Secure Optical-transport-network Technology in Anticipation of the Quantum Computer Era

Keizo Murakami, Atsushi Taniguchi, Fumiaki Kudo, Sakae Chikara, Yutaro Kiyomura, Akio Mukaiyama, Yusuke Iijima, Yasuhiro Mochida, Yasuyuki Sanari, and Naohiro Kimura

Abstract

In the January 2022 issue of NTT Technical Review, we introduced the *secure optical transport network* for enabling secure optical transport even in the era of quantum computers. In this article, two concepts, cryptographic agility and Multi-Factor Security, which are key factors in the transition from current cryptographic techniques to quantum-resistant cryptographic techniques and need to be considered in the era of quantum computers, are explained, and our efforts to incorporate these concepts into secure optical transport networks (i.e., elastic-key-control technology and disaggregation technology for cryptographic processing) are introduced.

Keywords: optical transport network, post-quantum cryptography, IOWN Global Forum

1. Background

The amount of data, such as video and voice data, flowing over the network is becoming ever larger. The need for low-latency communications is becoming ever more important in areas such as finance and telemedicine. On top of that, it is important to reduce power consumption while maintaining services.

The All-Photonics Network (APN), one of the three components of the Innovative Optical and Wireless Network (IOWN), which is being researched and developed by NTT, aims to provide services with three appealing features: low power consumption, large capacity and high quality, and low latency [1]. In addition to the above-described issues, financial and telemedicine applications require a high level of security due to the financial losses and risk to human lives in the event of a system attack. These features are also important from the perspective of data distribution.

Quantum computers are expected to be put to practical use in the 2030s in applications such as solving traffic congestion, analyzing risks concealed in financial data, and developing new drugs. However, current cryptosystems, such as RSA (Rivest–Shamir–Adleman algorithm) and elliptic curve cryptography, will be vulnerable.

NTT Social Informatics Laboratories and NTT Network Innovation Laboratories are working to add security to IOWN APN by sharing a common key between optical transponders—by using post-quantum cryptography (PQC) and quantum-key distribution (QKD)—and communicating by using that key, and also have been researching and developing a secure optical-transport-network technology that is safe even in the quantum-computer era by encrypting communications with the key [2] (**Fig. 1**). From the viewpoint of data distribution, in addition to encryption of transmission paths and stored data, end-to-end

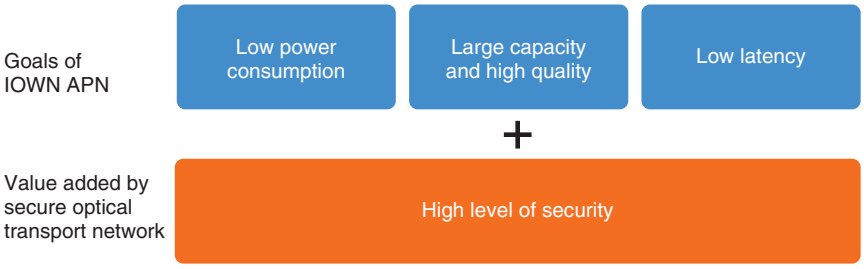


Fig. 1. Features of secure optical transport network.

security is required, and secure optical-transport-network technology is especially designed for transmission paths.

Furthermore, the IOWN Global Forum (IOWN GF) is currently discussing the ideal form of quantum-safe security[*1] required of IOWN in the quantum-computer era.

2. Challenges

Conventional key sharing by the secure optical transport network [2] guarantees secure information communications—even if conventional public-key cryptography is compromised[*2] by the development of quantum computers—by choosing either PQC or QKD depending on the application. PQC is a cryptographic scheme that uses a problem that even a quantum computer cannot solve efficiently as a basis for security. Although it has a shorter history than current cryptographic schemes, it is in the process of moving from the research stage to practical application. The National Institute of Standards and Technology (NIST) has begun standardization of key-exchange and signature schemes using PQC, which is expected to be implemented and widely used. On the contrary, research on the security of PQC is still in its developmental stage, and the possibility that it will suddenly be compromised is not zero. In fact, supersingular isogeny Diffie–Hellman key exchange (SIKE or SIDH), a key-sharing scheme that was being considered for standardization in Round 4 of NIST's competition to select PQC schemes, was found to be breakable during the competition by an attack method that can decrypt SIKE in just over an hour on a computer (as of July 2022) [3]. Accordingly, as we look ahead to the era of quantum computing, we need to satisfy the following requirements:

- Communications are not immediately threatened by the compromise of a single cryptographic algorithm.
- Flexibility to switch from one compromised cryptographic algorithm to another uncompromised one or to adopt a new algorithm must be assured.

