Highly Secure Network Switches with Quantum Key Distribution Systems

Mikio Fujiwara[1], Tomoyasu Domeki[2], Shiho Moriai[1], and Masahide Sasaki[1]
(Corresponding author: Mikio Fujiwara)

National Institute of Information and Communications Technology[1]
4-2-1 Nukui-Kita, Koganei, Tokyo 184-8795, Japan
NEC Communication Systems, Ltd.[2]
Chuou Aoba, Sendai, Miyagi 980-0021, Japan
(Email: fujiwara@nict.go.jp)
(Received Oct. 9, 2013 ; revised and accepted Mar. 13, 2014)

Abstract

We have developed network "switches" with security enhanced by "quantum key distribution (QKD) systems". In a Layer 2 "switch", media access control (MAC) addresses are encrypted to prevent unauthorized access from internal network. After an initial authentication, common random key bits are shared between the Layer 2 "switch" and users. MAC addresses are encrypted with shared key at every packet. In Layer 3, secure keys from a "QKD system" are used in the Internet Protocol Security (IPSEC) protocol for encrypting a payload in one-time pad, and also for extracting a message digest for unconditionally secure message authentication. In this way, network security can be effectively enhanced by QKD in an IP compatible manner.

Keywords: IPSEC, layer 2, layer 3, network switch, quantum key distribution

1 Introduction

Data theft is on the increase and set to rise dramatically in the upcoming years. Optical fiber transmission cannot be an exception, despite its reputation for being more secure than standard wiring or airwaves. Indeed, photon crosstalk between neighboring fibers in a field-installed cable is commonly occurred and information theft could easily take place if novel photon detectors are used [4]. Therefore, technology for information security has become a critical issue for the advanced information and communications network infrastructure. Conventionally, data encryption is performed at Layer 3 or above (in terms of OSI layer model) on the basis of protocols such as Internet Protocol Security (IPSEC) and the Secure Socket Layer (SSL) Virtual Private Network (VPN) solution. On the other hand, data protection technology performed at Layer 1 has been developed in recent years. Quantum key distribution (QKD) [5] allows two users, Alice and Bob, to share random key bits in an unconditionally secure manner based on the fundamental laws of physics. BB84 [2] is known as the most famous protocol. The unconditional security of QKD is ensured only for point-to-point link connected via an optical transmission line. Recently, its distance limit has been extended to 250 km [9]. For networking QKD links for multiple users, and extending the range of QKD services, one should currently rely on key encapsulating relay via trusted nodes where eavesdroppers cannot enter [1, 3, 7, 8]. Therefore proper key management is required for the QKD network. Security loopholes are inevitably associated with such a network layer structure, leaving a possibility of causing more serious security problems. Therefore, not only the security of the physical layer but also that of the upper layers should be properly cared using appropriate security technology in a whole network. In such a situation, security functions of switches in Layers 2 and 3 are of particular importance. Secure keys seeded from the QKD layer should be efficiently used in those network "switches".

We have thus developed integrated network "switches" for Layer 2 and Layer 3 whose securities are enhanced with secure keys from "QKD systems". In this paper, we describe a secure architecture of a network-structure via "QKD systems". In Section 2, we introduce the Layer 2 "switch" in which the media access control (MAC) addresses are encrypted per packet to prevent MAC address spoofing and unauthorized access from an internal network. In Section 3, we explain the Layer 3 "switch" in which the secure keys from the QKD system is used in an enhanced IPSEC protocol. IPSEC has an authentication function and, needless to say, an encryption feature. Information-theoretic secure keys are used in encryption and authentication, and information-theoretic security is guaranteed in both. We have developed the "switches" embedded in PCs. We report the performance of the new Layer 2 and Layer 3 "switches" shown in Figure 1.

