1E-05

# 結合律を満たすXOR拡張3値入力カードプロトコルの実装可能性

# A Report about implementability of XOR extended ternary-input card protocols with associative property

須賀 祐治 *
Yuji SUGA

**あらまし** 2者のXOR演算プロトコルをベースに0でも1でもない第3の値「不定」を入力可能な拡張プロトコルを考える．結合律を満たすような代数的構造を持つ場合のみを想定し，真偽表として構成可能なパターンを分類し，カードプロトコルとしての実装可能性について報告する．

**Keywords:** Card-based cryptography, Secure multi-party computation, non-committed format, Five-Card Trick, Three-valued logic, Commutative Semi-group

## 1 はじめに

本稿はカードベースプロトコルのうち非コミット型のプロトコルを扱う．一般的なカードベース暗号では1ビット入力を2種類2枚のカードが用いられる [1]．例えば，ユーザによる1ビット入力は以下の一般的なエンコーディングルールに従う：$\boxed{\clubsuit}\boxed{\heartsuit}=0$, $\boxed{\heartsuit}\boxed{\clubsuit}=1$.

出力がコミット型であるとは，プロトコル停止時に得られる結果が，入力のエンコーディングルールに基づいた形式であることを指す．一方で非コミット型であるとは，プロトコル停止時に利用されたカードを開示するなどして結果を得る方式である．最も有名な非コミット型カードプロトコルのひとつである Five-card trick [2] はハートとクラブ2種類のスートのカードを用いる2ユーザ間での AND 演算を行うプロトコルである．2入力を $a,b\in\{0,1\}$ としたとき $\boxed{?}\boxed{?}(=\bar{a})$ $\boxed{\heartsuit}$ $\boxed{?}\boxed{?}(=b)$ として5枚のカードを並べてランダムカット（巡回置換を $c_5$ としたとき，恒等置換 $id$ と $c_5, c_5^2, c_5^3, c_5^4$ の5通りから等確率で選択してカード束に処理する操作）を行う．ここで $\boxed{?}$ は裏面にして入力したことを示しており $\bar{a}$ は $a$ の否定 (negation) である．

| $(a,b)$ | sequence |
|---|---|
| (0,0) | ♡ ♣ ♡ ♣ ♡ |
| (0,1) | ♡ ♣ ♡ ♡ ♣ |
| (1,0) | ♣ ♡ ♡ ♣ ♡ |
| (1,1) | ♣ ♡ ♡ ♡ ♣ |

表 1: Five-Card Trick 初期入力状態

Five-Card Trick は，カード入力時の一般置換（このケースでは $b$ を入力の際にカードを倒置して置いているため5枚のカード全体として $\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}$ の置換を行っていると考える）とランダムカットのみで構成されるシンプルなプロトコルである．

## 2 表面裏面ともに全く同じ絵柄であるカードを利用するメリット

本稿では表面裏面ともに全く同じ絵柄であるカード（例えば名刺や麻雀牌）を用いることを考えるこのときカードの上下配置の違いを用いて，それぞれ（一般的なカードプロトコルで用いられる）異なるスートと対応づけることができる．つまり $\boxed{\downarrow}$ を $\boxed{\clubsuit}$ と，$\boxed{\uparrow}$ を $\boxed{\heartsuit}$ と同一視することを考える．スートを表現するメモ書きをしないでも，同一カードの束を用いてプロトコルを構成することができる点も一つのメリットである．

このような状況下においてSCIS2022では2者の AND 演算プロトコルが提案されている [3]．ビルディングブロックとして2者間の拡張 AND 演算プロトコルを用い，複数のプロトコルを連続して実行することを想定すると，この拡張演算は推移律を満たす必要がある．自明な場合を取り除いた位数3の可換半群のうち AND の代数構造を持つ半群のうちの一つが次の AND-$(0,\theta,\theta)$ である．

AND-$(0,\theta,\theta)$:

| $a\backslash b$ | 0 | $\theta$ | 1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| $\theta$ | 0 | $\theta$ | $\theta$ |
| 1 | 0 | $\theta$ | 1 |

### 2.1 AND-$(0,\theta,\theta)$ の実装

実装には次のテクニックが用いられる．アイデアとしてはランダム2等分カットを勘弁に実装する方式で用いられている方式によく似通っており，上下関係をランダ

* 株式会社インターネットイニシアティブ, 〒 102-0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム, Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo, 102-0071 Japan suga@iij.ad.jp

ムに入れ替えること（この操作を上下シャッフルと呼ぶ）によりカード束を同一視する手法を導入している．実装方法としてはランダムカット後のカード束にさらにエクストラカード 1 枚を用いて 3 枚のカードのうちの 1 枚めの表面を秘匿し，放り投げる等して上下関係を入れ替えた後にエクストラカードを抜き去るという方式が考えられる（1 枚だけを抜き去る作業において 1 枚と 3 枚のカード束に容易に分離可能である）．

