3-3 Channel Estimation Experiment for Physical Layer Cryptography in Free-space Optical Communication

Hiroyuki ENDO, Mikio FUJIWARA, Mitsuo KITAMURA, Orie TSUZUKI, Toshiyuki ITOH, Ryosuke SHIMIZU, Morio TOYOSHIMA, Hideki TAKENAKA, Masahiro TAKEOKA, and Masahide SASAKI

Physical layer cryptography is the cryptographic technique which realizes the information-theoretically secure message transmission and key establishment by exploiting physical properties of transmission channels. In this paper, we give an outline of fundamental model for physical layer cryptography and present the main result of channel estimation experiment toward the physical layer cryptography in free space optical communication which is carried out by Quantum ICT Advanced Developed Center.

1 Introduction

Recently, information networks are one of the important infrastructure for our lives as IT technology develops and spreads rapidly, and we receive many benefits from them. On the other hand, it is indispensable to protect confidential information by use of encryption techniques because cases of transmission of highly confidential information are increasing such as in online shopping or electronic application to public organizations.

The security of present networks is protected by so-called "modern cryptography" such as symmetric key cryptography that ensures confidentiality of messages or public key cryptography for key establishment and authentication. The algorithms of modern cryptography are open to public, so it can be implemented regardless of physical media such as cables or radio waves. Moreover, the security of modern cryptography is based on mathematics related to the present technological level. For example, as for public key cryptography, the basis of the security is the difficulty in solving certain mathematical problem in a realistic timeline using computers, such as prime decomposition of a large composite number. It is relatively easy to ensure security by such a large amount of calculation. However, the security is threatened by the emergence of efficient decryption algorithms or quantum computers. In order to cope with such kind of threats, countermeasures such as extension of the key size or utilizing mathematical problems that are hard to solve even for quantum computers have been developed year by year. Because of the features listed above, the present cipher is implemented in various devices and systems, that is a technology to support the base of our present society.

On the other hand, an authority of information theory, Wyner, proposes a cipher technique that is based on a quite different paradigm from the present cipher. The wiretap channel encoding [1][2] he proposed not only corrects errors that occur during the communication process but also realizes confidential communication without sharing a key in advance by utilizing noise occurring at an eavesdropper. In addition, security against an eavesdropper with any computational ability, that is, information theoretical security [3], is verified basing on the unpredictability of the physical phenomenon of noise. Since then, Maurer [4] and Ahlswede [5] independently proposed secret key agreement that is method of key sharing utilizing physical noise by applying the ideas of Wyner. These techniques are deemed to operate at the most bottom physical layer, although the present cipher is operated at a higher-level layer in the OSI model. Therefore, wiretap channel encoding and secret key agreement are called physical layer cryptography.

It is astonishing that wiretap channel encoding [1] proposed by Wyner was already published one year before DH key sharing [6] which is a prototype of public key cryptography. However, these methods require estimating the information leaked against the eavesdropper in designing the encoding, which deteriorates convenience much compared with modern cryptography that guarantees its security by the computational cost. Hence, these encoding methods were not established as mainstream techniques to be used with current networks. However, they are valuable from the viewpoint of ensuring information security in theory, and thus research is underway to apply this physical layer cryptography to certain communication systems. For example, for radio wave wireless communication [7]–[12], there could be secret key agreement that extracts the key from temporal random variation of the received intensity caused by multipath reflection. On the other hand, in the case of quantum key distribution (QKD) [13]–[15] proposed before Maurer proposed secret key agreement, the feasibility of detecting the existence of an eavesdropper and estimating the amount of leaked information is proved mathematically and physically from the error rate, by transmitting a random number bit after being coded to photons in a special quantum state. Therefore, QKD allows establishing of secure keys that will prevent eavesdroppers with high computational ability from accessing communications assuming that devices have no defect leading to information leakage. QKD is the only physical layer cryptography that is realized as is 2017 for which verification experiments for ground optical fiber network have been demonstrated[16]–[20] and which is commercially available [21]. On the other hand, there are severe limitations such that the transmissible distance / key generation rate is 50 km and 1 Mbps, respectively, for optical fiber [22]. Thus, there still remain some technical problems in application.