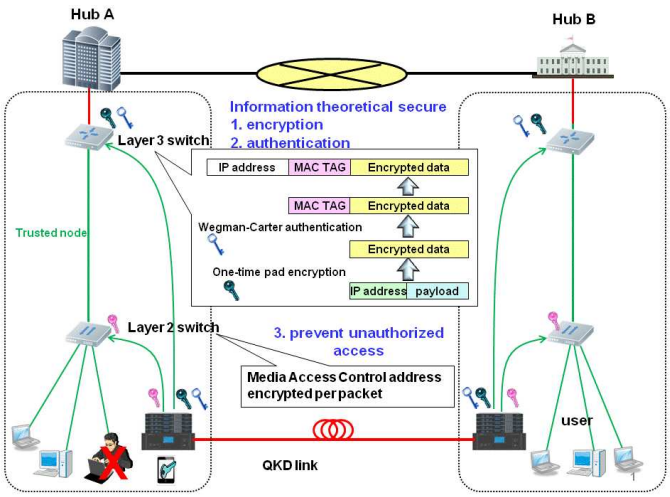


Figure 1: Conceptual view of the integrated network "switches"

2 Layer 2 Switch

The encryption scheme for data exchanged between VPNs has been drawing attention for use in layer 3. However, serious security holes are recognized at layer 2. Ethernet technology has been established on the assumption that users are fundamentally good. In other words, unauthorized access from an internal network PC is very easy because there is no authentication process in layer 2. To prevent such unauthorized accesses, deconcentration of access authority is usually adopted in the network. However, such a protection scheme may be destroyed by an impersonation from an internal-network PC. In fact, spoofing a MAC address, which identifies a "host (PC)" in the layer 2, may easily be made. However, even if network authentication is employed, unauthorized access is difficult to prevent completely due to the sophistication of spoofing attacks. To enhance the security of the internal-network, we have developed a Layer 2 "switch" that uses random bits provided from a "QKD system" for authentication of hosts. First, the switch sends each "host" the random bits by encrypting it with AES. Each "host" encrypts the MAC address by the random bits and sends it to the Layer 2 "switch". The random bits are used only once for each packet between the host and the Layer 2 switch. In the Layer 2 switch, consistency is checked by using a decrypted MAC address and IP address. If the host sends correct addresses, the Layer 2 "switch" passes the packet. Process are summarized as follows:

1) Authentication between the "QKD systems" using a pre-shared key.

2) Authentication between the Layer 2 "switch" and "QKD system" machine using a pre-shared key.

3) Blocks of random bits are downloaded to "switches".

4) Initial authentication process between the "switch" and "hosts" by using pre-shared (USB sticks) keys.

5) MAC addresses are enrolled and checked with registered list.

6) Random bits encrypted by AES are shared between the Layer 2 "switch" and "PCs".

7) MAC addresses are encrypted using the random bits per packet.

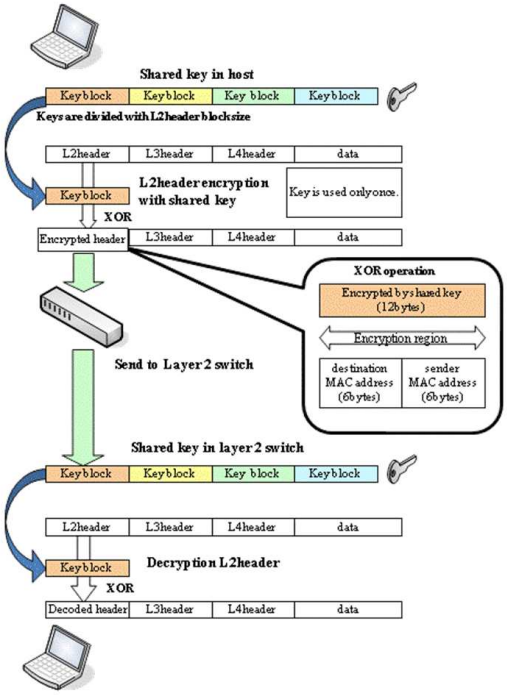
8) MAC addresses are decrypted and checked with IP addresses in the "switch".

9) If the MAC address and IP address are matched with the registered data, the switch allows connection. If not, the packet is silently discarded.

