A counter-intuitive phenomenon in Eve's information gain in two-state quantum communication

Kiyoshi Tamaki *, Masato Koashi and Nobuyuki Imoto

CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences,
SOKENDAI, The Graduate Univ. for Advanced Studies, Hayama, Kanagawa, 240-0193, Japan

We consider the situation that Alice sends Bob single photons, each of which randomly takes one of the two nonorthogonal polarization states $|0\rangle$ and $|1\rangle$, through the depolarizing channel with losses. Our problem is to determine the maximum information on correctly transmitted bits that can be extracted by Eve who stands between Alice and Bob, and simulates this channel. We first briefly report the optimization of Eve's information gain on correctly transmitted bits, and then report counter-intuitive behavior of Eve's information gain, that is, when the angle between Alice's two states is small, Eve's information gain decreases as the noises due to the back-action of her attempt to extract information get larger. We give an information-theoretical explanation that justifies this behavior from another point of view.

* e-mail: ktamaki@koryuw01.soken.ac.jp

We consider the following problem. Let $|0\rangle$ and $|1\rangle$ be two nonorthogonal single-photon polarization states, Alice determines a bit value $j=0$ or $j=1$ randomly, and sends the state $|j\rangle$ to Bob through the depolarizing channel with losses, i.e., Bob receives the mixed state ρ_j of the partially depolarized single-photon state and the vacuum. Eve replaces this channel by an ideal one and tries to extract information on Alice's and Bob's data while leaving the state ρ_j to Bob so that she hides her presence. In this case, how much information on the bits where Alice and Bob share the identical bit value (in the following, we call these bits as correct bits) can Eve extract?

This problem is important for the security proof of the practical quantum key distribution (QKD). In this scheme, if the maximum amount of information that can be extracted by Eve is estimated, we can perform a secure key distribution by virtue of the technique of classical imformation theory, such as privacy amplification. In relation to QKD, our problem corresponds to the estimation of the security against individual attack in the B92 protocol [2] based on photon polarization.

The outline of our study is as follows. We first obtain Eve's optimum information gain for correct bits by Lagrange's method of undetermined multipliers. Since the noises introduced by Eve are the back-action of her attempt to extract information, it might be expected that information gain increases as these noises increase. However, we find the counter-intuitive phenomenon that Eve's information gain decreases as these noises get larger when the angle between two states $|0\rangle$ and $|1\rangle$ is small. To clarify the mechanism behind this phenomenon, we give an explanation from the viewpoint of the information theory.

Since the state of the polarization of a single-photon and that of spin-$\frac{1}{2}$ particle have one to one correspondense, we use the spin-$\frac{1}{2}$ states to describe Alice's state $|0\rangle$ and $|1\rangle$ as

$$\begin{aligned} |0\rangle &\equiv \cos\frac{\alpha}{2}|z+\rangle - \sin\frac{\alpha}{2}|z-\rangle\,, \\ |1\rangle &\equiv \cos\frac{\alpha}{2}|z+\rangle + \sin\frac{\alpha}{2}|z-\rangle\,, \end{aligned}$$

where $|\,z+\,\rangle$ and $|\,z-\,\rangle$ are the eigenstates of σ_z (z component of Pauli matrix) whose eigenvalues are $+1$ and -1, respectively. α is the angle between $|0\rangle$ and $|\,z+\,\rangle$ on the x-z plane in the Bloch sphere, and also characterizes the nonorthogonality between the two states, such that

$$\langle 0|1\rangle = \cos\alpha\,.$$

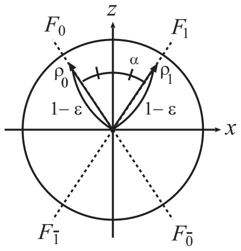

Figure 1: The states recieved by Bob and his measurement bases in the Bloch sphere.

After the noisy channel, $|j\rangle$ turns into a mixed state with the density matrix ρ_j which can be written by

$$\rho_j \;=\; T\left[(1-\epsilon)\,|j\rangle\langle j| + \epsilon\frac{\mathbf{1}}{2}\right] + (1-T)|\mathrm{vac}\rangle\langle\mathrm{vac}|\,, \tag{1}$$

where $\mathbf{1}$ is the identity operator which stands for random quantum noises, $|\mathrm{vac}\rangle$ is the vacuum state, and T is the probability that Bob recieves the single-photon states. These density matrices are shown in Fig. 1.

Eve replaces the noisy channel by an ideal one, prepares auxiliary system, interacts this system with Alice's particle, and sends Bob the density matrix ρ_j while she performs the optimum measurements on her system to extract information.

