

# Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel

Kiyoshi Tamaki<sup>1,\*</sup> and Norbert Lütkenhaus<sup>2</sup><sup>1</sup>*The Graduate University for Advanced Studies (SOKENDAI), Hayama, Kanagawa 240-0193, Japan*<sup>2</sup>*Institut für Theoretische Physik I and Institute for Optics, Information and Photonics (Max-Planck Research Group), Universität Erlangen-Nürnberg, Staudtstrasse 7/B3, 91058 Erlangen, Germany*

(Received 18 August 2003; published 22 March 2004)

We show that the security proof of the Bennett 1992 protocol over loss-free channel given by Tamaki, Koashi, and Imoto [Phys. Rev. Lett. **90**, 167904 (2003)] can be adapted to accommodate loss. We assumed that Bob's detectors discriminate between single-photon states on one hand and vacuum state or multiphoton states on the other hand.

DOI: 10.1103/PhysRevA.69.032316

PACS number(s): 03.67.Dd

## I. INTRODUCTION

Quantum key distribution (QKD) is one of the most interesting topics in quantum information processing, which allows the sender (Alice) and the receiver (Bob) to share a secret key with negligible leakage of information to an eavesdropper (Eve). This task is accomplished by making use of the properties of quantum mechanics, such as no-cloning theorem [1], indistinguishability of nonorthogonal quantum states, entanglement, and so on [2]. The Bennett 1992 (B92) protocol [3], where only two nonorthogonal states are used, is thought to be secure due to the fact that Eve cannot clone and distinguish the states deterministically.

Although the qualitative reason of the security is simple, it is quite hard to show the quantitative security against so-called coherent attack, which is the most general attack allowed by quantum mechanics. In Refs. [4–6], the unconditional security of the Bennett-Brassard 1984 (BB84) protocol [7] is proven. Especially, in Refs. [5,6] they show the security by showing the relationship between QKD and other important protocols in quantum information, such as the entanglement distillation protocol (EDP) [8] and the Calderbank-Shor-Steane (CSS) quantum error correcting codes [9]. Recently in Ref. [10], the unconditional security of the B92 protocol has been proved by relating the B92 protocol to an EDP [8] initiated by local filtering [11]. The assumptions of the proof are that Alice and Bob's devices are perfect and the quantum channel is loss-free. To study the unconditional security of B92 protocol over a lossy and noisy channel is interesting from the point of view of the quantum information theory, since the channel loss directly affects the security of the B92 protocol. The proof based on the equivalence between the security and EDPs gives us an idea how to distill the Einstein-Podolsky-Rosen (EPR) state from states that arise from the lossy and noisy channel.

In this paper, we study the unconditional security of the B92 protocol. We assume that Alice has a perfect single-photon source, Bob's polarization measurement is perfect and he has a perfect single-photon counter that discriminates

between single-photon states on one hand and vacuum state or multiphoton states on the other hand. Under these assumptions, we show the unconditional security of the B92 protocol. The proof follows the idea in Ref. [10]. This paper is organized as follows. In Sec. II, we propose the protocol based on EDP with local filtering and CSS codes [6], and we reduce this to the B92 protocol. In Sec. III we give the formula for the error estimations for EDP based on CSS code. Finally, in Sec. IV we give the examples of the resulting performance, and the summary and discussion follow.

## II. PROTOCOL BASED ON EDP AND ITS REDUCTION TO THE B92 PROTOCOL

In this section, we introduce the protocol that will turn out to be secure and will reduce to the B92 protocol. In this protocol, Alice first prepares a two-qubit nonmaximally entangled states that can be written as

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0_z\rangle_A|\varphi_0\rangle_B + |1_z\rangle_A|\varphi_1\rangle_B) \quad (1)$$

and sends system B to Bob. Here  $|\varphi_j\rangle \equiv \beta|0_x\rangle + (-1)^j\alpha|1_x\rangle$  ( $j=0,1$ ), where  $0 < \alpha < 1/\sqrt{2}$ ,  $\beta \equiv \sqrt{1-\alpha^2}$ , and  $\{|0_x\rangle, |1_x\rangle\}$  is a basis (X basis) of the qubit. X basis and Z basis are related through the relationship  $|j_z\rangle = [|0_x\rangle + (-1)^j|1_x\rangle]/\sqrt{2}$ .