Our "switch" has strong protection against MAC spoofing, IP address spoofing, spoofing using internet control message protocol (ICMP) redirects, address resolution protocol (ARP) poisoning attacks, and so on. This switch obtains 70-90% throughput performance without encryption. MAC addresses are changed in every packet shown in Figure 2. For example, we show the effect of this "switch" for the case of the IP address spoofing in Figure 3. When we operate this "switch", "hosts (PCs)" should be connected with the "switch" directly. In this system, a cascade arrangement is prohibited in order to prevent information leakage by monitoring packets in "hosts". Of course, it is possible to adopt an encryption technique in communication between "hosts", but it depends on the required security level. Moreover, the random number delivery could be more secured, if the host would receive it from a trusted courier, for example, by receiving it from the "switch" via an authenticated smart phone and installing it into the "host". By using this device, key sharing can be done with high security.

3 Layer 3 Switch

The scenario in which the QKD is used for key establishment between two local area networks has been demonstrated within the BBN DARPA network project [3] and other networks [5]. A point-to-point link in a local area network (LAN) or VPN encryptor provides secure keys to the Layer 3 "switch". Payloads are encrypted by IPSEC. The security of the transmitted data over such a link is limited by the security of the encryption scheme. Ideally, Vernam's one-time pad encryption can provide information-theoretical security. When, otherwise, used with modern cryptography, frequent key renewal of the symmetric key encryption also enhances the security level [7, 9]. Problems are the internet key exchange process and the randomness of the key. We are developing the QKD-based Layer 3 "switch" in that the symmetric-key is refreshed in each packet of the IPSEC protocol. Our "switch" uses Vernam's one-time pad



(a)

time	Sender's MAC address	Receiver's MAC address
202 138.096514	48:a1:70:89:4e:7d	d4:4a:47:c0:ba:d0
204 138.128000	e0:48:45:98:48:1a	d0:33:8b:ef:37:31
205 138.128499	58:1e:db:88:cf:44	94:ad:0c:14:fd:f4
208 138.248009	38:49:e5:30:f1:c3	74:b7:b9:5b:0c:75
209 138.248248	f0:a8:1f:11:63:7a	58:f8:a4:4d:67:f7
211 138.258376	08:bc:7c:16:07:8a	40:16:b4:eb:a4:9f
212 138.264384	90:f3:e2:b9:1b:15	f4:cf:87:4d:53:f6
215 138.412626	e0:ab:63:94:11:1e	58:51:03:8c:d3:af
216 138.413125	20:52:b7:ea:d0:48	08:22:09:b3:d0:0c
219 138.506751	b8:b3:17:db:e0:f9	5c:c2:53:2b:dc:18
221 138.517250	bc:74:67:6a:e8:65	f4:19:da:65:16:db
223 138.526251	c0:e4:e4:a2:52:11	24:5b:ac:e6:ee:2d
240 139.882261	ac:cf:e0:05:b3:11	d4:13:24:6a:0e:9c
242 139.964268	e4:0a:86:fb:92:31	20:ff:2e:cc:42:49
244 139.982007	54:be:1c:f2:bf:ee	84:54:63:45:14:00
246 140.040251	2c:3c:cf:00:be:e7	b0:36:19:65:f1:02
250 140.051001	9c:fb:8f:09:3a:57	64:04:97:7b:d6:0c
251 140.054379	c0:ed:e6:c3:d2:3d	4c:76:13:99:2c:95
252 140.057627	1c:e1:50:d4:e8:5d	4c:a8:c6:17:99:96
254 140.106503	0c:21:fe:a0:4f:bd	f4:4e:9c:03:d4:8d
256 140.213499	84:a5:89:e0:62:d7	64:08:6e:a6:d3:14
261 140.224015	44:a8:b1:b0:c2:35	04:f9:4b:70:8f:53
263 140.227499	04:cf:be:ba:26:37	4c:a1:45:0c:95:98

(b)

