Attack of many eavesdroppers via optimal strategy in quantum cryptography

Eylee Jung, Mi-Ra Hwang, and DaeKil Park
Department of Physics, Kyungnam University, Masan, 631-701, Korea

Hungsoo Kim
Department of Applied Mathematics, Pukyong National University, Pusan, 606-737, Korea

Eui-Soon Yim
Department of Computer Science, Semyung University, Chechon, 390-711, Korea

Jin-Woo Son
Department of Mathematics, Kyungnam University, Masan, 631-701, Korea

(Received 14 January 2009; published 30 March 2009)

We examine a situation that n eavesdroppers attack the Bennett-Brassard cryptographic protocol via their own optimal and symmetric strategies. Information gain and mutual information with sender for each eavesdropper are explicitly derived. The receiver's error rate for the case of arbitrary n eavesdroppers can be derived using a recursive relation. Although the first eavesdropper can get mutual information without disturbance arising due to other eavesdroppers, subsequent eavesdropping generally increases the receiver's error rate. Other eavesdroppers cannot gain information on the input signal sufficiently. As a result, the information each eavesdropper gains becomes less than optimal one.

DOI: 10.1103/PhysRevA.79.032339 PACS number(s): 03.67.Dd, 03.65.−w

I. INTRODUCTION

Quantum cryptography is one of the major applications of quantum information theories [1,2]. While other applications such as quantum teleportation and quantum computer require tens or even thousands of qubits, the quantum cryptography scenario such as Bennett-Brassard 1984 (BB84) protocol [3] can be implemented, at least theoretically, using only single qubit technology. This is the main reason why the quantum cryptography based on BB84 or Ekert 1991 (Ekert91) [4] is now at the stage of the industrial era [5].

According to the usual BB84 protocol the sender (Alice) sends a single qubit to the receiver (Bob) by choosing randomly one of the conjugate bases $\{|x\rangle,|y\rangle\}$ and $\{|u\rangle,|v\rangle\}$, where

$$|u\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle), \quad |v\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle). \tag{1.1}$$

Then Bob performs a quantum-mechanical measurements in these bases. After measurements, Alice and Bob communicate with each other via classical public channel and establish a secret quantum key by using only those cases in which the bases of Alice and Bob coincide.

How much information an eavesdropper (Eve) can gain when Alice and Bob perform the usual BB84 scheme? The answer of this question is important to check the security of the quantum cryptography. In this reason many authors examined the various strategies with one- and two-dimensional probes [6–9]. Among them Ref. [9] derived the optimal (or maximal) mutual information between Alice and Eve as a function of the disturbance D in the BB84 protocol. The final result can be summarized as follows:

$$\mathcal{I}_{xy} = \frac{1}{2}\phi[2\sqrt{D_{uv}(1-D_{uv})}], \quad \mathcal{I}_{uv} = \frac{1}{2}\phi[2\sqrt{D_{xy}(1-D_{xy})}], \tag{1.2}$$

where $\mathcal{I}_{xy}$ (or $\mathcal{I}_{uv}$) is the optimal mutual information when Alice sends a signal to Bob via $x-y$ (or $u-v$) basis, and $\phi(z)=(1+z)\log_2(1+z)+(1-z)\log_2(1-z)$. The constants D_{xy} and D_{uv} denote the disturbances in these bases. The most different point of the quantum cryptography from the classical one is the fact that Eve cannot get information from the trusted parties without arising the disturbance. This implies that the quantum scheme is more secure than the classical cryptography.

Recently, many different cryptographic protocols have been studied from the purely theoretical ground (at least at current stage) even if most quantum cryptography has been demonstrated by making use of either one of BB84 or Ekert91 protocols. One of the motivations for searching other protocols is to strengthen the security against eavesdropping. The simple extended protocol is a six-state protocol [10,11]. In this protocol Alice sends a signal to Bob after choosing randomly one of three conjugate bases $\{|x\rangle,|y\rangle\}$, $\{|u\rangle,|v\rangle\}$, and $\{|w\rangle,|z\rangle\}$, where

$$|w\rangle = \frac{1}{\sqrt{2}}(|x\rangle + i|y\rangle), \quad |z\rangle = \frac{1}{\sqrt{2}}(|x\rangle - i|y\rangle). \tag{1.3}$$

The basis $\{|w\rangle,|z\rangle\}$ corresponds to the circular polarization if Alice and Bob use a photon polarization as a qubit. The optimal mutual information between Alice and Eve is plotted in Fig. 1, which implies that the six-state protocol is more secure than usual four-state BB84 against eavesdropping. Another extended protocol [12–15] is that Alice and Bob use

©2009 The American Physical Society

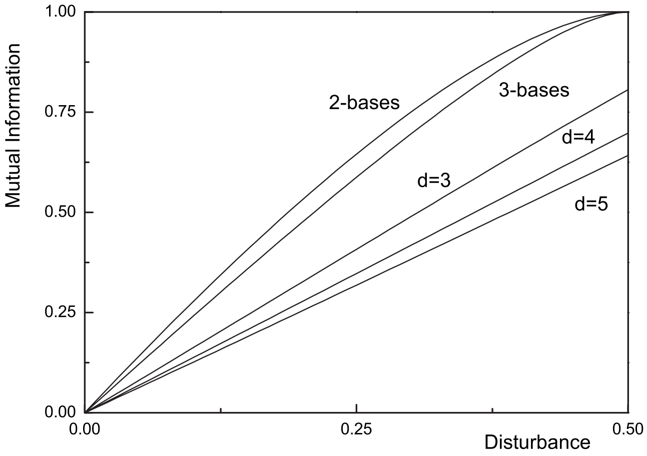

FIG. 1. Plot of D dependence of the optimal mutual information when Alice and Bob use the various different protocols.

qutrit ($d=3$) or more generally qudit ($d=4,5,\ldots$) instead of a qubit. The optimal mutual information in this protocol is also plotted in Fig. 1 when $d=3$, 4, and 5. Figure 1 indicates that the protocol with d-level system is more secure against eavesdropping with increasing d. Furthermore, the quantum cryptography with continuum [16] and noisy states [17] is under investigation. However, all of these other protocols seem to be far from embodiment in a few years from the aspect of experimental science.

