A-3

量子カード配布
Quantum Card Dealing

小泉康一 * 水木敬明† 西関隆夫 *
Koichi Koizumi Takaaki Mizuki Takao Nishizeki

1 はじめに

これまでメンタルポーカープロトコル[1]がいくつか考案されてきた．メンタルポーカープロトコルを用いると，ゲームをするプレーヤーが一ヶ所に集まらなくても，電話やインターネットなどの公開通信路を使用してカードゲームを公平に行うことができる．例えば，各々のプレーヤーに5枚ずつカードを配布したり，ある特定のプレーヤーに追加のカードを配布したりすることができる．ほとんどのメンタルポーカープロトコルは，計算量的に安全であり，情報理論的に安全というわけではなく，盗聴者（悪意のあるプレーヤー）の計算能力によっては安全ではなくなってしまう．

一般的に，電話やインターネットなどの公開通信路においては，盗聴者の発見は不可能である．それに対して，**量子通信路**においては，**量子暗号**を用いることにより盗聴者の発見が可能である量子暗号プロトコルの最も代表的なものの一つは，1984年にBennettとBrassardが開発した**BB84プロトコル**[2]である．

AliceとBobがいて，秘密鍵を共有したいとする．BB84プロトコルを使うと，AliceとBobはランダムなビット列を共有することができる．また，BB84プロトコルでは，もしEveがAliceとBobの共有するビット列を盗聴しようとすると，AliceとBobは盗聴者Eveの存在を発見することができる．BB84プロトコルは光子の量子的性質を利用している．

光子を用いてどのようにビット列を共有すればよいだろうか? 例えば，ビットに対して光子1つを対応させて，ビット値0を縦偏光，ビット値1を横偏光として送信することが考えられる．しかし，この方法では盗聴により光子の偏光方向が盗聴者に確実に知られてしまい，光子の捕獲再送攻撃により盗聴されてしまう．このとき，光子の量子的性質を利用すれば1つの光子の偏光方向を盗聴できないようにすることができる．例えば，ビット値の対応を縦方向と横方向ではなく斜め方向を取る場合もあることにすれば，不確定性原理により，盗聴により光子1つの偏光方向を確実に測定することができなくなる．BB84プロトコルに代表される量子暗号は，このような仕組みを利用することにより絶対に安全な暗号系を構築している．

本文では，量子暗号を利用したメンタルポーカープロトコル，すなわち**量子カード配布**を提案する．量子カード配布を用いると，盗聴者の発見が可能であり，情報理論的に安全なカード配布を実現することができる．本文で提案する量子暗号プロトコルはBB84プロトコルに基づいている．

*東北大学大学院情報科学研究科，〒980-8579 宮城県仙台市青葉区荒巻字青葉09
†東北大学情報シナジーセンター，〒980-8578 宮城県仙台市青葉区荒巻字青葉

2 量子カード配布

52枚のカードがあるとし，52次の対称群をS_{52}と書く．ディーラーおよびn人のプレーヤー$P_1, P_2, \cdots, P_n$がいるとする．$\pi \in_R S_{52}$をランダムな置換とする．プレーヤー$P_1, P_2, \cdots, P_n$はπを知っていても知らなくてもよいが，ディーラーはπを知らないとする．図1(a)のように，ディーラーおよびプレーヤー$P_1, P_2, \cdots, P_n$は52芯の光ファイバー通信路で直列に接続されており，ディーラーは装置Iを持ち，$P_1, P_2, \cdots, P_{n-1}$は装置IIIを持ち，$P_n$は装置IIを持つ．また，ディーラーと$P_1$との間に装置IVが設置されている．各装置の機能は次の通りである．

- 装置I　52芯のケーブルを使用して52個の光子を同時に送信することができる．なお，52個の光子各々に対して，0°，45°，90°，135°の4種類の偏光方向のうちいずれか1つを設定できる．(図1(b)参照.)
- 装置II　52芯のケーブルを使用して送られて来た52個の光子を，同時に読みとることができる．読み取る際に，それぞれの52個の光子について縦横基底測定か斜め基底測定かを設定できる．縦横基底測定では，0°，90°の光子を確実に読み取ることができ，45°，135°の光子を読み取ることができない．斜め基底測定では，45°，135°の光子を確実に読み取ることができ，0°，45°の光子を読み取ることができない．(図1(c)参照.)
- 装置III　左右のケーブルをストレートに結線する装置と，装置IIのどちらかを随時選択して使用できる装置である．(図1(d)参照.)
- 装置IV　置換πに対応して左右のケーブルを置換するケーブル置換装置である．(図1(e)参照.)

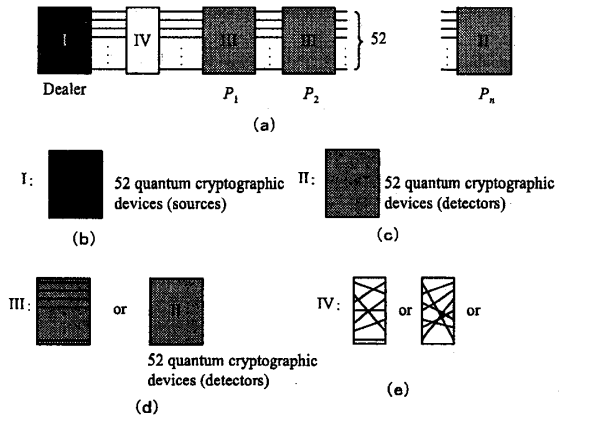

図1: 量子カード配布に使用する量子通信路.

