偏光板カードを用いた暗号プロトコル

品川 和雅 †§　　金山 直樹 †　　縫田 光司 §　　西出 隆志 †　　岡本 栄司 †

† 筑波大学
§ 産業技術総合研究所
shinagawa@cipher.risk.tsukuba.ac.jp

あらまし トランプのようなカードを用いて，任意の秘密計算を実現する暗号プロトコルを構成できることが知られている．その際，重要な演算である情報のコピーは，電子的な計算の場合と異なり，決して自明な操作ではない．そのため，コピープロトコルの効率化は，計算全体の効率化をもたらす．ここで，カードを用いた暗号プロトコルにおける効率性は，使用するカード枚数と，シャッフル操作の回数で評価する．本論文では，偏光板をカードとして用いることで，コピープロトコルと XOR プロトコルを効率化する．その他の基本演算も既存の結果と同程度効率的であるため，多くの計算において既存方式よりも効率的なプロトコルを構成することができる．

Card-Based Cryptographic Protocols using Polarization Plates

Kazumasa Shinagawa†§　　Naoki Kanayama†　　Koji Nuida§　　Takashi Nishide†
Eiji Okamoto†

†University of Tsukuba
§National Institute of Advanced Industrial Science and Technology
shinagawa@cipher.risk.tsukuba.ac.jp

Abstract It is known that card-based cryptographic protocols are able to compute any functions securely. In contrast to the electronic solutions, it is non-trivial to construct the copy protocol, which is an essential operation in the card-based protocols. Therefore, making the copy protocol efficient leads to having efficient card-based protocols. Here, we can evaluate the efficiency with the number of cards and shuffles. In this paper, we construct efficient copy and XOR protocols using polarization plates. Other fundamental protocols we proposed are as efficient as state-of-the-art protocols. Thus, we can construct various protocols efficiently.

1　はじめに

暗号プロトコルに関する研究が現在までに多く行われているが，それらの多くはコンピュータ上で実現することを目的としている．

それに対して，暗号プロトコルをコンピュータ以外で実現するという研究の流れも存在し，その代表的なものが，カードを用いた暗号プロトコルである [1][2][3][4][5][6]．使用するのはカード組だけであり，電気やコンピュータなどの特別な機器を使わないため，日常生活における公正な多数決や選挙に適している [6]．また，電子的なプロトコルと異なり，専門的な知識がなくとも原理を理解することが可能で，参加者全員がプロトコルの正しさや安全性を自らの目で確認することができる．

本論文は，偏光板を用いることで，カードを用いた暗号プロトコルを効率化することを目指す．

偏光板とは，特定の方向に偏向した光だけを透過させる板である．1 枚の偏光板を肉眼で観察しても，偏向方向を見分けることはできない．同じ偏向方向の偏光板を重ねると光を透過する

のに対し，直交した偏向方向の偏光板を重ねると光を遮断し暗くなる（図 1）．

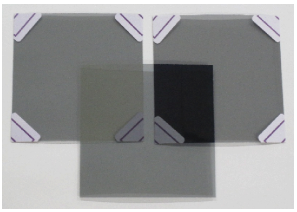


図 1: 偏光板

カードを用いた暗号プロトコルの既存研究は 3 章で，提案方式は 4 章で示す．

1.1 カードを用いた暗号プロトコル

カードを用いた暗号プロトコルでは，入力カード列に対して，並べ替えやシャッフルを実行することで計算を行う．NOT・AND・コピープロトコルが構成できるため，任意の回路計算に対する安全なプロトコルが構成可能である．

カードを用いた暗号プロトコルは，2009 年に提案されたランダム二等分割カットによって大幅に効率化された [5]．それ以前のプロトコルでは，ランダム巡回カットと呼ばれるシャッフルを用いて構成されていたが，使用するカード枚数は多く，また，複数回の試行が必要な確率的なプロトコルであった．ランダム二等分割カットの登場によって，使用するカード枚数の少ない決定的なプロトコルを実現できるようになった．

これらのプロトコルをさらに効率的に実現することはできるだろうか．NOT・XOR プロトコルは入力以外のカードを用いない最小の構成であるため，これ以上カード枚数を減らすことはできない．しかしながら，コピー・AND プロトコルは入力以外のカードも必要であるため，カード枚数を減らせる可能性はあり，これは未解決問題とされている [5][1]．また，プロトコル中のシャッフル操作を除去あるいは簡略化することができるかどうかも同様に興味深い問題である．

