

連動操作を用いない上下カード3枚 有限時間 AND プロトコルの不可能性証明

産学連携と数理・暗号分野連携による
カードベース暗号の深化と新境地III

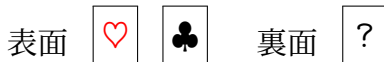
佐賀大学

岩崎淳

本発表は [Iwasaki25]A. Iwasaki, "Minimum Number of up-down Cards for Finite-Time Committed-AND Protocol Without Interlocking Operations," IWSEC2025. の再構成です

カードデッキ

- den Boer が世界初のプロトコルを発表して以来、二色カードデッキがカードベース暗号で最も広く研究されてきた



- ▶ 1bit のコミットメントは2枚のカードで作成： $\clubsuit\heartsuit = 0$, $\heartsuit\clubsuit = 1$
- ▶ AND プロトコルなどの基本的な計算に対して、種々の条件ごとの必要カード枚数の最小値が解明されている
- 他方で、さまざまなカードデッキも使用されてきた
 - ▶ トランプ、上下カード、正多角形カード、偏光板カード、不可視インクカード、トライアングルカード、UNO、等
 - ▶ プロトコルの提案が主で、非自明な計算限界の報告は少ない

上下カード [MS14]



表面

180° 回転に対して
非対称



裏面

180° 回転に対して
対称

● カードの置き方：

- ▶ 表を上に向けて、矢印上向き
- ▶ 表を上に向けて、矢印下向き
- ▶ 裏を上に向けて、矢印上向き
- ▶ 裏を上に向けて、矢印下向き

● コミットメント：

- ▶ 符号化規則：0=↓（矢印下向き），1=↑（矢印上向き）
- ▶ 1枚で1-bitの符号化
⇒ 二色デッキに比べてプロトコル全体のカード枚数を削減できる

[MS14] T. Mizuki and H. Shizuya, "Practical card-based cryptography," FUN2014.

上下カードデッキに対する操作

二色カードデッキと共通の操作:

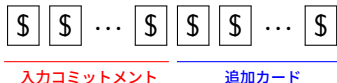
- 決定論的なカードの並び替え
- シャッフル（ランダムなカードの並び替え）
- 裏返し（表裏の反転）

上下カードデッキ特有の操作:

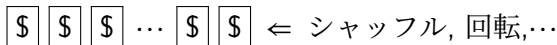
- カードの回転: $\boxed{A} \rightarrow \boxed{\forall}$
- カードのランダム回転: $\boxed{A} \rightarrow \boxed{A} \text{ or } \boxed{\forall}$
- カード束の回転・ランダム回転
 - ▶ 回転: $\boxed{A} \boxed{B} \boxed{C} \rightarrow \boxed{\forall} \boxed{B} \boxed{C}$
 - ▶ ランダム回転: $\boxed{A} \boxed{B} \boxed{C} \rightarrow \boxed{A} \boxed{B} \boxed{C} \text{ or } \boxed{\forall} \boxed{B} \boxed{C}$

上下カードを用いたプロトコル

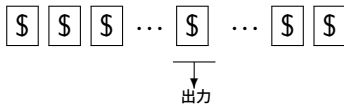
1 入力コミットメントと追加カードを並べる



2 並べたカード列に操作を加える



3 出力. (コミット型の場合, 計算結果のコミットメントを出力)



- ステップ数が有界 → “有限時間”
- 安全性 (秘匿性・正当性)
 - 入力情報が一切漏洩せず, 確率 1 で正しい計算結果を出力

連動操作を用いる既存プロトコル [MS14][SNNHO16]

上下カード 3 枚を用いる有限時間コミット型 AND プロトコルが既知



理論的下限

- 上下カード 1 枚を二色カード 2 枚（赤黒各 1 枚）で置き換え
⇒ 二色カードデッキ上のプロトコルに変換可能
- 有限時間コミット型 AND プロトコルに二色カードは 5 枚以上必要 [KWH15]

既存プロトコルは連動操作を用いる



（カードの位置の）シャッフルとランダム回転を連動させる

- MS シャッフル：

A	B	C
---	---	---

 →

A	B	C
---	---	---

 or

∇	C	B
---	---	---
- トルネードシャッフル：

A	B	C
---	---	---

 →

A	B	C
---	---	---

 or

C	B	∇
---	---	---

[SNNHO16]K. Shinagawa, et al, “Committed and protocol using three cards with more handy shuffle,” ISITA2016.

