数理解析研究所講究録
第1852巻 2013年 217-224

量子誤り訂正符号を用いた量子推定問題の解法とその応用

中央大学理工学研究科　吉田　雅一
Masakazu YOSHIDA
Graduate School of Science and Engineering, Chuo University
京都大学工学研究科原子核工学専攻　宮寺　隆之
Takayuki MIYADERA
Department of Nuclear Engineering, Kyoto University
芝浦工業大学システム理工学部　木村　元
Gen KIMURA
College of Systems Engineering and Science,
Shibaura Institute of Technology
中央大学理工学部　今井　秀樹
Hideki IMAI
Faculty of Science and Engineering, Chuo University

概要

量子推定問題の一つにMean King問題 [1] がある．Mean King問題は遅延情報を利用した量子状態識別問題としても捉えることができ，理論的な興味から様々な研究が行われてきた．一方で，同問題を量子鍵配送へ応用することも考えられている [2]．本講究録では，これらMean King問題および同問題を応用した量子鍵配送に関した既存研究を紹介するとともに，我々の成果である量子誤り訂正符号を用いたMean King問題の解法 [3] およびその解法を用いた量子鍵配送の修正 [4] を要約する．

1　はじめに

1.1　Mean King問題

Mean King問題はVaidman，Aharonov，Albert [1] により定式化され，その後は王様Kingが物理学者Aliceに問いを投げかける物語として語られることが多い [5, 6, 7]．まずKingはAliceに量子ビット系 $\mathcal{H}_K$ を好きな状態 $|\psi\rangle$ に準備するように指示する．KingはAliceから量子ビット系を受け取り，物理量 σ_x, σ_y および σ_z のうち一つをAliceに対して秘密裏に選び，その物理量の射影測定を行い測定値 $i \in \{1, -1\}$ を得る．ただし，AliceはKingが $\sigma_x, \sigma_y, \sigma_z$ から一つを選ぶことは知らされる．Aliceは Kingの測定後の状態で好きな測定 R を行い測定値 j を得る．その後，Kingは Aliceへ自分が選んだ物理量 $\sigma_k (k \in \{x, y, z\})$ を伝える．このとき，Aliceは直ちに測定値

j および物理量 σ_k から King の測定値 i を推定しなければならない．この設定において King の測定値を正しく推定 (King の測定値と推定値が等しくなる確率が 1) するような，Alice が準備する状態 $|\psi\rangle$ と測定 R および推定法が Mean King 問題の解である．Mean King 問題は非可換な物理量の固有状態を推定する問題と捉えることができるので，不確定性関係とも深く結びついているとも言える．

既存研究 [1] では，問題の定式化を行うとともに量子もつれを用いた解が示されている．Alice は King に渡す量子ビット系 $\mathcal{H}_K$ だけでなく，秘密裏に補助量子ビット系 $\mathcal{H}_A$ を準備する．次に Alice は二つの量子ビット系 $\mathcal{H}_A \otimes \mathcal{H}_K$ を Bell 状態 $|\Psi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ に準備し，King には $\mathcal{H}_K$ だけを渡し $\mathcal{H}_A$ は秘密裏に保持する．King は $\sigma_x, \sigma_y, \sigma_z$ のうち一つの物理量に関して射影測定を行う．その後，Alice は $\mathcal{H}_A \otimes \mathcal{H}_K$ 上の射影測定 $R = (R_j := |r_j\rangle\langle r_j|)_{j=1}^4$ を行い，測定値として添え字の j を得る．ただし，

$$
\begin{aligned}
|r_1\rangle &:= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{2}(|0\rangle|1\rangle e^{i\pi/4} + |1\rangle|0\rangle e^{-i\pi/4}),\\
|r_2\rangle &:= \frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{2}(|0\rangle|1\rangle e^{i\pi/4} + |1\rangle|0\rangle e^{-i\pi/4}),\\
|r_3\rangle &:= \frac{1}{\sqrt{2}}|1\rangle|1\rangle + \frac{1}{2}(|0\rangle|1\rangle e^{-i\pi/4} + |1\rangle|0\rangle e^{i\pi/4}),\\
|r_4\rangle &:= \frac{1}{\sqrt{2}}|1\rangle|1\rangle - \frac{1}{2}(|0\rangle|1\rangle e^{-i\pi/4} + |1\rangle|0\rangle e^{i\pi/4}),
\end{aligned}
$$

