n 次元量子状態を使用した量子コイン投げプロトコル

早稲田 篤志[†] 双紙 正和[†] 宮地 充子[†]

2 者間で行う量子コイン投げにおいて，片方が不正を行うと，コイン投げの結果が c であると納得させられる確率に，$Prob(c=0) \leq 1/2+\epsilon$，$Prob(c=1) \leq 1/2+\epsilon$ という偏りが生じる．この ϵ をバイアスという．このバイアス ϵ について，いかなる不正を行っても $\epsilon = 0$ とする理想的な量子コイン投げプロトコルは存在しないことが，Lo らにより示されている[7]．そのため，ϵ を可能な限り小さくするようなプロトコルの提案が求められている．このようなプロトコルの例として，Ambainis により提案されたプロトコルが存在する[2]．このプロトコルは 3 次元量子状態を使い，$\epsilon = 1/4$ を実現している．本稿では，Ambainis により提案された量子コイン投げプロトコルを拡張し，n 次元量子状態を使用する量子コイン投げを提案する．そのため，まず n 次元量子状態の構成法を提案し，次にコイン投げプロトコルを提案する．この提案プロトコルを解析し，片方のバイアスを犠牲にすることで，もう片方のバイアスを任意に小さくすることが可能であることを示す．これにより，様々な状況への適用が期待できる．また両者のバイアスを均等にすると，Ambainis により提案されたプロトコルと同じバイアス $\epsilon = 1/4$ となる．すなわち，Ambainis のプロトコルは提案プロトコルの特殊な場合として含まれている．

Quantum Coin Flipping Protocol Using n-dimensional Quantum States

Atsushi Waseda,[†] Masakazu Soshi[†] and Atsuko Miyaji[†]

When two players execute a ***quantum coin flipping protocol*** to reach an agreement on a value c, if one of them is dishonest, then deviation ϵ from probability $1/2$ arises, that is, we have $Prob(c=0) \leq 1/2+\epsilon$ and $Prob(c=1) \leq 1/2+\epsilon$. The value ϵ is called a *bias*. Lo and Chau show that there is no quantum coin flipping with bias 0 [7]. So, quantum coin flipping protocols which make bias as small as possible are desirable and many studies have been made about them. As an example of them, Ambainis proposed a protocol [2] with bias $1/4$ using three dimensional quantum states. In this paper, we propose a quantum coin flipping protocol using n dimensional quantum states by generalizing the protocol using three dimensional quantum states proposed by Ambainis [2]. In our protocol, we can reduce the bias of one player arbitrarily by accepting the increase of the bias of the other player. Our generalized protocol could be applied to various situations.

1. はじめに

DES や RSA といった既存の暗号系は，その安全性の根拠を離散対数問題や素因数分解問題等の，計算量的困難性においている．しかし，近年の計算機能力の向上や，将来的な量子計算機の登場により，これらの安全性に危惧が生じている．そこで，安全性の根拠を計算量的安全性ではなく，量子の物理的性質に置く量子暗号の研究がさかんになってきている．これに関連して，認証やマルチパーティプロトコル等の基礎であるビットコミットメントを拡張した量子ビットコミットメントや，その応用である量子コイン投げ等の研究もさかんに行われている[1)~8),10),13)~15)]．

2 者間で行われる量子コイン投げは，片方が不正を行うとコイン投げの結果を出す確率に偏り ϵ が生じる．この偏りをバイアスといい，このバイアス ϵ を 0 とする理想的なプロトコルは存在しないということが知られている[7]．そのため，このバイアス ϵ を可能な限り小さくするプロトコルが求められている．この例として，Ambainis により提案された量子コイン投げプロトコルが存在する[2]．Ambainis のプロトコルは 3 次元量子状態を使い，バイアス $\epsilon = 1/4$ を実現している．

本稿では，この量子コイン投げについて着目し，Ambainis の手法が 3 次元量子状態を使用していたのに対し，使用する量子状態を一般的な n 次元量子状態に

† 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology

拡張したプロトコルを提案する．このプロトコルを使用すると，片方のバイアスを犠牲にすることで，もう片方のバイアスを任意に小さくすることができることを示す．この結果から，提案プロトコルは様々な状況への適用が期待できる．また，両者のバイアスを均等にすると，Ambainis により提案されたプロトコルと同じバイアス $\epsilon = 1/4$ となるという結果が得られる．この結果は，Ambainis のプロトコルが提案プロトコルの特別な場合であることを示している．

本稿の構成は，以下のとおりである．まず，2 章では準備として，本稿で使用される記法および諸定義と，量子コイン投げに対する既存の研究について簡単に述べる．3 章で n 次元量子状態を用いる量子コイン投げの提案を行い，4 章では Alice と Bob のそれぞれが不正を行った場合のバイアスの評価を行う．5 章でいくつかの考察を行い，最後に 6 章でまとめとする．

2. 準　　備

この章では，本稿で使用する用語や記法について簡単に紹介し，量子コイン投げの既存研究について述べる．なお，用語等のより詳しい解説については文献 11) を参照されたい．