Now, at the Quantum ICT Advanced Development Center, we are promoting research on physical layer cryptography in classical free space optical communication as a complementary technique to solve the problem of throughput in QKD mentioned above. As free space optical communication is conducted in line-of-sight within a narrow beam extent, an eavesdropper is obliged to wiretap at the edge of the beam. Hence, the upper limit of the amount of information leaked to the eavesdropper can be estimated based on the physical condition, and utilization of the physical layer is therefore potentially feasible. Moreover, realization of confidential communication over a long distance at high speed of around several Gbps from the property of free space optical communication can be expected. Therefore, physical layer cryptography is expected to be applied to satellite communication where high-speed key generation is difficult by present QKD, drones that require safety technology, and various kinds of IoT devices.

On the other hand, as for the security of the physical layer in free space optical communication and the method of estimating the amount of leaked information, definitive discussion has not emerged yet, which is different from the case of QKD whose robust security has been proved mathematically and physically. Actually, on the contrary to sufficient theoretical studies [23]–[28], we do not know of any practical research in which the practical composition of devices and attacks to be supposed are fully discussed.

Thus, considering the present situation, we have been researching the realization of physical layer cryptography for free space optical communication by an experimental approach such as a communication channel estimation experiment where the communication channel and amount of leaked information are estimated based on data obtained from the free space optical communication testbed between the University of Electro-Communications (UEC) and NICT established by NICT in collaboration with UEC.

The purpose of this article is to explain the outline of basic technical items of physical layer cryptography, then to roughly explain the knowledge obtained from experiments we have carried out. First, in Sections **2** and **3**, we explain the principle of the wiretap channel coding and secret key agreement, both of which are representative models of physical layer cryptography. Then, in Section **4**, we explain the channel estimation experiment that NICT carried out.

2 Confidential communication by wiretap channel coding

2.1 Channel coding

The purpose of this section is to explain wiretap channel coding that is the most basic model in physical layer cryptography. We start with explaining the channel coding. In this paper, information is represented by a sequence of 0 and 1 bits, and the amount (length) of information is expressed in terms of bits.

Here, we assume that an error where a certain bit changes to another bit occurs during communication from the sender (Alice) to the receiver (Bob) via wireless or a communication channel. Alice needs to take countermeasure to transmit the correct information to Bob. To this end, Alice adds redundant information to a message to be sent in order that Bob can retrieve the original message using the redundant information. For example, in the case where Alice transmits each bit adding two copies of the bit (0 → 000 or 1 → 111), Bob can correct the error by a majority decision even when one of the three serial bits changed. Thus, the process of adding redundant information is called channel encoding and the bit sequence of a message with redundant information is called a code word. The operation to retrieve a message from the bit sequence that Bob received is called decoding.

Intuitively, as more redundant information is added, the probability of error in decoding ε_n could approach to 0, in turn, the transmission efficiency would decrease. So, it is very important to know the minimum redundant information that realizes error-free communication to design a communication system. Based on such motivation, Shannon showed that the decoding error probability ε_n can be decreased arbitrarily by extending *n* if encoding rate R_B = *k/n* that is a ratio of code word size *n* to message size *k*, is smaller than channel capacity *C* that is defined for each transmission channel. This theory is called channel coding theorem which is the most fundamental problem in information theory.

In order to evaluate channel capacity *C* concretely, here we define some probabilities in a communication system. Alice can select and transmit bit *x* based on independent and identical probability $P_X(x)$. Also, the probability of occurrence of error in the channel can be modeled with conditional probability (transition probability) where Bob can obtain symbol *y* when symbol *x* is input, W_B (*y* | *x*). Here, we assume a stationary and memoryless communication channel. Under such precondition, mutual information *I (X;Y)* is calculated from the following equation, which expresses the amount of transmissible information between Alice and Bob.

$$I(X;Y) = \sum_x \sum_y P_X(x) W_B(y \mid x) \log_2 \frac{W_B(y \mid x)}{\sum_{x'} P_X(x') W_B(y \mid x')} .$$

The input probability $P_X(x)$ can be optimized so that Alice can transmit as much information as possible to Bob. As a result, the channel capacity *C* is derived as follows.

$$C = \max_{P_X(x)} I(X;Y) .$$

2.2 Wiretap channel coding

Unlike the channel coding explained in the previous section, wiretap channel coding concerns the situation in which communication between Alice and Bob using a main channel is wiretapped by Eve using a wiretapper channel as shown in Fig. 1. However, in such a case, the purpose of Alice and Bob is to transmit information without not only decoding error but also leakage to Eve, that is, to communicate in a highly reliable and information theoretically secure way.

