Security of the Bennett 1992 quantum key distribution protocol estimating eavesdropper's information without the bit error rate

Toshiyuki Nakamura,* Kensuke Nakata, Akihisa Tomita, Kazuhisa Ogawa, and Atsushi Okamoto
Graduate School of Information Science and Technology, Hokkaido University.

A quantum key distribution (QKD) protocol without monitoring signal disturbance has an advantage over conventional QKD protocols that it can generate secure key under a noisy channel with an imperfect receiver. The amount of the information of an eavesdropper (Eve) on the sift key can be predetermined by the mean photon number of the transmitted pulses. We investigate a modification of Bennett 1992 protocol to have the above-mentioned features on the estimation of the Eve's information.

I. INTRODUCTION

In conventional QKD protocols, sender (Alice) and receiver (Bob) share secure key via privacy amplification by estimating the phase error rate from the error rate of the received data. Therefore, the final secure key rate decreases as the error rate is increased by noise in the transmission line and imperfections of the receiver, because the errors increase the sacrifice bits required in the privacy amplification to ensure security of the final key. Recently, Round-Robin Differential Phase Shift (RRDPS) protocol was proposed by Sasaki, et al. [1]. In this protocol, Alice and Bob estimate the upper limit of the information gained by an eavesdropper (Eve) from not the received data but the known transmission parameters. This protocol has an advantage that the amount of the sacrifice bits is independent of the disturbance during the transmission, so that the final key rate is immune against noise in the channel and imperfections in the receiver. However, since the implementation of the RRDPS is involved, it is desirable to find another easily implementable protocol with the similar advantage.

The following fact would provide a clue in exploring new protocols that the RRDPS limits the Eve's information obtainable by her measurement to attain the security of the final key. Since the measurement cannot fully distinguish non-orthogonal states, a QKD protocol that transmits non-orthogonal states contains a mechanism to limit the information on the states. This is in contrast to Bennett-Brassard 1984 protocol [2], where the transmitted states can be completely determined once the eavesdropper knows the basis. In this report, we considered Bennett 1992 (B92) protocol [3], a well-known protocol utilizing two non-orthogonal states, as a candidate for the new protocol. We found a slight modification on the B92 protocol yields secure final key by estimating the upper-bound of Eve's information limited by the incompleteness of her measurement in intercept/resend attack.

*Electronic address: nakamura@optnet.ist.hokudai.ac.jp

II. PROTOCOL

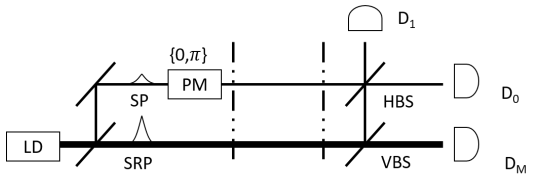

FIG. 1: Set up for B92 protocol with a strong reference pulse. LD: laser diode, PM: phase modulator, VBS: variable beam splitter, HBS: half beam splitter, D_0 and D_1: single photon-detectors discriminating vacuum, single photon and multi-photons, and D_M: a photodetector.

We begin with a brief review of the B92 protocol with a strong reference pulse[4] (SRP-B92), because the proposed protocol is based on it. The SRP-B92 protocol uses a setup depicted in Fig. 1. Alice splits a laser pulse to a signal pulse (SP) $|\alpha\rangle$ and strong reference pulse (SRP) $|\xi\rangle$, which satisfy the conditions $|\alpha|^2 < 1$ and $|\xi|^2 \gg 1$. She generates a random bit sequence, and relates the SP states with it by applying the phase shift 0 and π according to the bit value. Then, Alice sends SP and SRP to Bob. Bob splits the SRP with a variable beam splitter (VBS) into two pulses. One pulse interferes with the SP by a half beam splitter (HBS), where the amplitude of the pulses are set to that of the SP attenuated by the transmission line to $\sqrt{\eta}\alpha$. The other pulse is detected by a photo-detector D_M. If the detected photon number in D_M is out of a certain range, Alice and Bob stop key generation and discard their results. If not, Bob determines the bit value by a single photon detection in D_0 or D_1, where detectors D_0 and D_1 discriminate vacuum, one photon and multiphoton. Then, Alice and Bob perform the error correction and the privacy amplification to generate final key. The amount of the sacrifice bits for the privacy amplification is estimated by error rate, as is common with conventional QKD protocol.

Our proposal uses the same setup as Fig. 1. The proposed protocol differs from the SRP-B92 protocol on the following five points. First, Alice and Bob estimate the upper bound of Eve's information in advance from

mean photon number of signal pulse to use in the privacy amplification. Second, if the intensity of reference pulse changes greatly, Alice and Bob stop the key generation and discard all the key obtained in this sequence. Third, if the probability of simultaneous detection of D_0 and D_1 exceed $P_{sim}^{(lim)}$, Alice and Bob discard all the key obtained in this sequence, Fourth, mean photon numbers of SP and SRP at the output of the transmitter are known to Alice and Bob. Fifth, if experimental bit error rate e_{bit} exceeds the bit error rate shared in advance $e_{bit}^{(sh)}$, Alice and Bob discard all the key obtained in this sequence.