2.1 諸 定 義

- 純粋状態（Pure state）：
  系 A の純粋状態は，正規化されたベクトル $|\psi\rangle \in \mathbb{C}^n$ で表される．ここで，系 A の正規直交基底を $|0\rangle, |1\rangle, \ldots, |n-1\rangle$ とすると，系 A の任意の純粋状態は $|\psi\rangle = \sum_{i=0}^{n-1} a_i |i\rangle$ で表される．ここで，$a_i \in \mathbb{C}$ であり，$|\psi\rangle$ の正規化条件から $\sum_i |a_i|^2 = 1$ である．
- 混合状態（Mixed state）：
  混合状態は，純粋状態 $|\psi_i\rangle$ のアンサンブル $(p_i, |\psi_i\rangle)$ で与えられる．ここで，$0 \leq p_i \leq 1$ かつ $\sum_i p_i = 1$ である．すなわち，確率 p_i で状態 $|\psi_i\rangle$ をとることを意味している．
- 密度行列（Density matrix）ρ：
  密度行列は，混合状態 $(p_i, |\psi_i\rangle)$ を記述する統計作用素で，その量子系の統計的性質を完全に規定する．混合状態 $(p_i, |\psi_i\rangle)$ の密度行列 ρ は，以下で定義される：
  $$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{1}$$
- ユニタリ発展：
  量子系のユニタリ発展は，ユニタリ変換 U で記述される．純粋状態 $|\psi\rangle$ が U でユニタリ発展した場合は，$U|\psi\rangle$ となる．また，密度行列 ρ が U でユニタリ発展した場合は，$U\rho U^\dagger$ となる．
- 忠実度（Fidelity）：
  忠実度は，2 つの状態 ρ^A と ρ^B の間の距離の尺度である．ここで，ρ^A と ρ^B の間の忠実度を $F(\rho^A, \rho^B)$ と表す．さらに，忠実度について以下の 2 つの Lemma が知られている．

Lemma 1 [1),8)] 拡大空間 $H \otimes K$ の状態 $|\psi_A\rangle$ と $|\psi_B\rangle$ から，系 K の状態を部分トレースで取り除いた状態を，それぞれ ρ^A と ρ^B とする．このとき $\rho^A = \rho^B$ ならば，系 K の状態を変換することで，$|\psi_A\rangle$ を $|\psi_B\rangle$ に変換することができる．

Lemma 2 [16)]
$$F(\rho^A, \rho^B) = \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho^A}\rho^B\sqrt{\rho^A}} \right) \right)^2.$$

- 純粋化（Purification）：
  ρ^A を系 A の混合状態とする．このとき，ある補助的な系 R を用いることで，結合系 $R \otimes A$ に対する純粋状態 $|\psi^{RA}\rangle$ を構成することができる．このことを純粋化という．
- アクセシブル情報量（Accesible Information）：
  情報源を固定したとき，量子測定過程を通して得られる最大情報量を，アクセシブル情報量という．このアクセシブル情報量の上限 m は，以下の Holevo 限界の定理により与えられる．

Theorem 1（*Holevo* 限界）
$$m \leq S(\rho) - \sum_i p_i S(\rho_i) \tag{2}$$

ここで $\rho = \sum_i p_i \rho_i$ であり，$S(\rho)$ は *von Neumann* エントロピーと呼ばれ，$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$ である．

2.2 量子コイン投げ

ここでは，既存の量子コイン投げの研究について紹介する．まず，本稿の対象である strong 量子コイン投げについての定義を行う．

Definition 1 [2)] バイアス ϵ を持つ，*strong* 量子コイン投げプロトコルとは，*Alice* と *Bob* の *2* 者間で通信を行い，以下を満たすような値 $c \in \{0, 1\}$ を互いに合意することである．

- *Alice* と *Bob* がともに正直な（プロトコルに従う）場合，その確率は $Prob(c = 0) = Prob(c = 1) = 1/2$ を満たす．
- 片方のみが正直で，もう片方が不正を行う場合，確率は $Prob(c = 0) \leq 1/2 + \epsilon, Prob(c = 1) \leq 1/2 + \epsilon$ で与えられる．この ϵ をバイアスという．

量子コイン投げには strong コイン投げのほかに，weak 量子コイン投げが存在する．その定義は以下のようになる．

Definition 2 バイアス ϵ を持つ，*weak* 量子コイン投げプロトコルとは，*Alice* と *Bob* の *2* 者間で通信を行い，以下を満たすような値 $c \in \{0,1\}$ を互いに合意することである．

- *Alice* と *Bob* がともに正直な（プロトコルに従う）場合，その確率は $Prob(c=0) = Prob(c=1) = 1/2$ を満たす．
- *Bob* が正直で，*Alice* が不正を行う場合，確率は $Prob(c=0) \leq 1/2+\epsilon$ で与えられる．
- *Alice* が正直で，*Bob* が不正を行う場合，確率は $Prob(c=1) \leq 1/2+\epsilon$ で与えられる．

以上のように，weak コイン投げを strong 量子コイン投げと比較すると，Alice が不正をして $c=1$ に，Bob が不正をして $c=0$ とする場合については考慮しないという違いがある．

また，量子コイン投げにおけるバイアス ϵ については，Lo らにより，$\epsilon=0$ とする完全な量子コイン投げプロトコルは存在しないことが証明されている[7]．そこで，このバイアス ϵ を可能な限り小さくするプロトコルが求められている．その代表的な例として，strong コイン投げに対しては，Ambainis[2] により提案された方法が，weak コイン投げの例としては Spekkens ら[14]，Mochon[10] により提案されたプロトコル等が存在する．

weak 量子コイン投げの例である Spekkens らによる方法と Mochon により提案された方法のそれぞれのバイアスは $1/\sqrt{2}-1/2$，0.192 となっている．たとえば，Spekkens らによる方法では，weak コイン投げで考慮していない Alice が不正をして $c=1$ にする場合と，Bob が不正をして $c=0$ にする場合は，その不正成功確率は 1 となる