3. Activities of IOWN GF

3.1 IOWN Security (IOWNsec)

IOWN GF discusses architectures and use cases of new communications and computation infrastructures that will implement IOWN. More than two years have passed since the establishment of IOWN GF. In that time, the technologies and use cases for implementing the IOWN have gradually materialized, and discussions on security in the IOWN era have recently begun.

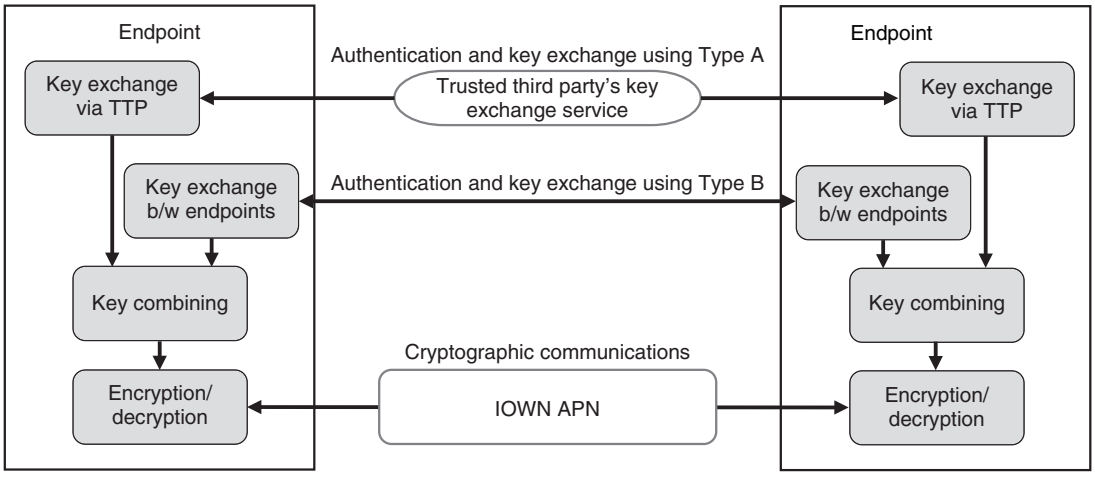
In anticipation of the quantum-computer era, the security report "IOWN Security (IOWNsec)" specifies an architecture for maintaining end-to-end quantum-resistant security for data communications in IOWN use cases, and "Technology Outlook of Information Security" will be published by IOWN GF as a technical document in 2023.

3.2 Multi-Factor Security

IOWNsec is promoting the concept called Multi-Factor Security (MFS) to ensure end-to-end communications with quantum-resistant security. MFS combines multiple technologies to achieve a level of security that cannot be achieved with a single technology. For example, PQC, QKD, and pre-shared key (PSK) are technologies for assuring quantum-security

*1 Quantum-safe security: A security level that provides resistance to attacks by quantum computers.

*2 Compromise: A cryptographic compromise is a situation in which the level of security of a cryptographic scheme has been reduced (compromised). It may be caused by the algorithm or implementation problems.



Type A: Key-exchange scheme involving third party service providers from an endpoint's point of view.
Type B: Key-exchange scheme that only requires sender and receiver as endpoints.

Fig. 2. Specific example of MFS.

resistance during key exchange for encrypting communications. However, each technology has advantages and disadvantages, and no single technology can provide perfect security. For example, QKD is a key-exchange technology with information-theoretic security*3, but long-distance key distribution requires a third-party network for relaying the key, and the risk of internal attacks cannot be avoided [4]. Moreover, the key-exchange scheme using PQC can be implemented using software, so it is possible to precisely exchange keys between endpoints, but its security is classified as computational security*4, which might be compromised in the future. Accordingly, IOWNsec uses MFS to combine multiple security technologies, such as PQC, QKD, and PSK, to compensate for their disadvantages and defines an architecture that can provide users with options that can respond to a wider range of threats (**Figs. 2** and **3**). As well as implementing MFS as an application on the main central processing unit for end-to-end communications, IOWN GF is also considering implementing MFS in gateways and network interface cards that forward data flows to optical paths. Thus, we hope that MFS can be used in a wider range of use cases.

