Unconditionally Security of the Bennett 1992 quantum-key distribution

Kiyoshi Tamaki[1], Masato Koashi[1], Nobuyuki Imoto[1], and Norbert Lütkenhaus[2]
[1] *The Graduate University for Advanced Studies (SOKENDAI), Hayama, Kanagawa, 240-0193, Japan,*
[2] *Quantum Information Theory Group, Zentrum für Moderne Optik, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany*

We prove the unconditional security of the Bennett 1992 protocol, by using a reduction to an entanglement distillation protocol initiated by a local filtering process. The bit errors and the phase errors are correlated after the filtering, and we can bound the amount of phase errors from the observed bit errors by an estimation method involving nonorthogonal measurements.

Quantum key distribution (QKD) is one of the interesting topics in the quantum information processing, which allows the sender (Alice) and the receiver (Bob) to share the secret key with negligibly small leakage of information to an eavesdropper (Eve). Since Bennett and Brassard introduced the first QKD protocol, called BB84 [1] protocol, several schemes for QKD have been proposed [2]. One of the simplest of such protocols is called B92 [3], which is based on the use of only two nonorthogonal states. This nonorthogonality prevents Eve from discriminating states deterministically, which makes this protocol secure.

It is quite hard, however, to prove the security against so-called coherent attack that is the most general attack allowed by quantum mechanics. In this attack, Eve lets all of the transmitted qubits interact with her probe system and she performs an optimum measurement on the probe. For the BB84 protocol Mayers first proved the unconditional security [4]. In [5–7], the security is proven 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]. It is natural to ask about the unconditional security of the B92 protocol, which is conceptually the simplest of the QKD protocols. The analyses of the B92 protocol is hence expected to give us an idea how the nonorthogonality is related to the ability to convey secret information. Since the security proofs of BB84 rely on the symmetry of the protocol which is not shared in B92 and in B92 the channel loss directly affects the security, it is not a trivial task to modify it for B92.

In this presentation, we talk about the unconditional security of the Bennett 1992 quantum-key distribution. In the proof, we have assumed that Alice has an perfect single photon source, Bob's polarization measurement is perfect and he has a perfect single photon counter that discriminates between single photon states and vacuum-state or multi-photon states. Under these assumptions, we show that a secure B92 protocol can be regarded as an EDP initiated by local filtering [10].

Now, let us follow the proof briefly. We first consider the QKD protocol based on EDP. Let us assume that Alice initially prepares the nonmaximally entangled state $|\Psi\rangle_{\rm AB} = \frac{1}{\sqrt{2}}(|0_z\rangle_{\rm A}|\varphi_0\rangle_{\rm B} + |1_z\rangle_{\rm A}|\varphi_1\rangle_{\rm B})$, where $|\varphi_j\rangle \equiv \beta|0_x\rangle + (-1)^j\alpha|1_x\rangle$, $(0 < \alpha < 1/\sqrt{2})$, $\beta \equiv \sqrt{1-\alpha^2}$, and $\{|0_z\rangle, |1_z\rangle\}$ and $\{|0_x\rangle, |1_x\rangle\}$ are the sets of eigenvectors of the Pauli operator of Z and X components respectively. $|\varphi_0\rangle$ and $|\varphi_1\rangle$ are the two nonorthogonal single photon polarization states that are used in the B92 protocol. After Alice sends the half of the state of $|\Psi\rangle_{\rm AB}$ to Bob, he performs a "local filtering operation" on qubit B, described by the Kraus operator operator $F_{\rm fil} \equiv \alpha|0_x\rangle_{\rm B}\langle 0_x| + \beta|1_x\rangle_{\rm B}\langle 1_x|$. When the channel is noiseless and Eve does nothing, this operation yields the maximally entangled state (EPR state) $(|0_x\rangle_{\rm A}|0_x\rangle_{\rm B} + |1_x\rangle_{\rm A}|1_x\rangle_{\rm B})/\sqrt{2}$ with probability $2\alpha^2\beta^2$, since the initial state is also written as $|\Psi\rangle_{\rm AB} = \beta|0_x\rangle_{\rm A}|0_x\rangle_{\rm B} + \alpha|1_x\rangle_{\rm A}|1_x\rangle_{\rm B}$. Since this filtering is probabilistic, in order to verify whether the filtering suceeds or not, Bob tells this to Alice by public channel. If the filtering failed, then Alice and Bob discard the event. Repeating theses procedures many times, each of Alice and Bob measures σ_z of the filtered pairs so that they obtain secure key.

