Quantum Photonic Network: Concept, Basic Tools, and Future Issues

Masahide Sasaki, Mikio Fujiwara, Rui-Bo Jin, Masahiro Takeoka, Te Sun Han, *Fellow, IEEE*, Hiroyuki Endo, Ken-Ichiro Yoshino, Takao Ochi, Shione Asami, and Akio Tajima, *Member, IEEE*

(Invited Paper)

Abstract—**We present practical GHz-clocked QKD systems, next generation entanglement QKD technologies, and QKD platform to manage the secure keys and to support a variety of applications. We then show the intrinsic limit of QKD, i.e., a key rate bound, and discuss how to realize the provable (information theoretic) security with a larger secrecy capacity over longer distances. In particular, we present a basic theory of physical layer cryptography, which characterizes the secrecy capacity, and engineers the tradeoff between the efficiency of reliable transmission and secrecy of communication. We introduce a concept to unify these schemes in photonic network, referred to as quantum photonic network. Future issues for realizing this new network paradigm are discussed.**

Index Terms—**Quantum communication, quantum cryptography, quantum key distribution, photonic network.**

I. Introduction

QUANTUM communication and cryptography are to realize communications with higher capacity than the Shannon limit [1] and unbreakable security, which cannot be possible with conventional technologies. Pursuing high capacity in optical communications, one has recently reached the quantum-limited regime where the signals are densely packed in the phase space so that quantum indistinguishability of the signal states becomes a matter [2]. Further improvement to increase the rate in bits/s/Hz/photon requires quantum engineering [3]–[6]. This is also important in optical space data links where no amplifiers can be used through a long distance transmission [7]. Quantum communication is expected eventually to achieve the ultimate channel capacity of such optical links [8]–[11]. The fact disclosed recently that fibers were actually tapped over a long time by intelligence agencies these decades has convinced one that physical layer security is an urgent concern. Even without such an active attack, information often leaks between fibers in the same cable through the fiber cross-talk phenomenon, especially at parts where the cable is bent [12]. Quantum cryptography, or more specifically quantum key distribution (QKD) [13], attracts more attention in this respect. QKD has been deployed in many field links and networks [14]–[20]. In addition, it has already been successfully commercialized and found practical use cases [21]. New generation GHz-clocked QKD systems have been deployed in the field network, demonstrating their reliable operations [16], [18]–[20]. The maximum key generation rate at present is something around 100 kb/s over a 50 km installed fiber. This performance, however, still falls short of the level for practical deployment in wide area public infrastructures.

Increasing the capacity and ensuring the security are generally competing tasks. The speed and distance limits of QKD are the price for realizing the unconditional security. For example, an expected key rate at -50 dB attenuation channel seems to be impractically poor even when one can operate the system at a few tens of GHz. Fiber links over 100 km or optical space links in deep space belong to such cases. A recent theoretical study shows that the theoretical key rates for known protocols, such as BB84 [22], are just a few times smaller than an upper bound of the maximum achievable secure key rate [23]. Therefore it is unlikely that dramatic performance improvement could be made with assuring the unconditional security against an eavesdropper with unbounded ability. It encourages one to study information theoretically secure (ITS) communication schemes which can cover a longer distance with a reasonable rate, even compromising assumptions on physical channel properties for a wire tapper. That is, the wiretap channel to an eavesdropper is assumed to have some physical restrictions, and the tradeoff between the two competing tasks, increasing the capacity and ensuring the security, are studied. Its security is not algorithmic, but ITS based on the existence of codes that cannot be decrypted by any powerful computers. This class of cryptography is referred to as physical layer cryptography [24].

In a new network paradigm, various QKD schemes, physical layer cryptography, algorithmic cryptography and optical/quantum communications are integrated in an inter-operable manner, depending on user needs and allowed costs. Such a paradigm unifying quantum communication and cryptography

Manuscript received September 22, 2014; revised October 31, 2014; accepted November 3, 2014. Date of publication November 12, 2014; date of current version December 18, 2014. This work was supported in part by the Impulsing Paradigm Change through Disruptive Technologies Program.

M. Sasaki, M. Fujiwara, R.-B. Jin, M. Takeoka, and T. S. Han are with Quantum ICT Laboratory, Advanced ICT Research Institute, National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan (e-mail: psasaki@nict.go.jp; fujiwara@nict.go.jp; ruibo@nict.go.jp; takeoka@nict.go.jp; han@ya2.so-net.ne.jp).

H. Endo is with the Department of Applied Physics, Waseda University, Shinjuku, Tokyo 169-8555, Japan, and also with the Quantum ICT Laboratory, National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan (e-mail: h-endo@nict.go.jp).

K.-I. Yoshino and A. Tajima are with Green Platform Research Laboratories, NEC Corporation, Kawasaki, Kanagawa 211-8666, Japan (e-mail: yoshino@bp.jp.nec.com; a-tajima@bk.jp.nec.com).

T. Ochi and S. Asami are with National Security Solutions Division, NEC Corporation, Minato-ku, Tokyo 108-0075, Japan (e-mail: t-ochi@cp.jp.nec.com; shione-asami@bc.jp.nec.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTQE.2014.2369507

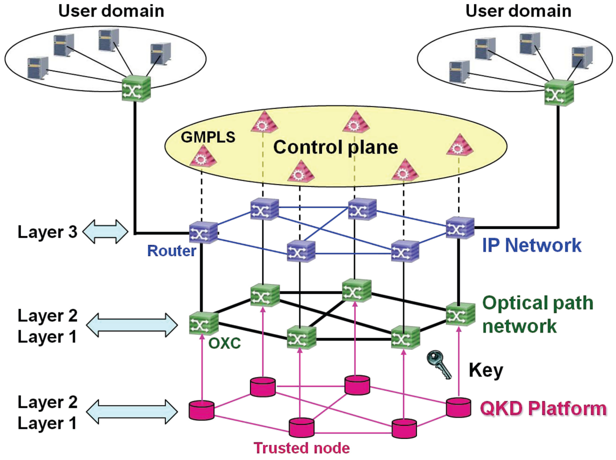

Fig. 1. Concept of secure photonic network.

with conventional optical communication and cryptography may be referred to as quantum photonic network. This emerging platform is to integrate QKD for the highest security, quantum communication for power-minimum maximum-capacity communications, and a new scheme of physical layer cryptography which merges the merits of these two to realize the secrecy capacity with the provable security into a network, so that the whole network can provide best solutions for various kinds of use cases.

In this paper, we first present the updated Tokyo QKD Network, consisting of novel QKD systems, and key management systems supporting variety of applications. We next mention a next generation entanglement-QKD system and related technologies. We then present a basic theory of physical layer cryptography which characterizes the secrecy capacity, and engineers the tradeoff between the efficiency of reliable transmission and secrecy of communication. We finally discuss future issues for realizing quantum photonic network.

II. Quantum Photonic Network

Photonic network is an emerging infrastructure of optical communications. It specifically means the IP over optical path network. Its structure is depicted in Fig. 1. The optical path network is at the physical layer (Layer 1), and is made as transparent as possible based on all optical processing nodes (photonic nodes), instead of conventional nodes of electrical processing. It is to utilize broadband of optical fields and to resolve the speed limit and heating of electrical devices. Actually broadband optical transmission is realized by wavelength division multiplexing (WDM) in a fiber. Networking and routing are carried out by all optical processing with wavelength switching, which is performed by the optical cross-connects (OXCs). The OXCs are directly connected to IP routers at the network layer (Layer 3) to set up a desired optical path. Routing, signaling, and link management at Layer 3 are supported by the generalized multi-protocol label switching in the control plane, which is implemented in out-of-band channels in optical fibers or sometimes over a dedicated control network. In this way, transparent optical links are formed in a flexible manner at Layer 1. The optical transparency is also the prerequisite for making a QKD link. If the photonic nodes could be employed in a QKD network, then flexible direct QKD connectivity can be realized. Unfortunately, however, current QKD performances are not sufficient for extending a distance through lossy photonic nodes.

Networking and extending the range of QKD must rely on the key relay via the trusted nodes at present. Security of the nodes should be protected classically. This means that there must be the same security loopholes in a QKD network as a classical one. In spite of this fact, the trusted-node-based QKD network is worth being developed as a practical network solution. One of new values added by QKD is the interconnectivity of crypto systems, thanks to the simplest encryption/decryption by XOR operation between a plain/cipher text and a key. This point should be contrasted to conventional algorithmic schemes. Their high-end solutions are specifically designed organization by organization, and their specifications are usually not disclosed. This makes it very hard to interconnect the systems of different organizations in a seamless secure link. The QKD network can solve this problem if the keys and their identifications could be properly managed in the trusted nodes.

We may call such a solution *QKD platform*, which integrate QKD network with a smart key management system and application interfaces (APIs) to support variety of applications. The point of interface is defined at the API of the QKD platform. Users will be able to request keys for their applications, and receive them from the QKD platform. Once supplied, the users are in charge of management and uses at the keys. The key management server in the QKD platform stores all the necessary information on the keys, including generation dates, supplying dates, key sizes, user ID information etc. When any security incident would occur in a user system, the user can delete the keys in it and receive new keys from the QKD platform at a time. We are updating the Tokyo QKD network to a prototype of the QKD platform. The QKD platform will be introduced to photonic network to enhance its security at each layer, whose concept, secure photonic network [25], is summarized in Fig. 1.

