Secret Key Distribution Protocol for Practical Optical Channels Using a Preshared Key and Phase Fluctuations

OPEN ACCESS
Japanese Journal of Applied Physics **49** (2010) 074401 **REGULAR PAPER**

Secret Key Distribution Protocol for Practical Optical Channels Using a Preshared Key and Phase Fluctuations

Tatsuya Tomaru*

Advanced Research Laboratory, Hitachi, Ltd., Hatoyama, Saitama 350-0395, Japan

Received March 29, 2010; accepted April 12, 2010; published online July 20, 2010

A practical secret-key-distribution protocol using general phase fluctuations is described. A preshared key is assumed and is used only inside a transmitter and a receiver. The probabilistic property of signal-light fluctuations works with the preshared key to produce a difference in bit-error rate between a receiver and an eavesdropper. Using the difference, new secret keys are generated information theoretically although a preshared key is used. The probabilistic property of signal-light fluctuations is essential in this protocol, and classical fluctuations as well as quantum fluctuations are applicable. Because signal states are classical, the system becomes tolerant of loss and amplification.

DOI: 10.1143/JJAP.49.074401

1. Introduction

Quantum cryptography, founded by Bennett and Brassard, has been widely studied and has given rise to interest beyond a specialized research area because it provides extremely high security.[1,2] In addition to the original idea of using a single photon, methods using an Einstein–Podolsky–Rosen state[3,4] or continuous quantum variables[5,6] have been proposed and demonstrated. These methods guarantee secret key distribution between two authenticated participants (Alice and Bob) based on so-called no-cloning theory[7,8] or the uncertainty principle of quantum mechanics. Although quantum cryptography is well established theoretically, its practical use is limited because a quantum state is not tolerant of loss and amplification. Although the idea of a quantum repeater was proposed to circumvent this limitation, its technology is not very easily applied.[9]

Quantum cryptography has established a valuable position in the sense that it gives unconditional security, and conventional cryptography gives computational security. However, do we necessarily need unconditional security? Because quantum cryptography is limited in practical use, we need to balance attainable security with practical convenience. In conventional cryptography, a seed key is normally used, and an eavesdropper, hereafter referred to as "Eve", cannot decrypt it very easily thanks to its computational complexity. In this case, the most potentially serious problem is that a decryption algorithm may be found at any time. If cryptography did not allow Eve to use a more efficient decryption method than a brute force attack against the seed key, then the cryptography would have the highest security among seed-key systems, and the security level of the cryptography would definitely be evaluated quantitatively. For example, we assume a seed key of 128 bits. When the one-process time for checking a key is 1 ns, the brute force attack requires on average 10^{22} years. If we could establish such a cryptographic system that operates in realistic circumstances, it would create a method different from quantum and conventional cryptography. This report describes a method for this aim using the probabilistic property of general phase fluctuations.

Secure communications are possible information theoretically when the mutual information $I(X;Y)$ between Alice and Bob is greater than the mutual information $I(X;Z)$ between Alice and Eve.[10–13] Very simply, this is achieved when Bob's bit error rate (BER) is less than Eve's. References 10–13 assume that Eve's channel is independent of Bob's and that they have independent fluctuations. Based on this assumption, information-theoretic security is obtained due to the fluctuations on Eve's side. These references principally assume free-space communications. Instead, we consider fiber communications in this report, where only a channel should be assumed, and we do not adopt the assumption in refs. 10–13. In this case, how can we produce this difference between Bob and Eve? Quantum–mechanical properties can achieve it, and quantum cryptography enables just that. However, we want to achieve it using general phase fluctuations, which are classical fluctuations as well as quantum fluctuations, from a practical point of view. One candidate to support this idea is using a preshared key. The importance of the preshared key has already been mentioned in ordinary quantum cryptography as a tool for authentication.[14] We aim to use the preshared key more actively. In this sense, Hwang *et al.* proposed determining a basis by using a preshared key.[15] However, when the preshared key is repeatedly used, a complete single-photon state is required as a carrier. Yuen proposed using a pseudo-random number generator together to determine a basis.[16] In this case, the effectiveness of the quantum fluctuations is required. In these methods, the preshared key itself directly determines a basis; therefore, the quantum nature is required to preserve the advantage of Bob. Instead, this paper describes a new protocol where a preshared key is used only inside a transmitter and a receiver, and a transmission basis is determined randomly. The receiver extracts meaningful signals by means of the preshared key. Here, signal-light fluctuations are essential because if this protocol is deterministically processed, the difference between $I(X;Y)$ and $I(X;Z)$ is simply the information of the preshared key, and a new key is never generated. We can break out of this dilemma to some extent by using the probabilistic property of signal-light fluctuations. When the preshared key is used only to make Bob more advantageous in BER than Eve, information theory, where the difference between $I(X;Y)$ and $I(X;Z)$ produces a secret capacity, is applicable. The important thing is the probabilistic property originating in signal-light fluctuations; therefore, the quantum nature is not necessarily required if the probabilistic property is sufficient.

*E-mail address: tatsuya.tomaru.yq@hitachi.com

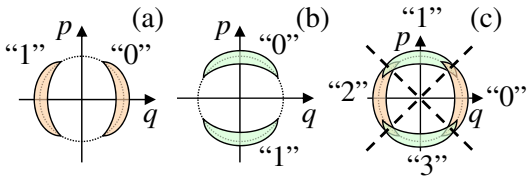

Fig. 1. (Color online) Binary signals in phase space. A crescent indicates fluctuations in a signal state. (a) Binary signal states on q-axis basis. (b) Binary signal states on p-axis basis. (c) Eve, who does not know signal bases, sees four-valued signals.

