社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (33)
2006／7／21

二つの状態を用いたしきい値量子秘密分散法

岡田 健† 桑門 秀典†† 森井 昌克††

† 神戸大学大学院自然科学研究科
〒657-8501 神戸市灘区六甲台町 1-1
†† 神戸大学工学部
〒657-8501 神戸市灘区六甲台町 1-1
E-mail: †068t209n@stu.kobe-u.ac.jp, ††{kuwakado,mmorii}@kobe-u.ac.jp

あらまし しきい値量子秘密分散法とは，量子状態で表される秘密情報を複数の分散情報に分割し，あるしきい値以上の分散情報から秘密情報を復元できる方法である．Cleve と Gottesman と Lo が提案したしきい値量子秘密分散法は，三つ以上の量子状態が必要となる．本論文では，量子ビット間に形成される量子力学特有のエンタングルメントの性質を利用し，二つの量子状態からなる分散情報を持つしきい値量子秘密分散法を提案する．
キーワード しきい値量子秘密分散法，エンタングルメント

Quantum Threshold Scheme Using Two States

Takeshi OKADA†, Hidenori KUWAKADO††, and Masakatu MORII††

† Graduate School of Science and Technology, Kobe University
1-1Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan
†† Faculty of Engineering, Kobe University
1-1Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan
E-mail: †068t209n@stu.kobe-u.ac.jp, ††{kuwakado,mmorii}@kobe-u.ac.jp

Abstract Cleve, Gottesman, and Lo have shown the (k,n) quantum threshold scheme using several states. However, it is not easy to implement three (or more) states. In this paper, we propose a (k,n) quantum threshold scheme using only two states. The proposed scheme is the generalization of the (n,n) quantum threshold scheme shown by Hillery, Buzek, and Berthiaume. The proposed scheme requires entangled particles as many as share holders.
Key words quantum threshold scheme, entanglement

1. はじめに

秘密情報を安全に管理する方法の一つとして，しきい値秘密分散法がある [1] [5]．(k,n) しきい値秘密分散法とは，秘密情報を n 個の分散情報に分割し，任意の k 個の分散情報から秘密情報を復元することができるが，任意の $k-1$ 個以下の分散情報からでは秘密情報を復元することができない方法である．特に，量子状態を秘密情報とする方法はしきい値量子秘密分散法と呼ばれる．(n,n) しきい値量子秘密分散法は，1998 年に Hillery と Buzek と Berthiaume [4] により提案され，1999 年に，Cleve と Gottesman と Lo [2] は，複数の量子状態を利用した (k,n) しきい値量子秘密分散法 (CGL 法) を提案した．

現在，量子暗号や量子コンピュータの研究開発が盛んに行われているが，三つ以上の量子状態を作り出すことや，その状態を用いて演算を行うことは難しいので，量子状態を表す素子として，二つの直交状態で表される粒子が用いられることが多い．

そこで，本論文では，二つの量子状態 (qubit) を用いた (k,n) しきい値量子秘密分散法を提案する．秘密情報を持つディーラと分散情報を持つユーザの間で，エンタングルメント状態の粒子を所有する．さらに，ディーラがベル状態の測定を行い，その結果を古典通信路で k 人のユーザに伝える．そして，k 人のユーザが協力し合うことで，二つの状態からなる (k,n) しきい値量子秘密分散法を行うことができる．

本論文の構成は以下の通りである．第 2 章で CGL 法について述べる．第 3 章で提案方式である二つの状態を用いた (k,n) しきい値量子秘密分散法について述べ，CGL 法と提案方式の比較を行う．最後に，第 4 章で結論を述べる．

2. CGL 法

CGL 法の手順を $(2,3)$ しきい値法を用いて述べる．秘密情

報を三つの量子状態 (qutrit) を用いて $\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle$ のような重ね合わせの状態で表し，秘密の量子状態を以下のように符号化する．

$$\begin{aligned}\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle \rightarrow\ & \alpha(|000\rangle+|111\rangle+|222\rangle) \\ & +\beta(|012\rangle+|120\rangle+|201\rangle) \\ & +\gamma(|021\rangle+|102\rangle+|210\rangle)\end{aligned} \tag{1}$$

