endeavor.

We serve a wide variety of customers, including users of our services, wholesale network providers, and Internet service providers. We will respond to customer's requests with sincerity, and if we are not able to provide requested services at the time, we will improve quality and introduce new technologies so that we can create appropriate services while keeping costs in mind. Our aim is to become a company that listens carefully to the voices of our customers. We look forward to your cooperation in achieving this aim.

Interviewee profile

■ Career highlights

Riaki Hoshino joined Nippon Telegraph and Telephone Corporation in 1990 and became a member of the Board of Directors of NTT EAST Corporation in 2018, president and representative director of NTT-ME Corporation in 2020, and senior executive manager of NTT EAST Network Business Headquarters and president and representative director of NTT e-Drone Technology in 2022. He assumed his current position in June 2022.

Science and Technology Are the Collective Wisdom of Our Predecessors. It Is Our Mission—the Researchers of Today—to Make Them Even Better

Hirokazu Kameoka
Senior Distinguished Researcher, NTT Communication Science Laboratories

Abstract

People have various feelings and discomforts related to speech as typified by comments such as "The voice of a cartoon character differs from what I imagined," "I'm not confident speaking owing to my stuttering," and "I want to regain my voice that I lost due to illness or injury." Hirokazu Kameoka, a senior distinguished researcher at NTT Communication Science Laboratories, aims to create an environment in which all people can communicate comfortably by removing various barriers in communication through signal-processing and machine-learning technologies, which are key elements of artificial intelligence. We interviewed him about the progress in his research and what he enjoys most about his research activities.

Keywords: voice conversion, sound-source separation, crossmodal signal generation

Pursuing crossmodal signal-generation technology to augment communication functions

—This is our second interview with you. Can you tell us about the research you are conducting?

In our daily communication with others, we may be unable to speak as we wish due to physical barriers caused by disabilities, aging, or other factors; skill constraints, such as inability to speak foreign languages; and psychological barriers such as nervousness. I'm engaged in the development of signal-processing and machine-learning technologies to overcome these various forms of barriers and constraints concerning communication.

Communication involves a sender and receiver, and my aim is to build a system that converts the signals sent by the sender into expressions appropriate to the situation in real time in a manner that enables messages to be sent and received as desired by each party. Sound-source-separation technique, which complements the auditory function of the receiver, and

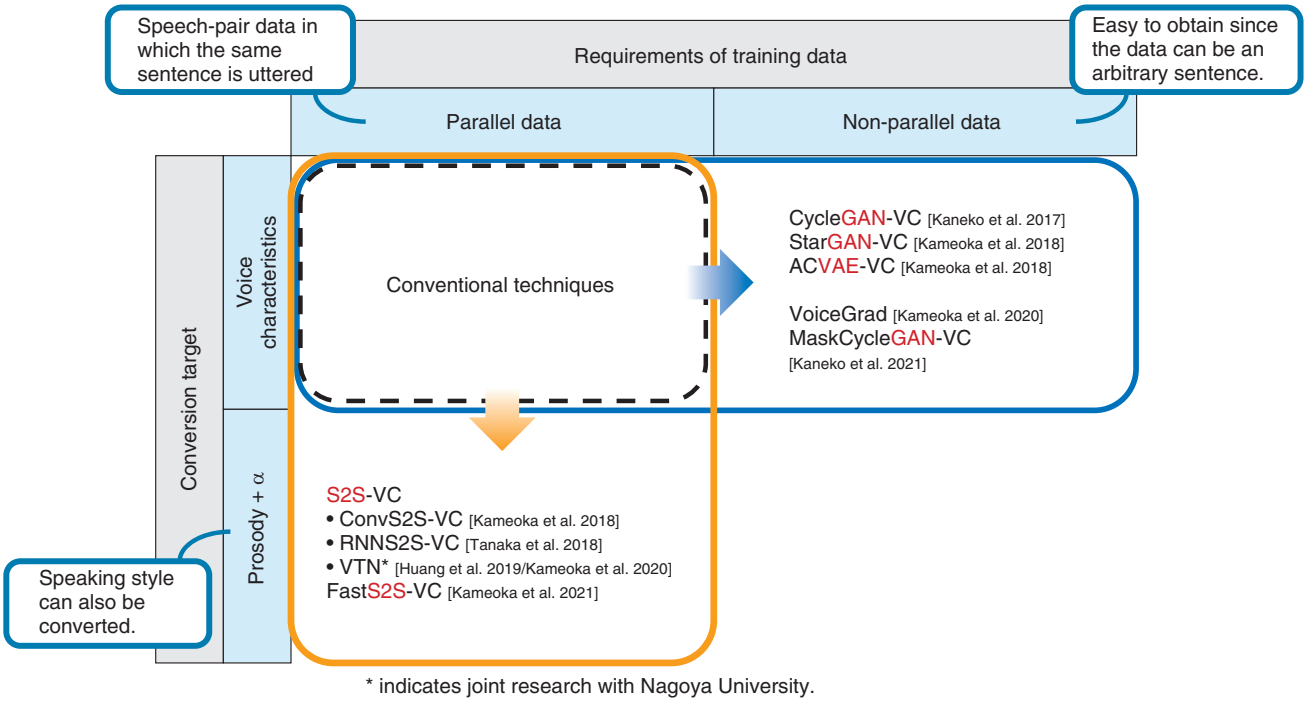


Fig. 1. Flexible voice conversion by using deep generative models.

voice-conversion technique, which complements the vocal function of the sender, are currently considered to be the core of such a system. Sound-source separation involves the decomposition of acoustic signals. Its purpose is to enhance the target sound source by extracting and separating multiple sound sources and removing reverberations and noise from an observed audio signal. The purpose of voice conversion is to change the features of speech to desired ones while preserving the speech content.

I'm also exploring the possibility of new communication methods that effectively use not only audio but also image, video, text, and many other types of media. For example, I'm considering enhancing communication by generating speech that matches a face and a face image that matches speech.

—How is your research on voice conversion with high quality and naturalness you mentioned last time going?

As I mentioned briefly in the previous interview, my research colleagues and I have developed many basic voice-conversion techniques and related peripheral techniques. We started researching voice conversion around 2016. At that time, the mainstream approach was to prepare two pieces of speech data uttering the same sentence, adjust the duration of one piece of the data so that the timing of each phoneme matched, and use the speech-pair data to train a *voice converter* to learn a conversion rule by which the features of the source speech are converted into the features of the target speech.

Such speech-pair data in which the same sentence is uttered by different speakers are called *parallel data*. This approach is effective when a large amount of parallel data can be collected. In many situations, however, parallel data cannot be easily obtained, for example, when the target speech is that of a particular celebrity. To address this issue, we turned our attention to deep generative models such as variational autoencoders (VAEs) and generative adversarial networks (GANs), which were attracting attention in fields such as machine learning and computer vision at the time. Using such deep generative models, we devised a non-parallel voice-conversion technique that can train a voice converter even from samples of source and target speech uttering arbitrary sentences (**Fig. 1**). Since this technique does not require parallel data for training, it is expected to greatly expand the use scenarios of voice conversion.

Most conventional techniques at the time were

limited to converting speech features such as voice characteristics and were not able to convert speaking styles such as intonation and rhythm. We wanted to develop a technique for converting speaking style as well as voice characteristics, so we focused on a framework called sequence-to-sequence (S2S) learning, which had been shown to be very effective in regard to machine translation, speech recognition, and text-to-speech synthesis. This framework is used for training neural-network models that transform one vector sequence into another (with different lengths) while capturing long-term dependencies. The key point regarding this framework lies in the model structure called the attention mechanism, which makes it possible to learn conversion rules as well as association rules between the elements of the source and target speech-feature sequences. As far as we knew at the time, few studies had attempted to apply S2S learning to voice conversion. I remember how excited my colleagues and I were when we tried it out and found through our experiments that, as we had hoped, it could flexibly convert not only voice characteristics but also intonation and speaking rhythm.

Almost without exception, current state-of-the-art voice-conversion techniques consist of two steps: (i) extracting a sequence of speech-feature vectors from the source speech and converting it into a mel-spectrogram and (ii) generating a speech waveform from the sequence of the converted mel-spectrogram. The aforementioned VAE, GAN, and S2S learning are all used for the first step of speech-feature conversion. For the second step, waveform generation, the waveform generator in the context of a neural network is called a *neural vocoder*. As those familiar with speech-related research probably know, a high-quality waveform-generation method called WaveNet was announced by DeepMind in 2016. Since then, many researchers have been actively working on improving its speed, quality, and training efficiency. Although our main focus has been on feature-conversion techniques, we have recently begun to focus on research targeting higher quality and lower delay in regard to waveform generation.

Each of the above-mentioned accomplishments has been reported at international conferences, such as International Conference on Acoustics, Speech, and Signal Processing (ICASSP) and Interspeech, and in academic journals such as IEEE Transactions on Audio, Speech, and Language Processing, and the total number of citations exceeds 1000 times. I think that our recent activities are gradually gaining recognition.

Building a machine-learning infrastructure for improving the accuracy, efficiency, and flexibility of voice conversion and sound-source-separation techniques

—These accomplishments are good news for those who have communication problems. Can you tell us about specific applications?

Applications of voice conversion that we have had good experimental results with include speaker-identity conversion, English-accent conversion, whisper-to-speech conversion, electrolaryngeal (EL)-speech enhancement, emotional-expression conversion, and stuttered-speech conversion.

I believe that English-accent conversion helps facilitate conversation by converting the speaker's English into an accent that is easier for the listener to understand. For example, for Japanese people (depending on the person, naturally), the so-called "Japanese English accent" may be easier to understand than the native speaker's accent, so it may be desirable to add a Japanese English accent to the native speaker's speech.

Whisper-to-speech conversion is a task that aims to convert a whispered voice into a normal speech sound. For example, you want to make a phone call or hold an online meeting in a situation where you are not comfortable speaking, such as on a crowded train or in a coffee shop. If this voice-conversion technique is available, you can speak in a whisper so that people around you cannot hear your voice, but your voice will be transmitted to the other party as normal speech.

EL-speech enhancement is a task for converting EL speech into natural-sounding speech. EL speech is speech produced using an electrolarynx by a person with a speech impediment who has lost their vocal cords due to laryngectomy or other surgery and sounds monotonous and mechanical. This voice-conversion technique makes it possible to convert such EL speech into speech like those of able-bodied people. It has also been found that it is possible to change the expression of emotions by changing the speaking style, and to some extent, it is possible to automatically omit stutter and filler words such as "Ah…" and "Um…" to make the entire speech fluent. Audio samples of these voice conversions are available on our demo sites [1–3].

Regarding sound-source separation, we have

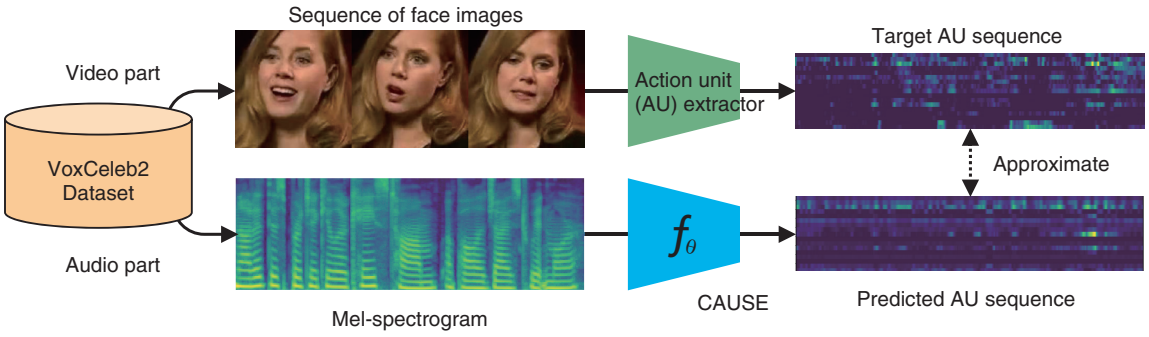


Fig. 2. Training crossmodal action unit sequence estimator (CAUSE).

previously proposed a multi-channel source-separation technique that uses the aforementioned VAE to model the source signals and have been studying ways to increase the speed and accuracy of this technique. The research field of multi-channel source separation has dealt with mixtures of a maximum of five sound sources. However, we have demonstrated that our technique can separate mixed signals from up to 18 sound sources with high accuracy, achieving unprecedented performance. Audio examples of this multi-channel source separation are also available on our demo site [4].

—Listening to the comparison between conventional techniques and your techniques, the listener can clearly hear the superiority of your techniques.

I'm thankful you think so. In addition to these studies, we are investigating crossmodal signal-generation technology that uses media other than sound to generate and control sound or uses sound to generate and control signals other than sound. For example, this technology can generate voice that matches a face image or generate a face image that matches the voice (**Fig. 2**). We aim not only to enrich voice communication but also enable intuitive control of communication to enhance communication functions. Specifically, we investigated crossmodal face-image generation, which predicts a speaker's face from speech alone and outputs the predicted face as an image, and crossmodal voice-characteristics conversion, by which the target voice characteristics can be specified via a face image (instead of a speaker identity). The demonstration of these techniques was well received at the NTT Communication Science Laboratories Open House 2022 and were covered by various media.

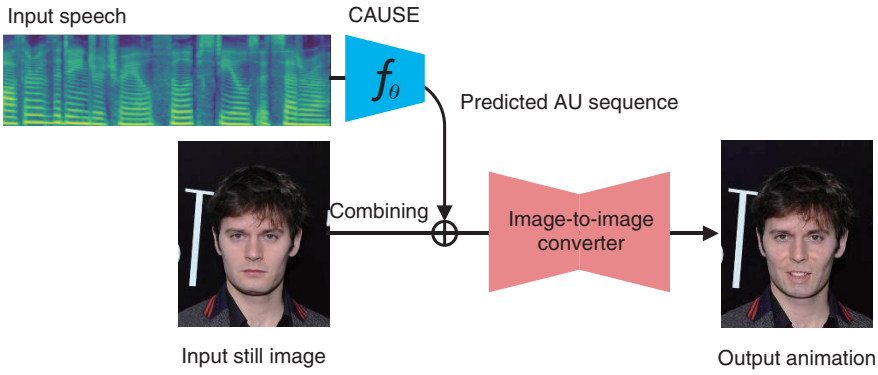
We also attempted to estimate a sequence of action units (AUs) (i.e., facial-muscle motion parameters) of the speaker from speech alone. To the best of our knowledge, no one else had attempted such an estimation, so we had no idea how accurate it would be. Through experimentation, we found that it was possible to estimate the AU sequence to some extent. By using an image-to-image converter and the AU sequence estimated from speech, it is possible to move the facial expression of a still face image in accordance with the speech (**Fig. 3**). If we improve the accuracy of this AU sequence estimation and make good use of it, we will be able to provide visual feedback on how one's speaking style and voice characteristics affect the conversation partner, which will be useful for improving one's presentation and customer-service skills.

Examples of each of these studies on crossmodal signal generation are available online on our demo sites [5, 6].

Keep "Think like an amateur, do as an expert" in mind

—Would you tell us what has been important to you as a researcher?

The title of Dr. Takeo Kanade's book, "Think like an amateur, do as an expert," is one of the mottos I always keep in mind as a researcher. As one's specialized knowledge increases, one tends to fall into the trap of "research for research's sake" and set research themes that seem like nitpicking. There is a chance that such a theme could develop into an important research theme. However, I try to ask myself as calmly as possible whether I find the research theme interesting and whether it is really useful to society.



Face images are acquired from VoxCeleb2 Dataset*1 and CelebA Dataset*2.
*1 J. S. Chung, A. Nagrani, and A. Zisserman: "VoxCeleb2: Deep Speaker Recognition," Proc. of Interspeech, pp. 1086–1090, 2018.
*2 Z. Liu, P. Luo, X. Wang, and X. Tang: "Deep Learning Face Attributes in the Wild," Proc. of ICCV, pp. 3730–3738, 2015.

Fig. 3. Facial-expression control from speech by using CAUSE and image-to-image converter.

For example, in my research on augmenting communication functions, I'm constantly thinking about whether there are any discomforts or inconveniences in our daily lives that we are not usually aware of and whether there are ways to overcome them. We are now entering an era of rapid development and upheaval in the fields of artificial intelligence (AI) and machine learning, and while it is obviously important to always follow the latest trends and research, I believe it is also important to remain calm and listen to our inner voice.

While researching AI, I've been reminded of the importance of doing as much hands-on work, namely, coding and experimentation, as possible. I have been rather good at research in which I take my time to formulate a hypothesis and a theory for each problem then develop a solution; in contrast, I feel that in research using deep learning and neural networks, it is important to repeat the process of verifying a hypothesis through experiments over and over again at a rapid pace. The behavior of a neural network is not always as intuitively imagined, and it may feel like you are dealing with a living being. I feel that the more I deal with it, the more I understand it, so now I try to code and conduct experiments at least once a day. In deep learning, many training samples are input to a neural network, and the network learns behaviors that match the training data. Through a large amount of coding and experimentation, I get the feeling that I'm also learning the behavior of neural networks, which is very refreshing and interesting.

—What are your future plans and what would you like to say to the younger generation of researchers?

My first plan is to conduct more research on voice conversion to meet the demands of using sensory language. For example, if a "cute voice," "gentle voice," or "stately voice" is requested, the voice conversion will convert speech to such a voice. For the voice conversion that we have been researching, the voice characteristics of the conversion target were easy to uniquely define; however, as the examples I mentioned show, the definition of a sensory language is ambiguous and varies from person to person. The key is how to quantify the sensory language the definitions of which are ambiguous and subjective, so I'm currently working on this issue with my colleagues.

When this voice-conversion system is put into practical use, we cannot deny the possibility that it could be misused to impersonate other people's voices in a malicious way. We thus intend to conduct research to prevent the misuse of voice-conversion systems.

I also think it is necessary to create a white-box model for practical use. In the example of voice conversion, if a system that converts a voice in real time is actually used, it must be guaranteed that no unexpected conversions will occur. This is because some conversions may give the listener an impression that is contrary to the speaker's intention. Neural networks are very good at learning behaviors that match the training data; however, their internal structure is a

black box that makes it difficult to predict their behavior when data that do not exist in the training data are input, so they are not always easy to control. Therefore, I believe that we must pursue research on model structures and control mechanisms to ensure that voice-conversion models can be used with confidence.

Finally, to younger generations of researchers, I believe that the mission of researchers is to make the world a better place. I hope that all researchers will cooperate, exercise their wisdom to meet the hidden human desire for convenience and comfort, and make the world a safer, more secure, and happier place.

You will face a lot of hard times when you are doing research. This may sound cliché, but I think it is important to enjoy your research instead of focusing only on the negative aspects. Many people at NTT laboratories are now working remotely, and I especially encourage those people to have online meetings frequently, which might just be for chatting, and create many opportunities to communicate with their colleagues and seniors. It will be fun and stimulating to talk with them. I also want you to remember to respect each other as researchers. I often work with students and have the opportunity to check their manuscripts, and sometimes I see statements that needlessly downplay conventional technologies so as to assert the superiority of their proposed technology. However, science and technology have been built up little by little by the collective wisdom of our predecessors, and it is our job as researchers to try to make them even better. Therefore, I want you to look at previous research from the viewpoint of finding the positive aspects and further improving them.

References

[1] S2S-VC (sequence-to-sequence voice conversion), https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/s2s-vc/index.html
[2] ACVAE-VC (non-parallel many-to-many voice conversion (VC) method using an auxiliary classifier variational autoencoder), https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/acvae-vc3/index.html
[3] StarGAN-VC (nonparallel many-to-many voice conversion (VC) method using star generative adversarial networks), https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/stargan-vc2/index.html
[4] Audio examples of MVAE and FastMVAE2, https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/mvae-ss/index.html
[5] Crossmodal voice conversion, https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/crossmodal-vc/index.html
[6] CAUSE (crossmodal action unit sequence estimation/estimator), https://www.kecl.ntt.co.jp/people/kameoka.hirokazu/Demos/cause/index.html

■ **Interviewee profile**

Hirokazu Kameoka received a B.E., M.S., and Ph.D. from the University of Tokyo in 2002, 2004, and 2007. He is currently a senior distinguished researcher and senior research scientist with NTT Communication Science Laboratories and an adjunct associate professor with the National Institute of Informatics. From 2011 to 2016, he was an adjunct associate professor with the University of Tokyo. His research interests include audio and speech processing and machine learning. He has been an associate editor for the IEEE/ACM Transactions on Audio, Speech, and Language Processing since 2015 and member of the IEEE Audio and Acoustic Signal Processing Technical Committee since 2017.