After receiving the state, Bob first performs the QND (quantum nondemolition) measurements that can be described by the POVM (positive operator valued measure) [2]

$$Q_s = \Pi_s, \quad (2)$$

$$Q_v = 1 - \Pi_s, \quad (3)$$

where  $\Pi_s$  is the projector onto the single-photon space and “v” means the detection of vacuum state or multiphoton states. Thanks to this QND measurements, even if Eve sends multiphoton states or vacuum state to Bob, Alice and Bob can work only on the qubit pairs, provided that the outcome is “s.” We also assume that, after this measurement, if the outcome is s, Bob performs the “local filtering operation” [11] on qubit B, described by the Kraus operator

\*Electronic address: tamaki\_kiyoshi@soken.ac.jp

$$A_{\text{fil}} \equiv \frac{\gamma}{\beta} (\alpha |0_x\rangle_B \langle 0_x| + \beta |1_x\rangle_B \langle 1_x|), \quad (4)$$

where  $\gamma \in (0, 1]$ . Note that if the channel is loss-free and noiseless or Eve does nothing, this operation yields the maximally entangled state (EPR state)  $(|0_x\rangle_A |0_x\rangle_B + |1_x\rangle_A |1_x\rangle_B) / \sqrt{2}$  with probability  $2\alpha^2\gamma^2$  due to the fact that the initial state is also written as  $|\Psi\rangle_{AB} = \beta |0_x\rangle_A |0_x\rangle_B + \alpha |1_x\rangle_A |1_x\rangle_B$ . Thus, the filtering operation with  $\gamma=1$  is optimum one in this case. When channel is lossy and noisy, or Eve is present, the filtered states may include bit errors, represented by the subspace spanned by  $\{|0_z\rangle_A |1_z\rangle_B, |1_z\rangle_A |0_z\rangle_B\}$ , and a phase error, represented by the subspace spanned by  $\{|0_x\rangle_A |1_x\rangle_B, |1_x\rangle_A |0_x\rangle_B\}$ . In order to distill the EPR pairs, Alice and Bob run the EDP based on CSS code [6] and after this EDP Alice and Bob measure each in the Z basis of the EPR pairs so that they obtain a secure key. Note that the QND measurement followed by the filtering  $A_{\text{fil}}$  and Z-basis measurement is equivalent to a measurement  $\mathcal{M}_{B92}^{L,\gamma}$  described by  $F_0^\gamma = \gamma^2 |\bar{\varphi}_1\rangle\langle \bar{\varphi}_1| / (2\beta^2)$ ,  $F_1^\gamma = \gamma^2 |\bar{\varphi}_0\rangle\langle \bar{\varphi}_0| / (2\beta^2)$ ,  $F_{\text{null}}^\gamma = \Pi_s - F_0^\gamma - F_1^\gamma$ , and  $F_v = 1 - F_0^\gamma - F_1^\gamma - F_{\text{null}}^\gamma$ , where  $|\bar{\varphi}_j\rangle \equiv \alpha |0_x\rangle - (-1)^j \beta |1_x\rangle$ . Thus  $\mathcal{M}_{B92}^{L,\beta}$  is the same measurement as in the B92 protocol with perfect photon detector, and  $\mathcal{M}_{B92}^{L,\gamma}$  corresponds to the generalized B92 protocol. For convenience, let  $\mathcal{M}_{B92}^\gamma$  be the measurements described by the set of the POVM elements  $\{F_0^\gamma, F_1^\gamma, F_{\text{null}}^\gamma\}$ . The following is the protocol that we want to be shown secure and reduce to the generalized B92 protocol.

