*Journal of Quantum Information Science*, **2013, 3, 16-19**
http://dx.doi.org/10.4236/jqis.2013.31004 Published Online March 2013 (http://www.scirp.org/journal/jqis)

# On the Security of Quantum Key Distribution Ping-Pong Protocol

**Masakazu Yoshida[1], Takayuki Miyadera[2], Hideki Imai[1]**
[1]Graduate School of Science and Engineering, Chuo University, Tokyo, Japan
[2]Department of Nuclear Engineering, Kyoto University, Kyoto, Japan
Email: masakazu-yoshida@imailab.jp

Received December 3, 2012; revised January 12, 2013; accepted January 20, 2013

## ABSTRACT

Computational based cryptography might not guarantee long term security if computational algorithms, computers, and so on are made remarkable progress. Therefore, quantum cryptography with unconditionally security attracts attention. In this paper, we consider security of a two-way quantum key distribution protocol, so called Ping-Pong protocol. As a result, we introduce not only robustness but also a different information disturbance theorem, which denotes a trade-off relationship between information gained for an eavesdropper and error rate, from the related works for an attack model.

**Keywords:** Two-Way Quantum Key Distribution; Ping-Pong Protocol; Robustness; Information Disturbance Theorem

## 1. Introduction

### 1.1. Back Ground

Cryptosystems used for internet, telecommunication, and so on, guarantee security by assuming computational based problems. For instance, RSA cryptosystem and El-Gamal cryptosystem guarantee security with assuming difficulty of factorization and discrete logarithm problem, respectively. Those cryptosystems might not guarantee long term security if computational algorithms, computers, and so on are made remarkable progress. Indeed, it has been showed that we can decode a cipher text to a plain text on RSA cryptosystem by using Shor's quantum factorization algorithm [1].

Quantum key distribution (QKD) protocols are expected to guarantee unconditionally security which dose not depend on any assumption. In QKD protocols, legitimate users Alice and Bob try to share secret key used for one-time pad cryptosystem guaranteeing unconditionally security. In 1984, Bennett and Brassard proposed BB84 protocol [2] and its security proofs have been showed. Ekert proposed E91 protocol [3] by using an essential property of entanglement.

In 2002, Boström and Felbinger proposed Ping-Pong protocol [4] using the Bell state. One-way quantum channels are used for BB84, E91, and so on. On the other hand, in Ping-Pong protocol, legitimate users Alice and Bob try to share secret key by using a two-way quantum channel: Bob sends a qubit system to Alice and she sends back the qubit system to Bob after encoding a bit into the qubit state deterministically. Then, Bob obtains the bit with Probability 1 if an eavesdropper Eve dose not attack. Therefore, they can share secret key without basis reconciliation (on the other hand, they need the reconciliation in BB84 or E91). We call such a QKD protocol without the reconciliation a deterministic quantum key distribution (DQKD) protocol. In Reference [4], the authors showed a trade-off relationship between information gained for Eve and error rate used for detecting the eavesdropping. After that, several security notions of the protocol are discussed from various points of view [5-12].

### 1.2. Contributions

In this paper, we reconsider security of Ping-Pong protocol from a viewpoint of the relationship between information gained for Eve and a detection function of the protocol, and we focus on whether Eve can gain information of secret key without being detected. In the process, we derive an alternate information disturbance theorem which denotes such a trade-off relationship between Eve's information gain and error rate. By necessary consequence of the theorem, Eve cannot gain information without being detected; moreover, Eve gains large information which induces high error rate. Unconditionally security proofs for BB84 based on the information disturbance theorems were shown. The results gave an intuitive and informational meaning to the security of QKD protocols. Our main contribution is to give a new insight as the first step of unconditionally security proof based on the information disturbance

 

theorems to Ping-Pong protocol.

This paper is organized as follows. In the next section, we give the original procedure of Ping-Pong protocol. In Section 3, we review several related works. In Section 4, we set our problem in the protocol and derive new information disturbance theorem. As a result, we show robustness of the protocol by using the theorem. Finally, in Section 5, we summarize this paper.