表 1 に，既存研究と提案方式の比較をまとめる．枚数の項目で (min) と表記してあるプロトコルは，入力以外にカードを必要としない最小の構成である．また，ランダム二等分割カットを二等分割，ランダム二等分割回転カットを二等分割回転と略記している．これらのシャッフルについては，3 章および 4 章で詳細を説明する．

表 1: 既存研究と提案方式の比較

	枚数	用いるシャッフル
○ NOT プロトコル		
Boer[1]	2(min)	なし
提案方式	2(min)	なし
○ AND プロトコル		
Mizuki-Sone[5]	6	二等分割
提案方式	6	二等分割回転
○ XOR プロトコル		
Mizuki-Sone[5]	4(min)	二等分割
提案方式	4(min)	再ランダム化
○ コピープロトコル		
Mizuki-Sone[5]	6	二等分割
提案方式	4(min)	なし

1.2 貢献

本論文では，通常のトランプのようなカードの代わりに，偏光板をカードとして用いた初めての暗号プロトコルを提案する．

提案方式において，最も基本的なプロトコルである NOT プロトコルは，既存方式と同様に自明に構成できる．また，ランダム二等分割カットによく似た，ランダム二等分割回転カットという新しいシャッフル手法を導入することで，AND プロトコルを構成する．

提案方式が既存方式と大きく異なる基本プロトコルは，XOR プロトコルとコピープロトコルである．

提案方式の XOR プロトコルは既存方式と同様に最小の構成であるが，既存方式では二等分割カットというシャッフルが必須であるのに対し，提案方式で用いる再ランダム化は状況によっては不要になる．シャッフルが不要となる場合があるため，既存方式と比べてプロトコルに必要な操作が少なくなっている．

さらに特筆すべき結果として，コピープロトコルにおいて，カードの種類は異なるが，必要

[1]明示的に未解決問題と述べられているのは AND プロトコルだけであるが，コピープロトコルも同様の問題意識が持たれている．また，NOT・XOR・AND・コピープロトコルのみを取り上げた理由は，これらが既存研究で特に重要視されている基本的なプロトコルだからである．

なカード枚数を減らすという前述の未解決問題を部分的に解決した．コピープロトコルは，既存方式では 6 枚のカードが必要であったが，提案方式では 4 枚のカードのみで実現でき，これは最小の構成である．また，提案方式のコピープロトコルは，プロトコル中のシャッフルが不要であるため，シャッフルが必須であった既存方式と比べて，必要な操作の観点からも単純化できている．

既存方式では，NOT プロトコル以外の基本プロトコルにおいて，シャッフルは不可欠であった．安全にシャッフルを実行するためには，シャッフルする回数を増やすといったコストがかかるため，一般的にシャッフル操作はプロトコルの計算コストの大部分を占めると考えられる．基本的なプロトコルであるコピープロトコルでシャッフルを取り除けたことは，重要な成果であると考えられる．

2 準備

カード（トランプや偏光板）を用いた暗号プロトコルでは，プロトコルに従って，入力，並べ替え，シャッフルを実行し，計算を行う．0,1 の情報はカード組によって符号化される．どちらの値が符号化されているか分からないカード組をコミットという．入力におけるコミットを入力コミット，出力におけるコミットを出力コミットという．また，コミットされたカードの情報を公開することを，開示という．

2.1 semi-honest モデル

カードを用いた暗号プロトコルにおいて，プロトコルの操作はすべて公開された場で行う．従って，プレイヤーはコミットされた情報を密かに得るようなことはできない．本論文では，semi-honest モデルによってプロトコルの安全性を議論する．semi-honest モデルとは，すべてのプレイヤーの振る舞いは，プロトコルから外れることはないが，正しい手続きの範囲内で他のプレイヤーの情報を引き出そうと行動する，と仮定するモデルである．

2.2 安全性定義

カードを用いた暗号プロトコルの安全性を定義する．

定義 2.1 (安全性定義)**.** プロトコル中に開示された値から，自明に得られる情報以外の情報が全く得られないとき，プロトコルは安全であるとする．

明らかに，一切のコミットを開示しないプロトコルは安全である．また，プロトコル中の開示された値がランダムであるとき，以下の定理が成り立つ．

定理 2.1 (ランダムな開示)**.** 任意の入力に対して，プロトコル中に開示されたすべての値が 0 と 1 の一様ランダムな分布に従うとき，そのプロトコルは安全である．