4. Relevant external trends

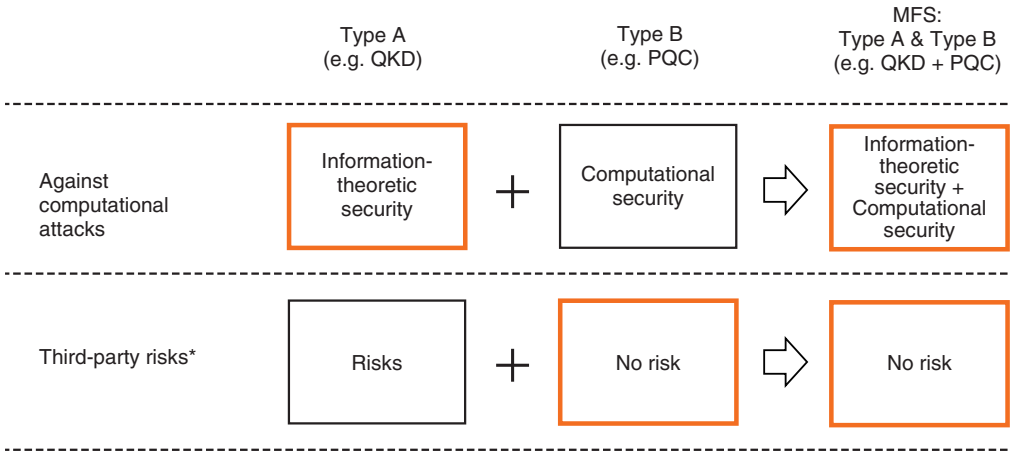
4.1 Crypto-agility

Cryptographic agility (crypto-agility) is a concept proposed by NIST [5, 6] to quickly switch the cryptographic scheme to be used when the scheme used in a network or system is compromised or when a new cryptographic algorithm is introduced. Crypto-agility aims to (i) minimize the impact of the switch on existing networks and systems and (ii) shorten the time required for verification of security.

4.2 Hybrid scheme

In the context of cryptography, the term "hybrid" often refers to hybrid cryptography, which combines public-key cryptography and symmetric-key cryptography. However, the term "hybrid scheme" refers to a scheme with which key exchange and digital signature are executed by multiple public-key cryptographic schemes, and the results are combined to generate a single private key and signature. This hybrid scheme has recently been proposed to the IETF (Internet Engineering Task Force), a forum that defines Internet standards, and others [7]. The hybrid scheme enables multiple schemes to be selected from "conventional" cryptography (such as RSA and elliptic curve cryptography), PQC, and PSK (including shared-key using QKD) and combines the generated

*3 Information-theoretic security: Security against the most-powerful attacker imaginable, i.e., an attacker with unlimited computational power.
*4 Computational security: Security based on the assumption that the amount of computation required for decryption is so much larger than the available computing power that it cannot be executed in a realistic amount of time.



* Third-party risks: Security risks such as internal attacks that third-party services may be involved with.

Fig. 3. Examples of MFS's effectiveness in key exchange.

results so that the system will not be immediately compromised even if one of the schemes is compromised. Using the hybrid scheme makes it possible to implement PQC in society while ensuring the security of conventional cryptography during the transition period to PQC. Even after the transition to PQC, it is effective to hybridize multiple PQC schemes to avoid rapid compromise.

5. Proposal

5.1 Elastic-key-control technology

The authors have proposed and developed elastic-key-control technology, which incorporates the hybrid scheme, as one way to implement the MFS concept stated in IOWNsec. With conventional secure optical-transport-network technology, either PQC or QKD can be selected as the key-exchange scheme according to the system requirements. Elastic-key control is a development of this technology. Elastic-key control allows flexible switching of the cryptographic algorithm used for key exchange according to user needs and the usage status of the cryptographic algorithm (**Fig. 4**). Available elastic-key-control algorithms include conventional ciphers, PQC, PSK alone, and any combination of hybrid scheme. The authors confirmed that a hybrid of conventional cryptography and PQC can be used for signatures for authenticating each server and their verification as well as for key exchange. ECDHE (Elliptic Curve Diffie–Hellman), CRYSTALS-Kyber, and NTRU have been implemented as key-exchange schemes, and ECDSA (Elliptic Curve Digital Signature Algorithm) and CRYSTALS-Dilithium have been implemented as signature methods; however, any algorithm that is implemented as a library can be added to the options. For example, it will be possible to combine conventional cryptography and PQC for practical use and, after accumulating a track record of social use of PQC, we can enter the quantum-computer era. Later, in the quantum-computer era, switching to a combination of multiple PQC algorithms will allow for the rapid implementation and use of future cryptographic algorithms while maintaining a secure situation as long as neither side is compromised. Elastic-key-control technology can thus increase crypto-agility.