Although a preshared key is required, the key generation itself is processed information theoretically; therefore, the security level of this method is beyond that of computational complexity, but is less than that of information-theoretic security because a preshared key is used. In other words, this method provides a new category of intermediate security between quantum and conventional cryptography.

2. Protocol

We assume binary phase coding using two bases. Phase coding involves not only phase-shift keying but also differential-phase-shift keying. Alice and Bob share a series of bases according to a preshared key. The schematic difference in the situation between Bob and Eve is shown in Fig. 1. Bob, who knows a basis, q- (a) or p-axis (b), detects a binary signal with a low BER. However, Eve, who does not know the basis, sees a four-valued signal, and her BER is relatively high because of overlapped fluctuations. The difference in the BER produces a secret capacity.

Eve is assumed to be able to eavesdrop on all signals that are communicated between Alice and Bob in most advantageous conditions. This means that Eve can eavesdrop on signals just near the transmitter. We consider this Eve's simple eavesdropping only in the following because we treat fluctuations classically. In quantum cryptography, an intercept-resend attack is considered as a basic attack. Because this type of attack changes a quantum signal state, this type of analysis is important in quantum cryptography. However, Eve can eavesdrop on all classical signals without disturbing them. If Eve intercepted and resent classical signals completely as information in phase space, it would be the same as simple eavesdropping. If Eve intercepted and resent classical signals with a four-value decision, Bob's BER would increase because Bob can potentially make a binary decision for the original signals. The increase in BER allows Alice and Bob to guess the existence of Eve by checking Bob's BER; therefore, simple eavesdropping is the most powerful strategy for classical signals. Collective attacks and coherent attacks, which are important attacks in quantum cryptography,[2,17] also cannot be beyond the simple eavesdropping strategy for classical signals.

The overall rough picture of the secret key generation process is as follows:

1. Alice and Bob share a series of bases determined by a preshared key.
2. Alice sends binary random numbers with random binary bases.
3. Bob detects four-valued signals, judges random bases, and checks them with shared bases.

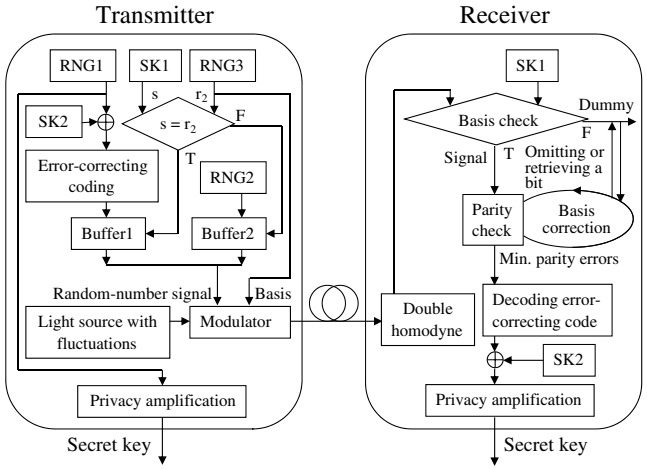

Fig. 2. Concrete configuration and chart diagram for achieving the protocol. RNG is a random-number generator. SK is a seed key. "T" indicates true logic, and "F" indicates false logic.

4. When a random basis coincides with the shared basis, the random-number datum is treated as a signal. When the random basis does not coincide with the shared basis, the random-number datum is treated as a dummy signal.
5. Alice and Bob distill a secret key from raw random-number signals through privacy amplification.[18,19]

This rough picture does not consider bit errors, so it is incomplete. The important point is that Eve sees the random numbers with random bases. However, Bob can extract random-number signals using shared bases held inside a receiver.

A complete protocol is schematically shown in Fig. 2, and an example of random-number signals is shown in Fig. 3. A transmitter includes three random-number generators (RNGs), and the transmitter and receiver preshare two seed keys (SKs). The output of "RNG1" is used as a raw random-number signal, which is encrypted with "SK2", is error-correcting-coded, and is held at "buffer 1". The output of "RNG2" is used as a dummy signal and is held at "buffer 2". "RNG3" determines the transmission basis. When the output of RNG3 coincides with the shared basis determined by SK1, a random number held at buffer 1 is transmitted. When the output of RNG3 does not coincide with the shared basis determined by SK1, a random number held at buffer 2 is transmitted. Although SK1 is essential, SK2 is not necessarily essential. The sum of SK1 and SK2 determines the size of the SKs.

At the receiver, two quadratures, i.e., the q-axis component, I_q, and the p-axis component, I_p, are measured with double homodyne detectors. A binary decision on each basis is directly done through the sign of I_q and I_p. A four-value decision is done through $\arctan(I_p/I_q)$. Bob first judges a signal basis based on the result of the four-value decision. When the judged basis coincides with the shared basis determined by SK1, then Bob treats the datum as a signal. When the judged basis does not coincide with the shared basis determined by SK1, then Bob treats the datum as a dummy. However, many judgment errors occur because Bob determines a basis from a four-valued signal. This basis-