It is a never-ending task in any practical security technologies to find security loopholes and side-channels, and to implement countermeasures. QKD itself is not an exception. Actually, several side-channels of QKD components have been identified, and their countermeasures have been developed [26]–[32]. On the other hand, some approaches have been proposed to remove side-channels by using a self-testing mechanism based on quantum effects, namely the entanglement and indistiguishable interference of photons. These schemes are device-independent (DI)-QKD [33] and measurement-device-independent-QKD [34]. They provide not only a new notion to combat the side-channel problem of crypto-technology, but also a basic protocol for fully quantum networking. In particular, DI-QKD based on the entanglement is essentially an elementary link in the quantum repeater network paradigm. These new schemes are, however, far from practical deployment yet. Some scalable architectures proposed so far still seem to require new technological developments. Therefore researches in this direction is still in fundamental research phase.

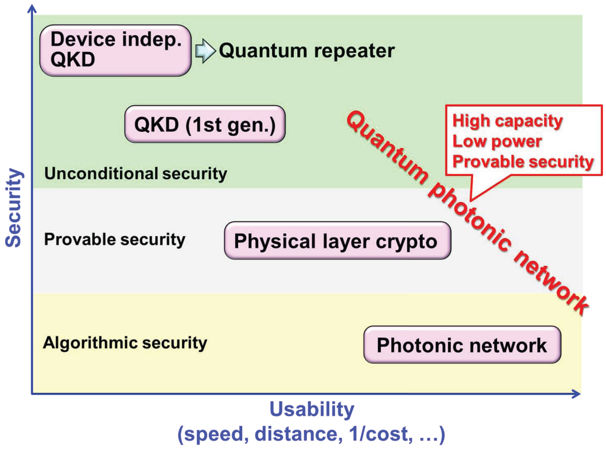

Fig. 2. Diagram to categolize main cryptographic schemes in terms of the security versus the usability.

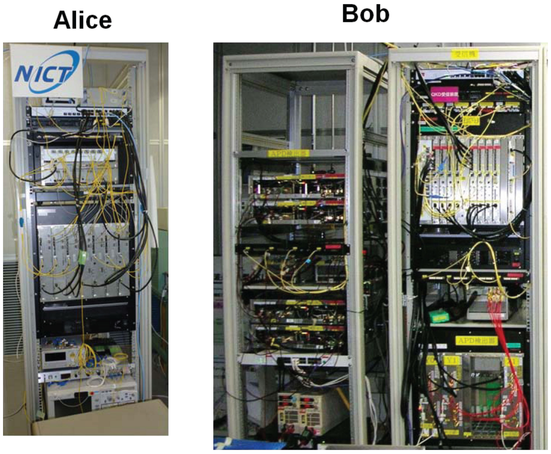

Fig. 3. A photo of the GHz-clocked WDM-QKD system. Alice's transmitter includes a laser source, a PLC time-bin encoder, eight mudulator units for the signal and decoy information, a multiplexer, a controller, and a key distillation engine. Bob's receiver consists of two 19-inch lacks. The right rack includes a PLC time-bin decoder, four demultiplexers, a photon detector unit containing four APDs, a controller, and a key distillation engine. The left rack include another photon detector unit. Thus in this photo, two-channel WDM is implemented.

The schemes mentioned above can be categorized in a rough diagram of the security versus the usability as in Fig. 2. The usability means speed, distance, inverse of cost, and so on. One-way QKD such as BB84, and entanglement-based QKD are in a higher security side, but the key rate is much lower than the standard rates of optical communication, and hence the usability is not so high. Photonic network is in a wider usability side, realizing broadband and long distance transmission. Its security is based on algorithmic cryptography, which is implemented in Layer 3 or the upper layers. There is still a big gap between QKD and photonic network. This gap will not be filled merely by improving QKD technology itself as discussed in Introduction. Physical layer cryptography can be an intermediate scheme to fill this gap. Instead of weakening assumptions on the physical channel to an eavesdropper (Eve), one exploits higher transmission rate over a longer distance with the provable security, i.e., ITS. This would be valid and sensible in space laser communications, which are basically line-of-sight communications between the sender (Alice) and the receiver (Bob). Eve should be apart from this main channel, otherwise she can be visible for Alice and Bob. The details will be explained in Section IV.

Thus Fig. 2 includes all schemes we know for secure wire and wireless communications. Quantum photonic network means a platform to integrated them to provide best solutions for various kinds of use cases. Its practical architecture and implementation are an on-going challenge.

III. QKD and Related Technologies

A. Novel BB84-QKD System

Currently the four-state protocol originally proposed by Bennett and Brassard, called BB84 [22], is most widely implemented in the world. Its key rate and distance had been improved rapidly until 2010, when GHz-clocked QKD systems were first deployed in a field environment [16]. Key generation at around 100 kb/s over a 50 km installed fiber became possible. Since then, however, further improvement of QKD performance has remained little. The main bottleneck is the performance limits of single photon detection. The maximum count rate is roughly a few hundred mega counts per sec (cps) for both avalanche photodiode (APD) and superconducting nanowire single photon detector (SSPD). APDs are usually operated in the gated mode, whose gating speed is limited at about 1 GHz. So the clock rate of a fast QKD system is also set at this rate. Dark counts (and after-pulses for APD) mainly limits the distance of successful key generation, where the signal counts fall down at the dark count noise level. Dark count and after-pulse probabilities for novel APDs for a gating period of 1 ns or less are $< 10^{-6}$ and $< 1\%$, respectively. Then the dark count noise level is roughly 1 kcps for a GHz-clocked QKD system. Assuming a standard fiber with a loss rate of 0.2 dB/km, the distance limit of meaningful key generation is roughly 90 km. If SSPDs are applied, the dark counts can be smaller by an order of magnitude, and hence the distance can be extended further at around 150 km. However, drastic improvement of single photon detectors from the current level is not easy. Array formatted detectors will enable faster operation, but suppression of dark count noise need to be realized.

A reasonable option to increase the key generation rate is to use WDM for a QKD system [35], [36]. We have developed a GHz-clocked WDM-QKD system with maximally eight wavelength channels. The scheme is decoyed BB84 using time-bin signals. The clock rate is 1.244 GHz. Fig. 3 shows a photo of this WDM-QKD system. The WDM encoder and decoder structures are summarized in Fig. 4. It provides a flexible solution to support a variety of applications including secure voice transmission and real-time secure TV conferencing with one-time pad (OTP) encryption. We put this system with two-channel WDM to field test. The two wavelengths were $\lambda_1 = 1547.72$ nm and $\lambda_2 = 1550.92$ nm. In the receiver, two APD systems were used. The quantum efficiency and dark count rate were 10–15% and 1–2 kcps.

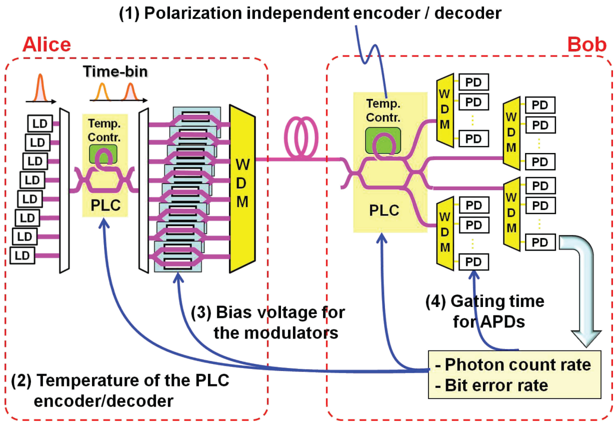
(1) Polarization independent encoder / decoder
Alice
Bob
Time-bin
LD
Temp. Contr.
PLC
W D M
PD
(3) Bias voltage for the modulators
(4) Gating time for APDs
- Photon count rate
- Bit error rate
(2) Temperature of the PLC encoder/decoder

Fig. 4. WDM encoder and decoder structures. At Alice, optical pulses of 50-ps-width pass through a 2×2 asymmetric Mach–Zehnder interferometer of PLC, and are converted into the time-bin pulses with a 400 ps separation. The time-bin pulses are de-multiplexed, and each wavelength component is independently encoded with the signal and decoy information. The signals are multiplexed again, together with the clock and frame synchronization signal, and input into a single fiber. At Bob, the clock signal is first separated, and the quantum signals pass through the PLC interferometer. They are then de-multiplexed at each of the four ports, and finally detected by the photon detectors.

The field fiber was 22 km in a loopback configuration between Koganei and Fuchu. The total loss is 12.6 dB. More than 95% of the channel is in an aerial fiber over poles. So it suffers from large polarization drift, which is mainly influenced by the sunlight time. In order to perform QKD in such a severe condition, we developed several stabilization techniques, as summarized in Fig. 4. [37]. One is polarization independent decoder based on planar light wave circuit (PLC). By carefully tuning the temperature, any polarization states can interfere properly at the output port of the PLC decoder. The similar PLC is also used in the encoder, where the temperature is fixed at a certain value, and photons passing through it are polarized. The PLC is connected to the WDM coupler and the modulators by polarization maintaining fibers. The polarization is disturbed in the channel, but its drift is not a matter in our decoder system. The other is feedback control to optimize temperature of the PLC encoder and decoder, bias voltage for the modulators, and gating time for APDs, by using photon count rate and bit error rate. These techniques allow one to realize stable high speed QKD for a long time, namely, quantum bit error rate (QBER) of 1.6% and key rate of 152 kb/s for the λ_1-channel, and QBER of 1.9% and key rate of 78 kb/s for the λ_2-channel for a 30-day period [19].

