

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

任意の関数に対する single-shuffle full-open カードベースプロトコル

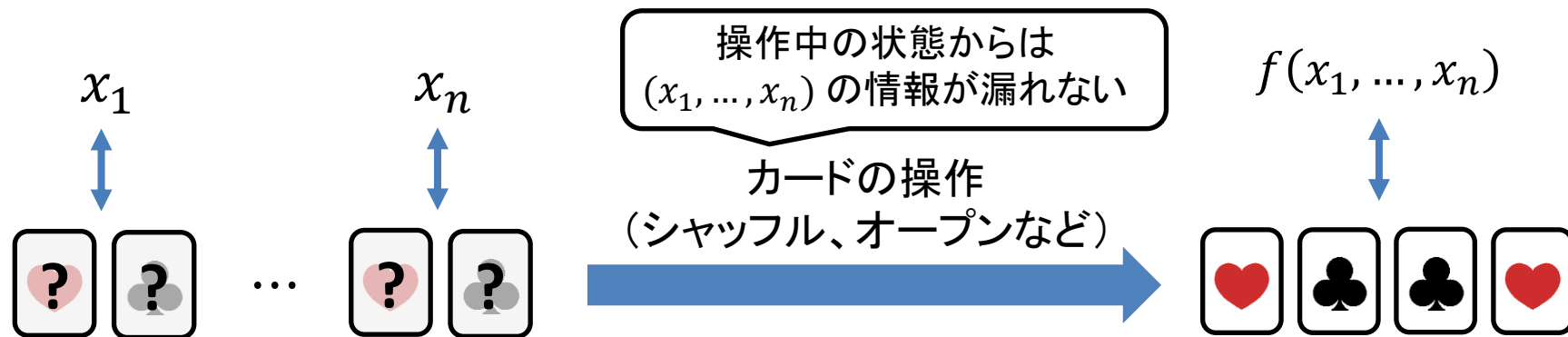
2026年7月9日

江利口 礼央
(産業技術総合研究所)

本研究は 品川和雅(筑波大)との共同研究

秘密計算

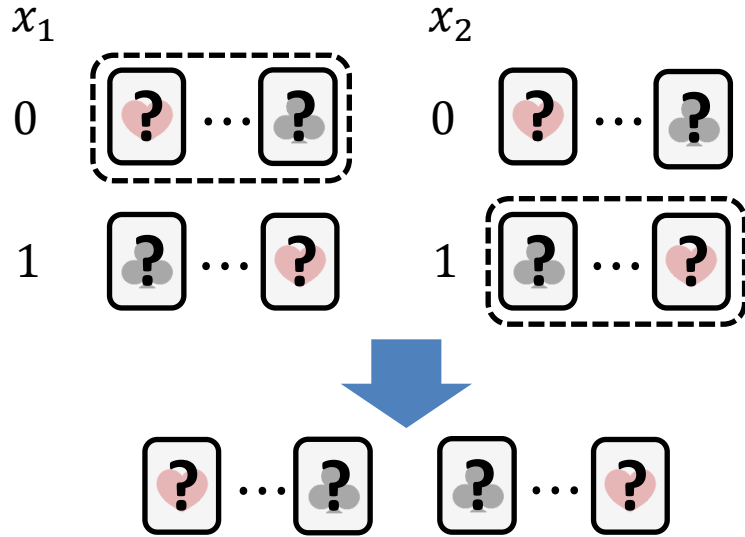
- カードベース暗号において最もポピュラーな暗号技術の一つ



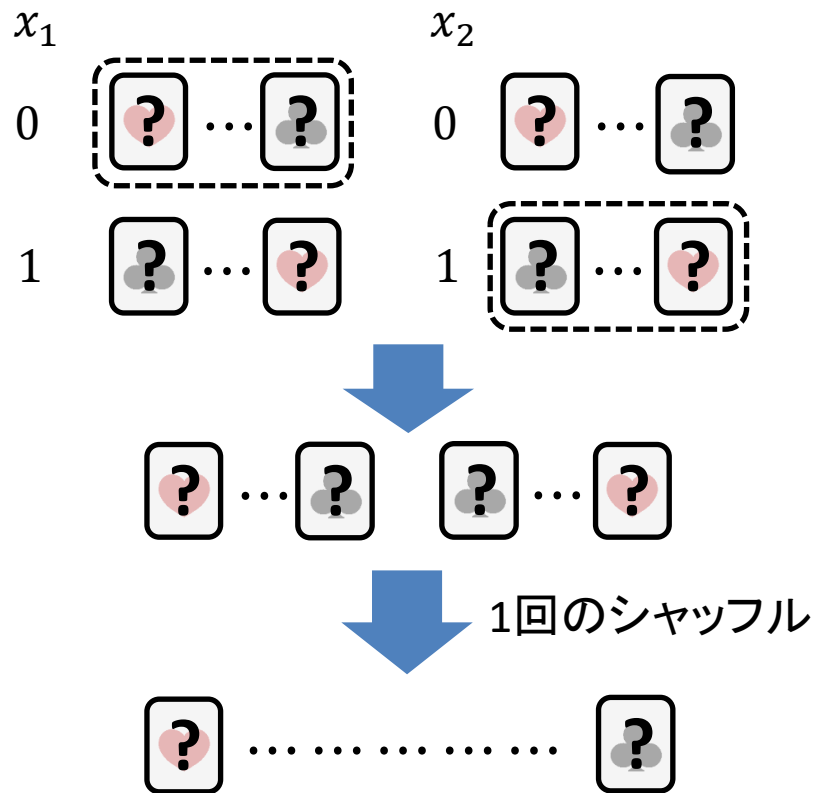
- 安全性の根拠
 - シャッフルにおいて、どの置換が適用されたのか誰にも分からない
 - オープンにおいて、めくられないカードの絵柄は誰にも分からない

シャッフルとオープンの操作をどこまで単純化できるか

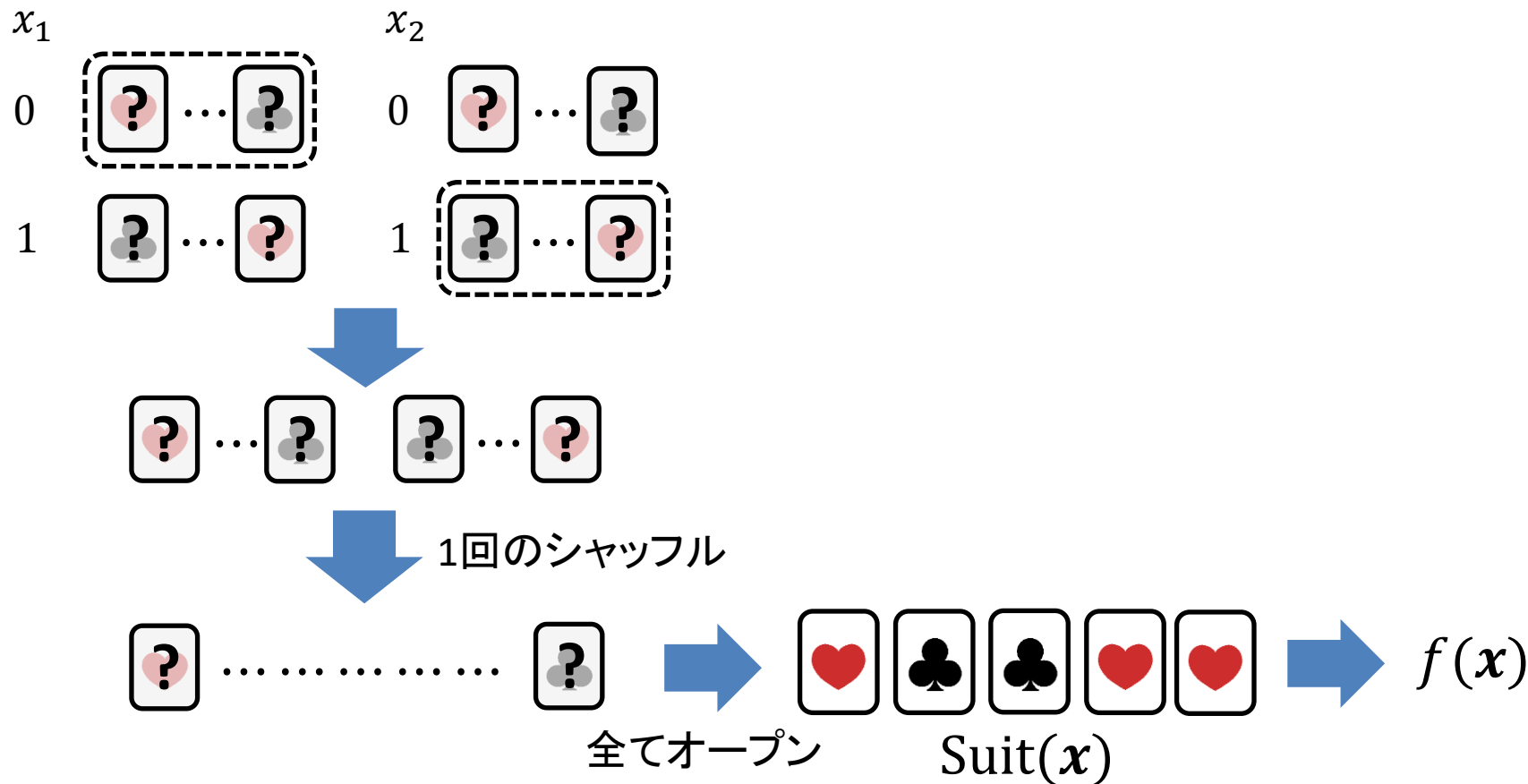
Single-Shuffle Full-Open (SSFO) Protocol