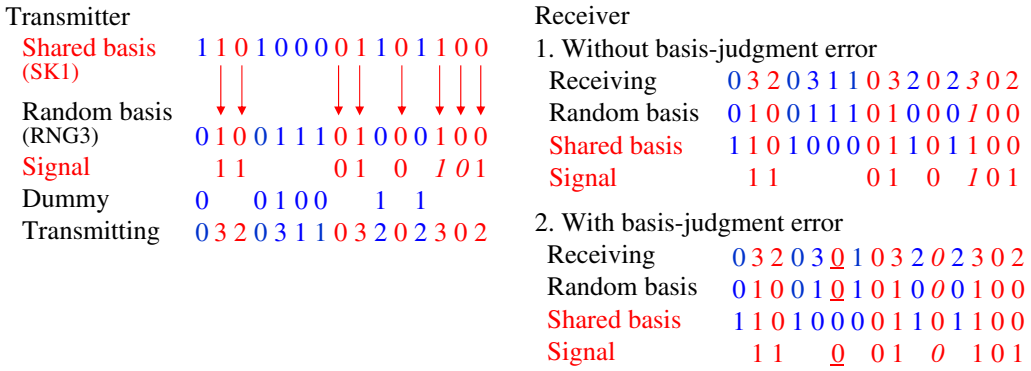

Fig. 3. (Color online) Example of random-number signals operated based on this protocol. Transmitter: A signal or dummy signal is transmitted using a random basis. Basis "0" indicates a *q*-axis basis, and basis "1" indicates a *p*-axis basis. Signals are transmitted as four-valued signals because of binary signals on two bases, which are defined in Fig. 1(c). An arrow shows the coincidence of a shared basis with a random basis. The signal is transmitted only in this case. A parity bit, which is the exclusive OR of the preceding five bits and is written in italics, is inserted in the sixth bit in the series of signals as a simple example. The encryption with "SK2" is skipped. Receiver: When the basis judged from a received four-valued signal coincides with the shared basis, the bit is treated as a signal. If no basis-judgment error occurs, random-number signals are recovered. If a basis-judgment error occurs, the recovered random-number signals become completely wrong after the misjudged bit. The sixth bit, which is underlined, is misjudged as an example.

judgment error means that a dummy bit is treated as a signal or that a correct signal bit is omitted as a dummy. For example, in the basis-judgment error case in Fig. 3, the sixth bit, which is underlined, is an incorrect extra bit. In this case, the data bits following the basis-judgment-error bit become errors with a probability of 0.5 because of the extra bit. Then, because the bit errors become successive, Bob can identify the region including the basis-judgment-error bit, using a parity check function incorporated in an error-correcting code. As a simple example, a parity of successive five bits is inserted in the sixth bit in Fig. 3, which is written in italics. When a basis-judgment error occurs, the parity bit shifts because of the extra bit, and the following parity bits have a probability of becoming wrong of 0.5. These successive errors teach Bob the region including the basis-judgment error. Although Fig. 3 shows a quite simple error-correcting code to demonstrate how a basis-judgment error causes an effect on parity bits, powerful forward error-correcting codes should be incorporated in an actual system.[20)]

Bob now knows the existence of a basis-judgment error and the region that includes the error. Although an error-correcting code can correct bit errors on definite bases, it cannot correct a basis-judgment error. Bob must find the exact position of the basis-judgment error exhaustively bit-by-bit. Bob omits a bit in the region and checks the parity, or he retrieves a bit that was originally omitted as a dummy and checks the parity. Repeating these omission and retrieval processes for all the bits in the region, Bob finds a raw random-number bit stream that gives a low BER. Through this retrieval process, the basis becomes definite and the signal judgment is reduced to being binary, not four valued. This fact is essential because the principle of obtaining the secret capacity is that Bob makes a binary decision from a binary signal and that Eve makes a binary decision from a four-valued signal. In the basis-retrieval process, Bob does not consume secret capacity. He uses only parity bits that are necessarily incorporated as a basic tool. The retrieval process is done exhaustively.

Through the basis-retrieval process, Bob obtains signals that are judged binary. He decodes the binary signals to error-corrected signals based on the original function of the error-correcting code. Bob furthermore decodes them with SK2. He now obtains raw random-number signals that are the same as the output of RNG1. The secret capacity is estimated from the BERs of Bob and Eve according to the standard information theory, described in the next section. A new secret key is obtained through privacy amplification in the transmitter and the receiver to the full extent of the secret capacity. Finally, secret communications are achieved with one-time-pad cryptography using the new secret key.

This protocol has two important points. The first is that a basis is randomly determined and that the preshared key is held inside the transmitter and the receiver. The transmitted random signals with random bases never reflect the preshared key in the key-generation process. Eve can never obtain meaningful information in this stage. This advantage is achieved in exchange of discarding half of the transmitted data. The second is that the basis becomes definite through the exhaustive basis-retrieval process using parity checking. This process makes Bob more advantageous in BER than Eve. In other words, the probabilistic property of signal-light fluctuations works to the advantage of Bob and not Eve due to the definiteness of the basis. This probabilistic property and privacy amplification generate a new key. If the privacy amplification is sufficient, Eve's information becomes asymptotically zero. Alice and Bob cryptographically communicate with each other using the generated new key through a public channel. In this stage, the preshared key-related information is first opened. If Eve performs, for example, the chosen plane-text attack in this stage, she obtains the information of the generated new key. However, if the privacy amplification is sufficient, Eve cannot correlate the generated key and the information on the random signals that Eve might have obtained in the key-generation process. Eventually, Eve cannot obtain the information on the preshared key.