Intuitively, security seems to be ensured if Eve uses channel code that fails in error correction. Here, we assume a schematic example where when Alice transmits a message of 3 bits in size, Bob can receive the message without error and Eve receives a correct message or a bit sequence with one-bit error in 1/2 probability for each case. In other words, when Alice transmits a message of 000, Eve would receive one bit sequence from four bit sequences, 000, 100, 010, and 001, in 1/4 probability. In this case, Eve cannot identify the message that Alice sent, but it should be noted that she can narrow down the possibilities. For example, if Eve received a bit sequence of 001, she can guess that Alice sent one from 001, 101, 011, or 000. This means that one bit of the information of the message has been leaked because the number of candidates of the correct message decreased from eight to four. So, it is not considered to be information-theoretically secure anymore.

When Alice and Bob want to communicate in an information theoretically secure way, they want to prevent even such one-bit leakage. The possible sequences generated at Eve when Alice transmits a message are listed in Table 1 for comparison. Then, it is clear that all the sequences possibly generated at Eve cover all the sequences expressed by 3 bits for both 000 and 111. Then, Alice combines two messages that meet such condition and assigns 2-bit message for each pair. This is a secret message that enables information theoretically secure transmission. In the case of sending a certain secret message, one of the 3-bit messages corresponding to the secret message is randomly selected and transmitted. As Bob can receive the

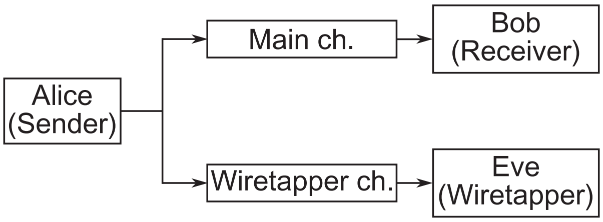


Fig. 1 Schematic view of wiretap channel encoding

Table 1 3 Bit messages and generated bit sequences possible at Eve and 2-bit secret messages

Messages	The possible sequences generated at Eve	2-bit secret messages
000	000, 100, 010, 001	00
111	111, 011, 101, 110	
100	100, 000, 110, 101	10
011	011, 111, 001, 010	
010	010, 110, 000, 011	01
101	101, 001, 111, 100	
001	001, 101, 011, 000	11
110	110, 010, 100, 111	

sequence without error, he can retrieve the secret message by referencing the correspondence shown in Table 1. On the other hand, all 3-bit sequences are possibly generated in the channel to Eve at uniform probability irrespective of the transmitted secret messages, given that 3-bit sequences to be transmitted to Eve are randomly selected.

Therefore, information-theoretical security is guaranteed. The above discussion is the core of the wiretap channel coding. In fact, as errors occur also in Bob's channel, error correction would be needed. In the following, we discuss the performance of the error correction. Here, Alice encodes a secret message of length k to a coding word of length n. The probability of decoding error is expressed as ε_n as in the channel coding theorem. In addition, the amount of leaked information is expressed as δ_n. Although this quantity is defined in various ways ([29]–[31], for example), basically it is estimated by statistical distance between the probability distribution of Eve and perfectly uniform distribution. Wyner showed that when the rate of secret message $R_B = k/n$ is smaller than the hiding capacity,

$$C_S = \max_{P_X(x)}[I(X;Y) - I(X;Z)],$$

both the decoding error probability ε_n and the amount of leaked information δ_n can be arbitrarily reduced by extending n [1]. Here, $I\ (X;Y)$ is the amount of information that Alice and Bob can share by error correction applying the channel coding theorem, and $I\ (X;Z)$ is the amount of information leaked against an eavesdropper. Actually, in the example shown above, the information theoretical securely transmissible bit is 2 bits derived by subtracting the leaked one bit of information from the 3-bit message. Although the conditions $I(X;Y) > I(X;Z)$ should be realized to apply the Wyner theorem mentioned above, Csiszár and Körner [2] generalized the theorem by removing the condition, using information theoretical techniques.