### Protocol

(1) Alice prepares the state  $|\Psi\rangle_{AB}$ , and she sends the system B to Bob over a quantum channel.

(2) Bob performs the QND measurement described by  $\{Q_s, Q_v\}$ , and he publicly announces the outcome. They take notes of the outcome.

(3) Alice and Bob repeats the steps (1) and (2)  $2N$  times. Let  $2LN$  be the number of outcomes that resulted in  $v$ .

(4) Alice and Bob discard all the pairs whose outcomes of the QND measurement are  $v$ . By public discussion, Alice and Bob randomly permute the positions of the remaining  $2(1-L)N$  pairs.

(5) For the first  $(1-L)N$  pairs (check pairs), Alice measures system A in the Z basis, and Bob performs measurement  $\mathcal{M}_{B92}^\gamma$  on his system. By public discussion, they determine the number  $n_{\text{err}}$  of errors in which Alice found 0 and Bob's outcome was 1 or Alice found 1 with Bob's outcome 0.

(6) For the second  $(1-L)N$  pairs (data pairs), Bob performs the filtering  $A_{\text{fil}}$  on each of his qubits, and announces the total number  $n_{\text{fil}}$  and the positions of the qubits that have passed the filtering.

(7) From  $L$ ,  $n_{\text{err}}$ , and  $n_{\text{fil}}$ , they estimate an upper bound for the number of bit errors  $n_{\text{bit}}$  and an upper bound for the number of phase errors  $n_{\text{ph}}$ , in the  $n_{\text{fil}}$  pairs. If these bounds are too large, they abort the protocol.

(8) They run an EDP that can produce  $n_{\text{key}}$  nearly perfect EPR pairs if the estimation is correct.

(9) Alice and Bob each measures the EPR pairs in Z basis to obtain a shared secret key.

In the following, we will reduce our protocol to the B92 protocol. Before this reduction, we should briefly mention what Alice and Bob do experimentally in the B92 protocol. In the B92 protocol, Alice randomly prepares the single-photon polarization in the state  $|\varphi_0\rangle$  or  $|\varphi_1\rangle$  and sends the state to Bob. After receiving the state, Bob performs measurement described by  $\mathcal{M}_{B92}^{L,\gamma}$ . When  $\gamma=\beta$  and Bob detects a single-photon state, this measurement effectively performs a polarization measurement on the single-photon state in a basis randomly chosen from  $\{|\varphi_0\rangle, |\bar{\varphi}_0\rangle\}$  and  $\{|\varphi_1\rangle, |\bar{\varphi}_1\rangle\}$ . In the case where  $\gamma=1$  and Bob detects a single-photon state, this measurement effectively performs a general measurement which describes the optimum unambiguous state discrimination between  $|\varphi_0\rangle$  and  $|\varphi_1\rangle$  [12].

Thanks to Bob's perfect detector, if the outcome of the QND measurement is  $s$ , then Bob's states are projected onto the single-photon space. This projection requires two more steps in our protocol compared to the *Protocol 1* in Ref. [10]. The benefit of this projection is that for the states projected onto qubit pairs Alice and Bob can use the one-way EDP based on CSS code [6]. In the context of QKD, this EDP allows Alice to perform Z-basis measurements immediately after she has prepared the state  $|\Psi\rangle_{AB}$  and Bob to perform Z-basis measurements immediately after he has performed the filtering. Now Bob's measurement is described by  $\mathcal{M}_{B92}^\gamma$ . Since Bob performs the QND measurement before the measurement  $\mathcal{M}_{B92}^\gamma$ , his measurement is equivalent to the measurement  $\mathcal{M}_{B92}^{L,\gamma}$ . As a whole, the protocol has been reduced into the protocol where Alice prepares and sends  $|\varphi_0\rangle$  or  $|\varphi_1\rangle$  randomly and Bob performs the  $\mathcal{M}_{B92}^{L,\gamma}$  measurement. This completes the reduction of our protocol into the generalized B92 protocol over lossy and noisy quantum channel.