証明. 0 と 1 の一様ランダムな分布から，非自明な情報を得ることはできない． □

2.3 プロトコルの効率性

本論文では，カードを用いた暗号プロトコルにおける効率性を，カードの枚数とシャッフルの回数によって評価する．直観的には，カードの枚数は計算メモリに，シャッフルの回数は計算時間に対応している．

カード枚数とは，入力コミットを含めたプロトコルで用いるカードの枚数であり，シャッフルとは，確率的なカード列の並べ替え操作である．カードを用いた暗号プロトコルの既存研究では，シャッフルを行ったときにどのように並べ替えられたかはシャッフルの実行者，観測者を含め誰も知らないことを暗に仮定している．

計算時間としてシャッフルのみを考える理由は，シャッフル以外の操作は定数時間で行われるのに対し，シャッフルはその場の全員が納得するまで繰り返す操作だからである．なお，シャッフルの回数とは，あるシャッフル中にカットする回数のことではなく，シャッフル自体の適用回数であることに注意されたい．

また，シャッフルがプロトコル中に行われる必要があるのか，それとも事前に実行できるのかということも重要な指標である．本論文では，事前に実行できるシャッフル操作は，プロトコルの効率性に影響しないものとする．

3 既存方式

本章では，カードを用いた暗号プロトコルの既存研究について述べる [5]．まず，プロトコルに用いるカードについての説明と，符号化の方法について述べる．次に，ランダム二等分割カットと呼ばれるシャッフルを導入する．また，このシャッフルを用いたプロトコルのイメージをつかんでもらうために，XOR プロトコルの構成について述べる．本章の最後に， semi-honest でないプレイヤーからの攻撃とその対策について述べる．

3.1 使用するカードと符号化方法

カードを用いた暗号プロトコルでは，$\boxed{\clubsuit}$や$\boxed{\heartsuit}$のような異なるカードを用いる．$\boxed{\clubsuit}$同士，$\boxed{\heartsuit}$同士のカードは全く同一で，区別することはできない．また，これらのカードを裏返した状態では，表が$\boxed{\clubsuit}$か$\boxed{\heartsuit}$のどちらであるかは区別できないものとし，この状態を$\boxed{?}$と表記する．

1 ビットの符号化は$\boxed{\clubsuit}\boxed{\heartsuit} = 0, \boxed{\heartsuit}\boxed{\clubsuit} = 1$のように 2 枚のカードで行う．各プレイヤーは，入力コミットとして自分の保持する秘密情報を裏返した状態で$\boxed{?}\boxed{?}$のように提出する．

3.2 ランダム二等分割カット

ランダム二等分割カットと呼ばれるシャッフルを用いることで，効率的なプロトコルが構成できることが知られている [5]．

例として以下のような 6 枚のカード列を考える．

$$\underbrace{\boxed{?}\boxed{?}\boxed{?}}_{\alpha}\underbrace{\boxed{?}\boxed{?}\boxed{?}}_{\beta}$$

このカード列にランダム二等分割カットを適用することを，以下のように表記する．

$$\left[\boxed{?}\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\boxed{?}\right]$$

シャッフルを適用した結果として，以下のどちらかが一様ランダムで出現する．

$$\underbrace{\boxed{?}\boxed{?}\boxed{?}}_{\alpha}\underbrace{\boxed{?}\boxed{?}\boxed{?}}_{\beta} \quad \text{or} \quad \underbrace{\boxed{?}\boxed{?}\boxed{?}}_{\beta}\underbrace{\boxed{?}\boxed{?}\boxed{?}}_{\alpha}$$

このシャッフルを手操作で実現することは難しくない．

3.3 XOR プロトコル

ランダム二等分割カットを用いて，XOR プロトコルを構成できる [5]．このプロトコルは a, b を入力として受け取り，$a \oplus b$ を出力として返す．また，プロトコルで用いるカードは入力を含めて 4 枚であり，入力以外に余分なカードを必要としない．

1. 4 枚のカードを次のように並べる．

$$\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}.$$

2. 真ん中の 2 枚の位置を入れ替える．
3. ランダム二等分割カットを適用する．

$$\left[\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\right] \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