3 Secret key agreement

Wiretap channel coding that realizes confidential communication without private key sharing using noise generated in communication seems to be an ideal cipher technique. However, there is a practical problem that it does not work as intended under a condition that is advantageous for Eve such as where the number of errors generated in the wiretap channel are less than in the main channel. The technique of secret key agreement published in 1993 [4]–[5] enables key establishment even though Eve can wiretap under advantageous conditions for her, by admitting use of an authenticated public channel as shown in Fig. 2. By secret key agreement, Alice and Bob share a key as a result of discussion over a public channel from a correlated random number that they shared in advance. Secret key agreement can be categorized into two types of protocols by the method of sharing the random number. One of the two is a source model where Alice and Bob (and Eve) receive a random number generated from a certain common source. The secret key agreement in radio wireless communication [7]–[12] is categorized into this type. On the other hand, the method where Alice transmits a prepared random number is called the channel model. One approach to achieve high-speed secret key agreement without its rate being influenced by modulation speed of the atmosphere is to use wide bandwidths in free space optical communication or line-of-sight communication. To this end, the latter communication model is suitable. In the following, we roughly explain secret key agreement based on the channel model assuming simple additive noise.

First of all, Alice generates random number x^n of length n and transmits it to Bob and Eve. Bob and Eve receive the output signals $y^n = x^n \oplus e^n$ and $z^n = x^n \oplus d^n$ to which statistically independent noises e^n and d^n generated in the main channel and wiretap channel were added. Here, $\oplus$ denotes exclusive OR for each bit. Next, Alice and Bob correct the discrepancies between the sequences by information reconciliation protocol [32] over the public channel. Here, we especially focus on so-called reverse information reconciliation where Bob transmits error-correction information to Alice and Alice estimates the sequence that Bob received based on the information. Of course, Eve tries to estimate the random number sequence of Bob using error-correction information obtained through public information. However, considering the condition where Eve wiretaps the random number sequence that Alice sent, it is more difficult for Eve to estimate Bob's received random

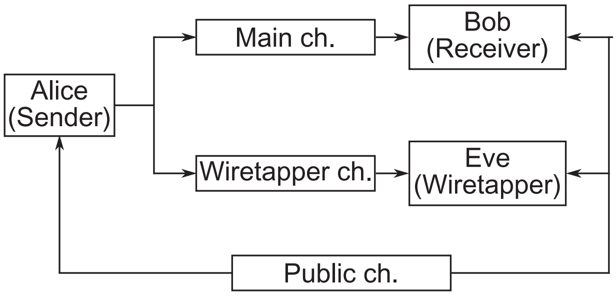


Fig. 2 Schematic view of secret key agreement

number sequence than that from Alice because independent noise was added to the former. Actually, the random number sequences of Alice and Eve expressed by Bob's random number sequence are $x^n = y^n \oplus e^n$ and $z^n = y^n \oplus e^n \oplus d^n$. That is, even if Eve wiretaps under a lower noise condition than that of Bob's, it is possible to make the condition disadvantageous for Eve by reverse information reconciliation. Finally, the random number sequence equivalent to the information leaked against Eve is compressed in privacy amplification [33][34]. This process removes the amount of information leaked to Eve. For this purpose, a trap door function is applied so that input information is hard to estimate from the output.

Here, the sharable key rate by secret key agreement can be derived utilizing the security analysis that Renner conducted in the context of QKD. Renner [35] showed that the sharable key rate using reverse reconciliation with any techniques and privacy amplification based on the Universal 2 hash function [36] could be derived as follows:

$$C_K \geq \max_{P_X(x)}[I(X;Y) - I(Y;Z)] \, .$$

Here, I(X;Y) is the information amount that can be shared in information reconciliation, and I(Y;Z) represents leaked information to be removed. It shows that it is possible to compose a practical secret key agreement protocol using practical error correction code such as LDPC or the Universal 2 hash function.

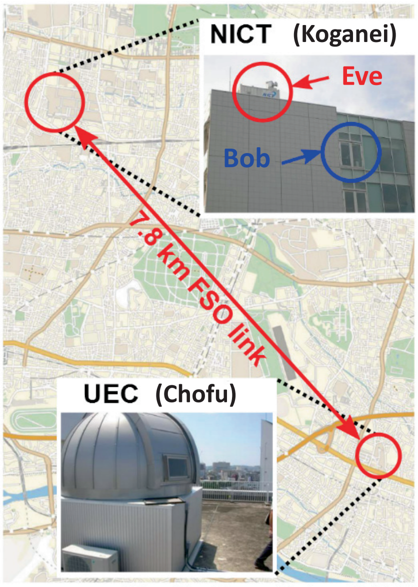
4 Experiment of channel estimation using free space optical communication testbed