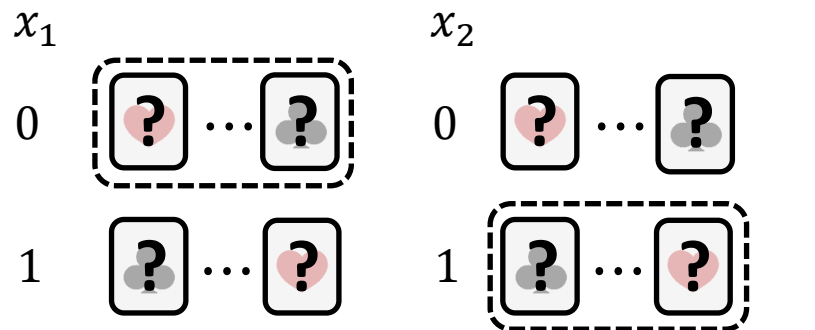
Single-Shuffle Full-Open (SSFO) Protocol



Single-Shuffle Full-Open (SSFO) Protocol

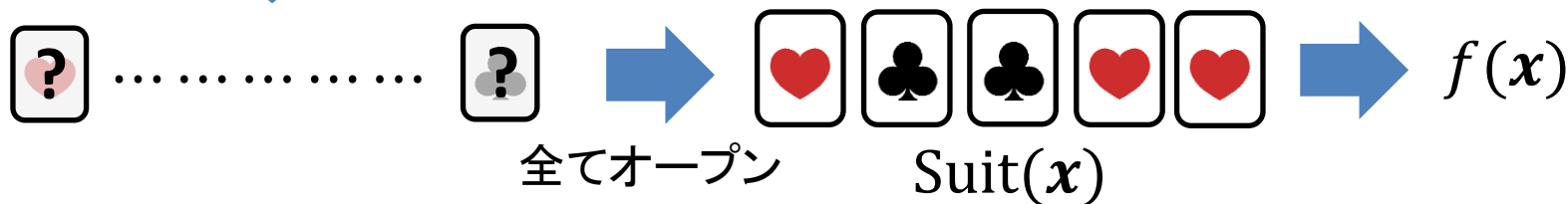
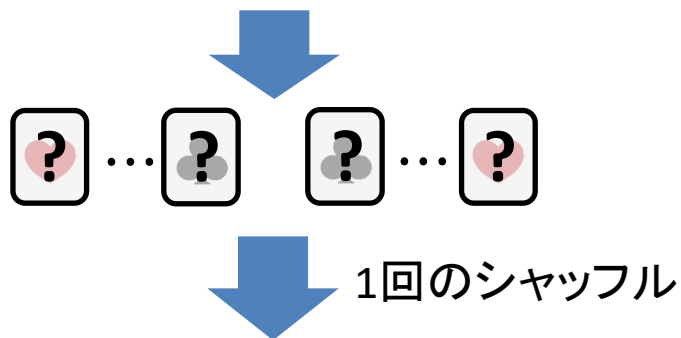


Single-Shuffle Full-Open (SSFO) Protocol

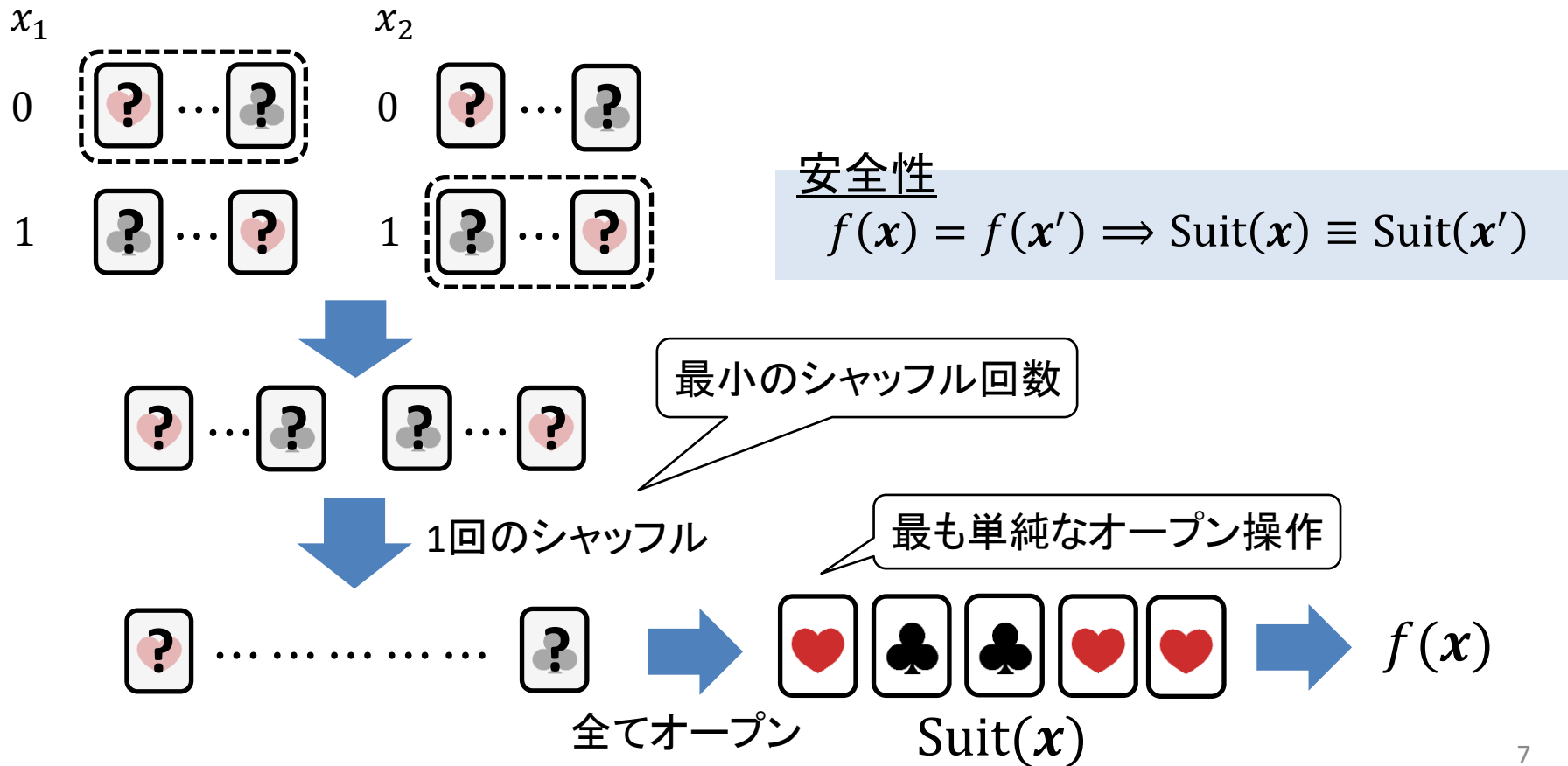


安全性

$$f(x) = f(x') \Rightarrow \text{Suit}(x) \equiv \text{Suit}(x')$$



Single-Shuffle Full-Open (SSFO) Protocol



既存研究

方式	関数	シャッフル	カード枚数
[Boe89]	2入力AND	$RC \times 1$	5
[SM18]	2入力XOR	$RC \times 1$	4
[SN25]	3入力XOR	$RC \times 1$	8
[KTMM22]	n 入力XOR	$PSh \times (n - 1)$	$2n$
		$PSc \times 2$	$O(n \log n)$
[TMM21]	3入力majority	$RC \times 1$ & $PSh \times 1$	6
[HST14, SM18]	3入力equality	$RC \times 1$	6