Magnetact Technology Based on Magnetic Forces with No Power Supply toward Tactile Presentation

Kentaro Yasu
Distinguished Researcher,
NTT Communication Science Laboratories

Abstract

In the research field of human-computer interaction, various types of studies are underway so that people can use computers in a more comfortable manner. As a part of this effort, NTT is conducting research and development on non-electrical devices to deal with contemporary issues such as the vast consumption of electric power and global warming. In this article, we talked with NTT Distinguished Researcher Kentaro Yasu about Magnetact technology that performs tactile presentation through magnetic forces without the use of electric power.

Keywords: Magnetact, magnetic force, tactile presentation

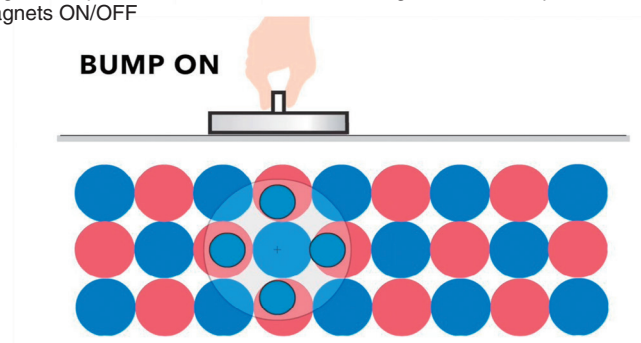
Magnetact technology for presenting an uneven sensation using magnetic forces

—Dr. Yasu, what exactly is Magnetact technology that you are now researching?

Since entering NTT, I have been researching tactile-information presentation technology using magnetic sheets. A magnetic sheet is a commonly sold, very ordinary sheet-shaped magnet. It is a flat object that mixes magnetic material as used in videotape and cassette tape with resin, and as such, it can be written with an S-pole and N-pole magnetic pattern when placed close to a strong magnetic field. Using this property, overlaying and rubbing together two magnetic sheets written with magnetic patterns can generate attractive and repulsive magnetic forces between the sheets. This in turn, can generate a bumpy, uneven sensation between the sheets despite their flatness. We named this technology "Magnetact" as a portmanteau combining the words *magnet* and *tactile*.

A key feature of Magnetact technology compared with conventional technologies is "no need for electric power." Before entering NTT, I worked as a research fellow at the National University of Singapore for three years, and during that time, I worked with Yuichiro Katsumoto—now an associate professor at Tokyo Denki University—on "Bump Ahead" technology, which is also being applied to Magnetact technology. In Bump Ahead technology, sliding a device equipped with four magnets across a board laid out alternately with S-pole and N-pole ferrite magnets can generate an extremely strong tactile sensation of unevenness due to attractive and repulsive

Bump Ahead
Magnetic haptic interface that can turn the magnetic forces of permanent magnets ON/OFF



K. Yasu and Y. Katsumoto, "Bump Ahead: Easy-to-design Haptic Surface Using Magnet Array," SIGGRAPH Asia 2015 Emerging Technologies, 2015. http://doi.acm.org/10.1145/2818466.2818478

Fig. 1. Bump Ahead technology.

magnetic forces. In addition, rotating the four magnets built into the device at a 45-degree angle can alter the sum total of the magnetic forces and instantaneously switch between having and not having that tactile sensation (**Fig. 1**). Before the development of this device, a commonly used technique to achieve this effect was to make a current flow through electromagnets to manipulate magnetic forces, but this was accompanied by a variety of issues such as the large amount of electric power required to produce strong magnetic fields and coil overheating. Against this background, Bump Ahead technology, which can instantaneously turn this tactile sensation ON/OFF simply by rotating magnets without using electromagnets, solved the above issues thereby achieving a major research target.

—How did Magnetact technology that generates an uneven sensation through magnetic forces come to be born?

In Bump Ahead technology, major issues remained in the section laid out with ferrite magnets. For example, when laying out ferrite magnets with a diameter of 20 mm and a thickness of 5 mm across an area of 40 × 40 cm, a total of 400 magnets would be needed, and at a weight of about 3 kg, it would be difficult to carry around the device. Furthermore, since those 400 magnets would attract each other while being laid out, even a momentary relaxation could cause a chain reaction in which all of the magnets become stuck to each other. We experienced this failure any number of times when attempting to implement this technology!

Thinking that this device in the above form would be difficult to use in real life, we thought about a method that could solve the problems of Bump Ahead technology in an easier way. One day, on going to the laboratory, a neodymium magnet happened to be placed on a magnetic sheet, and on observing this with a sheet called a "magnetic viewer" that had just been adopted for visualizing magnetic fields in research, I noticed that the magnetic fields of the magnetic sheet had been rewritten by the neodymium magnet on top of the sheet. However, the magnetic forces of a magnetic sheet are very weak compared with ferrite magnets, and no sense of unevenness can be felt without rubbing such sheets together. I therefore concluded that this scheme would not be very practical and never took it up for research. Later, though, after entering NTT, I considered that "If the magnetic patterns of such sheets could be easily rewritten, couldn't the feeling when rubbing them together be predicted by calculations and modified in various ways?" and "Couldn't a variety of applications become possible by rewriting magnetic fields?" I therefore took up this research again and ended up developing a "magnetic plotter."

A magnetic plotter is a piece of equipment that can rewrite the magnetic fields on a magnetic sheet. I began my research thinking that "If magnetic patterns can be easily rewritten, couldn't a machine be used to write detailed patterns?" Here, by attaching a compact neodymium magnet to a home-use plotting machine (equipment that can write graphical figures with a pen), I was able to magnetize detailed

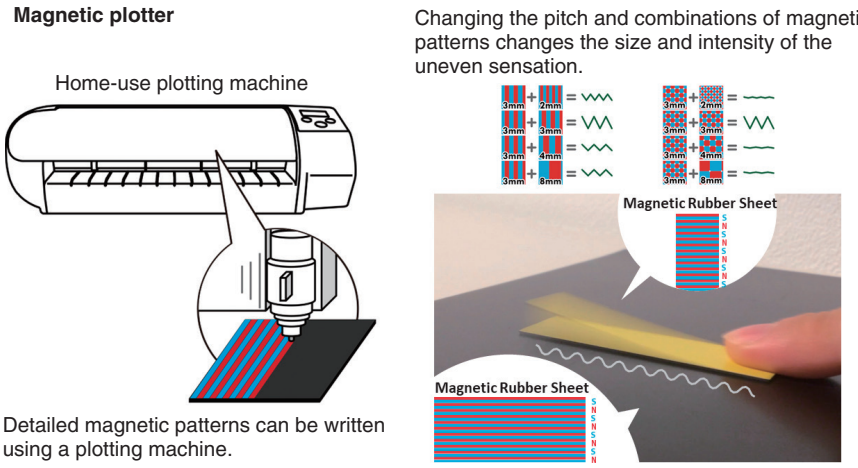


Fig. 2. Magnetic plotter technology and examples of tactile-presentation combinations.

magnetic patterns on magnetic sheets and use those patterns to control the bumpy, uneven sensation when rubbing two magnetic sheets together. Of course, it is also possible to write a magnetic pattern manually while holding a neodymium magnet in one's hand, but using a machine enables highly accurate and detailed patterns to be created. As shown in **Fig. 2**, changing the pitch and combination of written magnetic fields can vary the type of uneven sensation.

Then, in the following year after completing this technology, I conducted research on a technique for creating a haptic interface using this magnetic plotter. This technique takes a magnetic sheet written with a detailed magnetic pattern using the magnetic plotter and pastes it on a touch screen of a tablet or other device to create buttons and switches having a click-type feeling. Whenever presenting the results of this research, I have been reminded of the great potential of haptic technology using magnetic sheets, and I have given this technology in general the name of "Magnetact."

—How are you spreading the word on Magnetact technology to the world?

After presenting my research results on Magnetact technology in 2019, I studied methods of getting people in society to use the technology in a variety of formats. In 2020, I held a workshop called "Magnetact Idea Session" together with creators to brainstorm about ways of using Magnetact. Among the various ideas proposed, Masaya Ishikawa, one of the creators representing Japan, proposed the idea of "combining a magnetic sheet with paper to give movement to animal paper craft." Although Magnetact technology that I proposed presents a tactile sensation through magnetic forces, this idea showed that it was capable of evolving beyond that to the domain of "movement" by connecting a magnetic sheet and cardboard with paper. This idea fulfilled my research theme of "enabling even people with no prior knowledge, experience, facilities, or environment to create something that moves," which made me quite happy. In a short period after this proposal, Masaya Ishikawa took on a central role in obtaining the cooperation of a specialist in manufacturing paper products (Fukunaga Print Co., Ltd.) and turning this idea into a product called "Magnetact Animals" in 2021. Since then, we have been holding both online and offline workshops at a variety of locations to provide many people with the opportunity of experiencing the wonder of magnets and the joy of creating things that move.

In addition, we have recently been developing a technology called "MagneShape." This technology enables the magnetic forces of a magnetic sheet written with a magnetic pattern to move magnet-equipped pins up and down. It can display characters and animation in a non-electrical manner despite having a very simple configuration (**Fig. 3**). (See the article in this issue "MagneShape: A Simple Pin-based Shape-changing Display Using Magnetic Materials")

MagneShape
The magnetic forces of a magnetic sheet written with a magnetic pattern moves magnet-equipped pins up and down.

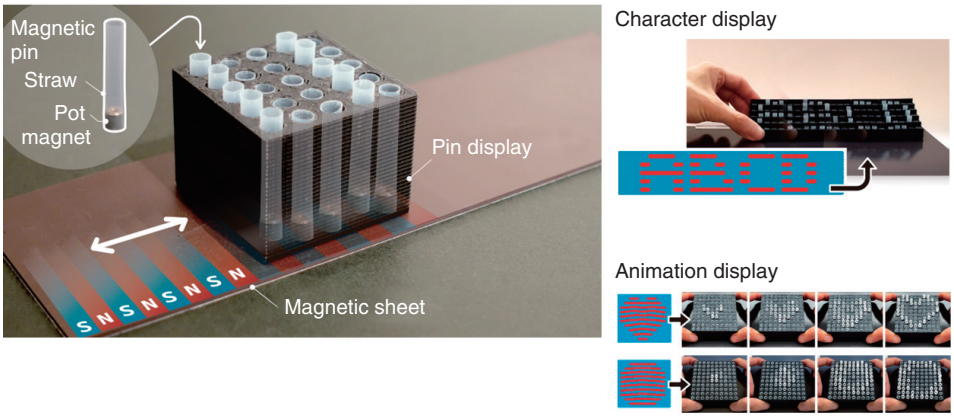


Fig. 3. MagneShape technology and examples of information display.

Creating new ways of making things and delivering value to many people

—What is your vision for future research?

In human-computer interaction (HCI), my research field, mutual interaction between humans and computers and human-friendly interfaces are common topics of research. Here, my technology, which has no need for a power supply or a machine, appears at first glance to be a technology unrelated to computers. Yet, Magnetact Animals, for example, involves an operation that "designs movement using components pasted to paper shapes or paper," which makes it very similar to programming using a computer. I believe that magnetic technology typified by Magnetact Animals will play a major role as equipment that can experience and learn the concept of computer operations without actually using a computer. Furthermore, though most computers today run on electric power, the means of achieving output based on numerical calculations, logical operations, and input information is not necessarily restricted to semiconductors and electric current. Indeed, in the outside world, much research is now being conducted on information processing technologies using slime mold and DNA, for example, and on mechanisms for performing calculations based on the physical characteristics of objects and fluids. In the HCI research field, many trials are being proposed on ways of programming shapes, colors, movement, etc. using non-electrical devices called "programmable matter" or "programmable material." In this regard, wouldn't magnetic-field-control and information-presentation technologies using magnetic material like what I'm researching here also extend the concept of existing computers and give many people a means of creating things?

—What do you think is an important attitude for a researcher to adopt in research and development activities?

In a song that I like titled *Ariamaru Tomi* by the Japanese singer-songwriter Ringo Sheena, the words

"value belongs to and is connected to life itself" appear in a certain verse. If we interpret these lyrics to mean "the strength of human beings is the ability to create something new when something is taken from them," they become words of encouragement to pursue the creation of something new. By the way, I not only show people things that I myself have created and present them to the world, I also focus on "creating new ways of making things." I would like many people to create interesting things using new ways of making things.

In research, meanwhile, there are many things that demand novelty and freshness, but if one becomes obsessed with cutting-edge tools and materials, the end result may be overly expensive products that cannot be used by anyone or technology that cannot be delivered to the people who really need it. To prevent this from happening, I think it is essential in research to always keep in mind "Who will use this and where?" and "What up to now has not been possible?" In my research, I make it a point to go to DIY (do-it-yourself) stores or supermarkets to check on what types of materials are readily available for ordinary people and to consider whether there are new ways of making things using those materials. I would like to press on with my research without taking my eyes off areas where technology will be needed in the future.

—Dr. Yasu, please leave us with a message for researchers, students, and business partners.

In the Sensory Interface Research Group of NTT Communication Science Laboratories that I belong to, each member is independently engaged in original research themes. Up to now, I have been conducting research using force-field presentation with magnetic materials based on my own judgment, and I am fortunate to have been able to decide on my own what themes to select, what academic societies to make presentations at, etc. When conducting research within a corporation, the significance of your research from a business perspective and what kind of profits it can generate in the short term are important considerations. At NTT, however, a long-term and strategic perspective is required when deciding on a research theme compared with a short-term perspective directly linked to company profits. This is why I feel that my working environment makes research very worthwhile. Furthermore, in addition to writing papers, I am responsible for preparing patent applications, producing demonstrations and videos, and commercializing my research, but at NTT, I am grateful that I can move my research forward thanks to the support provided in administration, intellectual-property, and commercialization matters and the understanding that I receive from my superiors and colleagues.

From here on, as I move forward in my research, my goal is not to present papers but rather to see my research as a starting point. It is certainly true that the number of presented papers has become one index for evaluating researchers, and for students, presenting a certain number of papers is perhaps a requirement for graduation. I, on the other hand, am a person that takes great pleasure first and foremost if someone can make use of the technology that I develop. For this reason, I will continue in my efforts to provide technology in a form that many people can easily use. As reflected by Magnetact Animals, I look forward to those moments in which something that had not occurred to me at all is born. For those of you who would like to try my technology, please feel free to contact me.

■ **Interviewee profile**

Kentaro Yasu completed his doctoral program in media design at the Graduate School of Keio University in 2013. He worked as a Research Fellow at the National University of Singapore from 2013 to 2016. He entered NTT in 2016 and has been an NTT Distinguished Researcher since 2019. He is currently engaged in the research of tactile-information presentation technology in the field of human-computer interaction.

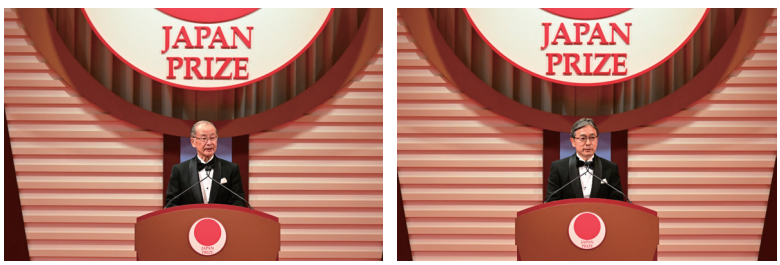
Keeping in Mind the Spirit Acquired at NTT Laboratories, We Will Continue to Challenge Ourselves to Contribute to the Development of Humankind

Masataka Nakazawa, Special Honorary Professor, Tohoku University
Kazuo Hagimoto, Principal Researcher, National Institute of Information and Communications Technology

Abstract

Masataka Nakazawa, special honorary professor at Tohoku University, and Kazuo Hagimoto, principal researcher at National Institute of Information and Communications Technology, who both researched at NTT, have been awarded the 2023 Japan Prize. This award recognized the development and practical application of a compact optical amplifier that amplifies optical signals without having to convert them into electrical signals and its contribution to high-capacity optical communication systems that use such amplifiers. Prof. Nakazawa and Mr. Hagimoto paved the way for long-haul, high-capacity optical data communications, which is the key technology supporting the current global Internet society, and handed down important achievements that are incorporated in the concept of IOWN (Innovative Optical and Wireless Network) being advocated by NTT. To commemorate winning this award, we interviewed Prof. Nakazawa and Mr. Hagimoto.

Keywords: Japan Prize, EDFA, optical repeater



Courtesy of the Japan Prize Foundation

Prof. Nakazawa (left) and Mr. Hagimoto (right).

Japanese researchers receive the Japan Prize for the first time in nine years in the field of electronics, information, and communications

—Congratulations on winning the Japan Prize. We heard that you were both very surprised when you learned that you'd won the award.

Prof. Nakazawa: I am very pleased to have received the award. I could hardly believe that I had won it. Because I have served as a member of the selection committee for various prizes, when I received a call from the Japan Prize secretariat in the late autumn or early winter of 2022, I thought they were asking me to be a member of the selection committee. However, some time later, the president of the Japan Prize Foundation contacted me and said, "Prof. Nakazawa, you have won the award. Would you accept it?" I was really surprised. I couldn't believe that I had received the award, so I first answered, "Is it true? It is! Well then, I'm very honored." I think Mr. Hagimoto felt the same way.

Mr. Hagimoto: Yes, I was very surprised. The Japan Prize has been awarded to prominent researchers. I was more than surprised than delighted to learn that I could join them. I think it was sometime in November when I was contacted. To tell the truth, I also had some misunderstandings, which took me some time to settle until I could experience the joy of receiving the award. The Japan Prize secretariat contacted the National Institute of Information and Communications Technology (NICT), where I'm the principal researcher of the Beyond 5G R&D Promotion Project. However, since I was working from home, I didn't understand the message clearly, and I was wary that the call might be suspicious, so it took me some time to realize that it was about the Japan Prize. I was told that Hiroshi Komiyama, the president of the Japan Prize Foundation, former president of the University of Tokyo, would call me, and like Prof. Nakazawa, I thought he would be talking about being the selection-committee member. However, for a moment, I thought, "The president has taken the trouble to contact me maybe because I am receiving the award..." But I thought, "That's impossible."

Prof. Nakazawa: Receiving the Japan Prize is such an incredible honor. The Fields Selection Committee determines two fields in which the Japan Prize will be awarded two years later and announce those fields in November every year. Then, more than 15,000 nominators from around the world nominate the candidates, which are subjected to a rigorous selection process that takes into account excellence in science and technology, degree of contribution to society, and other factors.

I heard that I had been nominated several times in the past, but we're not pursuing research to win prizes, so I forgot that I was previously nominated. Even so, I'm more than happy to be recognized for having changed the shape of information and communications on a global scale.

—What is the relationship between the two of you? And how did you come to work in the same field of research?

Prof. Nakazawa: We both joined NTT (then Nippon Telegraph and Telephone Public Corporation) the same year (1980), myself as a Ph.D. in engineering, and Mr. Hagimoto as a master of engineering.

Mr. Hagimoto: When I met Prof. Nakazawa for the first time at a job interview, I discovered that we

Courtesy of the Japan Prize Foundation

Prototype in 1989

Paper:
M. Nakazawa, Y. Kimura, and K. Suzuki, "Efficient Er^{3+}-doped optical fiber amplifier pumped by a 1.48 mm InGaAsP laser diode," Appl. Phys. Lett., Vol. 54, pp. 295–297 (1989).

Patent: JP2128337 "Optical fiber amplifier"

Features:
• High speed and high capacity
• Low noise
• Low latency
• Compact and high reliability

Fig. 1. World's first semiconductor-laser-pumped EDFA.

actually went to the same university (Tokyo Institute of Technology). Although we were in different years and had never met face to face, we have been close ever since.

Prof. Nakazawa: After receiving training as a new employee, I was assigned to the former Ibaraki Electrical Communication Laboratory, where I was engaged in research on technology for identifying broken optical fibers in optical communications, and Mr. Hagimoto was engaged in research on transmission systems using optical fibers at the former Yokosuka Electrical Communication Laboratory.