である．このとき，King の選ぶ物理量および測定値と Alice の測定値の関係は表 1 で与えられ，Alice は King から遅延情報である物理量の種類と自分の測定値から King の測定値を一意に推定できる．また，初期状態 $|\Psi^+\rangle$ と終状態 $|r_j\rangle$ が与えられたとき，King が物理量 σ_k を選び測定値 i

表 1: King の測定と Alice の測定 R の関係

	R_1	R_2	R_3	R_4
σ_x	1	-1	1	-1
σ_y	1	-1	-1	1
σ_z	1	1	-1	-1

を得た確率は

$$
\frac{|\langle R_j|\,\mathbb{I}\otimes\sigma_k(i)|\Psi^+\rangle|^2}{\sum_i |\langle R_j|\,\mathbb{I}\otimes\sigma_k(i)|\Psi^+\rangle|^2} \tag{1}
$$

で与えられる．ただし，$\sigma_k(i)$ は σ_k の固有値 i の固有空間への射影演算子である．式 (1) は Aharonov-Bergmann-Lebowitz ルール [8] と呼ばれる．いま，その値は 0 か 1 となるので，Alice が King の測定値を正しく推定できるときその確率は 1 であることがわかる．

Mean King 問題は King の測定の種類や初期状態の準備の仕方を変えることで様々な設定で考えられてきた．特に King の測定が Mutually Unbiased Basis(MUB) [9, 10] から作られる射影測定の場合での解は既存研究 [6, 11, 12, 13] などで示されている．これらの成果は Alice の状態準備として量子もつれも許したものである．一方で，量子もつれの準備を許さず一つの量子系のみしか用意できない場合には，Alice が King の測定値を正しく推定する確率が 1 にならないことも示されている [14, 15].

1.2 Mean King問題を用いた量子鍵配送

Mean King問題は量子鍵配送への応用も考えられている [2]．量子鍵配送では，既存研究 [1] で示された解に従いAliceはKingの測定値を正しく推定して，その測定値をAliceとKingは共通鍵として使用する．ただし，Aliceが準備する初期状態はBell状態であるが，Kingが選ぶ物理量はMean King問題とは異なり σ_x か σ_z の二種類のみである．Aliceが行う測定は，Kingから送り返された量子ビット系と保持しておいた量子ビット系上の測定 $R = (|r_j\rangle\langle r_j|)_{j=1}^4$ である．測定 R は三種類の物理量を扱うMean King問題の解であるので，二種類の物理量を扱う量子鍵配送においても，Aliceは遅延情報と自分の測定値からKingの測定値を推定することができる．このとき，KingとAliceはそれぞれ測定値と推定値を $1 \to 0, -1 \to 1$ とビット値に変換することで，1ビットを共有する．同様のやり取りを十分な回数行うことで篩い鍵を共有し，その後篩い鍵のいくつかを利用し鍵の誤り率を求める．このとき，誤り率が高い場合には盗聴があったとして鍵配送を中止し，誤り率が十分小さい場合には残りの篩い鍵に対して誤り訂正と秘匿性増強を施し最終的な共有鍵とする．

Mean King問題を用いた量子鍵配送の安全性に関しては，Wernerらが，AliceからKingへの量子通信路，KingからAliceへの量子通信路および両者が使用する公衆通信路を盗聴し共通鍵の情報を得ようとする攻撃者に対してrobustnessを満たすことを示した [16]．つまり，攻撃者は鍵に誤りを生じさせないような情報搾取を行った場合には，鍵に関して一切情報を得ることができないと言える．

2 量子誤り訂正符号を用いたMean King問題の解法 [3]