We have also developed a compact demonstration model for single channel operation at 1.244 GHz, whose photo is shown in Fig. 5. The transmitter/receiver is enclosed in a half-height rack. The transmitter occupies even less than half a volume of it. A typical key rate is 100 kb/s at a distance of 60 km assuming a fiber loss rate of 0.2 dB/km.

B. Entanglement QKD

Now let us turn our attention to a next generation QKD, entanglement-based QKD scheme [38]. The entanglement-based QKD schemes require no random number sources because random selection of bases can be automatically done in a passive manner in the measurement process. This allows one a simpler implementation. The scheme is also less susceptible to side-channel attacks. When highly efficient photon detectors are employed, DI security can be ensured by setting a criterion of appropriate inequalities testing the degree of entanglement.

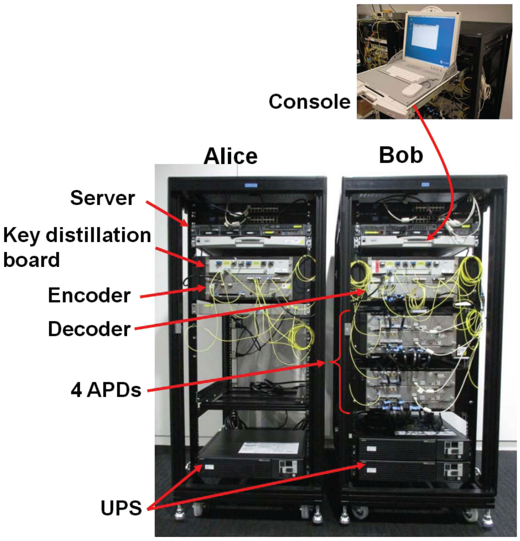

Fig. 5. A photo of the demonstration model.

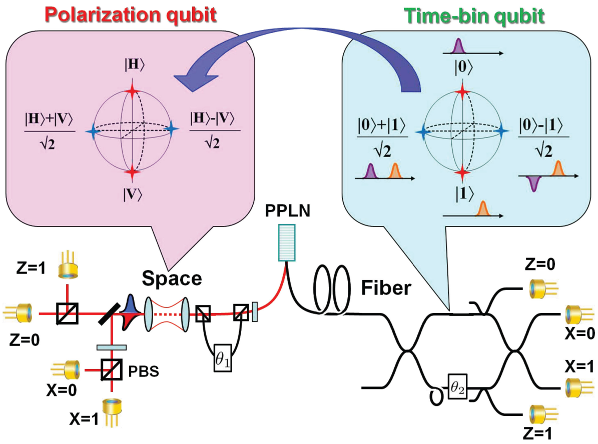

Fig. 6. Schematic of hybrid entanglement distribution.

We are particularly develop a scheme based on a hybrid entanglement source, which generates entangled photons between two different degrees of freedoms, time-bin format for fiber transmission at a telecom wavelength and polarization format for free space transmission at a near-infrared wavelength. This hybrid entanglement source will allow one to make a quantum link between fiber and space channels. It will also be useful for storing and relaying quantum information encoded in telecom photons via atomic or electronic systems with resonance at a near-infrared wavelength.

The scheme is depicted in Fig. 6. A periodically poled lithium niobate (PPLN) crystal pumped by continuous wave laser at 532 nm generates pairs of two photons in the two different wavelengths, one at 1550 nm and the other at 810 nm, in the same polarization. They are separated by a dichroic mirror. The pair correlation time is roughly 20 ps which was estimated from the spectral distribution of down converted photons from PPLN, and specifies the temporal scale of photon wave packets. This is much shorter than the detector time resolution of 400 ps. So the photons are correlated at each instantaneous time t, and are randomly distributed in the time domain.

Time-bin qubit is defined at Bob by his decoder, which is an asymmetric PLC interferometer. The long and short arms make a time difference of τ for the time-bin qubit. The long arm has a phase shifter with θ_2. Alice encodes polarization qubit by the format transformer from the time-bin qubit. Alice first rotates the polarization into 45° and put the photon into the format transformer. It is a polarization dependent delay line, consisting of a Glan laser prism with a delaying fiber. In this circuit, the horizontal polarization goes though straight, while the vertical polarization is reflected, delayed with a phase shift of θ_1, and finally comes back into the straight line.

With these delay circuits, a photon is distributed in three time slots, centered at $t - \tau$, t, and $t + \tau$. Alice and Bob finally select only the slot at t, and discards the other time slots. After all, the entanglement is formed between the polarization qubit at Alice and the time-bin qubit at Bob such as, for example, by selecting Z-basis measurement,

$$\frac{1}{\sqrt{2}}\left\{ e^{i\theta(\tau)}|H\rangle_A|1\rangle_B + e^{i[\theta(t+\tau)-\theta_1-\theta_2]}|V\rangle_A|0\rangle_B \right\} \qquad (1)$$

where $\theta(\tau)$ and $\theta(t+\tau)$ represent the phases of the pump beam.

We had performed a hybrid entanglement distribution experiment with the time-bin signal of 2.5 ns time separation using Si APDs for Alice and InGaAs APDs for Bob [39]. The quantum interference visibility of 95.8% and 88% with tolerance ±0.2% and ±1% along *Z–Z* and *X–X* axes, respectively, were demonstrated with a coincidence count rate of more than 800 cps, violating the threshold of 70.7% of the Bell inequality.

We have recently extended the scheme to an entanglement QKD system based on the modified Ekert 91 protocol [40]. The time separation was shortened to 800 ps. Alice's detectors were extended from four APDs to six, comprising the measurement with three sets of polarization qubit basis whose relative offset angles are 0°, −22.5°, −67.5°, respectively. Bob's detection of 1550 nm-wavelength photons were carried out by highly efficient SSPDs with detection efficiency of 60–70%. With this setup, we could have demonstrated the violation of the Clauser–Horne–Shimony–Holt inequality for the entanglement between the polarization qubit in free space and the time-bin qubit through 20 km fiber transmission. The secure key rate in our system is estimated to be ∼70–150 b/s.

C. *Efficient Photon Source*

The distance and key rate of the entanglement-QKD are still poorer than one-way QKD like BB84. For improving the key rate, more efficient photon sources are desired. We have developed the photon source based on type-II parametric down-conversion with a group-velocity matched periodically poled KTiOPO$_4$ (GVM-PPKTP) for the telecom bands. Picosecond laser pulses with a duration of 2 ps, whose central wavelength is tunable from 700 to 1000 nm, are used to pump a 30-mm-long PPKTP crystal with a poling period of 46.1 μm. This source could generate photon pairs with high spectral purity and tunability that can cover a wide range from 1460 to 1675 nm, namely covering the S-, C-, L-, and U-band in telecommunication wavelengths [41], [42].

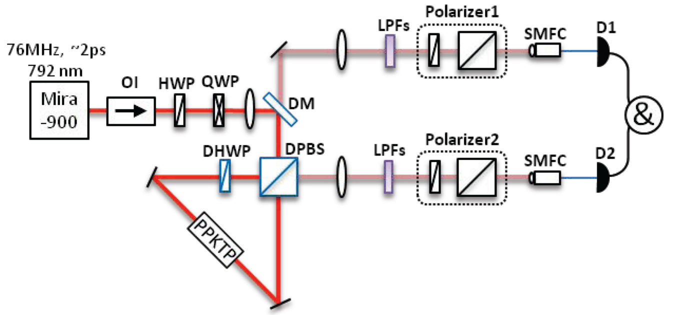

Fig. 7. Schemetic of Sagnac polarization-entangled photon source with a PPKTP crystal.

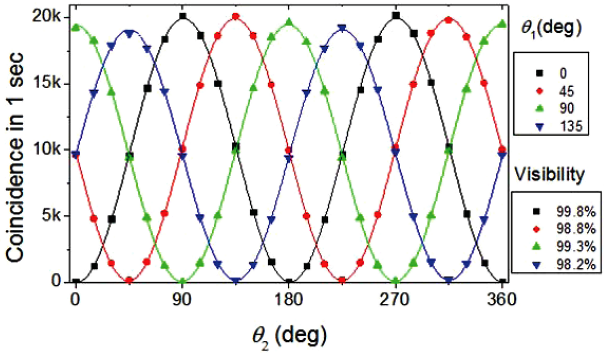

Fig. 8. Interference visibility of entangled photons from the Sagnac-PPKTP source.

We have also implemented Sagnac polarization-entangled photon source with a PPKTP crystal, which is compact, stable, highly entangled, spectrally pure and ultra-bright. The schemetic is shown in Fig. 7. The photons were detected by two SSPDs with detection efficiencies of 70% and 68% at dark counts of less than 1 kcps [43]. Recently the coincidence count rate has been doubled from the result reported in [43], by optimizing the alignment in the Sagnac loop. As shown in the interference pattern in Fig. 8, at 10 mW pump, the maximum coincidence count was 20 kcps (with single counts of 90 kcps for D1 and 120 kcps for D2), which corresponded to a coincidence of 40 kcps without polarizers. The visibility has also been increased from 96% in [43] to 98%. Thus a new tool box of quantum light source and detector at the telecom bands is now available, which surpasses the performace obtained so far in the near infrared wavelengths matched for the Si APD window. It will bring us a step closer to the realization of quantum information and communications technology in optical fiber infrastructures.

