博士学位論文要旨 (2012 年度)

A Solution of Quantum Estimation Problem Using Quantum Error-Correcting Codes and Its Applications

情報セキュリティ科学専攻 吉田 雅一
Masakazu YOSHIDA

1 Introduction

Quantum information theory plays a role of not only a resource of advanced technologies such as quantum cryptography, quantum computer, and so on, but also a bridge between information science and physics. It is necessary for remarkable development of scientific technology and engineering. We focus on Mean King's problem which is a kind of quantum estimation problems with delayed information. This problem is also interpreted as an uncertainty principle among noncommutative observables with delayed information. A purpose of research shown in this thesis is to give new information scientific insights to the problem as an example of the bridge. Specifically, we show a solution to the problem using quantum error-correcting codes and reformulate the problem using Shannon's entropy. We also consider the relationship between solutions to the problem and security of quantum key distribution to applied the problem.

Mean King's problem is told as a tale that mean King gives physicist Alice a retrodiction problem, and is constructed form the following steps: 1) Alice's preparation of an initial quantum state, 2) King's measurement, 3) Alice's measurement, 4) Revealing the measurement employed by King as a delayed information, 5) Estimating King's outcome with Alice's outcome and the delayed information. In this problem, we try to find a pair of an initial state and a measurement employed by Alice. This problem is solved in several settings, for instance, general King's measurements, entanglement preparation as an initial state, and so on. The problem is also applied to quantum key distribution protocol which is a technique to share secret key used for one-time pad cryptosystem. Security analysis of the protocol is studied against several attack models. In this way, both of the problem and the protocol are studied in the previous works. However, those works are results from viewpoints of physics and information science, respectively.

In the thesis, we show three main results. As the first result, we show a solution for general Mean King's problem using quantum error-correcting codes which are a technique to prevent disturbing of quantum states on quantum communications, and so on. We also prove existence of solutions of the problem in several cases. Furthermore, we extend classes of settings of solved problems by using the above solution method. As the second result, we reformulate Mean King's problem using Shannon's entropy and introduce an alternative proof of nonexistence of solutions of the problem in a case of qubit system without quantum entanglement. In the last result, we modify measurement scheme in quantum key distribution protocol using Mean King's problem, and consider security of the protocol against several attacks. As a result, we show that solving Mean King's problem are necessary but are not sufficient to construct secure quantum key distribution protocol. In this paper, we review the main results shown in the thesis briefly.

2 Mean King's Problem and Its Application for Quantum Key Distribution

Mean King's problem is formulated by Vaidman, Aharonov, and Albert [1] in 1987. The problem is told as a tale that mean King gives physicist Alice a retrodiction problem. King asks Alice to prepare a qubit system in an arbitrary state. Then, King measures the system with one of observables σ_x, σ_y, and σ_z and obtains an outcome 1 or -1. After this measurement, King gives back Alice the system. Alice measures the post measurement system with an arbitrary measurement. After that King reveals the observable which he employed, then, Alice has to guess the outcome obtained by King immediately by using the outcome obtained by her and knowledge of the observable. The problem is to find the measurement employed by Alice and the initial state such that she guesses the outcome obtained by King perfectly.

In Ref.[1], a solution to the problem is shown using the Bell state. Alice prepares the qubit system given to King and an ancillary qubit system kept by her in the Bell state, then Alice guesses the King's outcome

perfectly by using a measurement derived on the bipartite qubits system. Mean King's problem has been generalized concerning the prepared quantum system and King's measurements. In particular, it has been proved [2, 3] that Alice can estimate King's outcome by using a maximally entangled state in a setting that King measures one of the systems with one of projective measurements constructed from mutually unbiased bases. On the other hand, Alice cannot retrodict the outcome with certainty without using entangled states in the setting [4]. In the reference, an upper bound of the success probability is also introduced.

In 2001, Bub [5] proposed a quantum key distribution protocol using Mean King's problem. In the protocol, Alice prepares a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ in the Bell state. She gives the system $\mathcal{H}_K$ to King and keeps the system $\mathcal{H}_A$ with her. King measures the system $\mathcal{H}_K$ with one of observables σ_x, σ_z and returns the system to Alice. He keeps the outcome as a secret key, where he transpose:$1 \mapsto 0$ and $-1 \mapsto 1$. Alice measures the bipartite system exactly with an observable $\hat{R}$ with four kinds of outcomes, which solves Mean King's problem for σ_x, σ_y, and σ_z, and she estimates King's outcome. If there is not an eavesdropper, Alice and King are able to share the key as $\hat{R}$ solves Mean King's problem for σ_x and σ_z

An eavesdropper called Eve has opportunities to gain information of the secret key on a quantum channel from Alice to King and it from King to Alice. Suppose that Eve try to gain information with a measurement on the quantum channel from King to Alice and sends the post measurement state to Alice. Then, it was shown that bit error rate of the secret key is greater than or equal to 3/8 [5]. Werner et al., [6] showed that Eve cannot gain information about the secret key without being detected even if Eve can attack qubits twice on the channels in an arbitrary way. That is, they showed that the information gain by Eve inevitably disturbs the outcomes obtained by the legitimate users.