Mr. Hagimoto: Symbolic of our joint research is our paper on the erbium-doped fiber amplifier (EDFA), which led to the Japan Prize, presented at the Optical Fiber Communication Conference (OFC) in 1989 (**Fig. 1**). Hearing from Prof. Nakazawa's colleagues specializing in optical fibers that gain could be obtained with a semiconductor-laser-pumped erbium-doped fiber (EDF), I began preparing for experiments on optical amplification using EDF from the end of 1988 to the beginning of the next year. It was a fairly rushed project. With only about two weeks were left before the OFC deadline, we conducted the world's first transmission experiment using an optical fiber amplifier.

Distinguished contributions to global long-distance, high-capacity optical fiber networks through the development of semiconductor-laser-pumped optical amplifier

—Now let me ask you about your achievements recognized by receiving the Japan Prize. The citation for the award was given as follows: "Through their development and practical application of semiconductor laser pumped optical amplifier, Professor Masataka Nakazawa and Mr. Kazuo Hagimoto have made major contributions to wavelength division multiplexing (WDM), quadrature amplitude modulation (QAM), digital coherent transmission technologies, and other elements necessary to achieving long-distance, high-capacity optical fiber communication networks. They helped carve out a path for the basic long-distance, high-capacity optical data communication technologies needed to support intercontinental communications through submarine optical fibers, and to handle the immense annual increase in data volume our global internet society deals with today." Can you give us some background information concerning these achievements?

Prof. Nakazawa: In the 1980s, optical communications using single-mode fibers were put to practical use; however, for long-distance communications, it was necessary to install repeaters every several dozen kilometers to electrically restore the signal weakened due to attenuation as light propagates through an optical fiber and retransmit it. In other words, the optical repeaters used electrical amplifiers with which optical

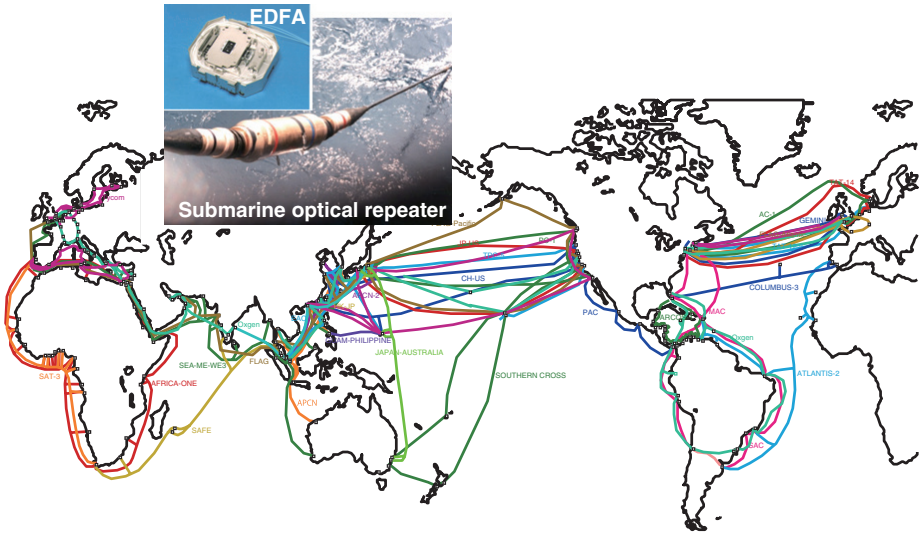


Fig. 2. International submarine optical cable networks.

signals are converted into electrical signals and increased (amplified) the signal strength, and the amplified electrical signals are then converted back into optical signals and transmitted. However, the bandwidth of signals that can be handled by electrical amplifiers was narrow, signals were sometimes distorted, and equipment including photodetectors were large and consumed much power; therefore, there was demand for optical amplifiers that amplify optical signals without having to convert them into electrical signals, which would make it possible to amplify optical signals within the wide bandwidth using compact amplifiers.

In response to this demand, Mr. Hagimoto and I have developed a compact, highly efficient, broadband optical amplifier, EDFA, which had been said to be difficult to put into practice. This EDFA had excellent features, namely, high speed, high capacity, low noise, low latency, compactness, and high reliability. I proposed the world's first method of using a 1.48-μm InGaAsP (indium gallium arsenide phosphide) semiconductor laser diode as a light source for exciting EDFs. In the 1.5-μm band, which is the minimum loss wavelength band with attenuation due to scattering and absorption of 0.2 dB/km, an amplifier using this method achieved a gain of 12.5 dB over a wide wavelength range of more than 50 nm. This method made it possible to develop a compact, battery-powered broadband optical amplifier with size of only about 10-cm square—significantly smaller than conventional amplifiers, which required an extremely large excitation light sources of about 1.5-m square. I received positive evaluations stating that the developed laser has opened up prospects for building a practical optical communication system.

Mr. Hagimoto: On the basis of Prof. Nakazawa's proposal, I increased the output power of his optical amplifier and successfully conducted a long-distance transmission of 212 km using a 1.8-Gbit/s intensity-modulated direct-detection (IMDD) system, demonstrating its practicality of optical amplifiers for the first time in the world. Our achievement has been recognized as a major breakthrough in the practical application of optical communication systems; namely, our EDFA was widely adopted as an optical repeater in long-distance transmission networks such as the trans-Pacific and trans-Atlantic optical submarine cables for connecting the world in about five years after the development of the EDFA (**Fig. 2**).

EDFAs can amplify multiple optical signals at different wavelengths simultaneously; therefore, combined with the development of high-capacity technology such as WDM, the use of optical communications has grown rapidly since the mid-1990s. I was also recognized for leading the international standardization of this technology. Although other methods of optical amplification have been developed, using EDFAs remains the world's dominant method.

Our achievements have been recognized for enabling the diversification and increased capacity of information resources used on the Internet around the world as well as for enabling the provision of

high-speed, large-capacity optical communication systems at low cost, which supported the explosive growth of the Internet.

—The citation for the award also states that your work "has made possible the dramatic expansion of the social networks, cloud services, and other elements of the information infrastructure we use in our daily lives." Your hard work paid off, and you played a part in building a modern information society.

Prof. Nakazawa: Our work is like an unsung hero; that is to say, it is generally taken for granted that communications are always connected, but being connected is actually an amazing thing. Winning the award reminded me of the days when I was wrestling with the problems of extending the transmission distance of optical signals and identifying the location of breaks in fibers.

Mr. Hagimoto: Yes, that's right. I remember that at that time, my colleague and I were conducting experiments by installing a repeater in a maintenance hole. We had to go down the maintenance hole in which the repeater was installed for transmission experiments. Maintenance holes are dangerous places because of the thin air and accumulated rainwater, so I thought that if we could operate such a repeater in the future for long-distance transmission, we would be able to reduce the number of repeaters, thereby reduce such dangerous underground work.

—It seems you've been through a lot of dramas, but could you tell us a little about the stories behind the development of the EDFA?

Prof. Nakazawa: In a system for detecting break points in optical fibers, since the level of Rayleigh scattering in optical fibers is extremely low, it is necessary to input strong optical pulses into the fiber under inspection; however, in 1980, high-power semiconductor lasers that could achieve strong optical pulses were not available.

Therefore, in collaboration with a group from NEC Corporation, we developed a YAG laser[*1] operating at a wavelength of 1.32 μm and summarized the technical details of an optical time-domain reflectometer using such a laser in a document after subjecting it to an on-site test by evaluating Fresnel reflection loss. It was probably the first time that a solid-state laser was put to practical use for a communication-measurement device. Since the distance between repeaters of the single-mode optical fiber transmission system was about 80 km, we only needed to measure 40 km of fiber from one repeater; however, we needed a wide dynamic range, so we started looking for an even better light source.

Optical pulses can travel through optical fibers the furthest at the wavelength band of 1.55 μm (the minimum loss wavelength); thus, a high-power light source operating at a wavelength of 1.55 μm can achieve the longest distance for detecting faulty points. Therefore, we looked at the oscillation wavelengths of various solid-state lasers and came up with erbium, which has a transition line at a wavelength of 1.55 μm between the ground state[*2] ($^4I_{15/2}$) and excited state ($^4I_{13/2}$). It was the spring of 1982, two years after I joined the company. I immediately asked my supervisor for permission for creating an erbium laser, and he said, "Let's give it a try." However, at that time, I heard that a researcher had researched an erbium solid-state laser in the US, and no one was paying attention to it, and neither information nor technical papers were available. Therefore, we decided to fabricate our own laser rods from scratch and asked Hoya Corporation, which had been manufacturing neodymium (Nd)-phosphate laser rods, if they would be interested in fabricating erbium laser rods with us. The division manager of Hoya readily agreed, saying, "We've never done that before, but let's give it a try." If they had declined our request at that time, the EDFA might not have been developed.

Two findings struck me as strange during the development of the EDFA. One is that erbium ions are optically active in silica glass. Normally, rare earths radiate light well in materials with small, non-radiative (phonon relaxation) transitions, such as phosphate glass and fluoride glass, but erbium is an exception. For the other finding, the excitation wavelength of Raman amplification for the 1.55-μm optical signal in silica fiber is 1.48 μm, which is the same as the quasi-two-level excitation wavelength of erbium. Who knows, if those excitation wavelengths of the two amplification methods were different, the EDFA might have taken longer to develop or it might not have been developed at all. It was thus fortunate that my group—as the only group in the world—was working on Raman amplification and erbium amplification simultaneously in one laboratory.

Mr. Hagimoto: Although Prof. Nakazawa and I kept in touch, our research activities were split between

*1 YAG laser: A solid-state laser that uses crystals of yttrium, aluminum, and garnet.

*2 Ground state: The lowest energy and most stable arrangement of electrons.


Courtesy of the Japan Prize Foundation

Prof. Nakazawa (left) and Mr. Hagimoto (right) at the award ceremony.

Ibaraki and Yokosuka; however, Dr. Sadakuni Shimada, who was overseeing both of us at the time, encouraged us to cooperate closely in conducting experiments of a transmission system, and in 1989, we worked on the first transmission experiment using an optical fiber amplifier. The output power of the excitation laser at that time was not sufficient, and while devising ways to increase stability, we selected one EDF that satisfied the conditions. We then thought of using this fiber by dividing it in two according to the golden ratio (instead of simply dividing it into two) and rewind it. It subsequently became clear that the longer fiber was suitable for power amplifiers, and the shorter fiber was suitable for preamplifiers. It felt like magic that a wire that looked like just a fiber could provide enough amplification power to make up for the loss in an 80-km stretch of optical fiber.

At that time, IMDD systems reached a dead end in terms of improving performance, and optical amplification was thought to be the final method to challenge coherent optical transmission systems. I still vividly remember our successful optical amplification transmission experiment in 1989, and the more experiments we conducted, the more impressed I was with the performance of the EDFA.

Optical amplifiers can amplify multiple optical signals at different wavelengths simultaneously without distortion, and bandwidth can be secured even when 300 amplifiers are connected. In the blink of an eye, several projects began for relaying signals across the Pacific Ocean by using optical amplifiers only. I was surprised that KDD (currently, KDDI) and AT&T decided to apply optical amplifiers to their submarine systems, which emphasized reliability, at about the same time as it was adopted by NTT's terrestrial system. I have wanted to conduct research that would impress people, but I was impressed by their quick decision.

Even if we take twists and turns, we are getting ever closer to our goal

—The birth of the EDFA is an achievement that paved the way for long-distance, large-capacity optical data communications, which is the core technology that supports today's global Internet society and led to IOWN. How did you successfully pursue research that leaves behind such outstanding achievements?

Prof. Nakazawa: Impactful research achievements like the EDFA are rare, and research never ends once one mountain is climbed. Our achievements are based on our good fortune in encountering erbium and the tireless investigation of this material by various researchers in this field.

If you know from the beginning that you should do something, everyone will take up the same challenge. Since that is not known, researchers not only increase knowledge but also expand connections with other researchers and combine materials, individual results, and knowledge, etc. to produce great results.

Mr. Hagimoto: Dr. Shimada was very pleased with the results of our 1989 transmission experiment, but when I was preparing for my presentation of those results at OFC, he told me to get someone else to do the presentation. When I asked why, he said, "Because you will be much busier with a press release and subsequent correspondence." So I had to ask a colleague to present the results that I had produced. In retrospect, he may have been worried that I was at the limit of my physical strength.

I have fond memories of the fact that Dr. Shimada submitted the results to the Kenjiro Sakurai Memorial Prize of the Optoelectronics Industry and Technology Development Association that year (1989), and together with Prof. Nakazawa, we were awarded the prize. After that, although I stumbled in various ways from research to implementation, I managed to fulfill my objectives thanks to the support of my seniors and the research community, leading to receiving the Japan Prize.

From an engineering perspective, standardization and collaboration are important to ensure that we deliver our achievements to the world, so sometimes it is necessary to let go of one's attachment to own achievements. We are also grateful for the support of the government, which enabled us to form a dream team to assemble the intellectual property held by each organization and company, contributing to the success of our research. Cross-organizational cooperation can be difficult. However, I believe that Japanese researchers will be able to compete on the global stage and achieve outstanding results if we work together for the purpose of not only increasing Japan's competitiveness but also contributing to society as a whole and the development of humankind.

Prof. Nakazawa: Speaking of collaboration, Mr. Hagimoto was quick to recognize the importance of transmission equipment and optical amplifiers, so he worked with other companies to introduce them into an optical communication system. He also demonstrated his ability to connect people by taking the lead in international standardization. That is easy to put into words, but it is no mean feat.

—Needless to say, researchers contribute greatly to the development of society and humankind. What qualities are required of researchers?

Prof. Nakazawa: I believe that, by nature, people live their lives with the intention of improving their daily lives, and researchers are the ones who make that intention their profession, take pride in it, and feel a sense of mission. Having curiosity, passion, and a strong will is essential qualities for researchers.

Even if no one expects you to do anything, it is important that you carve out a path for yourself and that you do your best. You have to be willing to enjoy your research even when you are having trouble. That is because even if you pursue research without making a detour, it does not necessarily mean that your research will bear fruit.

I also think it's important to study the things that you can only study when you're young, because you can study the things that you can study through books when you're older. I grew up in the countryside and lived in a world far removed from the research world, catching fish and picking the fruit of akebi (chocolate vine). When I was in junior high school, I liked making plastic models and vacuum-tube radios. I think that such experiences help deepen and improve the capability of a researcher.

Mr. Hagimoto: Prof. Nakazawa's pursuit of lasers for optical fibers and his contributions to the development of the technology have earned him extraordinary respect. When I visited him in his laboratory at Tohoku University, he was conducting experiments, as he did back then, and his enthusiasm was truly unwavering. He is now 70, but he seems the same as when he was in his 20s and 30s. That is extraordinary. There is no limit on his inquisitive mind. I'd like to emulate his level, but I cannot.

I think that researchers have aspirations and dreams as well as the capability to approach things with curiosity while thinking, "I wish it could be better…" It is important to have the kind of curiosity that makes you want to climb a mountain that no one has climbed before. Researchers are the people who can sustain that feeling even when they face twists and turns. Looking back on my own path, I believe that if we do not forget our initial feelings, we will gradually get closer to where we want to go, even if there are twists and turns, and, at least, we will not go in the opposite direction.

Doing something that you've never done before is the first step toward success

—Could you tell us about the principal spirit you cultivated at NTT's research laboratories?

Prof. Nakazawa: When we joined NTT, it was still the Nippon Telegraph and Telephone Public Corporation. I think the research laboratories were, in a sense, a sanctuary, where excellent researchers from various

universities gathered to conduct research and development in diverse fields. In this environment, we always conducted our research with an eye to how we could compete with the best laboratories in the world such as Bell Labs in the US.

My supervisor was very open-minded and supportive. EDFAs were not my specialty at the time; even so, when I offered to do research on EDFAs, he said, "Sounds interesting. Why don't you give it a try?" And he supported me by accompanying me to Hoya Corporation and securing the budget for the research. The spirit of supporting younger researchers with an open-minded and supportive attitude lives on in me, and I'm still competing with international researchers.

Mr. Hagimoto: I cherish the words of Goro Yoshida, the first director of NTT laboratories, "Do research by drawing from the fountain of knowledge and provide specific benefits to society through its practical use." NTT has been conducting a wide range of research from basic research to applied research in a wide array of fields, which is very rare in the world, and has contributed to society by collaborating with other companies for practical applications. According to Dr. Masao Kawachi (former director of NTT Science and Core Technology Laboratory Group), a center of excellence (CoE) is defined as "an organization in which second-rate researchers can produce first-rate results." The fact that NTT has established its base technologies that can be reusable is an important asset and a foundation that enables the inheritance and development of value. In that sense, the ability to transform advanced technologies into devices, measuring instruments, equipment, subsystems, and other means of implementation is an important step toward the next generation. Cumulative progress, in which past technologies are accumulated and the next person climbs the stairs based on them, is the proof that "phase matching" is achieved in the organization.

I can sometimes achieve results outside my field of expertise by superimposing new ideas on top of first-rate research results. I approach my research activities with this mindset, and I hope that the CoE will be passed on to subsequent researchers in the field of optical fiber communications as well.

—Finally, could you give a few words to future generations of researchers?

Mr. Hagimoto: To all future generations of researchers, keep your curiosity in mind and take a long-term view in your own research. I also encourage you to attend academic conferences because it is very important to have peers beyond the organization in your research activities. I expect your research activities will have an impact on society.

Prof. Nakazawa: What I want to say to younger researchers who are conducting basic research is "don't follow the lead." I hope that you will have a frontier spirit and pursue new research with a dream. I know you have research that you are assigned to do, but I think you should have one research project that you'd like to pursue in addition to the ones you have been assigned. Therefore, you will broaden the scope of your research, and doing something you have never done before is the first step toward success.

■ Interviewees' profiles

Masataka Nakazawa joined Nippon Telegraph and Telephone Public Corporation in 1980 and researched at the Electrical Communication Laboratory. He was a visiting scientist at Massachusetts Institute of Technology in 1984. He became an NTT R&D Fellow in 1999. He became a professor at the Research Institute of Electrical Communication (RIEC), Tohoku University in 2001, where he became a distinguished professor in 2008 then the director of RIEC in 2010. He also became the director of the International Advanced Research and Education Organization, Tohoku University and director of the Advanced Interdisciplinary Synergy Research Institute, Tohoku University in 2010. He became the director of Japan Council for Research Institutes and Centers of National Universities and the director of the Research Organization of Electrical Communication (ROEC), Tohoku University in 2011. He became a specially appointed professor of ROEC in 2018, when he also became the director (part-time) of Kanazawa University (to the present). In 2022, he became a specially appointed professor of the International Research Institute of Disaster Science, Tohoku University. He was granted the title of special honorary professor at Tohoku University in 2023 (to the present).
Selected awards: He received the Kenjiro Sakurai Memorial Prize (jointly with Mr. Hagimoto) in 1989, the IEICE Achievement Award (jointly with Mr. Hagimoto) in 1994, Science and Technology Agency Director-General's Award (Research Achievement Award) in 1997, IEEE Daniel E. Noble Award in 2002, OSA R. W. Wood Prize in 2005, Shida Rinzaburo Prize from Ministry of Post and Telecommunications in 2008, Prime Minister's Award for Industry-Academia-Government Collaboration Meritorious Achievement (jointly with Mr. Hagimoto) and IEICE Distinguished Achievement and Contributions Award in 2009, Medal with Purple Ribbon, JSAP Optics and Quantum Electronics Achievement Award, and the IEEE Quantum Electronics Award in 2010, Japan Academy Prize in 2013, OSA Charles H. Townes Award in 2014, Fujiwara Prize from Fujiwara Foundation of Science and Kahoku Cultural Prize from Kahoku Cultural Foundation in 2015.