Due to this equivalence, it is sufficient to prove the security of the protocol for the security analysis of the B92 protocol. The most important part in the quantitative security analysis of our protocol is to estimate phase errors and bit errors in the step (7). If this estimation is not exponentially reliable, then in the protocol Alice and Bob cannot distill the state sufficiently close to EPR state so that the protocol is not secure [5,6]. In the following section, we will give the formula to estimate the bit errors and phase errors.

### III. PHASE ERROR ESTIMATION FROM THE BIT ERROR

In this section, we consider the error estimations in the step (7) of the protocol. Thanks to Bob's perfect detector, the filtered states are qubit states, which allows us to directly apply some inequalities from Ref. [10].

First, note that bit errors  $n_{\text{bit}}$  in the data pairs could be determined if Alice measures those pairs in Z basis, Bob performs measurement  $\mathcal{M}_{B92}^\gamma$  onto those pairs, and they compare their results. Thus, the bit error rate in the check pairs and the bit error rate in the data pairs are determined by the same measurements. Furthermore thanks to the random

permutation in step (4), we can apply the classical probability estimation so that we obtain

$$|n_{\text{bit}} - n_{\text{err}}| \leq (1-L)N\epsilon_1. \quad (5)$$

For any strategy by Eve, the probability of violating this inequality is asymptotically less than  $\exp[-(1-L)N\epsilon_1^2]$ .

Since the POVM elements that give the bit error rate on the filtered states  $\Pi_{\text{bit}}$  and phase error rate on the filtered states  $\Pi_{\text{ph}}$  do not commute [13], the classical probability argument cannot be applied to the estimation of the phase errors from the bit errors. For the estimation, let us perform the gedanken measurements in the  $|i_x\rangle_A|j'_x\rangle_B$  basis ( $i=0,1, j'=0,1, v$ ), and let the numbers  $n_{ij'}$  of the pairs found in the state  $|i_x\rangle_A|j'_x\rangle_B$ . Here we define  $n_{iv}$  as the outcome where Alice obtains the bit value  $i$  and Bob obtains vacuum or multiphoton states. As far as we consider the measurement outcomes of the POVM elements that are diagonal with respect to  $|i_x\rangle_A|j'_x\rangle_B$  basis, we are allowed to apply the classical argument for the estimation. Thus, we have the following inequalities:

$$\left| \frac{\gamma^2}{\beta^2} [\alpha^2(n_{00} + n_{10}) + \beta^2(n_{01} + n_{11})] - n_{\text{fil}} \right| \leq (1-L)N\epsilon_2, \quad (6)$$

$$\left| \frac{\gamma^2}{\beta^2} (\alpha^2 n_{10} + \beta^2 n_{01}) - n_{\text{ph}} \right| \leq (1-L)N\epsilon_3, \quad (7)$$

which are violated with probability asymptotically less than  $\exp[-2(1-L)N\epsilon_2^2]$  and  $\exp[-2(1-L)N\epsilon_3^2]$ , respectively. Similarly, since neither the noisy channel nor Eve can touch the qubits held by Alice, we have

$$|\alpha^2 N - (n_{10} + n_{11} + n_{1v})| \leq N\epsilon_4, \quad (8)$$

with probability of violation asymptotically less than  $\exp(-2N\epsilon_4^2)$ .

In order to represent the bit error in the check pairs in terms of gedanken measurements, we introduce the global gedanken measurements in the basis  $|\Gamma_{ij}\rangle$  ( $i=0,1, j=0,1$ ) and the number of the corresponding measurement outcomes  $m_{ij}$ , where  $|\Gamma_{ij}\rangle \equiv (-1)^{ij} \beta |i_x\rangle_A |j_x\rangle_B + (-1)^{i(j+1)} \alpha |(i+1)_x\rangle_A |(j+1)_x\rangle_B$ . Here the summation is taken modulo 2. Since the POVM element for the bit error is diagonal with respect to the  $|\Gamma_{ij}\rangle$  basis [12], we have

$$\left| \frac{\gamma^2}{\beta^2} (m_{11} + m_{01}) - n_{\text{err}} \right| \leq (1-L)N\epsilon_5, \quad (9)$$

which is violated with probability asymptotically less than  $\exp[-2(1-L)N\epsilon_5^2]$ .