[KWH15]A. Koch, et al., “Card-based cryptographic protocols using a minimal number of cards,” ASIACRYPT2015.

本発表の概要

- 既存の有限時間コミット型 AND プロトコルは連動操作を用いてカード枚数の下限である 3 枚を達成
- 単体のシャッフルやランダム回転に比べ、連動操作の実装は難しい



最小枚数の達成に連動操作は不可欠か？

本発表においては

連動操作を禁止した場合、有限時間コミット型 AND プロトコルを上下カード 3 枚では実現できないことを証明し、連動操作がカード枚数の削減に貢献していることを示す

主結果

Theorem

連動操作を禁止した場合，有限時間コミット型 *AND* プロトコルを上下カード 3 枚では実現できない

以下証明の概略を見ていく

- 厳密な計算モデルは [Iwasaki25] を参照
- 考える操作：並び替え，シャッフル，回転，ランダム回転，裏返し
- 「3 枚のプロトコルを仮定して，それが有限時間でない」ことを示す
- 証明のフローは [KWH15] とほぼ同様.
- [KWH15] の用語を多少定義を変えて用いる

証明の仮定

一般性を失うことなく以下の仮定を置く：

- カードはすべて裏向きで置かれている
- 一回の「裏返し」操作は1枚のカードのみを裏返す
- 「裏返し」により表を向けたカードは矢印の向きを確認した後、すぐに再び裏返して裏向きにする
- すべてのシャッフル操作の台（そのシャッフルが正の確率で実行しうる置換の集合）はid（恒等置換）を含む
- すべてのランダム回転において、回転する確率・回転しない確率はどちらも正である

簡約ステート

プロトコルの実行中の任意の時点を固定する.

S : その時点でのカード列を表す確率変数

(a, b) : プロトコルの入力

カード列 s を分類する:

- $\Pr[S = s \mid a \wedge b = 0] > 0$ かつ $\Pr[S = s \mid a \wedge b = 1] = 0$ のとき **0-sequence**
- $\Pr[S = s \mid a \wedge b = 0] = 0$ かつ $\Pr[S = s \mid a \wedge b = 1] > 0$ のとき **1-sequence**
- $\Pr[S = s \mid a \wedge b = 0] > 0$ かつ $\Pr[S = s \mid a \wedge b = 1] > 0$ のとき **$\perp$ -sequence**
- それ以外のとき, **null-sequence**

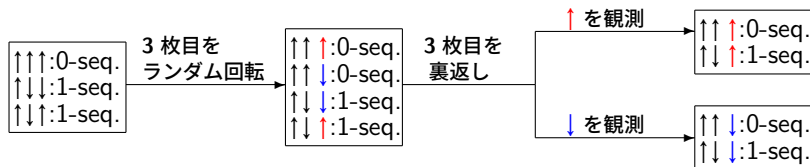
定義

分類をラベル付けした null-sequence 以外のカード列の集合を
その時点での**簡約ステート**という

簡約ステートの遷移・簡約 KWH ツリー

プロトコル中の各操作は簡約ステート間の遷移に対応付けられる

- 「カードの裏返し」 ⇒ 遷移先の簡約ステートは2つ
- それ以外以外の操作 ⇒ 遷移先の簡約ステートは1つ



定義

プロトコルの実行中に発生しうる全ての遷移を表す
遷移図を簡約 KWH ツリーという

有効簡約ステート

定義

- 0 -sequence と 1 -sequence をそれぞれ一つ以上以上含み、かつ、
- $\perp$ -sequences を含まない

とき、簡約ステートは有効であるという

- $\perp$ -sequence を含む $\Rightarrow$ 正しい計算結果が得られない確率 > 0
- 0 -seq. か 1 -seq. のどちらかしか含まない ($\perp$ -seq. も含まない)
 $\Rightarrow$ 入力情報が漏洩

命題

プロトコルが安全性を満たすならば、そのプロトコルの簡約 KWH ツリーは有効な簡約ステートのみを含む (**※安全性の必要条件**)