ここで，各 qutrit を分散情報とする．このとき，個々の分散情報から秘密情報を推測したり復元できない．しかし，どの二つの分散情報からでも秘密情報を復元することができる．例えば，一番目の分散情報と二番目の分散情報が与えられたとき，法を 3 として，一番目の分散情報の値を二番目の分散情報に加え，次に，二番目の分散情報の値を一番目の分散情報に加えることで，式 (1) から以下の状態を得ることができる．

$$(\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle)(|00\rangle+|12\rangle+|21\rangle) \tag{2}$$

このとき，一番目の qutrit から秘密情報を得ることができる．他の分散情報の組合せの場合も，三つの qutrit の循環的並べ替えにより，同様に秘密情報を得ることができる．

この方法では，秘密情報を二つの量子状態，つまり qubit で表すことは可能であるが，分散情報は qubit で表すことができず，全て qutrit で表さなくてはならない．このことは，1 qubit の消失誤りを訂正する 3 qubit 誤り訂正符号が存在しないことから証明されており [3]，その場合，qubit の秘密情報 $\alpha|0\rangle+\beta|1\rangle$ は以下のように符号化される．

$$\begin{aligned}\alpha|0\rangle+\beta|1\rangle \rightarrow\ & \alpha(|000\rangle+|111\rangle+|222\rangle) \\ & +\beta(|012\rangle+|120\rangle+|201\rangle)\end{aligned} \tag{3}$$

秘密情報を復元するときは，上記と同様の処理を行うことで，以下の状態を得ることができる．

$$(\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|12\rangle+|21\rangle) \tag{4}$$

一番目の qutrit から秘密情報を得ることができる．このことから，CGL 法では，(2,3) しきい値法を行うために三つの状態を必要とすることがわかる．

3. 二つの状態を用いたしきい値法

本章では，二つの状態を用いた (k,n) しきい値法について述べる．量子状態として，スピン $\frac{1}{2}$ の粒子を用いる．ここで，二つの直交状態 $|0\rangle$ と $|1\rangle$ を，z 軸方向の上向きと下向きに対応させると，$|0\rangle$ と $|1\rangle$ を用いて異なる直交基底である x 軸方向の上向き $|+x\rangle$ と下向き $|-x\rangle$ はそれぞれ，

$$|+x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ |-x\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{5}$$

となる．

提案方式では，秘密情報をディーラが持ち，n 人のユーザがそれぞれ分散情報を持つ．そして，k 人のユーザの協力によって，秘密情報を復元する．

例として，(2,3) しきい値法の手順について述べる．まず，分割の手順を説明する．初めに秘密の量子情報を所有するディーラを Alice，分散情報を所有する三人のユーザを Bob，Charlie，Diana とする．秘密分散を行うために，Alice と Bob と Charlie がエンタングル状態の三粒子を所有する．ここで，エンタングルメントとは，複数の qubit 間に形成される量子もつれ合いのことで 1 qubit の状態が決定することにより，他の qubit の状態も決定するという性質のことである．また，Alice と Bob と Diana，Alice と Charlie と Diana もエンタングル状態の三粒子をそれぞれ所有する．つまり，Alice は秘密の量子情報を持つ粒子を含めて四つの粒子を所有し，Bob，Charlie，Diana はそれぞれ二つの粒子を所有する．次に，Alice は所有している四つの粒子を作用させる．この作業により，秘密の粒子の情報は失われる．ここまでが分割の手順である．