## 2. Ping-Pong Protocol [4]

Let us consider that the legitimate users Alice and Bob try to share secret key by using Ping-Pong protocol. Suppose that a quantum channel and a public channel are equipped between Alice and Bob. In the protocol, they share secret keys with a message mode and detect Eve with a control mode. The protocol consists of the following steps:

Bob prepares a bipartite system $H_B \otimes H_A$ $^2 \otimes$ $^2$ in a Bell state $|\psi^0\rangle := 1/\sqrt{2}\left(|0|0+|1|1\right)$. He sends $H_A$ to Alice over the quantum channel and keeps $H_B$ by himself.

Alice performs the following operation randomly on the system $H_A$:

Message_*A*: Alice generates a random number $s \in \{0,1\}$ and keeps it as a sifted key. She performs a unitary evolution $I$ on the system such like $(I \otimes I)|\psi^0\rangle = |\psi^0\rangle$ if $s=0$, or performs a unitary evolution $Z$ on the system such like $(I \otimes Z)|\psi^0\rangle = |\psi^1\rangle$ if $s=1$, where $|\psi^1\rangle := 1/\sqrt{2}\left(|0\rangle|0\rangle - |1\rangle|1\rangle\right)$. She sends back the post operation system to Bob over the quantum channel.

Control_*A*: Alice measures the system with a projective measurement relevant to an observable $\sigma_z = \left(|0\rangle\langle 0|, |1\rangle\langle 1|\right)$ and obtains an index $i \in \{0,1\}$ as an outcome, then the post measurement state on $H_B \otimes H_A$ is $|i\rangle|i\rangle$ if the pre-measurement state is $|\psi^0\rangle$. She sends the outcome to Bob over the public channel.

Bob performs the following operation on the bipartite system $H_B \otimes H_A$ or the system $H_B$ according to the operation employed by Alice in Step II:

Message_*B*: If Alice chooses Message_*A*, Bob measures the bipartite system $H_B \otimes H_A$ with the Bell measurement relevant to an observable $\left(|\psi^0\rangle\langle\psi^0|, |\psi^1\rangle\langle\psi^1|, |\psi^2\rangle\langle\psi^2|, |\psi^3\rangle\langle\psi^3|\right)$ and obtains an index $s' \in \{0,1,2,3\}$ as a sifted key, where $|\psi^2\rangle := 1/\sqrt{2}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)$ and $|\psi^3\rangle := 1/\sqrt{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$.

Control_*B*: If Alice chooses Control_*A*, Bob measures the system $H_B$ with the measurement relevant to $\sigma_z$ and obtains an outcome $i' \in \{0,1\}$.

They repeat the above steps sufficiently many times and calculate rate $P_\perp$ defined as value of the number of events of $i \neq i'$ divided by the number of events of Control _*A* and *B*.

They abort the protocol if $P_\perp \geq P_S$, where $P_S$ is a preset security parameter to detect an eavesdropper. Otherwise, they perform error correction and privacy amplification to generate secret key on the sifted keys over the public channel.

It is also suggested that Ping-Pong protocol is applied to direct quantum communications. Alice can send Bob any massage string to choose not random bit but any bit in Message_*A*. However, Eve might gain the massage string when Alice and Bob abort the protocol in Step V. Therefore, we should need to discuss security notion of the application for the direct quantum communications in a wary manner.

## 3. Related Works

In this section, we review several related works focusing on security of Ping-Pong protocol against several attacks.

In Reference [4], Boström and Felbinger not only proposed Ping-Pong protocol but also analyzed security of the protocol against an attack that an eavesdropper Eve performs any quantum operation on the quantum channel from Bob to Alice. Eve tries to obtain information of a secret key with distinguishing two kinds of qubits encoded by Alice. They show a relationship between information gain for Eve and error rate of bits on the control mode by using Holevo's bound as the limit of obtaining information for Eve. On the other hand, in this paper, we show an alternate relationship against the same attack model by using trace distance applied to security proof with the information disturbance theorems easily.

