Security against individual beamsplitting attack for quantum cryptography using balanced homodyne detection

Ryo Namiki* and Takuya Hirano
Department of Physics, Gakushuin University, Mejiro 1-5-1, Toshima-ku, Tokyo, 171-8588, Japan

We investigate the security of quantum cryptography using balanced homodyne detection against the individual beamsplitting attack. Under the assumption that the eavesdropper can use a positive operator valued measure (POVM) on the individual split signal, we estimate the upper bound for the potentially leaked information by the loss. The key gain rate for a given optical loss is then calculated. The secure key gain can be positive for a sufficiently large threshold if the loss is less than unity.

Introduction- Quantum cryptography allows two parties, Alice (the sender) and Bob (the receiver), to share a random bit sequence, called key, which is unknown to the eavesdropper Eve [1].

For any practical implementation of quantum cryptography, degrade of the performance due to the transmission loss is important [2, 3]. The loss weakens the signal intensity and at the same time it potentially causes the information leakage to Eve. The loss is usually modeled by a beamsplitter and the split signal is assumed to be received by Eve. This eavesdropping strategy is called beamsplitting attack.

The conventional security measure of quantum cryptographic system is the secure key gain which represents the secure key bits gain per signal [4, 5]. che Here we show the key gain for a coherent state protocol [6] against the individual beamsplitting attack, that is, Eve can use a positive operator valued measure (POVM) for the individual split signal.

Protocol and basic quantities- The protocol we study here is a four state protocol using phase modulation of weak coherent pulse and balanced homodyne detection [6]. Alice randomly chooses one of the four coherent states $|\alpha e^{im\pi/2}\rangle$ with $\alpha > 0$, $m = 0, 1, 2, 3$ and sends it to Bob. Then Bob randomly measures one of the two quadratures $\hat{x}_k$ with $k = 1, 2$. After the transmission of a large number of pulses, Bob informs Alice of the choice of quadratures through a classical channel. For the pulses $m-k = odd$, Bob sets a threshold $x_0 (\geq 0)$ and constructs his bit sequence by the following decision:

$$(\text{bit value}) = \begin{cases} 1 & \text{if } x > x_0 \\ 0 & \text{if } x < -x_0, \end{cases} \tag{1}$$

where x is the result of Bob's measurement.

In a simple loss model Bob receives the signal $|\sqrt{\eta}\alpha e^{im\pi/2}\rangle$, $0 \leq \eta \leq 1$ is the parameter characterizing the loss $1-\eta$ (see Fig. 1). If $m - k = odd$, the

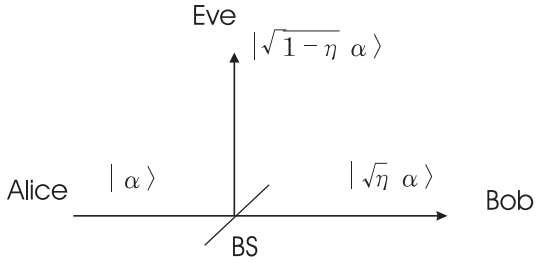

FIG. 1: A simple loss model is a beamsplitter (BS). The loss is characterized by the reflectivity of the BS $1-\eta$, $0 \leq \eta \leq 1$. In the beamsplitting attack we consider that the split pulse is recieved by Eve. Thus the loss causes some information leakage even if the signal is undisturbed.

probability that the measurement results x is given by

$$\text{Prob}(x) = \frac{1}{\sqrt{2\pi}} \left\{ e^{\left[-2(x-\sqrt{\eta n})^2\right]} + e^{\left[-2(x+\sqrt{\eta n})^2\right]} \right\}, \tag{2}$$

where $n = \alpha^2$ is the pulse intensity (the mean photon number per pulse). Therefore Bob's Shannon information gain per pulse is given by

$$\frac{1}{2} \sum_{|x|>x_0} \text{Prob}(x) i_{AB}(x, \eta n), \tag{3}$$

where the factor $1/2$ is the probability that the basis is correct i.e., $m - k = odd$ and

$$\begin{aligned} i_{AB}(x,n) &= 1 + \text{Prob}(\sqrt{n}|x) \log_2 \text{Prob}(\sqrt{n}|x) \\ &+ \text{Prob}(-\sqrt{n}|x) \log_2 \text{Prob}(-\sqrt{n}|x) \end{aligned} \tag{4}$$

is the Shannon information gain when x is triggered where

$$\begin{aligned} \text{Prob}(\alpha|x_1) &= \frac{|\langle x_1|\alpha\rangle|^2}{|\langle x_1|\alpha\rangle|^2 + |\langle x_1|-\alpha\rangle|^2} \\ &= \frac{1}{1+\exp(-4\alpha x_1)} \end{aligned} \tag{5}$$

is the conditional probability that the state is $|\alpha\rangle$ when the measurement results x_1.