4. 真ん中の 2 枚の位置を入れ替える．
5. 左端のコミットを開示し，その結果によって出力コミットを得る．

$$\underbrace{\boxed{\clubsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}}_{a\oplus b} \quad \text{or} \quad \underbrace{\boxed{\heartsuit}\boxed{\clubsuit}\boxed{?}\boxed{?}}_{\overline{a\oplus b}},$$

既存方式の XOR プロトコルでは，ランダム二等分割カットを 1 回用いている．既存方式の AND プロトコル，コピープロトコルも同様にランダム二等分割カットを 1 回用いている．それらのプロトコルの詳細については省略する．

3.4 semi-honest モデルから外れた攻撃

semi-honest モデルにおいて，上記のプロトコルは定義 2.1 の意味で安全である．しかし，プレイヤーが semi-honest でない場合は，プロトコルは安全ではない．

例えば，$\boxed{\clubsuit}\boxed{\clubsuit}, \boxed{\heartsuit}\boxed{\heartsuit}$ のような不正な入力コミットをすることで，相手の入力情報を得る不正入力攻撃が考えられる．不正入力攻撃の対策として，コミットされた情報を漏らすことなく，不正な入力コミットでないことを確かめる検証プロトコルが提案されている [4]．しかし，入力コミットに対して検証プロトコルを実行することは，コストもかかることであるため，できることなら検証プロトコルが不要である状況が望ましい．

4　提案方式

本章では，提案方式である，偏光板カードを用いた暗号プロトコルについて述べる．まず，プロトコルに用いる偏光板カードについての説明と，符号化の方法について述べる．次に，いくつかの新しいシャッフルを導入し，AND プロトコル，XOR プロトコル，コピープロトコルを構成する．本章の最後に，semi-honest でないプレイヤーからの攻撃とその対策について述べる．

4.1　偏光板カードと符号化方法

定義 4.1 (偏光板カード)．正方形の偏光板を，偏光板カードという．すべての偏光板カードは，同じ大きさで，偏向方向がそろっているとする．

任意の 2 枚の偏光板カードをぴったり重ねると，透過するか，暗くなるかのどちらかである．ある偏光板カード a に対して，a を 90° 回転したものを $\overline{a}$ と表記する．以後，a と $\overline{a}$ を異なる偏光板カードとして区別し，a と $\overline{\overline{a}}$ を同一の偏光板カードとみなすことにする．

次に，偏光板カードによる符号化方法を定める．既存方式と同様に，1 ビットの情報を 2 枚のカードで符号化する．

定義 4.2 (偏光板カードの符号化)．2 枚の偏光板カード a_0, a_1 に対して，a_0, a_1 を重ねたとき暗くなるときは $(a_0, a_1) = 1$ とし，透過するときは $(a_0, a_1) = 0$ とする．

偏光板の性質から，$a = (a_0, a_1) = (\overline{a_0}, \overline{a_1})$ が成り立つ．また，$\overline{a} = (\overline{a_0}, a_1) = (a_0, \overline{a_1})$ である．ただし，左辺の $\overline{a}$ は真理値の否定を，右辺の $\overline{a_i}$ は 90° 回転した偏光板を表していることに注意されたい．

入力コミットの片方の偏光板カードを 90° 回転する操作が NOT プロトコルであることは明らかである．

4.2　再ランダム化

ランダムな偏光板カードを次のように定義する．

定義 4.3 (ランダムな偏光板カード)．偏光板カード s がランダムであるとは，s 以外の任意の偏光板カード p に対して，(p, s) が一様ランダムとなることである．

ランダムな偏光板カードを手操作で実現するのは難しくない．偏光板カードを回数がわからなくなるまで回転すればよい．

ランダムな偏光板カードを作ることは，プロトコルの前に行うことができるので，この操作はプロトコルの効率性を損なわない．

次に，再ランダム化という，コミットの値を変えないシャッフルを定義する．

定義 4.4 (再ランダム化)．コミット $a = (a_0, a_1)$ の再ランダム化とは，$(a_0, a_1), (\overline{a_0}, \overline{a_1})$ が一様ランダムに生じるシャッフルのことである．

再ランダム化を手操作で実現する場合は，2 枚の偏光板 a_0, a_1 を重ねて，回数がわからなくなるまで回転する．このとき，裸の偏光板カードで素直に行うと，偏光板カードが重ねたときに秘密情報が漏れてしまう．そこで図 2 のように偏光板カードにカバーをかけることで，この問題を回避することができる．プロトコルの実行中は常にカバーをかけておき，コミットを開示するときのみカバーを外せばよい．