続いて，復元の手順を説明する．まず，Bob，Charlie，Diana が相談して三人のうちどの二人で秘密情報を復元するかを決定する．ここでは，Bob と Charlie の二人で復元することとする．Bob と Charlie はそれぞれ Diana の所有する粒子とエンタングルしている粒子の状態を測定する．それぞれの粒子はエンタングルしているので，この測定によって Bob と Charlie は，Diana から全く情報を得ずに Diana の所有する粒子の状態を知ることができる．次に，Alice は，Bob と Charlie の粒子とエンタングルしている粒子と秘密情報を表す粒子の二粒子に対してベル状態を測定し，その結果を Bob と Charlie に送る．そして，Bob と Charlie は二人のうちどちらが秘密情報を復元するのかを決める．ここでは，Charlie とする．Bob は自分の粒子を x 基底で測定し，その測定結果を Charlie に送る．最後に，Charlie は，Alice と Bob からの情報をもとに自分の粒子に対して特定の変換を行うことで，秘密情報を復元することができる．

この分散法の手順を式や図を用いて具体的に説明する．Alice の所有する秘密情報を表す粒子の状態を，

$$\alpha|0\rangle+\beta|1\rangle \tag{6}$$

とする．まず，Alice と Bob と Charlie の三人の組み合わせを考える．その三人が所有する三粒子のエンタングル状態を，

$$\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle) \tag{7}$$

とする．式 (7) は，3 qubit のうちどれか 1 qubit を測定したとき，その測定結果が $|0\rangle$ であれば残りの 2 qubit の状態も $|0\rangle$ となり，$|1\rangle$ であれば残りの 2 qubit の状態も $|1\rangle$ となることを意味する．また，他の三人の組合せの場合のエンタングル状態も式 (7) と同様とする．このとき，四人の所有する粒子は図 1 のようになる．次に，Alice が所有している四つの粒子を作用させると以下の式のようにそれぞれの状態のテンソル積をとることになる．

$$\begin{aligned}&(\alpha|0\rangle+\beta|1\rangle)\otimes\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle) \\ &\otimes\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)\otimes\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)\end{aligned} \tag{8}$$

ここまでが分割である．復元において，Bob と Charlie はそれ

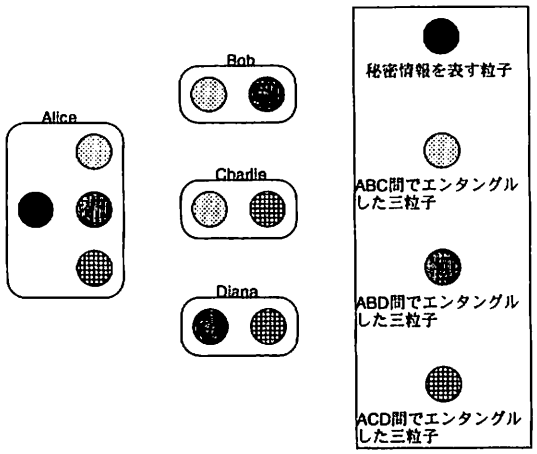

図 1　四人の所有する粒子

ぞれ Diana の粒子とエンタングルしている粒子の状態を測定すると，$|0\rangle$ か $|1\rangle$ の値を得る．このとき，Bob と Charlie の測定結果によって，二つの場合がある．

（1）　測定結果がともに $|0\rangle$ またはともに $|1\rangle$ の場合

Alice と Bob と Charlie の所有する四粒子の状態は，

$$\frac{1}{2}\big(|\Psi_+\rangle(\alpha|00\rangle-\beta|11\rangle)+|\Psi_-\rangle(\alpha|00\rangle+\beta|11\rangle) +|\Phi_+\rangle(\beta|00\rangle-\alpha|11\rangle)+|\Phi_-\rangle(-\beta|00\rangle-\alpha|11\rangle)\big) \quad (9)$$

で表される．ここで，$|\Psi_+\rangle$，$|\Psi_-\rangle$，$|\Phi_+\rangle$，$|\Phi_-\rangle$ は，以下の式で表されるベル状態である．

$$|\Psi_+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\quad |\Psi_-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),$$
$$|\Phi_+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\quad |\Phi_-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \quad (10)$$