When noise is present or there exists Eve, the filtered states may include bit errors, represented by the subspace spanned by $\{|0_z\rangle_{\rm A}|1_z\rangle_{\rm B}, |1_z\rangle_{\rm A}|0_z\rangle_{\rm B}\}$, and a phase error, represented by the subspace spanned by $\{|0_x\rangle_{\rm A}|1_x\rangle_{\rm B}, |1_x\rangle_{\rm A}|0_x\rangle_{\rm B}\}$. In order to distill the EPR pairs, Alice and Bob run the EDP based on CSS code [7] and after this EDP Alice and Bob measure each σ_z of the EPR pairs so that they obtain secure key. For this EDP, tight estimations of the bit and phase error rate on the qubit pairs are required. To accomplish the estimation, Alice and Bob sacrifice the half of the randomly chosen qubit pairs as the test bits, perform σ_z measurement on the qubits, and exchange the outcome by public channel. However, this test bits give the estimation of only the bit error rate on untested qubit pairs. For the estimation of the phase error rate, we use the fact that the bit error and phase error will be correlated after the filtering. This can be understood by looking at the corresponding POVM. The POVM that corresponds to the bit error rate can be written as $\Pi_{\rm bit} = (|\Gamma_{11}\rangle\langle\Gamma_{11}| + |\Gamma_{01}\rangle\langle\Gamma_{01}|)/2$, where$|\Gamma_{11}\rangle \equiv \alpha|0_x\rangle_{\rm A}|0_x\rangle_{\rm B} - \beta|1_x\rangle_{\rm A}|1_x\rangle_{\rm B}$ and $|\Gamma_{01}\rangle \equiv \beta|0_x\rangle_{\rm A}|1_x\rangle_{\rm B} - \alpha|1_x\rangle_{\rm A}|0_x\rangle_{\rm B}$, while the POVM that corresponds to phase error can be written as $\Pi_{\rm Ph} = \alpha^2|1_x\rangle_{\rm A}\langle 1_x| \otimes |0_x\rangle_{\rm B}\langle 0_x| + \beta^2|0_x\rangle_{\rm A}\langle 0_x| \otimes |1_x\rangle_{\rm B}\langle 1_x|$, which

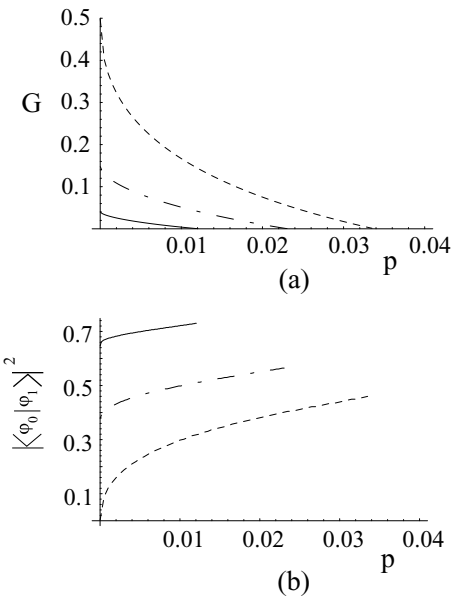

FIG. 1: (a) The optimum key generation rate G and (b) The optimum value of $|\langle\varphi_0|\varphi_1\rangle|^2$. In each figure, we assume that the quantum channel is the depolarizing channel with loss. The dotted line, the dot-dashed, and solid line represent the case where $L = 0$, $L = 0.2$, and $L = 0.5$ respectively.

is not orthogonal to $\Pi_{\rm bit}$. By using this fact and the generalizing the estimation scheme involving nonorthogonal states, we estimate the phase error rate given bit error rate.

Thanks to the fact that we use the EDP based on CSS after the filtering, we can use Shor and Preskill's method [7] to reduce the protocol described just above into the B92 protocol. In the limit of the number of qubits sent is infinity, the key generation rate G in the B92 that is the probability that Alice and Bob share the secret key per one pulse can be calculated by $G = \eta_{\rm fil}[1 - h(\eta_{\rm bit}) - h(\eta_{\rm ph})]$. Here, $h(x) \equiv -x\log_2 x - (1-x)\log_2(1-x)$ is the entropy function, $\eta_{\rm fil}$, $\eta_{\rm bit}$, and $\eta_{\rm ph}$ are the probabilities that filtering suceeds, bit error rate on the filtered states, and phase error rate on the filtered states, respectively. To illustrate the 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 ρ evolves into $L|V\rangle\langle V| + (1-L)\left[(1-p)\rho + \sum_{i=x,y,z}\sigma_i\rho\sigma_i\right]$, where $ketV$ is the vacuum state, L is the loss rate of quantum channel, p is the depolarizing rate, and σ_i is the i component of Pauli matrix. In Fig. 1 (a), we plot the key generation rate optimized over $|\langle\varphi_0|\varphi_1\rangle|^2$ and in (b) the optimum value of $|\langle\varphi_0|\varphi_1\rangle|^2$. From Fig. 1 (a), it is seen that the B92 protocol as described here is secure up to $p \sim 0.034$ (in the case of $L = 0$), $p \sim 0.0225$ (in the case of $L = 0.2$), and $p \sim 0.012$ (in the case of $L = 0.5$).

In summary, the B92 protocol can be regarded as an EDP with a filtering process, and the filtering relates the phase and bit errors to each other, which enables us to estimate the phase error rate from the bit error rate.

This presentation is the extended version of the results obtained in [11]. KT appreciates the warmth and hospitality of Quantum Information Theory Group, Zentrum für Moderne Optik in Germany.

[1] 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).
[2] A. K. Ekert, Phys. Rev. Lett, **67**, 661 (1991), B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A**51**, 1863 (1995), L. Goldenberg and L. Vaidman, Phys. Rev. Lett, **75**, 1239 (1995), M. Koashi and N. Imoto, Phys. Rev. Lett, **79**, 2383 (1997).
[3] C. H. Bennett, Phys. Rev. Lett, **68**, 3121 (1992).
[4] D. Mayers, Lecture Notes in Computer Science, **1109**, Springer–Verlag, 1996, pp. 343–357.
[5] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, quant-ph/9912053; H. Inamori, N. Lütkenhaus, and D. Mayers, quant-ph/0107017; M. Koashi and J. Preskill, quant-ph/0208155.
[6] H. -K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[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 A **452**, 2551 (1996).
[10] N. Gisin, Phys. Lett. A **210**, 151 (1996) ; M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[11] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003)