ANDプロトコルにまつわる未解決問題

水木 敬明
東北大学サイバーサイエンスセンター

産学連携によるカードベース暗号の数理的未解決問題と新課題の整理｜共2023a020
九州大学 伊都キャンパス ウエスト1号館 D棟 4階 IMIオーディトリアム（W1-D-413）
2023年5月31日（水）10:00-11:30　オープニング、セッション1

ANDプロトコルにまつわる未解決問題

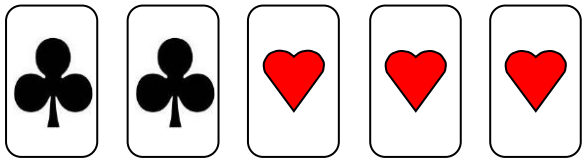
- 2色カード組、1ビット2枚符号化
- 標準モデル（パブリックモデル、シャッフルモデル）[MS14]
- 2入力や多入力のANDを秘密計算するプロトコル
- コミット型、非コミット型

※　ANDを扱う理由：(i) ANDができるとORもできる、(ii) XORは容易

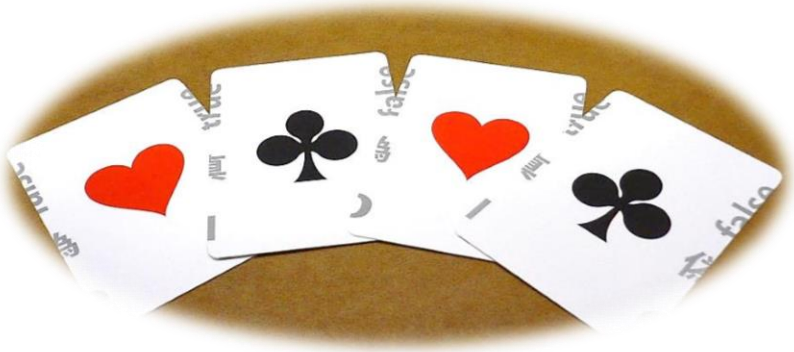
[MS14] Takaaki Mizuki and Hiroki Shizuya. A formalization of card-based cryptographic protocols via abstract machine. Int. J. Inf. Secur., 13(1):15–23, 2014.

目次

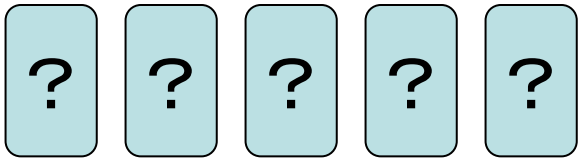
2色カード組



表

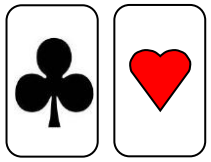


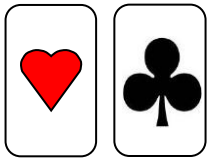
ひっくり返す

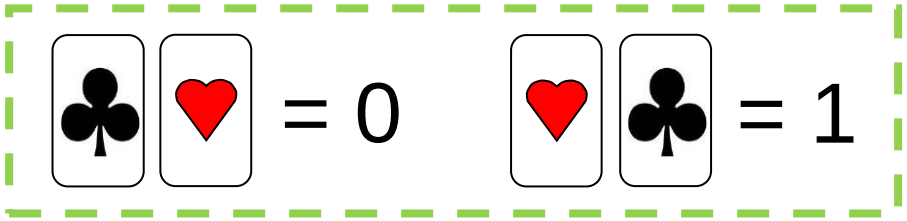


裏

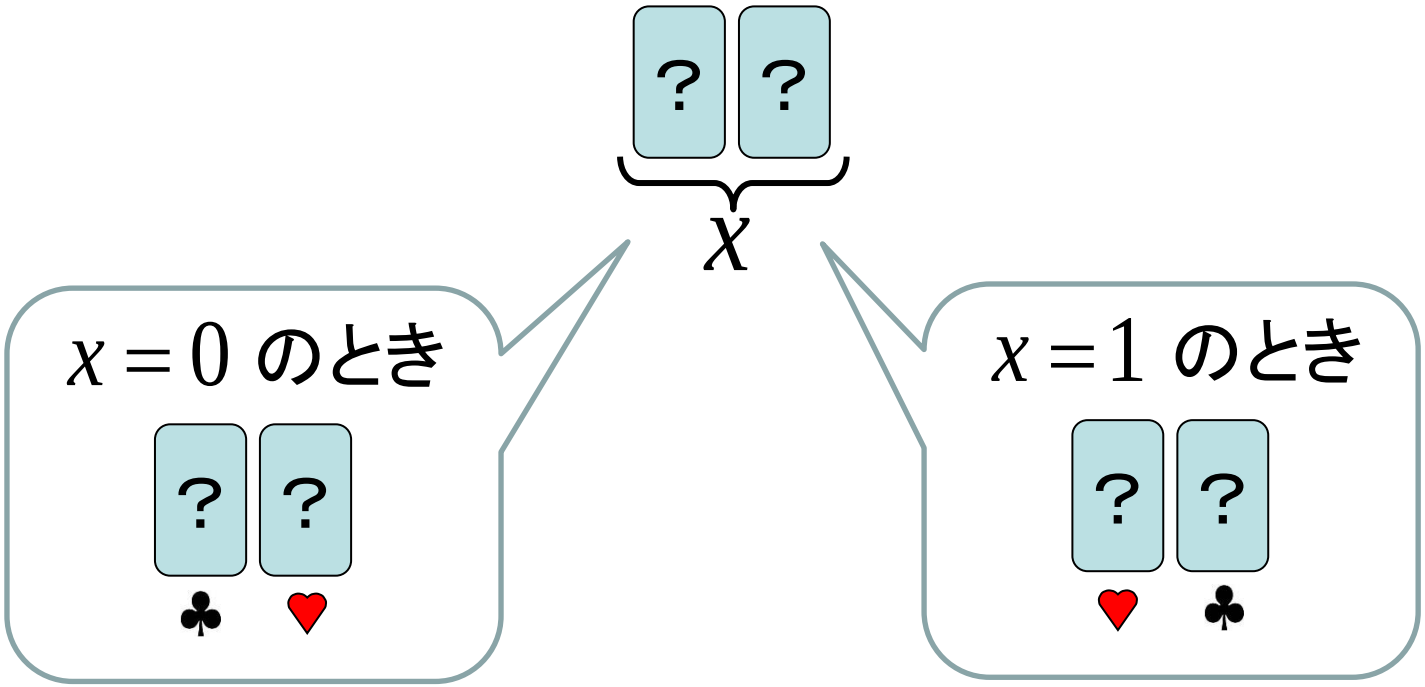
符号化

 = 0

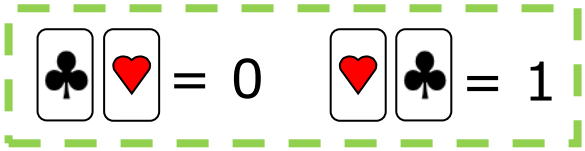
 = 1

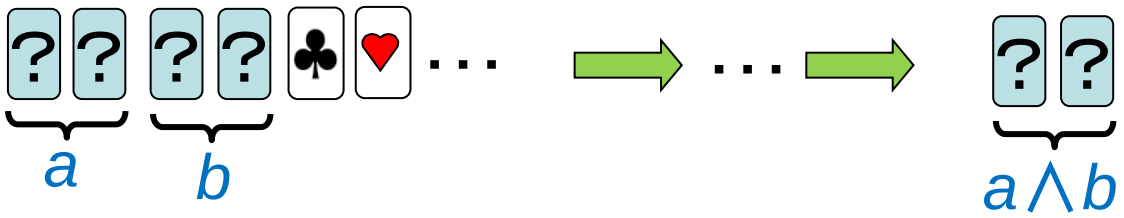


符号化に従う裏に置かれたカードを*コミットメント*と呼ぶ:



コミット型（2入力）ANDプロトコル

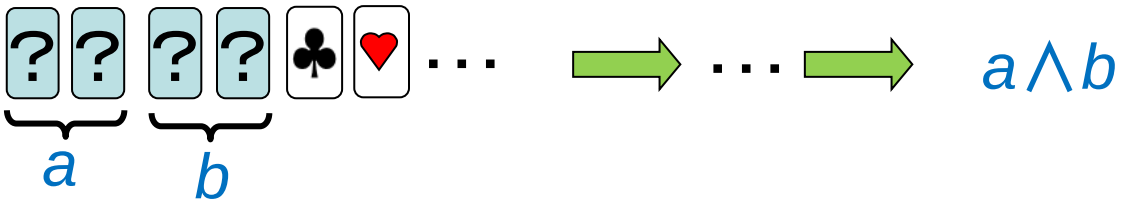




例：Mizuki-Sone ANDプロトコル [MS09]

出力がコミットメント

非コミット型（2入力）ANDプロトコル



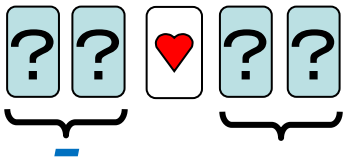
例：Five-Card Trick [DB90]

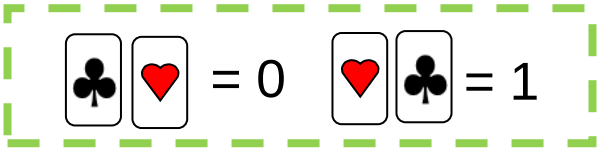
そうではない

[DB90] Bert Den Boer. More efficient match-making and satisfiability the five card trick. Advances in Cryptology—EUROCRYPT ’89, volume 434 of LNCS, pages 208–217, Berlin, Heidelberg, 1990. Springer.
[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR. Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

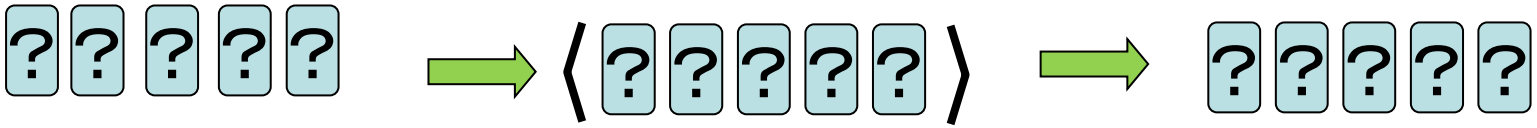
非コミット型ANDプロトコルの例：Five-Card Trick [DB90]

1. 5枚のカードを次のように置く:

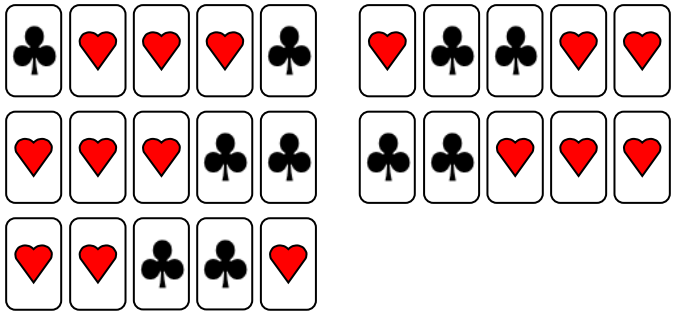




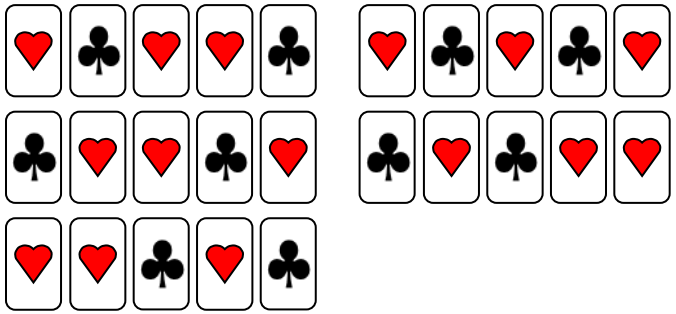
2. 真ん中のカードを裏にして，ランダムカットを適用する:



3. 5枚すべてのカードを表にする:



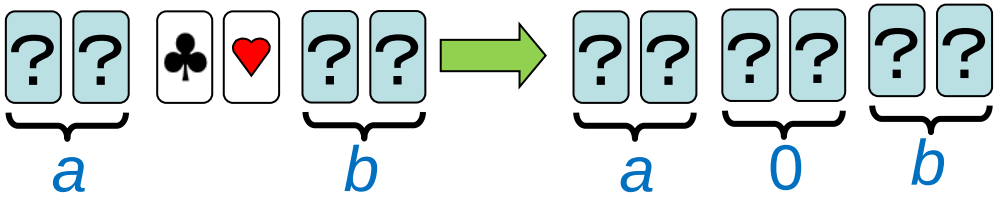
$a \wedge b = 1$

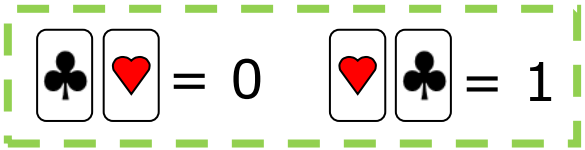


$a \wedge b = 0$

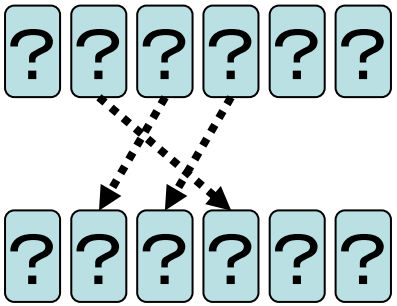
コミット型ANDプロトコルの例：Mizuki-Sone AND [MS09]

1. 初期配置:

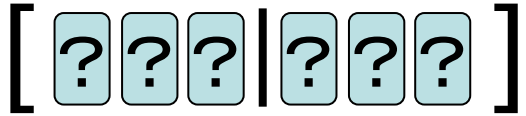




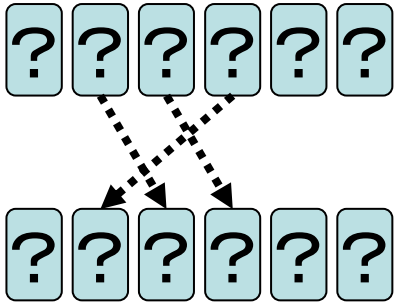
2. 並べ替え:



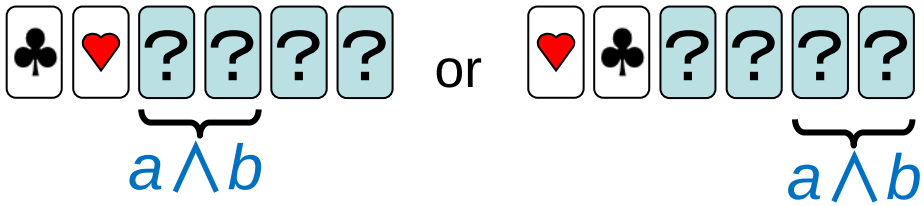
3. ランダム二等分割カット:



4. 並べ替え:



5. 左端の二枚をめくる:



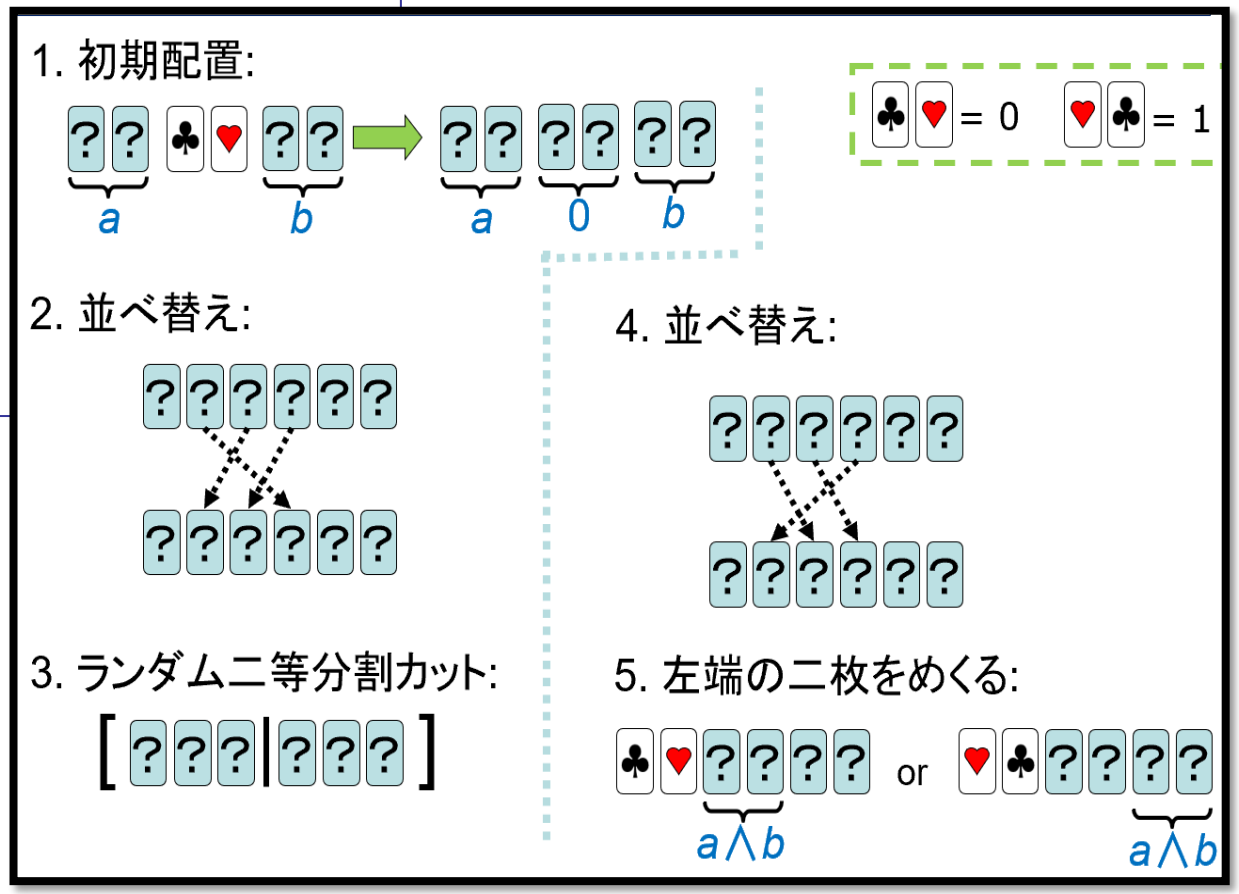
標準モデルにおけるプロトコル

- プロトコルは抽象機械によって定式化されている[MS14]

- 簡単に言うと、次の3つの動作の組み合わせ
  - (turn, T): T に含まれる番目のカードをめくる
  - (perm, π): 置換π の並べ替え
  - $(\mathrm{shuf}, \Pi, \mathcal{F})$: 分布$\mathcal{F}$ に従って, 置換 $\pi \in \Pi$ を適用
    （一様のとき分布の記述は省略）

Mizuki-Sone ANDプロトコルの疑似コード

```
(turn, {3, 4})
(perm, (2 4 3))
(shuf, {id, (1 4)(2 5)(3 6)})
(perm, (2 3 4))
(turn, {1, 2})
if ♣♡ appears then
 (result, (3, 4))
else
 (result, (5, 6))
```



シャッフルの性質

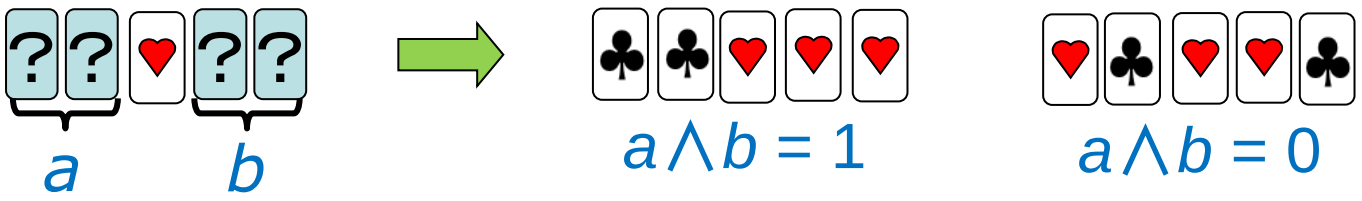
$(\mathrm{shuf}, \Pi, \mathcal{F})$: 分布$\mathcal{F}$ に従って, 置換 $\pi \in \Pi$ を適用

- $\mathcal{F}$が一様分布のとき、そのシャッフルは**一様**と言う
- Πが閉じている（部分群になっている）とき、そのシャッフルは**閉じている**と言う

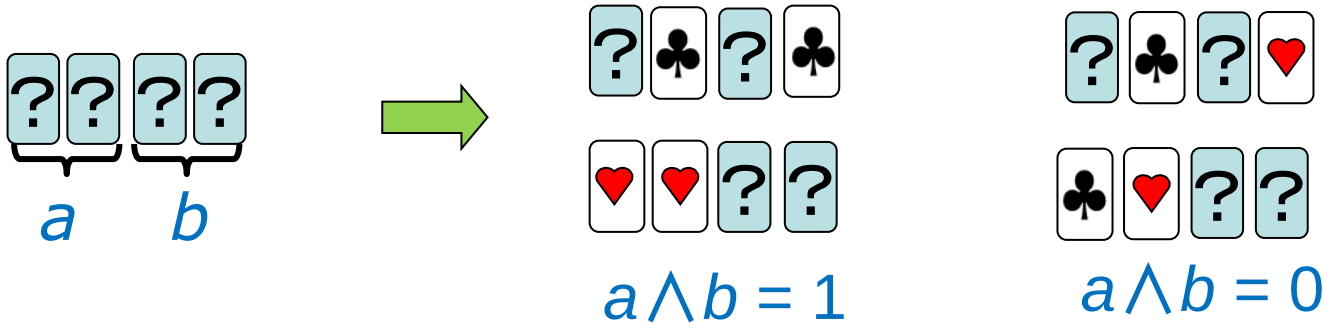
- ランダムカットやランダム二等分割カットは、どちらも一様で閉じているシャッフルである
- 一般に、一様で閉じているシャッフルは、人間が実装しやすいと考えられている

目次

- ✓ Den Boer の ***Five-Card Trick*** [DB90]は, ***5*** 枚の非コミット型ANDプロトコル:

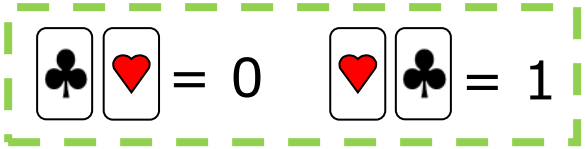


- ✓ ***4*** 枚の非コミット型ANDプロトコル [MKS12]:

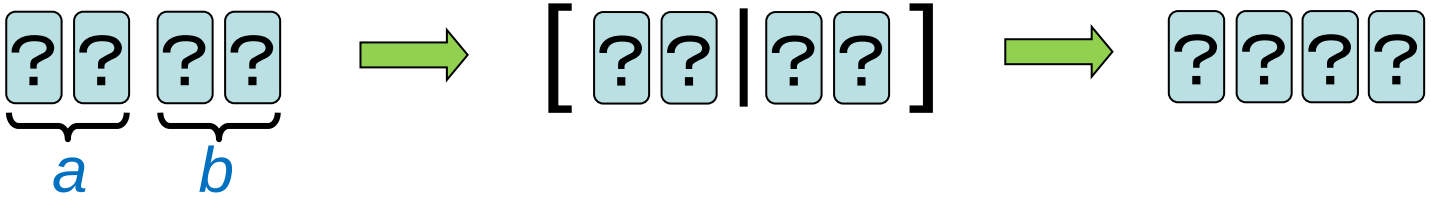


[MKS12] Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone. The five-card trick can be done with four cards. Advances in Cryptology—ASIACRYPT 2012, volume 7658 of LNCS, pages 598–606, Berlin, Heidelberg, 2012. Springer

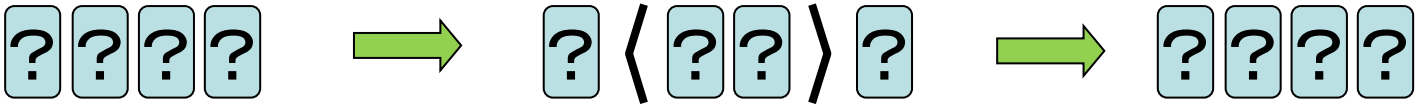
Mizuki-Kumamoto-Sone AND プロトコル[MKS12]