Since  $\{|\Gamma_{01}\rangle, |\Gamma_{10}\rangle\}$  and  $\{|0_x\rangle_A|1_x\rangle_B, |1_x\rangle_A|0_x\rangle_B\}$  span the same subspace, we can relate  $m_{10} + m_{01}$  and  $n_{10} + n_{01}$  by the classical probability estimate as

$$|(m_{10} + m_{01}) - (n_{10} + n_{01})| \leq (1-L)N\epsilon_6, \quad (10)$$

which is violated with probability asymptotically less than  $\exp[-(1-L)N\epsilon_6^2]$ . For the estimate of the phase error rate in the data qubit from the bit error rate in the check qubit,

we need to relate  $m_{01}/(m_{01} + m_{10})$  to  $n_{01}/(n_{01} + n_{10})$ . This relation cannot be obtained by classical arguments, since  $|\Gamma_{01}\rangle$  and  $|0_x\rangle_A|1_x\rangle_B$  are nonorthogonal. In Ref. [10], the authors consider the qubits that are invariant under the random permutation in the limit of large number. Then they showed that when we consider the measurement outcomes onto such qubits, we are allowed to regard the qubits as if they arose from the independently and identically distributed quantum source. Their argument can be directly applied to our case, since in step (4) of the protocol we have also applied the random permutation. Thus, we can make use of the exponentially reliable inequality derived in Ref. [10] as

$$\sin^2(\theta_l - \theta) - \epsilon_7 \leq \sin^2 \phi_l \leq \sin^2(\theta_l + \theta) + \epsilon_8 \quad (11)$$

for  $l=0,1$ , where all the angles are defined in  $[0, \pi/2]$  by the relations  $n_{11}/(n_{11} + n_{00}) = \sin^2 \theta_0$ ,  $n_{01}/(n_{01} + n_{10}) = \sin^2 \theta_1$ ,  $m_{11}/(m_{11} + m_{00}) = \sin^2 \phi_0$ ,  $m_{01}/(m_{01} + m_{10}) = \sin^2 \phi_1$ , and  $\alpha^2 = \sin^2 \theta$ .

The Eqs. (5)–(11), together with the relation  $\sum n_{ij'} = N$  and  $\sum m_{ij} = (1-L)N$  can be used to derive the formula for the estimation of the phase error from bit error. In the following we set  $\epsilon_i \rightarrow 0$  ( $i=1,2,\dots,8$ ) by taking the limit  $N \rightarrow \infty$  so that Eqs. (5)–(10) are now linear equations.

We first consider the special case for the B92 protocol where bit error rate in the filtered qubits is zero while the phase error rate in the qubits is not zero. Eve can accomplish this by using channel loss. From  $n_{\text{bit}}=0$ , i.e.,  $m_{11}=m_{01}=0$ , one can easily find that for  $n_{\text{fil}}/N = 2\alpha^2\gamma^2(1-L)$ ,

$$\max \left( \frac{n_{\text{ph}}}{n_{\text{fil}}} \right) \begin{cases} = \frac{\alpha^2}{\beta^2 - \alpha^2} \frac{L}{1-L} & \text{for } L \leq \beta^2 - \alpha^2 \\ \geq 1/2 & \text{for } L > \beta^2 - \alpha^2. \end{cases} \quad (12)$$

The limiting loss rate  $\beta^2 - \alpha^2$  coincides with the case where Eve employs optimum unambiguous state discrimination measurement [13]. In this attack, if she obtains the conclusive outcome, then she sends the corresponding state to Bob, otherwise she does not.