出力簡約ステート

定義

有効な簡約ステートに含まれるカード列に対して、

- 全ての 0 -sequence の i 枚目のカードは $\downarrow$ (矢印下向き)
- 全ての 1 -sequence の i 枚目のカードは $\uparrow$ (矢印上向き)

となる i が存在するとき、その簡約ステートを**出力簡約ステート**と呼ぶ。

出力簡約ステートに達すれば、 i 枚目のカードが計算結果を正しくエンコードするコミットメントになっている

命題

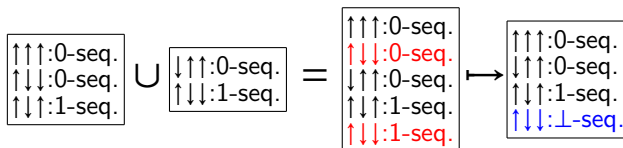
プロトコルが正当性を満たすならば、その簡約 KWH ツリーの全ての葉は出力簡約ステートである。

簡約ステートの和集合

簡約ステート同士の和集合を定義できる。
ただし、ルールを追加する：

和集合にラベルが異なる同一のカード列が含まれるならば、それらのラベルを $\perp$ -sequence に書き換える

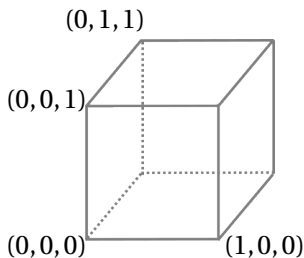
⇒ 和集合も簡約ステートになる



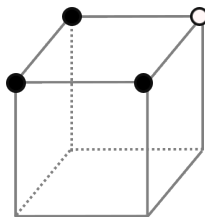
有効簡約ステートのダイアグラム表示

証明を見やすくするため単位立方体を用いた有効簡約ステートのダイアグラム表示を導入する

- $\downarrow=0$, $\uparrow=1$ としてカード列と単位立方体の頂点を対応させる
- 0-sequence に対応する頂点を黒丸, 1-sequence に対応する頂点を白丸で表す



(a) 単位立方体



(b) 初期簡約ステート

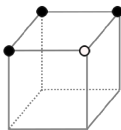
簡約ステートの分類

9 タイプの有効簡約ステートを定義する

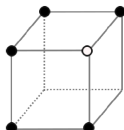
ダイアグラムの回転により
右図の Type- r に重なる有効
簡約ステートを type- r に分類

T : type-1~9 の簡約ステート
全体の集合

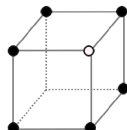
初期簡約ステートは type-1
 $\Rightarrow$ 初期簡約ステート $\in T$



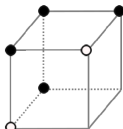
(a) Type-1



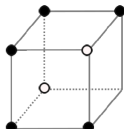
(b) Type-2



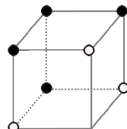
(c) Type-3



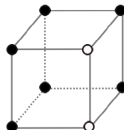
(d) Type-4



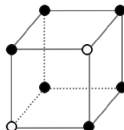
(e) Type-5



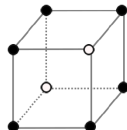
(f) Type-6



(g) Type-7



(h) Type-8



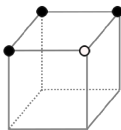
(i) Type-9

出力簡約ステート

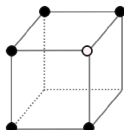
有効簡約ステートが出力簡約ステート



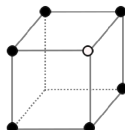
xy, yz, xz 平面のいずれかと
平行な平面でダイアグラムを
切り分けて黒丸と白丸を分離
できる



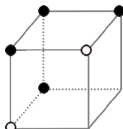
(a) Type-1



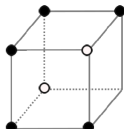
(b) Type-2



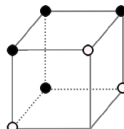
(c) Type-3



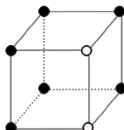
(d) Type-4



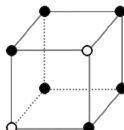
(e) Type-5



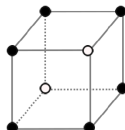
(f) Type-6



(g) Type-7



(h) Type-8



(i) Type-9

type-1~9 は分離不能

⇒ 出力簡約ステート $\notin T$

証明方針

P を安全性を満たす上下カード 3 枚のコミット型 AND プロトコルとする

- P の簡約 KWH ツリーは有効簡約ステートのみで構成される
- P の簡約 KWH ツリーの葉は出力簡約ステートである
- 初期簡約ステート $\in T$ かつ 出力簡約ステート $\notin T$