In this paper we would like to explore the situation where many eavesdroppers (Eve1, Eve2, …) attack the BB84 protocol optimally. We assume that all of the eavesdroppers think they are unique eavesdropper. Our computation is based on the quantum circuit expression of the optimal eavesdropping strategy [18]. This paper is organized as follows. In Sec. II we review Ref. [18] briefly. In this section we develop a computational technique, which is useful when many eavesdroppers try to attack optimally. In Sec. III we examine the situation where Eve1 and Eve 2 attack the usual BB84 protocol. Information gain $G^{(i)}$ and mutual information $I^{(i)}$ are explicitly computed, where $i=1$ or 2 corresponds to Eve1 and Eve2, respectively. When Eve1 and Eve2 attack via symmetric optimal strategy, we compute Bob's error rate or disturbance $D_{\mathrm{B},2}$ explicitly, where the subscript "2" denotes the two eavesdroppers. It turns out that both optimal strategies fail. Although Eve1 can gain information on Alice's signal as much as possible, Eve2 increases the disturbance or Bob's error rate. For Eve2 she cannot gain information sufficiently due to Eve1's disturbance. In Sec. IV we examine the situation where three eavesdroppers attack the BB84 protocol. The mutual information for each eavesdropper is analytically derived. Furthermore, Bob's error rate $D_{\mathrm{B},3}$ is also explicitly derived on condition that all eavesdroppers use the symmetric strategies. In Sec. V we have generalized the results of the previous sections. When n eavesdroppers attack, the mutual information for each eavesdropper is analytically derived. Also the recursive relation of the Bob's error rate is derived. It turns out that all optimal strategies eavesdroppers choose eventually fail except very rare cases. Finally a brief concluding remark is given.

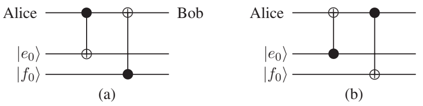

FIG. 2. Quantum circuit expression for the optimal eavesdropping strategy. (a) and (b) represent the optimal strategy when Alice sends a signal using $x-y$ or $u-v$ basis, respectively. The bottom two lines belong to Eve and the top line to Alice. Time advances from left to right.

II. ONE EAVESDROPPER

The quantum circuits for the optimal eavesdropping in $x-y$ and $u-v$ bases are given in Fig. 2. The top line belongs to Alice and Bob, and the bottom two lines to Eve. In order to perform the optimal eavesdropping strategy Eve prepares the initial states as following:

$$|e_0\rangle = \sqrt{1-\Delta_{uv}}|x\rangle + \sqrt{\Delta_{uv}}|y\rangle = \sqrt{1-D_{uv}}|u\rangle + \sqrt{D_{uv}}|v\rangle,$$

$$|f_0\rangle = \sqrt{1-D_{xy}}|x\rangle + \sqrt{D_{xy}}|y\rangle = \sqrt{1-\Delta_{xy}}|u\rangle + \sqrt{\Delta_{xy}}|v\rangle, \tag{2.1}$$

where Δ and D are related, when they have same subscripts, through the formula

$$\Delta = \frac{1}{2} - \sqrt{D(1-D)}, \quad D = \frac{1}{2} - \sqrt{\Delta(1-\Delta)}. \tag{2.2}$$

If Alice sends a signal using $x-y$ basis, Fig. 2(a) shows that the entangled states between Alice and Eve becomes

$$|x\rangle \to |X\rangle = \alpha_0|xxx\rangle + \alpha_1|yxy\rangle + \alpha_2|xyx\rangle + \alpha_3|yyy\rangle,$$

$$|y\rangle \to |Y\rangle = \alpha_0|yyx\rangle + \alpha_1|xyy\rangle + \alpha_2|yxx\rangle + \alpha_3|xxy\rangle, \tag{2.3}$$

where

$$\alpha_0 = \sqrt{1-\Delta_{uv}}\sqrt{1-D_{xy}}, \quad \alpha_1 = \sqrt{1-\Delta_{uv}}\sqrt{D_{xy}},$$

$$\alpha_2 = \sqrt{\Delta_{uv}}\sqrt{1-D_{xy}}, \quad \alpha_3 = \sqrt{\Delta_{uv}}\sqrt{\Delta_{xy}}. \tag{2.4}$$

For later use it is necessary to express Eq. (2.3) more compactly. This can be achieved by

$$|X\rangle = \sum_{i=0}^{3} \alpha_i|i\rangle_2|i\rangle_4, \quad |Y\rangle = \sum_{i=0}^{3} \alpha_i|i+1\rangle_2|i+2\rangle_4, \tag{2.5}$$

where $|j\rangle_2$ and $|j\rangle_4$ means $|j$ modulo $2\rangle$ and $|j$ modulo $4\rangle$. Thus $|j\rangle_2$ and $|j\rangle_4$ represents the one- and two-qubit states, respectively, with ordering x and y for $|j\rangle_2$ and xx, xy, yx, and yy for $|j\rangle_4$. This compact notation will be usefully used in the following sections when many eavesdroppers attack.

When Alice sends a signal using $u-v$ basis, the usual controlled-NOT gate changes

$$|uu\rangle \to |uu\rangle, \quad |uv\rangle \to |vv\rangle, \quad |vu\rangle \to |vu\rangle, \quad |vv\rangle \to |uv\rangle. \tag{2.6}$$

Thus the controlled-NOT gate in $x-y$ basis can be easily understood in $u-v$ basis by exchanging the control gate with target gate. This is a reason why Fig. 2(b) used in $u-v$ basis is different from Fig. 2(a).