対して，strong 量子コイン投げについては，本稿が基としている Ambainis により提案された手法が存在する．このプロトコルは，量子ビットコミットメントを応用したプロトコルである．また，このプロトコルは，Alice と Bob のバイアスが等しくなるように構成されており，そのバイアスは $\epsilon=0.25$ である．この結果は，Alice と Bob のそれぞれのバイアスを等しくした場合についての strong 量子コイン投げにおけるバイアスの理論的な下限である $1/\sqrt{2}-1/2$[3),6)] に最も近いプロトコルである．しかしながら，この strong 量子コイン投げのバイアスの理論的な下限は，量子ビットコミットメントを使用した量子コイン投げでは実現できないことも知られている[13]．

3. 提案プロトコル

この章では，本稿で提案する strong 量子コイン投げプロトコルについて述べる．量子コイン投げプロトコルでは，n 次元量子状態を使用するため，まずその量子状態を定義する．

3.1 n 次元量子状態の構成

本プロトコルは，Ambainis により提案された，3 次元量子状態を使用した量子コイン投げプロトコルを基に構成している．そこで，まず Ambainis により提案された量子状態を紹介する．

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) & \cdots \ b=0, x=0, \\ \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) & \cdots \ b=0, x=1, \\ \frac{1}{\sqrt{2}}(|0\rangle+|2\rangle) & \cdots \ b=1, x=0, \\ \frac{1}{\sqrt{2}}(|0\rangle-|2\rangle) & \cdots \ b=1, x=1. \end{cases} \quad (3)$$

これを基に $|3\rangle$ を付け加えることで，単純に 4 次元量子状態を構成する方法として以下のようなものがあげられる[4]．

$$|\psi_{b,x,y}\rangle = \begin{cases} \sqrt{\frac{2}{3}}|\phi_{b,x}\rangle+\sqrt{\frac{1}{3}}|3\rangle & \cdots \ y=0, \\ \sqrt{\frac{2}{3}}|\phi_{b,x}\rangle-\sqrt{\frac{1}{3}}|3\rangle & \cdots \ y=1. \end{cases} \quad (4)$$

ここで，$|\phi_{b,x}\rangle$ は Ambainis により提案された量子状態である．このケースで Alice が不正を行った場合の Alice のバイアス ϵ_{Alice} と，Bob が不正を行った場合の Bob のバイアス ϵ_{Bob} を計算すると，$\epsilon_{Alice}=1/3$ と $\epsilon_{Bob}=1/6$ となり，Alice 側にバイアスが偏ることが分かる．以上から，同様に状態を付加していくことで n 次元量子状態を実現しても，Alice 側にバイアスを偏らせることはできるが，Bob 側にバイアスを偏らせることはできないことが分かる．このように，Alice，Bob の任意の側にバイアスを偏らせることが可能で，かつ両者のバイアスの値を平等にしたときには，Ambainis のプロトコルと同じバイアスを持つような量子状態の構成法については自明でなく，今まで知られていなかった．そこで，我々はバイアスを任意に偏らせることができるように，新たな状態の構成法を以下のように提案する．

(1) 必要とされるバイアスに対応した量子の次元数 n と，$t \in \{0,\ldots,n\}$ を選ぶ．ただし $n-t \equiv 0 \pmod 2$ を満たすものとする（バイアスと n, t のより具体的な関係については Lemma 3，4 を参照）．

(2) 高さ $h = t+(n-t)/2$ となる完全 2 分木を考える．ここで，各々の葉に状態名に対応する番号付け $b, x_1, \ldots, x_{h-1}$ を行う．ただし，$b \in \{0,1\}$ であり，$x_i \in \{0,1\}$ $(i = 1, \ldots, h-1)$ である．

(3) 下記に従い，各レベル（根からの距離）ごとの節点に状態 $\pm|0\rangle, \pm|1\rangle, \ldots, \pm|n-1\rangle$ を割り振る．

(a) レベル 1 のとき，

(i) $t = 0$ ならば，片方の節点に $+|0\rangle$ を，もう片方の節点に $+|1\rangle$ を割り振る．

(ii) $t \neq 0$ ならば，両方の節点に $+|0\rangle$ を割り振る．

(b) レベル $2 \leq \ell \leq t$ のとき，
同じ親からなる 2 節点のうちの片方に $+|\ell-1\rangle$ を，もう片方の節点に $-|\ell-1\rangle$ を割り振る．

(c) レベル $t < \ell \leq h$ のとき，

(i) 木の右半分については，同じ親からなる 2 節点のうち，片方の節点に $+|t+2(\ell-t-1)\rangle$ を，もう片方の節点に $-|t+2(\ell-t-1)\rangle$ を割り振る．

(ii) 木の左半分については，同じ親からなる 2 節点のうち，片方の節点に $+|t+2(\ell-t-1)+1\rangle$ を，もう片方の節点に $-|t+2(\ell-t-1)+1\rangle$ を割り振る．