CS: complete shuffle

RC: random cut

PSc: pile-scramble shuffle

PSh: pile-shifting shuffle

未解決問題

任意の f に対して SSFO は存在するか

※ 置換の合成も一回のシャッフルとみなす

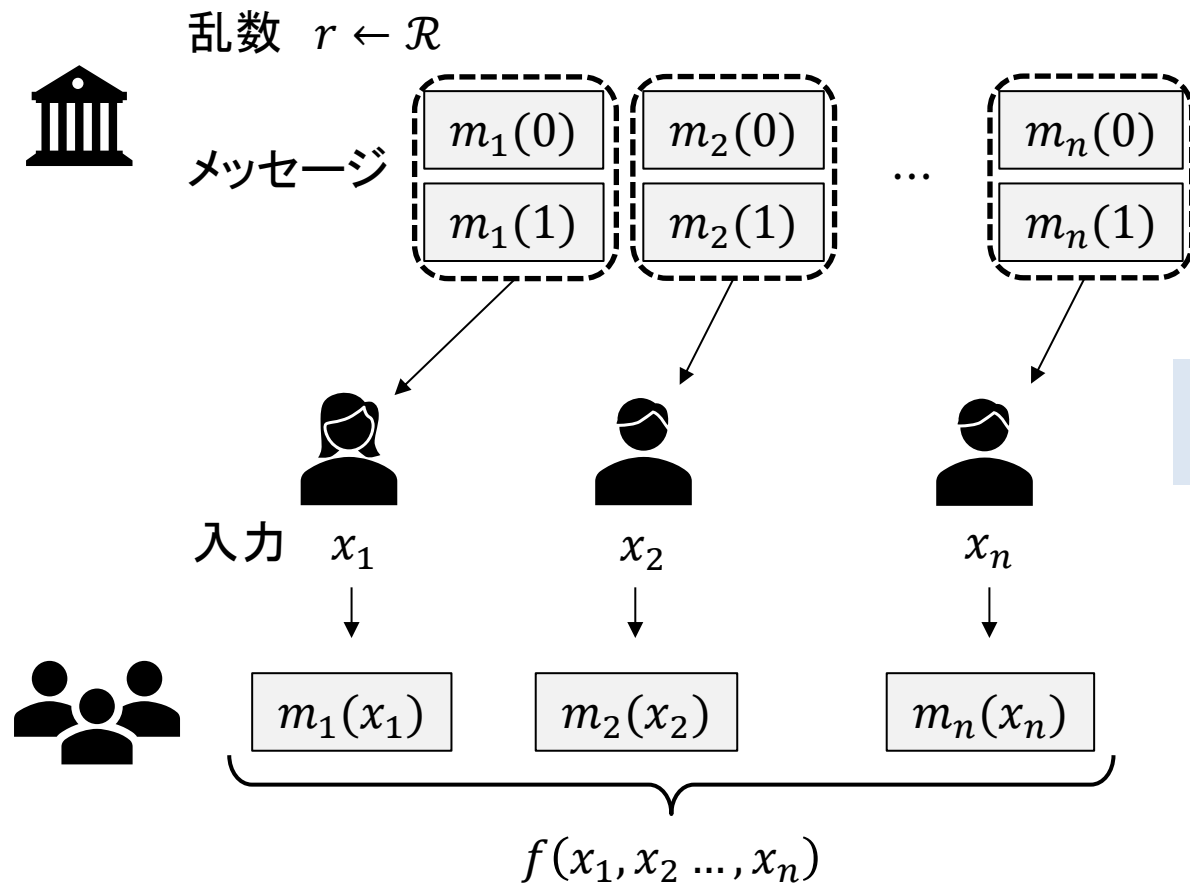
本研究の成果

方式	関数	シャッフル	カード枚数
[Boe89]	2入力AND	$RC \times 1$	5
[SM18]	2入力XOR	$RC \times 1$	4
[SN25]	3入力XOR	$RC \times 1$	8
[KTMM22]	n 入力XOR	$PSh \times (n - 1)$	$2n$
		$PSc \times 2$	$O(n \log n)$
[TMM21]	3入力majority	$RC \times 1$ & $PSh \times 1$	6
[HST14, SM18]	3入力equality	$RC \times 1$	6
本研究	Any function $f : \{0,1\}^n \rightarrow \{0,1\}$	$PSh \times 1$ & $CS \times 1$	$2^{O(n^3 2^{n/2})}$
		$PSh \times O(n 2^n)$ & $PSc \times 1$	$O(n^2 2^n)$

本研究の成果

方式	関数	シャッフル	カード枚数
[Boe89]	2入力AND	$RC \times 1$	5
[SM18]	2入力XOR	$RC \times 1$	4
[SN25]	3入力XOR	$RC \times 1$	8
[KTMM22]	n 入力XOR	$PSh \times (n - 1)$	$2n$
		$PSc \times 2$	$O(n \log n)$
[TMM21]	3入力majority	$RC \times 1$ & $PSh \times 1$	6
[HST14, SM18]	3入力equality	$RC \times 1$	6
本研究	Any function $f : \{0,1\}^n \rightarrow \{0,1\}$	$PSh \times 1$ & $CS \times 1$	$2^{O(n^3 2^{n/2})}$
		$PSh \times O(n 2^n)$ & $PSc \times 1$	$O(n^2 2^n)$

Private Simultaneous Messages (PSM) [FKN94]



本研究の貢献

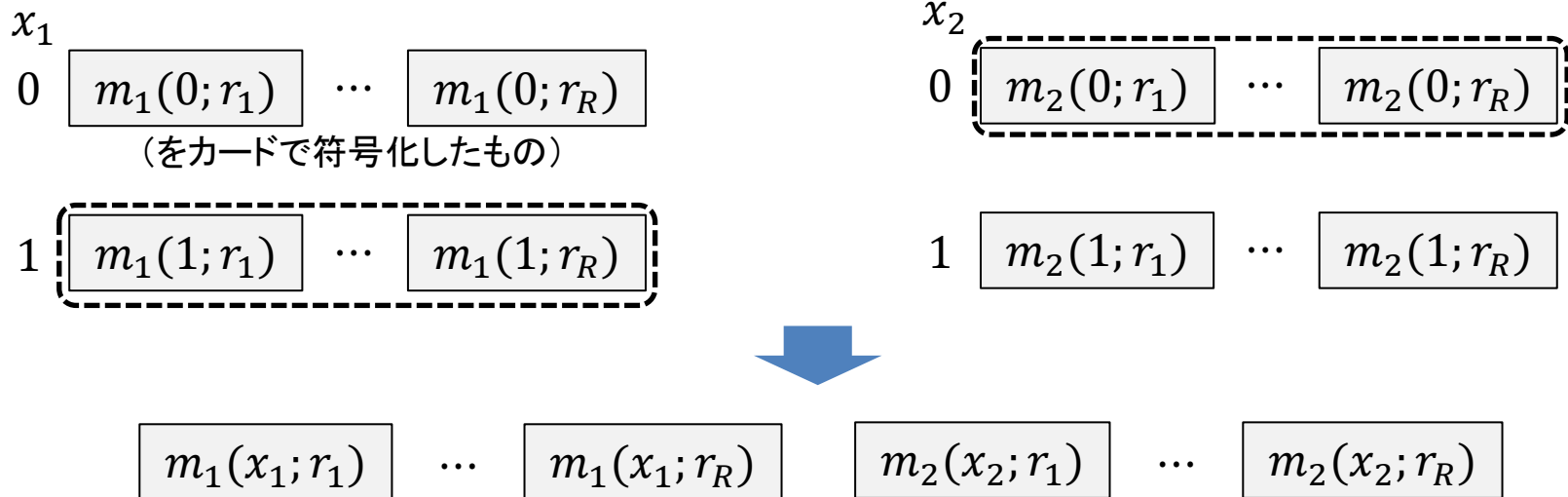
PSM から SSFO への変換

任意の f に対して PSM が存在する
[FKN94, IK97, BKN18]

SSFO Protocol Based on PSM

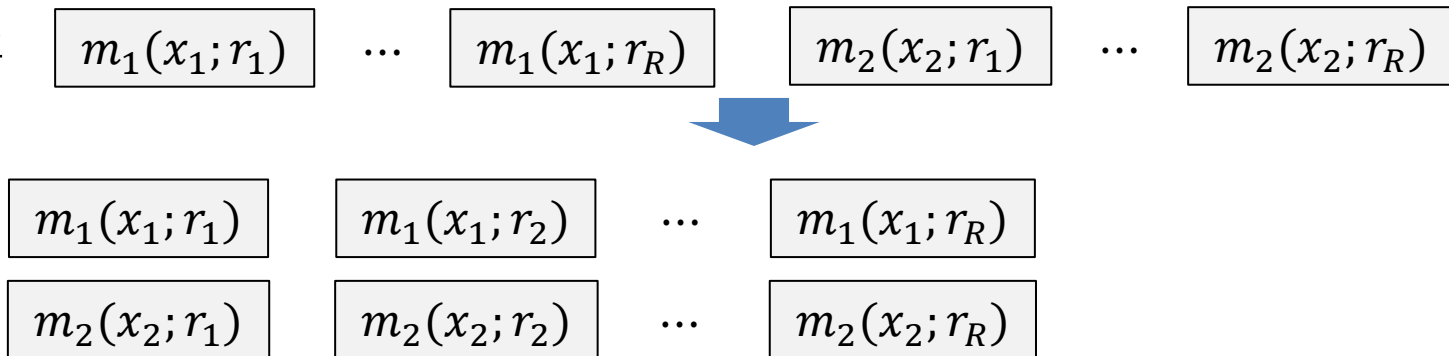
- 符号化 $0 \rightarrow \spadesuit \heartsuit$ $1 \rightarrow \heartsuit \spadesuit$ 例. 010 $\rightarrow \spadesuit \heartsuit \heartsuit \spadesuit \spadesuit \heartsuit$
- PSMの乱数集合 $\mathcal{R} = \{r_1, \dots, r_R\}$