Kazuo Hagimoto joined Nippon Telegraph and Telephone Public Corporation in 1980 and researched at Yokosuka Electrical Communication Laboratory. He became a group leader at NTT Transmission Systems Laboratories in 1994, a senior manager of the long-distance network business unit at NTT Communications in 1999, an executive manager at NTT Network Innovation Laboratories in 2000, and the director of NTT Network Innovation Laboratories in 2005. He then became head of NTT Science and Core Technology Laboratory Group in 2009, president and chief executive officer of NTT Electronics Corporation in 2013, a fellow of NTT Electronics Corporation in 2019 (to the present), and principal researcher at National Institute of Information and Communications Technology in 2021 (to the present).
Selected awards: He received the Kenjiro Sakurai Memorial Prize (jointly with Prof. Nakazawa) in 1989, IEE Oliver Lodge Premium in 1991, Kenjiro Takayanagi Memorial Award in 1994, IEICE Achievement Award (jointly with Prof. Nakazawa) in 1994, IEICE Achievement Award in 2006, the Maejima Hisoka Award in 2007, IEEE Fellow in 2008, the Commendation for Science and Technology by the Minister of

Education, Culture, Sports, Science and Technology in 2009, Prime Minister's Award for Industry-Academia-Government Collaboration Meritorious Achievement (jointly with Prof. Nakazawa) in 2009, IEICE Distinguished Achievement and Contributions Award in 2013, and the Medal with Purple Ribbon in 2016.

Development of Modern Cryptography and Research on Quantum Cryptography

Masayuki Abe

Abstract

The foundation of modern cryptography developed in 1976 considered security by modeling adversaries as polynomial-time Turing machines. However, recent advances in developing a general-purpose quantum computer have made a significant impact on modern cryptography because it overturns the security model. NTT's research on cryptography aims to provide technologies to ensure the security of modern information systems and create applications when quantum computers become widespread. This article reviews the 40 years of cryptologic research at NTT and outlines our current efforts.

Keywords: foundation of cryptography, post-quantum cryptography, quantum cryptography

1. Cryptographic research at NTT

NTT's research on cryptography, which began in 1982 with a bank card forgery incident involving an employee of Nippon Telegraph and Telephone Public Corporation, has lasted more than 40 years. In 1992, the Cryptography Research Team, which initially included only three members, became an official research group of eight members within the Information and Communication Network Laboratories. Along with the emergence of the Mosaic web browser in 1993, the Internet exploded, leading to the recognition of the importance of information security. In response to these developments, the group was reorganized as the Information Security Project in 1999 then as NTT Secure Platform Laboratories in 2012. Today, information security technologies have become commoditized to support daily life. Now known as NTT Social Informatics Laboratories, the research group continues to engage in a wide range of research on cryptography and information security.

Advanced networks have enabled the operation of various information distribution systems. The scope of cryptography has expanded from a basic *defensive* stance centered on concealment and authentication to an *offensive* stance of creating applications for cryptocurrency, cloud computing, and other new areas. With the increased likelihood of achieving general-purpose quantum computers, it has also become clear that public-key cryptosystems currently in use will rapidly become compromised. Therefore, new measures are now needed for defense purposes. The creation of cryptographic applications that proactively use general-purpose quantum computers and the establishment of the fundamental theories underpinning them will likely become a reality.

This article discusses *modern cryptography*, in which both system users and attackers use currently available classical computers; *quantum-resistant cryptography*, in which only attackers use quantum computers; and *quantum cryptography*, in which both users and attackers use quantum computers (**Fig. 1**). An overview of topics mainly related to public-key cryptography and its relationship with NTT's cryptographic theory research is provided. Another important research topic, symmetric-key cryptography, is discussed in terms of quantum-resistant cryptography.

2. Advances in modern cryptography

Secure and efficient cryptographic schemes are

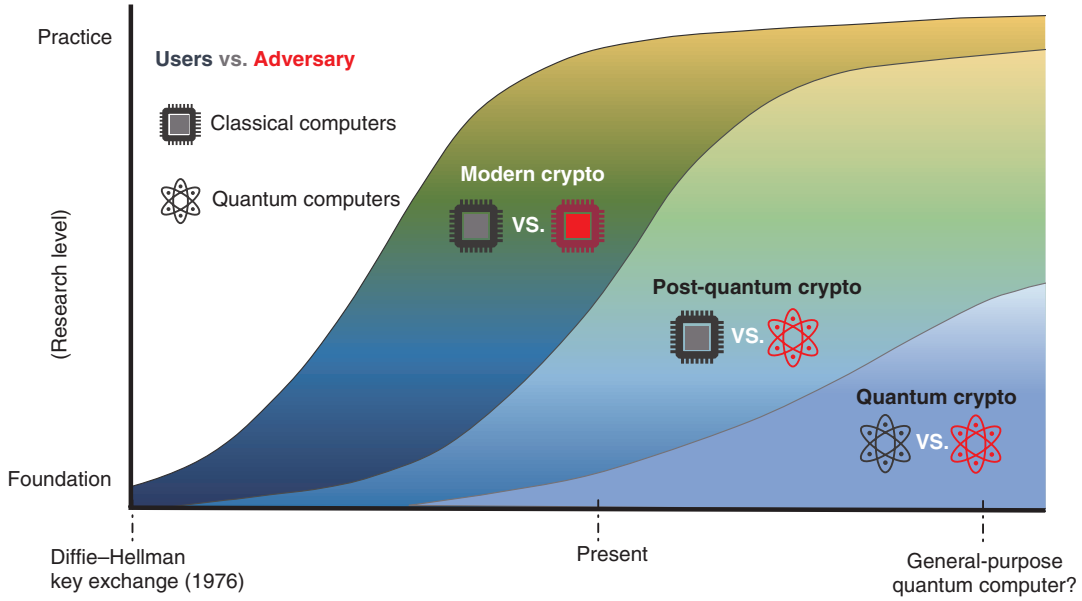


Fig. 1. Development from modern to quantum cryptography.

constructed on the basis of computational assumptions that it is, on average, difficult to solve a particular class of problems with a probabilistic Turing machine. However, as the algorithms and hardware available to the adversaries become more advanced, individual problems can be solved in less time than before. When this occurs, cryptographic schemes based on that class of problems would require larger keys for security, thus degrading performance. Rivest–Shamir–Adleman (RSA) encryption in 1977, Rabin encryption in 1978, and ESIGN (Efficient Digital Signature) system developed by NTT in 1990 take advantage of the hardness of the prime factorization problem. RSA's public key was considered secure at 512 bits at the time of its development, but now at least 3072 bits are recommended [1]. Diffie–Hellman key exchange in 1976, ElGamal encryption in 1985, and DSA (Digital Signature Algorithm) signature in 1993, which are also pioneering cryptographic techniques, were initially constructed using the discrete logarithm problem over multiplicative groups but have transitioned into instantiations based on the elliptic-curve discrete logarithm problem (such as ECDSA (Elliptic Curve Digital Signature Algorithm) signature in 2005), which enables a smaller public key at the same security level.

As networks advance, advanced cryptographic applications such as cloud computing have emerged. Cryptography has evolved from technologies for traditional purposes, such as information hiding and authentication, to more valuable technologies for constructing advanced information-sharing services. Bilinear mapping (pairing) over elliptic curve groups was first used for secure key generation by Kalisky, Jr. in 1987. It became widely known through the security analysis of the elliptic curve cryptography (MOV (Menezes–Okamoto–Vanstone) reduction) by Tatsuaki Okamoto of NTT and co-researchers in 1991. Since then, it has been widely used for cryptography in identity (ID)-based key exchange (Ogishi et al., 2000) and ID-based cryptography (Boneh et al., 2001), and has generated many practical applications to date. In particular, non-interactive zero-knowledge proofs, the practical value of which had been limited until then, have rapidly expanded with pairing-based constructions (Groth et al., 2008). At NTT, research has also progressed on structure-preserving cryptography (Abe et al., 2009), which enables advanced functions by freely combining cryptographic schemes over pairing groups. Pairing technology has contributed significantly to the realization of the advanced concept of computationally sound proof (Micali, 2000), which enables efficient verification of complex statements with a short proof, in the form of the Zero-Knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARK) (Gennaro et al., 2012). Since short proofs are highly demanded in blockchain applications, zk-SNARK is foreseen to become

the foundation technology for the Web3 era. Its usefulness is rapidly improving with the development of front-end compilers that translate statements in high-level languages such as C++ into an NP (non-deterministic polynomial time)-complete intermediate language that the back-end zk-SNARK can handle.

With the deployment of cryptography in various information systems and the advancement of the functionality of cryptography, the notion of security has also become more sophisticated. Proofs based on relatively simple security notions such as indistinguishability have been typically demonstrated by a simple reduction to a hardness assumption; it includes the Blum–Micali pseudo-random generator based on the discrete logarithm problem in 1982 and Rabin encryption based on the integer factorization problem in 1986. Higher levels of security have complicated the security proofs and constructions. In the well-known security notion of indistinguishability against adaptive chosen ciphertext attacks (IND-CCA) security (Bellare and Rogaway, 1991), an adversary is allowed to participate more actively in the input and output of cryptosystems. The random oracle paradigm introduced by Bellare et al. in 1993, which idealized hash functions, contributing significantly to simplifying construction and security proofs. Various encryption schemes and applications demonstrated as secure in the random oracle model were proposed from the late 1990s into the 2000s, leading to the spread of the paradigm of provable security. At NTT, the Fujisaki–Okamoto (FO) transformation in 1998, PSEC-KEM (Provably Secure Elliptic Curve encryption with Key Encapsulation Mechanism) in 1999, and the message-recovery signature scheme ECAOS (Elliptic Curve Abe–Okamoto–Suzuki signature) in 2008 have been developed in the random oracle model. However, many studies have been conducted to pursue efficient, provable, and secure constructions that do not rely on random oracles.

The cryptographic techniques developed for today's computers and networks will continue to be passed down as foundations, providing insight into the construction of secure cryptography even in a post-quantum computer world, as discussed below.

3. From modern cryptography to post-quantum cryptography

It is believed that it will take a considerable amount of time before adversaries can use general-purpose quantum computers. However, since most of the present information in circulation is being collected and accumulated, cryptographic technologies deployed now need to withstand future attacks using general-purpose quantum computers to ensure privacy of the accumulated information. Lattice-based problems are promising as basic hardness assumptions to be used in constructing post-quantum secure cryptography. The use of the lattice problem in cryptography began with the construction of a one-way function by Ajtai in 1996. Subsequently, a lattice-based, concretely efficient N-th degree Truncated polynomial Ring Units (NTRU) encryption was proposed in 1998. For digital signatures, constructions based on multivariate polynomials and hash functions are also promising options to achieve post-quantum security.

In the Post-Quantum Cryptography (PQC) Competition launched by the U.S. National Institute of Standards and Technology (NIST) in 2017, open calls for quantum-computer-safe public-key cryptosystems and digital signatures were made, and the final candidates were announced in 2022. This means that post-quantum cryptography is rapidly approaching practical application. It will become the new standard by 2024 and is expected to replace the current ones by 2030. NTT has contributed to the competition as a proponent of NTRU encryption and in evaluating many candidates. Since quantum computers can operate over superposition states, and the computational principles of the adversaries differ, techniques for the security proofs have been reconstructed to match quantum computers. The aforementioned FO transformation has also been re-examined so that safety can be established in a quantum random oracle model that executes computations in the quantum state. FO transformation is used to make CRYSTALS-Kyber, the cryptographic scheme adopted in the NIST PQC competition, IND-CCA secure.

Lattice-based cryptography is fundamental for developing advanced cryptosystems, aside from being quantum-safe. Fully homomorphic encryption, which enables addition and multiplication on encrypted plaintext, is an essential cryptographic technology with a wide range of applications, including cloud computing. NTT has been engaged in security analysis of lattice-based cryptography and research on fully homomorphic encryption since 2013.

By doubling or tripling the key length and block size, symmetric-key cryptography, such as block ciphers and hash functions, can be secured against key search attacks that use general-purpose quantum algorithms irrespective of their internal structures.

Thus, unlike public-key cryptography based on number-theoretic assumptions, they are thought to be impervious to the fatal consequences of such attacks. Attacks by quantum computers also pose a new risk for symmetric-key cryptography because they have been shown to be effective against specific well-known structures. The feature article in this issue entitled "Security of Hash Functions against Attacks Using Quantum Computers" [2] explains the security of hash functions against attacks using quantum computers, particularly, the quantum resistance of SHA-2.

Although research on post-quantum zero-knowledge proofs and cryptographic protocols is also advancing, further research is needed to promptly replace current technologies. For example, in anonymous electronic voting, the size of one vote in conventional classical cryptography will expand from a few kilobytes to several hundred kilobytes in quantum-safe voting systems. These technologies are essential for the transition to quantum-resistant security of information distribution systems based on current encryption technologies, and are expected to develop at an early stage.

4. Toward quantum cryptography

The remarkable increase in computing power of edge devices has made a variety of applications possible. When quantum computers will be widely used not only by adversaries but also by ordinary users, what technologies and applications would be possible? Quantum physicist Stephen Wiesner described the idea of applying the loss of quantum states by observation into creating unforgeable quantum money in 1969. (Current anti-counterfeiting of cryptocurrencies and e-money relies on online verification by transaction registers, post-detection by cryptography, or tamper resistance in a trusted execution environment.) Although current digital technologies can prove that information is stored, they cannot prove that it has been deleted. This makes the disposal of information uncertain and creates the risk of information leakage. The feature article entitled "Functional Encryption Enabling Secure Leasing of Private Keys" [3] introduces research for proving that cryptographic private keys have been deleted. Now that quantum computers have become a common topic, not only are new applications sought, but research is also being conducted to integrate quantum physics, quantum information processing, and cryptography with the aim of establishing the basic theories. The feature article entitled "Quantum Algorithms with Potential for New Applications" [4] introduces research demonstrating quantum superiority, i.e., how the computational power of quantum computers surpasses current computers for certain tasks.

5. Conclusion

In this article, an overview of NTT's research on cryptography from the viewpoint of the development of quantum computers was presented. NTT Social Informatics Laboratories will continue to conduct research on a variety of topics, from foundations of cryptography, which will continue to be important as a basis of information sharing, to exciting applications far into the future. Going forward, we will continue to deploy technologies that will contribute to information distribution in the present as well as in the future.

References

[1] Cryptography Research and Evaluation Committees, "CRYPTREC Ciphers List," https://www.cryptrec.go.jp/en/list.html
[2] A. Hosoyamada, "Security of Hash Functions against Attacks Using Quantum Computers," NTT Technical Review, Vol. 21, No. 7, pp. 43–47, July 2023. https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202307fa4.html
[3] R. Nishimaki, "Functional Encryption Enabling Secure Leasing of Private Keys," NTT Technical Review, Vol. 21, No. 7, pp. 33–37, July 2023. https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202307fa2.html
[4] T. Yamakawa, "Quantum Algorithms with Potential for New Applications," NTT Technical Review, Vol. 21, No. 7, pp. 38–42, July 2023. https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202307fa3.html

Masayuki Abe
Senior Distinguished Researcher, NTT Social Informatics Laboratories.

He received a Ph.D. from the University of Tokyo in 2002. He joined NTT Network Information Systems Laboratories in 1992 and engaged in the development of fast algorithms for cryptographic functions and their software/hardware implementation and the development of a software cryptographic library. From 1996 to 1997 he was a guest researcher at ETH Zurich, where he studied cryptography, specifically multi-party computation, supervised by Professor Ueli Maurer. From 1997 to 2004 he was with NTT Information Sharing Platform Laboratories (now NTT Social Informatics Laboratories), where he worked on the design and analysis of cryptographic primitives and protocols, including electronic voting, a key escrow system, blinding signatures for digital cash systems, message recovery, and publicly variable encryption schemes. He also engaged in efficient multiparty computation based on cryptographic assumptions and zero-knowledge proofs in multiparty computation. From 2004 to 2006 he was a visiting researcher at IBM T. J. Watson Research Center, NY, USA, working with the Crypto Group, where he researched hybrid encryption, zero-knowledge proofs, and universally composable protocols.

He served as a program chair for the 7th Cryptographers' Track at the RSA Conference on Topics in Cryptology in 2007, ACM Symposium on Information, Computer and Communications Security in 2008, and the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security in 2010. His research interests include digital signatures, public-key encryption, and efficient instantiation of cryptographic protocols.

Functional Encryption Enabling Secure Leasing of Private Keys

Ryo Nishimaki

Abstract

Proving the non-existence of something is a difficult proposition called "the devil's proof." However, quantum mechanics can be used to prove that private keys used in functional encryption have been deleted (do not exist). It can also be used to prevent duplication of private keys. In this article, the method that my research colleague and I proposed at an international conference held by the International Association for Cryptologic Research in 2022 is overviewed, and the innovations expected when this method is implemented are described.

Keywords: cryptography, quantum computation, deletion of information

1. Advanced cryptography and private keys for the cloud era

One of the cryptographic methods used for one-to-many communication is called public-key cryptography. Anyone can encrypt a message without sharing a key in advance, and a private key is used to decrypt the message. Various *intelligent cryptosystems* that embed advanced logic in public-key cryptosystems are currently being proposed. A well-known example is attribute-based encryption in which user attributes are set in a private key and its decryption capability is based on those attributes. For example, if the encryption incorporates the conditions "personnel department" and "section chief," only the person holding the key with exactly the same attributes can decrypt it. Confidentiality of the message is protected because keys with attributes such as "personnel department/subsection chief" or "sales department/section chief" that only partially meet the conditions cannot decrypt the ciphertext above.

Functional encryption, which is studied by my research colleague and I in a paper titled "Functional Encryption with Secure Key Leasing" [1] published in January 2023, is a more-powerful type of intelligent cryptography. In contrast to attribute-based encryption, which can only obtain entire plaintext, functional encryption can obtain processed information computed from plaintext by decrypting ciphertext (**Fig. 1**). If functional encryption is practically applied, it will, for example, make it possible to calculate only statistical information from an encrypted database stocked with medical information on patients with intractable diseases in a manner that does not infringe the privacy of the patients. Advanced cryptography is expected to be a powerful tool for assuring information security in the cloud era.

Private keys can be generated on current computers.

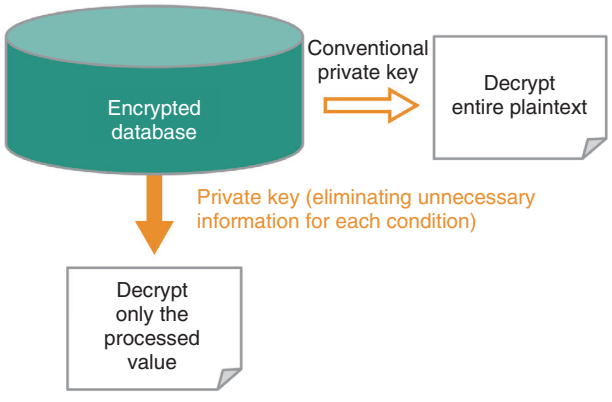


Fig. 1. Functional encryption.

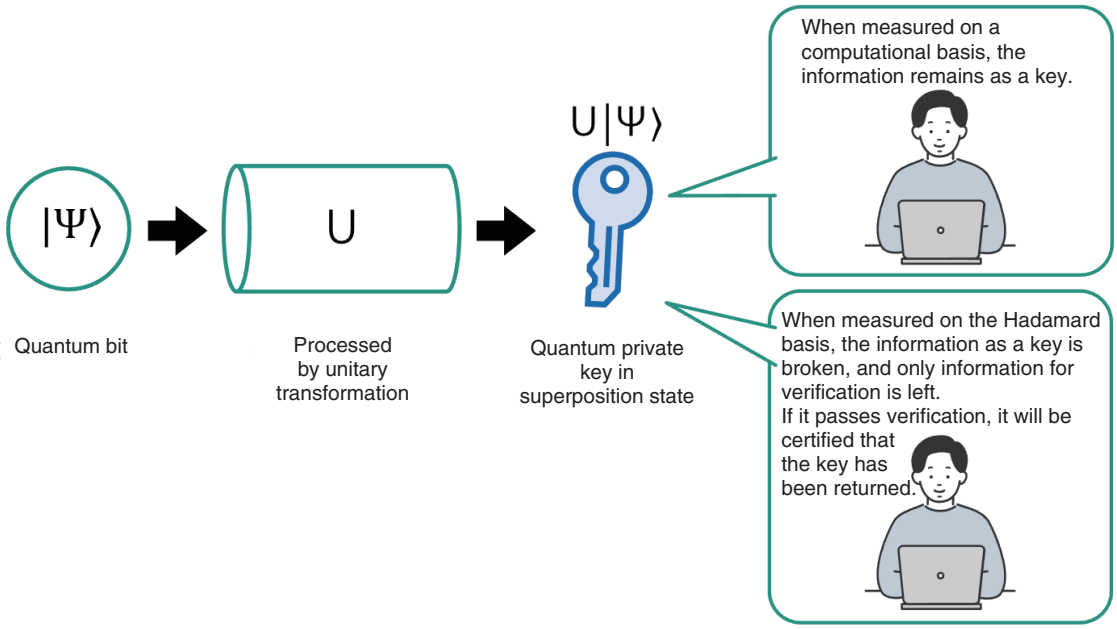


Fig. 2. How a quantum private key works.