(4) 根から葉 $b, x_1, \ldots, x_{h-1}$ までの経路上の節点に割り振られた状態を $a_i|y_i\rangle (a_i \in \{+1,-1\}, 1 \leq i \leq h)$ とする．このとき，量子状態 $|\phi_{b,x_1,\ldots,x_{h-1}}\rangle$ を以下のように定義する．

$$|\phi_{b,x_1,\ldots,x_{h-1}}\rangle = \frac{1}{\sqrt{h}} \sum_{i=1}^{h} a_i|y_i\rangle. \quad (5)$$

例として，$\epsilon_{Alice} = 1/3$ と $\epsilon_{Bob} = 1/6$ とする場合，その 2 文木は**図 1** のようになり，$n = 4$，$t = 2$ とした場合の 2 分木に対応する．この木により，状態 $|\phi_{010}\rangle$ は $(|0\rangle - |1\rangle + |2\rangle)/\sqrt{3}$ で与えられることが分かる．

3.2 量子コイン投げプロトコル

3.1 節において定義された，n 次元量子状態を使用した strong 量子コイン投げを定義する．

(1) Alice は，$b, x_1, \ldots, x_{h-1} \in \{0,1\}$ をランダムに選び，状態 $|\phi_{b,x_1,\ldots,x_{h-1}}\rangle$ を Bob に送る．

(2) Bob は，ランダムに $b' \in \{0,1\}$ を選び，Alice に送る．

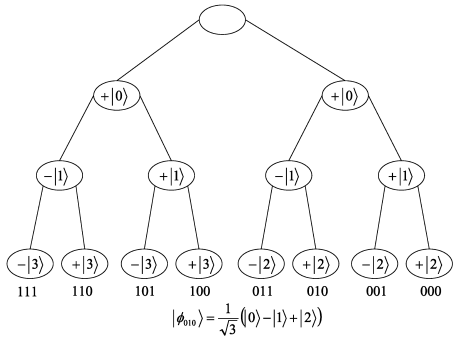

図 1 $n = 4$，$t = 2$，$|\phi_{010}\rangle$ の場合
Fig. 1 Case of $n = 4$, $t = 2$ and $|\phi_{010}\rangle$.

(3) Alice は，$b, x_1, \ldots, x_{h-1}$ を Bob に送る．

(4) Bob は，(1) で受け取った状態 $|\phi_{b,x_1,\ldots,x_{h-1}}\rangle$ が正しいものかを観測する☆．もし正しく観測できなければ，Alice が不正を行ったと判断し，プロトコルを停止する．

(5) 正しく観測できたなら，$c = b \oplus b'$ をコイン投げの結果とする．

4. 評　　価

この章では，提案した n 次元量子状態を使用した量子コイン投げにおいて，Alice または Bob が不正を行って $b \oplus b' = 0$（$b \oplus b' = 1$）が得られる確率を計算する．なお，攻撃モデルは Ambainis [2] によるモデルと同様のモデルである．

まず，Alice が Bob に送信する状態を考える．もし Alice が $b = 0$ を選んだ場合，Alice が送る混合状態 ρ^0 は，各状態 $|\phi_{0,x_1,\ldots,x_{h-1}}\rangle, x_i \in \{0,1\}$ を確率 $1/2^{h-1}$ の等確率で選んだものと等しい．同様に，Alice が $b = 1$ を選んだ場合，Alice が送る混合状態 ρ^1 は，各状態 $|\phi_{1,x_1,\ldots,x_{h-1}}\rangle, x_i \in \{0,1\}$ を確率 $1/2^{h-1}$ の等確率で選んだものに等しい．以上から，密度行列 ρ^0 の ij 成分を ρ^0_{ij} とすると以下の式で与えられる：

$$\rho^0_{ii} = \begin{cases} \frac{1}{h} & \cdots \ 1 \leq i \leq t, \text{ または} \\ & \quad i = t+2k-1 \ (1 \leq k \leq \frac{n-t}{2}), \\ 0 & \cdots \ i = t+2k \ (1 \leq k \leq \frac{n-t}{2}), \end{cases}$$
$$\rho^0_{ij} = 0 \quad \cdots \ \text{それ以外}.$$

同様に ρ^1 の各成分は

☆ 観測は，送られてきた量子状態から Gram-Schmidt の直交化法等の方法を用いることで正規直交基底を量子状態の次元数分だけ作成し，それに対応する測定作用素を生成して行う．

$$\rho^1_{ii} = \begin{cases} \frac{1}{h} & \cdots \ 1 \le i \le t, \text{ または,} \\ & \quad i=t+2k \ (1 \le k \le \frac{n-t}{2}), \\ 0 & \cdots \ i=t+2k-1 \ (1 \le k \le \frac{n-t}{2}), \end{cases}$$
$$\rho^1_{ij} = 0 \quad \cdots \ \text{それ以外}.$$

次に，$X = t/n$ $(0 \le X \le 1)$ と定義する．X は，ρ_0 と ρ_1 の非直交度を表す尺度になっている．本稿ではこの X を使ってプロトコルの解析を行う．

4.1 Bob が不正を行う場合

まず，Bob が $b \oplus b' = 0$ $(b \oplus b' = 1)$ となるように不正を行う場合を考える．ここで，Bob の不正とは，Alice から送られてきた状態 $|\phi\rangle$ を，Bob が b' を選択する前に観測することで b を予測し，自分に都合の良い b' を選択することをいう．このときの Bob のバイアスについて以下が成り立つ．