5.2 Disaggregation technology for cryptographic processing

Conventionally, an optical transponder has been provided in the form of an integrated optical module. Thus, the open & disaggregated optical transponder has been investigated. This disaggregated architecture allows operators to choose a flexible configuration of various hardware and software. However, the cryptographic-processing module (hardware) is provided as an integrated module within the optical transponder, and the library (software) that controls the module is provided by the network operation system (NOS) of the optical transponder. From the viewpoint of crypto-agility, it is necessary to have a configuration that is rapidly applicable to new cryptographic algorithms. For an optical transport system,

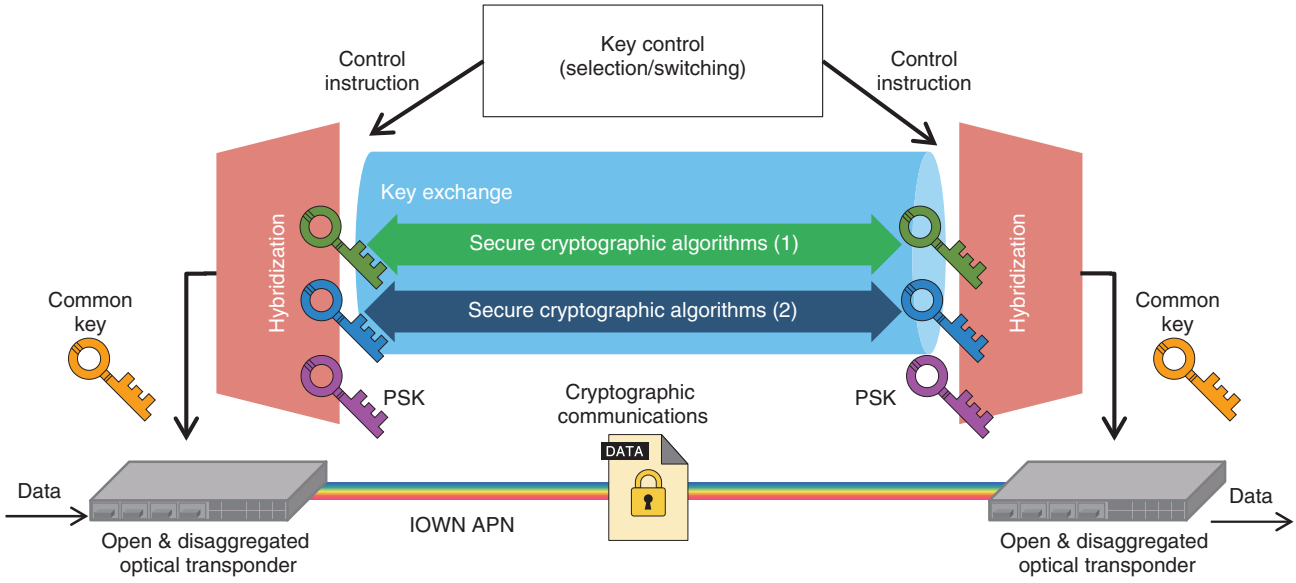


Fig. 4. Elastic-key-control technology.