However, it is impossible to prevent copying of key data once the key has been distributed. Even if the user insists the key is returned or deleted, the ciphertext can still be decrypted if the duplicate key is hidden. With that possibility in mind, we therefore applied the principle of quantum mechanics to prove mathematically that private keys of functional encryption can be deletable and uncopiable and proposed a secure key leasing based on that principle.

2. Using the uncertainty principle to delete the key by measurement

As a premise, it is assumed that both the host (who lends the key) and the user (who borrows the key) are using quantum computers. A quantum computer with a memory that can store quantum states and execute arbitrary algorithms is now in practical use, and private keys lent to users are also expressed in terms of quantum states. A private key is in a *superposition state* that changes on observation.

To delete such a private key, the quantum bit (qubit) of the key is first processed by a unitary transformation[*1] to generate a quantum key. During that transformation, information remains as a key when the key's superposition state is measured on a computational basis[*2] ($|0\rangle$, $|1\rangle$) but is deleted when it is measured on the Hadamard basis[*3] ($|+\rangle$, $|-\rangle$).

When the time comes to return the key, the user is asked to measure the quantum key on the Hadamard basis. If the superposition state is correctly measured, the key information is deleted in accordance with the uncertainty principle to leave behind only the classical information described as 0s or 1s (called certificate), and the certificate can be submitted as evidence of deletion.

If the measurement method differs from the specified one, the key information remains, and the key is not considered to have been returned. Therefore, changing the method of observing the superposition state makes it possible to delete part of the key information and delete the function of the key (**Fig. 2**).

There is a simple method for proving that a private key has been deleted and provide "the devil's poof." When the private key is deleted, a classical certificate is submitted as evidence of its deletion. After verifying the certificate, the host sends a new ciphertext to

*1 Unitary transformation: Changing an input qubit by applying an operation.

*2 Computational basis: A basic measurement to obtain information from the quantum state. A superposed qubit is represented as $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and if the qubit is measured by the computational basis, a measurement value of 0 will be obtained with probability $|\alpha|^2$ and the state will be $|0\rangle$ or 1 will be obtained with probability $|\beta|^2$ and the state will be $|1\rangle$.

*3 Hadamard basis: Whether the quantum state is $|+\rangle$ or $|-\rangle$ is measured. Hadamard operation converts $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$.

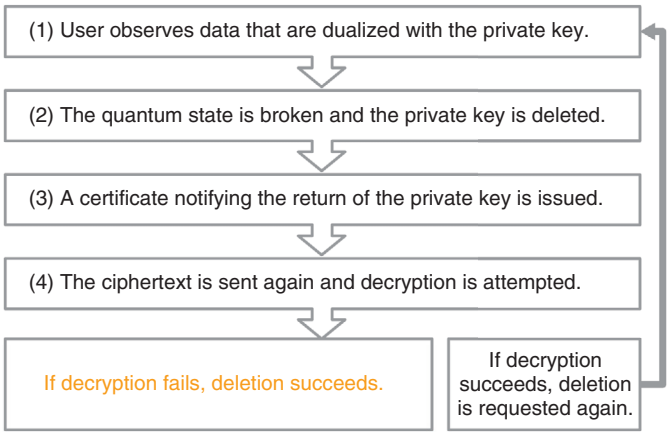


Fig. 3. Proof of deletion of quantum private key.

the user for decryption. If decryption fails, it is judged that the key does not exist; in other words, decryption failure equals deletion. This procedure/method is formulated in **Fig. 3**.

3. Copy protection from no-cloning

3.1 Private-key copy protection

Quantum mechanics are used to prevent copying of private keys. A quantum state created by oneself can be duplicated; however, according to the no-cloning theorem, an unknown quantum state given by another person cannot be duplicated. Even if an adversarial user attempts to duplicate an unknown quantum state, they will not be able to correctly decrypt a ciphertext by one of two quantum keys.

With this quantum key, it is impossible to extract the information that enables us to decrypt ciphertext. This status is explained by the fact that, as mentioned above, the uncertainty principle states that the state of the key will change at the moment it is observed to be copied, and the key will be lost. The only option is to leave the key in the quantum state without trying to measure it. Therefore, we have formulated and proved copy protection for such a private key.

The security of cryptography is classified into computational security, which is proven by computationally hard problems, and information-theoretic security, which is unbreakable even by an attacker with unlimited computational power. The proposed method, functional encryption with secure key leasing, guarantees computational security because it uses both quantum properties and computationally secure cryptography (**Fig. 4**).

3.2 Cryptographic technology for the future quantum society

Today, the cloud model is regarded as more important than the on-premises[*4] model, and quantum computers released in the US and Canada are operated by cloud services. Stronger cryptographic technologies are thus required in such one-to-many communication environments. Several technologies for revoking key data on classical computers have been proposed; however, they are inefficient and inconvenient if the private key is re-created for each generation of ciphertext. Moreover, if the ciphertext is updated all at once, various costs are incurred in proportion to the volume of the original data. The risk of old data is also a concern. We therefore thought that applying quantum mechanics to advanced cryptography would be an effective way to alleviate the costs and risks associated with encryption. We expect the scope of research on encryption procedures and theories for developing specific technologies to continue expanding.

4. Expansion into content services and the "right to be forgotten"

In the future, we believe that it will be possible that something based on the method reported in this article (i.e., functional encryption with secure key leasing) will become an international standard and be implemented in society. We say this because if the National Institute of Standards and Technology

*4 On-premises: Information systems are installed and operated in facilities managed by the user (e.g., a company).

Fig. 4. Copy protection of a quantum private key.

(NIST) in the US selects functional encryption as a next-generation encryption method, it will be standardized worldwide.

Although we are limiting ourselves to private keys in this article, our ultimate goal is to provide proof of program deletion and copy protection. When proof of program deletion and copy protection are implemented, they will change the way companies conduct research and development, manage information, and provide content services. In an example implementation, a quantum key is given to the customer and is valid only during the service usage period, and the key is invalidated when the contract period expires. These next-generation encryption technologies will also increase trust in third-party servers and cloud services and provide stronger protection for copyrights and other rights.

If old ciphertext remaining in search engines could be deleted completely, functional encryption may also be applicable to the "right to be forgotten" stipulated in Article 17 of the General Data Protection Regulation (GDPR) of the EU. We currently have no choice but to trust the other party's claim that "I deleted it," but quantum mechanics may enable us to respond technically to new concepts of rights (**Fig. 5**).

However, applying quantum mechanics is only possible if quantum computers are universal and used by general users. Considering the current error-correction capability, we believe that implementation of quantum-mechanics-based cryptographic technology is still some way off and requires further engineering in the development stage.

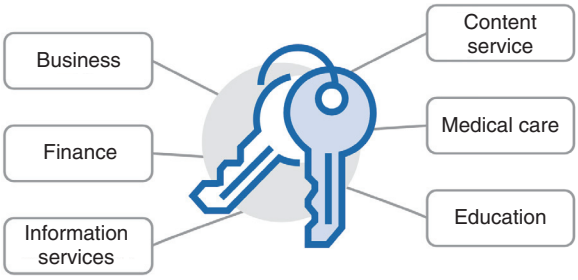


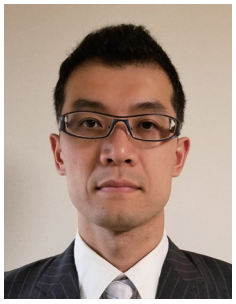
Fig. 5. Example categories in which functional encryption can be implemented.

Once quantum-mechanics-based cryptographic systems start working, the cryptographic technology will become global, so updating it will not be easy. From formulating theories to developing technologies and implementing them in society, various elements are intertwined, and we believe that process

will take a considerable amount of time.

Reference

[1] F. Kitagawa and R. Nishimaki, "Functional Encryption with Secure Key Leasing," Proc. of ASIACRYPT 2022, LNCS, Vol. 13794, pp. 569–598, 2022. https://doi.org/10.1007/978-3-031-22972-5_20



Ryo Nishimaki
Distinguished Researcher, Cryptography Research Laboratory, NTT Social Informatics Laboratories.
He received a B.E. and M.I. from Kyoto University and D.S. from Tokyo Institute of Technology in 2005, 2007, and 2010. He joined NTT in 2007. His research is focused on design and foundation of cryptography. He is currently researching cryptography and information security at NTT Social Informatics Laboratories.

Quantum Algorithms with Potential for New Applications

Takashi Yamakawa

Abstract

This article outlines a new algorithm devised by NTT for quantum computers (Yamakawa et al. "Verifiable Quantum Advantage without Structure"). Quantum computers are being developed worldwide. However, the types of algorithms that use them are scarce, which may limit their applications. The new algorithm presented in this article is a possible solution to this problem. For the first time, NTT demonstrated a super-fast quantum algorithm that solves a type of difficult problem called "NP (non-deterministic polynomial time) search problem without structure." This algorithm was highly acclaimed in academia as potentially leading to the discovery of new applications for quantum computers.

Keywords: quantum algorithm, hash function, NP problem

1. Introduction

Quantum computers, which are expected to be the next generation of super-fast computers, have a major challenge. They are currently limited to a narrow range of applications. The greatest advantage of quantum computers is that they are capable of much faster computation than current computers. To benefit from this advantage, it is essential to have algorithms that take advantage of quantum computers to compute efficiently. However, such algorithms are scarce.

It is estimated that at least 5 to 10 years of development are still needed before quantum computers are ready for practical use. In the meantime, if we do not devise many algorithms that can theoretically support fast computation, we may end up with a waste of treasure.

The algorithm developed by NTT has the potential to change this situation because it can solve a type of problem for which quantum speed was not thought possible [1]. Previously, researchers believed that quantum algorithms require a structure to solve problems[*1], but NTT's algorithm is able to solve problems without any structure. A typical example of a quantum algorithm that solves a problem with structure is Shor's algorithm [2], which is well-known for cracking ciphers widely used on the Internet. Shor's algorithm was published in 1994.

NTT's algorithm has been highly acclaimed in academia. The paper describing the algorithm [1] was published at the IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2022, the premier international conference in theoretical computer science, the same conference where Shor's algorithm was presented. Professor Scott Aaronson of the University of Texas at Austin, one of the leading experts in quantum computing, cited it as the latest breakthrough in a talk at the Solvay Conference, known for its historic discussions on quantum mechanics [3]. According to Quanta Magazine, a well-known online scientific publication, many researchers have been inspired by it and have begun exploring the possibility of new applications [4].

2. Verifiability

Figure 1 summarizes the positioning of this new algorithm. Its key feature is that it simultaneously satisfies the properties of verifiability in addition to super-fastness and structureless properties. As the figure shows, there have been super-fast algorithms that can solve structureless problems such as the

*1 Professor Aaronson et al. conjectured that super-fast quantum algorithms exist only for structured problems [3]. The difference is that the target of this conjecture is a decision problem, whereas NTT's quantum algorithm is for a search problem.

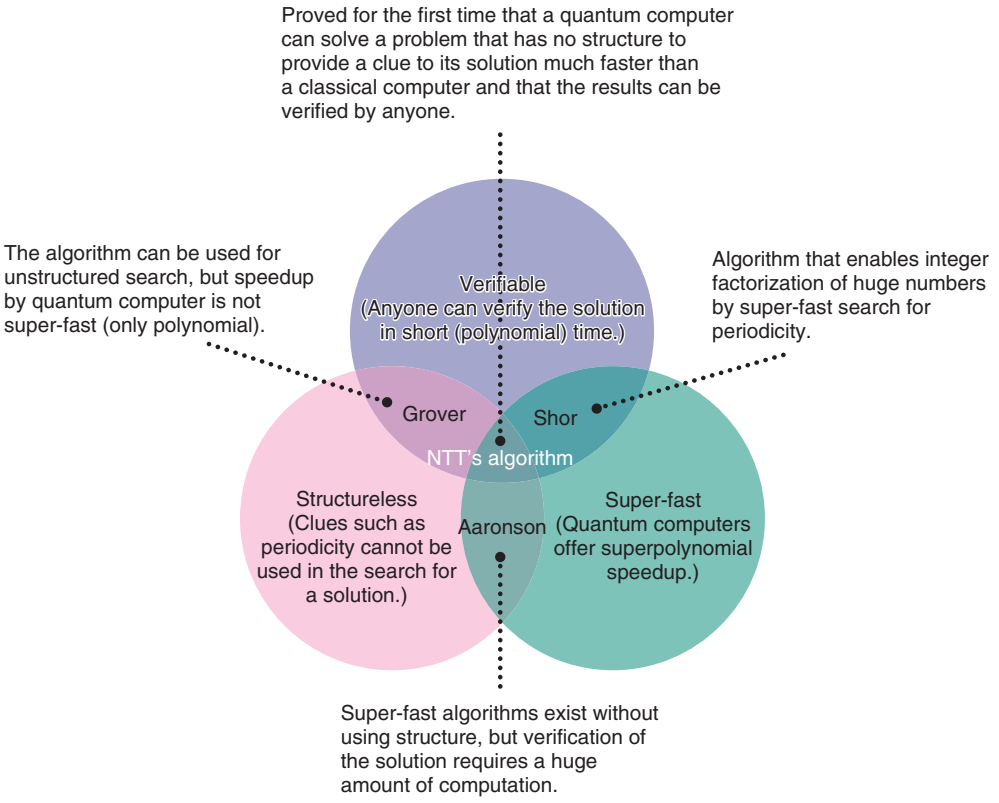


Fig. 1. Positioning of NTT's quantum algorithm.

algorithm proposed by Professor Aaronson [5]. However, these algorithms lack verifiability.

Verifiability means that it is easy to check whether the solution produced by the algorithm is correct. This is usually done using a conventional computer (called a classical computer in contrast to a quantum computer) rather than a quantum computer, and it must be possible to verify the solution in a short time. Current algorithms, however, require extremely long verification times, making it virtually impossible to verify whether the solution they produce is correct. In contrast, NTT's algorithm requires only a short time to verify the result.

Shor's algorithm is intended for integer factorization with large digits. For example, when 39,617 is factorized, the solution is 173 × 229. This is the correct solution, which can be quickly verified by simply multiplying them. When the number of digits is very large, the integer factorization is beyond the capability of a classical computer, but since the result can be verified only by multiplication, it does not take much time even for a classical computer.

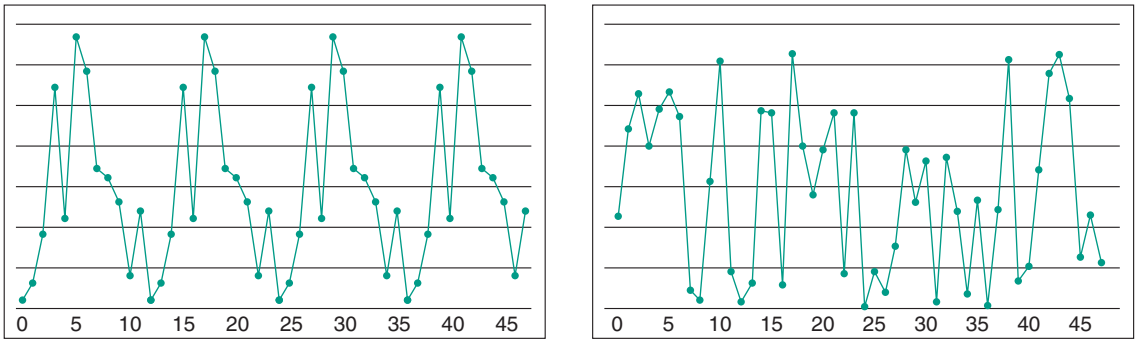
Problems that can be easily verified (in a short time[*2]) are called NP (non-deterministic polynomial time) problems, and the algorithm developed by NTT also targets an NP problem, or more precisely, an NP search problem.

3. Superpolynomial speedup

As Fig. 1 shows, there are also algorithms that solve structureless problems and still satisfy verifiability. An example is Grover's algorithm, which is a well-known algorithm that appears in quantum-computing textbooks. This algorithm lacks the super-fastness expected of quantum computers. At best, it can only achieve a polynomial speedup compared with the best classical algorithm[*3].

*2 Short time here refers to polynomial time. Polynomial time means that the computation time can be expressed in terms of a polynomial in the size of the problem (e.g., the number of bits to factorize). It increases slower than an exponential function.

*3 Grover's algorithm finds a solution from n candidates. The classical algorithm requires an average of $n/2$ times and maximum of n queries, while Grover's algorithm requires only $\sqrt{n}$ times. Comparing the two algorithms, the speedup is only quadratic.



(a) Remainder of a power of a natural number (periodic)

(b) Output of hash function (no structure such as periodicity)

Fig. 2. Difference between structured and structureless functions.

NTT's algorithm and Shor's algorithm are capable of a significant speedup that can be expressed in terms of mathematical expressions beyond polynomials, such as exponential functions. For example, the integer factorization of a 2048-bit integer used in standard Internet cryptography is a difficult problem that would take tens of thousands of years on a classical computer. However, it is estimated that a future large-scale quantum computer running Shor's algorithm could solve this problem in eight hours [6].

4. Finding the input of a random function

What is the structure used by Shor's algorithm? Shor's algorithm solves the integer factorization of a number N by reducing it to another problem. First, a natural number x that is coprime to N is chosen at random, and we consider the remainder of x^r divided by N. As the value of r changes, the remainder changes periodically, as shown in **Fig. 2(a)**. This period is the structure behind the problem.

The factors of N can be easily computed if this period can be found. While classical computers require a large number of computations to find the period, Shor's algorithm uses a method called quantum Fourier transform to achieve super-fast computation.

The structureless problems that NTT's algorithm targets are those that cannot be solved using such clues. The development of quantum algorithms often involves an oracle, which is a black-box that computes a function. An unstructured problem is based on a random oracle, which is an oracle that computes a completely random function. We focus on hash functions[*4] as a concrete example of a random oracle. As shown in **Fig. 2(b)**, there is no rule between the input and output of a hash function, and we can regard the output to be random.

However, hash functions are believed to be secure against attacks by quantum computers. Therefore, we make two modifications. The first is to use a vector of a special form as input, and the second is to apply a hash function, the output of which is one bit for each coordinate of the vector. For the former, we add the condition that the input vector is an error-correcting code[*5] converted from another bit string (**Fig. 3**).

The problem of finding the input from the output in this construction is the target of NTT's algorithm. This is a structureless NP search problem. While a classical computer requires a large amount of computation to solve this problem, we demonstrated that NTT's quantum algorithm can find a solution exponentially faster than a classical computer. The verification of the solution can also be easily implemented on a classical computer. In other words, all three conditions shown in Fig. 1 are satisfied.

5. Toward practical application

Figure 4 shows NTT's algorithm. In quantum computing, algorithms are usually represented as a quantum circuit, which is a combination of quantum gates, as shown in the figure. Although the details are beyond the scope of this article, it can be said that one

*4 Hash function: A function, the outputs of which look random. SHA-2 is a standard hash function used in cryptography.

*5 Error-correcting code: A coding method that converts data into a redundant data so that the original data can be recovered even if there is noise in communication. NTT's algorithm uses a code called Folded Reed Solomon code.