Next, we describe Bob's measurement. Bob measures the polarization on the basis $\{|0\rangle, |\overline{0}\rangle\}$ or $\{|1\rangle, |\overline{1}\rangle\}$, which is selected randomly. Here $|\overline{0}\rangle$ and $|\overline{1}\rangle$ are defined as

$$\begin{aligned} |\overline{0}\rangle &\equiv \sin\frac{\alpha}{2}|z+\rangle + \cos\frac{\alpha}{2}|z-\rangle, \\ |\overline{1}\rangle &\equiv \sin\frac{\alpha}{2}|z+\rangle - \cos\frac{\alpha}{2}|z-\rangle\,. \end{aligned}$$

The whole measurement process is described by the following POVM [5]

$$F_i \equiv \frac{1}{2}\,|i\rangle\langle i|\,, \quad F_{\mathrm{V}} \equiv 1 - \sum_{i=0,1,\overline{0},\overline{1}} F_i\,,$$

where $i = 0, 1, \overline{0}, \overline{1}$, and "V" means the vacuum states. F_i and $F_{\overline{i}}$ ($i = 0, 1$) are shown in Fig. 1 schematically using Bloch sphere. We call the events conclusive where Bob's outcome of POVM is $\overline{0}$ or $\overline{1}$. In the events where Alice sends $j(=0,1)$ and Bob receives $\overline{j}$, Alice and Bob obtain identical bit values, which we call the correct bits.

Using Schmidt decomposition, Eq. (1) leads to the expressions of the total pure states

$$\begin{aligned} U|\,0\rangle\,|\,w\rangle_{\rm E} &= \sqrt{T\,\left(1-\frac{\epsilon}{2}\right)}\,|0\rangle\,|a_1\rangle_{\rm E} \\ &+ \sqrt{T\,\frac{\epsilon}{2}}|\overline{0}\rangle\,|\,a_2\,\rangle_{\rm E} + \sqrt{1-T}|\,{\rm vac}\rangle\,|\,a_{\rm v}\rangle_{\rm E}\,, \end{aligned}$$

and

$$\begin{aligned} U|\,1\rangle\,|\,w\rangle_{\rm E} &= \sqrt{T\,\left(1-\frac{\epsilon}{2}\right)}\,|1\rangle\,|\,b_1\,\rangle_{\rm E} \\ &+ \sqrt{T\,\frac{\epsilon}{2}}|\,\overline{1}\rangle\,|\,b_2\,\rangle_{\rm E} + \sqrt{1-T}|\,{\rm vac}\rangle\,|\,b_{\rm v}\rangle_{\rm E} \end{aligned}$$

where $|\,a_i\rangle_{\rm E}$ and $|\,b_i\rangle_{\rm E}(i=1,2)$ are orthogonal to the space spanned by $|\,a_{\rm v}\rangle_{\rm E}$ and $|\,b_{\rm v}\rangle_{\rm E}$, since Eve knows the photon number she has sent. $|a_i\rangle_{\rm E}$ and $|b_i\rangle_{\rm E}(i=1,2)$ satisfy

$${}_{\rm E}\langle a_i|\,a_j\rangle_{\rm E} = \delta_{i,j},\ \ {}_{\rm E}\langle b_i|\,b_j\,\rangle_{\rm E} = \delta_{i,j},\ \ |\,b_i\rangle_{\rm E} = \hat{\xi}|\,a_i\rangle_{\rm E},$$

where $\hat{\xi}$ is the unitary operator that relates them.

For the correct bits, the state of Eve's probe when the bit value is 0 is a pure state $C_0\langle\overline{1}\,|\,U\,|\,0\,\rangle\,|\,w\,\rangle_{\rm E} \equiv |\,\phi_0\rangle_{\rm E}$, and the state when the bit value is 1 is $C_1\langle\overline{0}\,|U\,|\,1\,\rangle\,|\,w\,\rangle_{\rm E} \equiv |\,\phi_1\rangle_{\rm E}$, where C_0 and C_1 are constants for normalization. The optimum measurement which maximizes the information extracted from two pure states has already been known [3, 6], and this measurement yields the information gain with respect to Shannon entropy as

$${\rm I}_{\rm S}^{\rm Gc} \ \ \equiv\ \ 1-[-p_e\log_2 p_e-(1-p_e)\log_2(1-p_e)]\ ,$$

where p_e is given by

$$p_e = \frac{1-\sqrt{1-|Q|^2}}{2}\ , \quad (Q\equiv {}_{\rm E}\langle\,\phi_0\,|\,\phi_1\,\rangle_{\rm E})\ .$$