Figure 2: (a) Process of MAC addresses encryption in Layer 2. (b) Packet monitor image in Layer 2. MAC addresses are encrypted in every packet.

encryption option. The Internet key exchange process

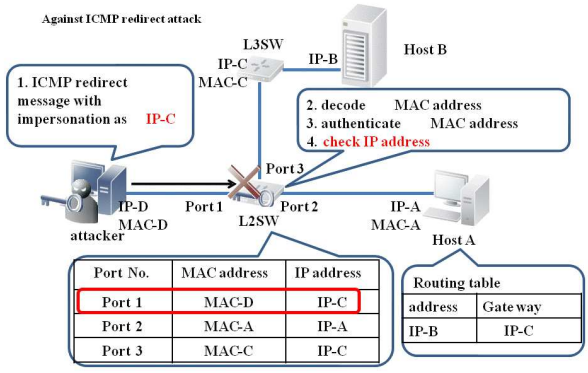


Figure 3: Protection from IP address spoofing. In the layer 2 "switch", decrypted MAC address and IP address are checked.

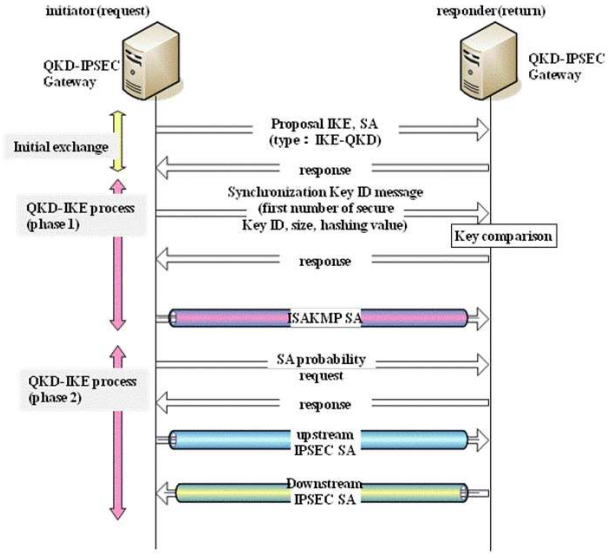


Figure 4: Internet key exchange (IKE) protocol using "QKD System". Secure key is fed from the "QKD system". IKE can be finished without complex calculation. Internet Security Association and Key Management Protocol Security Association (ISAKMP SA) is a generic name of exchanging authentication and encrypted data.

with a "QKD system" is shown in Figure 4. We obtain information-theoretical secure communication through an IP-based network without complex calculation often required in modern cryptography which slows down an effective data transmission rate. Such a secure network switch enables us to use various applications with high security. The packet structure of IPSEC in our "switch" is shown in Figure 5. Tunneling mode is employed. Figure 6 shows the operation image of the Layer 3 "switch". Moreover, a secure key is used to make the message au-

thentication code. We adopt Wegman-Carter authentication [10] to extract message digest. In this process, we use Universal$_2$ hash function. Figures 7(a) and (b) show the processes in the Universal$_2$ hash function and Wegman-Carter authentication, respectively. The one-time pad encoding makes sure no information about the message digest leaks to an eavesdropper. When 12000-bit data are hashed with the Wegman-Carter algorithm, 2048 bits of secure key is used in our system. Our network "switch" simultaneously encrypts and authenticates data with unconditional security.

Our current Layer 3 "switch" consists of a PC-based 100 Mbps router. The throughput of this switch with one-time pad encryption (and AES encryption) is more than 80 Mbps. However, when the authentication function is activated, the throughput falls drastically due to heavy computation load. In the future, the implementation will be made on a dedicated hardware such as the field programmable gate array instead of PCs and the throughput will not degrade.