As we discussed above, the performance of physical layer cryptography is measured by the secrecy capacity for wiretap channel coding and by (lower limit) of the secret key capacity for secret key agreement. Thus, in order to design appropriate code, Alice and Bob estimate the probability distribution of the channel in advance, then estimate and reconstruct the probability model from the data, and calculate these capacities. However, there exist some difficulties. First of all, the refractive index of the atmosphere temporally changes as temperature varies. This effect is called atmospheric fluctuation and can cause variation of the received intensity on a time scale of several millimeter seconds and shift of beam direction. Hence, performance evaluation considering the effect of atmospheric fluctuation is difficult.

In addition, there is a difficulty in the estimation of the leaked information against Eve.

Therefore, in order to experimentally solve the problem, the Quantum ICT Advanced Development Center established a free space optical communication testbed of 7.8 km in length, connecting the University of Electro-Communications (UEC) and NICT as shown in Fig. 3. In this testbed configuration, Alice is a dome on the top of a building of the UEC, Bob is the receiving system installed on the 6th floor of a building of NICT, and Eve is a terminal set on the rooftop of the same building.

In this article, we report on the experiment implemented on November 17, 2015 [37][38], with the purpose of revealing the relation between the effect of weather conditions and physical layer cryptography, by evaluating the transmission performance of physical layer cryptography under various weather conditions. In this experiment, Alice transmitted a pseudorandom number sequence with a cycle of 2^{15}-1 by on-off keying. The light source was an eye-safe laser of wavelength 1,550 nm and output power 100 mW. As the beam diverging angle of the transmission lens was about 1 mrad, the radius of the beam at NICT became about 8 m. Due to the configuration constraint of the experiment, the center of the beam was adjusted so that Eve could receive the light by approaching the beam center from Bob to Eve by about 1 m. Bob and Eve independently measure the power of light detected by a PIN photodiode detector and avalanche photodiode detector using a telescope of about 100 mm diameter to collect light beams. In addition to the difference in sensitivity of the



© OpenStreetMap contributors, CC-BY-SA

Fig. 3 Schematic view of Tokyo FSO Testbed [37]. ©OpenStreetMap contributors, CC-BY-SA.

detectors, as a window pane was set in the light path to the detector of Bob, this experiment simulated one of the typical scenarios of wiretapping in free space optical communication where Eve wiretaps using a more sensitive detecting system than that of Bob.

Under the experimental conditions mentioned above, Alice transmitted a pseudorandom number of length 2×10^6 in a transmission duration of 200 ms. Then, we derived the intensity distribution of the channel based on the output of photo-detectors of Bob and Eve and calculated mutual information, *I(X ; Y)* and *I(X ; Z)* for every 4 ms, respectively. Here, we assumed that, realistically, the surroundings of Bob were monitored and guarded firmly and another wiretapper who could obtain more information than Eve on the roof could not exist. Under these conditions, we evaluated the transmission performance of the wiretap channel coding, which is the simplest physical layer cryptography. Although the performance of wiretap channel coding is measured by secrecy capacity as described above, we cannot estimate the secrecy capacity because we did not optimize power and the frequency of 0s and 1s in the pseudorandom number sequence in this study. Hence, we evaluate the amount of confidentially transmissible information using the secrecy rate which is a simple difference of the mutual information,

$$R_S = I(X;Y) - I(X;Z)\ .$$

We performed such analysis in five time zones, 14:43, 15:57, 16:33 (sunset time of the day), 17:37, and 18:10. In each time zone, ten transmissions are conducted by intervals of 20 seconds.

The time variations of the secrecy rate calculated from the experimental data obtained at 16:43:20 and 17:37:00 are shown in Fig. 4. Here, we note that Bob's channel was almost error free in this experiment.

The secrecy rate changed dramatically from 10 Mbps (from 24 ms to 28 ms) to 0 bps (from 144 ms to 148 ms) during the 200 ms period at 16:43:20, that was just after sunset, as shown in Fig. 4(a). On the other hand, the time variation of the secrecy rate was small at 17:37:00, that was after sunset, as shown in Fig. 4(b). From the above, it is shown that fatal information leakage occurred due to the effect of intensity modulation or beam wandering caused by atmospheric fluctuation just before and after sunset, however such effects are suppressed during night so that stable confidential transmission would be realized using physical layer cryptography.