Lemma 3 *Bob* のバイアス ϵ_{Bob} について以下が成り立つ：

$$\epsilon_{Bob} = \frac{1}{4} - \left(\frac{3}{4} - \frac{1}{1+X}\right). \tag{6}$$

Proof 文献 1) の Theorem 3 より，Bob が $b' = b$ を得られる確率は，たかだか以下のようになる．

$$\begin{aligned} & \frac{1}{2} + \frac{\mathrm{Tr}\,|\rho^0 - \rho^1|}{4} \\ &= \frac{1}{2} + \frac{n-t}{4h} \\ &= \frac{1}{2} + \frac{n-t}{2(n+t)} \\ &= \frac{1}{2} + \frac{1-X}{2(1+X)}. \end{aligned} \tag{7}$$

したがって，Bob のバイアスは，以下のようになる．

$$\begin{aligned} \epsilon_{Bob} &= \frac{1-X}{2(1+X)} \\ &= \frac{1}{4} - \frac{3X-1}{4(1+X)} \\ &= \frac{1}{4} - \left(\frac{3}{4} - \frac{1}{1+X}\right). \end{aligned} \tag{8}$$

■

また，Kent [5] や Tsurumaru [15] は量子 n ビット列コミットメントに対し，アクセシブル情報量より，ビットが漏洩することを示している．そこで本プロトコルにおいて，Alice が送信した ρ のアクセシブル情報量 m を計算すると以下のようになる．

$$\begin{aligned} m &\le -\rho \log \rho - \left(-\frac{1}{2}\rho^0 \log \rho^0 - \frac{1}{2}\rho^1 \log \rho^1\right) \\ &= \frac{1-X}{1+X} \le 1 \end{aligned} \tag{9}$$

ここで $\rho = \rho^0/2 + \rho^1/2$ である．

本プロトコルでは，Alice のコインとして ρ_0 か ρ_1 を送信している．したがってアクセシブル情報量 m が 1 を超えてはならない．しかし，式 (9) より m は条件を満たしている．

これらの結果より，Bob の不正に対しバイアスを下げるには，X の値を大きくとればよいことが分かる．

4.2 Alice が不正をする場合

Alice が不正を行って，$b \oplus b' = 0$ とできる確率を求める．ここでいう Alice の不正とは，本来 Bob に送信する状態 $|\phi\rangle$ とは異なった状態 $|\psi\rangle$ を送り，観測時に Bob に $|\psi\rangle$ を $|\phi\rangle$ であると納得させることをいう．なお，まったく同じ議論が $b \oplus b' = 1$ とする場合についても成り立つ．このとき，Alice のバイアスについて以下が成り立つ．

Lemma 4 *Alice* のバイアス ϵ_{Alice} について，以下が成り立つ：

$$\epsilon_{Alice} = \frac{1}{4} + \left(\frac{3}{4} - \frac{1}{1+X}\right). \tag{10}$$

Proof 文献 2) の Lemma 6 と同様の方法により，Alice がプロトコルの (1) で使用する状態 ρ に対し，同じ不正成功確率で以下のような ρ' も Bob に送信することができる．

$$\rho' = \begin{pmatrix} \delta_0 & & & 0 \\ & \delta_1 & & \\ & & \ddots & \\ 0 & & & \delta_{n-1} \end{pmatrix};$$

$$\sum_{i=0}^{n-1} \delta_i = 1.$$

この ρ' は以下のように生成できる．以下の条件を満たす $n \times n$ の対角行列 U_i $(i = 0, \ldots, 2^{n-1})$ を用意する．

(1) 対角成分 a_{ii} は，$a_{ii} \in \{1, -1\}$.

(2) $i \ne j$ ならば，$U_i \ne U_j$ かつ $U_i \ne -U_j$.

このような行列 U_i は，以下の性質を持つ．

(1) 任意の U_i $(1 \le i \le 2^{n-1})$ と $|\phi_{b,x}\rangle$ $(b \in \{0,1\}, 0 \le x \le 2^{h-1}-1)$ に対し，$|\phi_{b,x}\rangle = U_i|\phi_{b,x'}\rangle$ となるような x' $(0 \le x' \le 2^{h-1}-1)$ が存在する．

(2) $U_i^\dagger = U_i$.
(3) $U_i^2 = I$.
(4) $U_iU_jU_i = U_j$.

U_i を用いることで，0 か 1 が得られる確率が同じまま，Alice がプロトコルの (1) で使用する状態 $|\phi_{b,x}\rangle$ を，$U_i|\phi_{b,x}\rangle$ に置き換えることができる．以上から，Alice によって送られる状態の密度行列は，次の式で与えられる．

$$\rho' = \frac{1}{2^{n-1}} \sum_{i=1}^{2^{n-1}} U_i \rho U_i^\dagger. \tag{11}$$

よって，ρ' を以後の解析に用いる．まず，以下の Lemma 5，6 を証明する．

Lemma 5 *Alice* が *Bob* に対し，$b = 0$ と納得させる確率はたかだか $F(\rho', \rho^0)$ である．

Proof Alice が Bob に対し，$b = 0$ であるという不正を行うために選択した状態 ρ' を純粋化すると式 (12) になるとする．

$$|\psi\rangle = \sum_i a_i |i\rangle|\psi_i\rangle \tag{12}$$

ここで，Alice は Bob に対して $b = 0$ であるという不正を行うので，$|\phi_{0,0\cdots00}\rangle, \cdots, |\phi_{0,1\cdots11}\rangle$ のいずれかであると納得させることになる．次に，$|\psi_i\rangle$ と $|\psi_j\rangle = U_k|\psi_i\rangle$ が同じグループになるようにグループ分けを行う．このグループについて以下が成り立つ．