2.1 量子誤り訂正符号

我々は既存研究におけるMean King問題の設定を一般化し，その設定において量子誤り訂正符号を用いた解法を示した [3]．そこで，まずは量子誤り訂正符号について復習する．d 準位量子系に対して d 次元Hilbert空間 $\mathcal{H}$ が付随する．また，その量子系の量子状態は一般に $\mathcal{H}$ 上の密度演算子 ρ で記述される．ただし密度演算子とは $\mathrm{tr}\,\rho = 1$ と $\rho \geq 0$ を満たす演算子である．我々は次のようなKraus表現で表される量子操作を量子系 $\mathcal{H}$ に加わる誤りとして扱う．複素線形空間となる $\mathcal{H}$ 上の演算子の集合を E とする．この E を誤りと呼び，$\sum_i E_i^\dagger E_i = \mathbb{I}$ を満たす部分集合 $\{E_i\}_i$ を用いて量子状態 ρ に誤りが加わるという量子操作を $\rho \mapsto \sum_i E_i \rho E_i^\dagger$ と表す．

量子系 $\mathcal{H}$ の部分空間 C を量子符号と呼び，C の純粋状態を符号状態と呼ぶ．量子符号 C と誤り E に対して量子誤り訂正符号を定義する．C および E に対して，次の条件を満たすKraus演算子の組 $R_E = (R_{E_j})_j$ が存在するとき (C, R_E) を誤り E に対する量子誤り訂正符号と呼ぶ：$\max_{|\psi\rangle\in C} \sum_{i,j} \|(R_{E_j}E_i - \langle\psi|R_{E_j}E_i|\psi\rangle)|\psi\rangle\|^2 = 0$．このとき，$R_E$ をリカバリ演算子の組と呼ぶ．また，次の定理が示されている．

定理 1 *(Knill-Laflamme [17])*. 量子符号 C と誤り $E = \{E_i\}_i$ に対してリカバリ演算子の組が存在することは次と同値である：任意の $E_i, E_{i'} \in E$ に対して

$$PE_i^\dagger E_{i'} P = \eta_{ii'} P$$

が成り立つ．ただし P は C への射影演算子であり，$\eta_{ii'} \in \mathbb{C}$ である．

2.2 解法

我々は Mean King 問題を次のように一般化する.

1. Alice は King に渡す量子系 $\mathcal{H}_K$ と秘密裏に保持する $\mathcal{H}_A$ を状態 $|\psi\rangle$ に準備する. ただし $\dim \mathcal{H}_K = d, \dim \mathcal{H}_A = d'$ とする.
2. King は $\mathcal{H}_K$ で一般測定 [1] $M^J = (M_i^J)_i (J = 1, 2, \ldots, m)$ の一つを行い, 測定値として添え字の i を得る.
3. Alice は $\mathcal{H}_A \otimes \mathcal{H}_K$ で Positive-Valued Measure(POVM) [2]測定 $Q = (Q_j)_j$ を行い測定値として添え字 j を得る.
4. King は選んだ測定の種類 J を Alice に開示する.
5. Alice は J および j から King の測定値 i を推定する.

上記の問題に対して量子誤り訂正符号を用いた解法となる次の定理を示した. 同定理は Mean King 問題の解が存在するための十分条件である.

定理 2 $C \subset \mathcal{H}_A \otimes \mathcal{H}_K$ を量子符号とし, P を C への射影演算子とする. $\mathcal{H}_K$ 上の *Kraus* 演算子の組 $(E_k)_{k=1}^l$ と空でないインデックス集合 $X^{(J,i)} \subset \{1, 2, \ldots, l\}$ が次を満たすとする :

$$\mathbb{I} \otimes M_i^J = \sum_{k \in X^{(J,i)}} \mathbb{I} \otimes E_k \text{ on } C \tag{2}$$

$$X^{(J,i)} \cap X^{(J,i')} = \emptyset \quad (\forall J, \forall i \neq i'), \tag{3}$$

$$P(\mathbb{I}_A \otimes E_k)^\dagger (\mathbb{I}_A \otimes E_{k'}) P = \lambda_{kk'} \delta_{kk'} E \quad (\lambda_{kk'} \in \mathbb{C}). \tag{4}$$

このとき,
(i)Alice は C の任意の符号状態を用いて *King* の測定値を確率 1 で正しく推定できる.
(ii)C は $\{\mathbb{I}_A \otimes L_k\}_{k=1}^l$ で張られる誤りに対する量子誤り訂正符号である.