3 A Solution of the Problem Using Quantum Error-Correcting Codes

We introduce a solution of the general Mean King's problem by using the relationship between the problem and quantum error-correcting codes. Note that the following theorem is a solution to Mean King's problem. In the thesis, we also prove existence of the solution in prime power dimensional case and expand the class of settings of the problem a solution is existent.

We suppose that Alice can prepare an ancillary system in secret in addition to the system given to King. Then, she answers the problem to King by using correlation between the systems. Let d dimensional Hilbert space $\mathcal{H}_K$ be the system given to King and d' dimensional Hilbert space $\mathcal{H}_A$ the ancillary system kept by Alice. King measures the system with one of projective measurements in the conventional setting of Mean King's problem. In this paper, we deal with more general setting with respect to the measurements. King measures the system $\mathcal{H}_K$ with one of the measurements described by families of measurement operators $M^{(J)} = (M_i^{(J)})_i (J = 1, 2, \ldots, m)$ satisfying $\sum_i {M_i^{(J)}}^\dagger M_i^{(J)} = \mathbb{I}$ [1]. Alice measures the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ in the post measurement state with a suitable Positive Operator Valued Measure (POVM) $P = (P_j)_j$ [2] and she obtains jth outcome. Alice try to estimate King's outcome with her outcome and J employed by King. In this setting, we obtain the following theorem.

Theorem 1 *Let $C \subset \mathcal{H}_A \otimes \mathcal{H}_K$ be a n dimensional subspace (i.e., C is a $[dd', n]$ quantum code) and E the projection operator onto C. If there exists l-tuple of Kraus operators $(L_k)_{k=1}^l$ on $\mathcal{H}_K$ with $\sum_k L_k^\dagger L_k = \mathbb{I}_K$ and non-empty index sets $X^{(J,i)} \subset \{1, 2, \ldots, l\}$ satisfying*

$$\begin{aligned} \mathbb{I}_A \otimes M_i^{(J)} &= \textstyle\sum_{k \in X^{(J,i)}} \mathbb{I}_A \otimes L_k \text{ on } C, \\ X^{(J,i)} \cap X^{(J,i')} &= \emptyset, \quad \forall J, \forall i \neq i', \\ E(\mathbb{I}_A \otimes L_k)^\dagger (\mathbb{I}_A \otimes L_{k'}) E &= \lambda_{kk'} \delta_{kk'} E, \end{aligned}$$

for some $\lambda_{kk'} \in \mathbb{C}$, then

(i) Alice can solve King's problem for any initial state in C,

(ii) C is a quantum error-correcting code against $\mathrm{span}\{\mathbb{I}_A \otimes L_k\}_{k=1}^l$.

Thus, it is a solution of Mean King's problem that Alice prepares a code state of a quantum error-correcting code against errors into decomposed the measurement operators and distinguishes a kind of the error operators belong to the measurement perfectly.

[1] Remind that the system in a state ρ is measured with the measurement operators $(M_i^{(J)})_i$, then, recall that the probability of obtaining ith outcome corresponding to $M_i^{(J)}$ is given by $p_i = \mathrm{tr} {M_i^{(J)}}^\dagger M_i^{(J)} \rho$ and the post measurement state is represented as $M_i^{(J)} \rho {M_i^{(J)}}^\dagger / p_i$.

[2] $P_j \geq 0$ and $\sum_j P_j = \mathbb{I}$ hold

4 Re-formulation of the Problem Using Shannon's Entropy

We reformulate the general Mean King's problem by using Shannon's entropy. In the thesis, we also confirm the reformulation by proofing non existence of solutions of the problem in the qubit setting without entanglement.

In the problem, with given $d(= \dim\mathcal{H}_K)$ and measurements $M^{(k)} = (M_j^{(k)})_{j=0}^m (k = 0, 1, \ldots, m')$ [3], we say that a solution to Mean King's problem exists if and only if a pair of an initial state and a measurement employed by Alice exist such that she estimates King's outcome with probability 1. Notice that Alice can utilize an entanglement: In step 1, she secretly prepares an ancilla system and chooses an appropriate entangled state on the bipartite system. In step 3, she performs a POVM measurement $P = (P_i)_{i=0}^n$ on the bipartite system. In this section, we reformulate the problem using Shannon's conditional entropy.