P の簡約 KWH ツリーの根から葉に至る任意の経路上に,

T に含まれる簡約ステートから T に含まれない簡約ステートへの遷移

が存在

どのような操作がその遷移を引き起こすかを見ていく

簡約ステートの和集合

先に和集合について見ておく

R : type-2~type-9 の簡約ステート

全体の集合 ($R \subset T$)

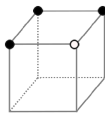
W : $\perp$ -sequence を含む

簡約ステート全体の集合

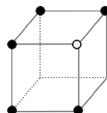
$$\forall \mu_1 \in T, \forall \mu_2 \in W, \mu_1 \cup \mu_2 \in W$$

$$\forall \mu_1 \in T, \forall \mu_2 \in R, \mu_1 \cup \mu_2 \in R \cup W$$

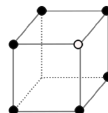
type-1 $\cup$ type-1 を除いて和集合が
 T の外の有効簡約ステートになる
ことはない



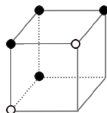
(a) Type-1



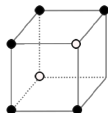
(b) Type-2



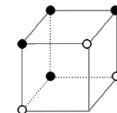
(c) Type-3



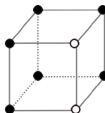
(d) Type-4



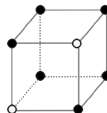
(e) Type-5



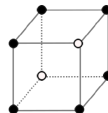
(f) Type-6



(g) Type-7



(h) Type-8



(i) Type-9

決定論的な操作

決定論的な操作はすべて「2枚のカードの位置を交換」と「1枚のカードの回転」に帰着できる

ダイアグラムへの作用

- 「2枚のカードの位置を交換」
⇒ 平面 $x = y$, $y = x$, $x = z$ で面对称となる位置に点を移す
- 「1枚のカードの回転」
⇒ 平面 $x = \frac{1}{2}$, $y = \frac{1}{2}$, $z = \frac{1}{2}$ で面对称となる位置に点を移す

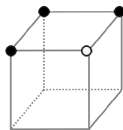
決定論的な操作

平面 $x = y$, $y = x$, $x = z$,
 $x = \frac{1}{2}$, $y = \frac{1}{2}$, $z = \frac{1}{2}$

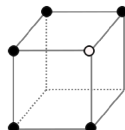
のいずれかで面対象



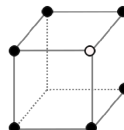
type- r は type- r に移される



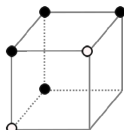
(a) Type-1



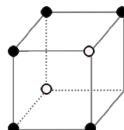
(b) Type-2



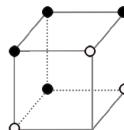
(c) Type-3



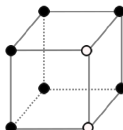
(d) Type-4



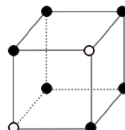
(e) Type-5



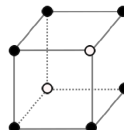
(f) Type-6



(g) Type-7



(h) Type-8



(i) Type-9

決定論的な並び替え・回転では
 T の中から外への遷移は起きない

シャッフル

- μ : type-1 の有効簡約ステート, σ : カードの置換
 $\Rightarrow \mu \cup \sigma(\mu)$ は, μ そのもの or type-2 or type-4 or $\perp$ -seq. を含む
- 任意の $\mu \in T$ は, type-1 の簡約ステート $\mu_1, \mu_2, \dots, \mu_m$ が存在して,
 $\mu = \cup_{i=1}^m \mu_i$ の形に書ける