Next we consider the general case. The relationship can be obtained by solving the equations that we have mentioned just above. After straightforward calculations, we find the implicit constraint

$$\frac{\beta^2}{\gamma^2} |n_{\text{fil}} - 2n_{\text{err}}| \leq N\alpha \beta f(x),$$

where

$$f(x) \equiv \sqrt{(x-L_1)^2 - \left(-\Delta + \frac{L_1}{\alpha^2 - \beta^2}\right)^2} + \sqrt{(1-x-L_0)^2 - \left(\beta^2 - \alpha^2 - \Delta + \frac{L_0}{\alpha^2 - \beta^2}\right)^2},$$

$$\Delta \equiv [(\beta^2/\gamma^2)n_{\text{fil}}/N - 2\alpha^2\beta^2]/(\beta^2 - \alpha^2),$$

$$x \equiv (\beta^2/\gamma^2)2n_{\text{ph}}/N - (\beta^2 - \alpha^2)\Delta,$$

$$L_0 \equiv \alpha^2n_{1v}/N + \beta^2n_{0v}/N,$$

$$L_1 \equiv \alpha^2n_{0v}/N + \beta^2n_{1v}/N. \quad (13)$$

Here,  $x-L_1$  and  $1-x-L_0$  are equal to  $(n_{10}+n_{01})/N$  and  $(n_{00}+n_{11})/N$ , respectively, so that they must be positive. Combining these positivity constraints with the positivities inside the square roots, we have  $L_1 + |-\Delta + L_1/\alpha^2 - \beta^2| \leq x \leq 1-L_0 - |-\Delta - \alpha^2 + \beta^2 + L_0/\alpha^2 - \beta^2|$ . We can easily confirm that these equations are the same as equations in Ref. [10] where  $\gamma = \beta$  and the channel has no loss, i.e.,  $L_0=L_1=0$ . Equation (13) gives us the possible parameter set  $\{n_{\text{err}}, n_{\text{ph}}\}$  for fixed  $\alpha, \gamma, L_0, L_1, L$ , and  $n_{\text{fil}}$ . By taking the optimum ratio between  $L_0$  and  $L_1$  with respect to  $n_{\text{ph}}$  for given  $n_{\text{err}}, n_{\text{fil}}$ , and  $L$ , we obtain an upper bound  $\bar{n}_{\text{ph}}$  on the number of phase errors  $n_{\text{ph}}$ , as a function of the observed values  $n_{\text{err}}, n_{\text{fil}}$ , and  $L$ , and the chosen parameters  $\alpha$  and  $\gamma$ .

#### IV. EXAMPLES AND CONCLUSION

In this section, at first we give the examples of the phase error estimation and resulting performance of the B92 protocol.

To illustrate the accuracy of the phase error estimation and security performance of the B92 protocol, we assign values to the observable data as they would arise from a depolarizing quantum channel with loss, i.e., the state  $\rho$  evolves into  $L|V\rangle\langle V| + (1-L)[(1-p)\rho + \sum_{i=x,y,z} \sigma_i \rho \sigma_i]$ , where  $|V\rangle$  is the vacuum state,  $L$  is the loss rate of quantum channel,  $p$  is the depolarizing rate, and  $\sigma_i$  is the Pauli matrix. In Fig. 1, we show the upper bound of the estimated phase error rate, the actual phase error rate, and bit error rate for the case (a)  $p=0.01, L=0$  and (b)  $p=0.01, L=0.5$ . These figures are independent of  $\gamma$ , since we plot the phase error rates normalized by  $n_{\text{fil}}$  so that the prefactor  $\beta^2/\gamma^2$  is canceled. In each figure, it is seen that when  $|\langle\varphi_0|\varphi_1\rangle|^2$  becomes smaller, the estimation of the phase errors becomes poorer. On the other hand, larger values of  $|\langle\varphi_0|\varphi_1\rangle|^2$  make the signal more vulnerable to noise and loss. Furthermore, due to the loss, the estimation in (b) is poorer than that in (a), especially in the region for small  $|\langle\varphi_0|\varphi_1\rangle|^2$ .