入力フェーズ 各パーティは自分の入力に基づきカード列を選ぶ



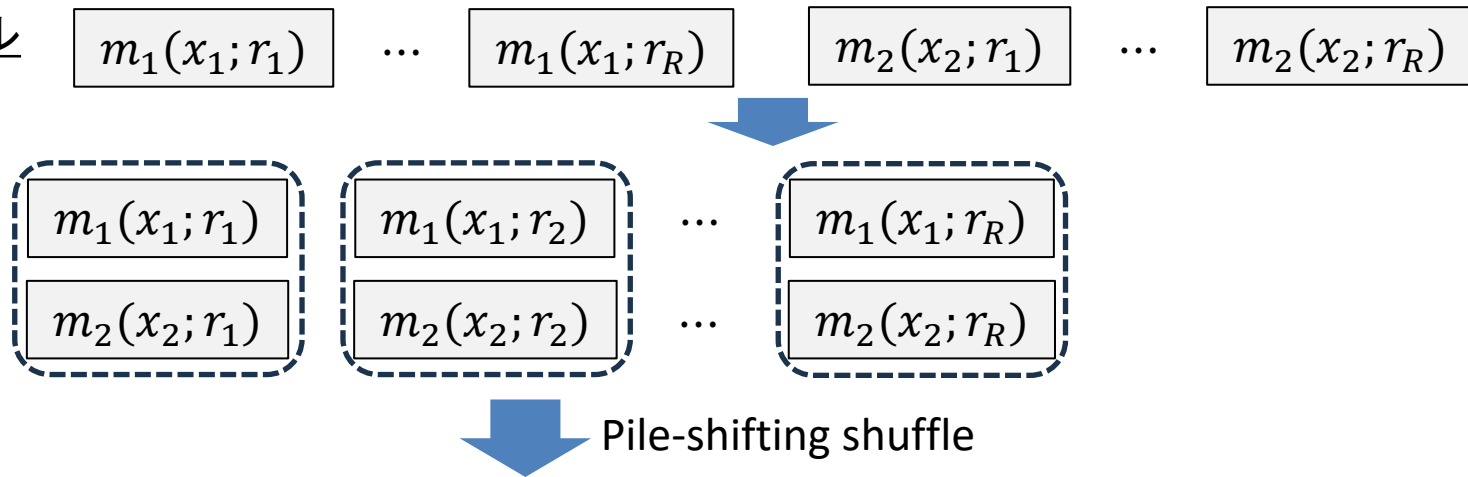
SSFO Protocol Based on PSM

シャッフル



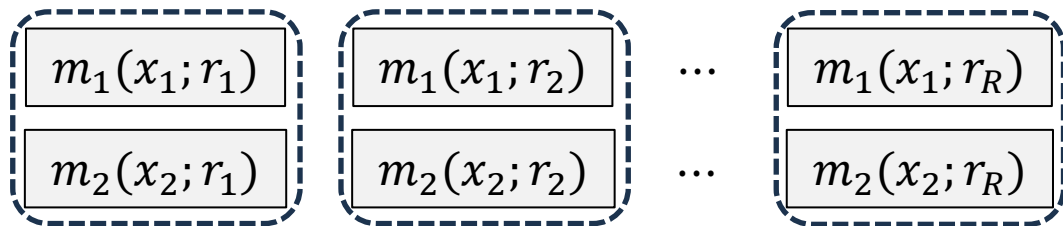
SSFO Protocol Based on PSM

シャッフル



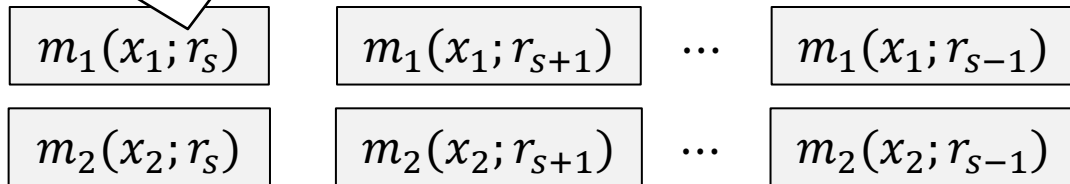
SSFO Protocol Based on PSM

シャッフル



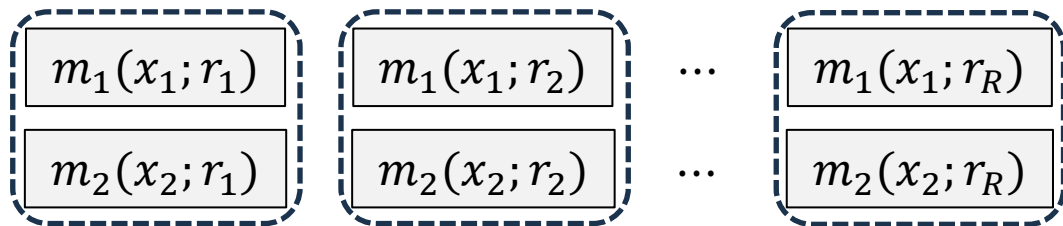
s は $\{1, \dots, R\}$ 上の一様乱数

Pile-shifting shuffle



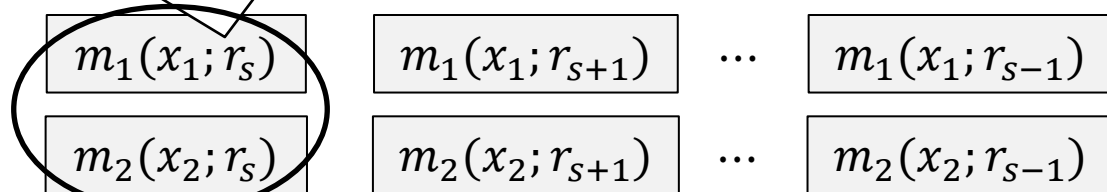
SSFO Protocol Based on PSM

シャッフル



s は $\{1, \dots, R\}$ 上の一様乱数

Pile-shifting shuffle

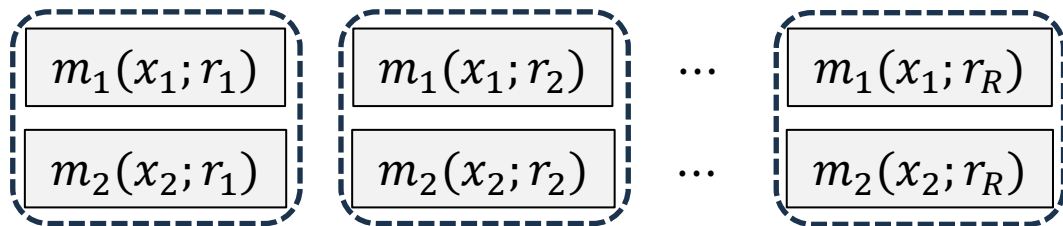


オープン

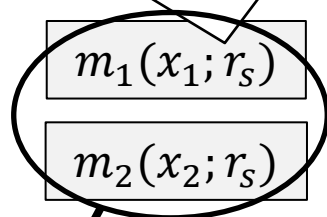
PSMで公開されるメッセージと同一
→ $f(x)$ のみを得られる

SSFO Protocol Based on PSM

シャッフル



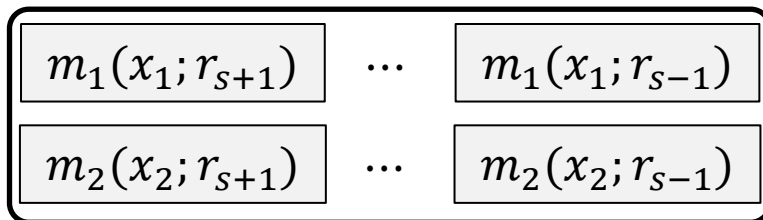
s は $\{1, \dots, R\}$ 上の一様乱数



オープン

PSMで公開されるメッセージと同一
→ $f(x)$ のみを得られる

Pile-shifting shuffle

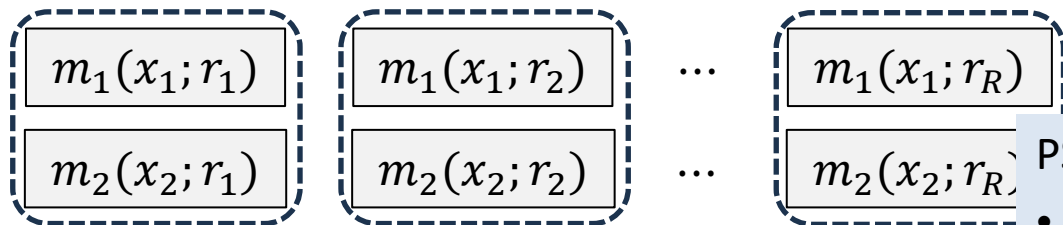


Complete shuffle

一様ランダムなカード列

SSFO Protocol Based on PSM

シャッフル

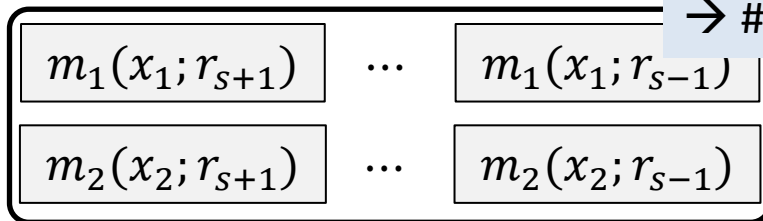
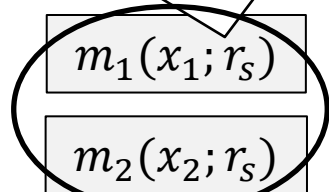