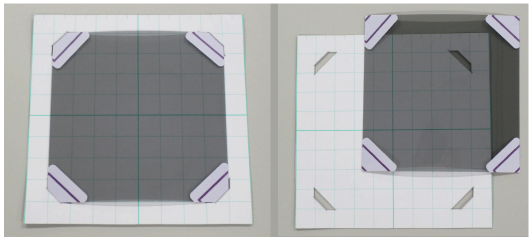


図 2: 偏光板カードのカバー

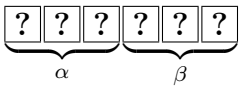
再ランダム化はコミットに依存しているので，ランダムな偏光板カードを作るときと異なり，プロトコルの効率性に影響する．

4.3　ランダム二等分割回転カット

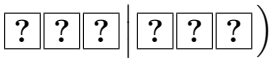
偏光板カードで AND プロトコルを構成するために，ランダム二等分割カットに似た新しいシャッフルを導入する．これをランダム二等分割回転カットと呼ぶ．

ランダム二等分割回転カットを適用したい k 個のコミットの列（$2k$ 枚の偏光板カード列）が

あったとき，最初の k 枚のカード列を α，残りのカード列を β と表すことにする．



ランダム二等分割回転カットを以下のように表記する．

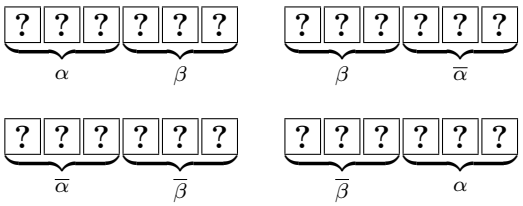


シャッフルの操作手順を以下に示す．

1. カード列を左端が一番上になるように重ね，上半分のカード束を α，下半分のカード束を β とする．
2. α を 90° 回転しながらカード束 β の下に持っていく．

ランダム二等分割回転カットはこの操作をランダムな回数だけ繰り返す．ランダム二等分割カットとの違いは，α を 90° 回転するところのみである．

シャッフルを適用した結果として，以下の 4 つのパターンが一様ランダムで出現する．



ここで $\overline{\alpha}$ は，$\alpha = a_1, \cdots, a_k$ としたとき，$\overline{\alpha} = \overline{a_1}, \cdots, \overline{a_k}$ のように順番を変えずに 90° 回転したカード列である．偏光板カードの符号化に関する性質から，$\alpha\beta$ と $\overline{\alpha}\overline{\beta}$，$\beta\overline{\alpha}$ と $\overline{\beta}\alpha$ はコミットの値について同じ情報を保持している．従って，コミットの値について着目しているとき，ランダム二等分割回転カットは $\alpha\beta$ と $\beta\overline{\alpha}$ が一様ランダムに生じるシャッフルであると考えてよい．

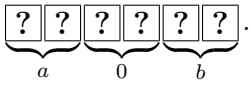
なお，ランダム二等分割回転カットを手操作で実行する場合にも，前節で述べたように偏光板カードにカバーをかける必要がある．

4.4 AND プロトコル

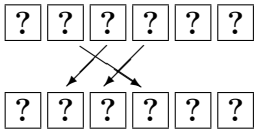
既存方式では，1 回のランダム二等分割カットと 6 枚のカードを用いて，AND プロトコルを構成できた．提案方式では，1 回のランダム二等分割回転カットと 6 枚のカードを用いて，AND プロトコルを構成する．

提案方式の AND プロトコルを以下に示す．

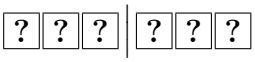
1. 6 枚の偏光板カードを次のように並べる．



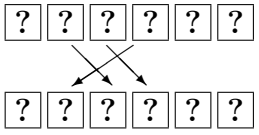
2. 次のように並べ替える．



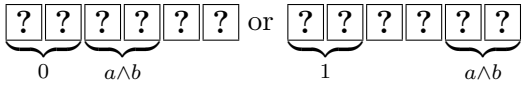
3. ランダム二等分割回転カットを適用する．



4. 次のように並べ替える．



5. 左端のコミットを開示し，その結果によって出力コミットを得る．



提案方式と既存方式の異なる点は，シャッフルとしてランダム二等分割カットではなく，ランダム二等分割回転カットを用いていることである．

上記の AND プロトコルの正しさは次のように確かめられる．4. の操作を終えた段階で，コミット列は $a, 0, b$ と $\overline{a}, b, 0$ が一様ランダムに生じる．左端のコミットの値が 0 なら，$a \wedge b$ は真ん中のコミットの値に等しく，左端のコミットの値が 1 なら，$a \wedge b$ は右端のコミットの値に等しい．