D. QKD Platform

Various QKD protocols can be integrated into a network by key relay via trusted nodes. In our QKD platform, the key management layer plays a role of networking. At each node, key management agent (KMA) is located, and receives the key material, resizes and saves them as well as to store information on quantum BER, key generation rate and so on. Secure key is encapsulated with the other key, and is relayed securely to the terminal. The KMAs also have APIs and supply secure key to variety of applications in the upper layers.

Fig. 9 depicts a secure network scheme which includes QKD-enhanced Layer-2 and Layer-3 switches. Layer-2 switches identify the media access control address (MAC address) of both sending and receiving devices, and switch packets in LANs. Currently high speed Layer-2 crypto-systems are commercially available, which directly encrypt data stream from the Layer-2 switch by using advanced encryption standard. The cipher text includes not only payload but also MAC and IP addresses of the users. QKD platform supports key refresh to Layer-2 encryptor/decriptor, and also adds OTP mode in Layer 2. Layer-3 switches perform routing based in IP addresses. The QKD-enhanced Layer-3 switches at Alice and Bob receive two kinds of secure key pairs. At Alice, one is used for encrypting payload and IP address by OTP, creating an OTP-encrypted IP packet. The other is used together with universal hash functions such as Wegman–Carter protocol, for generating an authentication tag from that packet. The packet consisting of the encrypted IP packet and the authentication tag is then routed to to Bob at the terminal node. Thus both encryption of data transfer and ITS authentication can be realized simultaneously in a compatible manner with the current standard of IPsec.

E. Key Rate Bound

Before closing this section, let us consider what is the maximum achievable key rate for the unconditionally secure QKD. The key rates of all the known point-to-point QKD protocols (BB84, CV-QKD, etc. without quantum repeater or trusted nodes), decay exponentially with the fiber distance, i.e., decay linearly with the transmittance of the channel. A natural question arisen is then whether there are yet-to-be discovered protocols that could circumvent this rate-loss tradeoff without using quantum repeaters. Recent theoretical progress revealed that this is impossible. This is shown by establishing a fundamental upper bound on the secret key generation rate of a point-to-point QKD [23].

To derive the fundamental bound, we need to consider the most generic point-to-point optical QKD protocol. Suppose Alice and Bob are given a pure-loss optical channel with transmittance η ($0 \leq \eta \leq 1$). Alice transmits n pulses of optical quantum states where n can be arbitrarily large (asymptotically long code) and the transmitted state can be any possible quantum states (perfect single photons, highly entangled states over n pulses and/or Alice's auxiliary system, etc). Bob can make any possible measurements allowed by quantum mechanics to detect these n pulses sent through a channel. They are also allowed unlimited two-way public classical communication over an authenticated channel in order to generate secret keys. As usual in QKD theory, Eve is assumed to make any kind of access to the channel allowed by quantum mechanics (note that we do not consider the Eve's attack on the devices kept by Alice and Bob since we assume that they can prepare perfectly noiseless/lossless ones). She also has access to all the public communication between Alice and Bob. In the above setting, Alice and Bob try to share secret keys that guarantee the information theoretic security. The question to be asked is what is the maximum secret key generation rate per pulse in the above setting.

The classical version of the problem was rigidly formulated in 1993 by Maurer [44] and Ahlswede and Csiszàr [45] (interestingly, [44] mentions that it was inspired by the invention of BB84) where they introduced the secret key agreement capacity on the classical wiretap channel assisted by two-way public communication and proved its lower and upper bounds. Though its exact capacity formula has not been known yet, Maurer and Wolf later introduced a quantity called the *intrinsic information* and proved that this quantity optimized over all channel input distribution is a sharp upper bound on the secret key agreement capacity [46].

This intrinsic information was extended to the quantum realm. Christandl and Winter defined the *squashed entanglement* of a bipartite quantum state and showed that it works as a good entanglement measure in quantum information theory [47]. More recently, we further extended these results by defining the *squashed entanglement of a quantum channel* and proved that this quantity has a more direct analog to the intrinsic information, i.e., it is an upper bound on the secret key agreement capacity, as well as the quantum capacity, in a quantum channel assisted by two-way classical public communication [48]. This upper bound has a relatively simple form and thus one can calculate it for various channels. In particular, applying it to a pure-loss optical channel, we can show that the key generation rate per pulse R is bounded by [23]

$$R \leq \log_2 \frac{1+\eta}{1-\eta}. \tag{2}$$

For a lossy channel, $\eta \ll 1$, this upper bound is approximated to be $\sim 2\eta/\ln 2$ which clearly shows that the linear tradeoff between the key rate and the loss (or transmittance) in the channel is a fundamental limit of any repeaterless QKD protocols. It should be stressed that the upper bound in Eq. (2) is solely a function of the channel loss (or transmittance) regardless of how much optical power the protocol may use. This is in sharp contrast with the normal communication (without secrecy) where without input power constraints the capacity can be arbitrarily high. Also it should be noted that Eq. (2) is just an upper bound of the capacity and thus it is an important open question whether this bound is achievable or not.

Fig. 10 compares the upper bound and the key rate achievable by the ideal BB84 where we assume a perfect single-photon source, detectors, and other devices, an ideal key distillation protocol, and the efficient BB84 protocol [49]. Note that the key rate per mode for the ideal BB84 is given by $\eta/2$ where the factor two comes from the fact that the BB84 usually encodes one

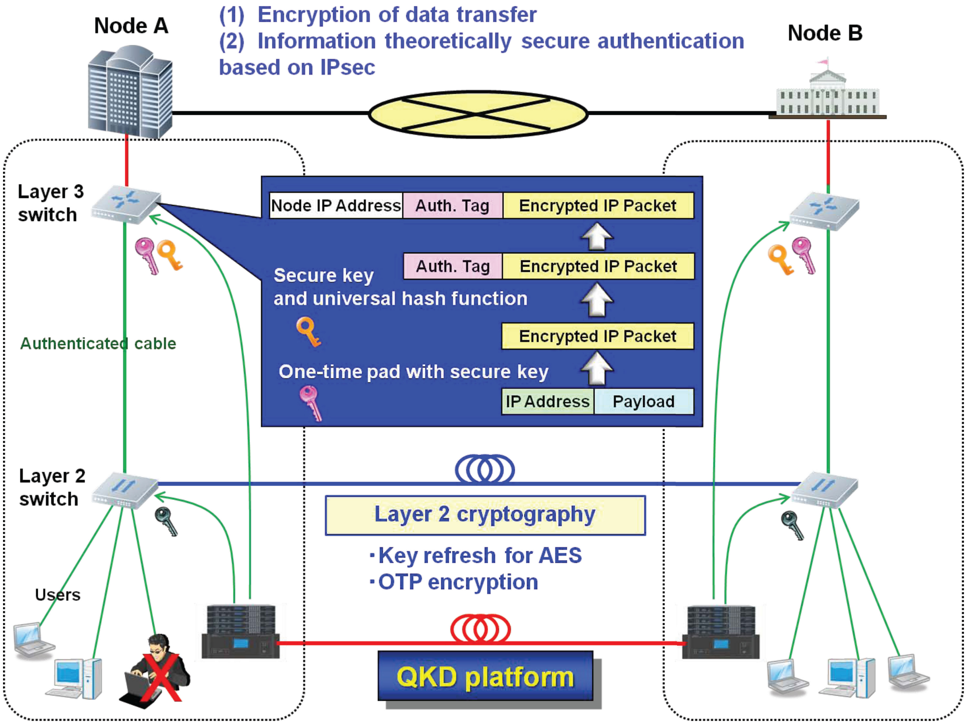

Fig. 9. QKD-enhanced Layer-2 and Layer-3 switches.

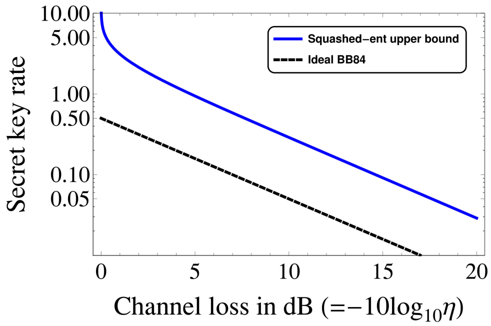

Fig. 10. Upper bound on the secret key capacity in a pure-loss optical channel assisted by two-way public communication (blue solid line) and the achievable key rate by the ideal BB84 (black dashed line).

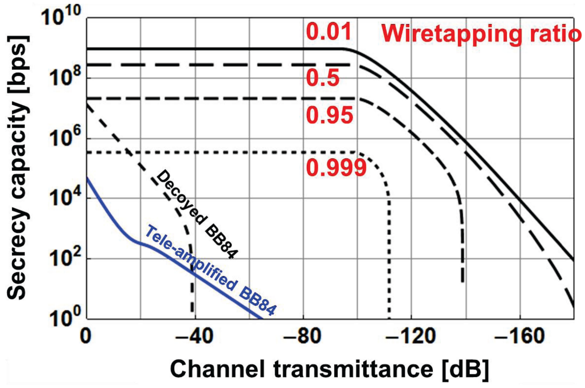

Fig. 11. A numerical example of the secrecy capacities for a wiretap channel with various tapping ratios in red by an eavesdropper.

qubit into two modes (two polarization modes or two temporal modes). The figure shows that though there exists some gap between the upper bound and the ideal BB84 key rate, it does not seem very worth to pursue alternative repeaterless QKD protocols for higher key rate over a lossy optical channel. Note that the discussion here does not include technical imperfections and excess channel noises. It is another issue to consider better protocols against the excess noises, device imperfections, side attacks, etc.