PSM for f [BKN18]

- $R = 2^{O(n^3 2^{n/2})}$
 - $c = |m_i(x; r)| = O(n^3 2^{n/2})$
- #cards = $O(cR) = 2^{O(n^3 2^{n/2})}$

s は $\{1, \dots, R\}$ 上の一様乱数

Pile-shifting shuffle



オープン

PSMで公開されるメッセージと同一
→ $f(x)$ のみを得られる

Complete shuffle

一様ランダムなカード列

Single-Shuffle *Static-Open* Protocol

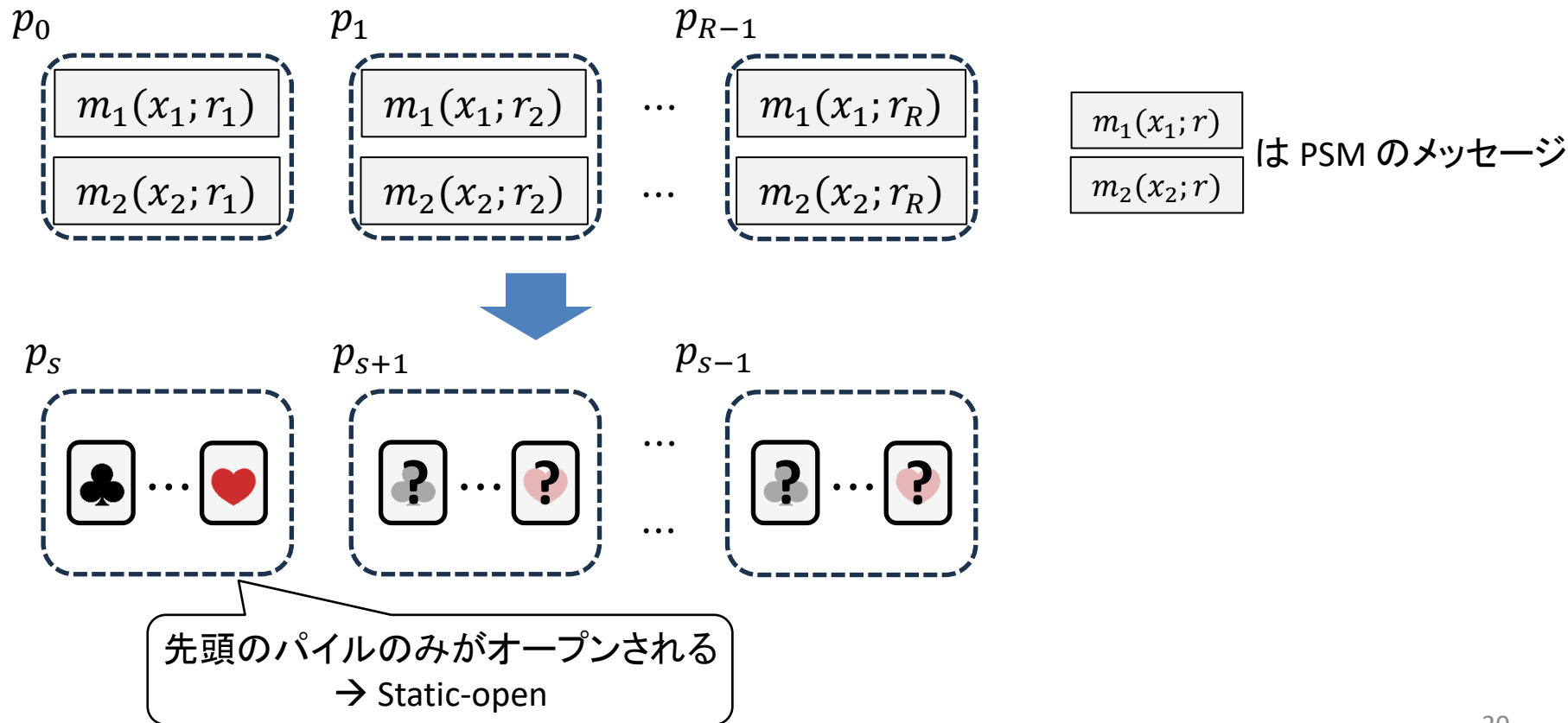
- カード組の一部のみをオープンする場合、ランダムカット1回で十分。

方式	関数	シャッフル	オープン	カード枚数
[SN21, TMM23, OSNW124]	Any function	$\text{PSc} \times O(C_f + n)$	Adaptive	$O(C_f + n)$
本研究		$\text{PSh} \times 1 \ \& \ \text{CS} \times 1$	Full	$2^{O(n^3 2^{n/2})}$
		$\text{PSh} \times O(n2^n) \ \& \ \text{PSc} \times 1$	Full	$O(n^2 2^n)$
		$\text{RC} \times 1$	Static	$2^{O(n^3 2^{n/2})}$

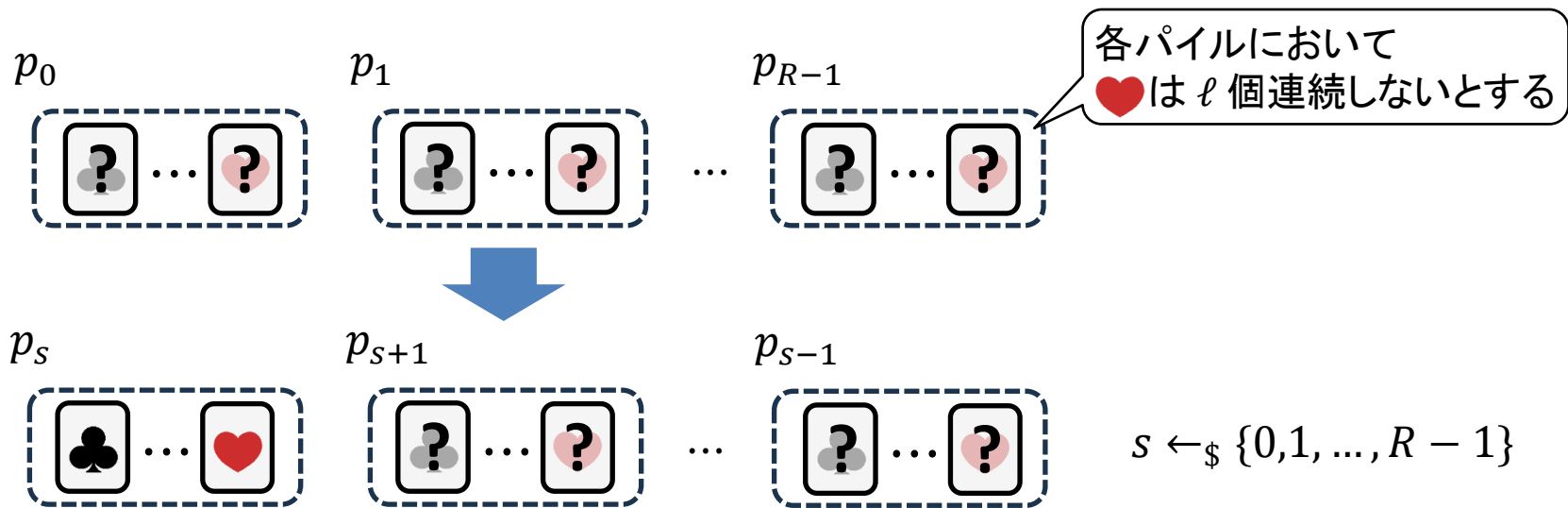
C_f : f を計算する最小回路サイズ

- Adaptive open ... オープンするカードの位置がそれまでのオープンの結果に依存する
- Static open ... オープンするカードの位置が固定（例えば、先頭のxx枚）