証明 (i)$|\psi\rangle \in C$ を Alice が準備する初期状態とする. King は測定 M^J を選び測定値 i を得たとする. このとき測定後の状態は $\mathbb{I}_A \otimes M_i^J |\psi\rangle \in \bigoplus_{k \in X^{(J,i)}} K_k$ を規格化した純粋状態となる. ただし $K_k (k = 1, 2, \ldots, l)$ は $\{\mathbb{I}_A \otimes E_k C\}$ で張られた空間である. 条件 (4) より任意の相異なる k と k' に対して K_k と $K_{k'}$ は互いに直交する空間である. そこで K_k への射影演算子 Q_k から Projection Valued Measure(PVM) [3] $Q = (Q_k, Q_\perp)_{k=1}^l$ を構成する. ただし, $Q_\perp := \mathbb{I}_A \otimes \mathbb{I}_K - \sum_{k=1}^l Q_k$ である. Alice は King の測定後の状態で PVM 測定 Q を行い, 測定値 k を得る. Alice は King の測定の種類 J と k から, King の測定値を $k \in X^{(J,i)}$ を満たす i と推定する. このとき, 条件 (3) より King の測定値は一意に定まるので, Alice は King の測定値を確率 1 で正しく推定できる.
(ii) 任意の $\tilde{E}_\alpha = \sum_{k=1}^l \alpha_k (I_A \otimes E_k), \tilde{E}_\beta = \sum_{k=1}^l \beta_k (I_A \otimes E_k) \in \text{span}\{\mathbb{I}_A \otimes E_k\}_{k=1}^l$ に対して, $P \tilde{E}_\alpha^\dagger \tilde{E}_\beta P = (\sum_{k,k'=1}^l \overline{\alpha_k} \beta_{k'} \lambda_k) P$ が成り立つ. ただし, $\alpha_k, \beta_k \in \mathbb{C}$ である. 上式と定理 1 より C が $\{\mathbb{I}_A \otimes L_k\}_{k=1}^l$ で張られる誤りに対する量子誤り訂正符号となるリカバリ演算子の組が存在する.
■

---

[1] $(M_i^J)_i$ が一般測定とは, まず $\sum_i M_i^{J\dagger} M_i^J = \mathbb{I}$ を満たし, 状態 ρ で測定を行ったとき測定値 i を得る確率が $p_i = \text{tr}\, M_i^J \rho M_i^{J\dagger}$ で与えられ, 測定後の状態が $M_i^J \rho M_i^{J\dagger} / p_i$ で与えられることである.
[2] $(Q_j)_j$ が POVM とは, $\sum_i Q_i = \mathbb{I}$ および任意の i に対して $Q_i \geq 0$ を満たすことである.
[3] $(Q_j)_j$ が PVM とは, POVM かつ任意の j に対して $Q_j = Q_j^\dagger = Q_j^2$ を満たすことである.

定理2より，Kingの測定に対して条件(2)，(3)および(4)を満たすインデックス集合$X^{(J,i)}$とKraus演算子$(E_k)_k$および量子符号Cの組が存在するとき，Mean King問題の解が存在することがわかる．しかしながら一般にそのような組が存在するかはわからない．我々は[11]の設定において，Kingが扱うMUBから構成する射影測定に対して，量子符号を最大エンタングルド状態で張られる1次元空間としたときにインデックス集合とKraus演算子の存在性を示した．よって，本結果は[11]の結果を含み，さらに量子誤り訂正符号の理論をMean King問題に応用できることを示している．また，任意の$\mathcal{H}_K$の正規直交基底より，本解法が適用可能なMean King問題の設定を示すことで，解が存在する問題設定を拡張した．

3 解法の応用：量子鍵配送における測定の修正とその考察 [4]