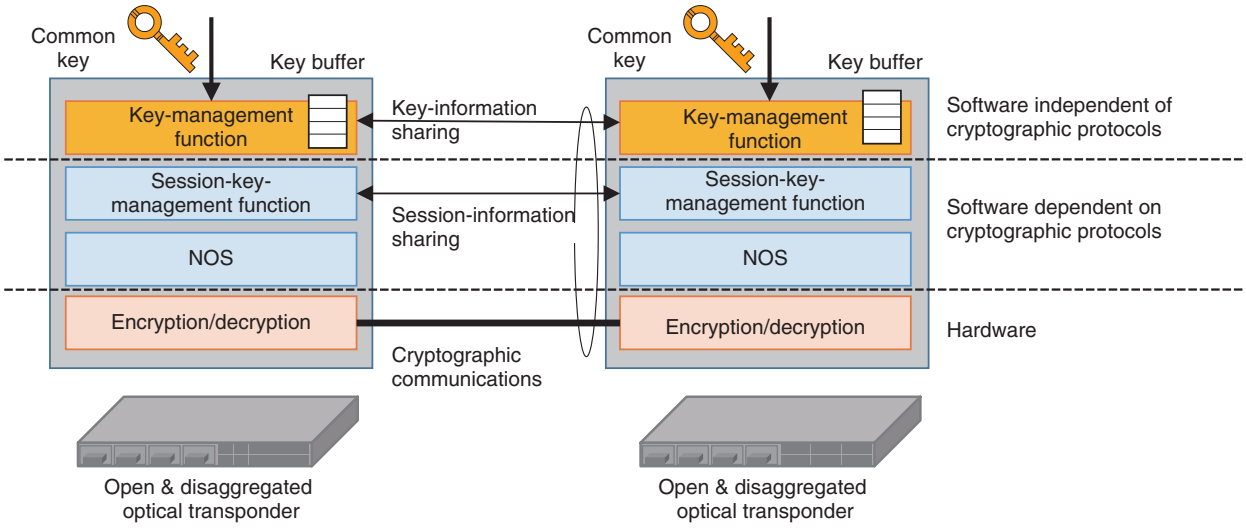


Fig. 5. Disaggregation architecture for cryptographic processing.

stable cryptographic communications must be possible even if the communication channel for exchanging the common key is interrupted.

The authors have also proposed and developed disaggregation architecture for cryptographic processing in the optical transponder as shown in **Fig. 5**. A key-management function receives a common key and manages the key in a way that does not depend on lower-level cryptographic protocols (MACsec (Media Access Control Security), OTN (Optical Transport Network) encryption, etc.) such as key-information sharing between optical transponders. A session-key-management function manages the key in a way that depends on lower-level cryptographic protocols such as session-information sharing between optical transponders. By implementing separate functions in cryptographic processing (executed with hardware) in this manner and loosely coupling

the key-management and session-key-management functions, it is possible to implement cryptographic processing that does not depend on the NOS.

High-speed encryption and decryption is possible because it is executed in hardware as before. By standardizing the interface between the key-exchange, key-management, and session-key-management functions, it will be possible to accommodate differences in upper-level cryptographic-exchange methods and differences in lower-level cryptographic processing, making cryptographic processing possible on a variety of devices using the same key-supply method. Furthermore, by developing a redundant key feature that generates multiple shared keys from the shared key obtained through key-exchange communications and stores them in a buffer, cryptographic communications can continue even if certain shared keys cannot be obtained from certain key schemes due to communication failures or shortage of keys.

6. Future directions

In NTT's efforts to develop secure optical-transport-network technology, elastic-key-control technology and disaggregation technology for cryptographic processing were introduced. The authors are now preparing for trials of these technologies by implementing them into part of the network of NTT laboratories. We expect to improve these technologies and provide them as a general service for use in fields that require large capacity, low latency, and high security (such as telemedicine and finance).

References

[1] Website of NTT R&D, "What is the All-Photonics Network?", https://www.rd.ntt/e/iown/0002.html

[2] T. Okuda, K. Chida, D. Shirai, S. Chikara, T. Saito, M. Nakabayashi, K. Yamamura, Y. Tanaka, K. Natsukawa, and K. Takasugi, "Secure Optical Transport Network," NTT Technical Review, Vol. 20, No. 1, pp. 32–39, Jan. 2022. https://doi.org/10.53829/ntr202201fa6

[3] W. Castryck and T. Decru, "An Efficient Key Recovery Attack on SIDH (Preliminary Version)," Cryptography ePrint Archive, 2022.

[4] Website of National Security Agency/Central Security Service, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[5] W. Barker, W. Polk, and M. Souppaya, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," Apr. 2021. https://doi.org/10.6028/NIST.CSWP.04282021

[6] W. Barker, M. Souppaya, and W. Newhouse, "Project Description: Migration to Post-Quantum Cryptography," Aug. 2021. https://csrc.nist.gov/publications/detail/white-paper/2021/08/04/migration-to-post-quantum-cryptography/final

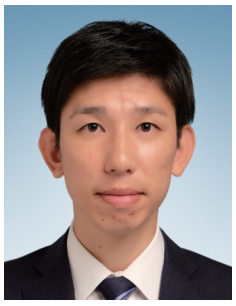
[7] D. Stebila, S. Fluhrer, and S. Gueron, "Hybrid Key Exchange in TLS 1.3," Feb. 2023. https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design

Keizo Murakami
Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.
He received a B.S. and M.S. from the University of Tokyo in 2008 and 2010. Since 2010, he has been engaged in research and engineering on information security at NTT.