In Reference [6], Wójcik proposed an attack focusing imperfect quantum channel and analyzed the relationship between mutual information for Alice and Eve and mutual information Alice and Bob. Eve prepares two quantum systems in an ancillary system and an empty mode, respectively, and she performs a Hadamard gate and a SWAP gate on the systems and a qubit sent by Bob. As a result, it was shown that Eve can gain information without being detected if the quantum channel is imperfect. In Reference [7], Zhang, Man, and Li improved the attack indicated by Wójcik. Those attacks are effective in obtaining information on the original protocol with imperfect channels. However, in Reference [10], Boström and Felbinger claimed that Ping-Pong protocol becomes secure if a simple modification is applied to the protocol.

In Reference [11], we dealt with the protocol with perfect quantum channel and derived a trade-off inequality between indistinguishability for Eve and error rate of

 

the bits on the control mode. We applied fidelity to indistinguishability of the qubits encoded by Alice. Fidelity is also suited to be a method for deriving the information disturbance theorems. We also introduced a variant of the protocol and showed the relevant trade-off inequality on the variant protocol.

Recently, in Reference [12], Miszczak and Zawadzki generalized Wójcik's approach. They dealt with general imperfect (noisy) quantum channel described as Kraus representation and considered security of the protocol in the setting based on quantum bit error rare (QBER). Error caused by Eve's attack is hidden behind QBER caused by environment systems. They showed an estimation method for QBER on the protocol and showed an example of estimation of QBER on a depolarizing channel.

A series of DQKD protocols based on Ping-Pong protocol was proposed. In Reference [13], DQKD protocol so called LM05 was proposed. This protocol is a kind of DQKD protocols without entanglement. A similar protocol without entanglement so called four-state protocol was proposed [14]. In Reference [15,16], Lu *et al.*, and Beaudry *et al.* analyzed security of four-state protocol and LM05 on the perfect quantum channels, respectively. In Reference [17], Fung *et al.* showed a relationship between delayed privacy amplification and security of DQKD protocols without entanglement.

## 4. Analysis

We consider security analysis of Ping-Pong protocol against the following attack model:

On the perfect quantum channel from Bob to Alice, an eavesdropper Eve performs a quantum operation on each system $H_A$. She obtains the system $H_A$ operated by Alice on the perfect quantum channel from Alice to Bob and gains information of secret key by distinguishing quantum states.

The purpose of the analysis is to obtain a first step for theoretical proofs of unconditional security based on the information disturbance theorems.

Eve prepares s quantum system $H_E$ in a state $|\Omega\rangle$ and performs a unitary evolution $U_{AE}$ on the bipartite system $H_A \otimes H_E$:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle U_{AE}|0\rangle|\Omega\rangle + |1\rangle U_{AE}|1\rangle|\Omega\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left\{|0\rangle\left(\alpha|0\rangle|x_0\rangle + \beta|1\rangle|x_1\rangle\right) + |1\rangle\left(\alpha'|0\rangle|x_0'\rangle + \beta'|1\rangle|x_1'\rangle\right)\right\},$$

where $|x_0\rangle, |x_1\rangle, |x_0'\rangle, |x_1'\rangle$ are determined by $U_{AE}$ and $|\alpha|^2 + |\beta|^2, |\alpha'|^2 + |\beta'|^2 = 1$ hold. We obtain probability of $i \neq i'$ in Control_*B* as follow:

$$P_e := 1 - \frac{1}{2}\left(|\alpha|^2 + |\beta'|^2\right).$$

We call $P_e$ error rate for 1 bit. Note that $P_e$ plays a role of efficiency of detecting function directly if we preset $P_S = 0$. In this case, we detect Eve by using Control_*A* and *B* if and only if $P_e > 0$ holds. In Message_*A*, the post operation state is given by