(1) $|\psi_i\rangle$ と $|\psi_j\rangle$ が同じグループに含まれている場合，$a_i = a_j$ である．
(2) $|\psi_i'\rangle = U_k|\psi_i\rangle$ と $|\psi_j'\rangle = U_k|\psi_j\rangle$ について，$\langle\psi_i|\psi_i'\rangle = \langle\psi_j|\psi_j'\rangle$ が成り立つ．

以上から式 (12) は以下のように変形できる．

$$|\psi\rangle = \sum_i a_i \sum_{j=0}^{2^{h-1}-1} \frac{1}{\sqrt{2^{h-1}}} |i,j\rangle|\psi_{i,j}\rangle. \tag{13}$$

ここで $|\psi_i'\rangle = |\phi_i\rangle$ と置くと，$|\psi_i\rangle$ を $|\psi_i'\rangle$ として Bob に受理される確率は，$|\langle\psi_i|\psi_i'\rangle|^2$ で与えられる．したがって，Bob が受理する確率の合計は，

$$\sum_i |a_i|^2 \frac{1}{2^{h-1}} \sum_{j=0}^{2^{h-1}-1} |\langle\psi_j|\psi_j'\rangle|^2. \tag{14}$$

である．
次に，$|\varphi_i\rangle$ と $|\varphi_i'\rangle$ を次のように定義する．

$$|\varphi_i\rangle = \sum_{j=0}^{2^{h-1}-1} \frac{1}{\sqrt{2^{h-1}}} |i,j\rangle|\psi_{i,j}\rangle. \tag{15}$$

$$|\varphi_i'\rangle = \sum_{j=0}^{2^{h-1}-1} \frac{1}{\sqrt{2^{h-1}}} |i,j\rangle|\psi_{i,j}'\rangle. \tag{16}$$

このように定義すると以下の式が得られる．

$$\begin{aligned}\langle\varphi_i|\varphi_i'\rangle &= \frac{1}{2^{h-1}} \sum_{j=0}^{2^{h-1}-1} \langle\psi_j|\psi_j'\rangle \\ &= \langle\psi_{i,k}|\psi_{i,k}'\rangle \ (0 \le k \le 2^{h-1}-1).\end{aligned} \tag{17}$$

よって式 (14) は以下の式に変形できる．

$$\sum_i |a_i|^2 |\langle\varphi_i|\varphi_i'\rangle|^2. \tag{18}$$

次に，ρ_i を確率 $1/2^{h-1}$ で状態 $|\psi_{i,j}\rangle$ $(0 \le j \le 2^{h-1}-1)$ をとる密度行列とすると，$\rho' = \sum_i |a_i|^2 \rho_i$ が成り立つ．$|\varphi_i\rangle$ と $|\varphi_i'\rangle$ は，ρ_i と ρ_0 を純粋化したものであるので，$|\langle\varphi_i|\varphi_i'\rangle|^2 \le F(\rho_i, \rho^0)$ が得られ，次式が得られる．

$$\sum_i |a_i|^2 |\langle\varphi_i|\varphi_i'\rangle|^2 \le \sum_i |a_i|^2 F(\rho_i, \rho^0). \tag{19}$$

最後に忠実度の凹性[11] より，次式が得られる．

$$\begin{aligned}\sum_i |a_i|^2 F(\rho_i, \rho^0) &\le F\left(\sum_i |a_i|^2 \rho_i, \rho^0\right) \\ &= F(\rho, \rho^0).\end{aligned} \tag{20}$$

■

同様に以下が成り立つ．

Lemma 6 *Alice* が *Bob* に対し，$b = 1$ と納得させる確率はたかだか $F(\rho', \rho^1)$ である．

以上を使用すると，文献 2) の Lemma 8 より，Alice が，$b \oplus b' = 0$ とできる確率はたかだか $(F(\rho', \rho^0) + F(\rho', \rho^1))/2$ であることが示されているので，Lemma2 より，

$$\begin{aligned}F(\rho', \rho^0) &= \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho'}\rho^0\sqrt{\rho'}}\right)\right)^2 \\ &= \left(\sqrt{\frac{\delta_0}{h}} + \ldots + \sqrt{\frac{\delta_{t-1}}{h}} + \sqrt{\frac{\delta_t}{h}}\right.\end{aligned}$$

$$+\sqrt{\frac{\delta_{t+2}}{h}}+\ldots+\sqrt{\frac{\delta_{n-2}}{h}}\Bigg)^2. \quad (21)$$

$$F(\rho',\rho^1)=\left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho'}\rho^1\sqrt{\rho'}}\right)\right)^2$$
$$=\Bigg(\sqrt{\frac{\delta_0}{h}}+\ldots+\sqrt{\frac{\delta_{t-1}}{h}}+\sqrt{\frac{\delta_{t+1}}{h}}$$
$$+\sqrt{\frac{\delta_{t+3}}{h}}+\ldots+\sqrt{\frac{\delta_{n-1}}{h}}\Bigg)^2. \quad (22)$$

