Quantum key distribution protocol with slow basis change

Toshihiko Sasaki,[1] Kiyoshi Tamaki,[2] and Masato Koashi[1]

[1]*Photon Science Center, Graduate School of Engineering, The University of Tokyo, 7-3-1 Bunkyo-ku, Tokyo 113-8656, Japan*
[2]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan*

In many quantum key distribution (QKD) protocols, the receiver has to randomly change a measurement basis for each pulse or each train of pulses. This random change requires us to generate a huge amount of random numbers. It is also cumbersome for some QKD protocols, such as the round-robin differential phase shift QKD protocol, to change the basis rapidly. In this presentation, we address these issues by analyzing the security of QKD protocols with slow basis change. In particular, we show a sufficient condition that allows a QKD protocol to employ the slow basis change. It turns out that the slow basis change does not compromise the key generation rate in a relatively high loss regime when we change the basis as frequently as the photon detection events. Our security proof relaxes technological demands on the receiver side without frustrating the performance.

I. INTRODUCTION

Most of quantum key distribution (QKD) protocols assume a random change of the working basis to deduce the degree of the intervention of an eavesdropper (Eve). Usually a protocol dictates that the change of basis should be done at every round of transmitting an optical signal from the sender (Alice) to the receiver (Bob). As a result, the signal repetition rate can never exceed the inverse of the switching time of the active device used for the basis change. Sometimes a faster active device is available only in exchange for making a compromise on insertion loss, stability, and cost. Although the use of passive elements for routing photons to detection devices with different bases removes this constraint, the increase in the number of detectors is a disadvantage in terms of the cost and the dark counts. Such a technological demand is especially severe in the protocols using many different bases like the round-robin differential phase shift (RRDPS) QKD protocol [1]. This has motivated us to consider the possibility of making the update of the basis less frequently than usual, which is the main goal of this paper. Such a modification will have another merit of reducing the consumption rate of random numbers, allowing the use of slower physical random number generators.

In this presentation, we propose a way to construct a modified protocol where Bob changes the measurement basis only every M signals. If the original protocol satisfies specific conditions, we can derive its security without looking into how the security of the original protocol is proved. Moreover, as long as $1/M$ is larger than the detection rate, the key rate of the modified protocol is almost the same as that of the original one. It means that we can reduce the rate of the basis change almost as low as the detection rate without compromising the performance.

II. SLOW BASIS CHANGE AND SECURITY

In this section, we explain a condition that allows a QKD protocol to employ the slow basis change. Although this condition applies to many protocols, we particularly consider the BB84 protocol with an ideal single-photon source to explain how and why our main idea works. Let us call the two complementary bases in the BB84 protocol as the Z basis and the X basis. In our proof, we assume that the detection efficiency of Bob's measurement apparatus is independent of the measurement basis, which is a crucial property for our argument. Note that the same assumption has been used in many security proofs. The BB84 protocol is composed of the following procedures, which we call Protocol I:

1. Alice randomly selects a basis from the Z basis and the X basis. She also randomly chooses one of the eigenstates in the chosen basis to encode a bit on the single-photon pulse and sends it to Bob over a quantum channel.
2. (Fast basis change) Bob randomly chooses a measurement basis from the Z basis and the X basis, and uses the chosen basis for measuring the incoming pulse.
3. They repeat procedures 1 and 2 a predetermined number of times.
4. By using an authenticated classical public channel, Alice and Bob disclose the bases of the detected instances and keep the bases of the other instances private. They discard the instances where they have used difference bases. After this sifting step, they perform error correction and privacy amplification to generate the final key.

The security of this protocol against general attacks has been proven [2–6] and the key generation rate is also known.

The key insight about this protocol is that the procedure 2 is equivalently replaced by

2. (Basis change upon heralding) Bob performs the non-demolition measurement of the photon number to determine whether photons are present or not before choosing a measurement basis. Only when the photon number is nonzero, he randomly

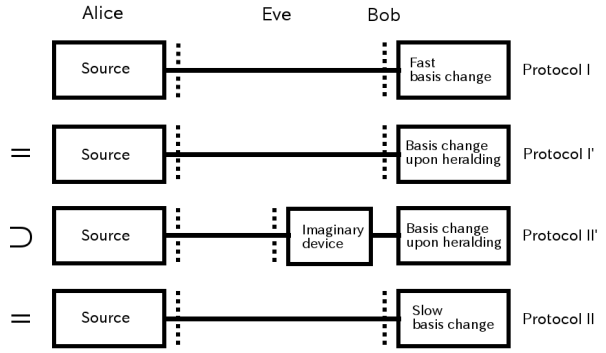

FIG. 1. Relation between Protocol I, Protocol I', Protocol II', and Protocol II. The dotted lines divide the areas which belong to Alice, Eve, and Bob. Protocol I' is equivalent to Protocol I. Protocol II' is the same as Protocol I' except that Bob employs the imaginary device just before his measurement apparatus. Protocol II is equivalent to Protocol II'.

chooses a measurement basis, and use it for the measurement.

The equivalence is justified by the condition that the detection efficiency is independent of the measurement basis. For later use, we call Protocol I whose procedure 2 is replaced with this equivalent procedure as Protocol I'. (see Fig. 1)

Now we introduce the BB84 protocol with slow basis change, which we call Protocol II. Let us divide the pulse train into *sequences*, each of which contains M successive pulses. In Protocol II, the measurement basis is updated only after every sequence of M pulses. We also include a procedure that assures that at most one detection occurs in a sequence. The procedure 2 of Protocol II is described as follows.

2. (Slow basis change) If the round is the beginning of a sequence, Bob randomly chooses a new basis and uses it for the measurement. Otherwise, he uses the same basis as the previous round. If there was already a round with detection in the same sequence, he ignores the measurement outcome and treats it as undetected.