IV. Physical Layer Cryptography

A. Background

The key rate bound shown in the last subsection tells us how difficult it is to implement the unconditionally secure key distribution against Eve with unbounded physical and computational powers. The performance of this bound, even if realized, is insufficient to cover the ranges of rate and distance required for nation-wide and global scale uses of QKD. In principle, trusted-node QKD network can be extended to the nation-wide scale, however, an extention to the global scale including space links faces the intrinsic limit. Although quantum relay based on tele-amplification was proposed for space links, the key rate is always sacrificed (see Fig. 11) [51]. This fact motivates us to study more practical schemes that can cover the ranges mentioned above with reasonably compromised assumptions on Eve while keeping a required security level.

The notion of cryptographic security can be categorized into the two; algorithmic security and provable security (or information-theoretic security, ITS). The former relies on that certain mathematical problems are practically impossible to solve with current computer resources and well-known attacks. The latter is based on security proofs made in an information theoretic manner by showing the existence of channel coding that can effectively establish the statistical independence between the legitimate users and the eavesdropper, given a physical model of a channel [50]. Provably secure cryptography is also referred to as physical layer cryptography [24]. This has been originally studied in the RF domain in wireless networks. Studies in the optical domain also attract attention recently, especially in free space optical communications. Some milestone demonstrations of optical space data links have been successful recently, and the security concern is becoming an issue. Established algorithmic crypto-schemes should be a first option, but updating their specifications in satellites would not be easy when security vulnerabilities come out. Next option may be physical layer cryptography. In fact optical space communications are done in a line of sight between the sender (Alice) and the receiver (Bob). If an eavesdropper (Eve) is in the channel, then she is easily visible for Alice and Bob. So what Eve should do is to hide from Alice and Bob away from the channel, and try to collect scattered light to get information from Alice. Thus one may limit the physical ability of Eve. Note here that Eve can have unbounded computational power. Then in such a degraded condition for Eve, Alice and Bob can realize a much higher transmission rate with ITS.

B. Assumptions on the Channel Model

QKD is an extreme example of physical layer cryptography in the sense that the provable security is ensured for Eve with unlimited physical abilities and computational power. In the standard context of physical layer cryptography, however, the channel from Alice to Eve (wiretap channel) is assumed to be degraded compared with that from Alice to Bob (main channel). As an typical example, consider space laser link with photon counting by Bob and Eve. The main and wiretap channels are modeled by the channel transmittances η_y and η_z, and the dark count rates λ_y and λ_z. In the most common scenario, the signal-to-noise ratio (SNR) of Eve is worse than that of Bob, equivalently $\eta_z/\lambda_z < \eta_y/\lambda_y$, referred to as the degraded condition. On the other hand, other cases can also be possible, such as $\lambda_z \ll \lambda_y$ and $\eta_z < \eta_y$, if the mutual information between Alice and Bob $I(X;Y)$ is greater than that between Alice and Eve $I(X;Z)$, which is referred to as the more-capable condition. In any case, the mutual information difference between them should remain positive as

$$C_S = \max_{P_x} [I(X;Y) - I(X;Z)] \tag{3}$$

where X, Y, and Z are the variables for input from Alice to the channels, output from the main channel to Bob, and output from the wiretap channel to Eve, respectively, and P_x is the probability distribution for X. The quantity C_S, referred to as the secrecy capacity [50], specifies the asymptotically achievable transmission rate maximized by the probability distribution and channel coding, keeping the leaked information to Eve arbitrarily small.

C. Our Numerical Results

Here we present our numerical results on the secrecy capacity of physical layer cryptography with an on–off keying scheme based on pulse position modulation (PPM) coding for a carrier wavelength centered at 1550 nm. Fig. 11 compares the secrecy capacities as a function of the channel transmittance η_y (for the Alice-Bob main channel) for decoyed BB84 and physical layer cryptography. Here we assume that the pulse generation rate is 1 GHz. For decoyed BB84, the dark count probability is assumed to be 10^{-6} per pulse (1000 cps), which is typical for the current detectors used in QKD systems. The final key rate is typically 100 kb/s at a distance of -20 dB loss, roughly corresponding to a 100 km distance for a low loss fiber. The key rate rapidly falls down at a distance of -40 dB loss, which is roughly the best link budget for a low-earth-orbit-to-ground distance in optical space communication. The curve entitled *Tele-amplified BB84* represents a scheme with quantum relay to extend a distance [51]. One sees that there is a tradeoff between the final key rate and the distance, namely extension of distance sacrifices the key rate. Decoyed BB84 hardly generates the secure key at around -40 dB, while tele-amplified BB84 can make a QKD link over longer distances. But the key rate may still be poor.

The secrecy capacities of an on–off keyed PPM scheme are shown by solid, long-dashed, dashed, and dotted lines with the wiretap ratios $\eta_z/\eta_y = 0.01$, 0.5, 0.95, and 0.999, respectively. The pulse generation rate is again 1 GHz, and the transmission power is assumed to be 1 W. We then numerically calculate the secrecy capacity under this power constraint. Background counts are assumed to be $\lambda_y = 10^4$ cps for Bob and $\lambda_z = 1$ cps for Eve, i.e. Eve has a much less noisy system. As seen, we can cover a wide range of performance of the provably secure communications with relatively high transmission rates. As the channel transmittance decreases below -100 dB, the transmission rate starts to decrease because the SNR gets smaller.

D. Our Theory of Finite Length Analysis

The secrecy capacity is the achievable rate in the asymptotic limit at code length $n \to \infty$. A stronger characterization can be made at any finite code length n, namely by showing how fast Bob's error probability and the leaked information to Eve decrease as code length n increases. In coding for physical layer cryptography, one should add not only redundant bits to perform error correction but also randomness bits to deceive Eve. So there are two kinds of rates, the reliable transmission rate R_B for Bob (message bit length/n), and the randomness rate R_E to deceive Eve (randomness bit length/n) as shown in Fig. 12. The redundancy and randomness are in a tradeoff relation, and to be minimal within the tradeoff. We would like to know how Bob's error probability and the leaked information to Eve can be small for various rates R_B and R_E at finite code length n. We want to estimate required resources of bits for any given level of reliability for Bob and secrecy against Eve.

Conceptual codeword structure and the definitions of related metrics are shown in Fig. 12. Bob's decoding error ϵ_n^B is defined

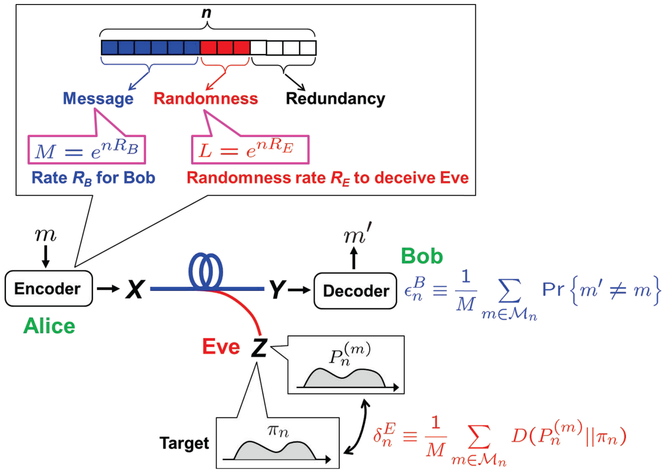
n
Message
Randomness
Redundancy
$M = e^{nR_B}$
$L = e^{nR_E}$
Rate R_B for Bob
Randomness rate R_E to deceive Eve
m
Encoder
X
Y
Decoder
m'
Bob
$\epsilon_n^B \equiv \frac{1}{M}\sum_{m\in\mathcal{M}_n} \Pr\{m' \neq m\}$
Alice
Eve
Z
$P_n^{(m)}$
Target
π_n
$\delta_n^E \equiv \frac{1}{M}\sum_{m\in\mathcal{M}_n} D(P_n^{(m)}||\pi_n)$

Fig. 12. Conceptual codeword structure, the rate R_B for Bob and the randomness rate R_E to deceive Eve, as well as the related metrics of the decoding error and the KL distance.

as an average over all the messages of M in code length n

$$\epsilon_n^B \equiv \frac{1}{M}\sum_{m\in\mathcal{M}_n} \Pr\{m' \neq m\}. \tag{4}$$

There are some candidates of secrecy measures. We adopt here the averaged Kullback–Leibler (KL) distance δ_n^E between an output distribution $P_n^{(m)}$ and a target distribution π_n at Eve due to an arbitrarily prescribed input distribution to the wiretap channel,

$$\delta_n^E \equiv \frac{1}{M}\sum_{m\in\mathcal{M}_n} D(P_n^{(m)}||\pi_n) \tag{5}$$

because it can quantify the strongest security in an information theoretic way. In fact if the KL distance δ_n^E goes to zero, then both the mutual information I_n^E and the variable distance d_n^E go to zero as well [53].