Now, we want to show that the entangled states (2.3) with suitable positive operator-valued measure (POVM) measurement enables Eve to get information optimally. The complete set of the positive operators, which is used for POVM, can be derived generally as projective operators onto the eigenvectors of $\Gamma_{xy}=\rho_x-\rho_y$, where [19]

$$\rho_x = \mathrm{Tr}_{\mathrm{Alice}}|X\rangle\langle X|, \quad \rho_y = \mathrm{Tr}_{\mathrm{Alice}}|Y\rangle\langle Y|. \tag{2.7}$$

For our case the complete set of the positive operators is $\{E_0,E_1,E_2,E_3\}$ with $E_0=|xx\rangle\langle xx|$, $E_1=|xy\rangle\langle xy|$, $E_2=|yx\rangle\langle yx|$, and $E_3=|yy\rangle\langle yy|$. Then it is easy to compute $P_{\lambda i}=\langle I|\mathbb{1}\otimes E_\lambda|I\rangle$ with $I=X$ or Y and $i=x$ or y, which is the probability that Eve detects outcome λ when Alice sends a signal i,

$$P_{0x}=\alpha_0^2, \quad P_{1x}=\alpha_1^2, \quad P_{2x}=\alpha_2^2, \quad P_{3x}=\alpha_3^2,$$

$$P_{0y}=\alpha_2^2, \quad P_{1y}=\alpha_3^2, \quad P_{2y}=\alpha_0^2, \quad P_{3y}=\alpha_1^2. \tag{2.8}$$

Using Eq. (2.8), one can compute $q_\lambda=(1/2)(P_{\lambda x}+P_{\lambda y})$ and $Q_{i\lambda}=(1/2)P_{\lambda i}/q_\lambda$,

$$q_0=\frac{1}{2}(1-D_{xy}), \quad q_1=\frac{1}{2}D_{xy},$$

$$q_2=\frac{1}{2}(1-D_{xy}), \quad q_3=\frac{1}{2}D_{xy}, \tag{2.9}$$

and

$$Q_{x0}=1-\Delta_{uv}, \quad Q_{x1}=1-\Delta_{uv}, \quad Q_{x2}=\Delta_{uv}, \quad Q_{x3}=\Delta_{uv},$$

$$Q_{y0}=\Delta_{uv}, \quad Q_{y1}=\Delta_{uv}, \quad Q_{y2}=1-\Delta_{uv}, \quad Q_{y3}=1-\Delta_{uv}. \tag{2.10}$$

The quantity q_λ is a probability that Eve has outcome λ when Alice uses $x-y$ basis. The quantity $Q_{i\lambda}$ is posterior probability on Eve's guess after she has a outcome λ. Then the information gain is defined as $G_\lambda=|Q_{x\lambda}-Q_{y\lambda}|$, which, for our case, is λ independent,

$$G_\lambda=1-2\Delta_{uv}=2\sqrt{D_{uv}(1-D_{uv})}. \tag{2.11}$$

Thus, the mutual information $\mathcal{I}^{\mathrm{AE}}$ between Alice and Eve reduces to

$$\mathcal{I}^{\mathrm{AE}}\equiv\frac{1}{2}\sum_\lambda q_\lambda\phi(G_\lambda)=\frac{1}{2}\phi[2D_{uv}(1-D_{uv})], \tag{2.12}$$

where $\phi(z)=(1+z)\log_2(1+z)+(1-z)\log_2(1-z)$.

Now, let us derive Bob's error rate, usually called disturbance when Alice sends a signal using the $x-y$ basis. First, we consider the following quantities:

$$d_{\lambda u}\equiv 1-\frac{\langle U|B_u\otimes E_\lambda|U\rangle}{\langle U|\mathbb{1}\otimes E_\lambda|U\rangle}, \quad d_{\lambda v}\equiv 1-\frac{\langle V|B_v\otimes E_\lambda|V\rangle}{\langle V|\mathbb{1}\otimes E_\lambda|V\rangle}, \tag{2.13}$$

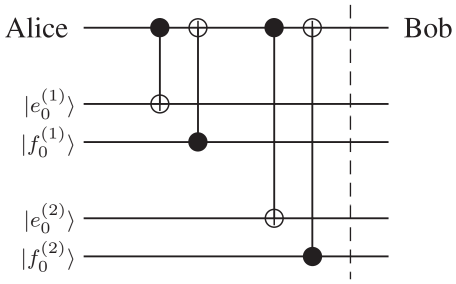

FIG. 3. Quantum circuit expression for the situation where two eavesdroppers Eve1 and Eve2 attack the usual BB84 protocol when Alice sends a signal to Bob using $x-y$ basis. The top line belongs to Alice, next two lines to Eve1, and bottom two lines to Eve2. If Alice uses a $u-v$ basis, this figure should be modified by exchanging the control gates with target gates in all controlled-NOT gates. Time advances from left to right.

where $|U\rangle=(1/\sqrt{2})(|X\rangle+|Y\rangle)$, $|V\rangle=(1/\sqrt{2})(|X\rangle-|Y\rangle)$, $B_u=|u\rangle\langle u|$, and $B_v=|v\rangle\langle v|$. These are probabilities Bob gets a wrong result *conditioned upon* Alice sending $|u\rangle$ or $|v\rangle$, and Eve measuring λ. Computation of $d_{\lambda u}$ and $d_{\lambda v}$ is straightforward. The result is that $d_{\lambda u}$ is identical to $d_{\lambda v}$ and they are also λ independent as follows:

$$d_{\lambda u}=d_{\lambda v}\equiv d_\lambda=D_{uv} \quad (\lambda=0,1,2,3). \tag{2.14}$$

Then Bob's error rate D_{B} is given by

$$D_{\mathrm{B}}\equiv\sum_\lambda q_\lambda d_\lambda=D_{uv}. \tag{2.15}$$

Thus Eq. (2.12) can be rewritten as

$$\mathcal{I}^{\mathrm{AE}}=\frac{1}{2}\phi[2D_{\mathrm{B}}(1-D_{\mathrm{B}})], \tag{2.16}$$

which is the optimal mutual information derived in Ref. [9] when Alice sends a signal using $x-y$ basis. If Alice uses $u-v$ basis, we should repeat the previous calculation using Fig. 2(b). The final result is identical with Eq. (2.16) except $D_{\mathrm{B}}=D_{xy}$. Thus, the strategies expressed by Fig. 2 give optimal information to Eve regardless of the basis Alice is using.