ここで $\sum_{i=0}^{n-1}\delta_i=1$ である．

したがって，

$$\frac{1}{2}(F(\rho',\rho^0)+F(\rho',\rho^1))$$
$$=\frac{1}{2h}\Big(\Big(\sqrt{\delta_0}+\ldots+\sqrt{\delta_{t-1}}$$
$$+\sqrt{\delta_t}+\sqrt{\delta_{t+2}}+\ldots+\sqrt{\delta_{n-2}}\Big)^2$$
$$+\Big(\sqrt{\delta_0}+\ldots+\sqrt{\delta_{t-1}}$$
$$+\sqrt{\delta_{t+1}}+\sqrt{\delta_{t+3}}+\ldots+\sqrt{\delta_{n-1}}\Big)^2\Big);$$
$$\sum_{i=0}^{n-1}\delta_i=1 \quad (23)$$

式 (23) は $\delta_0=\delta_1=\ldots=\delta_{t-1}=4/(n+3t)$, $\delta_t=\delta_{t+1}=\ldots=\delta_{n-2}=\delta_{n-1}=1/(n+3t)$ のとき，$(n+3t)/(4h)=(n+3t)/(2(n+t))=1/2+t/(n+t)=1/2+X/(1+X)$ で最大になる．以上から Alice のバイアス ϵ_{Alice} は，以下のようになる．

$$\epsilon_{Alice}=\frac{X}{1+X}$$
$$=\frac{1}{4}+\left(\frac{3}{4}-\frac{1}{1+X}\right) \quad (24)$$

■

5. 考　　察

この章では，提案プロトコルについて，いくつかの観点で議論する．

5.1 不正成功確率の妥当性

Alice が不正を行い出力を 1 にできる確率を p_{1*}, Bob が不正を行い出力を 1 にできる確率を p_{*1} としたとき，その確率は次の式を満たすことが知られている[3]．

$$p_{1*}p_{*1}\geq\frac{1}{2}. \quad (25)$$

したがって，$\max\{p_{1*},p_{*1}\}\geq\frac{1}{\sqrt{2}}$ である．提案プロトコルでは，p_{1*} と p_{*1} は次で与えられる．

$$p_{1*}=\frac{1}{2}+\epsilon_{Alice}=\frac{3}{4}+\left(\frac{3}{4}-\frac{1}{1+X}\right), \quad (26)$$
$$p_{*1}=\frac{1}{2}+\epsilon_{Bob}=\frac{3}{4}-\left(\frac{3}{4}-\frac{1}{1+X}\right). \quad (27)$$

ここで $0\leq X\leq 1$ であるから，$p_{1*}p_{*1}\geq 1/2$ を満たすことが分かる．このように，範囲内で任意に X をとっても式 (25) に抵触しない．

5.2 アクセシブル情報量による漏洩

Alice は n 次元量子状態である ρ_0 か ρ_1 を，Bob に送信している．一般に，n 次元量子状態を使用した場合のアクセシブル情報量は $n\log n\geq 1$ となり，この場合は b の値が漏洩することになる[15]．しかし，Holevo 限界の定理と使用する状態を使い，厳密にアクセシブル情報量を求めると，提案プロトコルのアクセシブル情報量は $(1-X)/(1+X)\leq 1$ で与えられる．以上から提案プロトコルでは，アクセシブル情報量の観点から，b の値が漏洩することはないことが分かる．

5.3 Ambainis [2] のプロトコルとの関係

我々のプロトコルは，n と t を選択することで，Alice か Bob のバイアスを任意に選ぶことができるという特徴が存在する．これはまた，一度バイアスを決定すると，n と t の値も最小にすることができることも意味している．このように，提案プロトコルは様々な状況に応じて効率的に対応できる．さらに，大きな特徴として，一方のバイアスを増やすことで，もう一方のバイアスを任意に小さくすることができるという特徴がある．このことが有用に使用できる例として，下記のような乱数共有をあげる．認証等において，二者間で乱数を共有することがよく行われる[9),12)]．この乱数共有ステップをコイン投げで実現することを考える．Bob は検証者である認証サーバ（またはセンタ）であると仮定し，Alice は正規のユーザ（Charlie）に成りすまして認証を行う攻撃者と仮定する．このとき，Alice は Charlie と Bob のやりとりから，乱数 r と，Charlie の秘密情報 x と r から作り出した情報 $I=f(x,r)$ を記録する．次に Alice は Charlie に成りすまし，認証を試みる．Alice としては乱数共有時に $r'=r$ とできれば I を使用することで Charlie に成りすますことができる．この例の場合，Bob はセンタであるため，Alice，Charlie という個人に比べ信用を置くというのは一般的によく用いられる仮定である．したがって，Bob のバイアスをある程度犠牲にし，Alice のバイアスを下げることができる．さらに，Alice は

表 1 代表的な場合のバイアス
Table 1 Biases in typical cases.