3. Secret Capacity

This protocol treats four-valued signals in the transmission stage. Although signal states are four valued, the signals themselves are binary. In this report, we call them four-valued-state signals. When the channel capacity for the four-valued-state signals is C_f, the mutual information between Alice and Eve is given by

$$I(X;Z) \leq C_f. \tag{1}$$

Because Alice and Bob know the preshared key K, the mutual information between them becomes conditional, i.e., $I(X;Y|K)$. Bob transforms the four-valued-state signals into real binary signals through the basis-retrieval process using the preshared key and parity checking in the receiver. Because Bob makes binary decisions as a result, the mutual information $I(X;Y|K)$ can be described by channel capacity C_b for the binary signals. When the amount of information δC is expended in the basis-retrieval process, the mutual information $I(X;Y|K)$ is given by

$$I(X;Y|K) \leq C_b - \delta C. \tag{2}$$

The secret capacity is given by $C_s = \max[I(X;Y|K) - I(X;Z)]$, and when a binary symmetric channel is assumed, the secret capacity is given by

$$C_s = h(p_f) - h(p_b) - \delta C, \tag{3}$$

where $h(\cdot)$ is the binary entropy function, and p_f and p_b are BERs for four-valued-state and binary signals.[11,12] A basis-retrieval process using parity checking, described in §2, is done with parity check symbols inherently involved in an error-correcting code. Therefore, the basis-retrieval process does not use special information except for the ordinary parity check symbols for bit correction. For this reason, δC should be zero for an appropriately designed error-correcting code.

As described in eq. (2), secret capacity C_s of eq. (3) is generated using the preshared key K. If the preshared key directly determined bases, the preshared key could only be used once. However, this protocol determines the bases randomly, and the preshared key is used only inside a transmitter and receiver. It is only used to make the mutual information conditional and is not the origin of secret capacity C_s. The probabilistic property of signal-light fluctuations generates secret capacity C_s. This fact allows for the repeated use of the preshared key.

The BERs for binary and four-valued-state signals are estimated as follows: We assume a signal "0" on a q-axis basis. Phase fluctuations are assumed to be sufficiently larger than the quantum fluctuation, so we can treat the measurement classically. When the probability phase distribution of signal "0" is given by $P(\theta)$, the BER for binary signals p_b is given by

$$p_b = \int_{-\pi}^{-\pi/2} P(\theta)\, d\theta + \int_{\pi/2}^{\pi} P(\theta)\, d\theta. \tag{4}$$

Eve must make a binary decision from a four-valued-state signal. When signals "0" and "1" on each axis are assumed, as shown in Figs. 1(a) and 1(b), Eve judges a four-valued "0" or "1" signal in Fig. 1(c) as "0" and a four-valued "2" or "3" signal as "1". This judgment corresponds to a method

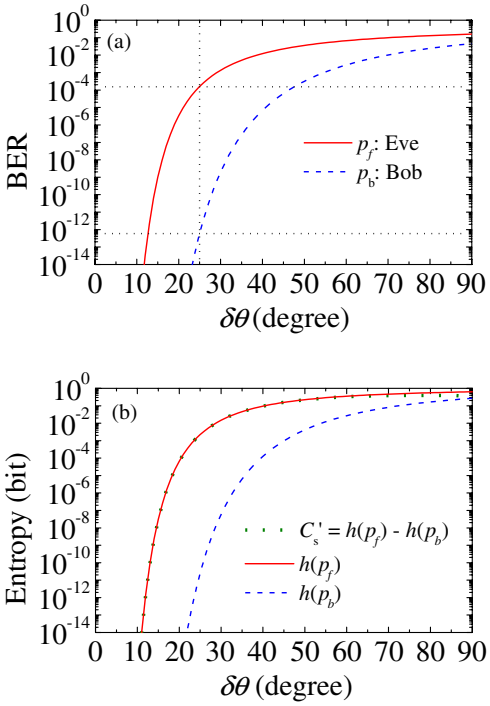

Fig. 4. (Color online) (a) Plots of BER with respect to fluctuations $\delta\theta$, assuming Gaussian fluctuations. p_f and p_b correspond to BERs of Eve and Bob. (b) BER is translated to equivocation. The difference between two equivocations gives C_s', which is the sum of secret capacity C_s and δC.

using the so-called "Breidbart basis", mentioned in ref. 21. In this case, the BER for four-valued-state signals p_f is given by

$$p_f = \int_{-\pi}^{-\pi/4} P(\theta)\, d\theta + \int_{3\pi/4}^{\pi} P(\theta)\, d\theta. \tag{5}$$

When probability distribution is given by

$$P(\theta) = \sqrt{\frac{2}{\pi}}\frac{1}{\delta\theta}\exp\left[-2\left(\frac{\theta}{\delta\theta}\right)^2\right], \tag{6}$$

the BER is concretely estimated as a function of fluctuation $\delta\theta$. Figure 4(a) plots p_b and p_f with respect to $\delta\theta$. For example, when we set 25° for $\delta\theta$, we get $p_b = 6.0 \times 10^{-13}$ and $p_f = 1.6 \times 10^{-4}$, leading to a factor of 10^8 between Bob and Eve. The plot of BERs can be translated to the entropy of information, and these are shown in Fig. 4(b). Quantity C_s', defined by $C_s' = h(p_f) - h(p_b) = C_s + \delta C$, gives an offset secret capacity but is nearly the secret capacity because δC should be zero. The plot of C_s' almost overlaps with the plot of $h(p_f)$, and it hardly depends on $h(p_b)$, as shown in Fig. 4(b). In this estimation, fluctuations are intentionally introduced once to control BER. We must consider extra noise added in a real channel, where Eve should be assumed to be able to detect signals without the extra noise just near the transmitter. In this case, $h(p_f)$, which corresponds to the equivocation of Eve, is not changed, but $h(p_b)$, which corresponds to the equivocation of Bob, is increased. However, if the extra noise is no larger than the intentional fluctuations, secret capacity C_s is not affected by the extra noise because C_s' is almost solely determined by $h(p_f)$. The extra noise is concretely estimated in §5.