In order to examine such atmospheric effects discussed above, we evaluated the probability that secrecy rate R_S is smaller than a certain threshold R_{th},

$$P_{out}\,(R_{th}) = \Pr(R_{th} > R_S)\ .$$

for the data obtained in the above five experimental time zones. This is called secrecy outage probability $P_{out}(R_{th})$, because it can be deemed as a possibility of fault in confidential transmission of designed code, if this threshold is regarded as a target rate determined at design of code. We calculated this $P_{out}(R_{th})$ for the five time zones based on the data taken in the experiment and the results are shown in Fig. 5. It is impossible to decrease the secrecy outage probability to 0 before sunset no matter how low the threshold R_{th} is set. On the other hand, there exists a threshold that

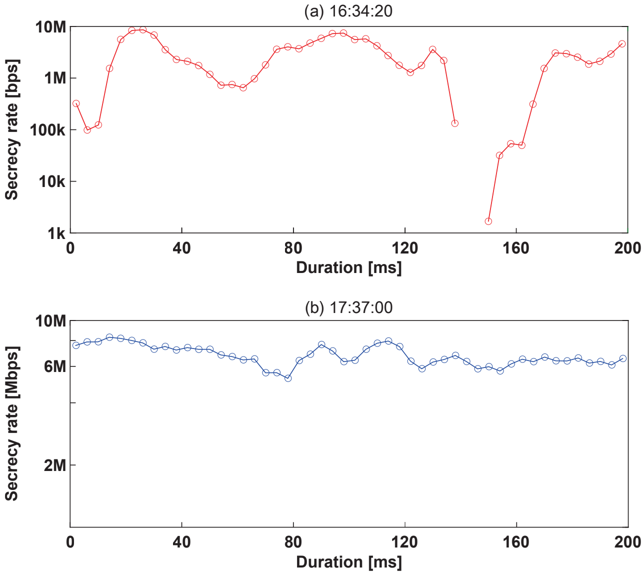


Fig. 4 (a) Secrecy rate calculated from experimental data obtained at (a) 16:34:20 and (b) 17:37:00, on November 17, 2015. Time interval of each measurement is 4 ms and corresponds to pseudorandom number sequences of length 4 × 10^4 [38].

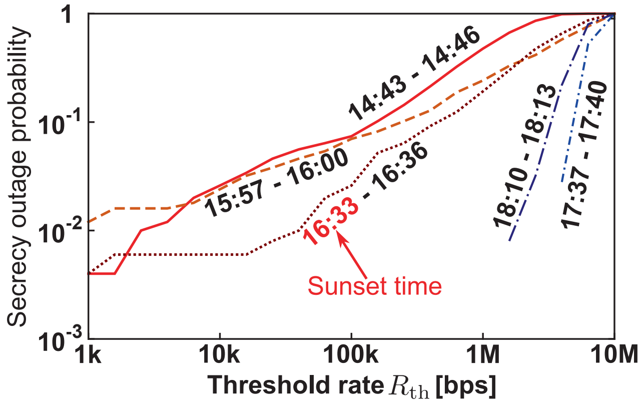


Fig. 5 Secrecy outage probability calculated from the experimental data obtained on 17th November 2015 [38].

realizes a secrecy outrage probability of 0 after sunset when atmospheric fluctuations are stable. This fact agrees with the discussion on time variation of the secrecy rate just before and after sunset shown in Fig. 4.

Such discussion based on experimental data where atmospheric fluctuation affects physical layer cryptography is, as far as we know, unprecedented. We have obtained important knowledge for future studies on physical layer cryptography in free space optical communication and development of protocols.

5 Summary

In this paper, we presented the outline of a technique for physical layer cryptography from the information theoretical aspect and the research on the effect of various atmospheric conditions on the physical layer cipher using experimental data. This study has been undertaken by the Quantum ICT Advanced Development Center to put the technique into practical use. Now, we are engaged in development of a secret key agreement based on the technique of QKD we experienced and in study on a novel key distribution protocol utilizing the properties of optical communication.

The promising application field for the technology is laser communication between satellites and earth terminals in which key generation at practical speed is difficult to realize by QKD. Also, an application field that requires low-cost and high-speed confidential communication such as last-mile communication that connects vehicles or basic networks and users would be an important candidate. Moreover, a multi-layer security protocol and flexible cryptography system that can switch to QKD according to user needs could be supplied by combining modern cryptography operated on a different OSI layer. As mentioned in the introduction, physical layer cryptography in free space optical communication has not been verified and reported yet. So, it is very important to verify such technology for the first time in the world not only for development of communication systems but also for academic research.