$(I \otimes I \otimes I)|\Phi\rangle = |\Phi\rangle$,

if $s = 0$,

$$(I \otimes Z \otimes I)|\Phi\rangle$$

$$= \frac{1}{\sqrt{2}}\left\{|0\rangle\left(\alpha|0\rangle|x_0\rangle - \beta|1\rangle|x_1\rangle\right) + |1\rangle\left(\alpha'|0\rangle|x_0'\rangle - \beta'|1\rangle|x_1'\rangle\right)\right\},$$

if $s = 1$.

Define reduced density operators $\rho_0 := tr_{BA}|\Phi\rangle\langle\Phi|$ and

$\rho_1 := tr_{BA}|\Phi^-\rangle\langle\Phi^-|$, where $|\Phi^-\rangle := (I \otimes Z \otimes I)|\Phi\rangle$.

Let $A$ and $E$ be random variables expressing values of $s \in \{0,1\}$ in Message_*A* and results of guessing a key $s$ for Eve, respectively. We try to estimate Shannon's mutual information $I(A;E)$, which is regarded as information gain for Eve, by using trace distance. Trace distance for two quantum states $\rho$ and $\sigma$ is defined as,

$$\|\rho - \sigma\|_1 := \frac{1}{2} tr|\rho - \sigma|.$$

Trace distance takes a value from 0 to 1 and $\|\rho - \sigma\|_1 = 0$ if and only if $\rho = \sigma$. Therefore, trace distance is regarded as distinguishability of two quantum states.

We obtain the following inequality:

$$I(A;E) \leq \|\rho_0 - \rho_1\|_1 = \frac{1}{2} tr|\rho_0 - \rho_1|$$

$$= \frac{1}{2} tr\left|\alpha\bar{\beta}|0\rangle|x_0\rangle\langle 1|\langle x_1| + \bar{\alpha}\beta|1\rangle|x_1\rangle\langle 0|\langle x_0|\right.$$

$$\left. + \alpha'\bar{\beta}'|0\rangle|x_0'\rangle\langle 1|\langle x_1'| + \bar{\alpha}'\beta'|1\rangle|x_1'\rangle\langle 0|\langle x_0'|\right|,$$

$$= \frac{1}{2}\left\{tr\left|\alpha\bar{\beta}|0\rangle|x_0\rangle\langle 1|\langle x_1| + \bar{\alpha}\beta|1\rangle|x_1\rangle\langle 0|\langle x_0|\right|\right.$$

$$\left. + tr\left|\alpha'\bar{\beta}'|0\rangle|x_0'\rangle\langle 1|\langle x_1'| + \bar{\alpha}'\beta'|1\rangle|x_1'\rangle\langle 0|\langle x_0'|\right|\right\}$$

$$= |\alpha\beta| + |\alpha'\beta'|.$$

We substitute $P_e$ into the above inequality, then, we obtain the following theorem.

Theorem 1. In Ping-Pong protocol, the following trade-off relationship between information gain for Eve and error rate on the control mode holds.

$$I(A;E) \leq 2\sqrt{P_e}.$$

The trade-off inequality has two meanings:

1) Robustness:

Error rate $P_e > 0$ holds if and only if Eve gain information, *i.e.*, $I(A;E) > 0$ holds. Moreover, Eve cannot gain information without being detected if Alice and

 

Bob preset $P_S = 0$.

2) Information disturbance theorem:

The inequality means a trade-off relationship between information gain for Eve and error rate, *i.e.*, if the attack yields Eve large information gain, it induces large error rate.

## 5. Conclusion

We derived the alternate information disturbance theorem on Ping-Pong protocol against the attack model. The theorem showed that Eve cannot gain information without being detected; moreover, the larger Eve gain information, the larger error rate becomes. However, full proof of unconditionally security of the protocol based on the information disturbance theorem is not known. Therefore, we mention full proof on perfect and imperfect situation as future works. Moreover, it should be needed to discuss security notion, definition, and so on by using a unified method such as on theory of modern cryptography.