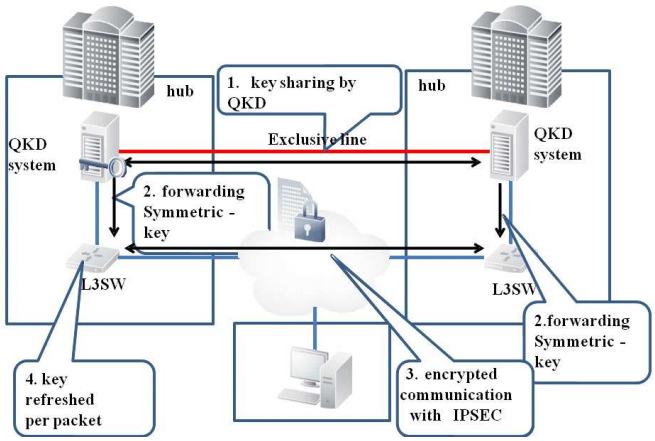


Figure 6: Conceptual view of Layer 3 "switch" connected to the "QKD system"

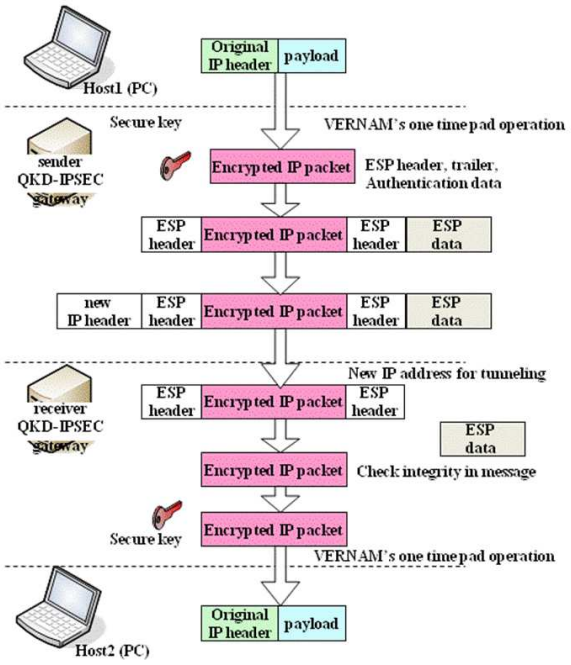


Figure 5: Packet structure of IPSEC with "QKD system". In Encapsulating Security Payload (EPS) data, message digest is stored. Secure key is used in encryption and authentication process in one-time pad manner.

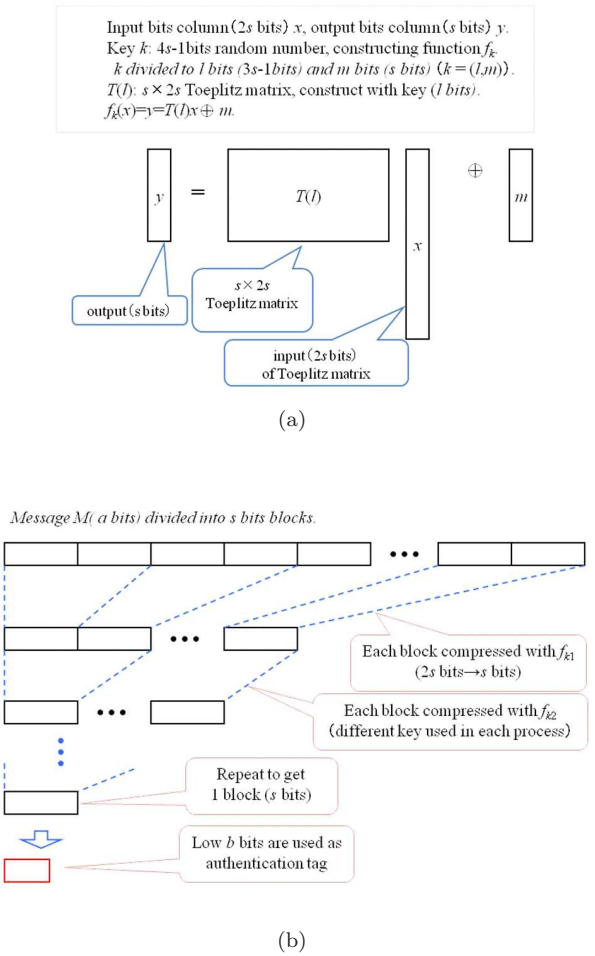


Figure 7: (a) Toeplitz matrix strongly Universal$_2$ hash function. (b) Wegman-Carter authentication.