III. ANALYSIS

In this section, we describe the estimation of the upper limit of Eve's information with mean photon number of the signal pulses for the intercept/resend attack.

The signal states used in B92 protocol are a mixture of coherent states for Eve. The coherent states $|\alpha\rangle, |-\alpha\rangle$ of mean photon number $\mu = |\alpha|^2$ are non-orthogonal($\langle\alpha| - \alpha\rangle \neq 0$). It is well-known that two non-orthogonal states cannot be distinguished, and that it is impossible to make perfect clones of the states[5]. Measurement on the non-orthogonal states disturbs the quantum states, if Eve try to draw the information. Moreover, photon number splitting attack using quantum non-demolition measurement does not work, because no special basis exists for B92 protocol to measure the state perfectly. Therefore, we can bound the amount of Eve's information by calculating mutual information between Alice and Eve and between Eve and Bob when she measures signal states and resend them to Bob.

The discrimination of two coherent states becomes more difficult as mean photon number decreases. This applies to both Eve and Bob. However, Eve's information is affected more severely, because she should resend the received states. In the following analysis, we assume that Eve maximizes her information, no matter how many errors she causes. We calculate the amount of her information obtained from the following two types of measurements.

A. Unambiguous State Discrimination

Eve obtains information from non-orthogonal states without errors by using unambiguous state discrimination (USD) measurement. However, the measurement returns inconclusive results with non-zero probability. Thus, she resends the signal states only when she obtains conclusive results. First, the mutual information between Alice and Bob is

$$I_{AE} = P_{Con}, \tag{1}$$

where P_{Con} represents probability that Eve obtains the conclusive results:

$$\begin{aligned} P_{Con} &= 1 - |\langle\alpha| - \alpha\rangle| \\ &= 1 - e^{-2\mu}. \end{aligned} \tag{2}$$

Eqs. (1)-(2) indicate that I_{AE} will increase as mean photon number μ increases.

Next, we should analyze the mutual information between Bob and Eve. We should consider that Eve resends signal and reference pulses. Eve may choose a strategy from the following:

- Reference pulse
  - She changes the intensity of the pulse
  - She unchanges the intensity of the pulse
- Signal pulse
  - If she gets a conclusive result then send a pulse according to the result. Otherwise, she does NOT send a signal pulse.
  - If she gets a conclusive result then send a pulse according to the result. Otherwise, she sends a signal pulse with randomly selected phase shift $\{0, \pi\}$.

In order to reduce Bob's detection when Eve gets the inconclusive results, she may change the intensity of the reference pulse. However, Alice and Bob will stop generating and discard the key when the intensity greatly changed. Therefore, she has to send reference pulse without changing the intensity.

Eve may reduce single photon detection probability by increasing power of signal pulses when the measurement results are inconclusive. The condition that Alice and Bob stop the session when the multiphoton detection exceed a limit prevents Eve from employing this strategy. The analysis shows that vacuum is the most advantageous for her. The mutual information between Eve and Bob is

$$I_{EB} = \frac{P_{Con} \cdot P_{Succ,sig}^{(B)}}{P_B} \tag{3}$$

with receiving rate of Bob

$$P_B = \left[P_{Con} \cdot P_{Succ,sig}^{(B)} + P_{In} \cdot P_{Succ,vac}^{(B)} \right], \tag{4}$$

the probability of conclusive results P_{con}, the probability of inconclusive results $P_{In} = e^{-2\mu}$ and the one photon detection probabilities of Bob when Eve resends the signal pulse or vacuum as

$$P_{Succ,sig}^{(B)} = 2\eta\mu e^{-2\eta\mu}, \tag{5}$$

$$P_{Succ,vac}^{(B)} = \eta\mu e^{-\eta\mu/2}, \tag{6}$$

respectively.

B. Minimum-error state discrimination

Minimum-error measurement minimizes the probability of error in discriminating two non-orthogonal pure states. The error rate in this measurement is

$$e_{min} = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\alpha| - \alpha\rangle|^2}\right). \quad (7)$$

Using this error rate, the mutual information between Alice and Eve is given by at most

$$I_{AE} = 1 - h(e_{min}) \quad (8)$$

with Shannon entropy $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. Eve measures a fraction $r = e_{bit}/e_{min}$ of the pulses sent by Alice to keep Bob's bit error rate lower than a designed value $e_{bit}^{(sh)}$. The mutual information between Eve and Bob is given by

$$I_{EB} = r \cdot (1 - h(e_{min}))\,. \quad (9)$$

In order to determine Eve's optimal measurement, we compare amount of information obtained by the USD measurement and the minimum error measurement, as shown in Fig. 2. The analysis showed that we should take the amount of Eve's information as I_{AE} for minimum error measurement given by (7) and (8), which depends only on the mean photon number.