定理 4.1. 提案方式の AND プロトコルは，定義 2.1 の意味で安全である．

証明. 開示するコミットは，それぞれ 1/2 の確率で a と $\overline{a}$ のどちらかになる．これは一様ランダムな値であるので，定理 2.1 より提案方式の AND プロトコルは安全である． □

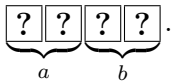
NOT プロトコルと AND プロトコルを用いれば，$a \vee b = \overline{\overline{a} \wedge \overline{b}}$ より，直ちに OR プロトコルを得られる．

4.5 XOR プロトコル

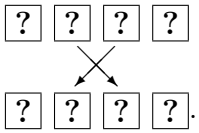
提案方式の XOR プロトコルは，カードの枚数については既存方式と同等であるが，ある状況ではシャッフル操作が不要になるため，既存方式よりも効率的である．

提案方式の XOR プロトコルを以下に示す．

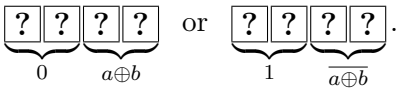
1. 4 枚の偏光板カードを次のように並べる．



2. 次のように並べ替える．



3. 左端のコミットを開示し，その結果によって $a \oplus b$ のコミットを得る．



4. $a \oplus b$ のコミットを再ランダム化して，それを出力コミットとする．

上記の XOR プロトコルの正しさは次のように確かめられる．$a \oplus b$ は a と b が同じ値なら 0 に，異なる値なら 1 になる．$a = (a_0, a_1), b = (b_0, b_1)$ としたとき，開示するコミットは (a_0, b_0) である．開示した値が $(a_0, b_0) = 0$ のとき，$(a_1, b_1) = 0$ なら $a = b$ であり，$(a_1, b_1) = 1$ なら $a \neq b$ である．すなわち $(a_1, b_1) = a \oplus b$ であり，(a_1, b_1) が出力コミットである．開示した値が $(a_0, b_0) = 1$ のときも同様である．

定理 4.2. 提案方式の XOR プロトコルは，定義 2.1 の意味で安全である．

証明. コミット (a_0, b_0) の値には，a_0, b_0 の部分情報が含まれている．しかし，a_1 が秘匿されている状況において，a_0 の情報から (a_0, a_1) を推測することはできない．同様に，b_0 の情報から (b_0, b_1) を推測することはできない．よって，提案方式の XOR プロトコルは安全である． □

以下の状況では，XOR プロトコルの再ランダム化は不要になる．

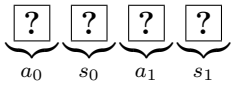
- XOR プロトコルの直後に AND プロトコルを適用するとき
- XOR プロトコルの直後に OR プロトコルを適用するとき

AND プロトコルや OR プロトコルで用いられる二等分割回転カットは，再ランダム化と同じ効果をもたらす．すなわち，XOR プロトコルの直後に二等分割回転カットを適用する状況においては，再ランダム化を省略することができる．従って，秘密計算をしたい関数によっては，提案方式の XOR プロトコルは既存方式に比べて，必要な操作の観点から効率化されている．

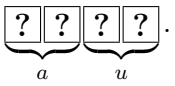
4.6 コピープロトコル

コピープロトコルは，1 ビットのコミットを 2 ビットのコミットに複製するプロトコルである．既存方式では必要なカード枚数は 6 枚であったが，提案方式で必要な枚数は 4 枚であり，これは最小の構成である．コピープロトコルで必要なランダムな偏光板は，事前に作っておくことができるため，プロトコル中でシャッフル操作を行う必要はない．従って，カードの枚数とシャッフルの回数のどちらの観点からも，提案方式は効率的である．