3.1 測定の修正

Mean King問題を応用した量子鍵配送[2]においてAliceが扱う測定RはKingが三種類の物理量$\sigma_x, \sigma_y, \sigma_z$を扱うMean King問題の解であった．ところが量子鍵配送においてKingが扱う物理量はσ_x, σ_zの二種類である．そこで，我々はまず定理2を用いて二つの物理量を扱うMean King問題の解を三種類示すことで，量子鍵配送においてAliceが扱う測定を修正する．

測定M 次の$\mathcal{H}_K$上のKraus演算子の組$E = (E_k)_k$を次のように定義する：$E_1 := \sigma_x(1)\sigma_z(1), E_2 := \sigma_x(1)\sigma_z(-1), E_3 := \sigma_x(-1)\sigma_z(1), E_4 := \sigma_x(-1)\sigma_z(-1)$．これらの演算子はBell状態$|\Psi^+\rangle$に対して$\langle\Psi^+|(\mathbb{I}\otimes E_k)^\dagger(\mathbb{I}\otimes E_{k'})|\Psi^+\rangle = 1/4\delta_{kk'}, \sigma_x(1) = E_1 + E_2, \sigma_x(-1) = E_3 + E_4, \sigma_z(1) = E_1 + E_3, \sigma_z(-1) = E_2 + E_4$を満たす．以上より，$C$をBell状態で張られる量子符号とすると，上記の$E$はKingの扱う物理量$\sigma_x, \sigma_z$に対して定理2の条件を満たし，また条件を満たすインデックス集合も作れることがわかる．よって，Mean King問題の解となるAliceの測定が存在し，それは，

$$M_1 := \sigma_z(1)\otimes\sigma_x(1), M_2 := \sigma_z(-1)\otimes\sigma_x(1),$$

$$M_3 := \sigma_z(1)\otimes\sigma_x(-1), M_4 := \sigma_z(-1)\otimes\sigma_x(-1),$$

で与えられるPVM測定$M = (M_i)_{i=1}^4$である．このPVM測定を用いることにより，AliceとKingは鍵を共有できる．

測定N Kraus演算子の組$E' = (E'_k)_k$を次のように定義する：$E'_1 := \sigma_z(1)\sigma_x(1), E'_2 := \sigma_z(-1)\sigma_x(1), E'_3 := \sigma_z(1)\sigma_x(-1), E'_4 := \sigma_z(-1)\sigma_x(-1)$．測定$M$のときと同様に定理2よりAliceが扱うPVM測定$N = (N_i)_{i=1}^4$が次のように定義できる：

$$N_1 := \sigma_x(1)\otimes\sigma_z(1), N_2 := \sigma_x(1)\otimes\sigma_z(-1),$$

$$N_3 := \sigma_x(-1)\otimes\sigma_z(1), N_4 := \sigma_x(-1)\otimes\sigma_z(-1).$$

測定L 次のようにAliceが扱うPOVM測定$L = (L_i)_{i=1}^4$を測定MとNから構成する：

$$L_1 := \frac{1}{2}(\sigma_z(1)\otimes\sigma_x(1) + \sigma_x(1)\otimes\sigma_z(1)), L_2 := \frac{1}{2}(\sigma_z(-1)\otimes\sigma_x(1) + \sigma_x(1)\otimes\sigma_z(-1)),$$

$$L_3 := \frac{1}{2}(\sigma_z(1)\otimes\sigma_x(-1) + \sigma_x(-1)\otimes\sigma_z(1)), L_2 := \frac{1}{2}(\sigma_z(-1)\otimes\sigma_x(-1) + \sigma_x(-1)\otimes\sigma_z(-1)).$$

上記のAliceの測定とKingの物理量および共有する鍵の関係を表2に示す．

表 2: 測定と共有する鍵の関係

	M_1, N_1, L_1	M_2, N_2, L_2	M_3, N_3, L_3	M_4, N_4, L_4
σ_x	$0, \sigma_x(1)$	$0, \sigma_x(1)$	$1, \sigma_x(-1)$	$1, \sigma_x(-1)$
σ_z	$0, \sigma_z(1)$	$1, \sigma_z(-1)$	$0, \sigma_z(1)$	$1, \sigma_z(-1)$