III. TWO EAVESDROPPERS

Now we consider a situation that two eavesdroppers, Eve1 and Eve2, attack the usual BB84 protocol. We assume that Eve1 and Eve2 do not know each other and they use their own optimal strategies. Thus corresponding quantum circuit should be Fig. 3 when Alice sends a signal using $x-y$ basis. From now on we will use the superscript (i) to distinguish the quantities (or states) which belong to Eve1 and Eve2.

Using the compact notation used in Eq. (2.5), one can derive the entangled states at the stage represented as a dotted line in Fig. 3,

$$|x\rangle \to |X\rangle = \sum_{i,j=0}^{3} \alpha_i^{(1)}\alpha_j^{(2)}|i+j\rangle_2|i\rangle_4|2i+j\rangle_4,$$

$$|y\rangle \to |Y\rangle = \sum_{i,j=0}^{3} \alpha_i^{(1)}\alpha_j^{(2)}|i+j+1\rangle_2|i+2\rangle_4|2i+j+2\rangle_4. \tag{3.1}$$

In order to derive the POVM elements for Eve1 we construct the operator

$$\Gamma_{xy}^{(1)} = \rho_x^{(1)} - \rho_y^{(1)}, \tag{3.2}$$

where

$$\rho_x^{(1)} = \mathrm{Tr}_{\mathrm{A,E2}}|X\rangle\langle X|, \quad \rho_y^{(1)} = \mathrm{Tr}_{\mathrm{A,E2}}|Y\rangle\langle Y|. \tag{3.3}$$

In Eq. (3.3) $\mathrm{Tr}_{\mathrm{A,E2}}$ means a partial trace over Alice and Eve2's qubits. Then it is easy to compute the eigenvectors of $\Gamma_{xy}^{(1)}$, which gives the complete set of the positive operators $\{E_0^{(1)},E_1^{(1)},E_2^{(1)},E_3^{(1)}\}$ to Eve1, where

$$E_0^{(1)} = |xx\rangle_{2,3}\langle xx|, \quad E_1^{(1)} = |xy\rangle_{2,3}\langle xy|,$$

$$E_2^{(1)} = |yx\rangle_{2,3}\langle yx|, \quad E_3^{(1)} = |yy\rangle_{2,3}\langle yy|. \tag{3.4}$$

The subscript 2,3 means qubits of second and third lines in Fig. 3. By same way one can construct the complete set of the positive operators for Eve2, which is

$$E_0^{(2)} = |xx\rangle_{4,5}\langle xx|, \quad E_1^{(2)} = |xy\rangle_{4,5}\langle xy|,$$

$$E_2^{(2)} = |yx\rangle_{4,5}\langle yx|, \quad E_3^{(2)} = |yy\rangle_{4,5}\langle yy|. \tag{3.5}$$

Then the remaining calculation for the mutual information $\mathcal{I}^{\mathrm{AE}_1}$ between Alice and Eve1, and $\mathcal{I}^{\mathrm{AE}_2}$ between Alice and Eve2 is straightforward. The information gains $G_\lambda^{(1)}$ for Eve1 and $G_\lambda^{(2)}$ for Eve2 turn out to be λ independent as follows:

$$G_\lambda^{(1)} = 1 - 2\Delta_{uv}^{(1)},$$

$$G_\lambda^{(2)} = (1-2\Delta_{uv}^{(2)})(1-2D_{xy}^{(1)}) \quad (\lambda = 0,1,2,3). \tag{3.6}$$

Therefore from a comparison of Eq. (3.6) with Eq. (2.11) Eve1 seems to be able to get information as much as the case of unique eavesdropper. This is due to the fact that Eve1 attacks the BB84 protocol earlier than Eve2 and therefore, gathers information without perturbation arising due to Eve2. However, this does not mean that Eve1's optimal strategy is succeeded. As shown in Fig. 1 optimality of the eavesdropping does not uniquely depend on the quantity of information that eavesdropper can gain. In order to get success in the eavesdropping, eavesdropper should decrease the disturbance as much as possible. These two factors, increase in information gain and decrease in disturbance, determine the success or failure of the optimal strategy. As will be shown shortly, Eve1's optimal strategy fails because Eve2 increases Bob's error rate. For Eve2 the information gain involves an interesting factor $1-D_{xy}^{(1)}$. Thus Eve2's information gain depends on the Eve1's choice of $D_{xy}^{(1)}$. This is manifestly due to the fact that Eve2 performs her optimal strategy after Eve1. If Eve1 chooses $D_{xy}^{(1)}=0$, Eve2 can get information as much as Eve1 if $\Delta_{uv}^{(1)}=\Delta_{uv}^{(2)}$. This indicates that Eve2 can increase her information gain if Eve1 does not disturb the signal Alice sent to Bob. The mutual information $\mathcal{I}^{\mathrm{AE}_1}$ and $\mathcal{I}^{\mathrm{AE}_2}$ reduce to

$$\mathcal{I}^{\mathrm{AE}_1} = \frac{1}{2}\phi(G_\lambda^{(1)}), \quad \mathcal{I}^{\mathrm{AE}_2} = \frac{1}{2}\phi(G_\lambda^{(2)}). \tag{3.7}$$

Now, let us turn to Bob's error rate. Unlike the unique eavesdropper case discussed in Sec. II the situation is very complicated. In this case it could happen that Eve1's disturbance and Eve2's successive disturbance does not generate an error to Bob. Thus equation corresponding to Eq. (2.13) in Sec. II should have one more index, i.e., $d_{\lambda u} \to d_{\lambda\lambda' u}$ and $d_{\lambda v} \to d_{\lambda\lambda' v}$. Since, furthermore, both optimal strategies Eve1 and Eve2 have chosen do not get success, we expect to have $d_{\lambda\lambda' u} \neq d_{\lambda\lambda' v}$. Thus we should compute the Bob's error rate separately when Alice sends $|u\rangle$ and $|v\rangle$. Since computation in this way needs long and tedious calculation, we will try to make the situation simpler.