Single-Shuffle *Static-Open* Protocol

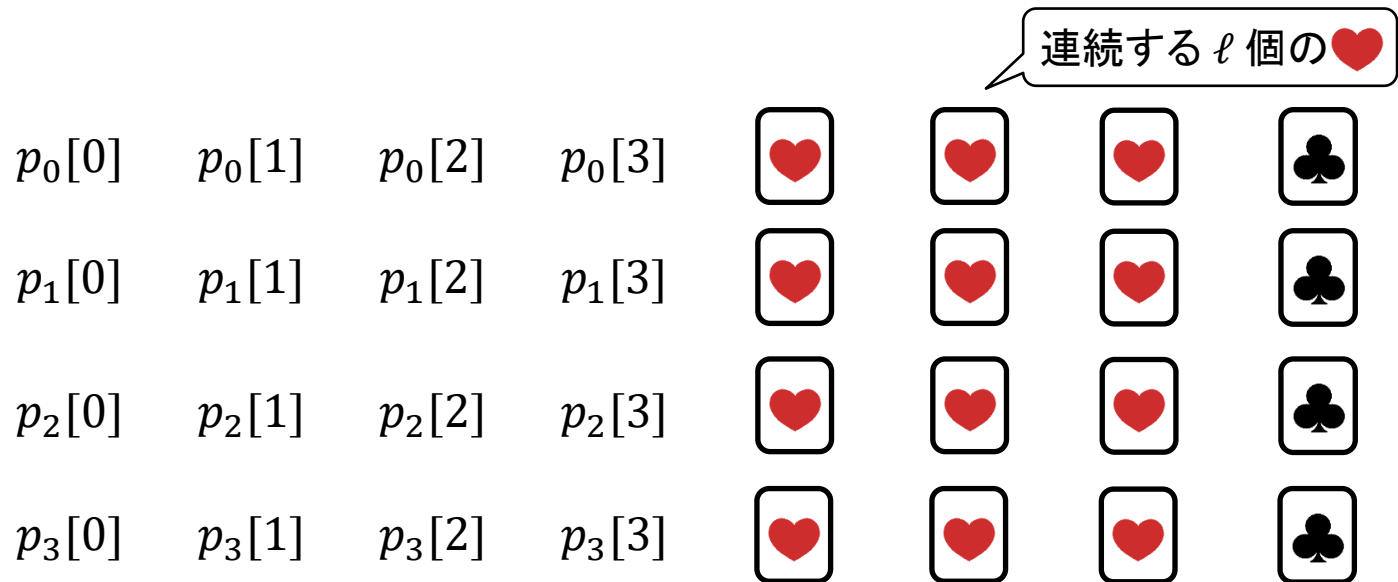


Uniform Selection

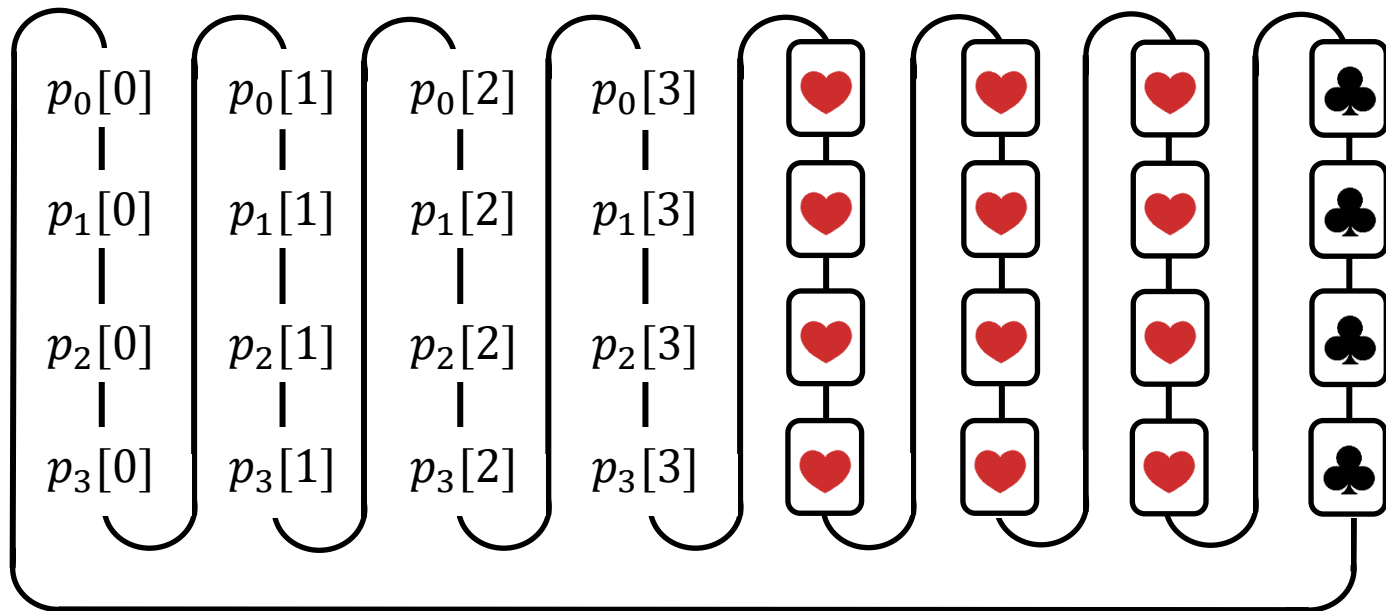


- 追加カード $(\ell + 1)R$ 枚
- シャッフル $RC \times 1$
- Static open

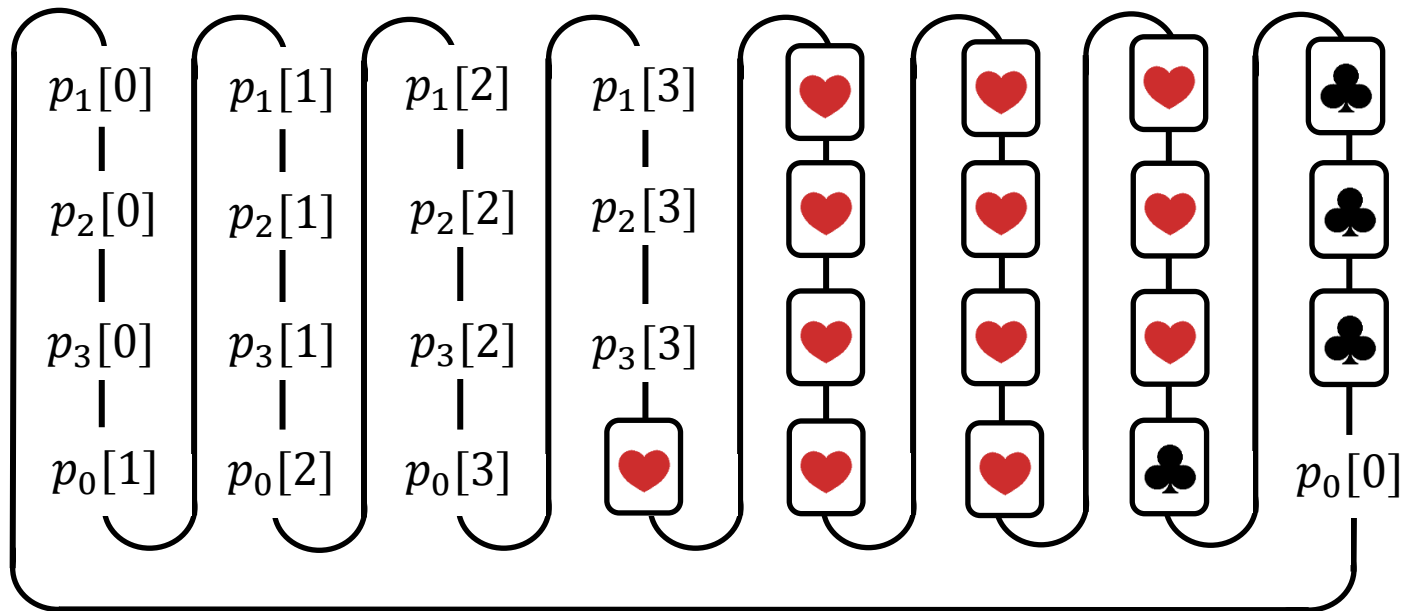
Our Method for Uniform Selection



Our Method for Uniform Selection

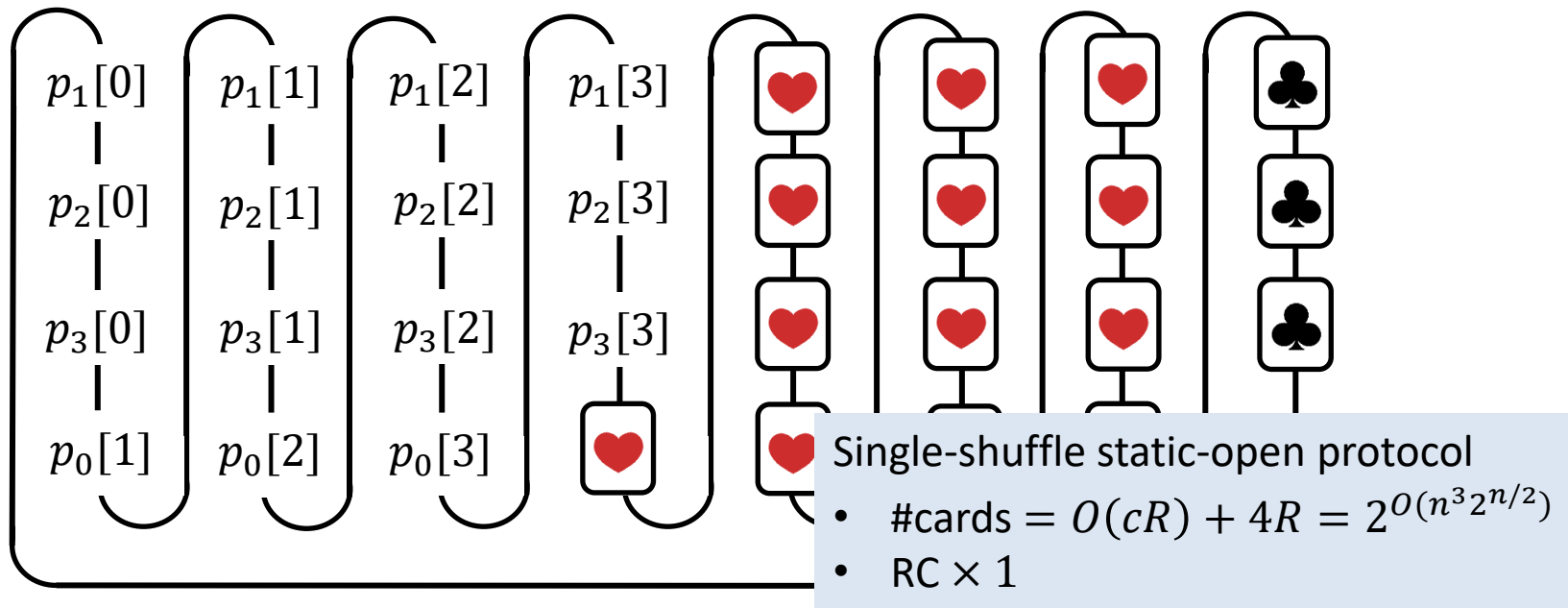


Our Method for Uniform Selection



- ♥♥♥♣により p_s の先頭カードを特定可能 → PSMの復号を実行可能

Our Method for Uniform Selection



- ♥♥♥♣により p_s の先頭カードを特定可能 → PSMの復号を実行可能

本研究の成果

方式	関数	シャッフル	カード枚数
[Boe89]	2入力AND	$RC \times 1$	5
[SM18]	2入力XOR	$RC \times 1$	4
[SN25]	3入力XOR	$RC \times 1$	8
[KTMM22]	n 入力XOR	$PSh \times (n - 1)$	$2n$
		$PSc \times 2$	$O(n \log n)$
[TMM21]	3入力majority	$RC \times 1$ & $PSh \times 1$	6
[HST14, SM18]	3入力equality	$RC \times 1$	6
本研究	Any function $f : \{0,1\}^n \rightarrow \{0,1\}$	$PSh \times 1$ & $CS \times 1$	$2^{O(n^3 2^{n/2})}$
		$PSh \times O(n 2^n)$ & $PSc \times 1$	$O(n^2 2^n)$

Reduction to SSFO for AND

- SSFO for n -input AND があれば SSFO for general f を構成できる。