1. コミットメントを置き，ランダム二等分割カットを適用する：

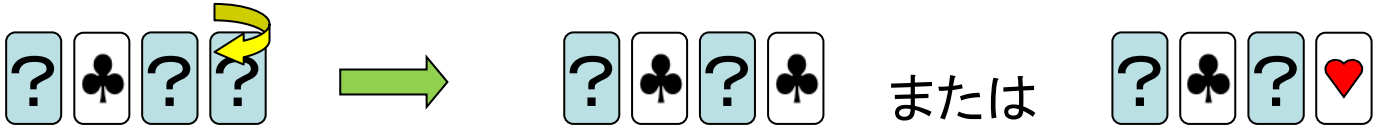


2. 中央の二枚に普通のシャッフルを適用する：

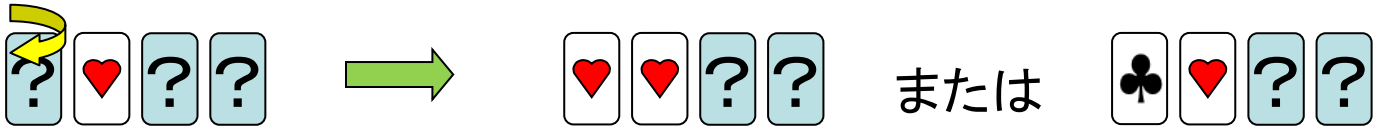


3. 2枚目をめくり，(1) 黒なら4枚目，(2) 赤なら1枚目をめくる：

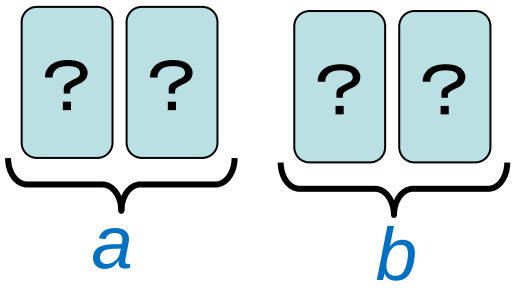
(1)



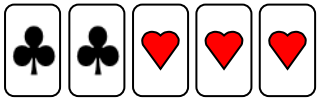
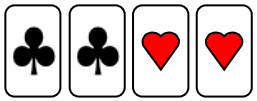
(2)



非コミット型ANDプロトコルのまとめ



$a \wedge b = ?$

	枚数等	シャッフル回数
Den Boer [DB09]	5 	1
Mizuki-Kumamoto-Sone [MKS12]	4 	2

非コミット型2入力ANDプロトコルの現在地

- 知られているものは、Five-Card TrickとMizuki-Kumamoto-Soneプロトコルの2つだけ
- （このモデルにおいて）4枚というカード枚数は最小であり、これ以上減らせない
- 出力フォーマットやシャッフルについては検討の余地がありそう

Mizuki-Kumamoto-Soneプロトコルの2つのシャッフル

(shuf, {id, (1 3)(2 4)})
(shuf, {id, (2 3)})

どちらも一様で閉じている

これらは1つのシャッフルに結合できる:
(shuf, {id, (1 3)(2 4),(2 3),(1 3 4 2)})

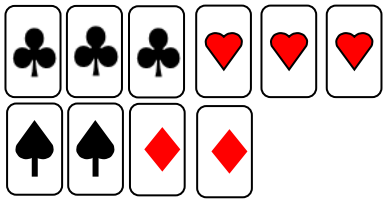
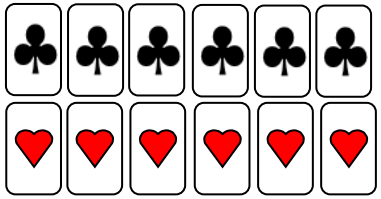
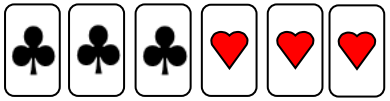
しかし、この置換の集合は閉じていない（部分群になっていない）

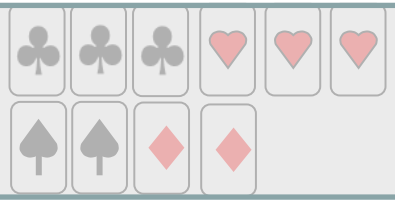
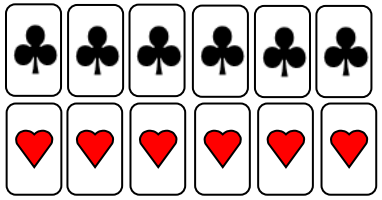
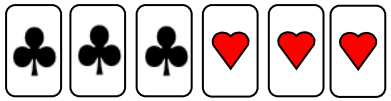
【課題】
一様で閉じているシャッフル1つで4枚非コミット型ANDプロトコルは構成できるか？

訂正：プレゼン時に「4枚コミット型」となっていたのは間違いです

目次

コミット型ANDプロトコルの歴史（2009年まで）:

	枚数等	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CR94]	10 	✔		8
Niemi-Renvall [NR98]	12 	✔		7.5
Stiglic [Sti01]	8 	✔		2
Mizuki-Sone [MS09]	6 		✔	1

	枚数等	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CR94]	10 	✔		8
Niemi-Renvall [NR98]	12 	✔		7.5
Stiglic [Sti01]	8 	✔		2
Mizuki-Sone [MS09]	6 		✔	1

[CK94] Claude Crépeau and Joe Kilian. Discreet solitary games. Advances in Cryptology—CRYPTO' 93, volume 773 of LNCS, pages 319–330, Berlin, Heidelberg, 1994. Springer
[NR98] Valtteri Niemi and Ari Renvall. Secure multiparty computations without computers. Theor. Comput. Sci., 191(1–2):173–183, 1998.
[Sti01] Anton Stiglic. Computations with a deck of cards. Theor. Comput. Sci., 259(1–2):671–678, 2001.

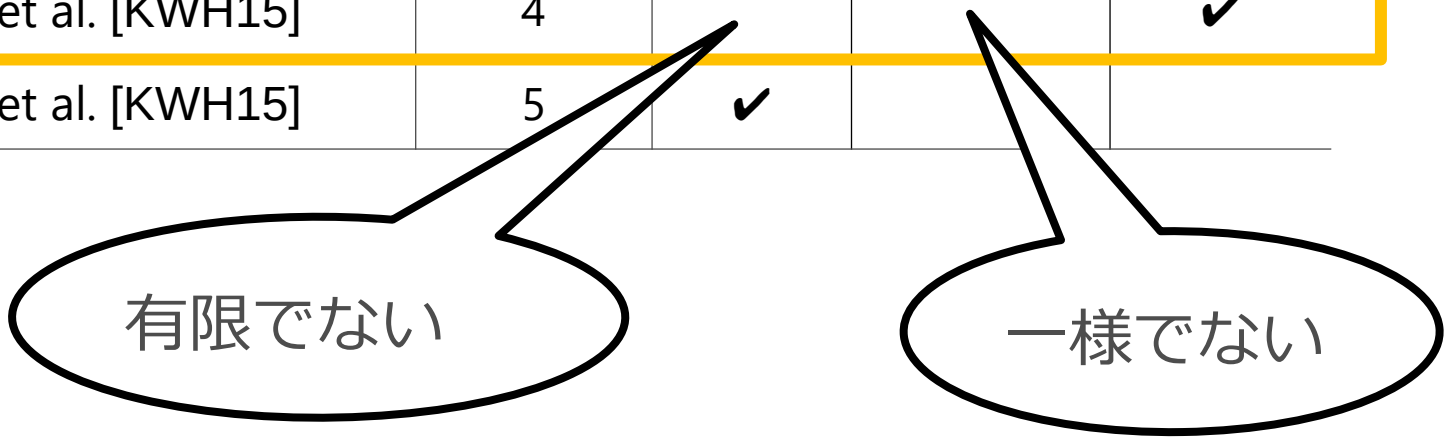
Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔

6枚より減らせるか？

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		

[KWH15] Alexander Koch, Stefan Walzer, and Kevin H¨artel. Card-based cryptographic protocols using a minimal number of cards. Advances in Cryptology—ASIACRYPT 2015, volume 9452 of LNCS, pages 783–807, Berlin, Heidelberg, 2015. Springer.

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		



[KWH15] Alexander Koch, Stefan Walzer, and Kevin H¨artel. Card-based cryptographic protocols using a minimal number of cards. Advances in Cryptology—ASIACRYPT 2015, volume 9452 of LNCS, pages 783–807, Berlin, Heidelberg, 2015. Springer.