Let K, J, and I be random variables expressing the kind of the measurements employed by King, the outcomes obtained by King, and the outcomes obtained by Alice's measurement P, respectively. Then, we can reformulate Mean King's problem using the conditional entropy as follows: Find an initial state ρ and a measurement P such that

$$H(J \mid I, K) = 0, \tag{1}$$

where $H(\cdot \mid \cdot)$ denotes Shannon's conditional entropy. Note that $H(J \mid I)$ is generally strictly positive, otherwise Alice can guess King's outcome without a delayed information K. By the chain rule of the conditional entropy, eq.(1) is equivalent to the following relation:

$$H(K, J \mid I) = H(K \mid I), \tag{2}$$

Let $P_{K,J,I}(k, j, i)$ be a joint probability of K, J, I, and let $P_{K,I}(k, i) = \sum_j P_{K,J,I}(k, j, i)$ be the marginal joint probability of K and I. We find that eq.(2) holds if and only if

$$P_{K,J,I}(k, j, i) = 0 \quad \text{or} \quad P_{K,J,I}(k, j, i) = P_{K,I}(k, i), \tag{3}$$

holds for each k, j, and i. In our setting, a solution to Mean King's problem is to find an initial state ρ and a measurement P such that condition eq.(1), eq.(2), or eq.(3) holds. As a result, we can consider the problem as a problem in information theory or probabilistic theory.

[3] Note that this notation is slightly different for the indexes: $J \leftrightarrow k$.

5 Security Analysis of Quantum Key Distribution

In the conventional setting of the problem, King measures the system with one of the observables $\hat{X}, \hat{Y}$, and $\hat{Z}$ [4], and Alice measures the bipartite system with $\hat{R}$. On the other hand, in the quantum key distribution protocol using Mean King's problem proposed by Bub, King uses only $\hat{X}$ and $\hat{Z}$, while Alice measures $\hat{R}$. It should be noted that $\hat{R}$ is not a unique solution for Mean King's problem for these two observables. In addition, it is difficult to realize the measurement of $\hat{R}$, as it has projections on to the entangled bases $|r_j\rangle$ $(j = 1, 2, 3, 4)$ [5]. In the following, by using the solution introduced in theorem 1, we show three observables $\hat{M}, \hat{N}$, and $\hat{L}$ employed by Alice that also solve Mean King's problem for $\hat{X}$ and $\hat{Z}$. These observables are rather simple compared with $\hat{R}$. We apply them to the quantum key distribution and study their security. Note that Table 1 denotes the relationship between King's observables and four outcomes of $\hat{M}, \hat{N}$, and $\hat{L}$.

Measurement $\hat{M}$

Define a Projection-Valued Measure (PVM) $\hat{M} := (M_k)_{k=1}^4$ [6] on $\mathcal{H}_A \otimes \mathcal{H}_K$: $M_1 := Z_0 \otimes X_0$, $M_2 := Z_1 \otimes X_0, M_3 := Z_0 \otimes X_1$, $M_4 := Z_1 \otimes X_1$ [7]. Alice measures the post measurement state with $\hat{M}$ and obtains an outcome $k \in \{1, 2, 3, 4\}$. She can estimate King's outcome by using the relationship (see Table 1) between King's observables and her outcome, e.g., if King chooses $\hat{X}$ and Alice obtains an outcome 2, she estimates King's outcome as 0.

Measurement $\hat{N}$

We obtain a PVM measurement $\hat{N} = (N_k)_{k=1}^4$ on $\mathcal{H}_A \otimes \mathcal{H}_K$ in a similar way: $N_1 := X_0 \otimes Z_0$, $N_1 := X_0 \otimes Z_1, N_3 := X_1 \otimes Z_0$, $N_4 := X_1 \otimes Z_1$.

Measurement $\hat{L}$

Lastly, we define a POVM $\hat{L} := (L_k)_{k=1}^4$ on $\mathcal{H}_A \otimes \mathcal{H}_K$ by $L_1 := \frac{1}{2}(Z_0 \otimes X_0 + X_0 \otimes Z_0)$, $L_2 := \frac{1}{2}(Z_1 \otimes X_0 + X_0 \otimes Z_1), L_3 := \frac{1}{2}(Z_0 \otimes X_1 + X_1 \otimes Z_0)$, $L_2 := \frac{1}{2}(Z_1 \otimes X_1 + X_1 \otimes Z_1)$.