例えば，Alice がベル状態 $|\Psi_+\rangle$ を測定したとすると，Bob と Charlie の二粒子は，エンタングルメント状態

$$(\alpha|00\rangle-\beta|11\rangle) \quad (11)$$

となることを，式 (9) は意味している．また式 (11) は，x 基底を用いることで，

$$\alpha|00\rangle-\beta|11\rangle = \frac{1}{\sqrt{2}}\big(|+x\rangle(\alpha|0\rangle-\beta|1\rangle)+|-x\rangle(\alpha|0\rangle+\beta|1\rangle)\big) \quad (12)$$

となるので，Bob が $|+x\rangle$ を測定した場合，式 (12) の量子相関より Charlie の粒子の状態が $\alpha|0\rangle-\beta|1\rangle$ となっている．そこで，Charlie は，Bob から測定結果が $|+x\rangle$ であることを聞いた後，自分の粒子に対して Pauli のスピン行列 σ_z を用いて，

$$\sigma_z(\alpha|0\rangle-\beta|1\rangle)=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}\alpha\\-\beta\end{pmatrix} =\begin{pmatrix}\alpha\\\beta\end{pmatrix} =\alpha|0\rangle+\beta|1\rangle \quad (13)$$

表 1　測定結果がともに同じ場合に Charlie が行う変換

ベル状態	Bob の状態	変換	ベル状態	Bob の状態	変換
$\|\Psi_+\rangle$	$\|+x\rangle$	σ_z	$\|\Phi_+\rangle$	$\|+x\rangle$	$\sigma_x\sigma_z$
	$\|-x\rangle$	変換なし		$\|-x\rangle$	σ_x
$\|\Psi_-\rangle$	$\|+x\rangle$	変換なし	$\|\Phi_-\rangle$	$\|+x\rangle$	$\sigma_z\sigma_x\sigma_z$
	$\|-x\rangle$	σ_z		$\|-x\rangle$	$\sigma_z\sigma_x$

表 2　測定結果が互いに異なる場合に Charlie が行う変換

ベル状態	Bob の状態	変換	ベル状態	Bob の状態	変換
$\|\Psi_+\rangle$	$\|+x\rangle$	$\sigma_x\sigma_z\sigma_x$	$\|\Phi_+\rangle$	$\|+x\rangle$	$\sigma_z\sigma_x$
	$\|-x\rangle$	$\sigma_x\sigma_z\sigma_x\sigma_z$		$\|-x\rangle$	$\sigma_z\sigma_x\sigma_z$
$\|\Psi_-\rangle$	$\|+x\rangle$	$\sigma_x\sigma_z\sigma_x\sigma_z$	$\|\Phi_-\rangle$	$\|+x\rangle$	σ_x
	$\|-x\rangle$	$\sigma_x\sigma_x\sigma_x$		$\|-x\rangle$	$\sigma_x\sigma_z$

なる変換を行うことで自分の粒子の状態を秘密情報と同じ状態にすることができる．

Alice のベル状態の測定結果と Bob の x 基底の測定結果によって，Charlie が自分の粒子に行う変換は異なる．Charlie が行う変換を表 1 に示す．表 1 において，σ_x，σ_z は，Pauli のスピン行列である．

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \quad (14)$$

（2）　測定結果が互いに異なる場合

Bob と Charlie がそれぞれ Diana の所有する粒子とエンタングルしている粒子の状態を測定した測定結果が互いに異なり，Bob が $|0\rangle$ を測定し，Charlie が $|1\rangle$ を測定したと仮定する．このとき，Alice と Bob と Charlie の所有する四粒子の状態は，

$$\frac{1}{2}\big(|\Psi_+\rangle(-\alpha|00\rangle+\beta|11\rangle)+|\Psi_-\rangle(-\alpha|00\rangle-\beta|11\rangle) +|\Phi_+\rangle(-\beta|00\rangle+\alpha|11\rangle)+|\Phi_-\rangle(\beta|00\rangle+\alpha|11\rangle)\big) \quad (15)$$