X	0	$\frac{1}{3}$	1
ϵ_{Alice}	0	$\frac{1}{4}$	$\frac{1}{2}$
ϵ_{Bob}	$\frac{1}{2}$	$\frac{1}{4}$	0

Charlie と Bob の間で共有された乱数 r に結果を合わせることが目的である．したがって，Alice が不正をして，共有する情報を $c=0$ とする場合のみを考えている weak コイン投げでは対応ができないといえる．

ここで代表的な場合について**表 1** にまとめる．

この例のように，X のとり方により，Alice，Bob のバイアスは $0 \leq \epsilon \leq \frac{1}{2}$ からとることができることが分かる．例として，$X=1/3$ とすると，ϵ_{Alice} と ϵ_{Bob} は 1/4 となり同じ値になる．これは，ちょうど Ambainis によるプロトコルと同じ結果になっている．すなわち，Ambainis のプロトコルは，提案プロトコルの特別な場合となっているといえる．また，提案プロトコルは，一方のバイアスを増やすことで，もう一方のバイアスを任意に小さくすることができるという Ambainis のプロトコルが持たない機能を持ち，Ambainis のプロトコルの拡張となっていることが分かる．

6. ま と め

本稿では，Ambainis により提案された，3 次元量子状態を使用した量子コイン投げを拡張し，n 次元量子状態を使った量子コイン投げの提案を行った．その結果，Alice と Bob のバイアスはそれぞれ $\epsilon_{Alice} = 1/4 + (3/4 - 1/(1+X))$，$\epsilon_{Bob} = 1/4 - (3/4 - 1/(1+X))$ という結果が得られた．これは一方のバイアスを犠牲にすることで，もう一方のバイアスを任意に小さくすることが可能であることを意味している．さらに，両者のバイアスを $\epsilon = 0$ とすることはできないが，片方のみならばバイアスを $\epsilon = 0$ とすることができることを示している．この結果より，様々な状況への適用が期待できる．また，$X=1/3$ としたとき，$\epsilon_{Alice} = \epsilon_{Bob} = 1/4$ となり，Ambainis により提案されたコイン投げも，特別な場合として提案プロトコルに含まれているといえる．

謝辞 本研究成果は文部科学省 21 世紀 COE プログラム，および，文部科学省科学技術振興調整費による．

参 考 文 献

1) Aharonov, D., Ta-Shma, A., Vazirani, U. and Yao, A.: Quantum bit escrow, *Proc. STOC'00*, pp.705–714 (2000).
2) Ambainis, A.: A New Protocol and Lower Bounds for Quantum Coin Flipping, *Journal of Computer and System Sciences* (2004).
3) Ambainis, A., Buhrman, N., Dodis, Y. and Röhrig, H.: Multiparty Quantum Coin Flipping. quant-ph/0304112.
4) 福田明香，双紙正和，宮地充子：量子コイン投げにおけるバイアスの考察—3 状態から 4 状態プロトコルへの拡張，TECHINICAL REPORT OF IEICE, ISEC2003-4 (2003).
5) Kent, A.: Quantum Bit String Commitment, *Phy. Rev. Lett.*, Vol.90, No.237901 (2003).
6) Kitaev, A.Y.: Quantum Coin Flipping (2002). Talk at QIP2003 (slides and video at MSRI).
7) Lo, H. and Chau, H.: Why quantum bit commitment and ideal quantum coin tossing are impossible, *Physica D*, Vol.120, pp.177–187 (1998).
8) Mayers, D.: Unconditionally secure quantum bit commitment is impossible, *Phy. Rev. Lett.*, Vol.78, No.3414 (1997).
9) 宮地充子，菊池浩明：情報セキュリティ，オーム社 (2003).
10) Mochon, C.: Quantum weak coin-flipping with bias of 0.192, *45th Annual IEEE Symposium on Foundations of Computer Science*, pp.2–11 (2004).
11) Nielsen, M. and Chuang, I.: *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
12) 岡本龍明，山本博資：現代暗号，産業図書 (1997).
13) Spekkens, R.W. and Rudolph, T.: Degrees of concealment and bindingness in quantum bit commitment protocols, *Phy. Rev. A*, Vol.65, No.012310 (2001).
14) Spekkens, R.W. and Rudolph, T.: Quantum protocol for cheat-sensitive weak coin flipping, *Phy. Rev. Lett.*, Vol.89, No.227901 (2002).
15) Tsurumaru, T.: An Implementable Protocol of Quantum Bit String Commitment. quant-ph/0407174.
16) Uhlmann, A.: The 'transition probability' in the state space of *-algebra, *Report on Mathematical Physics*, Vol.9, pp.273–279 (1976).

(平成 16 年 12 月 2 日受付)
(平成 17 年 6 月 9 日採録)

早稲田篤志

平成 12 年電気通信大学電気通信学部電子情報学科卒業．平成 14 年北陸先端科学技術大学院大学情報科学研究科情報システム学専攻博士前期課程修了．現在，同博士後期課程在学．

双紙　正和（正会員）

1991 年東京大学工学部卒業．1993 年同大学大学院理学系研究科情報科学専攻修了．電気通信大学大学院情報システム学研究科助手を経て，1999 年から 2003 年 1 月まで北陸先端科学技術大学院大学情報科学研究科助手．2003 年 2 月から同研究科特任助教授．現在に至る．情報セキュリティの研究に従事．博士（工学）．

宮地　充子（正会員）

1988 年大阪大学理学部数学科卒業．1990 年同大学大学院修士課程修了．同年松下電器産業株式会社入社．1998 年北陸先端科学技術大学院大学・情報科学研究科助教授．現在に至る．2002〜2003 年カリフォルニア大学デービス校客員研究員．情報セキュリティの研究に従事．博士（理学）．SCIS93 若手論文賞，科学技術庁注目発明賞，坂井記念特別賞，標準化貢献賞各受賞．電子情報通信学会，IACR 各会員．