3.2 考察

前節において，量子鍵配送に適用可能な Alice が扱う三種類の測定を新たに示した．これらの測定を用いたとしても，共通鍵を盗もうとする攻撃者に対して安全に鍵共有を行うことが可能か考察する．

次のような攻撃モデルを考えよう．攻撃者 Eve は King から Alice への量子通信路上において，鍵の情報を盗むような任意の量子操作を 1 量子ビットごと行う．いま，King が物理量 σ_x を選び射影測定を行ったとする．このとき，Eve が手にする量子ビット系 $\mathcal{H}_K$ の量子状態は King の得た測定値に応じて σ_x の固有状態 $|+\rangle\langle+|$ か $|-\rangle\langle-|$ となる．Eve は手に入れた量子系 $\mathcal{H}_K$ と自分で準備した補助系 $\mathcal{H}_E$ を相互作用させ後，$\mathcal{H}_K$ を Alice へ送り $\mathcal{H}_E$ はプロトコルが終了するまで保持する．このとき，Eve は $\mathcal{H}_E$ の状態を識別することで鍵の情報を得る．King が σ_x を選び得る鍵が 0（測定値 1）だった場合と 1（測定値 -1）だった場合の，Eve が保持する $\mathcal{H}_E$ の最終的な状態をそれぞれ $\Lambda_E^*(|+\rangle\langle+|)$ と $\Lambda_E^*(|-\rangle\langle-|)$ とする．我々は Eve が得る二種類の状態の識別可能性をトレースノルムで表すことにする：

$$0 \leq \|\Lambda_E^*(|+\rangle\langle+|) - \Lambda_E^*(|-\rangle\langle-|)\|_1 \leq 1$$

この値は $\Lambda_E^*(|+\rangle\langle+|) = \Lambda_E^*(|-\rangle\langle-|)$ のときにのみ 0 となる．

次に King と Alice が共有する鍵の誤り率を求める．いま，King が物理量 σ_z を選んだとする．このとき，King の得る鍵が 0（測定値 1）だった場合と 1（測定値 -1）だった場合に応じて，Alice が保持している量子ビット系 $\mathcal{H}_A$ の状態は $|0\rangle\langle0|$ か $|1\rangle\langle1|$ となる．また，Eve の量子操作の後の $\mathcal{H}_K$ の状態をそれぞれ ρ_0' と ρ_1' とする．最終的に Alice が測定前に手にする量子系 $\mathcal{H}_A \otimes \mathcal{H}_K$ の状態は $|0\rangle\langle0| \otimes \rho_0'$ か $|1\rangle\langle1| \otimes \rho_1'$ となる．これらの状態に対して鍵の誤り率（Mean King 問題における Alice が King の測定値 i を正しく推定できない確率）を計算すると，Alice が測定 R を選んだ場合には $P(\mathrm{error}_R \mid \sigma_z(i)) = 1/2(1 - \langle i|\rho_i'|i\rangle)$ であり，測定 L を選んだ場合には $P(\mathrm{error}_L \mid \sigma_z(i)) = 1/2(1 - \langle i|\rho_i'|i\rangle)$ である．これらの誤り率と上記の識別可能性から次の定理を得た．

定理 3 *Alice* が測定 $S \in \{R, L\}$ を選んだとき次が成り立つ：

$$\|\Lambda_E^*(|+\rangle\langle+|) - \Lambda_E^*(|-\rangle\langle-|)\|_1 \leq 2\sqrt{2} \sum_{i \in \{1,-1\}} \sqrt{P(\mathrm{error}_S \mid \sigma_z(i))}$$

定理 3 は，Eve が σ_x から作られる鍵を識別できればできるほど，σ_z から作られる鍵の誤り率が高まることを意味している．よって，鍵の誤り率が 0 でない場合には Eve が情報を得たと検知できる．また，σ_x と σ_z の役割を入れ替えることで，σ_z の鍵の識別可能性と σ_x の鍵の誤り率に関する不等式も同様に得られる．