The secret capacity monotonically increases as fluctuation $\delta\theta$ increases, and it saturates at $\delta\theta = 60^\circ$. When we consider only the secret capacity, the optimum fluctuations might be $\delta\theta = 60^\circ$. However, hard basis-retrieval processing is required in a receiver in this case. In addition, an appropriate BER exists, depending on an applied error-correcting code. Practical optimum fluctuations will be determined by using the tradeoff between these factors.

4. Discussion

We discuss the meaning of fluctuations. When we treat fluctuations classically, even if a signal state is probabilistically distributed in phase space, the state itself is deterministic according to classical physics. This characterizes the difference between classical and quantum fluctuations because quantum fluctuation remains uncertain until the corresponding observable is measured. However, this protocol uses only the notion that signal states are probabilistically distributed in phase space, and it does not matter when a signal point in phase space becomes definite. The important thing is that errors are intentionally introduced, and they make Bob more advantageous than Eve. Therefore, classical fluctuations are applicable to this protocol. An analogy is found in quantum cryptography, too, where intentional errors increase the performance of quantum cryptography.[17,22)]

As repeatedly mentioned, the probabilistic property of phase fluctuations is essential in this protocol because the difference in BER between Bob and Eve produces the secret capacity. Although Bob judges a basis with certainty through the basis-retrieval process, the signal is still a point in phase space according to the phase fluctuations. Bob sees the point as a binary signal, and Eve sees it as a four-valued-state signal. This is the origin of the secret capacity. Another essential point of this protocol is that the preshared key is used only inside a transmitter and receiver in a new-key generation process. The preshared key is never reflected in transmission signals. However, after privacy amplification, the new secret key is used in cryptographic public communications. If the privacy amplification is not enough, some secret information leaks statistically. Therefore, sufficient privacy amplification is important, and the privacy amplification should be done with as long of a bit length as possible to reduce statistical fluctuations. The problem of statistical fluctuations is common in probabilistic phenomena, including ordinary quantum cryptography. The discussed security is assuredly asymptotic behavior.

This protocol generates new keys information theoretically using fluctuations under the condition of using a preshared key. Although a preshared key is used, the key-generation process itself is information theoretic, and the conditional secret capacity of eq. (3) is obtained. The security should be beyond that of computational complexity due to the probabilistic property of the fluctuations, because computational complexity is a security level, where Bob and Eve are assumed to have completely the same information except for a seed key and no probabilistic properties are included. From this point of view, this protocol belongs to a new category. We must establish the information theory on the new category to describe it thoroughly. That is beyond the scope of this report and is a future subject. According to the concrete consideration in this report, this protocol requires making a new category.

Because the new protocol assumes a preshared key, it might be categorized as "a key growing protocol".[14)] However, because the new key generation is processed information theoretically under the condition of using a preshared key, we call it "a key generation protocol" in this report.

Ideal phase fluctuations are antisqueezing.[23,24)] We may more easily use fluctuations of a laser diode (LD) operated near its threshold, where phase fluctuations are large. Alternatively, we have a selection where fluctuations are superimposed at a phase modulator on an ordinary LD output. The concrete protocol in this report is one achievement, which may be modified through a practical system design.

5. Applicability to Long-Haul Transmission

Although Eve is not affected by the extra noise added in a real channel due to the assumption, Bob is affected. We estimate an example of the extra noise and discuss its effect on the secret capacity. In this report, classical states are assumed, and they can be amplified. Based on this fact, we consider long-haul transmission because it is a good example of showing the practicality of this protocol, and the extra noise can be estimated. The principal limiting factor in long-haul transmission is amplified spontaneous emission (ASE). The ASE increases phase noise directly, and the amplitude noise of the ASE is transformed to phase noise through the Kerr effect of optical fibers.[25)] We roughly estimate two kinds of phase noise. The dispersion of optical fibers is assumed to be properly managed.

We assume an amplifier of gain g. When input signal light is amplified, fluctuations are equally amplified, and ASE noise is added. When the two quadrature fluctuations input are δa_1 and δa_2 and when the vacuum fluctuation is δa_0, the amplified fluctuations are given based on the input-output relation of an amplifier[26,27)] by

$$\delta a_i'^2 = g\delta a_i^2 + \beta(g-1)\delta a_0^2, \quad i = 1 \text{ or } 2, \tag{7}$$

assuming a Gaussian distribution. Here, we added the excess noise factor β, which is the population inversion factor.[25,28,29)] The noise figure NF, which is the ratio of the input signal-to-noise ratio to the output signal-to-noise ratio, of an erbium-doped fiber amplifier (EDFA) is given by $NF = 2\beta$ when the input average photon number $\bar{n}$ per signal and the gain g are sufficiently larger than 1.[28,29)] A phase-fluctuated signal state is crescent-shape distributed in phase space, as shown in Fig. 1. To estimate the phase fluctuations roughly, we approximate the phase fluctuations using the phase quadrature fluctuations. In this case, the input phase fluctuations are given by $\delta a_2/\sqrt{\bar{n}}$. An amplifier increases signals and fluctuations equally and adds ASE noise. Thus, the phase fluctuations become

$$\delta\theta' = \frac{\sqrt{g\delta a_2^2 + \beta(g-1)\delta a_0^2}}{\sqrt{g\bar{n}}}. \tag{8}$$