To obtain the maximum information gain, we have to optimize U such that $|Q|$ takes the minimum value. We have solved this problem by Lagrange's method of undetermined multipliers, and we plot this optimum information gain as a function of ϵ as in Fig. 2 in the cases of $\alpha=45°, T=0.8$ and $\alpha=10°, T=0.3$. Since the parameter ϵ corresponds to the noises due to the back-action of her attempt to extract information, it might be expected that Eve's information gain increases when ϵ gets larger. But, the behavior of the information gain in the right figure of Fig. 2 is counter-intuitive, namely, there exist regions where increase of noises reduces Eve's information gain.

In order to explain this counter-intuitive phenomena, we consider the mutual information between Eve and the joint system of Alice and Bob for the conclusive bits, i.e., ${\rm I(E;A,B|conc)}$. Using the simple relationship between the entropy and the mutual information, this is upper bounded as follows.

$${\rm I(E;A,B|conc)} \leq {\rm I(A;B,E|conc)} + {\rm I(B;E|conc)}\,.$$

Because of the nonorthogonality of Alice's states and that of Bob's POVM elements, both ${\rm I(A;B,E|conc)}$ and ${\rm I(B;E|conc)}$ have an upper bound and so ${\rm I(E;A,B|conc)}$ does. Quantitatively, this upper bound ($\equiv\nu$)can be written as

$$\left[\frac{1-h\left(\frac{1-\sqrt{1-\cos^2\alpha}}{2}\right)}{P_{\rm conc}}\right] + \left[1 -h\left(\frac{1}{2}-\frac{\sin\alpha}{4(P_{\rm conc}/T)}\sqrt{1-\left(\frac{2(P_{\rm conc}/T)-1}{\cos\alpha}\right)^2}\right)\right]$$

where $h(x)$ is the entropy function and $P_{\rm conc}$ is the probability that Bob obtains conclusive results.

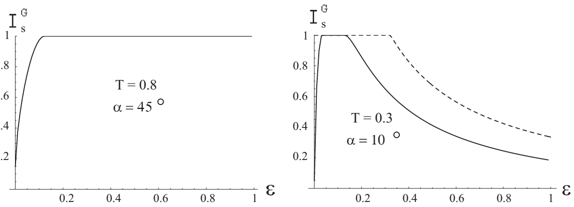

Figure 2: Eve's maximum information gain ${\rm I}_S^G$ vs ϵ when $\alpha=45°, T=0.8$ (left) and $\alpha=10°, T=0.3$ (right). The dashed line is the information bound based on Eq. (2).

The optimum total Shannon information gain for correct bits is $nP_{\rm conc}(1-e){\rm I}_{\rm S}^{\rm G}$ where n is the number of pulses that Alice sends to Bob and e is the bit error rate, which is determined by ϵ and α. The total Shannon information gain $nP_{\rm conc}(1-e){\rm I}_{\rm S}^{\rm G}$ is no greater than the total Shannon information gain for conclusive bits $nP_{\rm conc}\nu$ so that

$${\rm I}_{\rm S}^{\rm G} \leq \frac{\nu}{1-e} \equiv {\rm I}_{\rm S}^{\rm upper}\,. \qquad (2)$$

In Fig. 2, we plot this information bound ${\rm I}_{\rm S}^{\rm upper}$ by the dashed line. The dashed line decreases as ϵ gets larger. Intuitively, this behavior can be explained as follows. Note that ϵ represents the random noises and since Alice's two input states are almost identical for small α, Bob's recieved states are almost identical for large ϵ so that the measurement outcomes of Bob are almost independent of the states Alice has sent. Thus, this situation is almost equivalent to that Alice and Bob independently determine the bit value randomly. In this case, all Eve can do is just guessing their bit value, and then Eve's information gain is very low.

References

[1] C. H. Bennett *et al.*, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[2] C. H. Bennett, Phys. Rev. Lett, **68**, 3121 (1992).

[3] B. A. Slutsky *et al.* Phys. Rev. A, **57**, 2383 (1998).

[4] C. A. Fuchs *et al.* Phys. Rev. A **53**, 2038 (1996).

[5] J. Preskill,
http://www.theory.caltech.edu/people/preskill
/ph229/ .

[6] L. B. Levitin, in Quantum Communication and Measurement, edited by V. P. Belavkin, O. Hirota, and R. Hudson (Plenum, New York, 1995), pp.439-448.