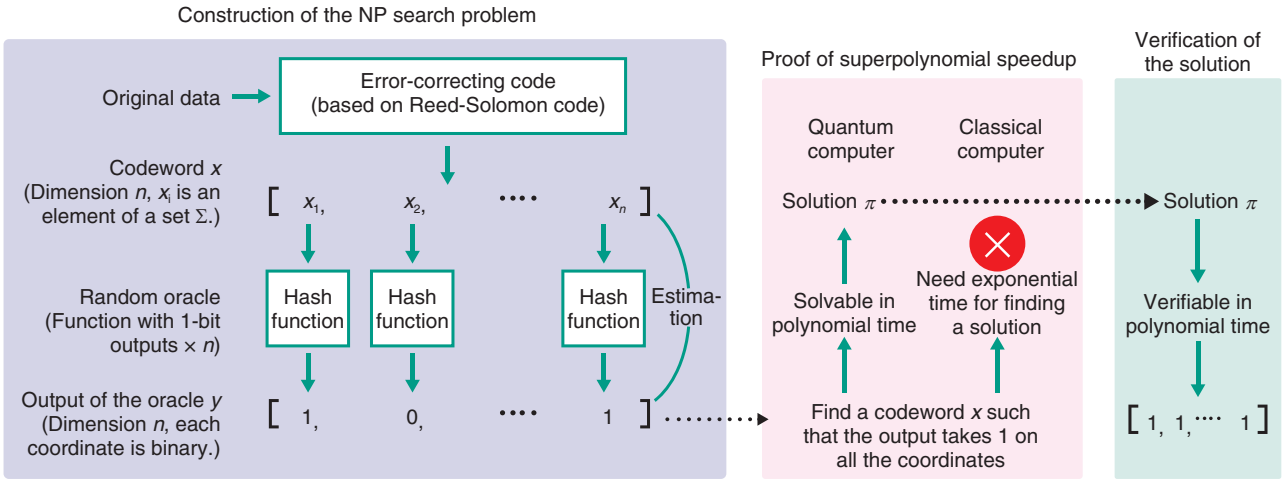


Fig. 3. The target NP search problem and the methods of proving and verification.

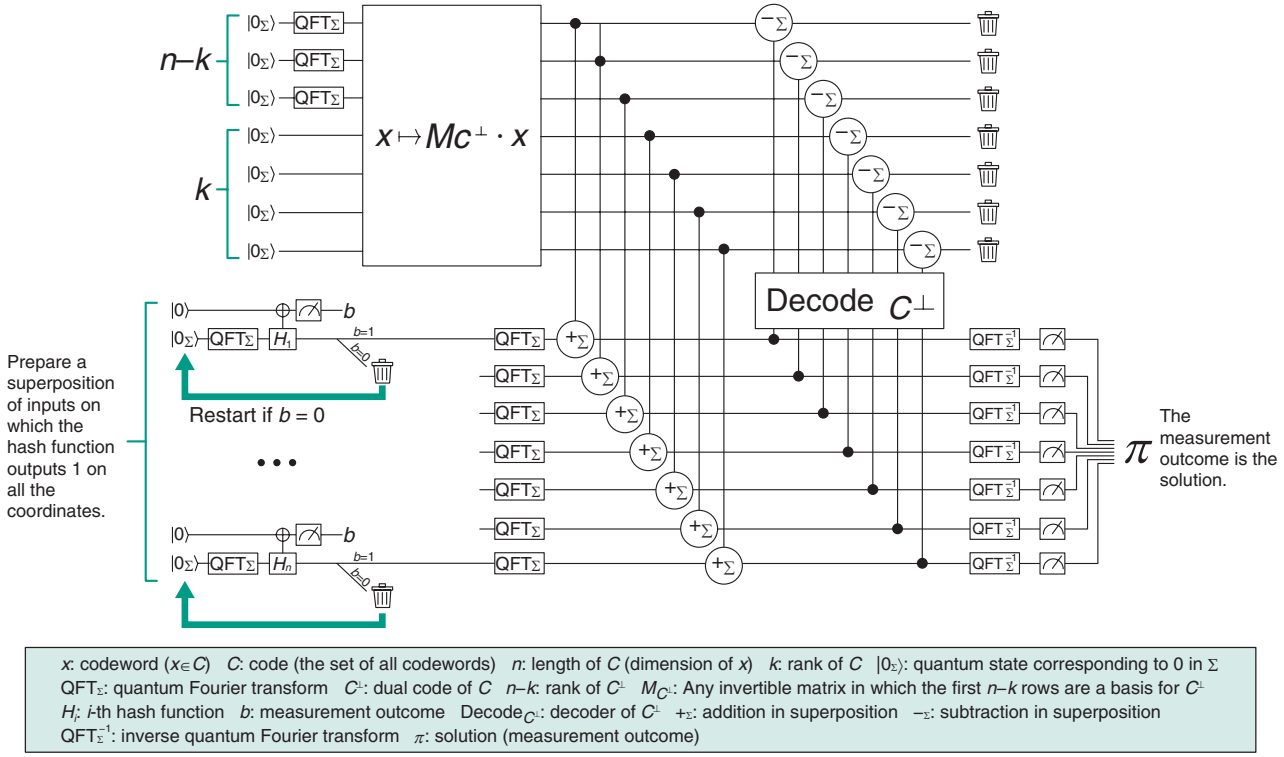


Fig. 4. Quantum algorithm that finds a solution.

of the key points of speedup is the quantum Fourier transform, indicated with QFT in the figure. Unlike Shor's algorithm, however, it is not used to find a structure.

What is the use of this algorithm? The problem solved in this study is intended only to explore the possibilities of quantum computers and has no specific application. The search for algorithms to solve realistic problems in the new direction presented in this article is a major challenge for researchers

around the world, including at NTT.

Peter Shor, who developed Shor's algorithm, recalls that a paper by Daniel R. Simons at a conference was a major inspiration [7]. The algorithm presented in the paper was for an unrealistic problem, and despite the support of Shor, who was a member of the program committee, the paper was rejected at the conference. We hope that the next Shor's algorithm will emerge from the many researchers who read our paper.

References

[1] T. Yamakawa and M. Zhandry, "Verifiable Quantum Advantage without Structure," Proc. of 63rd IEEE Annual Symposium on Foundations of Computer Science (FOCS 2022), pp. 69–74, Denver, CO, USA, Nov. 2022. https://doi.org/10.1109/FOCS54457.2022.00014

[2] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proc. of 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS 1994), Santa Fe, NM, USA, Nov. 1994. https://doi.org/10.1109/SFCS.1994.365700

[3] S. Aaronson, "How Much Structure Is Needed for Huge Quantum Speedups?", arXiv:2209.06930, Sept. 2022. https://doi.org/10.48550/arXiv.2209.06930

[4] M. Rorvig, "Quantum Algorithms Conquer a New Kind of Problem," Quanta Magazine, July 2022. https://www.quantamagazine.org/quantum-algorithms-conquer-a-new-kind-of-problem-20220711/

[5] S. Aaronson, "BQP and the Polynomial Hierarchy," Proc. of 42nd ACM Symposium on Theory of Computing (STOC 2010), Cambridge, MA, USA, pp. 141–150, June 2010. https://doi.org/10.1145/1806689.1806711

[6] C. Gidney and M. Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," Quantum, Vol. 5, p. 433, Apr. 2021. https://doi.org/10.22331/q-2021-04-15-433

[7] P. W. Shor, "The Early Days of Quantum Computation," arXiv:2208.09964, Aug. 2022. https://doi.org/10.48550/arXiv.2208.09964

Takashi Yamakawa

Distinguished Researcher, NTT Social Informatics Laboratories.

He studied cryptography at the Graduate School of Frontier Sciences, The University of Tokyo and received a Ph.D. in 2017. He entered NTT in the same year. He has been a distinguished researcher at NTT Social Informatics Laboratories since 2022 conducting research on quantum cryptography. He was a visiting scholar at Princeton University from 2020 to 2021 conducting joint research with Mark Zhandry, a leading scientist in this field. His papers have been accepted for presentation at Eurocrypt and CRYPTO sponsored by the International Association for Cryptologic Research (IACR), STOC sponsored by Association for Computing Machinery (ACM), FOCS sponsored by the Institute of Electrical and Electronics Engineers (IEEE), and other conferences.

Security of Hash Functions against Attacks Using Quantum Computers

Akinori Hosoyamada

Abstract

SHA-2 is a cryptographic hash function used worldwide. The possibility of attacks that exploit quantum computers can no longer be ignored; therefore, it is necessary to verify how the emergence of quantum computers could affect the security of SHA-2. The results of research conducted by my colleague and I indicate—as a world's first—that in a world in which quantum computers are available, the number of breakable steps in a collision attack on SHA-2 will increase.

Keywords: cryptographic hash function, SHA-2, quantum algorithm

1. Introduction to SHA-2

If a large-scale, general-purpose quantum computer becomes available for practical use, a malicious attacker could use it to break cryptosystems. To prepare for such attacks, it is necessary to verify the extent to which conventional cryptographic schemes can withstand them.

SHA-2 is one of the most-important cryptographic hash functions. It is standardized by the National Institute of Standards and Technology (NIST) and used unsuspectedly by users browsing websites on their personal computers and smartphones in a manner that supports the advanced information society from behind the scenes. Although hash functions are not ciphers, they are used as parts of various other cryptographic techniques and closely related to the security attained with such techniques[*1].

The main role of a cipher is to encrypt a message and write its content. It of course must be possible to restore the ciphertext (by using a private key) to the original message. In contrast, the role of a hash function (represented as "h") such as SHA-2 is to receive a message M as input and output a random value, h(M), in a manner that does not hide the content of M. A pair of separate messages, M and M', that satisfy h(M)=h(M') is called a *collision*, and a secure hash function must be able to withstand (i.e., be collision-resistant) attacks that attempt to discover collisions (**Table 1**).

When we consider collision attacks, we assume that an attacker is given a hash function h[*2] and simply wants to find M and M' that satisfy h(M)=h(M'). Therefore, a collision attack is slightly different from cryptanalyzing ciphers, which is an attack that attempts to recover the original message given the ciphertext encrypted with a cipher.

The extent to which a collision attack can be withstood is limited. An important concept that explains this limitation is the birthday paradox[*3]. An attack applying this concept (birthday attack) finds a collision of an arbitrary hash function with time complexity $2^{n/2}$ if the length of outputs is n-bit. A birthday attack is a generic attack that can be applied regardless of the degree of security of the hash function.

This, in turn, means that a secure hash function must resist collision attacks (using classical computers) with time complexity less than $2^{n/2}$. For example, if a dedicated attack finds a collision of a certain hash

*1 Design of practical hash functions is included in symmetric-key cryptography mainly because it often appropriates the design techniques of symmetric-key ciphers.

*2 More precisely, the algorithm that computes h.

*3 The birthday paradox: Each person has 365 possible birthdays. Even if 20 or so random people are gathered and asked about their birthday, the probability of finding a pair of people with the same birthday is fairly high.

Table 1. Comparison between cipher and cryptographic hash function.

	Cipher	Cryptographic hash function
Functionality	(1) Encrypt messages to produce ciphertexts (2) Decrypt ciphertexts to original messages (given the secret key used in encryption)	Given a message M, output a random value h(M)
Security	(1) Original messages cannot be guessed from ciphertexts (2) Indistinguishability, etc. (details omitted in this article)	(1) It is difficult to find distinct messages M and M' such that h(M)=h(M') (such a pair (M, M') is called a collision of h). Namely, h has resistance against attacks to find a collision (="collision resistance"). (2) Preimage resistance, etc. (details omitted in this article).

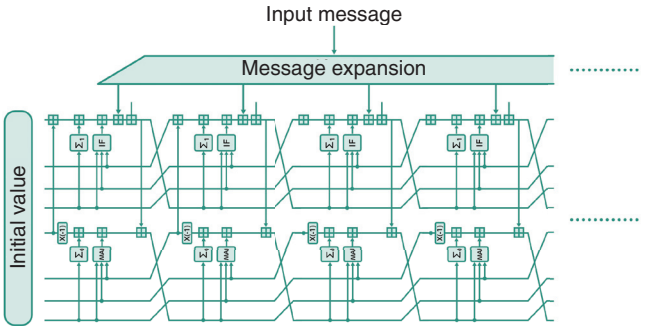


Fig. 1. Many steps are iterated to produce hash values. (In fact, there is a finalization procedure, which is omitted in this article. The representation of step functions is the one shown in [1].)

function with computational complexity of less than $2^{n/2}$, it is considered that the hash function has a unique weakness and has been broken. In other words, computational complexity $2^{n/2}$ of a birthday attack is the criterion for judging whether a dedicated attack targeting a specific hash function is a meaningful one.

2. Security indicators of SHA-2

The mechanism by which SHA-2 calculates the output is explained as follows. First, the input data are expanded into message blocks. Each message block is used to update the value of the internal state. With an initial value as the start point, the final output (hash value) is computed by repeatedly updating the internal state many times by using the message blocks (**Fig. 1**).

The design of typical hash functions, including SHA-2, involves many iterations of similar operations, and, as the number of iterations decreases, the hash function generally becomes less secure. Accordingly, the measure of security is based on the idea to what extent the hash function can be weakened to the point where it can be broken. For example, suppose that the original hash function is configured as ten iteration steps (**Fig. 2**, left) and it is known that if the number of steps is reduced to six, it is possible to find a collision with computational complexity less than $2^{n/2}$. Then, it is said that the reduced (six-step) version of the hash function is broken (Fig. 2, right). A hash function is considered broken when the original function without step reductions is broken. Even if the number of attacked steps has not reached the original number, an attack can be considered a meaningful attack if the number of broken steps is increased.

When a hash function carefully designed by a professional is broken, the number of broken iterations gradually increases. It is rare that the original function suddenly breaks. The fact that researchers from all over the world have tried to attack SHA-2 but only considerably weakened versions are broken ensures the security of the hash function.

3. Can quantum computers even promptly break hash functions?

Since hash functions such as SHA-2 do not have a neat algebraic structure like that of prime factorization, it has been thought that they would not be

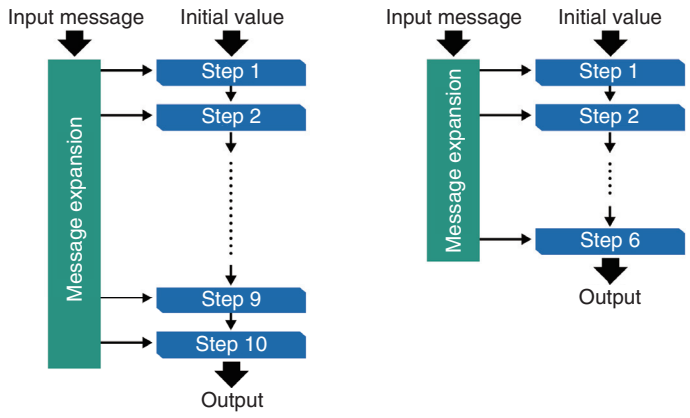


Fig. 2. A hash function the number of steps of which is ten (left). The 6-step reduced version (right).

Table 2. The number of breakable steps (AES-MMO and Whirlpool).

Attack target	Number of total steps	Number of breakable steps (classical)	Number of breakable steps (quantum)
AES-MMO	10	6	7
Whirlpool	10	5	6

immediately breakable with the advent of quantum computers. It has been shown that the computational complexity of the generic collision attack*4 fell from $2^{n/2}$ of the birthday attack to $2^{n/3}$ (i.e., that of the Brassard–Høyer–Tapp (BHT) algorithm). However, the reduction in computational complexity is not so large, so it is accepted that it poses no particular problem as long as a hash function with a slightly larger n is used.

However, as research progressed, it became clear that the situation was not so simple. First, as shown in **Table 2**, it was shown that hash functions, such as Advanced Encryption Standard Matyas–Meyer–Oseas (AES-MMO) and Whirlpool, can be broken by quantum computers in one more iteration, namely, one more step than in the case of classical computers. Quantum computers are clearly more capable of breaking hitherto robust cryptography than classical computers [2].

The increase in the number of breakable steps is based on the idea that while the computational complexity of generic collision attacks does not decrease significantly, the computational complexity of dedicated attacks that target specific hash functions may decrease to a greater degree, so the power of dedicated attacks may increase relatively. For example, when a quantum algorithm called Grover's algorithm is used for attacks, the computational complexity of differential cryptanalysis, which is often used for dedicated attacks, could fall to about the square root of the original [3]. On the contrary, it has been proven that the computational complexity of a generic collision attack does not fall below that of the BHT algorithm, and the degree of decrease in computational complexity does not reach the square root of the original (**Table 3**).

As described above, one (classical) measure of security of a hash function is how many steps must be removed to break the function. The effectiveness of a dedicated attack on a hash function that has been reduced to a specific number of steps was determined by whether the computational complexity of the attack was less than that of the generic attack. In a world where quantum computers are available, the computational complexity of a generic attack, which should be the criterion for determining whether the attack is successful, does not change much. In comparison, the speed-up for dedicated attacks by quantum computers is relatively greater. It must therefore

*4 Generic collision attack: A collision attack, such as a birthday attack, that can be applied to any secure hash function.

Table 3. Comparison of quantum speed-up for generic attacks and differential cryptanalysis. The complexity of quantum generic attack changes depending on computational resources assumed to be available, the details of which are omitted in this article.

Attack	Classical	Quantum	Speed-up
Generic	$2^{\frac{n}{2}}$	$2^{\frac{n}{3}}$	Less than quadratic
Differential cryptanalysis	T	$\sqrt{T}$	Quadratic

Table 4. Comparison of the number of breakable steps (SHA-256 and SHA-512). The classical results are from [5] and [6].

Attack target	Number of total steps	Number of breakable steps (classical)	Number of breakable steps (quantum)
SHA-256	64	31	38
SHA-512	80	27	39

be concluded that there are more types of dedicated attacks judged to be more effective in the quantum world than in the classical world.

By carefully investigating such a criterion under the assumption that quantum computers are available, collision attacks on 7-stage AES-MMO and 6-stage Whirlpool turned out to be effective in a world where quantum computers are available, even though they were not judged effective in the classical sense. These attacks are concrete examples demonstrating the importance of the aforementioned viewpoint.

4. Attacks on SHA-2 by quantum computers

Hash functions such as AES-MMO and Whirlpool are, however, minor compared to SHA-2, and their usage scenarios are relatively limited. That situation naturally raises the question of whether the number of breakable steps of SHA-2, i.e., the most widely used hash function today, is increased if quantum computers are available. This question is the main theme of this report.

We eventually found that the number of breakable steps can be increased as expected. SHA-2 is a generic term that includes several functions with different output lengths such as SHA-256 and SHA-512, and we found collision attacks on SHA-256 and SHA-512 that are classically ineffective but judged effective in a world with quantum computers [4].

If a classical computer is used, the collision resistance of SHA-256 is broken when the number of steps is reduced to 31, while the original number of steps is 64. However, no attacks were found that would break collision resistance when more than 31 steps were iterated. We found that, in a world where quantum computers are available, collision resistance is broken even after 38 steps. It can thus be said that quantum computers degrade the security of SHA-2, and we obtained a similar result on the security of SHA-512 (**Table 4**).

Of course, this result does not immediately indicate that the collision resistance of SHA-2 has been broken. SHA-2 is still safe to use. However, the above-mentioned results clearly indicate that the traditional broad view that quantum computers may not have much impact on the security of SHA-2 should be reconsidered.

5. Future developments

In a short period, information and communication technology (ICT) has made rapid progress, and in conjunction with that progress, cryptographic technology, which is the cornerstone of security, has become firmly established. Consequently, international-standard cryptographic techniques that can be used by anyone across the world[*5] have been established. However, there are many research questions

*5 Responding to the rapid development of quantum computers, NIST has been working on the standardization of quantum cryptography, especially public-key cryptography (and key encapsulation mechanism) and digital signatures, and has gathered a wide range of schemes from around the world. As of January 2023, some of the schemes have been completed, and some are set to be standardized.

yet to be investigated, especially when it comes to security against attacks using quantum computers.

Even the security of SHA-2, which plays a vital role in society, is not well understood. To address this lack of understanding, we conclude that in a world where quantum computers are available, the number of breakable steps in a collision attack on SHA-2 will increase.

We must continue to search for unknown attacks. Feedback from the study of these attacks will help us design more-secure hash functions in the future. Moreover, we believe that the publication of the results of such research on attacks will further enhance the security of ICT worldwide. Since an attacker may already be secretly conducting similar research, the goal is to anticipate further attacks by quantum computers and create cryptosystems that can sufficiently withstand them. It may be difficult to grasp the reality of these issues because they are of a dimension different from that of our daily lives. Regardless, as quantum computers come into practical use, it will be necessary to consider these issues before attackers do.

A dedicated attack targeting a specific cryptographic technique exploits the internal structure of the technique, so it is not necessarily applicable to other research. Even so, since the security of cryptography is closely related to our daily lives, we expect it to be of broad interest.