Atsushi Taniguchi
Senior Research Engineer, NTT Network Innovation Laboratories.
He received a B.S. and M.S. from the University of Electro-Communications, Tokyo, in 2001 and 2003 and Ph.D. from the Graduate University for Advanced Studies (SOKENDAI), Kanagawa, in 2020. In 2003, he joined NTT. He worked for the National Institute of Information and Communications Technology (NICT) from 2006 to 2008, and NTT Communications from 2008 to 2014. He has been engaged in the research and development of optical transport networks, network virtualization, and quantum networks. He received the Best Paper Award in 2007 from the Optoelectronics and Communications Conference (OECC) and in 2021 from the Institute of Electronics, Information and Communication Engineers (IEICE).

Fumiaki Kudo
Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.
He received a B.E. and M.S. in engineering from Waseda University, Tokyo, in 2009 and 2011. Since joining NTT in 2011, he has been studying identity federation and authentication and is currently involved in applied research on post-quantum cryptography. He was also with NTT DOCOMO from 2017 to 2020, where he was engaged in security enhancement of authentication infrastructure and planning, development and sales of an electronic Know Your Customer (eKYC) service.

Sakae Chikara
Employee, Social Information Sharing Research Project, NTT Social Informatics Laboratories.
He received a B.E. and M.E. in electrical and electronic engineering from Tokyo Institute of Technology in 1988 and 1990. He joined NTT Telecommunication Networks Laboratory in 1990 and studied network architecture, network management systems, and distributed computing systems. He was also involved with the development of intelligent transport systems, cryptographic systems, and information security systems. His current interests are secure network systems, especially quantum computing systems, post-quantum computing systems, and fiber-optic network systems.



Yutaro Kiyomura
Research Engineer, Security Engineering Group, Information Security Technology Research Project, NTT Social Informatics Laboratories.

He received an M.S. from Kyushu University, Fukuoka, in 2014. He joined NTT the same year and is currently a research engineer at NTT Social Informatics Laboratories. He worked for NTT WEST from 2017 to 2020. He has been engaged in the research and development of post-quantum cryptography and secure optical transport networks. He received the Tsujii Shigeo Security Special Award in 2022 from Japan Society of Security Management (JSSM).

Akio Mukaiyama
Researcher, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

He received a B.S. and M.S. from the University of Yamanashi in 2001 and 2003. In 2003, he joined NTT. He was a member of NTT-CERT (Computer Security Incident Response and Readiness Coordination Team) from 2005 to 2011. He worked for NTT DOCOMO from 2015 to 2017 in the Information Security Department. He has been engaged in the research and development of post-quantum cryptography and secure optical transport networks.

Yusuke Iijima
Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

He received an M.S. from Tsukuba University in 2017 and joined NTT the same year. He has been engaged in the research and development of post-quantum computing cryptography, and secure optical transport networks.

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

He received a B.E. and M.E. from the University of Tokyo in 2009 and 2011. Since he joined NTT laboratories in 2011, he has been engaged in research on video transmission over IP networks including transport protocol, presentation synchronization, and video conferencing. His current research interest is in low-latency video transmission over high-speed optical networks. He is a member of IEICE.

Yasuyuki Sanari
Frontier Communication Laboratory, NTT Network Innovation Laboratories.

He received a B.S., M.S., and Ph.D. from Kyoto University in 2016, 2018, and 2021. He joined NTT Network Innovation Laboratories in 2021. He has been engaged in the research and development of optical transport networks, quantum cryptography, and quantum networks.

Naohiro Kimura
Research Engineer, Frontier Communication Laboratory, NTT Network Innovation Laboratories.

He received a B.S. and M.S. in mechanical engineering from the University of Tokyo in 1991 and 1993. From 1993 to 1998, he was with NTT Transmission Systems Laboratories, where he was engaged in the research and development of programmable transmission equipment and transmission protocol. From 1998 to 2010, he was with operating companies such as NTT EAST and NTT WEST, where he worked on system integration of imaging systems and development of business systems. He is currently with Frontier Communication Laboratory, where he joined as a research engineer in 2010. His current research interests include creating new services using video.