We introduce a trade-off relationship between the information gain by Eve and the error probability of secret key for a attack model that Eve try to gain information on the quantum channel from King to Alice (we also consider several attack models in the thesis). We ob-

[4] Note that this notation is slightly different for the indexes: $\hat{X} \leftrightarrow \sigma_x, \hat{Y} \leftrightarrow \sigma_y$, and $\hat{Z} \leftrightarrow \sigma_z$.

[5] See in Ref.[1].

[6] PVMs are a class of POVMs constructed from projection operators.

[7] Z_0 and Z_1 are projections into eigenspaces corresponding to eivenvalues 1 and -1 of $\hat{Z}(= \sigma_z)$, respectively. X_0 and X_1 are projections into eigenspaces corresponding to eivenvalues 1 and -1 of $\hat{X}(= \sigma_x)$, respectively.

Table 1: The relationship between King's observables and Alice's measurements

	1	2	3	4
$\hat{X}$	0	0	1	1
$\hat{Z}$	0	1	0	1

tains the following theorem.

Theorem 2 *If Alice employs the observable $\hat{R}$ or $\hat{L}$,*

$$\begin{aligned} & \|\Lambda_E^*(|+\rangle\langle+|) - \Lambda_E^*(|-\rangle\langle-|)\|_1 \\ \leq \quad & 2\sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i)}, \end{aligned}$$

holds for the attack model, where the left hand side denotes Eve's distinguishability of a secret key generated by $\hat{Z}$ and the right hand side denotes error probability of the secret key generated by $\hat{X}$.

The inequality shows that Eve cannot distinguish a secret key without increasing the error probability of the secret key. Moreover, if the attack yields Eve large information gain, it induces large error probability. For the observables $\hat{M}$ and $\hat{N}$, the trade-off is not hold, i.e., it means that the error probability of the secret key is zero even if Eve gains information. Moreover, this result implies that observables solving Mean King's problem for two observables are necessary but are not sufficient to construct secure quantum key distribution protocols.

6 Summary

We introduced three main results in the thesis. As the first results, we show a solution to the general Mean King's problem by using quantum error-correcting codes. As the second result, we reformulated the problem using Shannon's entropy. As the last result, we analyzed security of the quantum key distribution protocol with modified measurement schemes. From the first and the second result, we give new informational scientific insights to Mean King's problem from viewpoints of quantum coding theory and information theory. From the last result, we give a new physical insight to security analysis of quantum key distribution protocol from a viewpoint of quantum estimation problems.

Acknowledgment

MY thank Prof. H.Imai, Dr. T.Miyadera, Dr. M.Hagiwara, Dr. G.Kimura, Dr. K.Imafuku, and Dr. T.Kitagawa for valuable comments and precious study opportunity.

Research Papers

- M. Yoshida, M. Hagiwara, T. Miyadera, and H. Imai, "A Numerical Evaluation of Entanglement Sharing Protocols Using Quantum LDPC CSS Codes,"IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E95-A, No. 9, pp.1561-1569, Sep., 2012.
- M. Yoshida, and H. Imai, "Re-formulation of Mean King 's Problem using Shannon's Entropy,"Journal of Quantum Information Science, Vol. 3, No. 1, Mar., 2013. to appear
- M. Yoshida, T. Miyadera, and H. Imai, "Separability Criterion in prime dimensions based on Landau-Pollak Uncertainty Relation,"International Symposium on Information Theory and Its Applications, pp.467-472, Dec., 2008.
- M. Yoshida, T. Miyadera, and H. Imai, "On the security of the quantum key distribution using the Mean King Problem,"International Symposium on Information Theory and Its Applications, pp.917-921, Oct., 2010.
- M. Yoshida, T. Miyadera, and H. Imai, "Quantum Key Distribution using Mean King Problem with Modified Measurement Schemes,"International Symposium on Information Theory and Its Applications, pp.265-269, Oct., 2012.

References

[1] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett., vol. **58**, pp.1385-1387, 1987.

[2] A. Hayashi, M. Horibe, and T. Hashimoto, Phys. Rev. A, vol. **71**, 052331, 2005.

[3] G. Kimura, H. Tanaka, and M. Ozawa, Phys. Rev. A, vol. **73**, 050301(R), 2006.

[4] G. Kimura, H. Tanaka, and M. Ozawa, "Comments on "Best conventional solutions to the King's problem"," Z. Naturforsch. vol. **62a**, pp.152-156, 2007.

[5] J. Bub, Phys. Rev. A, vol. **63**, 032309, 2001.

[6] A. H. Werner, T. Franz, and R. F. Werner, Phys. Rev. Lett., vol. **103**, 220504, 2009.