一方で，Alice が測定 M または N を選んだ場合を考察しよう．King が σ_z を選び Alice が測定 M を選んだ場合の鍵の誤り率は $P(\mathrm{error}_M \mid \sigma_z(i)) = 0$ となる．つまり，Eve が σ_x の鍵を識別できたとしても σ_z の鍵の誤り率は 0 となるので，鍵の誤り率から Eve が情報を得たことを検知できな

い．また，King が σ_x を選び Alice が測定 N を選んだ場合の鍵の誤り率は $P(\mathrm{error}_N \mid \sigma_x(i)) = 0$ となる．よって，σ_x と σ_z の役割を入れ替え測定 M の場合と同様のことが言える．これらの結果より，二種類の Mean King 問題を解くことは安全な量子鍵配送を構成するための十分条件でないことがわかる．

4 まとめ

本講究禄では，量子推定問題の一つである Mean King 問題に関する既存研究を要約した．Mean King 問題は非可換な物理量の固有状態を遅延情報を利用し推定する問題として捉えることができ，理論的興味から様々な研究が行われてきた．その中でも本講究禄では，我々が示した一般化した Mean King 問題に対する量子誤り訂正符号を用いた解法と，同解法を応用した Mean King 問題を用いた量子鍵配送の修正と考察に関して詳しく述べた．前者は，Mean King 問題と量子誤り訂正符号の関係の理解が深めるだけでなく，解が存在する Mean King 問題の設定を拡張することができた成果である．後者は，Mean King 問題を解くことが安全な量子鍵配送を構成することの十分条件でないことを示した成果である．

参考文献

[1] L. Vaidman, Y. Aharonov, and D. Z. Albert, "How to ascertain the values of σ x, σ y, and σ z of a spin-1/2 particle," Phys. Rev. Lett. 58, 1385-1387 (1987).

[2] J. Bub, "Secure key distribution via pre- and postselected quantum states," Phys. Rev. A 63, 032309 (2001).

[3] 吉田，宮寺，木村，今井，"量子誤り訂正符号を用いた Mean King 問題の解法，" 量子情報技術研究会 (QIT26) 予稿集 (2012).

[4] M. Yoshida, T. Miyadera, and H. Imai, "Quantum Key Distribution using Mean King Problem with Modified Measurement Schemes," Proc. of International Symposium of Information Theory and Its Applications(ISITA2012), pp.317-212 (2012).

[5] Y. Aharonov and B.-G. Englert, "The mean king's problem: Spin 1," Z. Naturforsch., A:Phys. Sci. 56a, 16 (2001).

[6] B.-G. Englert and Y. Aharonov, "The mean king's problem: Prime degrees of freedom," Phys. Lett. A 284, 1 (2001).

[7] A. Klappenecker and M. Rotteler, "New Tales of the Mean King," e-print quant-ph/0502138.

[8] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz, "Time Symmetry in the Quantum Process of Measurement," Phys. Rev. 134, B1410 (1964).

[9] W. K. Wootters, and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," Ann. Phys. 191, Issue 2, pp.363-381 (1988).

[10] I. D. Ivonović, "Geometrical description of quantal state determination," J. Phys. A 14, 3241 (1981).

[11] A. Hayashi, M. Horibe, and T. Hashimoto, "Mean king ' s problem with mutually unbiased bases and orthogonal Latin squares," Phys. Rev. A 71, 052331 (2005).

[12] G. Kimura, H. Tanaka, and M. Ozawa, "Solution to the mean king ' s problem with mutually unbiased bases for arbitrary levels," Phys. Rev. A 73, 050301(R) (2006).

[13] M. Reimpell, and R. F. Werner, "A Meaner King uses Biased Bases," Phys. Rev. A 75, 062334 (2007).

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

[15] P. K. Aravind, "Best conventional solutions to the King's Problem," Z. Naturforsch. 58a, pp.682-690 (2003).

[16] A. H. Werner, T. Franz, and R. F. Werner, "Quantum cryptography as a retrodiction problem," Phys. Rev. Lett. 103, 220504 (2009).

[17] E. Knill, and R. Laflamme, "Theory of Quantum Error-Correcting Codes," Phys. Rev. A 55, pp.900-911 (1997).