Since Alice and Bob apply random permutation in the protocol, the achievable length of the final key is given by  $n_{\text{key}} = n_{\text{fil}}[1 - h(n_{\text{bit}}/n_{\text{fil}}) - h(\bar{n}_{\text{ph}}/n_{\text{fil}})]$  [10,14], when  $\bar{n}_{\text{ph}}/n_{\text{fil}} \leq 1/2$ . Here  $h(p) \equiv -p \log_2 p - (1-p) \log_2 (1-p)$ . The positivity of  $n_{\text{key}}$  means that Alice and Bob generate a secure key. In Fig. 2(a), we have numerically calculated the key generation rate  $G \equiv n_{\text{key}}/N$  in the case of  $\gamma = \beta$  for the fixed value of

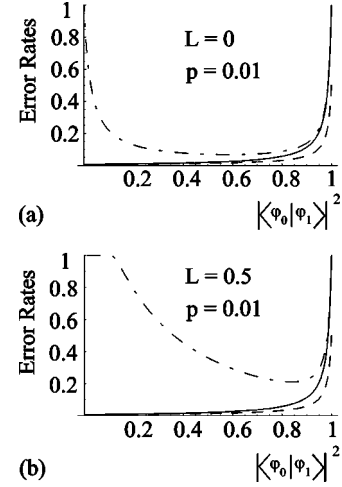


FIG. 1. The estimated phase error rate  $\bar{n}_{\text{ph}}/n_{\text{fil}}$  (dot-dashed line), the actual phase error rate (solid line), and bit error rate (dotted line) in case of  $p=0.01$ . (a) is for  $L=0$  and (b) is for  $L=0.5$ . We assume that quantum channel is a depolarizing channel with loss.

$|\langle\varphi_0|\varphi_1\rangle|^2, L$ , and  $p$ , and plot  $G$  optimized over  $|\langle\varphi_0|\varphi_1\rangle|^2$  as a function of  $p$ . The optimum value of  $|\langle\varphi_0|\varphi_1\rangle|^2$  is shown in Fig. 2(b). Since the optimization of the ratio between  $L_0$  and  $L_1$  is complicated, we have optimized the ratio numerically. From Fig. 2(a), it is seen that the B92 protocol as described here is secure up to  $p \sim 0.034$  (in the case of  $L=0$ ),  $p \sim 0.023$  (in the case of  $L=0.2$ ), and  $p \sim 0.012$  (in the case of  $L=0.5$ ). The use of the general B92 measurement, i.e.,  $\gamma=1$  yields the higher secret key gain, however this does not change the cutoff of the gain nor the optimum angle in Fig. 2(b). This is again because of the fact that the cutoff is determined by the error rate normalized by  $n_{\text{fil}}$ .

In the BB84 protocol or six-state protocol [15], thanks to the randomly chosen conjugate bases, phase error estimation is more precise than that in the B92 protocol. The poor estimation in the B92 protocol makes this protocol more vulnerable to eavesdropping. Actually, it is known that the BB84

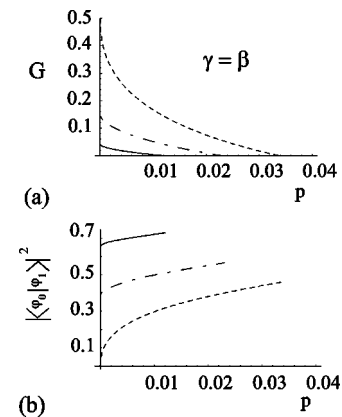


FIG. 2. (a) The optimum key generation rate  $G$  for the case  $\gamma = \beta$  and (b) the optimum value of  $|\langle\varphi_0|\varphi_1\rangle|^2$ . Here we assume that the quantum channel is the depolarizing channel with loss. The dotted line, the dot-dashed line, and solid line represent the case where  $L=0, L=0.2$ , and  $L=0.5$ , respectively.



protocol and six-state protocol are secure up to  $p \sim 0.165$  [6] and  $p \sim 0.1905$  [16] corresponding to bit error rates of 11% and 12.7%, respectively.