These functions are used in making authentication data. If the message is composed of z blocks, where each block length is s bits, then the affine transformation defined by Toeplitz matrix and column vector is applied *z-1* times to obtain the authentication tag. Since a *4s-1* bit random sequence is used for each transformation, *(z - 1)(4s - 1)* bit randomness must be prepared in total. To save the random bits prepared by the QKD, we have other choices such as " evaluation hash function", and "division hash function". By employing the evaluation hash function (EFH) as an example, the message M of length ts bits is first divided into t blocks, de-

noted by $M_{t-1} \ldots, M_0$, and then the polynomial $P(x) = M_{t-1}x^{t-1} + M_{t-2}x^{t-2} + \ldots + M_0$ (on some suitable field) is generated. Finally, the authentication tag of the message M becomes $P(r)r$, where$r$ is a random sequence. Thus in this case, the randomness used is only r of length s bits.

4 Secure Key Feed on Smartphone

The "QKD system" guarantees the security at data transmission. When we discuss the security of the network system, we have to consider how to identify authenticated users and store data safely. Secret sharing (SS) is a promising candidate for secure data storage, but it needs a multi-party network. Of course, SS will have affinity to the QKD network. However, we must contemplate the effective utilization of the end-to-end link. Specifically, multi-users are assumed to use the "QKD system", so user administration is very important. We have thus proposed and developed a user management system with smartphones. To access the "QKD system", passwords are given for each smartphone. When the user downloads the secure key from the "QKD system", the key management agent (KMA) checks the password and the SIM card ID in the smartphone. A shared key is used to encrypt data in accordance with the shared key ID at a sender side. At that time, the sender can set access right control on data. Figure 8 shows the conceptual diagram of the "QKD-smartphone system". Security of data transfer is guaranteed by the normal QKD operation. In this system, the smartphone is the ID device and provides the security of the stored data at the receiver side. This system can be applied to the electric medical chart. Gene information of each person will be used for medical care. Such information must be strictly prevented from leaking, because misuse negatively influences kith and kin too. Our system will contribute to improving its security level. Unfortunately, counterfeiting a SIM card is not difficult. Thus, we should consider combining the biometric authentication technique with the smartphone.

In our current system, authentication between "QKD systems" is carried out using pre-shared key. Authentication protocol using quantum channel has been proposed [6]. However, key pre-sharing using a smartphone has high reliability, and it can be matured as a personal device for authentication and privacy protection.

5 Conclusions

We have developed a QKD-based network "switch" that efficiently enables prevention of unauthorized accesses from external and internal networks. This switch will contribute to constructing the trusted node and playing an indispensable role in embedding the QKD network into the current infrastructure of secure networks. Moreover,

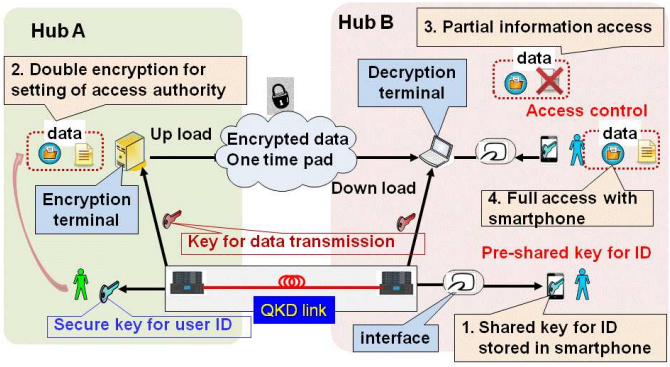


Figure 8: Conceptual diagram of "QKD-smartphone ID system". Access right control can be done using smartphones.

this "switch" can enhance convenience of the "QKD system" and provide seamless connection between QKD network and IP-based network. Poor convenience of the secret communication tool can provoke human errors that pose serious threats to the network security. Moreover, the QKD network rests with the key relay via trusted nodes. Therefore, we must make the trusted node more trustworthy. The QKD-based network "switches" and access right control using smart phones would also be useful to reduce such risks by enhancing the security while maintaining user-friendliness.