1. 入力コミット $a = (a_0, a_1)$ と，ランダムな 2 枚の偏光板カード s_0, s_1 を次のように並べる．



2. (a_0, s_0) を開示し，その結果が 1 なら $u_0 = \overline{s_0}$ とし，そうでないなら $u_0 = s_0$ とする．
3. (a_1, s_1) を開示し，その結果が 1 なら $u_1 = \overline{s_1}$ とし，そうでないなら $u_1 = s_1$ とする．
4. $a = (a_0, a_1), u = (u_0, u_1)$ を出力コミットとする．



明らかに $(a_0, a_1) = (u_0, u_1)$ であり，上記のコピープロトコルは正しい．

定理 4.3. 提案方式のコピープロトコルは，定義 2.1 の意味で安全である．

証明．s_0, s_1 はランダムな偏光板カードであるから，コミット $(a_0, s_0), (a_1, s_1)$ の値は一様ランダムになる．定理 2.1 より提案方式のコピープロトコルは安全である． □

4.7 semi-honest モデルから外れた攻撃

既存方式と同様に，プレイヤーがsemi-honestでない場合は，提案方式のプロトコルは安全ではない．

しかし，提案方式では，既存方式のときに有効であった不正入力攻撃は存在しない．なぜなら，どのように (a_0, a_1) をコミットしても，0,1 以外の不正な値を入力することはできないからである．不正入力攻撃の対策が不要であることは，既存方式と比べて提案方式の利点である．

提案方式に特有の攻撃方法として，偏光板めがねを用いた攻撃がある．これは，偏光板を仕込んだめがねを装着することで，コミットされた秘密情報を得る攻撃である．偏光板めがね攻撃には，コンタクトレンズに偏光板を仕込む方法や，水晶体に偏光板を埋め込む方法などのさまざまな派生が考えられる．

偏光板めがね攻撃の対策として，プロトコルを実行する前に，不正に持ち込んだ偏光板が存在しないことを調べる方法がある．偏光板めがねの検出は，偏光板めがねを装着することで可能である．

5 おわりに

本論文では，偏光板カードという新しい要素を取り入れることで，カードを用いた暗号プロトコルの効率化ができることを示した．

本論文では 1 ビットを 2 枚で符号化する方法についてのみ取り上げたが，ある偏光板カード p を 1 枚固定することで，1 ビットを 1 枚で表現することも可能である．その場合，偏光板カード s の値は (p, s) として定義される．

1 ビットを 1 枚で符号化する方法は，従来のカードを用いた暗号プロトコルでも研究されている [4]．しかし，AND プロトコルにおいて必要となるシャッフルが，ランダム二等分割カットなどと比べて手操作での実現が難しいことが問題点である．偏光板カードにおいても全く同じ状況が生じる．上記の問題を解決することができる，新しいカードや符号化が存在するのかどうかは，未解決問題である．

謝辞

本稿に対し有益な意見をいただいた新・明るい暗号勉強会の皆様に感謝する．また，有益な情報を快く提供してくださった東北大学の水木敬明先生に深く感謝する．本研究の一部は，公益財団法人倉田記念日立科学技術財団 倉田奨励金による補助のもとで行われた．

参考文献

[1] B. den Boer, “More efficient match-making and satisability: the five card trick,” Proc. EUROCRYPT ’89, Lecture Notes in Computer Science, vol. 434, pp. 208—217, Springer-Verlag, 1990.

[2] T. Mizuki, M. Kumamoto, and H. Sone, “The five-card trick can be done with four cards,” Proc. ASIACRYPT 2012, Lecture Notes in Computer Science, Springer-Verlag, vol. 7658, pp. 598—606, 2012.

[3] T. Mizuki and H. Shizuya, “A Formalization of Card-Based Cryptographic Protocols via Abstract Machine,” International Journal of Information Security, Springer-Verlag, vol.13, no.1, pp.15-23, 2014.

[4] T. Mizuki and H. Shizuya, “Practical Card-Based Cryptography,” Fun with Algorithms 2014, Lecture Notes in Computer Science, Springer-Verlag, vol.8496, pp.313-324, 2014.

[5] T. Mizuki and H. Sone, “Six-card secure AND and four-card secure XOR,” Proc. Frontiers in Algorithmics (FAW 2009), Lecture Notes in Computer Science, vol. 5598, pp. 358—369, Springer-Verlag, 2009.

[6] 西田 拓也, 林 優一, 水木 敬明, 曽根 秀昭, 「カードを用いた安全な三入力多数決について」, Computer Security Symposium 2013.