So we would like to make Bob's decoding error ϵ_n^B and Eve's KL distance δ_n^E as small as desired. The upper bound of Bob's decoding error was derived in the form of exponentially decreasing function of length n by Gallager [52]. The exponent is called the reliability function. This method was extended to upper-bounding the leaked information (the mutual information) to Eve by Hayashi [54] without the cost constraint. We extend it to the cost constrained case with the KL distance.

In Fig. 13, we depict a channel model and the quantities necessary to describe the main result. We define the following dual functions;

$$\phi(\rho|W_B, q, r) =$$
$$-\log\left[\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} q(x)W_B(y|x)^{\frac{1}{1+\rho}} e^{r[\Gamma-c(x)]}\right)^{1+\rho}\right] \tag{6}$$

$$\phi(-\rho|W_B, q, r) =$$
$$-\log\left[\sum_{z\in\mathcal{Z}}\left(\sum_{x\in\mathcal{X}} q(x)W_E(z|x)^{\frac{1}{1-\rho}} e^{r[\Gamma-c(x)]}\right)^{1-\rho}\right] \tag{7}$$

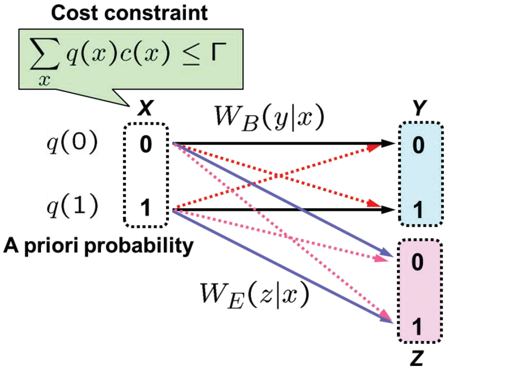

Fig. 13. The channel matrices $W_B(y|x)$ and $W_E(y|x)$ for the main and wiretap channels, respectively, and the *a priori* probabilities $q(x)$ for X. The cost constraint Γ, which may be the power constraint and so on, is imposed in the input X.

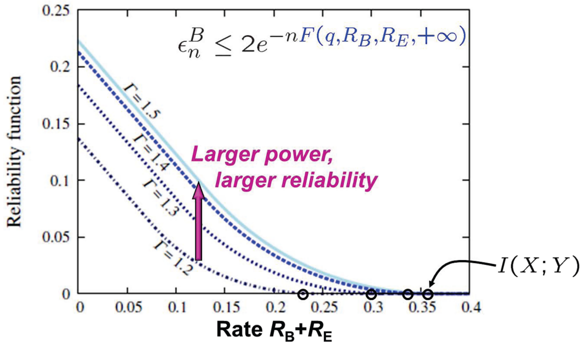

Fig. 14. The reliability functions for several cost constraints.

and define the reliability and secrecy functions, respectively,

$$F_c(q, R_B, R_E, \infty) = \sup_{0\leq\rho\leq 1}\sup_{r\geq 0}\Big[\phi(\rho|W_B, q, r)$$
$$-\rho(R_B + R_E)\Big] \tag{8}$$

$$H_c(q, R_E, \infty) = \sup_{0<\rho<1}\sup_{r\geq 0}\Big[\phi(-\rho|W_E, q, r) + \rho R_E\Big]. \tag{9}$$

Then for stationary memoryless channels, we can show that Bob's decoding error and Eve's KL distance are upper bounded as [53]

$$\epsilon_n^B \leq 2e^{-nF_c(q,R_B,R_E,+\infty)}, \tag{10}$$

$$\delta_n^E \leq 2e^{-nH_c(q,R_E,n)}. \tag{11}$$

Fig. 14 plots the reliability functions for several cost constraints in the case of the on-off keying photon channel presented in Fig. 11 (at −90 dB of η_y with $\eta_z/\eta_y = 0.5$). Γ is understood here as a given transmission power. As seen, larger power allows

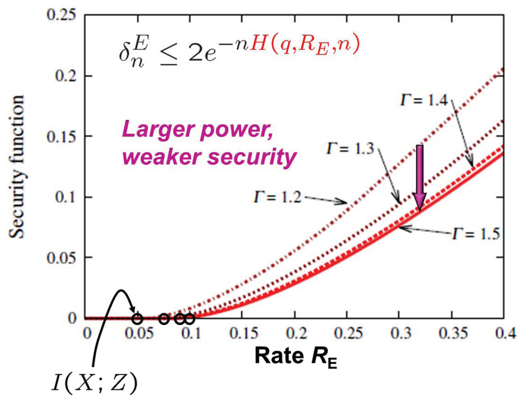

Fig. 15. The secrecy functions for several cost constraints.

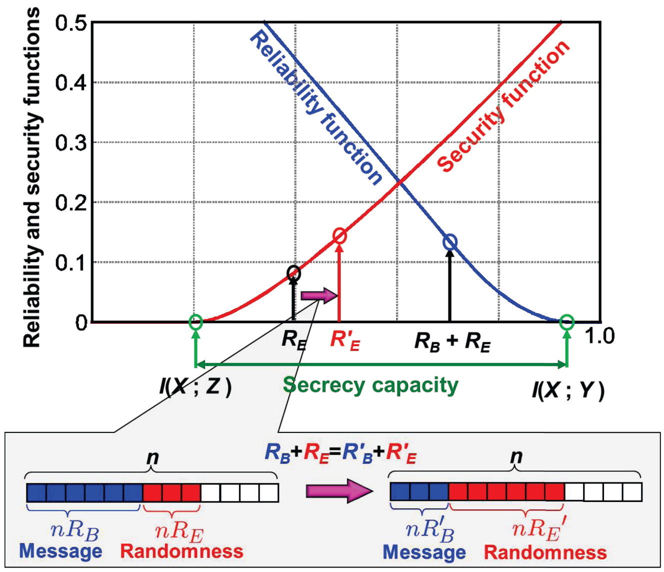

Fig. 16. The reliability and secrecy functions, and the tradeoff engineering to increase the secrecy against Eve, keeping the reliability for Bob.

larger reliability. The horizontal axis is a sum of the rates R_B and R_E. The points of the rates where the reliability function becomes zero, correspond to the mutual information between Alice and Bob, $I(X;Y)$.

On the other hand, Fig. 15 plots the secrecy functions. Larger power implies weaker secrecy. The horizontal axis is the randomness rate R_E.

In Fig. 16, we plot the reliability and secrecy functions at the same time. The reliable transmission with the provable security is possible for the rates in the interval indicated by the green arrow. The figure also shows an example of the tradeoff engineering to increase the secrecy, keeping the reliability of Bob. The randomness rate R_E is increased to R'_E, while the rate for Bob R_B is decreased, keeping the sum of the two the same value. The change of the secrecy function quantifies the increase of the secrecy level.

Finally we consider the maximum criteria, m–ϵ_n^B and m–δ_n^E over all possible message $m \in \mathcal{M}_n$, instead of the averaged criteria ϵ_n^B and δ_n^E. The m–δ_n^E is particularly important, because even with small δ_n^E, we cannot exclude a possibility that the KL distance is very large for some particular message m, which implies that the message m is not saved from successful decryption by Eve. On the other hand, with small m–δ_n^E, *every* message $m \in \mathcal{M}_n$ is guaranteed to be highly confidential against Eve. This kind of criterion has never been shown for the KL distance against Eve. We apply Gallager's technique for the decoding error [52] and have derived that the maxima of Bob's decoding error and Eve's KL distance are upper bounded as [53];

$$\begin{aligned} \text{m}\!-\!\epsilon_n^B &\equiv \max_{m\in\mathcal{M}_n} \Pr\{m' \neq m\} \\ &\leq 6e^{-nF_c(q,R_B,R_E,+\infty)} \qquad (12) \\ \text{m}\!-\!\delta_n^E &\equiv \max_{m\in\mathcal{M}_n} D(P_n^{(m)}||\pi_n) \\ &\leq 6e^{-nH_c(q,R_E,n)}. \qquad (13) \end{aligned}$$

Thus the maximum criteria relaxes the upper bounds only by a factor of three times. Especially one can clearly see that there must exist a good wiretap channel code which can exclude the worst exceptional cases, which was not proven so far with the averaged secrecy metrics.

V. Concluding Remark

We have presented our recent results on GHz-clocked BB84 QKD systems, entanglement QKD technologies, and the theories of QKD key rate bound and physical layer cryptography. Our QKD systems are deployed into practical metoroplitan-scale networks, and are integrated into the QKD platform for a new solution for key exchange and key supply. Entanglement QKD can be put into shorter distance links, such as important intra-networks. The point-to-point QKD link performance, however, has the intrinsic limit as shown in Section III-E. Quantum repeater is yet to be met with the criteria for practical application to QKD. So at present efforts should be paid on widening QKD applications in metoroplitan-scale networks.

In order to realize secure global network with the provable security, one must rely on physical layer cryptography while assuming that the wiretap channel to Eve is physically bounded. We have developed a theory to quantify the tradeoff between the reliability and the secrecy in finite code length n under the cost constraint. Namely we derived a dual set of the reliability and secrecy functions, those specify exponentially decreasing rates of Bob's decoding error and leaked information to Eve as n increases.