## 6. Acknowledgements

M. Y. would like to thank an anonymous referee for helpful comments.

## REFERENCES

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, Vol. 26, No. 5, 1997, pp. 1484-1509. doi:10.1137/S0097539795293172

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 10-19 December 1984, pp. 175-179.

[3] A. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, Vol. 67, No. 6, 1991, pp. 661-663. doi:10.1103/PhysRevLett.67.661

[4] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," *Physical Review Letters*, Vol. 89, No. 18, 2002, Article ID: 187902. doi:10.1103/PhysRevLett.89.187902

[5] Q.-Y. Cai, "The 'Ping-Pong' Protocol Can Be Attacked without Eavesdropping," *Physical Review Letters*, Vol. 91, No. 10, 2003, Article ID: 109801. doi:10.1103/PhysRevLett.91.109801

[6] A. Wójcik, "Eavesdropping on the 'Ping-Pong' Quantum Communication Protocol," *Physical Review Letters*, Vol. 90, No. 15, 2003, Article ID: 157901. doi:10.1103/PhysRevLett.90.157901

[7] Z. Zhang, Z. Man and Y. Li, "Improving Wójcik's Eavesdropping Attack on the Ping-Pong Protocol," *Physics Letters A*, Vol. 333, No. 1-2, 2004, pp. 46-50. doi:10.1016/j.physleta.2004.10.025

[8] Q.-Y. Cai and B.-W. Li, "Improving the Capacity of the Boström-Felbinger Protocol," *Physics Letters A*, Vol. 69, No. 5, 2004, Article ID: 054301. doi:10.1103/PhysRevA.69.054301

[9] Q.-Y. Cai, "Eavesdropping on the Two-Way Quantum Communication Protocols with Invisible Photons," *Physics Letters A*, Vol. 351, No. 1-2, 2006, pp. 23-25. doi:10.1016/j.physleta.2005.10.050

[10] K. Boström and T. Felbinger, "On the Security of the Ping-Pong Protocol," *Physics Letters A*, Vol. 372, No. 22, 2008, pp. 3953-3956. doi:10.1016/j.physleta.2008.03.048

[11] T. Miyadera, M. Yoshida and H. Imai, "On Ping-Pong Protocol and Its Variant," Cornell University Library, Ithaca and New York, 2009.

[12] J. A. Miszczak and P. Zawadzki, "General Method for the Security Analysis in a Quantum Direct Communication Protocol," Cornell University Library, Ithaca and New York, 2013

[13] M. Lucamarini and S. Mancini, "Secure Deterministic Communication without Entanglement," *Physical Review Letters*, Vol. 94, No. 14, 2005, Article ID: 140501. doi:10.1103/PhysRevLett.94.140501

[14] F.-G. Deng and G. L. Long, "Secure Direct Communication with a Quantum One-Time Pad," *Physical Review A*, Vol. 69, No. 5, 2004, Article ID: 052319. doi:10.1103/PhysRevA.69.052319

[15] H. Lu, C.-H. F. Fung, X. Ma and Q.-Y. Cai, "Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel," *Physical Review A*, Vol. 84, No. 4, 2011, Article ID: 042344. doi:10.1103/PhysRevA.84.042344

[16] N. J. Beaudry, M. Lucamarini, S. Mancini and R. Renner, "Security of Two-Way Quantum Key Distribution," Cornell University Library, Ithaca and New York, 2013.

[17] C.-H. F. Fung, X. Ma, H. F. Chau and Q.-Y. Cai, "Quantum Key Distribution with Delayed Privacy Amplification and Its Application to the Security Proof of a Two-Way Deterministic Protocol," *Physical Review A*, Vol. 85, No. 3, 2012, Article ID: 032308. doi:10.1103/PhysRevA.85.032308

 