(shuf, {id, (1 3)(2 4)})
(shuf, {id, (2 3)})
(turn, {2})
if visible seq. = (?, ♣, ?, ?) then
(turn, {2})
(shuf, {id, (1 3)})
1 (shuf, {id, (1 2)(3 4)}, id→1/3, (1 2)(3 4)→2/3)
(turn, {4})
if visible seq. = (?, ?, ?, ♣) then
(result, 1, 2)
else if visible seq. = (?, ?, ?, ♡) then
(turn, {4})
(shuf, {id, (1 3)})
(perm, (1 3 4 2))
goto 2

else if visible seq. = (?, ♡, ?, ?) then
(turn, {2})
(shuf, {id, (3 4)})
2 (shuf, {id, (1 3)(2 4)}, id→1/3, (1 3)(2 4)→2/3)
(turn, {1})
if visible seq. = (♡, ?, ?, ?) then
(result, 2, 4)
else if visible seq. = (♣, ?, ?, ?) then
(turn, {1})
(shuf, {id, (3 4)})
(perm, (1 2 4 3))
goto 1

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		

(shuf, {id, (5 4 3 2 1)}, id→2/3, (5 4 3 2 1)→1/3)

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		

一様かつ閉じるようにできないか？

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		
Abe et al. [AHMS18]	5		✔	✔

uniform closed＆5枚で実現

[AHMS18] Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Five-card AND protocol in committed format using only practical shuffles. In 5th ACM on ASIA Public-Key Cryptography Workshop, APKC '18, pages 3–8, New York, 2018. ACM

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		
Abe et al. [AHMS18]	5		✔	✔
Koch [Koc22]	4		✔	
Ruangwises, Itoh [RI19]	5	✔	✔	

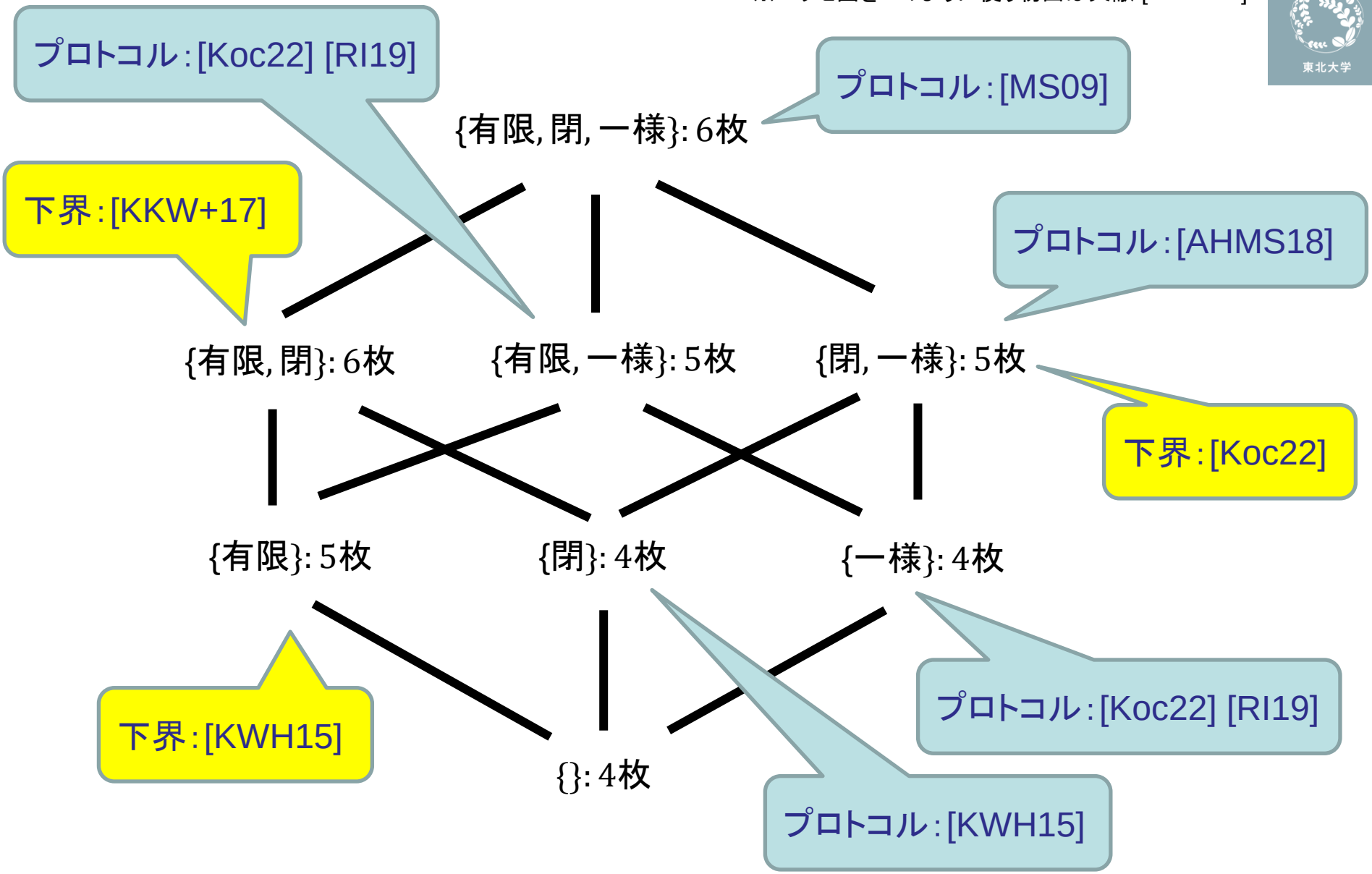
Koch et al., [KWH15]のをベースに，uniformへ

[Koc22] Alexander Koch. The landscape of optimal card-based protocols. Mathematical Cryptology, 1(2):115–131, 2022
[RI19] Suthee Ruangwises and Toshiya Itoh. AND protocols using only uniform shuffles. Computer Science–Theory and Applications, volume 11532 of LNCS, pages 349–358, Cham, 2019. Springer.

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		
Abe et al. [AHMS18]	5		✔	✔
Koch [Koc22]	4		✔	
Ruangwises, Itoh [RI19]	5	✔	✔	

次ページで、下界と最適なプロトコルを示す

※ハッセ図をこのように使う初出は文献 [KKW+17]



[KKW+17] Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. The minimum number of cards in practical card-based protocols. Advances in Cryptology—ASIACRYPT 2017, volume 10626 of LNCS, pages 126–155, Cham, 2017. Springer.

コミット型2入力ANDプロトコルの現在地

- 許されるシャッフルを「有限」「一様」「閉じている」の三つで条件を作り、各条件に対して、カード枚数が最小という意味で計算限界は解明されている

- しかし、シャッフルの回数や種類を考慮して条件を作ると、まだまだ計算限界は解明されていない（最適なプロトコルは見つかっていない）

Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔
Koch et al. [KWH15]	4			✔
Koch et al. [KWH15]	5	✔		
Abe et al. [AHMS18]	5		✔	✔
Koch [Koc22]	4		✔	
Ruangwises, Itoh [RI19]		✔	✔	

ランダムカットとランダム二等分割カットを計7回（期待値）使う

Protocols	# of cards	shuffle		
		finite	uniform	closed
Abe et al. [AHMS18]	5		✔	✔

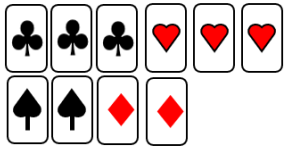
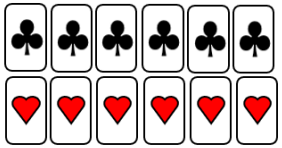
ランダムカットとランダム二等分割カットを計7回（期待値）使う

その後、7回から4.5回に改良されている[AHMS21]。

【未解決問題】
一様で閉じているシャッフルに限定し、4.5より少ない回数（期待値）のシャッフルで5枚コミット型ANDプロトコルは構成できるか？

[AHMS21] Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Five-card AND computations in committed format using only uniform cyclic shuffles. New Gener. Comput., 39(1):97–114, 2021.