In optical space communications which are basically line-of-sight links, the degraded wiretap channel condition seems reasonable in practice. On the other hand, in optical fiber communications, the degraded condition is highly non-trivial. In fact, assuming that Alice and Bob know Eve's channel is unrealistic in most fiber network scenarios. So coding must be designed to withstand the uncertainty of the wiretap channel.

A reasonable approach is to deal with multiple possible realizations for the wiretap channel, each of which is actually occur is unknown. An interesting scheme in this deirection has been proposed as *security embedding codes* [55], where the high-security message can be embedded into the low-security message at full rate without incurring any loss on the overall rate of communication. The number of secure bits delivered to Bob depends on the actual realization of the wiretap channel. When the wiretap channel realization is weak, all bits at Bob need to be secure. When the wiretap channel realization is strong, a prescribed part of the bits needs to remain secure. Another interesting approach is to combine network coding with wiretap channel coding [56]. This so-called *secure network coding* on a wiretap network deals with multiple statistically independent messages from multiple nodes as the random bits making a certain message ambiguous to Eve.

Our theory and the above mentioned approaches are still within a classical framework based on classical symbols, for given channel matrices $W_B(y|x)$ and $W_E(y|x)$. In the quantum setting, given and fixed is a quantum channel (a completely positive trace preserving map), and input states, detection strategy, and coding can be the variables. Extending the theories into the quantum domain remains completely open.

Eventually the known schemes of QKD and prospective schemes of physical layer cryptography will be integrated on photonic network infrastructures to realize high capacity communications with the provable security. These schemes should cooperate with modern cryptographic technologies which are already operating in the upper layers. This new network paradigm is referred to as quantum photonic network. It indicates a direction to unify optical/quantum communications with coding and cryptographic technologies, which is indeed an endeavour in information and communications technologies.

REFERENCES

[1] C. E. Shannon, “A mathematical theory of communication-Part I/Part II,” *Bell Syst. Tech. J.*, (Part I) vol. 27, pp. 379–423, (Part II) pp. 623–656, Jul./Oct. 1948.

[2] A. Waseda, M. Takeoka, M. Sasaki, M. Fujiwara, and H. Tanaka, “Quantum detection of wavelength-division-multiplexing optical coherent signals,” *J. Opt. Soc. Amer. B*, vol. 27, no. 2, pp. 259–265, Feb. 2010.

[3] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, “A demonstration of superadditivity in the classical capacity of a quantum channel,” *Phys. Lett. A*, vol. 236, nos. 1/2, pp. 1–4, Dec. 1997.

[4] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, “Quantum channels showing superadditivity in classical capacity,” *Phys. Rev. A*, vol. 58, no. 1, pp. 146–158, Jul. 1998.

[5] M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, “Exceeding classical capacity limit in quantum optical channel,” *Phys. Rev. Lett.*, vol. 90, no. 16, pp. 167906-1–167906-4, Apr. 2003.

[6] M. Takeoka, M. Fujiwara, J. Mizuno, and M. Sasaki, “Implementation of generalized quantum measurements: Superadditive quantum coding, accessible information extraction, and classical capacity limit,” *Phys. Rev. A*, vol. 69, pp. 052329-1–052329-14, May 2004.

[7] A. Waseda, *et al.*, “Numerical evaluation of PPM for deep-space links,” *J. Opt. Commun. Netw.*, vol. 3, no. 6, pp. 514–521, Jun. 2011.

[8] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, “Classical information capacity of a quantum channel,” *Phys. Rev. A*, vol. 54, no. 3, pp. 1869–1876, Sep. 1996.

[9] A. S. Holevo, “The capacity of the quantum channel with general signal states,” *IEEE Trans. Inf. Theory*, vol. 4, no. 1, pp. 269–273, Jan. 1998.

[10] B. Schumacher and M. Westmoreland, “Sending classical information via noisy quantum channels,” *Phys. Rev. A*, vol. 56, no. 1, pp. 131–138, Jul. 1997.

[11] V. Giovannetti, *et al.*, “Classical capacity of the lossy Bosonic channel: The exact solution,” *Phys. Rev. Lett.*, vol. 92, no. 2, pp. 027902-1–027902-4, Jan. 2004.

[12] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, “Photon level crosstalk between parallel fibers installed in urban area,” *Opt. Exp.* vol. 18, no. 21, pp. 22199–22207, Oct. 2010.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[14] C. Elliott, *et al.*, “Current status of the DARPA quantum network: Quantum information and computation III,” *Proc. SPIE*, vol. 5815, pp. 138–149, Jun. 2005.

[15] M. Peev, *et al.*, “The SECOQC quantum key distribution network in Vienna,” *New J. Phys.*, vol. 11, pp. 075001-1–075001-37, Jul. 2009.

[16] M. Sasaki, *et al.*, “Field test of quantum key distribution in the Tokyo QKD Network,” *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, May 2011.

[17] D. Stucki, *et al.*, “Long-term performance of the SwissQuantum quantum key distribution network in a field environment,” *New J. Phys.*, vol. 13, no. 12, p. 123001-/1–123001-18, Dec. 2011.

[18] J. F. Dynes, *et al.*, “Stability of high bit rate quantum key distribution on installed fiber,” *Opt. Exp.*, vol. 20, no. 15, pp. 16339–16347, Jul. 2012.

[19] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, “Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days,” *Opt. Exp.*, vol. 21, no. 25, pp. 31395–31401, Dec. 2013.

[20] K. Shimizu, *et al.*, “Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area,” *J. Lightw. Technol.*, vol. 32, no. 1, pp. 141–151, Jan. 2014.

[21] ID Quantique. (2001), [Online] Available: http://www.idquantique.com/; MagiQ Technologies, Inc. (1999), [Online] Available: http://www.magiqtech.com/MagiQ/Home.html; QuintessenceLabs Pty Ltd. (2006), [Online] Available: http://www.quintessencelabs.com/; SeQureNet. (2008), [Online] Available: http://www.sequrenet.com/.

[22] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore India, Dec. 1984, pp. 175–179.

[23] M. Takeoka, S. Guha, and M. M. Wilde, “Fundamental rate-loss tradeoff for optical quantum key distribution,” *Nat. Commun.*, vol. 5, pp. 5235-1–5235-7, Oct. 2014.

[24] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Thoery*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[25] K. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, “Security in photonic networks: Potential threats and security enhancement,” *J. Lightw. Technol.*, vol. 29, no. 21, pp. 3210–3222, Nov. 2011.

[26] L. Lydersen, *et al.*, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photon.* vol. 4, no. 10, pp. 686–689, Aug. 2010.

[27] Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Avoiding the blinding attack in QKD,” *Nature Photon.* vol. 4, no. 12, pp. 800–801, Dec. 2010.

[28] L. Lydersen, V. Makarov, and J. Skaar, “Secure gated detection scheme for quantum cryptography,” *Phys. Rev. A*, vol. 83, no. 3, pp. 032306-1–032306-7, Jan. 2011.

[29] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, “Controlling a superconducting nanowire single-photon detector using tailored bright illumination,” *New J. Phys.*, vol. 13, no. 11, pp. 113042-1–113042-14, Nov. 2011.

[30] L. Lydersen, J. Skaar, and V. Makarov, “Tailored bright illumination attack on distributed-phase-reference protocols,” *J. Mod. Opt.*, vol. 58, no. 8, pp. 680–685, Dec. 2010.

[31] T. Honjo, *et al.*, “Countermeasure against tailored bright illumination attack for DPS-QKD,” *Opt. Exp.*, vol. 21, no. 3, pp. 2667–2673, Feb. 2013.

[32] M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, and M. Sasaki, “Characteristics of superconducting single photon detector in DPS-QKD system under bright illumination blinding attack,” *Opt. Exp.*, vol. 21, no. 5, pp. 6304–6312, Mar. 2013.

[33] A. Acin, *et al.*, “Device-independent security of quantum cryptography against collective attack,” *Phys. Rev. Lett.*, vol. 98, no. 23, pp. 230501-1–230501-4, Jun. 2007.

[34] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, pp. 130503-1–130503-4, Mar. 2012.

[35] K. Yoshino, *et al.*, “High-speed wavelength-division multiplexing quantum key distribution system,” *Opt. Lett.*, vol. 37, no. 2, pp. 223–225, Jan. 2012.

[36] A. Tanaka, *et al.*, "High-speed quantum key distribution system for 1 Mbps real-time key generation," *IEEE J. Quantum Electron.*, vol. 48, no. 4, pp. 542–550, Apr. 2012.

[37] Y. Nambu, K. Yoshino, and A. Tomita, "Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit," *J. Mod. Opt.*, vol. 55, no. 12, pp. 1953–1970, Jul. 2008.

[38] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[39] M. Fujiwara, *et al.*, "Performance of hybrid entanglement photon pair source for quantum key distribution," *Appl. Phys. Lett.*, vol. 95, no. 26, pp. 261103-1–1261103-3, Dec. 2009.

[40] M. Fujiwara, *et al.*, "Modified E91 protocol demonstration with hybrid entanglement photon source," *Opt. Exp.*, vol. 22, no. 11, pp. 13616–13624, Jun. 2014.

[41] R. Jin, *et al.*, "Nonclassical interference between independent intrinsically pure single photons at telecommunication wavelength," *Phys. Rev. A*, vol. 87, no. 6, pp. 063801-1–063801-4, Jun. 2013.