However, there are still many problems to be solved. Although the beam used for free space optical communication is narrow, the wireless communication is still easily accessible to eavesdroppers. Therefore, Eve can take various wiretapping measures, such as wiretapping or detection of reflected or scattered light in a position away from the center of the beam or wiretapping from a small instrument. It is not an exaggeration that prevention of wiretapping by Eve by monitoring, etc. is the first priority in our tasks because there is no definitive and effective measure for estimation of the worst value of the amount of leaked information. At present, we are endeavoring to solve this problem involving physical layer cryptography in free space optical communication, by studying methods to estimate the ability of an eavesdropper with certain detection systems, as well as developing the practical protocol mentioned above.

Acknowledgments

This study was commissioned from Impulsing Paradigm Change Through Disruptive Technologies Program (ImPACT) designed by the Council for Science, Technology and Innovation, via JST. We thank Prof. Takao AOKI, Department of Applied Physics, Waseda University, Assoc. Prof. Ryutaro MATSUMOTO, School of Engineering, Tokyo Institute of Technology, and Prof. Yoshihisa TAKAYAMA, Information and Telecommunication Engineering, Tokai University, for their kind cooperation.

References

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

2 I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. on Inform. Theory, vol.24, no.3, pp.339–348, March 1978.

3 C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J., vol.28, no.4, pp.656–715, 1949.

4 U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inform. Theory, vol.39, no.3, pp.733-742, March 1993.

5 R. Ahlswede, and I. Csiszár, "Common randomness in information theory and cryptography: I. Secret sharing," IEEE Trans. Inform. Theory, vol.39, no.4, pp.1121–1132, April 1993.

6 W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol.22, no.6, pp.644–654, Nov. 1976.

7 T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Trans. Antennas Propag, vol.53, no.11, pp.3776–3784, Nov. 2005.

8 S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. 14th Annu. Int. Conf. Mobile Comput. Netw., pp.128–139, 2008.

9 Jana, S., Pnemath, S., N., Clark, M., Kasera, S., K., Patwari, N., and Krishnamurthy, S., V., On the effectiveness of secret key extraction from wireless signal strength in real environments. Proc. 15th Annu. Int. Conf. Mobile Comput. Netw., pp.321–332 (2009).

10 S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," IEEE Trans. Mobile Comput., vol.12, no.5, pp.917–930, May 2013.

11 J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," IEEE Access, vol.4, pp.614–626, Jan. 2016.

12 Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, “Physical layer security in wireless networks: a tutorial,” IEEE Wireless Commun. vol.18, no.2, pp.66–74, April 2011.

13 C. H. Bennett and G. Brassard, “Quantum cryptography: public-key distribution and coin tossing,” in Proc. IEEE ICCSSP, pp.175–179, 1984.

14 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol.74, no.1, pp.145–195, Jan. 2002.

15 V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Düsek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys., vol.81, no.3, pp.1301–1350, July 2009.

16 C. Elliott, et al., “Current status of the DARPA quantum network,” quantum information and computation III Proc. SPIE 5815 pp.138–149, 2005.

17 M. Peev, et al. “The SECOQC quantum key distribution network in Vienna,” New J. Phys., 11, 075001, July 2009.

18 M. Sasaki, et al., “Field test of quantum key distribution in the Tokyo QKD network,” Opt. Express, vol.19, no.11, pp.10387–10409, May 2011.

19 D. Stucki, et al., “Long-term performance of the SwissQuantum quantum key distribution net-work in a field environment,” New J. Phys. vol.13, 123001, Dec. 2011.

20 S. Wang, et al., “Field and long-term demonstration of a wide area quantum key distribution network,” Opt. Express, vol.22, no.18, pp.21739–21756, Sept. 2014.

21 ID Quantique (2001), http://www.idquantique.com/; MagiQ Technologies, Inc. (1999), http://www.magiqtech.com/MagiQ/Home.html; QuintessenceLabs Pty Ltd. (2006), http://www.quintes-sencelabs.com/; QuantumCTekCo., Ltd. (2009), http://www.quantum-info.com.