To make the situation more simple we assume that both eavesdropping strategies are symmetric, i.e., $D_{xy}^{(1)}=D_{uv}^{(1)}$ and $D_{xy}^{(2)}=D_{uv}^{(2)}$. In this case we can compute Bob's error rate directly from the entangled states Eq. (3.1), which is

$$D_{\mathrm{B}} = D^{(1)}(1-D^{(2)}) + D^{(2)}(1-D^{(1)}). \tag{3.8}$$

In Eq. (3.8) we omit the subscript because it is useless in the symmetric strategies. If $D^{(2)}=0$, D_{B} becomes $D^{(1)}$ which is Bob's error rate if Eve1 is an unique eavesdropper. If $D^{(1)}=0$, D_{B} becomes $D^{(2)}$ which is also Bob's error rate if Eve2 is an unique eavesdropper. The general Bob's error rate becomes nice combination of $D^{(1)}$ and $D^{(2)}$.

Figure 4 is D_{B} dependent of $\mathcal{I}^{\mathrm{AE}_1}$ [Fig. 4(a)] and $\mathcal{I}^{\mathrm{AE}_2}$ [Fig. 4(b)]. We plot $\mathcal{I}^{\mathrm{AE}_1}$ in Fig. 4(a) when $D^{(2)}=0.1$, 0.2, and 0.3, respectively. For comparison we plot the optimal information $\mathcal{I}_{\mathrm{opt}}$ [see Eq. (1.2)] and mutual information $\mathcal{I}^{\mathrm{AB}}$ between Alice and Bob defined,

$$\mathcal{I}^{\mathrm{AB}} = 1 + D_{\mathrm{B}}\log_2 D_{\mathrm{B}} + (1-D_{\mathrm{B}})\log_2(1-D_{\mathrm{B}}), \tag{3.9}$$

together. As Fig. 4(a) indicates, Eve1's mutual information with Alice is in general smaller than $\mathcal{I}_{\mathrm{opt}}$ when $D^{(2)}\neq 0$. If $D^{(2)}$ approaches to zero, $\mathcal{I}^{\mathrm{AE}_1}$ approaches to $\mathcal{I}_{\mathrm{opt}}$. This means that failure of the Eve1's optimal strategy is only due to the fact that Eve2 increases the disturbance. We plot $\mathcal{I}^{\mathrm{AE}_2}$ in Fig. 4(b) when $D^{(1)}=0.1$, 0.2, and 0.3, respectively. For comparison we plot $\mathcal{I}_{\mathrm{opt}}$ and $\mathcal{I}^{\mathrm{AB}}$ together. As expected $\mathcal{I}^{\mathrm{AE}_2}$ approaches to $\mathcal{I}_{\mathrm{opt}}$ in the limit $D^{(1)}\to 0$. In this case, however, $\mathcal{I}^{\mathrm{AE}_2}$ decreases very rapidly compared to $\mathcal{I}^{\mathrm{AE}_1}$ with increasing $D^{(1)}$. This seems to be mainly due to the fact that Eve2's information gain is affected by Eve1 as shown in Eq. (3.6).

In Fig. 5 we plot $\mathcal{I}^{\mathrm{AE}_1}$ and $\mathcal{I}^{\mathrm{AE}_2}$ together as functions of $D^{(1)}$ and $D^{(2)}$. In most regions $\mathcal{I}^{\mathrm{AE}_1}$ is larger than $\mathcal{I}^{\mathrm{AE}_2}$. This is also due to the $D^{(1)}$ dependence of Eve2's information gain $G_\lambda^{(2)}$. In the small $D^{(1)}$ region, however, $\mathcal{I}^{\mathrm{AE}_2}$ becomes larger than $\mathcal{I}^{\mathrm{AE}_1}$. This is due to the fact that Eve1 cannot gain information without increasing $D^{(1)}$ as Eq. (3.6) indicates.

