

修士学位論文要約（平成29年3月）

カードベース暗号プロトコルの効率化に関する研究

西村 明紘

指導教員：曾根 秀昭， 学位論文指導教員：水木 敬明

A Study on Efficient Card-Based Cryptographic Protocols

Akihiro NISHIMURA

Supervisor: Hideaki SONE, Research Advisor: Takaaki MIZUKI

Card-based cryptographic protocols provide secure multi-party computation using a deck of physical cards. There has been considerable research on reducing the number of cards to compute a fixed function (we say more effective when a protocol requires fewer cards). This paper presents secure implementation of non-uniform shuffles to perform effective AND protocols which have been proposed by Koch et al. in 2015. We utilize physical cases that can store piles of cards for the implementation. Two sufficient conditions for the implementation with cases are shown in this paper; that means our method can implement not only non-uniform shuffles in Koch's protocol, but also various shuffles. Furthermore, this paper proposes an effective copy protocol that can multiply an input with one fewer card than the most effective previously known protocol.

1. はじめに

カードベース暗号プロトコルは、物理的なカードを用いて計算を行う方法であり、自らの入力を秘匿したまま、ある関数の計算結果のみを得る方法である、秘密計算の実現も可能である。本論文では、表面が同種類のカード（黒♠または赤♥）同士は全て互いに区別できず、全てのカードは同一の裏面？であり、互いに区別できないという性質の物理的なカードを用いる。

カードベース暗号プロトコルを扱う。そして、1ビットは黒と赤のカードを1枚ずつ用いて表現し、 $\spadesuit \heartsuit = 0$, $\heartsuit \spadesuit = 1$ であると定義する。このような条件のもとに計算を行うプロトコルが多数提案されているが、同じ計算を行う場合には、必要なカード枚数がより少ないほうが「効率的」であると捉えることとする。

Kochらによって2015年に提案されたANDプロトコル[1]は、既存の最も効率的なANDプロトコル[2]よりも効率的なものである。しかし、プロトコルの一部に不均一な確率分布のシャッフルが含まれており、実現方法が未解決とされた。

そこで本論文では、Pile-Shifting Scrambleと呼ぶカードを格納できるケースを複数個用いて行う巡回的なシャッフルを提案し、Kochらのプロトコル[1]に含まれている不均一な確率分布のシャッフルが物理的なカードで実現可能であることを示す。

また、Pile-Shifting Scrambleで実現可能なシャッフルを含む、既存手法[2]より効率的なコピープロトコルを示す。

2. 不均一な確率分布のシャッフルの実現方法

本論文では Pile-Shifting Scramble と呼ぶシャッフル手法を提案する。提案手法を説明するために、Kochらが提案した AND プロトコルに用いられている、不均一な確率分布のシャッフルの一つの、

(shuffle, {id, (1 3)(2 4)}, id $\mapsto 1/3, (1 3)(2 4) \mapsto 2/3$) を例に、実現方法を示す。なお、id は恒等置換を意味し、(1 3)(2 4)は巡回置換の積である。つまり、カード列

1	2	3	4
?	?	?	?

に対してシャッフルを行い、その結果、

1	2	3	4
?	?	?	?

が確率 1/3 で、

3	4	1	2
?	?	?	?

が確率 2/3 で得られるシャッフルである。

このシャッフル操作を実行するためには、図 1 に示すような上下の面が蓋のようになっているケース（これらは区別がつかないが、説明のため C_1, C_2, C_3 と呼ぶ）を 3 つ用い、次の手順を実行する。

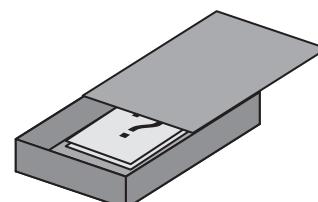


図 1: ケースの例

1. カード列 $\begin{array}{cccc} 1 & 2 & 3 & 4 \end{array}$ を $\begin{array}{cccc} 1 & 2 & 3 & 4 \end{array}$ を $\begin{array}{cccc} 1 & 2 & 3 & 4 \end{array}$ に分ける
2. $\begin{array}{cc} 1 & 2 \\ \square & \square \end{array}$ を C_1 に $\begin{array}{cc} 3 & 4 \\ \square & \square \end{array}$ を C_3 に格納し, C_2 は空にする.
3. ケースを閉じた後, C_1, C_2, C_3 を巡回的にシャッフルする.
4. シャッフルの結果得られたケースの並びからカードの並びを特定せずにカードを取り出す操作を行う.