[42] R.-B. Jin, R. Shimizu, K. Wakui, H. Benichi, and M. Sasaki, "Widely tunable single photon source with high purity at telecom wavelength," *Opt. Exp.*, vol. 21, no. 9, pp. 10659–10666, Apr. 2013.

[43] R.-B. Jin, *et al.*, "Pulsed Sagnac polarization-entangled photon source with a PPKTP crystal at telecom wavelength," *Opt. Exp.*, vol. 22, no. 10, pp. 11498–11507, May 2014.

[44] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Thoery*, vol. 39, no. 3, pp. 733–742, May 1993.

[45] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[46] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Thoery*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[47] M. Christandl and A. Winter, "Squashed entanglement: An additive entanglement measure," *J. Math. Phys.*, vol. 45, no. 3, pp. 829–840, 2004.

[48] M. Takeoka, S. Guha, and M. M. Wilde, "The squashed entanglement of a quantum channel," *IEEE Trans. Inf. Thoery*, vol. 60, no. 8, pp. 4987–4998, Aug. 2014.

[49] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and proof of its unconditional security," *J. Cryptogr.*, vol. 18, pp. 133–165, 2006.

[50] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[51] J. S. Neergaard-Nielsen, Y. Eto, C.-W. Lee, H. Jeong, and M. Sasaki, "Quantum tele-amplification with a continuous-variable superposition state," *Nature Photon.*, vol. 7, pp. 439–443, May, 2013.

[52] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968.

[53] T.-S. Han, H. Endo, and M. Sasaki, "Reliability and security functions of the wiretap channel under cost constraint," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6819–6843, Nov. 2014. arXiv:1307.0608 [cs.IT].

[54] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.

[55] H. D. Ly, T. Liu, and Y. Blankenship, "Security Embedding Codes," *IEEE Trans Inf. Forensics Security*, vol. 7, no. 1, pp. 148–159, Feb. 2012.

[56] N. Cai, and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

Masahide Sasaki received the B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Sendai, Japan, in 1986, 1988, and 1992, respectively. During 1992 to 1996, he worked on the development of semiconductor memory in Nippon-Kokan Company, which is currently JFE Holdings, Kanagawa, Japan. In 1996, he joined the Communications Research Laboratory, Ministry of Posts and Telecommunications, Koganei, Japan (since 2004, National Institute of Information and Communications Technology (NICT), Ministry of Internal Affairs and Communications). Since 1994, he has been working on quantum optics, quantum communication, and quantum cryptography. He is presently the Director of the Quantum ICT Laboratory, NICT, and the Chair of Quantum ICT Forum, Japan. He is a Member of the Japanese Society of Physics, and the Institute of Electronics, Information, and Communication Engineers of Japan.

Mikio Fujiwara received the B.S. and M.S. degrees in electrical engineering and Ph.D. degree from Nagoya University, Aichi, Japan, in 1990, 1992, and 2002, respectively. In 1992, he joined Communications Research Laboratory, Ministry of Posts and Telecommunications, and was involved in the development of Ge:Ga far-infrared photoconductors. Since 2000, he has been with the Quantum Information Technology Group. His current research interests include single photon detectors and an entanglement-based QKD system in the telecom-bands.

He is a Member of the Japanese Society of Physics, and the Institute of Electronics, Information, and Communication Engineers of Japan.

Rui-Bo Jin received the B.S. degree in physics from Henan Normal University, Xinxiang, China, in 2005, the M.Eng. degree in optical engineering from South China Normal University, Guangzhou, China, in 2008, and the Ph.D. degree in electronic engineering from Tohoku University, Sendai, Japan, in 2011. From 2011 October to 2012 March, he has been a Postdoctoral with Tohoku University, Sendai. Since April 2012, he has been a Researcher with the National Institute of Information and Communications Technology, Koganei, Japan. His research interests include experimental quantum information processing with linear optics. He is a Member of the Optical Society of America.

Masahiro Takeoka received the Ph.D. degree in electrical engineering from Keio University, Kanagawa, Japan, in 2001. He is currently a Senior Researcher with the National Institute of Information and Communications Technology, Koganei, Tokyo, Japan. His current research interests include quantum information theory, quantum optics, quantum communication, and optical quantum information processing.

Te Sun Han (M'79–SM'88–F'90) received the B.Eng., M.Eng., and Dr. Eng. degrees in mathematical engineering from the University of Tokyo, Tokyo, Japan, in 1964, 1966, and 1971, respectively.

From 1972 to 1975, he has been a research associate at University of Tokyo, Tokyo, Japan. From 1975 to 1983, he was an Associate Professor with the Department of Information Sciences, Sagami Institute of Technology, Fujisawa, Japan. He was a Visiting Professor with the Faculty of Mathematics, University of Bielefeld, Germany, in 1980 spring, and a Visiting Fellow at the Laboratory of Information Systems, Stanford University, USA, in 1981 summer. From 1983 to 1985, he was a Professor with the Mathematics Department, Toho University, Chiba, Japan. From 1985 to 1993, he was a Professor with the Department of Information Systems, Senshu University, Kawasaki, Japan. From 1993 to 2007, he was a Professor with the Graduate School of Information Systems, University of Electro-Communications, Tokyo. From 1990 to 1991, he was a Visiting Fellow with the Department of Electrical Engineering, Princeton University, USA, and at the School of Electrical Engineering, Cornell University, USA. In 1994 summer, he was a Visiting Fellow with the Faculty of Mathematics, University of Bielefeld. From 2007 to March 2010, he was a Visiting Professor with Waseda University, Japan, and since April 2010, he has been a Senior Visiting Researcher at the National Institute of Information and Communications Technology, Tokyo, Japan.

Dr. Han has published many papers, including papers in IEEE TRANSACTIONS ON INFORMATION THEORY.

From 1978 to 1990, he was involved in organizing activities in the Board of Governers for Society of Information Theory and Its Applications, Japan. He was the Members of the program committees for 1988 IEEE ISIT, Kobe, Japan; 1995 IEEE ISIT Whisler, Canada; 1997 IEEE ISIT, Ulm, Germany; 1998 IEEEE ISIT, Boston, USA: 2004 IEEE ISIT, San Antonio, USA; 2007 IEEE ISIT, Nice, France; 2009 IEEE ISIT, Toronto, Canada, respectively. He is also a Cochairman for the third, fifth, sixth, seventh Benelux-Japan Workshops on Information Theory and Communication, Eindhoven, June, 1994; Hakone, Japan 1996; Essen, Germany 1996; Eltville, Germany, 1997, respectively. Moreover, he is a Cochairman of the program committee for 2003 IEEE ISIT, Yokohama, Japan. From 1994 to 1996, he was a Chairman of the Tokyo Chapter for IEEE Information Theory Society.

From 1994 to 1997, he is an Associate Editor for Shannon Theory for IEEE TRANSACTIONS ON INFORMARTION THEORY, and a Member of the Board of Governers for IEEE Information Theory Society. He received the Shannon Award in 2010, and he is an IEICE Member of Honor from 2011.

His research interests include basic problems in Shannon Theory, multi-user source/channel coding systems, multiterminal hypothesis-testing and parameter estimation under data compression, large-deviation approach to information-theoretic problems, and especially, information-spectrum theory.

Hiroyuki Endo received the B.S. and M.S. degrees in physics from Waseda University, Tokyo, Japan, in 2012 and 2014, respectively.

Since 2013, he is a Cooperative Visiting Reseracher at National Institute of Information and Communications Technology (NICT), Tokyo, Japan. His research interests include informational security and free-space communication theory.

Ken-Ichiro Yoshino received the B.E. and M.E. degrees in applied physics from the University of Tokyo, Tokyo, Japan, in 2003 and 2005, respectively. Since 2005, he has been working on research and development of quantum communication/cryptographic system in NEC Corporation, Kawasaki, Japan.

Takao Ochi received the B.E. and M.E. degrees in electronics engineering from Osaka Prefecture University, Osaka, Japan, in 1991 and 1993, respectively, and the M.E. degree in informatics from the Institute of Information Security, Kanagawa, Japan, in 2008. In 1993, he joined the NEC Corporation, Tokyo, Japan. He is involved in development and project management of fingerprint authentication system, authentication system, and security operation center. Since 2012, he is involved in research and development of secure photonic network-based on quantum key distribution technology.

He is a Member of the Information Processing Society of Japan.

Shione Asami received the B.E. degree in communication engineering from the Shibaura Institute of Technology, Tokyo, Japan. In 1989, he joined the NEC Corporation, Tokyo. He is involved in proposal, development, and maintenance of decision-making support systems. Since 2000, he has been involved in construction and maintenance of security diagnostic, security education, and security monitoring center. He is currently responsible for collaboration with public office, including the Interpol, about countermeasure of cyber-attack.

Akio Tajima received the B.E. and M.E. degrees in electrical engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1990 and 1992, respectively.

In 1992, he joined the NEC Corporation, Kawasaki, Japan. His research interests include optical networking, quantum cryptosystem, and optical access systems. Since 2003, he has been involved in secure photonic network based on quantum key distribution technology. He is currently a principal researcher with NECfs Green Platform Research Laboratories. He is a Senior Member of the Institute of Electronics, Information, and Communication Engineers, Japan.