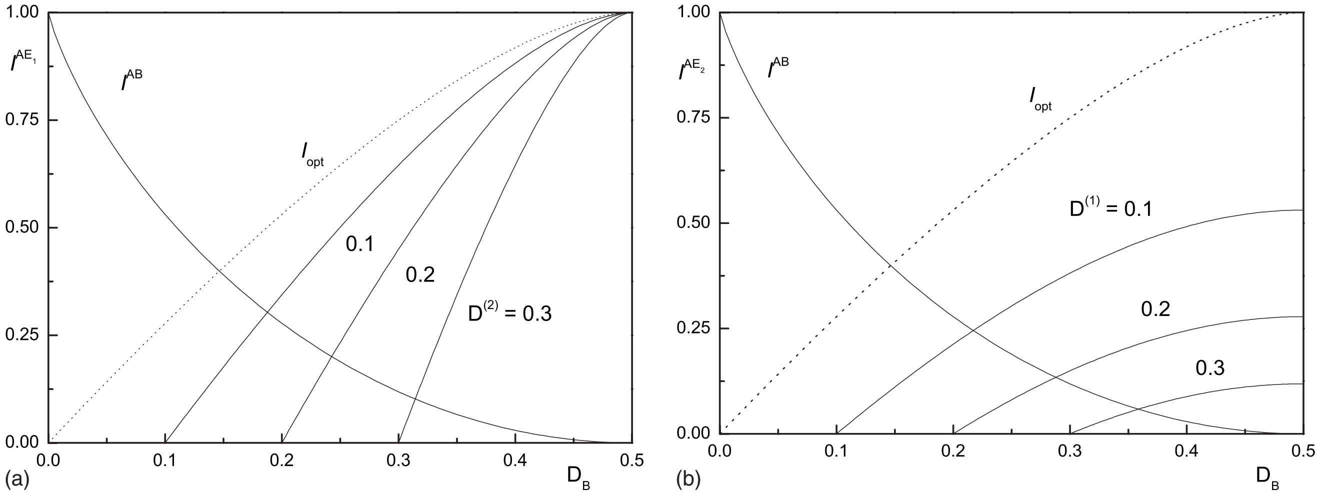

FIG. 4. Plot of D_B dependence of $\mathcal{I}^{AE_1}$ (a) and $\mathcal{I}^{AE_2}$ (b). The dotted line is a D_B dependence of the optimal strategy derived in Eq. (1.2). The monotonically decreasing line corresponds to $\mathcal{I}^{AB}$, mutual information between Alice and Bob. (a) implies that the mutual information of Eve1 is less than the optimal one except $D^{(2)}=0$. This is due to the fact that Eve2's eavesdropping process generally increases Bob's error rate. (b) implies that the mutual information of Eve2 is also less than the optimal one except $D^{(1)}=0$. This is due to the fact that Eve1's eavesdropping process generally decreases the information gain for Eve1.

IV. THREE EAVESDROPPERS

In this section we consider a situation that three eavesdroppers called Eve1, Eve2, and Eve3 attack the usual BB84 protocol. In Sec. III we assume that they think they are unique eavesdroppers and choose their own symmetric strategies. Thus corresponding quantum circuit should be Fig. 6 when Alice sends a signal using $x-y$ basis.

Using the compact notation used in Eq. (2.5), one can derive the entangled states at the stage represented as a dotted line in Fig. 6. The final result becomes

$$|x\rangle \to |X\rangle = \sum_{i,j,k=0}^{3} \alpha_i^{(1)}\alpha_j^{(2)}\alpha_k^{(3)}|i+j+k\rangle_2|i\rangle_4|2i+j\rangle_4 \times|2i+2j+k\rangle_4,$$

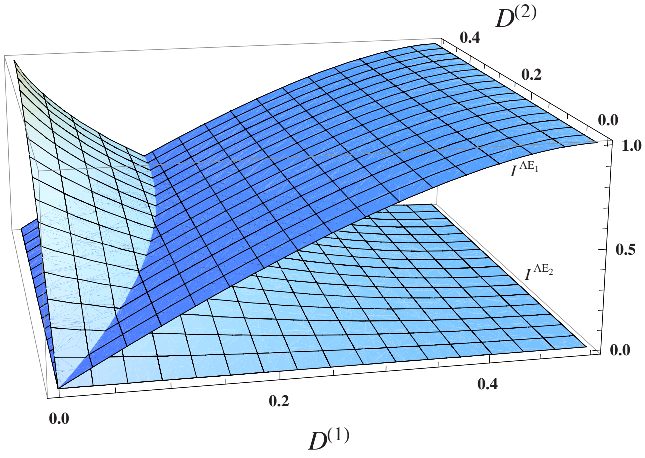

FIG. 5. (Color online) The $D^{(1)}$ and $D^{(2)}$ dependences of $\mathcal{I}^{AE_1}$ and $\mathcal{I}^{AE_2}$. In most regions $\mathcal{I}^{AE_1}$ is larger than $\mathcal{I}^{AE_2}$. This seems to be mainly due to the factor $1-D_{xy}^{(1)}$ in Eq. (3.6). However, in the small $D^{(1)}$ region $\mathcal{I}^{AE_2}$ becomes larger than $\mathcal{I}^{AE_1}$ because this multiplication factor becomes nearly unit in this region.

$$|y\rangle \to |Y\rangle = \sum_{i,j,k=0}^{3} \alpha_i^{(1)}\alpha_j^{(2)}\alpha_k^{(3)}|i+j+k+1\rangle_2|i+2\rangle_4|2i+j+2\rangle_4 \times|2i+2j+k+2\rangle_4. \tag{4.1}$$

Then, it is straightforward to construct the complete sets of the positive operators for eavesdroppers' POVM measurements. Following the similar calculational procedure, one can compute the information gain for each eavesdropper. The final result can be summarized as follows:

$$G_\lambda^{(1)} = 1 - 2\Delta^{(1)} = 2\sqrt{D^{(1)}(1-D^{(1)})},$$

$$G_\lambda^{(2)} = (1-2\Delta^{(2)})(1-2D^{(1)}) = 2(1-2D^{(1)})\sqrt{D^{(2)}(1-D^{(2)})},$$

$$G_\lambda^{(3)} = (1-2\Delta^{(3)})(1-2D^{(1)})(1-2D^{(2)}) = 2(1-2D^{(1)})(1-2D^{(2)})\sqrt{D^{(3)}(1-D^{(3)})}. \tag{4.2}$$

Note that we remove all subscripts because they are not nec-

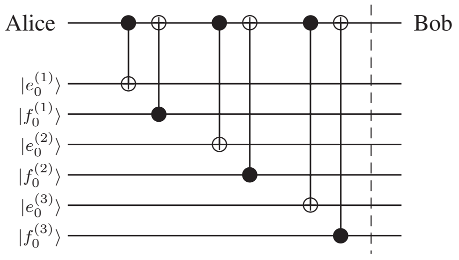

FIG. 6. Quantum circuit expression for the situation where three eavesdroppers Eve1, Eve2, and Eve3 attack the usual BB84 protocol when Alice sends a signal to Bob using $x-y$ basis. The top line belongs to Alice, next two lines to Eve1, next two lines to Eve2 and bottom two lines to Eve3. Time advances from left to right.