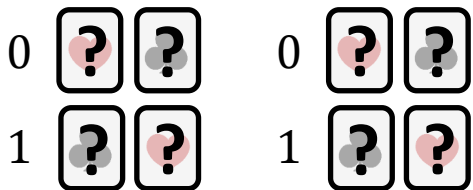
$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

Reduction to SSFO for AND

- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して

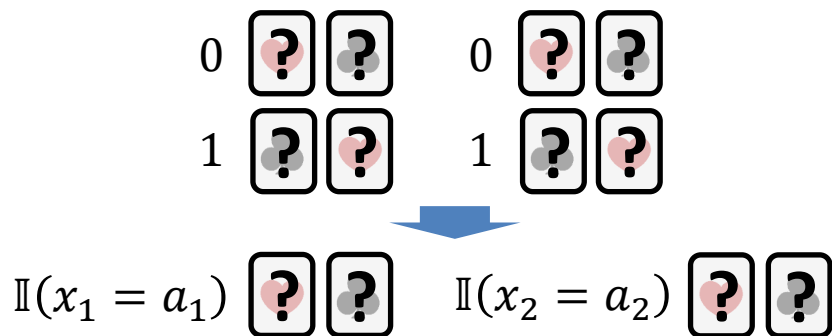


Reduction to SSFO for AND

- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して

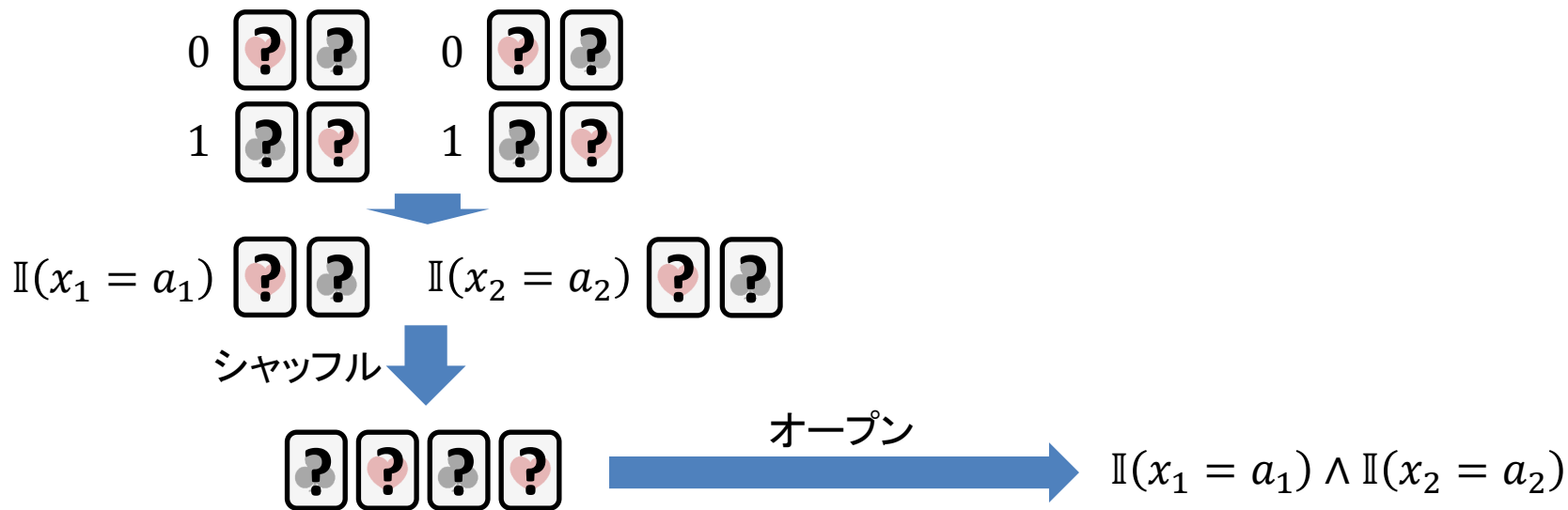


Reduction to SSFO for AND

- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して

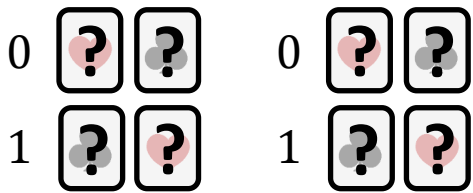


Reduction to SSFO for AND

- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して



シャッフル

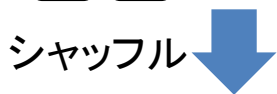
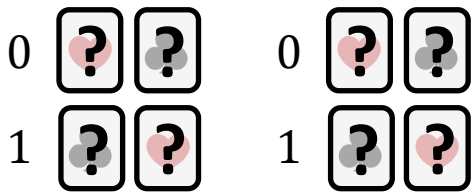



Reduction to SSFO for AND

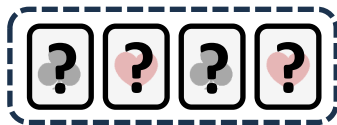
- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して



シャッフル



Apply PSc. to the $|f^{-1}(1)|$ piles

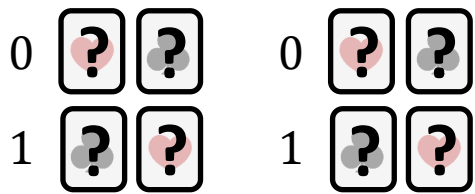


Reduction to SSFO for AND

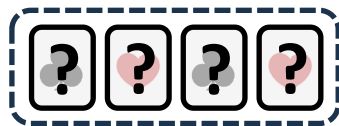
- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して