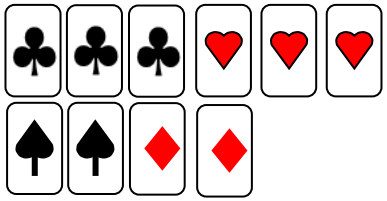
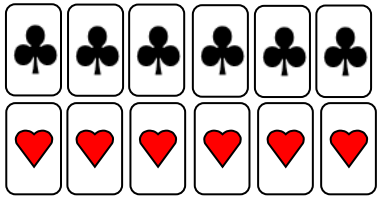
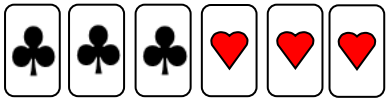
シャッフルをランダムカットのみに限定すると、

	枚数等	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CR94]	10 	✔		8
Niemi-Renvall [NR98]	12 	✔		7.5
Stiglic [Sti01]	8 	✔		2

以上のものに加え、2回のランダムカットで6枚コミット型ANDプロトコルを構成できることが2021年に示されている[AMS21] 。

下界：[KKW+17] {有限, 閉}: 6枚

[AMS21] Yuta Abe, Takaaki Mizuki, and Hideaki Sone, Committed-format AND Protocol Using Only Random Cut, Natural Computing, Springer, vol.20, no.4, pp.639-645, 2021.

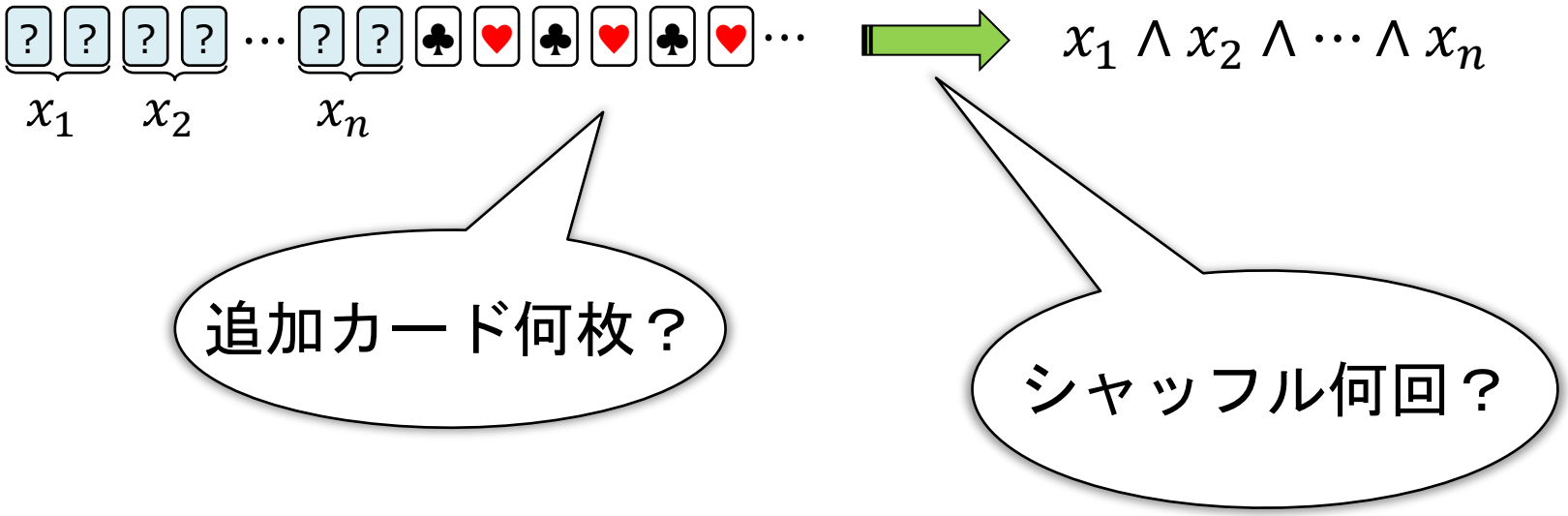
	枚数等	ランダムカット	シャッフル回数
Crépeau-Kilian [CR94]	10 	✔	8 有限でない
Niemi-Renvall [NR98]	12 	✔	7.5 有限でない
Stiglic [Sti01]	8 	✔	2 有限
Abe et. al [AMS21]	6 	✔	2 有限

すべてランダムカットしか使わない

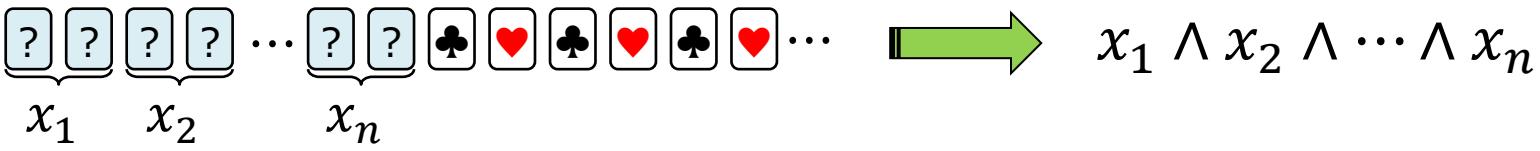
【未解決問題】
シャッフルはランダムカットしか使えないという条件のもと、5枚コミット型ANDプロトコルは構成できるか？（有限ではない）

目次

多入力ANDプロトコル



多入力ANDプロトコル

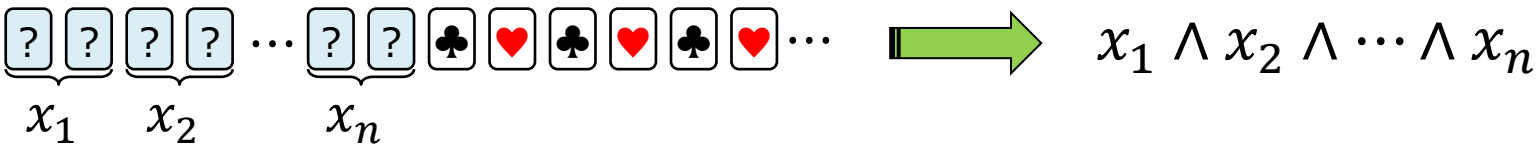


2016年に与えられた上界[Miz16]:

- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）
- 追加カード1枚 → シャッフル $n-1$ 回（非コミット型）
- 追加カードなし →
  - $n=3$ のとき、シャッフル 5 回（非コミット型）
  - $n \geq 4$ のとき、シャッフル $n+1$ 回（非コミット型）

[Miz16] Takaaki Mizuki. Card-based protocols for securely computing the conjunction of multiple variables. Theor. Comput. Sci., 622(C):34–44, 2016.