In summary, we have shown that the security proof of the B92 protocol over loss-free channel [10] can be adapted to lossy and noisy channels assuming Bob's detector that discriminates between single-photon states on one hand and vacuum state or multiphoton states on the other hand. We have derived the general formula for the estimation of the phase errors from bit errors. We have also shown that the boundary loss rate at which Eve can induce phase errors freely without inducing bit errors coincides with the case where Eve employs the optimum unambiguous state discrimination measurement. Finally, we have shown the examples of the security assuming the quantum channel is the depolarizing quantum channel with loss.

It is an interesting problem to compare our results to the case where Eve performs only individual attack. For the B92 protocol with loss, the security is estimated in Ref. [17]. However in that paper, it is assumed that Alice and Bob employ error discarding protocol so that we cannot compare

our result to their result directly. We leave this problem for future studies. Another interesting problem is to consider the case where Bob's detector is not perfect. In this case, some filtered states may remain vacuum state or multiphoton states so that our proof cannot be directly applied. The security analysis of the B92 protocol with coherent state is another interesting problem. We hope our study is helpful for solving these problems and we leave them for future studies.

#### ACKNOWLEDGMENTS

K.T. appreciates the warmth and hospitality of the Quantum Information Theory Group, Universität Erlangen-Nürnberg in Germany during his stay. We thank Marcos Curty, Peter van Loock, Philippe Raynal, and Aska Dolinska for helpful discussions. This work was supported in part by the Academic Frontiers Student Exchange Promotion Program under Grant No. 60 by the Ministry of Education, Culture, Sports, Science and Technology, Japan, and by the DFG under the Emmy-Noether programme.

- 
- [1] W. K. Wootters and W. H. Zurek, *Nature (London)* **299**, 802 (1982).
- [2] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publisher, Dordrecht, 1995).
- [3] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
- [4] D. Mayers, *Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 1996), Vol. 1109, p. 343; D. Mayers, *J. ACM* **48**, 351 (2001).
- [5] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
- [6] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
- [7] 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.
- [8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [9] A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996); A. M. Steane, *Proc. R. Soc. London, Ser. A* **452**, 2551 (1996).
- [10] K. Tamaki, M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **90**, 167904 (2003).
- [11] N. Gisin, *Phys. Lett. A* **210**, 151 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **78**, 574 (1997).
- [12] I. D. Ivanovic, *Phys. Lett. A* **123**, 257 (1987); D. Dieks, *ibid.* **126**, 303 (1988); A. Peres, *ibid.* **128**, 19 (1988).
- [13]  $\Pi_{\text{bit}}$  is given by  $(\gamma^2/2\beta^2)(|\Gamma_{11}\rangle\langle\Gamma_{11}| + |\Gamma_{01}\rangle\langle\Gamma_{01}|)$  (see the text for the definition of  $|\Gamma_{ij}\rangle$ ), while  $\Pi_{\text{ph}}$  is given by  $(\gamma^2/\beta^2)(\alpha^2|1_x\rangle_A\langle 1_x| \otimes |0_x\rangle_B\langle 0_x| + \beta^2|0_x\rangle_A\langle 0_x| \otimes |1_x\rangle_B\langle 1_x|)$ .
- [14] M. Hamada, e-print quant-ph/0308029.
- [15] D. Bruss, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [16] H.-K. Lo, *Quantum Inf. Comput.* **1**, 81 (2001).
- [17] K. Tamaki, M. Koashi, and N. Imoto, *Phys. Rev. A* **67**, 032310 (2003).