のような量子相関で表される．この場合の，Alice のベル状態の測定結果と Bob の x 基底の測定結果から，Charlie が行う変換を表 2 に示す．

Alice のベル状態と Bob の測定結果が同じ場合であっても，Bob と Charlie がそれぞれ Diana の所有する粒子とエンタングルしている粒子の状態を測定した測定結果によって，最終的に Charlie が自分の粒子に対して行う変換が異なる．これより，上記の例では，Diana の所有する二粒子の両方の状態がわかっていないと秘密情報を正しく復元することができない．つまり，Bob または Charlie のユーザー人だけでは，全ての粒子の状態を知ることができないので，一人だけで秘密情報を復元することはできない．

(2,3) しきい値量子秘密分散法において，CGL 法と提案方式における，必要な粒子の数，量子状態の数，秘密情報を復元するときの処理回数の比較を表 3 に示す．処理回数とは，演算や測定の回数を表す．また，粒子の数に秘密情報を表す粒子を含まない．この表 3 から提案方式では，必要となる粒子の数や処理回数が，従来方式に比べ増えていることがわかる．しかし，本論文の目的である二つの量子状態を用いることで，量子秘密分散法を実行できることがわかる．

表 3 (2,3) しきい値法における比較

	CGL 法	提案方式
粒子の数	2	9
状態の数	3	2
処理回数	2	5

ここでは，(2,3) しきい値量子秘密分散法についてのみ，その手順を説明した．この方法は，(k,n) しきい値量子秘密分散法に容易に拡張できる．まず，ディーラと n 人のユーザの間で，n 人から k 人を選ぶ全ての組合せにおいて，その k 人のユーザとディーラの間でエンタングルメント状態の粒子を所有する．そして，選ばれた k 人のユーザが残りの $n-k$ 人のユーザの粒子の状態をエンタングルメント粒子の測定により，$n-k$ 人のユーザの協力なしに知る．ディーラがベル状態を測定し，その結果を k 人のユーザに伝え，k 人の中から最終的に秘密情報を復元するユーザを一人決める．$k-1$ 人のユーザは自分の粒子の状態を x 基底で測定し，秘密情報を復元するユーザに伝える．そして，そのユーザが自分の粒子に対して得られた測定結果の情報から特定の変換を行うことで，秘密情報を復元することができる．

4. 結　　論

CGL 法による (k,n) しきい値量子秘密分散法は，秘密情報を表す粒子に対して，$n-1$ 個の粒子を付加し，その n 個の粒子を符号化することで，秘密情報を分割し，k 個の粒子を用いて演算を行うことで秘密情報を復元することができた．しかし，三つ以上の量子状態を用いる必要があった．

そこで本論文では，二つの量子状態を用いた (k,n) しきい値量子秘密分散法を提案した．提案方式では，秘密情報を持つディーラに対し，n 人のユーザを集め，それぞれ k 人のユーザがディーラとエンタングルメント状態の粒子を所有する．そして，ディーラが復元する k 人のユーザに対してベル状態の測定結果を伝え，$k-1$ 人のユーザが自分の粒子を測定し，最後の一人が自分の粒子に対して特定の演算を行うことで，秘密情報を復元することができた．

文　　献

[1] G. Blakely, "Safeguarding cryptographic keys," *American Federation of Information Processing Societies 1979 National Computer Conference*, vol. 48, pp. 313–317, 1979.

[2] R. Cleve, D. Gottesman, and H-K. Lo, "How to share a quantum secret," *quant-ph/9901025*, 1999.

[3] M. Grassl, T. Beth, and T. Pellizzari, "Code for the quantum erasure channel," *Physical Review A*, vol. 56, pp. 33–38, 1997.

[4] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *quant-ph/9806063*, 1998.

[5] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.