References

[1] F. Mendel, T. Nad, and M. Schläffer, "Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions," Proc. of ASIACRYPT 2011, LNCS, Vol. 7073, pp. 288–307, 2011. https://doi.org/10.1007/978-3-642-25385-0_16

[2] A. Hosoyamada and Y. Sasaki, "Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound," Proc. of EUROCRYPT 2020, Part II., LNCS, Vol. 12106, pp. 249–279, May 2020. https://doi.org/10.1007/978-3-030-45724-2_9

[3] M. Kaplan, G. Leurent, A. Leverrier, and M. N. Plasencia, "Quantum Differential and Linear Cryptanalysis," IACR Trans. Symmetric Cryptol., Vol. 2016, No. 1, pp. 71–94, 2016. https://doi.org/10.13154/tosc.v2016.i1.71-94

[4] A. Hosoyamada and Y. Sasaki, "Quantum Collision Attacks on Reduced SHA-256 and SHA-512," Proc. of CRYPTO 2021, Part I., LNCS, Vol. 12825, pp. 616–646, 2021. https://doi.org/10.1007/978-3-030-84242-0_22

[5] F. Mendel, T. Nad, and M. Schläffer, "Improving Local Collisions: New Attacks on Reduced SHA-256," Proc. of EUROCRYPT 2013, LNCS, Vol. 7881, pp. 262–278, 2013. https://doi.org/10.1007/978-3-642-38348-9_16

[6] C. Dobraunig, M. Eichlseder, and F. Mendel, "Analysis of SHA-512/224 and SHA-512/256," Proc. of ASIACRYPT 2015, Part II., LNCS, Vol. 9453, pp. 612–630, 2015. https://doi.org/10.1007/978-3-662-48800-3_25

Akinori Hosoyamada

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

He received a B.Sc. and M.Sc. from Kyoto University in 2014 and 2016 and Dr. Eng. from Nagoya University in 2021. He joined NTT Secure Platform Laboratories in 2016. Since then, he has been studying cryptography. He received the IWSEC 2017 Best Paper Award, SCIS Paper Award (2018), and Asiacrypt 2020 Best Paper Award. He is a member of the Institute of Electronics, Information and Communication Engineers (IEIEC) of Japan and the International Association for Cryptologic Research (IACR).

MagneShape: A Simple Pin-based Shape-changing Display Using Magnetic Materials

Kentaro Yasu

Abstract

Pin-based shape-changing displays provide dynamic shape changes by actuating numerous pins. However, the large number of actuators required to move so many pins complicates the electrical path and mechanical structure, and creates a need for significant resources if one is to build such a display. Therefore, my research colleague and I proposed a simple pin-based shape-changing display, called MagneShape, that outputs shapes and motions without any electronic components. MagneShape consists of magnetic pins, a pin housing, and magnetic sheet. The magnetic force generated between the magnetic sheet and the magnetic pins levitates the pins vertically. We devised two methods for fabricating alternative magnetic pins, devised a method for controlling the magnetic pins, and developed design tools for MagneShape.

Keywords: shape-changing interface, electronic-free, magnet

1. Introduction

Pin-based shape-changing displays have emerged as computer interfaces for presenting three-dimensional information for physical and haptic interactions [1, 2]. As the name implies, pin-based shape-changing displays have achieved dynamic shape presentation using dozens of pins with electronic actuators. However, as long as an electric motor is used as an actuator for each pin, the mechanical structure and wiring path increase in complexity as the pin array size increases. This issue is also argued in "Grand Challenges in Shape-changing Interface Research" [3], which calls for a toolkit for creating prototypes of shape-changing interfaces that do not require knowledge of electronics or mechanical engineering. Therefore, my research colleague and I aimed to create a shape-changing display with a non-electrical actuation system.

To tackle this issue, we focused on magnetic materials. Magnetic materials are used in many haptic-presentation techniques because they are passive but can generate physical force, and their magnetic polarity can be easily rewritten using a strong magnet [4, 5]. By applying these properties of magnetic materials, we devised a construction method for pin-based shape-changing displays that do not use electric actuators.

2. MagneShape

Our magnetically actuated pin-based shape displays are easy to build, easy to control, and can display characters and quick motions without any linear actuators. MagneShape (**Fig. 1(a)**), our simple pin-based shape-changing display, does not use electronic actuators to move the pins but instead relies on magnetic forces. The basic configuration of the display comprises magnetic pins, a plastic housing, and magnetic rubber sheet. The body of each magnetic pin consists of a plastic straw, and each straw has a small magnet inserted at its lower end. The pins are inserted into the housing to create a pin array. When the magnetic sheet is moved, the magnetic pins in the housing move up and down due to the attractive and repulsive forces generated between the magnetic pins

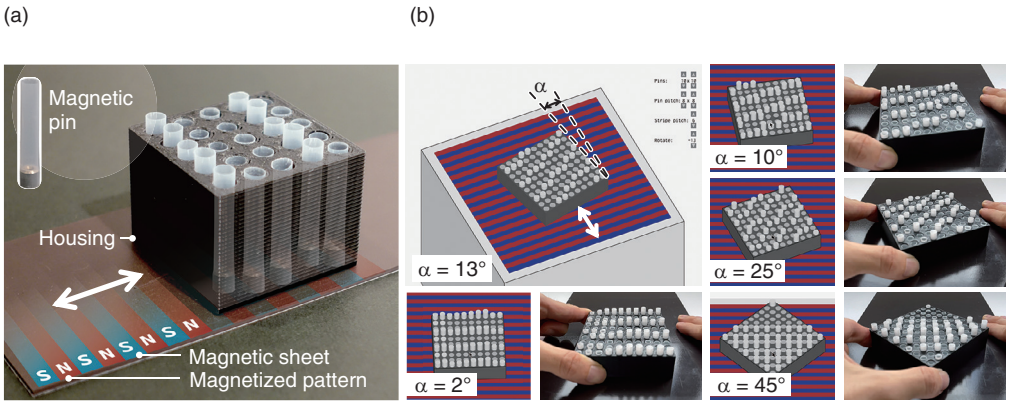


Fig. 1. The basic configuration of MagneShape (a) and comparison of simulation results with actual pin motions (b).

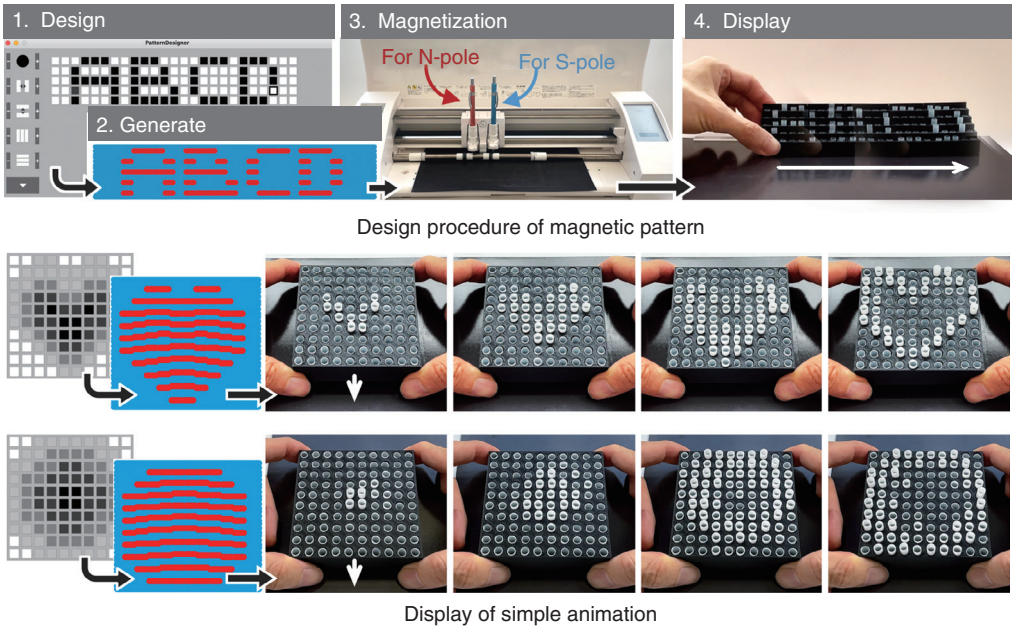


Fig. 2. Design process for magnetic-pattern generation and examples of simple animation presentations.

and magnetic sheet.

We have also implemented design tools for the pin-based shape-changing display. Our pin-motion simulator software allows the user to see how the pins will behave in advance (**Fig. 1(b)**), and our pattern-generation program automatically generates magnetic patterns in accordance with the shapes to be presented (**Fig. 2**). By moving the pin array on a magnetic sheet, it can display characters, flowing waves, a blinking heart, and a circular ripple. For this technique, no wiring, power supply, or programming is needed. This method enables users to design, build, and operate pin-based shape-changing displays without burdensome equipment, a large budget, or deep knowledge of electronics and engineering.

3. Challenges faced in achieving long pin strokes with high resolution

There were several challenges in determining the basic configuration of MagneShape. The first challenge was that posed by magnetic interference

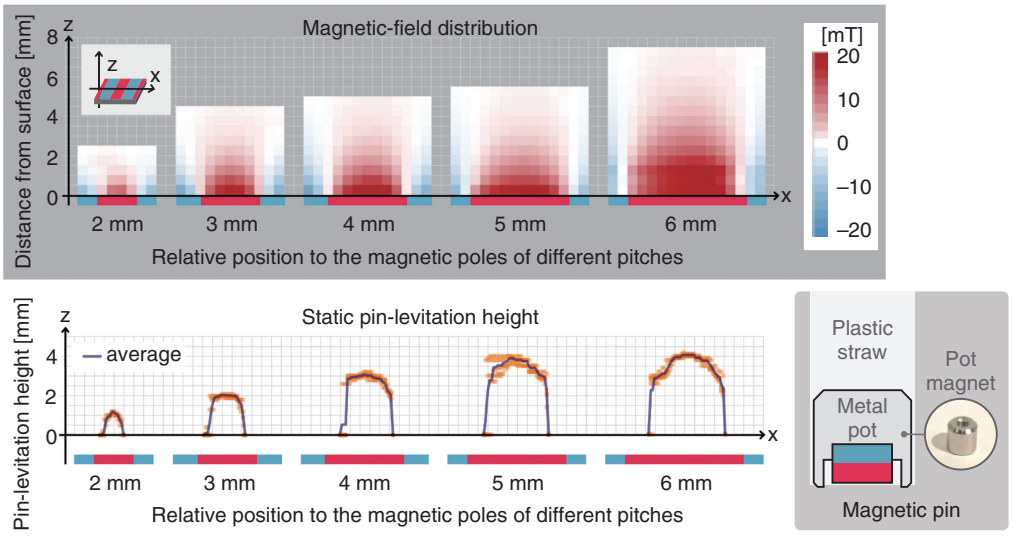


Fig. 3. The spatial magnetic flux density above the different magnetic stripes affects the levitation height of the magnetic pins.

between the pins. The larger the magnet, the stronger the magnetic field emitted, and the stronger the magnetic field, the higher the magnetic pins will levitate. However, if the magnetic fields around the magnetic pins are too strong, the spatial resolution of the pin-based shape-changing display will drop, because too strong a magnetic force will attract or repel magnetic pins adjacent to the one being targeted, causing interference and preventing the independent manipulation of each pin. To counter this interference problem, we used pot magnets in the pins of MagneShape. Pot magnets are fabricated by fixing a permanent magnet into a container called a pot, made of iron or other material with high magnetic permeability. Since the pot prevents the magnetic flux from leaking out from the sides or top of the magnet and concentrates it downwards, the spatial resolution of the pin array is improved significantly by using pot magnets.

We then examined how far the magnetic pins could levitate and how much the levitation height varied, depending on the pitch of the magnetic stripes on the magnetic sheet. We prepared magnetic sheets with 2–6-mm-pitch magnetic stripe patterns, placed the pin array on the magnetic sheet, and measured the levitation height of the five magnetic pins above the N-pole while adjusting the position of the pin array in 0.1-mm steps. **Figure 3** shows the results and average levitation height for the five pins. The pins gradually rose and reached their maximum height just above the centerline of the N-pole, and the maximum levitation height varied from 1–4 mm as the stripe width was changed from 2–6 mm.

However, in proposing this magnetic pin configuration as a component of the prototyping method for a pin-based shape-changing display, a problem presents itself in the small size range of commercially available pot magnets. Therefore, we devised two methods for fabricating alternative magnetic pins. The first method, which we called the *punch-sheet* method, uses a magnetic sheet and hole puncher or leather punch tool. The other method, which we called the *pot-like* method, involves building a pot-like structure by assembling some off-the-shelf parts. Although users need to assemble materials and craft them to make magnetic pins, these methods enable the creation of pins in various sizes, weights, and magnetic strengths. We created 23 different sizes of magnetic pins using these methods and investigated the minimum pin pitch across all of them. We then selected two alternative magnetic pins that functioned effectively when the margin between pins was equivalent to that in the array made with pins using commercially available pot magnets and measured the maximum dynamic levitation height for both of these two alternative magnetic pins. The measurement results reveal that the alternative magnetic pins reached maximum dynamic levitation heights of 16–20 mm when the pin array housing was moving at 80 mm/sec (**Fig. 4**). The pin stroke of the pin is thus significantly improved by using the alternative

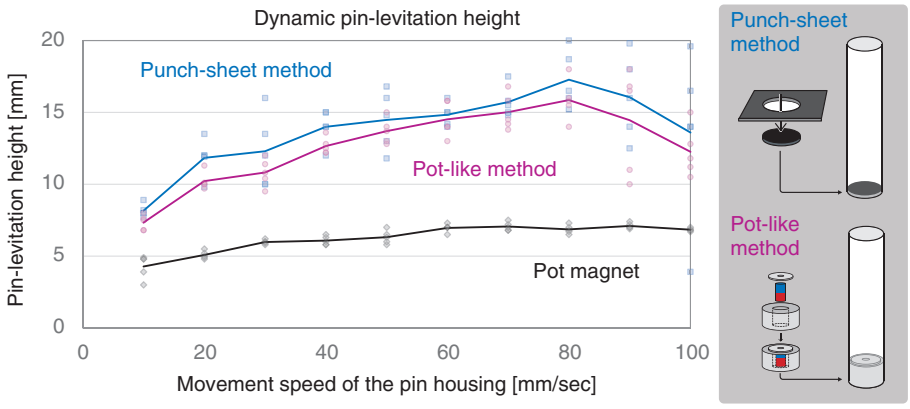


Fig. 4. The alternative magnetic pins produce significant improvements in dynamic levitation height compared with pins made with pot magnets.

magnetic pins.

4. Conclusion

We presented MagneShape: a simple pin-based shape-changing display that is easy to design, assemble, and operate. We also devised a method for controlling the levitation height of magnetic pins and developed design tools for the display. Using these design tools, MagneShape can present characters, a variety of waves, and simple animations.

To enable an increase in pin density within the array, we used pot magnets in the magnetic pins, which significantly improved the spatial resolution of the pin array. To address the generalizability of the magnetic pin concept, we devised two methods for fabricating alternative magnetic pins and found that some of such pins enable a much greater pin-levitation height than those made with pot magnets.

References

[1] S. Follmer, D. Leithinger, A. Olwal, A. Hogge, and H. Ishii, "inFORM: Dynamic Physical Affordances and Constraints through Shape and Object Actuation," Proc. of the 26th Annual ACM Symposium on User Interface Software and Technology (UIST '13), pp. 417–426, St. Andrews, Scotland, UK, 2013. https://doi.org/10.1145/2501988.2502032

[2] J. José Zárate and H. Shea, "Using Pot-magnets to Enable Stable and Scalable Electromagnetic Tactile Displays," IEEE Trans. Haptics, Vol. 10, No. 1, pp. 106–112, 2017. https://doi.org/10.1109/TOH.2016.2591951

[3] J. Alexander, A. Roudaut, J. Steimle, K. Hornbæk, M. B. Alonso, S. Follmer, and T. Merritt, "Grand Challenges in Shape-changing Interface Research," Proc. of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18), Montreal, QC, Canada, Paper no. 299, pp. 1–14, 2018. https://doi.org/10.1145/3173574.3173873

[4] K. Yasu, "Magnetic Plotter: A Macrotexture Design Method Using Magnetic Rubber Sheets," Proc. of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17), pp. 4983–4993, Denver, Colorado, USA, 2017. https://doi.org/10.1145/3025453.3025702

[5] K. Yasu, "Magnetact: Magnetic-sheet-based Haptic Interfaces for Touch Devices," Proc. of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19), Paper no. 240, pp. 1–8, Glasgow, Scotland, UK, 2019. https://doi.org/10.1145/3290605.3300470

Kentaro Yasu
Distinguished Researcher, Sensory Interface Research Group, Human Information Science Laboratory, NTT Communication Science Laboratories.

He received a B.E. in 2008, Master in media design in 2010, and Ph.D. in media design in 2013 from Keio University, Kanagawa. From 2013 to 2016, he worked as a research fellow at the National University of Singapore. In 2016, he joined NTT Communication Science Laboratories and began researching haptic display systems. In 2018, he developed Magnetact, a magnetic tactile printing technology. Since 2019, he has been a distinguished researcher and is engaged in work on information presentation technology using magnetic materials. His paper on magnetic field control technology through the layering of magnetic sheets received an honorable mention award at the 2020 CHI Conference on Human Factors in Computing Systems (CHI 2020), and his research into pin-based shape-changing display systems using magnetic materials won the best talk award at the 35th ACM Symposium on User Interface Software and Technology (UIST 2022). He is a member of the ACM Special Interest Group on Computer-Human Interaction (SIGCHI), and the Information Processing Society of Japan.

Efforts by TM Forum, an Operation Standards Organization

Shingo Horiuchi and Kenichi Tayama

Abstract

The TM Forum, an organization for standardization of operations, has been actively studying the Open Digital Architecture, which is the architecture of next-generation business support systems/operation support systems, the autonomous operation of networks using artificial intelligence, the use of metrics to penetrate digital transformation, and the transformation to a digitized organization including the skill elements of each individual. In Catalyst (proof-of-concept) projects, which are intended for a variety of business scenarios, efforts to use TM Forum assets for the autonomous operation of networks using intents in Smart-X business scenarios are underway. This article explains these efforts.

Keywords: TM Forum, autonomous network, intent management

1. What is the TM Forum?

1.1 Positioning and scope of the TM Forum

The TM Forum was established in 1988 as the Open Systems Interconnection/Network Management Forum, a non-profit organization for achieving information and communications network management that can be implemented comprehensively. Activities aimed at promoting network services in cooperation with other industries have been conducted. The forum has more than 850 member companies, including the world's leading companies in the telecommunications and information technology (IT) industries.

1.2 Themes and projects

The TM Forum is focused on transforming itself into a digital partner to enable flexible collaboration with other companies. To achieve this, the TM Forum established 6 focus themes: Cloud Native IT & Networks, AI (artificial intelligence), Data & Insights, Autonomous Operations, Beyond Connectivity, Customer Experience & Trust, and The Human Factor, among which 16 projects are being considered (**Fig. 1**). We describe the efforts of four projects we believe will deeply related to the actualization of NTT's digital transformation (DX) and IOWN (Innovative Optical and Wireless Network) Cognitive Foundation initiatives. This article also explains Catalyst (proof-of-concept (PoC)) projects at the TM Forum.