多入力ANDプロトコル



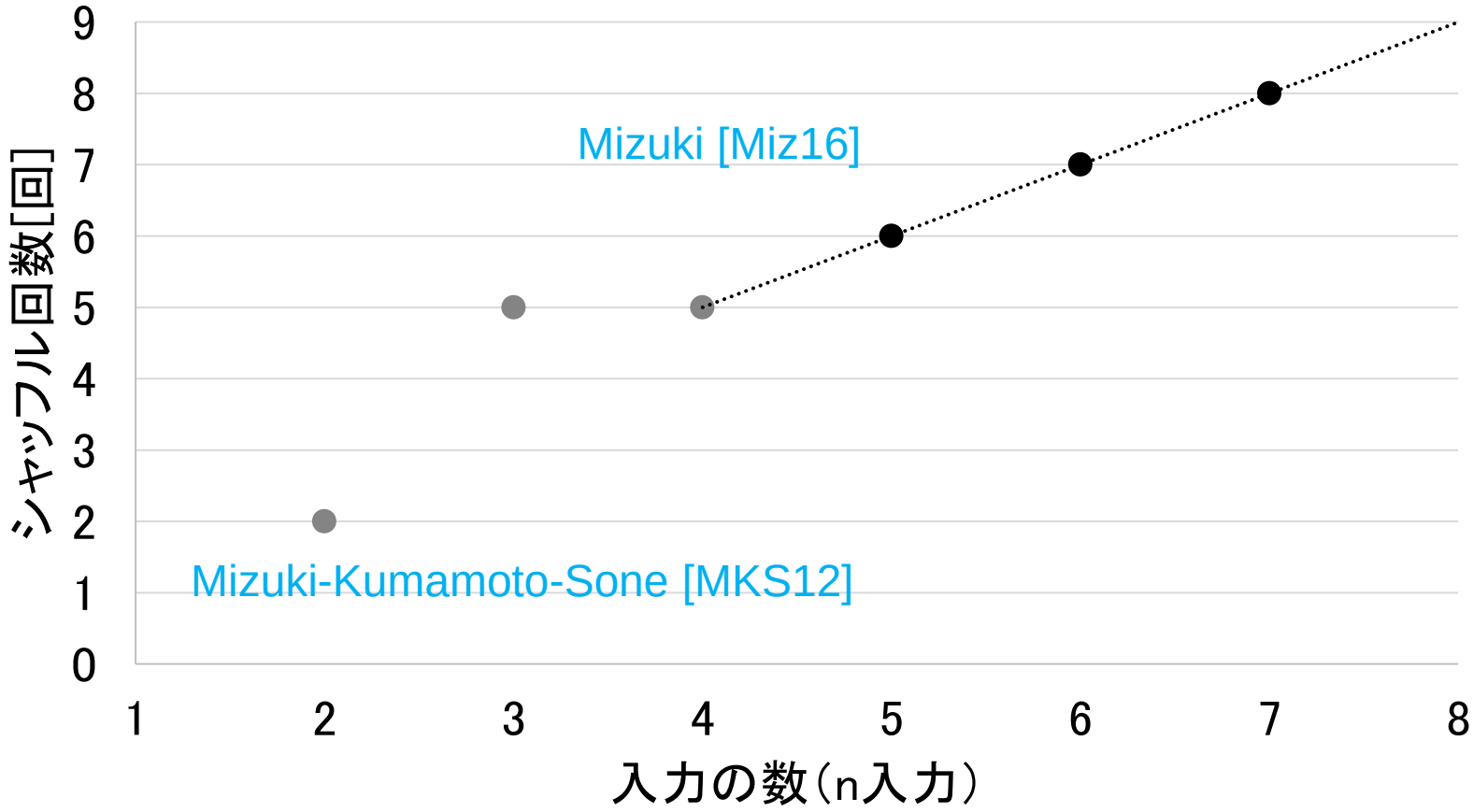
2016年に与えられた上界[Miz16]:

- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）
- 追加カード1枚 → シャッフル $n-1$ 回（非コミット型）
- 追加カードなし →
  - $n=3$ のとき、シャッフル 5 回（非コミット型）
  - $n \geq 4$ のとき、シャッフル $n+1$ 回（非コミット型）

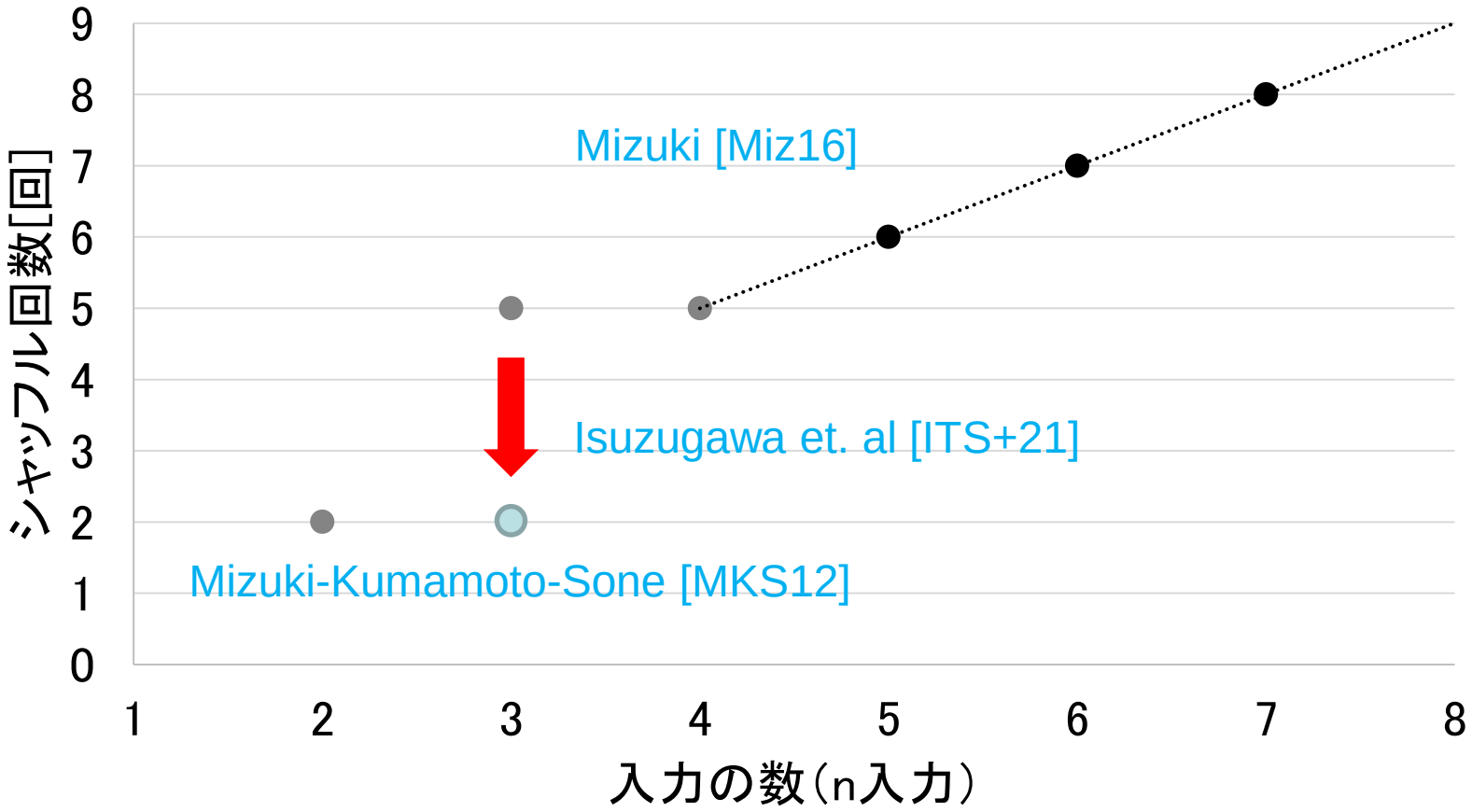
[Miz16] Takaaki Mizuki. Card-based protocols for securely computing the conjunction of multiple variables. Theor. Comput. Sci., 622(C):34–44, 2016.

2016年に与えられた上界[Miz16]:

- 追加カードなし　→
  - $n = 3$ のとき、シャッフル 5 回（非コミット型）
  - $n \geq 4$ のとき、シャッフル $n + 1$ 回（非コミット型）