台が $\{\text{id}, \sigma_1, \dots, \sigma_p\}$ のシャッフル shuffle, $\mu = \cup_{i=1}^m \mu_i \in T$ (各 μ_i は type-1) に対して

$$\text{shuffle}(\mu) = \cup_{j=1}^p \cup_{i=1}^m (\mu_i \cup \sigma_j(\mu_i))$$

- $\forall i, \forall j, \mu_i \cup \sigma_j(\mu_i) = \mu_i \Rightarrow \underline{\text{shuffle}(\mu) = \mu \in T}$
- $\exists (i, j), \mu_i \cup \sigma_j(\mu_i) \neq \mu_i \Rightarrow \underline{\text{shuffle}(\mu) \in T \text{ or } \text{shuffle}(\mu) \text{ は } \perp\text{-seq. を含む}}$

シャッフルでは T の中から外の有効簡約ステートへの遷移は起きない

ランダム回転

- μ : type-1 の有効簡約ステート, $RROT$: ランダム回転
 $\Rightarrow RROT(\mu)$ は, type-7 or type-8 or type-9 or $\perp$ -seq. を含む

ランダム回転 $RROT$, $\mu = \cup_{i=1}^m \mu_i \in T$ (各 μ_i は type-1) に対して

$$RROT(\mu) = \cup_{i=1}^m RROT(\mu_i)$$

よって, $RROT(\mu) \in T$ or $RROT(\mu)$ は $\perp$ -seq. を含む

ランダム回転では T の中から外の有効簡約ステートへの遷移は起きない

裏返し

「カードをめくって、そのカードの矢印の向きを見る」操作.

- ダイアグラムへの作用：

- ▶ 平面 $x = \frac{1}{2}$, $y = \frac{1}{2}$, $z = \frac{1}{2}$ のどれかでダイアグラムを2つに分割
- ▶ 観測した矢印の向きによって、分割後の2つのダイアグラムのうち、どちらかのダイアグラム（が表す簡約ステート）に遷移

- 安全性を満たすプロトコルの簡約 KWH ツリーには有効な簡約ステートしか含まれない

⇒ 分割後の2つのダイアグラムがどちらも有効な簡約ステートを表す「裏返し」のみを考えれば十分.

裏返し

type-4~9 のみ裏返し可能

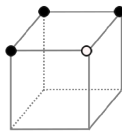
裏返しにより T の中から外の有効簡約状態への遷移が生じる

可能な全ての裏返しで
分割後のダイアグラムの
少なくとも一方は type-1

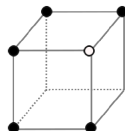
裏返しによる簡約状態の
遷移先は2つあるが、少なく
とも一方は T に含まれる

どちらに遷移するかは観測したカードの向き次第

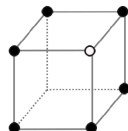
⇒ T の中から外への遷移が生じない確率は常に正



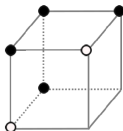
(a) Type-1



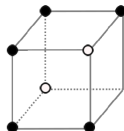
(b) Type-2



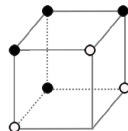
(c) Type-3



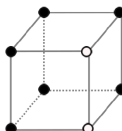
(d) Type-4



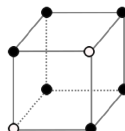
(e) Type-5



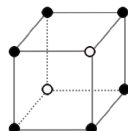
(f) Type-6



(g) Type-7



(h) Type-8



(i) Type-9

結論

連動操作を用いない上下カード3枚コミット型 AND プロトコル P は安全性を満たすとする

- 初期簡約状態 $\in T$ かつ 出力簡約状態 $\notin T$
- 有効簡約状態 $\in T$ から有効簡約状態 $\notin T$ への遷移は「カードの裏返し」によってのみ生じうる
- 「カードの裏返し」による有効簡約状態 $\in T$ の遷移先の少なくとも一方は T に含まれる



- P の簡約 KWH ツリーの根から葉に至る経路長は有界でない
- P は有限時間プロトコルでない
- 連動操作を用いない上下カード3枚有限時間 AND プロトコルは存在しない

まとめ

- 連動操作を用いない上下カード 3 枚の有限時間コミット型 AND プロトコルは存在しないことを証明
- 連動操作を用いた場合は 3 枚のプロトコルが存在する
⇒ 連動操作はカード枚数削減に不可欠
- 本発表では触れなかったが，上下カード 4 枚で連動操作なしの有限時間コミット型 AND プロトコルを構成可能
⇒ 最小枚数は 4 枚

今後の課題

連動操作を用いない場合，「有限時間でない」AND プロトコルを 3 枚で構成できるか？