入力者 A,B に対して異なるエンコーディングルールを適用する（エンコーディングルールは一緒でカードを置いた後に操作することが一般的であるが，ここでは説明を簡単にするために両者のエンコーディングルールが違うというセッティングをしている）．入力者 A（入力 $a$）は $\boxed{\uparrow}\boxed{\downarrow}=0$, $\boxed{\downarrow}\boxed{\uparrow}=\theta$, $\boxed{\downarrow}\boxed{\downarrow}=1$，入力者 B（入力 $b$）は $\boxed{\downarrow}\boxed{\uparrow}=0$, $\boxed{\uparrow}\boxed{\downarrow}=\theta$, $\boxed{\downarrow}\boxed{\downarrow}=1$ をエンコーディングルールとする．このとき真ん中にエクストラカード $\boxed{\uparrow}$を置いてその左側に $a$, 右側に $b$ を入力した場合，バリエーションとして表 2 の 9 パターンが得られる．

| $(a,b)$ | sequence |
|---|---|
| (0,0) | $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$ |
| (0,1) | $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$ |
| (1,0) | $\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$ |
| (1,1) | $\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$ |
| (0,$\theta$) | $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$ |
| ($\theta$,0) | $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$ |
| (1,$\theta$) | $\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$ |
| ($\theta$,1) | $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$ |
| ($\theta$,$\theta$) | $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$ |

表 2: AND-$(0,\theta,\theta)$ 実装の初期状態

このときランダムカットと上下シャッフルと行うことにより $(a,b)=(1,1)$ のときのみ $\boxed{\uparrow}$が 1 または 4 枚のパターンが現れる．また $(a,b)=(\theta,\theta),(\theta,1),(1,\theta)$ の場合 $\boxed{\uparrow}$または $\boxed{\downarrow}$が 3 枚連続現れ，これらの 3 パターンは全て同一視される．さらにそれ以外の 5 パターンは例えば $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$等が現れ，この形式がランダムカットと上下シャッフルした状態のいずれかに一致するため同一視される．

## 3 XOR 演算への拡張

本稿では XOR 演算を部分的に内包する位数 3 の半群の分類を試みた．手計算による証明を与えることで，自明なケースを除くと以下の 2 つのパターンしか存在しないことがわかった．

### 3.1 XOR-$(\theta,\theta,\theta)$ の実装

元々の XOR 演算部分以外の 5 つの出力が全て $\theta$ であることを用いると，入力としてどちらが $\theta$ が存在した時点で結果も $\theta$ であることが導かれる．前章で実装方法を示した際と同様に 1 ユーザに 2 枚の同一カードを配布し，入力として次のようなルールを用いることとする．$\boxed{\uparrow}\boxed{\uparrow}=0$, $\boxed{\downarrow}\boxed{\downarrow}=1$ を 2 枚重ねて裏にして入力する．また $\theta$ 入力時には 1 枚を表にする，つまり柄の表示されている面を合わせ 2 枚重ねて入力する．入力順番は問わず，相手が入力されていない場合には机などの平らなエリアにカードを置き，すでに入力済の場合には，そのカード束に重ねて置く．

XOR-$(\theta,\theta,\theta)$:

| $a\backslash b$ | 0 | $\theta$ | 1 |
|---|---|---|---|
| 0 | 0 | $\theta$ | 1 |
| $\theta$ | $\theta$ | $\theta$ | $\theta$ |
| 1 | 1 | $\theta$ | 0 |

XOR-$(0,\theta,1)$:

| $a\backslash b$ | 0 | $\theta$ | 1 |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| $\theta$ | 0 | $\theta$ | 1 |
| 1 | 1 | 1 | 0 |

置かれている 4 枚のカードを慎重に手に取り，カードを見ないようにランダムカットのシャッフルを行い，またカード束を机に戻す．戻した際にすでに表が表示されている場合はプロトコルを終了して出力を $\theta$ とする．また 4 枚のカード束をそのままひっくり返し同じように表が表示されている場合はプロトコルを終了して出力を $\theta$ とする．

それ以外の場合には 1 枚ずつ机に並べていく，並べる際に 1 枚でも表が表示された場合にはプロトコルを中止して出力を $\theta$ とする．3 枚めくって（残り 1 枚はそのまま表面か裏面が見ないように維持する）全て裏面のままだった場合には全てを表にして $\boxed{\uparrow}$と $\boxed{\downarrow}$が存在する場合には 出力は 1, そうでない場合には 0 とする．

## 4 まとめ

2 者の XOR 演算プロトコルをベースに 0 でも 1 でもない第 3 の値「不定」を入力可能な拡張プロトコルを考えた．結合律を満たすような代数的構造を持つ場合のみを想定し，真偽表として構成可能なパターンを分類し，カードプロトコルとしての実装可能性について議論を行い，XOR-$(\theta,\theta,\theta)$ の実装方法について提案した．

## 参考文献


[1] T. Mizuki, H.Shizuya, Practical Card-Based Cryptography, FUN2014, pp.313-324, 2014.

[2] B. denBoer, More efficient match-making and satisability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.

[3] 須賀, 3 値入力可能な可換半群の条件を満たす非コミットメント型 AND 演算拡張カードベースプロトコルの構成, SCIS2022, 2F4-2, 2022.