22 A. R. Dixon, et al., “High speed prototype quantum key distribution system and long term field trial,” Opt. Express, vol.23, no.6, pp.7583–7592, March 2015.

23 N. Wang, X. Song, J. Cheng, and V. C. M. Leung, “Enhancing the security of free-space optical communications with secret sharing and key agreement,” IEEE/OSA J. Opt. Commun. Netw., vol.6, no.12, pp.1072–1081, Dec. 2014.

24 F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, “Physical-layer security in free-space optical communications,” IEEE Photon. J., vol.7, no.2, 7901014, April 2015.

25 A. Mostafa and L. Lampe, “Physical-layer security for MISO visible light communication channels,” IEEE J. Sel. Areas Commun, vol.33, no.9, pp.1806–1818, Sept. 2015.

26 H. Endo, T. S. Han, T. Aoki, and M. Sasaki, “Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels,” IEEE Photon. J., vol.7, no.5, 7903418, Sept. 2015.

27 X. Sun and I. B. Djordjevic, “Physical-layer security in orbital angular momentum multiplexing free-space optical communications,” IEEE Photon. J., vol.8, no.1, 7901110, Feb. 2016.

28 D. Zou and Z. Xu, “Information security risks outside the laser beam in terrestrial free-space optical communication,” IEEE Photon. J., vol.8, no.5, 7804809, Jan. 2016.

29 M. Hayashi, “Exponential decreasing rate of leaked information in universal random privacy amplification,” IEEE Trans. Inf. Theory, vol.57, no.6, pp.3989–4001, June 2011.

30 T. S. Han, H. Endo, and M. Sasaki, “Reliability and secrecy functions of the wiretap channel under cost constraint,” IEEE Trans. Inform. Theory, vol.60, no.11, pp.6819–6843, Nov. 2014.

31 J. Hou and G. Kramer, “Effective secrecy: Reliability, confusion and stealth,” in proc. IEEE ISIT, pp.601–605, June 2014.

32 G. Brassard, and L. Salvail, “Secret key reconciliation by public discussion,” In Proc. EUROCRYPT ‘93, pp.410–423, 1994.

33 C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy amplification by public discussion,” SIAM J. Comput., vol.17, no.2, pp.210–229, 1988.

34 C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inform. Theory, vol.41, no.6, pp.1915–1923, June 1995.

35 R. Renner, “Security of quantum key distribution,” Ph.D. dissertation, Dept. Comput. Sci., ETH Zurich, Zurich, Switzerland, 2005.

36 J. L. Carter and M. N.Wegman, “Universal classes of hash functions,” J. Comp. Syst. Sci., vol.18, pp.143–154, 1979.

37 H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, Y. Takayama, H. Takenaka, R. Shimizu, N. Laurenti, G. Vallone, P. Villoresi, T. Aoki, and M. Sasaki, “Free-space optical channel estimation for physical layer security,” Opt. Express, vol.24, no.8, 259736, April 2016.

38 H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, H. Takenaka, R. Shimizu, T. Aoki, and M. Sasaki, “Physical layer cryptography in free-space optical communications: Performance estimation in real-field experiment and coding method,” IEICE Tech. Report, vol.IEICE-116, no.183, pp.7–12, Aug. 2016.

Hiroyuki ENDO, Ph.D

Researcher, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Physical layer cryptography, Free space optical communication

Mikio FUJIWARA, Ph.D

Research Manager, Qunatum ICT Advanced Development Center, Advanced ICT Reseach Institute
Quantum key distribution, Photon detection techology, Cryogenic electronics

Mitsuo KITAMURA

Technical researcher, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Optical communication

Orie TSUZUKI

Technical researcher, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Free space optical communication

Toshiyuki ITOH, Ph.D

Researcher, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Physical layer cryptography, Free space optical communication

Ryosuke SHIMIZU, Ph.D

Associate professor, The University of Electro-Communications
Quantum optics

Morio TOYOSHIMA, Ph.D

Director, Space Communications Laboratory
Satellite communications, Optical communcations, Atmospheric Turbulence, Laser beam propagation, Quantum cryptography

Hideki TAKENAKA, Ph.D

Researcher, Space Communications Laboratory
Free space optical communications, Error orrectign code

Masahiro TAKEOKA, Ph.D

Director, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Quantum optics, Quantum information theory

Masahide SASAKI, Ph.D

Distinguished Researcher, Advanced ICT Research Institute
Quantum communication, Quantum cryptography