We assume that a transmission system consists of N spans of fiber length L, i.e., the total fiber length L_{total} is NL, and that transponder amplifiers have the same gain. A signal with an average photon number of $\bar{n}_0$ is output from a

transmitter and is attenuated according to the relation $\bar{n} = \bar{n}_0 e^{-\alpha x}$ in the fiber transmission. We assume that the output signal state has significantly larger fluctuations than vacuum fluctuation, and we assume that the vacuum fluctuation superimposed through the loss process of fiber transmission is negligible.[27] In this case, the phase quadrature fluctuations $\delta a_2^{(0)}$ output from the transmitter are attenuated according to $\delta a_2 = \delta a_2^{(0)} e^{-\alpha x/2}$, similar to the signal, and the original phase fluctuations $\delta a_2^{(0)}/\sqrt{\bar{n}_0}$ are conserved in the loss process. A transponder amplifier increases the attenuated signal intensity $\bar{n}_0 e^{-\alpha L}$ to the original intensity $\bar{n}_0$, and the relation $g = e^{\alpha L}$ is satisfied. The transponder amplifier also increases the attenuated signal fluctuations $\delta a_2^{(0)} e^{-\alpha L/2}$ and adds ASE with gain g according to eq. (7). Thus, the phase fluctuations is expanded to $\sqrt{\delta a_2^{(0)2} + \beta(g-1)\delta a_0^2}/\sqrt{\bar{n}_0}$. The loss and amplification processes are repeated N times, and the total phase noise becomes

$$\delta\theta_{\mathrm{N}} = \frac{\sqrt{\delta a_2^{(0)2} + N\beta(g-1)\delta a_0^2}}{\sqrt{\bar{n}_0}}. \tag{9}$$

This is the direct ASE noise effect for phase fluctuations.

Next, we estimate phase fluctuations transformed from the amplitude fluctuations. We define n_2 as the nonlinear refractive index of an optical fiber, A_{eff} as the effective mode field area of the optical fiber, λ_0 as the free-space wavelength, and P_0 as the power of signal light. The nonlinear phase shift per unit length caused by the Kerr effect is $(2\pi n_2/\lambda_0 A_{\mathrm{eff}})P_0 \equiv k_2 P_0$. The power P_0 is given by $hc\bar{n}/\lambda_0 T$ using the duration T of a signal state, where h is the Plank constant and c is the speed of light. The power fluctuation δP is $2hc\sqrt{\bar{n}}\delta a_1/\lambda_0 T$. The phase fluctuations per unit length caused by the Kerr effect are $k_2\delta P$. Again, we assume that the vacuum fluctuation superimposed through the loss process of fiber transmission is negligible, then the amplitude quadrature fluctuations $\delta a_1^{(0)}$ output from a transmitter are attenuated according to the relation $\delta a_1 = \delta a_1^{(0)} e^{-\alpha x/2}$. The phase fluctuations caused by the Kerr effect in the first span are given by

$$\delta\varphi^{(1)} = \int_0^L k_2 \delta P\, dx = k_2 \frac{2hc\sqrt{\bar{n}_0}}{\lambda_0 T} \frac{1 - e^{-\alpha L}}{\alpha} \delta a_1^{(0)} \equiv K\delta a_1^{(0)}. \tag{10}$$

The amplitude fluctuations output from the mth transponder amplifier are given by

$$\delta a_1^{(m)} = \sqrt{\delta a_1^{(0)2} + m\beta(g-1)\delta a_0^2}. \tag{11}$$

The phase fluctuations caused in the mth span are $\delta\varphi^{(m)} = K\delta a_1^{(m-1)}$. The total phase fluctuations of N spans are given by

$$\delta\varphi_{\mathrm{total}} = \sum_{m=1}^{N} \delta\varphi^{(m)}. \tag{12}$$

These are the phase fluctuations transformed from the amplitude fluctuations through the Kerr effect.

We concretely evaluate two kinds of phase fluctuations using eqs. (9) and (12). We assume a total fiber length L_{total} of 10,000 km, one span of fiber length L is 80 km, i.e., the number N of amplifiers is 125, the NF of an amplifier is 5 dB ($\beta = 1.58$), the output intensity from a transmitter is -4 dBm, the transmission rate is 10 GHz, the duration T is 50 ps, and the fiber loss is 0.2 dB/km, i.e., gain g is 40. For example, when the original phase fluctuations at the transmitter $\delta\theta_0$ are 25°, the fluctuations are expanded to $\delta\theta_{\mathrm{N}} = 26.6°$ according to eq. (9), considering $\delta a_0 = 1$ that is consistent with eq. (6). When n_2 and A_{eff} are 2.6×10^{-20} m^2/W[30] and 85 μm^2, respectively, then k_2 is 1.2 rad/W/km, and K is 7.3×10^{-5} rad. We assume that the amplitude fluctuations at the transmitter are those of a coherent state amplified with the gain g that is equal to that of a transponder amplifier. In this case, the total phase fluctuations $\delta\varphi_{\mathrm{total}}$ are 30.9° according to eq. (12). Because $\delta\theta_{\mathrm{N}}$ in eq. (9) is the phase fluctuations themselves and $\delta\varphi_{\mathrm{total}}$ in eq. (12) is the phase fluctuations transformed from amplitude fluctuations, $\delta\theta_{\mathrm{N}}$ and $\delta\varphi_{\mathrm{total}}$ are fluctuations of different freedoms. Thus, the total phase fluctuations of the two are given by $(\delta\theta_{\mathrm{N}}{}^2 + \delta\varphi_{\mathrm{total}}{}^2)^{1/2}$, i.e., 40.8°.