Note that Protocol II is exactly what we want to prove the security of. We will prove the security of Protocol II by first showing that Eve's operation against Protocol II is limited compared with Eve against Protocol I. It follows that Protocol II is secure if Protocol I is secure, and we can use exactly the same key rate formula.

More specifically, for the proof, we introduce an imaginary device that works in the following way. It determines the number of photons in each pulse, and whenever it finds a pulse with nonzero photons, it lets the pulse pass through but replaces all the subsequent pulses in the sequence with the vacuum. Imagine that Bob employs this imaginary device just before his measurement apparatus, and then Alice and Bob follow the procedures of Protocol I'. We call it Protocol II'. Protocol II' is equivalent to Protocol II because both of them treat only the first detectable event in each sequence as a detected event, and Bob's random choice of the basis is used only for this detection. Protocol II' can be recognized as Protocol I' with a restriction on Eve's attack strategies; Eve has to use the imaginary device at the end of the quantum channel. Since Protocol I' is proven to be secure against general attacks, Protocol II' is also secure if the same key rate formula is used. It means that Protocol II is secure and we can employ the key rate formula of Protocol I for Protocol II.

The argument so far is applicable to the protocols satisfying the following conditions:

1. The detection probability does not depend on the basis choice.
2. There exists an input state to Bob's apparatus that ensures that the detection never occurs.

The condition 1 enables Bob to determine whether detection occurs or not before choosing the basis. The condition 2 is rather technical but ensures the existence of an imaginary device to guarantee at most one detection occurs in each sequence. The protocols satisfying these conditions include SARG04 protocol [7], Decoy-BB84 protocol [8–10], three-state protocol [11], and RRDPS protocol [12]. The exceptions are the protocols that uses the strong reference pulse [13, 14].

III. PERFORMANCE

In this section, we consider the effect of the slow basis change on the performance of QKD. Although we can use exactly the same key rate formula for Protocol II, it does not mean that Protocol II has the same performance as Protocol I. The effective transmission rate of Protocol II is smaller than that of Protocol I because Protocol II ignores the detection events except the first one in a sequence. However, if the detection rate is much smaller than $1/M$, the second detection rarely occurs, and therefore Protocol II has almost the same performance as Protocol I.

By taking the BB84 protocol discussed above as an example, we numerically compare the fast basis change and the slow basis change. We set the dark count rate d_c per pulse to be 10^{-6} and the length M of the sequence to be 10^2. We assume the same baseline system error rate $e_b(= 0.03)$ for the Z and X bases, which is independent of the transmission rate. For $Md_c \ll 1$, the asymptotic secure key generation rate G per pulse is given by

$$G = \frac{1-(1-\eta-d_c)^M}{M}\left(1-h(e)-h(e)\right), \qquad (1)$$

where $h(x)$ is $-x\log_2(x)-(1-x)\log_2(1-x)$, and e is $\frac{\eta\times e_b+d_c\times 0.5}{\eta+d_c}$. The key rates for the fast basis change ($M = 1$) and the slow basis change ($M = 100$) are illustrated in Fig. 2. In this example, the detection rate per pulse approximately equals to the transmission rate η. We find that the key generation rates of the two cases are almost the same when the detection rate is smaller

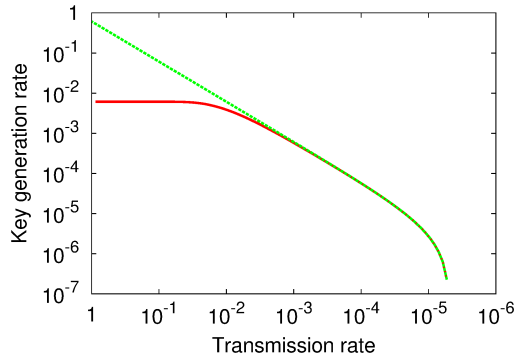

FIG. 2. The key generation rate per pulse of the BB84 protocol with the single photon source. We draw the $M = 1$ case (dashed line) and the $M = 100$ case (solid line) of the Eq. (1).

than $1/M$, which shows that we can employ the slow basis change in such a regime without sacrificing the performance.

IV. CONCLUSION

We have shown that the security of the protocol is essentially unchanged, even when Bob updates the measurement basis only at the beginning of the sequence, as long as the protocol satisfies the condition 1 and 2. We have also shown that the same key rate formula can be used for this modified protocol. Its performance is almost the same as that of the original protocol if the length of the sequence is smaller than the inverse of the detection rate. Thus, we can reduce the rate of changing the measurement basis to the order of the detection rate without sacrificing the performance.

One of the remaining problems is to consider what happens if we use multiple detections in a sequence. If we use the same classical post-processing as the original protocol, there is an example where an effective eavesdropping strategy exists [15]. This implies that we need to modify the key rate formula itself to reflect the effect of reducing the randomness for the basis choice. Such an analysis will also deepen our quantitative understanding on the role of randomness for the basis change in the QKD protocols.

ACKNOWLEDGMENTS

We thank H. Takesue, K. Azuma, W. Munro, G. Knee, and F. Furrer for valuable discussions. This work was funded in part by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan), Photon Frontier Network Program (MEXT).

[1] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat Photon **9**, 827 (2015).
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] D. Mayers, J. ACM **48**, 351 (2001).
[4] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[5] M. Koashi, New Journal of Physics **11**, 045018 (2009).
[6] M. Hayashi and T. Tsurumaru, New Journal of Physics **14**, 093014 (2012).
[7] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[8] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[10] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[11] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[12] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).
[13] A. Acín, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).
[14] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[15] T. Sasaki, K. Tamaki, and M. Koashi, arXiv preprint arXiv:1604.04460 (2016).