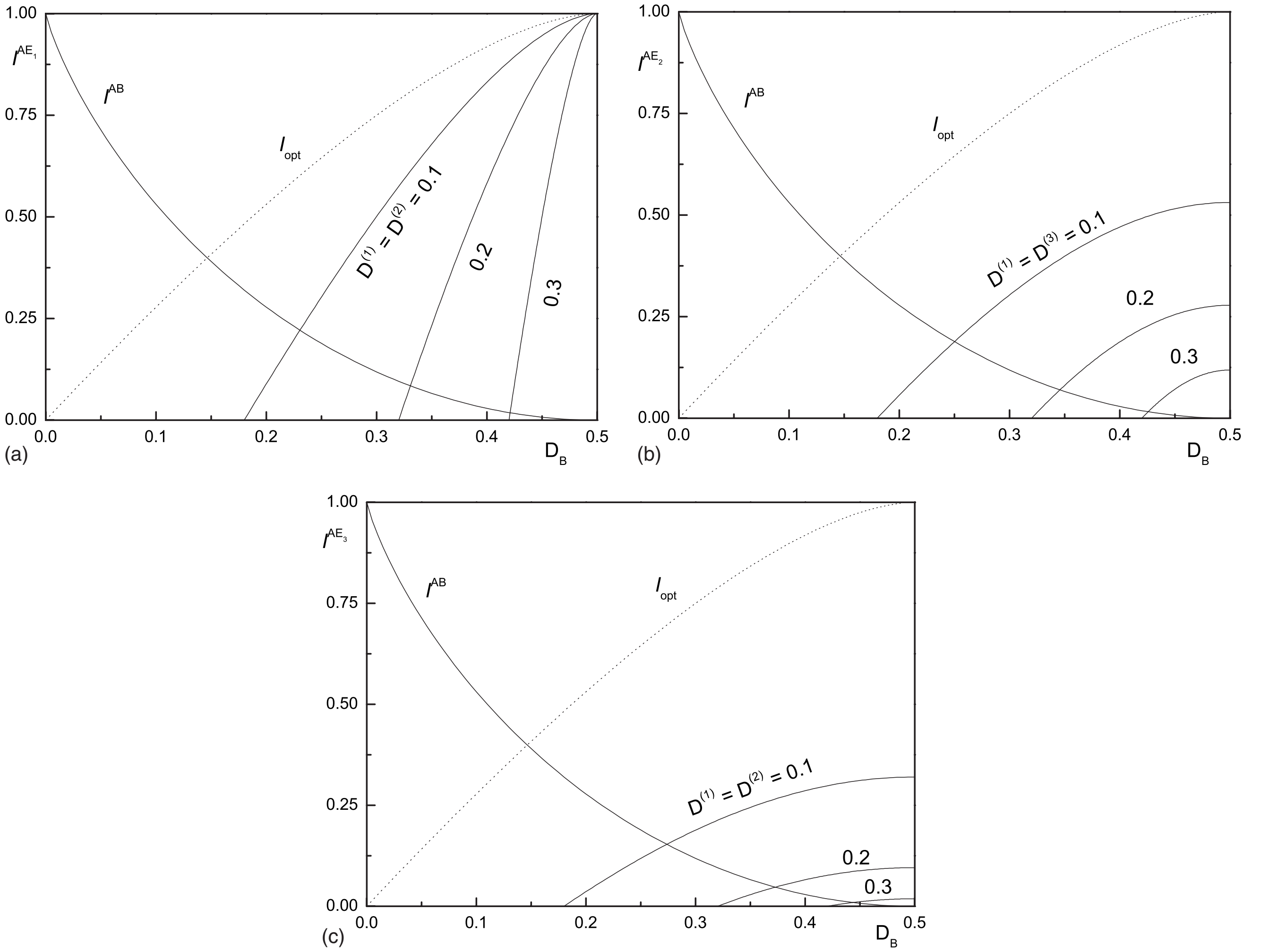

FIG. 7. Plot of D_B dependence of $\mathcal{I}^{AE_1}$ (a), $\mathcal{I}^{AE_2}$ (b), and $\mathcal{I}^{AE_3}$ (c). The optimal mutual information $\mathcal{I}_{opt}$ and Bob's mutual information $\mathcal{I}^{AB}$ are plotted together for comparison. This figure indicates that all optimal strategies performed by Eve1, Eve2, and Eve3 turn out fail.

essary in the symmetric strategy. Equation (4.2) exhibits a simple pattern: the information gain for each eavesdropper is a multiplication of her own $1-2\Delta$ factor with $1-2D$ factor of other eavesdroppers who perform their own strategies earlier. Using this rule, we can compute the information gains when n eavesdroppers attack with arbitrary number n without explicit calculation. The mutual information $\mathcal{I}^{AE_1}$, $\mathcal{I}^{AE_2}$, and $\mathcal{I}^{AE_3}$ reduce to

$$\mathcal{I}^{AE_1} = \frac{1}{2}\phi(G_\lambda^{(1)}), \quad \mathcal{I}^{AE_2} = \frac{1}{2}\phi(G_\lambda^{(2)}), \quad \mathcal{I}^{AE_3} = \frac{1}{2}\phi(G_\lambda^{(3)}). \tag{4.3}$$

Finally Bob's error rate D_B can be read straightforwardly from Eq. (4.1),

$$D_B = [D^{(1)}(1-D^{(2)}) + D^{(2)}(1-D^{(1)})](1-D^{(3)}) + [D^{(1)}D^{(2)} + (1-D^{(1)})(1-D^{(2)})]D^{(3)}. \tag{4.4}$$

When $D^{(3)}=0$, Eq. (4.4) exactly coincides with Eq. (3.8). If, furthermore, $D^{(1)}=0$ or $D^{(2)}=0$, Eq. (4.4) reduces to Eq. (3.8) with changing only Eve index.