When phase fluctuations increase from 25 to 41°, Bob's BER increases from 6.0×10^{-13} to 1.1×10^{-5}, according to Fig. 4(a). However, because the increased BER is still lower than Eve's BER of 1.6×10^{-4} at $\delta\theta = 25°$, as shown in Fig. 4(b), the secret capacity is obtained even if phase fluctuations increase from 25 to 41°. This result indicates that this protocol using phase fluctuations is tolerant of extra noise corresponding to a 10,000-km transmission. We showed only a concrete example, but the tolerance against extra noise is generally understandable in Fig. 4(b).

6. Applicability of Error-Correcting Codes

This protocol uses an error-correcting code as an important element. The secret capacity of eq. (3) is the so-called Shannon limit except for term δC. We must use an appropriate error-correcting code to obtain the secret capacity. Recent progress with error-correcting codes has been remarkable, and the performance of error correction approaches the Shannon limit, e.g., low-density parity-check (LDPC) codes.[31,32] Figure 5 shows schematic performance curves of error-correcting codes at a code rate. The BER after an error-correcting process depends on the raw BER. We assume using a code that has near Shannon-limit performance. An LDPC code is representative of it. Because existing error-correcting codes do not assume performing the basis-retrieval process, the amount of information δC is zero for the existing error-correcting codes. BER p_{b}, which corresponds to that for Bob, must be less than the threshold

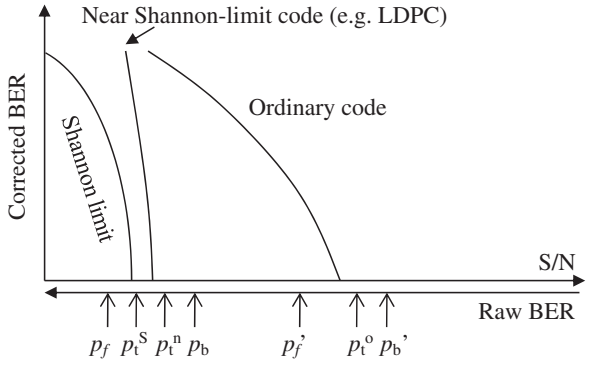

Fig. 5. Schematic performance curves of error-correcting codes at a code rate. When the raw BER is less than the threshold bit-error rate, i.e., p_t^S, p_t^n, or p_t^o, then the corrected BER asymptotically approaches zero.

BER p_t^n of the near Shannon-limit code to make Bob's error correction, where p_b is determined by including extra noise in a transmission channel. BER p_f, which corresponds to that for Eve, must be more than the threshold BER p_t^S for the Shannon limit to obtain secret capacity information theoretically. When these two conditions are satisfied, the secret capacity for this protocol is obtained. Because BERs p_b and p_f differ by multiple digits, as shown in Fig. 4(a), these two conditions are easily satisfied if the used error-correcting code has a near Shannon limit performance.

In estimating the secret capacity under the condition of using an error-correcting code, we should assume that Eve obtains the information of the Shannon limit determined by BER p_f because it gives the maximum amount of information for a given BER. However, Bob cannot obtain the information of the Shannon limit determined by p_b. Here, we first focus our attention to a code that has the Shannon-limit performance in Fig. 5. When the raw BER is less than the threshold BER p_t^S, then the corrected BER asymptotically approaches zero. This means that the amount of information Bob obtains is constant at a lower BER than at the threshold BER; therefore, the amount of information Bob can obtain is determined by p_t^S. A similar situation is applicable for a near Shannon-limit code. However, the amount of information is not determined by p_t^n, but by p_t^S because the Shannon limit imposes bounds on it when a code rate is given. Therefore, when we estimate the secret capacity under the condition of using an error-correcting code, p_b is replaced by p_t^S in eq. (3). Threshold BERs p_t^S and p_t^n are the same order, and we can adjust the difference between p_b and p_t^n, for example, in no more than one digit through a system design. Because p_f and p_b differ by multiple digits, we can achieve the condition $p_f \gg p_t^S$. In this case, the secret capacity is determined almost solely by Eve's BER, as mentioned in §3. For example, when the phase fluctuations $\delta\theta$ at a transmitter are 25°, the secret capacity is 2.3×10^{-3}, according to Fig. 4(b), which corresponds to a key generation rate of 11.5 MHz for a 10-GHz transmission rate, where we considered discarding half the transmitted random numbers and we set δC to zero. The secret capacity is the value for an asymptotic behavior. To avoid statistical leakage to Eve, privacy amplification should be strengthened. In this case, the key generation rate of 11.5 MHz is reduced according to the strength of the privacy amplification.

We assumed phase fluctuations of 25° as an example. If we choose phase fluctuations of 45°, then the secret capacity gives a key generation rate of 800 MHz for a 10-GHz transmission rate, although a hard exhaustive basis-retrieval process is required. Therefore, the key generation rate varies widely depending on a system design. In this discussion, we assumed phase fluctuations arbitrarily. However, an appropriate BER exists depending on the applied error-correcting code, although the appropriate BER can be designed to some extent. Optimum fluctuations should be determined by considering these factors, and a key generation rate will be determined according to the optimization.