*namiki@qo.phys.gakushuin.ac.jp

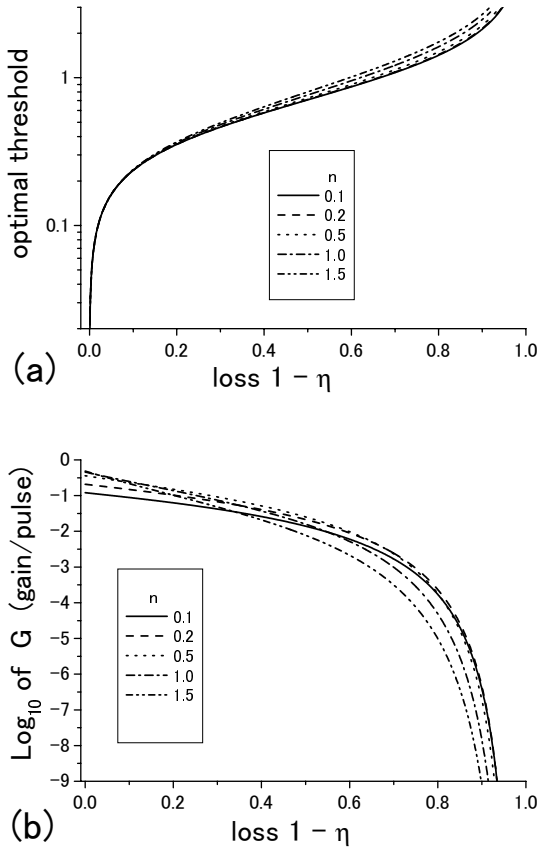

FIG. 2: (a) The optimal threshold x_0^{opt} for the values of the pulse intensity $n = 0.1, 0.2, 0.5, 1.0, 1.5, 2.0$ as functions of the loss $1-\eta$. (b) The key gain G at the optimal threshold.

Individual beamsplitting attack- Since Eve can perform her measurement after she knows the basis information, her task is to differentiate the binary phase shifted coherent pulse signals $|\pm\sqrt{1-\eta}\alpha\rangle$. For the differentiation problem of two pure state, the POVM which gives the minimum error rate (the maximum Shannon information) also gives the maximum Renyi information gain [7]. For some two pure states $\{|\Psi_1\rangle, |\Psi_2\rangle\}$, the maximum Renyi information gain is given by

$$I_{opt}^R = \log_2\left(2 - 4q + 4q^2\right), \tag{6}$$

where

$$q = \frac{1-\sqrt{1-|\langle\Psi_1|\Psi_2\rangle|^2}}{2} \tag{7}$$

is the minimum error rate (Helstrom bound [8]). For the coherent states $\{|\sqrt{1-\eta}\alpha\rangle, |-\sqrt{1-\eta}\alpha\rangle\}$ we obtain

$$I_{opt}^R(n,\eta) = \log_2\left(2 - \exp[-4(1-\eta)n]\right), \tag{8}$$

where $n = \alpha^2$.

Secure key gain- Using the expressions (3) and (8) we obtain the secure key gain (with ideal error correction) [5].

$$G(x_0, n, \eta) \;=\; \frac{1}{2}\sum_{|x|>x_0} \mathrm{Prob}(x)\big(i_{AB}(x,\eta n) - I_{opt}^R(n,\eta)\big). \tag{9}$$

Since $0 \le I_{opt}^R < 1$ for any finite $n \ge 0$ and i_{AB} is an increasing function of x having the limit $i_{AB} \to 1$, $(x \to \infty)$ if $\eta > 0$, we can always find $\tilde{x}$ which satisfies

$$i_{AB}(\tilde{x}, \eta n) - I_{opt}^R(n,\eta) \ge 0 \tag{10}$$

and a choice of the threshold $x_0 \ge \tilde{x}$ gives a positive gain with $\mathrm{Prob}(x) \ge 0$. Therefore secure key is always obtainable by setting a sufficiently large threshold if only η differs from zero.

The summation taken over the region where inequality (10) is satisfied maximizes the gain. Thus, if equality holds for some $\tilde{x}$, the choice of the threshold $x_0 = \tilde{x}$ gives the maximum gain. Otherwise the inequality should hold for any $\tilde{x} \ge 0$ and thus the threshold $x_0 = 0$ gives the maximum gain. The optimum threshold x_0 and gain $G(x_0^{opt}, \eta n)$ for $n = 0.1,\ 0.2,\ 0.5,\ 1.0,\ 1.5$ are shown in Fig. 2

Summary- We have calculated the secure key gain for a coherent state quantum cryptographic protocol against the individual beamsplitting attack. The threshold enables us to obtain a positive gain if the loss is less than unity. In this sense the transmission distance is unlimited. The optimal threshold is selected to maximize the gain.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74,** 145 (2002).

[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85,** 1330 (2000).

[3] J. Calsamiglia, S. M. Barnett, and N. Lütkenhaus, Phys. Rev. A **65,** 012312(2001).

[4] N. Lütkenhaus, Phys. Rev. A **59,** 3301 (1999).

[5] N. Lütkenhaus, Phys. Rev. A **61,** 052304 (2000).

[6] T. Hirano, T. Konishi, and R. Namiki, quant-ph/0008037; R. Namiki and T. Hirano, quant-ph/0205191.

[7] B. A. Slutsky, R. Rao, P. Sun, and Y. Fainman, Phys. Rev. A **57,** 2383 (1998).

[8] C. W. Helstrom, *Quantum detection and estimation theory* (1976).