2. Open Digital Architecture and Open Digital Framework

2.1 Each element and component implementation of Open Digital Architecture

The Telecommunications Management Network model defined in ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) M. 3400 has long been implemented in real systems as the business support system (BSS)/operation support system (OSS) architecture. The TM Forum has defined the Open Digital Architecture (ODA) to respond to the radical advancements in operations through collaboration with other business partners, diversification of customer experience (CX), and AI technology. ODA has the following functions:

- Engagement Management: A functional unit that serves as a contact point with customers and operators for management focused on improving CX.
- Party Management: Manages relationships with

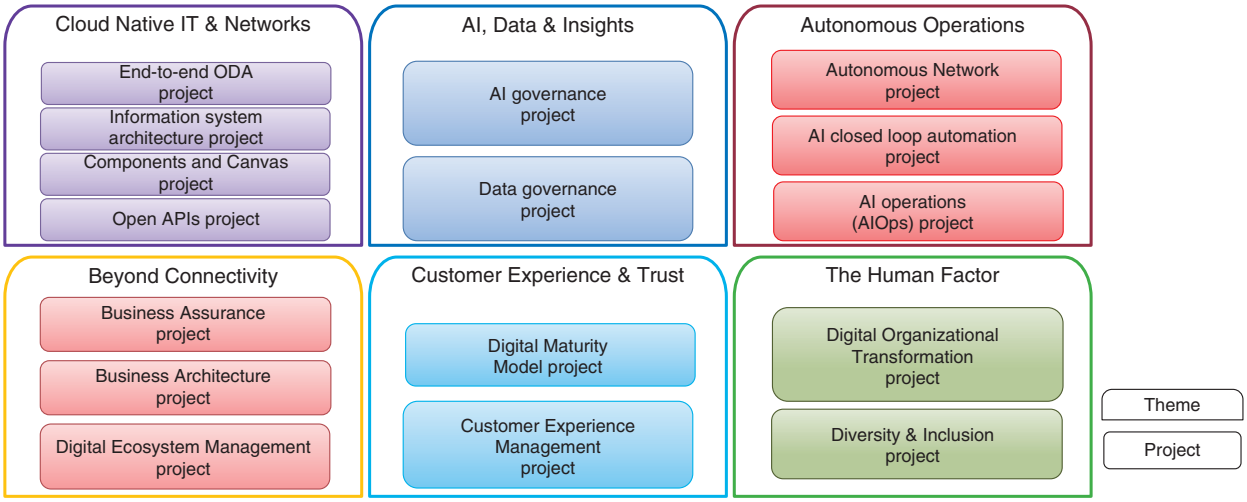


Fig. 1. Discussion themes and projects at TM Forum.

stakeholders such as characters and procurement partners in the B2B2X (business-to-business-to-x) business model.
- Core Commerce Management: For customer and product management and is equivalent to the BSS domain.
- Production: For service and resource management at end-to-end networks.
- Intelligence Management: Manages AI and other technologies to enable a closed loop in each management area.

The Components and Canvas project in the TM Forum is currently in the process of defining the components required for each area of ODA and developing microservices (**Fig. 2**).

2.2 Open Digital Framework and existing assets

The Open Digital Framework (ODF), a framework that uses tools and the maturity model, is currently being studied to make ODA a reality. The utilization and mapping of the business-process framework called the enhanced Telecom Operation Map (eTOM), application framework called Telecom Application Map (TAM), and information model called Shared Information/Data Model (SID), which have been conventionally specified in the TM Forum, are being examined. The content of eTOM, SID, and TAM is used as business requirements, information systems, and transformation tools, respectively, for building ODF systems.

3. Autonomous networks

3.1 Overall architecture and intent

The study of autonomous networks is aimed at the autonomous operation of networks. As well as at the TM Forum, discussions are being carried out with 3GPP (3rd Generation Partnership Project), ETSI (European Telecommunications Standards Institute) ZSM (Zero-touch network and Service Management) and ENI (Experiential Networked Intelligence), and others on the implementation architecture, model, and application programming interfaces (APIs) of autonomous networks. The overall architecture of autonomous networks is divided into a business-operation layer, service-operation layer, and resource-operation layer, and an autonomous network is achieved by linking the management layers. It also defines the level at which automation is possible and to implement an autonomous network in a gradual manner. The autonomous-network levels L0 to L5 provide definitions for stepping up from manual to automation from the execution, cognition, analysis, decision, intent, and application aspects (**Fig. 3**).

An autonomous network consists of business, service, and resource layers to enable a closed loop for each layer, automate each management layer in an optimal manner, and overall optimal autonomous operation by linking the closed loops of each layer (**Fig. 4**). In this context, the goal of each layer's closed loop is intent, and efforts to use intent as a key to link the layers of an autonomous network are attracting attention. The API and information models

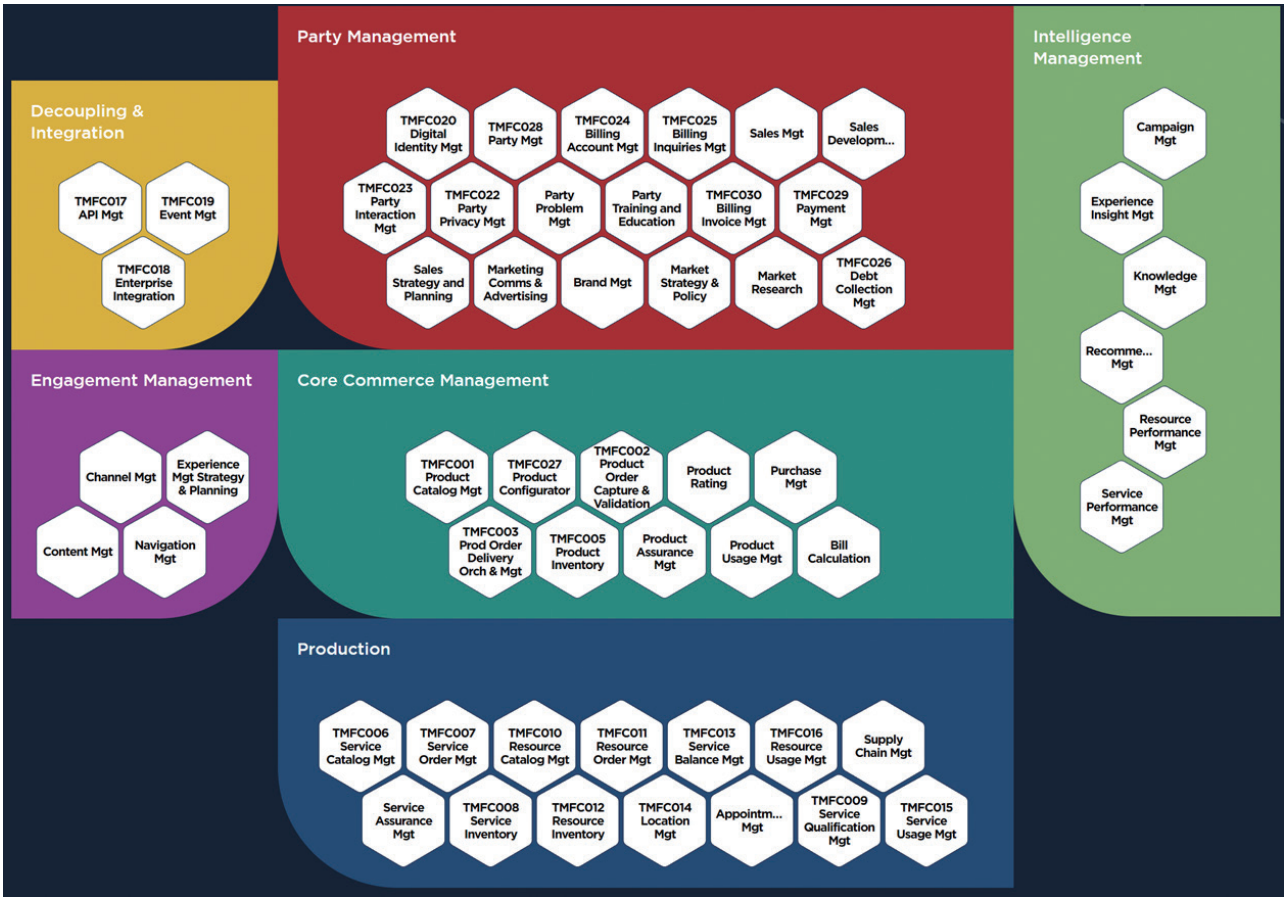


Fig. 2. ODA components.

Level Definition	L0: Manual Operation & Maintenance	L1: Assisted Operation & Maintenance	L2: Partial Autonomous Network	L3: Conditional Autonomous Network	L4: High Autonomous Network	L5: Full Autonomous Network
Execution	P	P/S	S	S	S	S
Awareness	P	P	P/S	S	S	S
Analysis	P	P	P	P/S	S	S
Decision	P	P	P	P/S	S	S
Intent/Experience	P	P	P	P	P/S	S
Applicability	N/A	Select scenarios				All scenarios

P: Personnel, **S:** Systems

Fig. 3. Autonomous network levels.

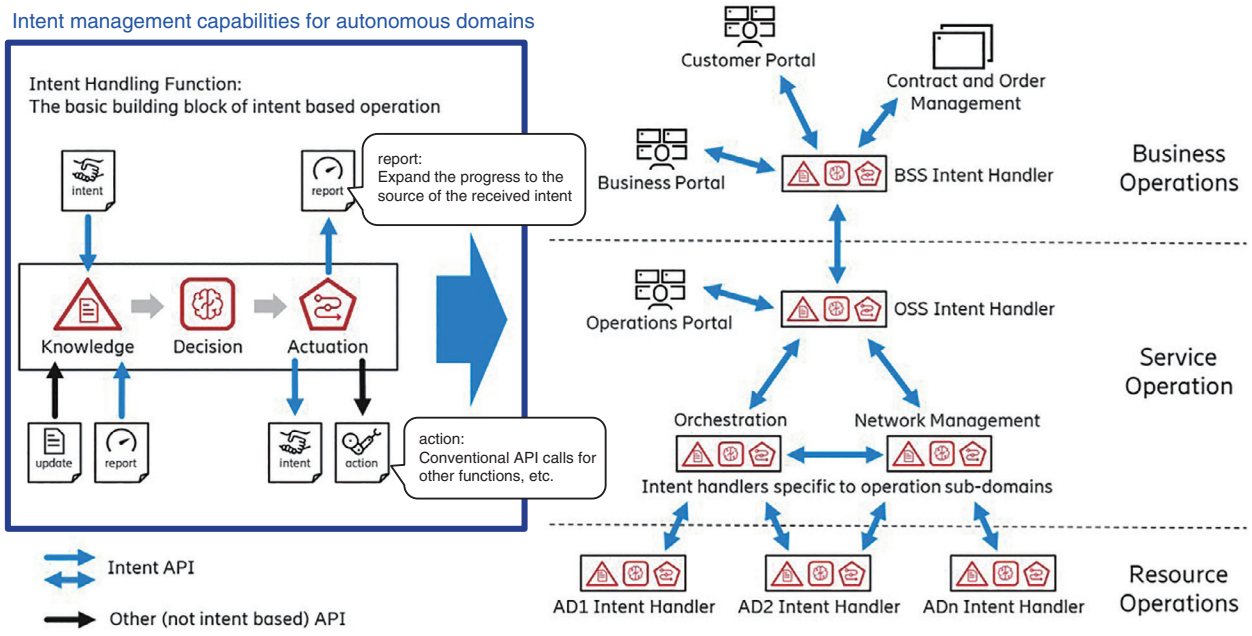


Fig. 4. Autonomous networks and intent.

needed to achieve these goals are being actively discussed, and many standards-related documents are being developed.

3.2 Closed loop

There are also discussions on reference architectures to achieve autonomous networks through closed loop mechanisms using AI technology. The functions and other aspects of Closed Loop Anomaly Detection & Resolution Automation, which is an architecture to enable automation of the maintenance phase based on ODA, are organized on the basis of the OODA (observe, orient, decide, act) structure, which is a decision-making framework, and the correspondence with specific use cases is summarized in TR 284 Closed Loop Automation Implementation Architecture (**Fig. 5**).

3.3 Intent Management API

The Intent Management API is an autonomous network with the role of an intent manager. The API for handling intents among systems such as BSS/OSS and Orchestrator is being studied. The intent manager includes the intent owner, which provides the intent, and the intent handler, which executes the configuration of service resources on the basis of the intent. In addition to creating, modifying, and deleting intents, the following functions, which are necessary for negotiating intents, are also being considered.

- JUDGE: Find the best intents that can be handled successfully.
- PROBE: Check with the owner if there are multiple actions derived by the handler after receiving an intent, and judgment is required.
- BEST: Check the feasibility of an intent.

4. Connectivity as a Service in the Digital Ecosystem Management project

4.1 CaaS

Connectivity as a Service (CaaS) is defined as a service in which a user who uses a network service provides the service by specifying only the start and end points and the characteristics required for the network. Users who use the network may not have specific requests or not know about routes in the middle of the network. CaaS is achieved by providing a combination of available services in response to user requirements. An API is being studied to achieve this goal, and a document summarizing the API requirements will be issued in fiscal year 2023.

4.2 Applying intents

CaaS requires users to derive specific services from order content, including vague requirements. Considerations are being made to incorporate the elements

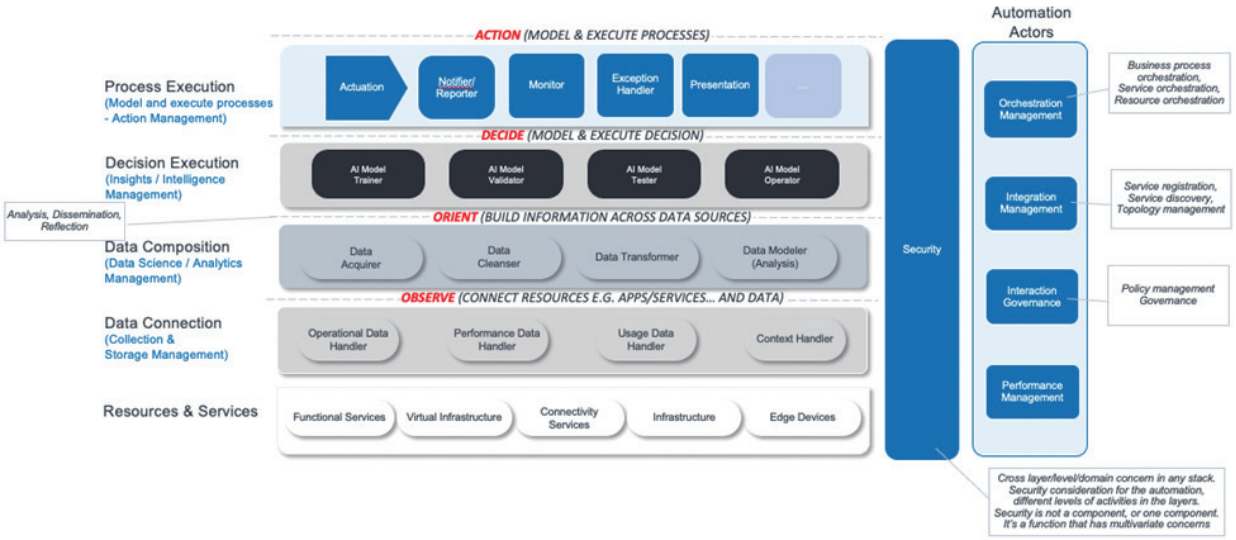


Fig. 5. Closed-loop automation architecture.

of intent discussed in the Intent Management API and apply intent as a condition for offering a 5G network slice. NTT Access Network Service Systems Laboratories (AS Labs) is investigating technologies to extract intents from user and operator interactions and reflect them in network services and is working to standardize use cases and technical requirements as CaaS APIs (Intent Management APIs).

5. Human-factor-related discussions

5.1 Digital Organizational Transformation project

As DX progresses, the Digital Organizational Transformation (DOT) project is being considered to bring the culture and skills of organizations and operators into a continuously evolvable form. In this project, factors such as the digital maturity model (DMM) and customer experience management (CEM) are also considered.

The DMM was originally an index used to objectively assess the degree of DX maturity of telecommunications operators and other entities, and using the DMM as an index to assess the maturity of digital culture from the perspectives of culture management, strategic alignment, collaboration, inclusion & diversity, and digital skills & enablement is being discussed. CEM has traditionally focused on each phase of a customer's recognition, use of a communication service, and the channel through which the customer is approached before finally canceling the service. DOT regards set up for success, frame the transformation, and execute transformation program "Transforming work, organization, skills & culture" as necessary phases for digital-culture transformation and has organized Strategic Leadership, Organizational Modelling and other enablers for each phase.

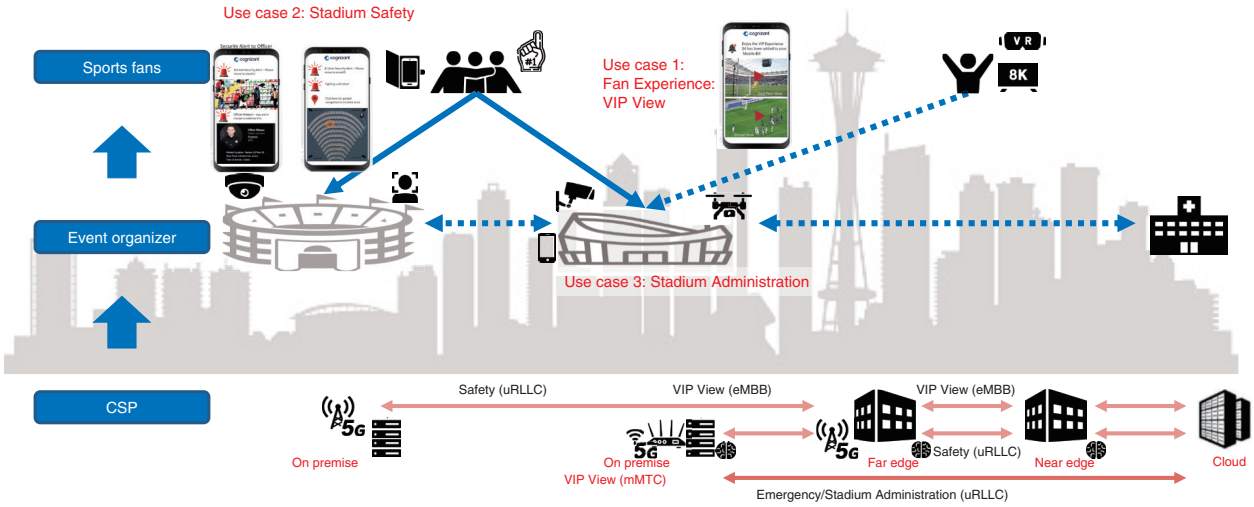
On the basis of these arrangements, the Digital Organizational Transformation Culture and Skills Guidebook analyzes digital culture and shows that it consists of an approach of initiation, realization, persistence, and iterative learning to keep changing the culture.

6. Catalyst (PoC)

6.1 Catalyst project

Catalyst refers to the PoC that conducts technology demonstrations at the TM Forum, which consists of a team of carriers and three or more vendors, and exhibits at Digital Transformation World (European event) and Digital Transformation World Asia (Asian event). Through Catalysts, we will increase the number of advocates for technical requirements and support their feasibility and practicality in reflecting the requirements in the standardized documents.

This fiscal year 2023's focus is on Smart X realization, and Catalysts that use metaverses and digital twins and address the ethics of AI algorithms as the governance of AI have attracted attention.



CSP: customer service provider
eMBB: enhanced mobile broadband
mMTC: massive machine type communications
uRLLC: ultra reliable and low latency communications
VIP: very important person
VR: virtual reality

Fig. 6. Scenario in the Catalyst called Autonomous-network hyperloops.

6.2 Catalyst example: Autonomous-network hyperloops

AS Labs is participating in a Catalyst called Autonomous-network hyperloops, consisting of Orange, Chunghwa Telecom, Verizon, TIM, Beyond Now, Futurewei, UBiqube, and NTT (**Fig. 6**). In fiscal 2023, we entered our fourth term, and since our third term, we have been conducting PoC demonstrations in various service-delivery scenarios on the basis of the intents of event organizers and participants at a smart stadium. In the fourth term, in addition to intent, we have begun to consider scenarios by adding requirements for mission-critical situations. Our Catalyst team won the Outstanding Showcase Award at Digital Transformation World Asia 2023 in March 2023.

Shingo Horiuchi
Senior Research Engineer, NTT Access Network Service Systems Laboratories.
He received a B.E. and M.E. in engineering from the University of Tokyo in 1999 and 2001 and joined NTT Access Network Service Systems Laboratories in 2001. He has been researching and developing access network operation systems. He has also been involved in standardization efforts for operations support systems in the TM Forum. He is a member of the Institute of Electronics, Information and Communication Engineers.

Kenichi Tayama
Group Leader, Senior Research Engineer, Supervisor, NTT Access Network Service Systems Laboratories.
He received a B.S. and M.S. from the University of Electro-Communications, Tokyo, in 1993 and 1995. Since joining NTT in 1995, he has been engaged in the research and development of access network operations and the planning and development of internal information technology systems and network operations and maintenance.