ディーラーは装置IVにアクセスできなく，π を知らないとする．したがって，ディーラーは，ディーラー側のケーブル番号とプレーヤー側のケーブル番号の対応がわからない．

ディーラーはケーブル番号の集合 C を準備する．C の初期状態は，$C = \{1, 2, \cdots, 52\}$ である．セキュリティパラメータとして，自然数 k を選ぶ．k が大きい程盗聴者を検出できる確率が1に近づく．

以下に本プロトコルを示す．これを k-量子カード配布と呼ぶ．プレーヤー P_i にカードを1枚配布するには，次のようにすればよい．

- $1 \leq j \leq i-1$ なる各プレーヤー P_j は，装置IIIとしてストレート結線装置を選択する．したがって，ディーラーとプレーヤー P_i は装置IVを介して直接結ばれるので，ディーラーがケーブル x $(1 \geq x \geq 52)$ に送った光子は，プレーヤー P_i においてはケーブル $\pi(x)$ に届く．
- ディーラーは，ランダムにカード番号 $c \in_R C$ と，時刻 $t \in_R \{1, 2, \cdots, k\}$ を選ぶ．ディーラーは次のようにして，時刻1から時刻 k までの間に，合計 $52k-1$ の光子を，装置Iを使って送信する．

  (i) 時刻 t 以外のとき
  52本のケーブルのそれぞれに対し，4種類の光子からランダムに1つを選び，選んだ光子を送る．すなわち，合計52個のランダムな光子を同時に52芯を使って送る．

  (ii) 時刻 t のとき
  ケーブル c 以外の51本のケーブルそれぞれに対し，4種類の光子からランダムに1つを選び，選んだ光子を送る．すなわち，合計51個のランダムな光子を同時に51芯を使って送る．ケーブル c には光子を送らない．

- プレーヤー P_i は，装置IIを使い，各々の光子に対しランダムに縦横基底か斜め基底かを設定して，送られてきた光子をすべて受け取る．プレーヤー P_i は，時刻 t においてケーブル $\pi(c)$ にだけ光子が送られなかったことを知ることにより，カード $\pi(c)$ を受け取ったとみなす．
- ディーラーは，以後カード $\pi(c)$ を配布しないようにするため，$C := C - \{c\}$ とする．

上のプロトコルを繰り返すことにより，ディーラーはプレーヤーにカードをランダムに配布することができる．

ディーラーおよび各プレーヤーが不正を行わないとき，ディーラーは置換 π を知らないので，プレーヤーに配布されるカードの中身 $\pi(c)$ を知ることはできない．また，プレーヤーも，自分に配布されたカード以外については知ることができない．

図2は，プレイヤー P_2 がカードを1枚受け取る場合のプロトコルの実行例である．ケーブル置換装置IVは $\pi(2) = 4$ なる置換 π に対応しているとする．ディーラーはケーブル（カード）番号 $c = 2$，時刻 $t = 3$ を選び，この部分には光子を送らない．プレーヤー P_2 は光子測定によりケーブル4を使用して送られた光子数が他のケーブルの光子数より1個だけ少ないことを知る．これにより，プレーヤー P_2 にはカード4が配布されたことになる．

次に，量子カード配布プロトコルの安全性を示す．量子カード配布プロトコルにより，プレーヤー P_i がカードを

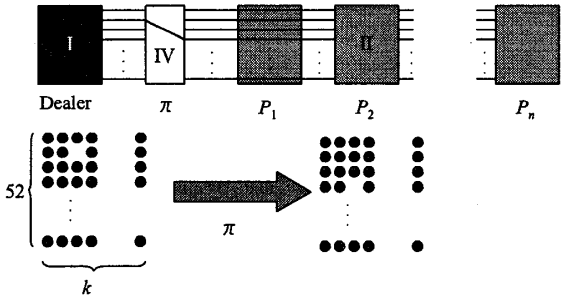

図2: カード配布の例．

1枚受け取ったとする．このとき，悪意のあるプレーヤー $P_j (j \leq i-1)$ が，プレーヤー P_i に配布されたカードを盗聴により不正に知ろうとしても，そのようなプレーヤーの存在を圧倒的確率で検出できる．悪意のあるプレーヤー P_j は，正規のプレーヤー P_i と同様にして光子を受信し，どのケーブルに $k-1$ 個の光子が送られたかを調べた後，光子を再送することにより，P_i のカードを知ることができる．これを**攻撃1**と呼ぶ．この攻撃を防ぐことはできないが，1に近い確率で検出する事が可能である．

定理 1 k-量子カード配布に対して攻撃1が行われたとする．このとき，確率 $1 - (\frac{7}{8})^{52k-1}$ で攻撃を検出できる．

定理1により，セキュリティパラメータ k を大きくすることで，圧倒的確率で攻撃1を検出できることがわかる．

3 むすび

本論文では，メンタルポーカープロトコルと量子暗号の融合ともいうべき，量子カード配布を提案した．量子カード配布により複数人のプレーヤーに対してカードを安全に配布することができ，公平なカードゲームを行うことができる．本方式は，情報理論的に安全であり，悪意のあるプレーヤーが無制限の計算能力を持っていても安全である．

本論文では，ディーラーの存在を仮定したが，ディーラーを必要としないプロトコルの考案は残された課題である．

参考文献

[1] A. Shamir, R. L. Rivest, and L. M. Adleman, "Mental poker," in Mathematical Gardner, D. E. Klarner, ed., Wadsworth International, pp.37–41, 1981.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp.175–179, 1984.