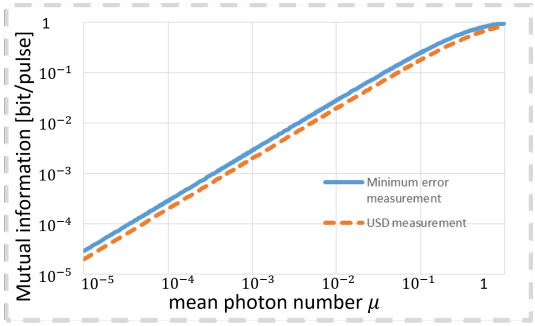

FIG. 2: Comparison of $I_E^{(USD)}$ (dashed line) and $I_E^{(MIN)}$.

IV. RESULTS AND CONCLUSION

We are interested in possibility of generating secure key rate against the above attack. Secure key capacity is given by Maurer[6] as

$$C_S \geq \max\left(I_{AB} - \max I_{AE}, I_{AB} - \max I_{EB}\right), \quad (10)$$

where the mutual information of Alice and Bob

$$I_{AB} = 1 - h(e_{bit}) \quad (11)$$

represents the capacity of error free communication. The key generation rate G is

$$G = Q\left[1 - h\left(e_{bit}\right) - I_E\right], \quad (12)$$

where Q is Bob's detection rate, and I_E is the amount of Eve's information defined by $I_E = \max\left(I_{AE}, I_{EB}\right)$. The detection rate Q is determined by mean photon number μ as

$$Q = 2\eta\mu e^{-2\eta\mu}, \quad (13)$$

where transmission rate is

$$\eta = \eta_{sys} \cdot \eta_{det} \cdot 10^{-\beta L}, \quad (14)$$

where η_{sys}, η_{det}, β and L are transmittance in system, detection efficiency of detectors D_0 and D_1, loss coefficient, and distance between Alice and Bob respectively. The bit error rate is given by

$$e_{bit} = \frac{Qe_{sys} + d_c \cdot 1/2}{Q + d_c}, \quad (15)$$

where e_{sys} represents the baseline system error rate originated from the system imperfections, such as state preparation flaw, decoherence, and mismatch of polarization and d_c is dark count probability of the detectors.

The key generation rate was calculated with dark count probability $d_c^{(APD)} = 6.3 \times 10^{-7}$, detection efficiency $\eta_{det}^{(APD)} = 10.8\%$, $\eta_{sys} = 0.32$ (-5dB) and $\beta = 0.21$ (dB/km) in system, reported in QKD experiments [7, 8], Fig. 3 indicates Alice and Bob can generate secure key with highly imperfect devices even at the error rate e_{sys} as large as 20%.

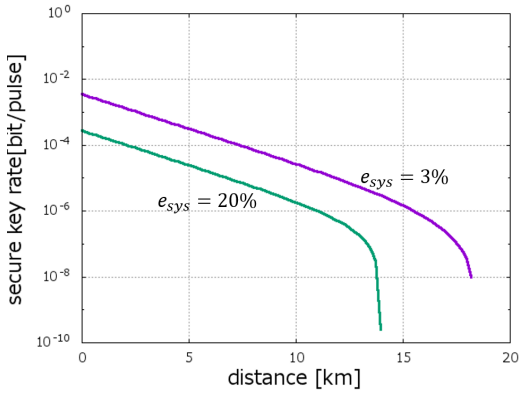

FIG. 3: Secure key rate of the proposed protocol with APD photodetectors

The maximum key generation distance of 18 km was predicted for the mean photon number of 0.09 with $e_{sys} = 3\%$.

In conclusion, we have proposed a protocol that generates key using the amount of Eve's information estimated without state disturbance as RRDPS protocol. The analysis showed that secure final key can be generated with the eavesdropper's information estimated without using error rate. We believe that analysis for intercept/resend attack should be a foothold to prove unconditional security.

[1] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).
[2] C. H. Bennett and G. Brassard, in Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp.175-179 (1984).
[3] C. H. Bennett, Phys. Rev. Lett., **68**, 3121 (1992).
[4] K. Tamaki, N. Lutkenhaus, M. Koashi, and J. Batuwantudawe. Phys. Rev. A **80**, 032302(2009).
[5] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett., **85**, 1754 (2000).
[6] U. Maurer, IEEE Trans. Information Theory **39**, 733 (1993).
[7] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[8] N. Namekawa, S. Adachi, and S. Inoue, Opt. Express **17**, 6275 (2009).