この操作の結果, C_1, C_2, C_3 というケースの並びからは置換 id が適用されたカード列を, C_2, C_3, C_1 および C_3, C_1, C_2 というケースの並びからは, 置換(1 3)(2 4)が適用されたカード列を得られる.

以上のようにケースを用いてシャッフルを行う方法が Pile-Shifting Scramble である.

3. Pile-Shifting Scramble で実現可能なシャッフル

3.1 カード列を複数に分割して巡回させるシャッフル

いま, $d \in \mathbb{N}$ 枚のカード列を, k ($1 \leq k \leq d$) 個に分割し, そのうち i ($1 \leq i \leq k$) 番目のカードの並びの枚数が s_i ($1 \leq s_i \leq d$) 枚である場合を考える. これらを巡回させることでできる k 種類の置換をからなる集合を $\Pi^{(s_1, s_2, \dots, s_k)}$ と表す.

定理 1 s_1, s_2, \dots, s_k を自然数とし, 確率分布 F の各確率は 0 でない有理数とするとき, 任意の

(shuffle, $\Pi^{(s_1, s_2, \dots, s_k)}, F$) は Pile-Shifting Scramble で実現できる.

3.2 恒等置換またはそれ以外の置換が適用されるシャッフル

定理 2 π を互いに素な長さが等しい巡回置換の積で表せる任意の置換とし, p_1 と p_2 を任意の自然数とするとき, $(\text{shuffle}, \pi, id \mapsto \frac{p_1}{p_1+p_2}, \pi \mapsto \frac{p_2}{p_1+p_2})$ は Pile-Shifting Scramble で実現できる.

4. コピープロトコルの効率化

1 ビットを定義に従って示す裏面になった 2 枚のカードをコミットメントと呼ぶ. コピープロトコルとは, このコミットメントを複数するプロトコルである. 本節では, 入力のコミットメントを n 個に複数するのに $2n+2$ 枚のカードを要する既存の最も効率的なコピープロトコル[2]よりも効率的なコピープロトコルを提案する.

なお, $x \in \{0,1\}$ のコミットメントは

$\underbrace{\square \square}_x$ と表し, その左右のカードを $\underbrace{\square}_x^0$, $\underbrace{\square}_x^1$ と表し,

入力は $a \in \{0,1\}$ とする.

1. 入力 a と 0 のコミットメント $n-1$ 個, \spadesuit のカード 1 枚を全て裏面にして並べる:

$$\underbrace{\square \square \square \square}_{a^0} \cdots \underbrace{\square \square \square}_{0}$$

2. 2 枚目のカードを $2n+1$ 枚目に移動する:

$$\underbrace{\square \square \square}_{a^0} \cdots \underbrace{\square \square \square}_{0} \underbrace{\square}_{a^1}$$

3. 次のシャッフルを行う:

$$\left[\begin{array}{c|c|c} \square \square & \square \cdots & \square \square \square \\ \hline \underbrace{\square \square}_{a^0} & 0 & \square \end{array} \right]_{a^1}.$$

これは id または $(1 \ 2n \ 2n-1 \ \dots \ 2 \ 2n+1)$ という置換が適用されるシャッフルであり, 定理 2 より Pile-Shifting Scramble で実現可能である.

4. 1 枚目のカードをめくる.

(a) \spadesuit の場合: $\underbrace{\spadesuit \square \square \square \square}_{a^0} \cdots \underbrace{\square \square}_{a^1}$

(b) \heartsuit の場合: $\underbrace{\heartsuit \square \square}_{\bar{a}} \cdots \underbrace{\square \square \square}_{\bar{a}}$

この場合, \bar{a} のコミットメントの左右のカードを入れ替えて a のコミットメントとしたのち, そのうち一つと, コミットメントとして使われていない 3 枚 ($\heartsuit \spadesuit \clubsuit$) のカードを用いて, ステップ 1 から $n=2$ の場合として再度実行すれば良い.

5. まとめ

本論文では, カードベース暗号プロトコルの効率化のために必要であったシャッフルの実現方法を明らかにした. また, 既存手法より効率的なコピープロトコルを提案した.

文献

- [1] A. Koch, S. Walzer, and K. Härtel, "Card-based cryptographic protocols using a minimal number of cards," Advances in Cryptology – ASIACRYPT 2015, eds. by T. Iwata and J. Cheon, vol.9452, pp.783–807, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2015.
- [2] T. Mizuki and H. Sone, "Six-card secure AND and four-card secure XOR," Frontiers in Algorithmics, vol.5598, pp.358–369, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009.