We mention the possibility of using an ordinary error-correcting code that does not have very high performance. When conditions $p_f > p_t^S$ and $p_t^o > p_b'$ are satisfied, where p_t^o is the threshold BER of the ordinary error-correcting code, and p_b' is the BER for binary signals, similar to p_b, then the secret capacity is always obtained. Because the condition $p_t^o > p_b'$ is inevitably satisfied to enable communications between Alice and Bob, the question is in the case of $p_f < p_t^S$. In this case, the secret capacity based on eq. (3) is not obtained. However, if $p_f' > p_t^o$ is satisfied, where p_f' is the BER for four-value-state signals, similar to p_f, then Bob is more advantageous in the error-correcting performance than Eve, according to Fig. 5. However, we cannot use the general formula of eq. (3). To use this advantage, we must formulate an equation corresponding to eq. (3), depending on the concrete error correcting code.

We discussed error-correcting codes in two cases, i.e., whether they were near the Shannon limit or not, from a viewpoint of secret capacity. We did not mention the structure of error-correcting codes. However, the structure is important to obtain better performance in this protocol because this protocol needs to perform an exhaustive basis-retrieval process, which is not considered in existing error-correcting codes. An error-correcting code should be optimally designed by taking the exhaustive basis-retrieval process into account in the future to make this protocol more efficient.

7. Summary

A practical secret key generation protocol that uses a preshared key and general phase fluctuations was described. New secret keys are generated information theoretically using phase fluctuations under the condition of using the preshared key. The security level of this protocol is less than that of information-theoretic security because a preshared key is used, but it is more than that of computational complexity due to the probabilistic property of the fluctuations. From this point of view, the protocol belongs to a new category. The condition to obtain the secret capacity in this new category is that relations $p_f > p_t^S$ and $p_t > p_b$ are satisfied, where p_t is the threshold BER of a used error-correcting code. Even if relation $p_f > p_t^S$ is not satisfied, if relation $p_f > p_t > p_b$ is satisfied, Bob is more advantageous than Eve. However, a formulation for the secret capacity is needed in this case, depending on the used error-correcting code. Because this protocol uses signal states classically, the signal light is tolerant of loss and amplification, satisfying the required conditions in realistic communication systems. For example, long-haul transmission of 10,000 km is possible.

Acknowledgments

The author thanks Shinya Sasaki for the helpful advice on long-haul transmission. This work was partly supported by Special Coordination Funds for Promoting Science and Technology.

1) C. H. Bennett and G. Brassard: Proc. IEEE Int. Conf. Computers, Systems and Signals, 1984, p. 175.
2) N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden: Rev. Mod. Phys. **74** (2002) 145.
3) A. K. Ekert: Phys. Rev. Lett. **67** (1991) 661.
4) C. H. Bennett, G. Brassard, and N. D. Mermin: Phys. Rev. Lett. **68** (1992) 557.
5) S. L. Braunstein and P. van Loock: Rev. Mod. Phys. **77** (2005) 513.

6) N. J. Cerf and P. Grangier: J. Opt. Soc. Am. B **24** (2007) 324.
7) W. K. Wootters and W. H. Zurek: Nature **299** (1982) 802.
8) D. Dieks: Phys. Lett. A **92** (1982) 271.
9) H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller: Phys. Rev. Lett. **81** (1998) 5932.
10) A. D. Wyner: Bell Syst. Tech. J. **54** (1975) 1355.
11) I. Csiszár and J. Körner: IEEE Trans. Inf. Theory **24** (1978) 339.
12) U. M. Maurer: IEEE Trans. Inf. Theory **39** (1993) 733.
13) R. Ahlswede and I. Csiszàr: IEEE Trans. Inf. Theory **39** (1993) 1121.
14) N. Lütkenhause: Phys. Rev. A **59** (1999) 3301.
15) W. Y. Hwang, I. G. Koh, and Y. D. Han: Phys. Lett. A **244** (1998) 489.
16) H. P. Yuen: arXiv:0906.5241.
17) R. Renner, N. Gisin, and B. Kraus: Phys. Rev. A **72** (2005) 012332.
18) C. H. Bennett, G. Brassard, and J.-M. Robert: SIAM J. Cmput. **17** (1988) 210.
19) C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer: IEEE Trans. Inf. Theory **41** (1995) 1915.
20) For example, J. Justesen and T. Hoholdt: *A Course in Error-Correcting Codes* (European Mathematical Society, Zürich, 2004).
21) C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin: J. Cryptol. **5** (1992) 3.
22) B. Kraus, N. Gisin, and R. Renner: Phys. Rev. Lett. **95** (2005) 080501.
23) T. Tomaru: Opt. Express **15** (2007) 11241.
24) T. Tomaru and S. Sasaki: Opt. Commun. **282** (2009) 1047.
25) J. P. Gordon and L. F. Mollenauer: Opt. Lett. **15** (1990) 1351.
26) C. M. Caves: Phys. Rev. D **26** (1982) 1817.
27) T. Tomaru and M. Ban: Phys. Rev. A **74** (2006) 032312.
28) K. Kikuchi: Electron. Lett. **26** (1990) 1851.
29) E. Desurvire: IEEE Photonics Technol. Lett. **2** (1990) 208.
30) K. S. Kim, R. H. Stolen, W. A. Reed, and K. W. Quoi: Opt. Lett. **19** (1994) 257.
31) For example, T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke: IEEE Trans. Inf. Theory **47** (2001) 619.
32) For example, S. Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke: IEEE Commun. Lett. **5** (2001) 58.