シャッフル



Apply PSc. to the $|f^{-1}(1)|$ piles

オープン

$$[\mathbb{I}(x_1 = a_1) \wedge \mathbb{I}(x_2 = a_2) : a \in f^{-1}(1)]$$

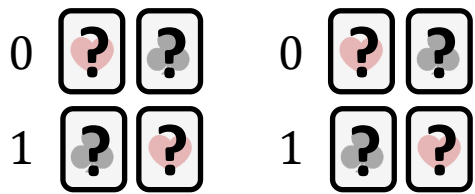
$$\begin{aligned} f(x) = 0 &\Rightarrow [0, 0, \dots, 0] \\ f(x) = 1 &\Rightarrow [1, 0, \dots, 0] \end{aligned}$$

Reduction to SSFO for AND

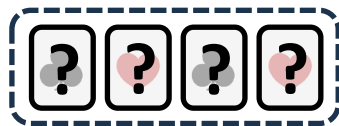
- SSFO for n -input AND があれば SSFO for general f を構成できる。

$$f(x_1, \dots, x_n) = \sum_{a \in f^{-1}(1)} \mathbb{I}(x_1 = a_1) \wedge \dots \wedge \mathbb{I}(x_n = a_n)$$

各 $a \in f^{-1}(1)$ に対して



シャッフル



Apply PSc. to the $|f^{-1}(1)|$ piles

オープン

$$[\mathbb{I}(x_1 = a_1) \wedge \mathbb{I}(x_2 = a_2) : a \in f^{-1}(1)]$$

Overhead

カード枚数 : $O(2^n)$ 倍

シャッフル : $O(2^n)$ 回合成 & PSc $\times 1$

$$\begin{aligned} f(\mathbf{x}) = 0 &\Rightarrow [0, 0, \dots, 0] \\ f(\mathbf{x}) = 1 &\Rightarrow [1, 0, \dots, 0] \end{aligned}$$

SSFO Tailored to AND

- PSM for n -input AND [FKN94]
 - $p > n$: 素数
 - 乱数: $u \in \mathbb{Z}_p^*$, $(r_1, \dots, r_n) \in \mathbb{Z}_p^n$ such that $\sum_i r_i = 0 \bmod p$
 - メッセージ: $m_i = u(1 - x_i) + r_i \bmod p$ for $x_i \in \{0,1\}$

$$\sum_i m_i = u(n - \sum_i x_i) \neq 0 \Leftrightarrow x_i = 1 \ (\forall i)$$

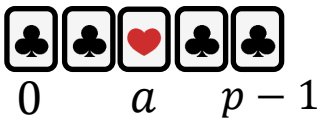
- 先ほどのPSM-to-SSFO変換により SSFO for AND を得ることはできる
 - カード枚数は $n^{O(n)} = 2^{O(n \log n)}$
- 上記の構造を利用するとカード枚数を削減できる ($O(n^2)$ 枚)

SSFO Tailored to AND

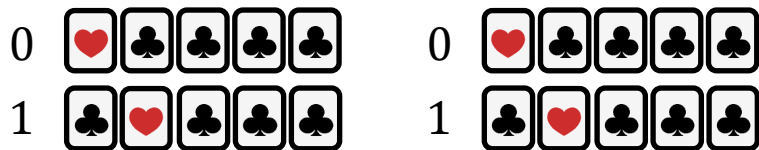
- 符号化 $a \in \mathbb{Z}_p \rightarrow$ 
0 a p-1
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$

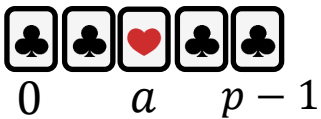
SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$ 
- メッセージ

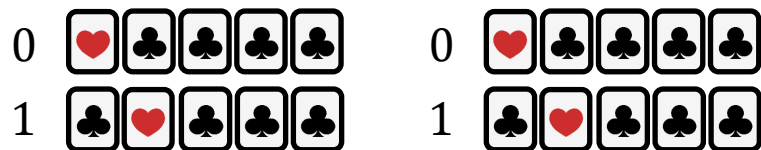
$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$



SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$ 
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$

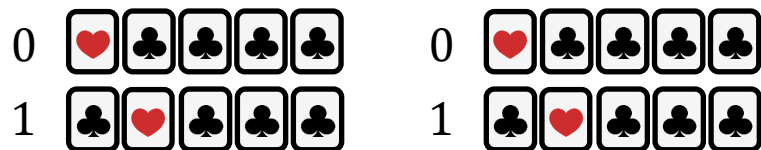


SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$ 

0
 a
 $p-1$
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$



Pile-shifting



uy_1

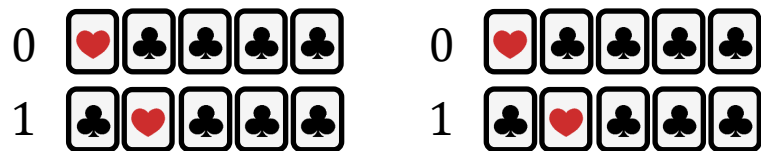
uy_2

$u \leftarrow \mathbb{Z}_p^*$

SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$  $0 \quad a \quad p-1$
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$



Pile-shifting



$$uy_1$$

$$uy_2$$

$$u \leftarrow \mathbb{Z}_p^*$$

Pile-shifting $\times (n-1)$

$$r_1 \leftarrow \mathbb{Z}_p$$



$$uy_1 + r_1$$



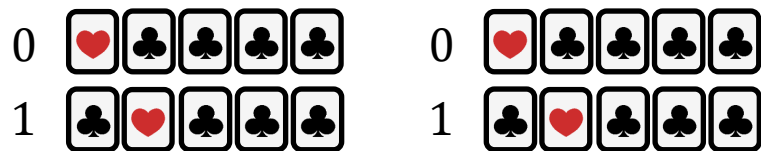
$$uy_2 - r_1$$

$$= uy_2 + r_2$$

SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$ 
0 a p-1
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$



Pile-shifting



uy_1

uy_2

$$u \leftarrow \mathbb{Z}_p^*$$

Pile-shifting $\times (n-1)$

$$r_1 \leftarrow \mathbb{Z}_p$$



$$uy_1 + r_1$$

$$uy_2 - r_1$$

$$= uy_2 + r_2$$

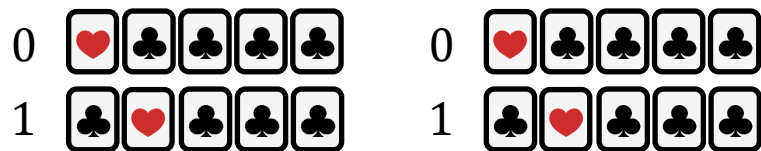
オープン

PSM for AND のメッセージ

SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$  $0 \quad a \quad p-1$
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$



Pile-shifting



uy_1

uy_2

$$u \leftarrow \mathbb{Z}_p^*$$

Pile-shifting $\times (n-1)$

$$r_1 \leftarrow \mathbb{Z}_p$$



$uy_1 + r_1$

$uy_2 - r_1$

$$= uy_2 + r_2$$

オープン

PSM for AND のメッセージ

SSFO for AND

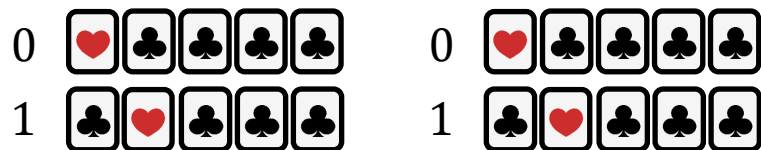
カード枚数: $pn = O(n^2)$

シャッフル: $\text{PSh} \times n$

SSFO Tailored to AND

- 符号化 $a \in \mathbb{Z}_p \rightarrow$ 
0 a p-1
- メッセージ

$$m_i = uy_i + r_i \text{ ただし } y_i = 1 - x_i$$



Pile-shifting



uy_1

uy_2

$$u \leftarrow \mathbb{Z}_p^*$$

Pile-shifting $\times (n-1)$

$$r_1 \leftarrow \mathbb{Z}_p$$



$uy_1 + r_1$

$uy_2 - r_1$

$$= uy_2 + r_2$$

オープン

PSM for AND のメッセージ

SSFO for AND

カード枚数: $pn = O(n^2)$

シャッフル: $\text{PSh} \times n$

SSFO for f

カード枚数: $O(n^2 2^n)$

シャッフル: $\text{PSh} \times O(n 2^n) \text{ \& } \text{PSc} \times 1$

まとめ

- 任意の関数に対する SSFO プロトコルを初めて提案

方式	関数	シャッフル	カード枚数
本研究	<i>Any function</i> $f : \{0,1\}^n \rightarrow \{0,1\}$	PSh $\times$ 1 & CS $\times$ 1	$2^{O(n^3 2^{n/2})}$
		PSh $\times O(n 2^n)$ & PSc $\times$ 1	$O(n^2 2^n)$

- カード組の一部のみをオープンする場合、ランダムカット1回に削減可能
- 今後の課題
 - カード枚数の削減
 - 特定の関数に特化した効率化