Acknowledgments

The authors thank Kenji Terada, Hirokazu Suzuki, Kenichiro Yoshino, Takao Ochi, Kaoru Shimizu, Toshimori Honjo, Kazuhiko Nakamura, Ryo Nojima and Akio Hanzawa for their support in setting up the Tokyo QKD Network and discussions.

References

[1] R. Alleaume, J. Bouda, and et al., *SECOQC white paper on quantum key distribution and cyrptography.*

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, pp. 175–179, 1984.

[3] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, , and H. Yeh, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, pp. 138–149. SPIE, 2005.

[4] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, "Photon level crosstalk between parallel fibers installed in urban area," *Optics Express*, vol. 18, no. 21, pp. 22199–22207, 2010.

[5] N. Gisin, G. Ribordy, W. Tittel, , and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2008.
[6] K. Kanamori, S. M. Yoo, D. A. Gregory, and F. T. Sheldon, "Authentication protocol using quantum superposition states," *International Journal of Network Security*, vol. 9, no. 2, pp. 101–108, 2009.
[7] M. Peev, C. Pacher, and et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, pp. 1–37, 2009.
[8] M. Sasaki, M. Fujiwara, and et al., "Field test of quantum key distribution in the tokyo QKD network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.
[9] D. Stuchi, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High late, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, no. 7, pp. 1–9, 2009.
[10] M. Wegman and L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Science*, vol. 22, no. 3, pp. 265–279, 1981.

Mikio Fujiwara received B.S. and M.S. degrees in electrical engineering from Nagoya University, Aichi Japan, in 1990 and 1992. In 2002, he received a Ph.D. degree in physics from Nagoya University. In 1992, He joined the Communications Research Laboratory, Ministry of Posts and Telecommunications, where he engaged in the development of Ge:Ga far-infrared photoconductors. Since 2000, he has been in the quantum information technology group. His current interests include single photon detectors and entanglement based QKD systems in the telecom-bands. Dr. Fujiwara is a member of the Japanese Society of Physics, and the Institute of Electronics, Information and Communication Engineers of Japan.

Tomoyasu Domeki received a B.E. degree from the College of Engineering, Nihon University, in 1991. The same year, he joined NEC Miyagi, Ltd. He is currently the manager of the software development division at NEC Communication Systems, Ltd. His interests include QKD based key management platforms for smartphones and entanglement based QKD systems in the telecom-bands.

Shiho Moriai received a B.E. degree from Kyoto University in 1993 and a Ph.D. from the University of Tokyo in 2003. She has worked at NTT Laboratories, Sony Computer Entertainment, Inc., and Sony Corporation. She has been involved in design, analysis, and standardization of cryptographic algorithms. She has also worked on designing security architectures of PlayStation platforms. Since 2013, she has been Director of Security Fundamentals Laboratory, Network Security Research Institute, NICT. She was awarded IPSJ Industrial Achievement Award in 2006 and Minister's Award of The Ministry of Economy, Trade and Industry, the Industrial Standardization Awards in 2011.

Masahide Sasaki received B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Sendai Japan, in 1986, 1988, and 1992. During 1992-1996, he worked on the development of Si-MOSFETs with Ayase Laboratory, Nippon Kokan Corporation, Kanagawa Japan. In 1996, He joined the Communications Research Laboratory, Ministry of Posts and Telecommunications. Since 1994, he has worked on Quantum Information Theory and Quantum Optics. He is presently a group leader of a quantum information technology group. Dr. Sasaki is a member of the Japanese Society of Physics and the Institute of Electronics, Information and Communication Engineers of Japan.