Figure 7 is the plot of D_B dependence of $\mathcal{I}^{AE_1}$ [Fig. 7(a)], $\mathcal{I}^{AE_2}$ [Fig. 7(b)], and $\mathcal{I}^{AE_3}$ [Fig. 7(c)]. We fixed $D^{(2)}=D^{(3)}=0.1$, 0.2, and 0.3 in Fig. 7(a), $D^{(1)}=D^{(3)}=0.1$, 0.2, and 0.3 in Fig. 7(b), and $D^{(1)}=D^{(2)}=0.1$, 0.2, and 0.3 in Fig. 7(c). For comparison the optimal mutual information $\mathcal{I}_{opt}$ and Bob's information $\mathcal{I}^{AB}$ are plotted together. As Fig. 7 indicates, all optimal strategies turn out to fail. Especially, Eve3 gains very little information compared to optimal one. This is mainly due to the fact that Eve1 and Eve2 disturb Alice's signal before Eve3 starts her optimal strategy. Comparison of Fig. 7 with Fig. 4 indicates that mutual information in the case of three eavesdroppers is overall less than those in the case of two eavesdroppers. This seems to be due to the fact that Eve3's disturbance of Alice's signal decreases $\mathcal{I}^{AE_1}$ and $\mathcal{I}^{AE_2}$ in the disturbance-information diagram.

V. CONCLUSION

In this paper we have examined the situation that many eavesdroppers attack usual BB84 protocol via their own symmetric optimal strategies. If the number of eavesdroppers

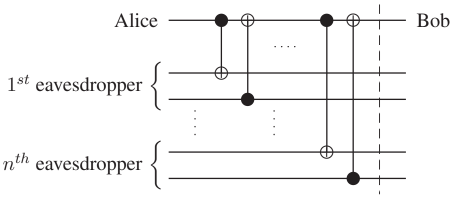

FIG. 8. Schematic for the situation that n eavesdroppers optimally attack the usual BB84 protocol performed by two trusted parties, Alice and Bob. We assume that Alice sends a signal using $x-y$ basis. If Alice uses $u-v$ basis, this diagram should be modified by exchanging all control gates with target gates.

is arbitrarily n as shown in Fig. 8, Eqs. (2.11), (3.6), and (4.2) imply that their information gains are

$$G^{(j)}=(1-2\Delta^{(j)})(1-2D^{(1)})\cdots(1-2D^{(j-1)}) \quad (j=1,\ldots,n), \tag{5.1}$$

and their mutual information with Alice are

$$\mathcal{I}^{(j)}=\frac{1}{2}\phi(G^{(j)}) \quad (j=1,\ldots,n). \tag{5.2}$$

Furthermore, Eqs. (2.15), (3.8), and (4.4) imply that Bob's error rate in the presence of n eavesdroppers can be computed as follows. In order to distinguish the number of eavesdroppers in the Bob's error rate, we use one more index such as $D_{B,j}$, which is Bob's error rate when j eavesdroppers attack with symmetric optimal strategies. Then $D_{B,n}$ can be computed from $D_{B,n-1}$ by a recursion relation,

$$D_{B,n}=D_{B,n-1}(1-D^{(n)})+D_{B,n-1}|_{D^{(n-1)}\rightarrow 1-D^{(n-1)}}D^{(n)}. \tag{5.3}$$

Since we know $D_{B,1}$ exactly, one can compute $D_{B,n}$ recursively.

Equations (5.2) and (5.3) enable us to plot the disturbance-information diagram for any eavesdroppers. As commented already in previous sections, all eavesdroppers' optimal strategies cannot succeed eventually except very rare cases. Although the first eavesdropper can obtain mutual information without disturbance arisen due to the other eavesdroppers, subsequent eavesdroppers increase Bob's error rate. This makes the mutual information of the first eavesdropper lower than the optimal one in the disturbance-information diagram except $D^{(2)}=\cdots=D^{(n)}=0$. The last eavesdropper cannot gain information due to the disturbance of Alice's signal arising due to the previous eavesdroppings. Thus the last eavesdropper's optimal strategy fails except $D^{(1)}=\cdots=D^{(n-1)}=0$. Similar reasons make all optimal strategies fail.

It seems to be of interest to extend our results to the case of asymmetric eavesdropping. Probably it needs very long and tedious calculation. Furthermore, asymmetric eavesdropping strategy may be not important practically because Alice and Bob can notice the presence of eavesdropper more easily than the symmetric case. However, from the purely theoretical point of view it is interesting issue because it may give origin of information gain and Bob's error rate.

Although much attention has been paid to the optimal strategy in the various protocol, the properties of the nonoptimal case are not examined sufficiently. Since, however, the effect of decoherence makes it impossible for eavesdropper to perform the exactly optimal one, it seems to be more important to explore the strategies near to optimal from the aspect of the practical reason. Recently, it is found [20] that the quantum resonance occurs in the Bob's error rate when Eve takes a near-optimal strategy. We believe that there are other new and interesting properties in the eavesdropping strategies near to optimal one. We would like to explore this issue in the future.

ACKNOWLEDGMENT

This work was supported by the Kyungnam University Foundation Grant, 2008.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[3] C. H. Bennett and G. Brassard, in *Quantum Cryptography, Public Key Distribution and Coin Tossings*, Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, A. Leverrier, N. Lutkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, e-print arXiv:quant-ph/0701168.
[6] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[7] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).
[8] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).
[9] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[10] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[11] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[12] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[13] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[14] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, J. Phys. A **35**, 10065 (2002).
[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[16] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett.

101, 200504 (2008).

[17] Z. Shadman, H. Kampermann, T. Meyer, and D. Bruss, e-print arXiv:0804.0587.

[18] R. B. Griffiths and C. S. Niu, Phys. Rev. A **56**, 1173 (1997).

[19] C. A. Fuchs, e-print arXiv:quant-ph/9611010.

[20] E. Jung, M. Hwang, D. Park, H. Kim, J. Son, E. Yim, S. Cha, S. Tamaryan, and S. Yoo, e-print arXiv:0901.0237.