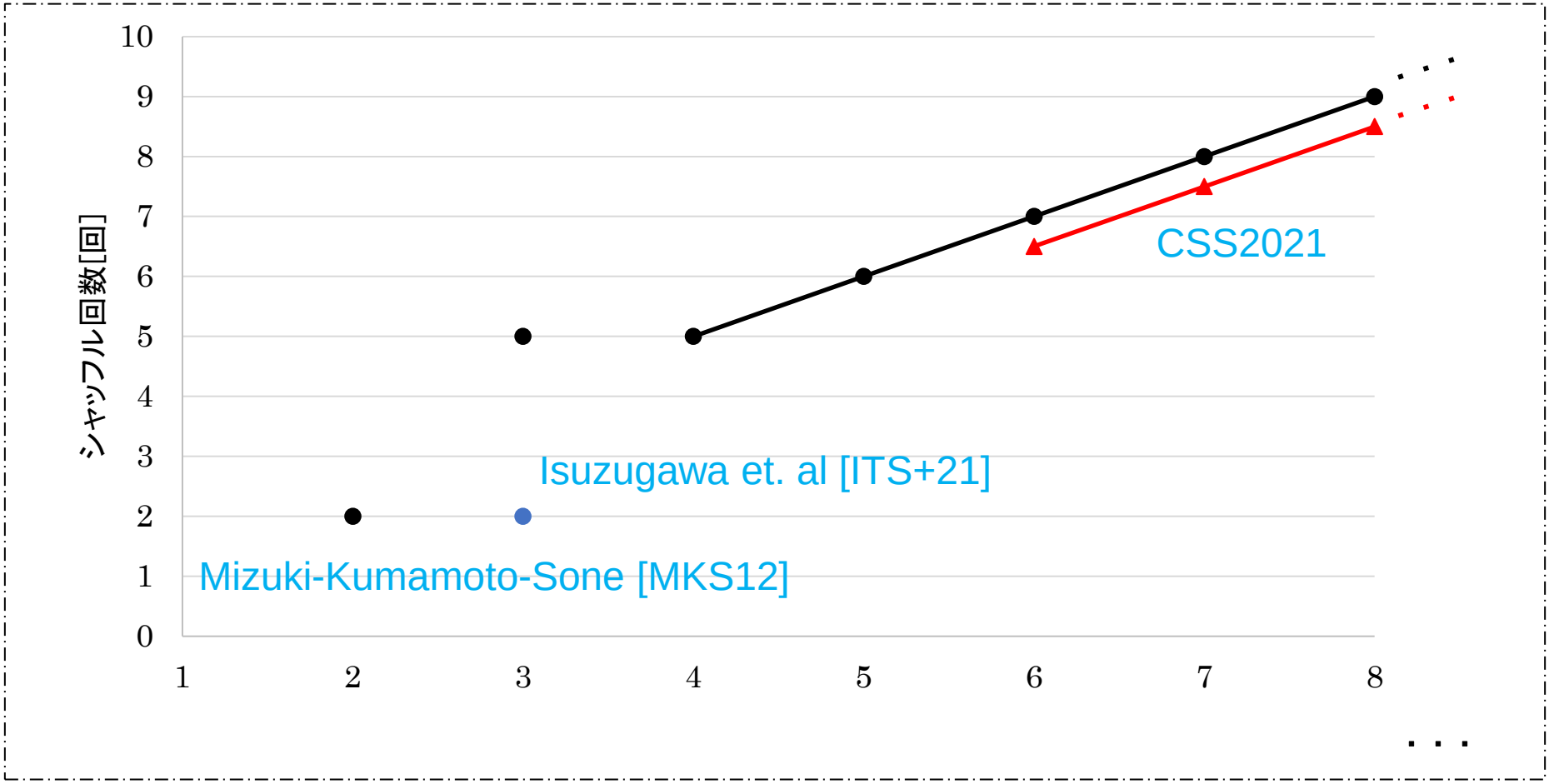


追加カードなしの2回シャッフルの3入力AND [ITS+21]：



[ITS+21] Raimu Isuzugawa, Kodai Toyoda, Yu Sasaki, Daiki Miyahara, and Takaaki Mizuki. A card-minimal three-input AND protocol using two shuffles. Computing and Combinatorics, volume 13025 of LNCS, pages 668–679, Cham, 2021. Springer.

6入力以上の場合の改善 [CSS2021]：



[CSS2021] 五十鈴川頼宗，宮原大輝，水木敬明，「最小枚数の非コミット型6入力ANDプロトコルのシャッフル回数の改善」，コンピュータセキュリティシンポジウム (CSS 2021)，2021.

追加カードなし非コミット型n入力ANDプロトコルの現在地

- 一様で閉じているシャッフルのみを使った、追加カードなし非コミット型n入力ANDプロトコルは存在する
- しかしながら、最小のシャッフル回数はわかっていない

【未解決問題】
4入力と5入力について（6入力以上も）、既存のプロトコルよりも少ないシャッフル回数で非コミット型ANDプロトコルを構成できるか？　ただし、シャッフルは一様で閉じているとする。

訂正：プレゼン時に「一様で閉じていないとする」となっていたのは間違いです

補足
- コミット型はKoch et al. [KWH15] の繰り返しで
- Mizuki-Kumamoto-Soneは（閉じていない）シャッフル1回にできる

再掲

東北大学

Mizuki-Kumamoto-Soneプロトコルの2つのシャッフル

(shuf, {id, (1 3)(2 4)})
(shuf, {id, (2 3)})

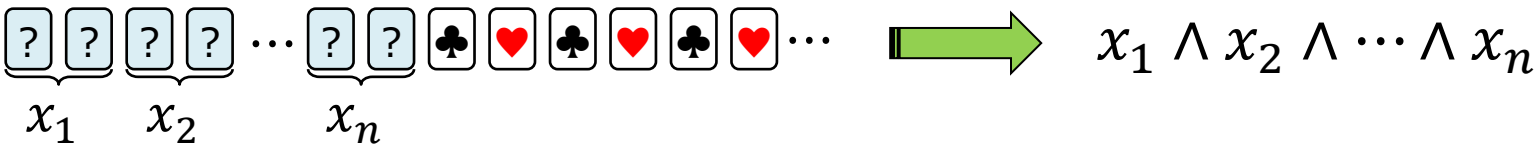
どちらも一様で
閉じている

これらは1つのシャッフルに結合できる:
(shuf, {id, (1 3)(2 4),(2 3),(1 3 4 2)})

しかし、この置換の集合は閉じていない（部分群になっていない）

【課題】
一様で閉じているシャッフル1つで4枚コミット型
ANDプロトコルは構成できるか？

多入力ANDプロトコル



2016年に与えられた上界[Miz16]:

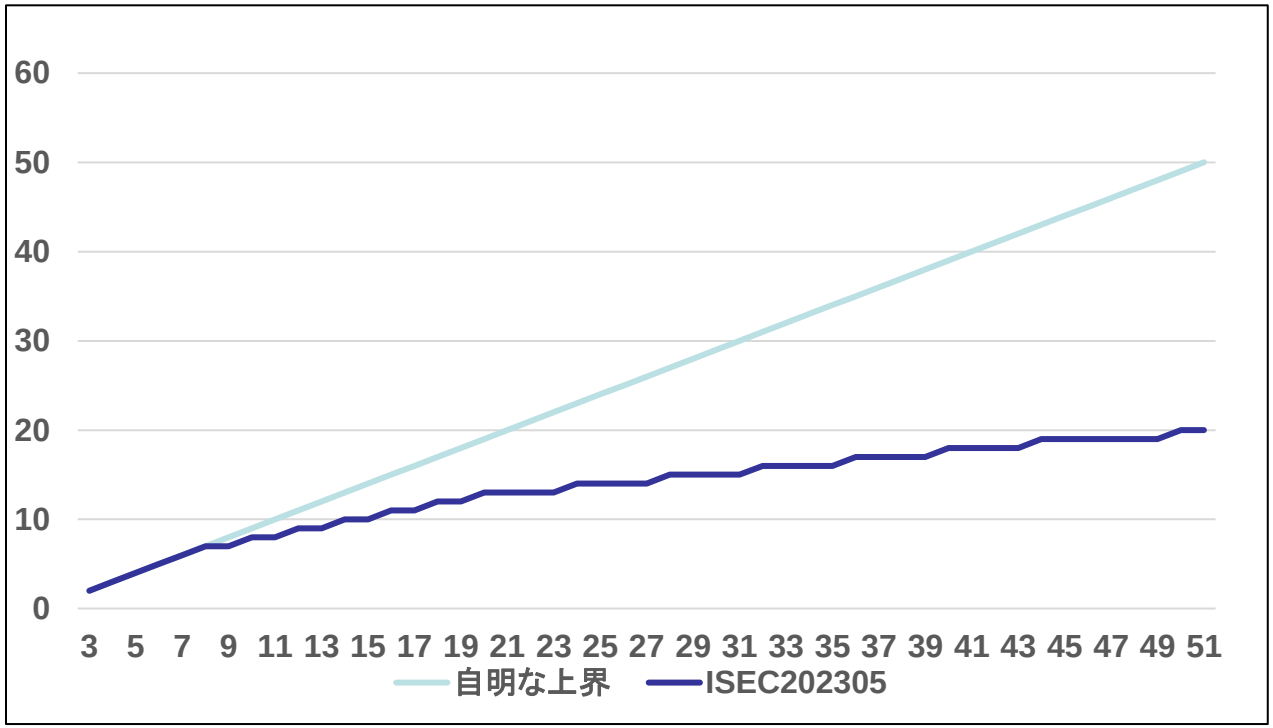
- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）
- 追加カード1枚 → シャッフル $n-1$ 回（非コミット型）
- 追加カードなし →
  - $n=3$ のとき、シャッフル 5 回（非コミット型）
  - $n \geq 4$ のとき、シャッフル $n+1$ 回（非コミット型）

[Miz16] Takaaki Mizuki. Card-based protocols for securely computing the conjunction of multiple variables. Theor. Comput. Sci., 622(C):34–44, 2016.

2016年に与えられた上界[Miz16]:

- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）

バッチングという技術 [SN21] を使うと、シャッフル回数を減らせることがわかっている [ISEC202305]



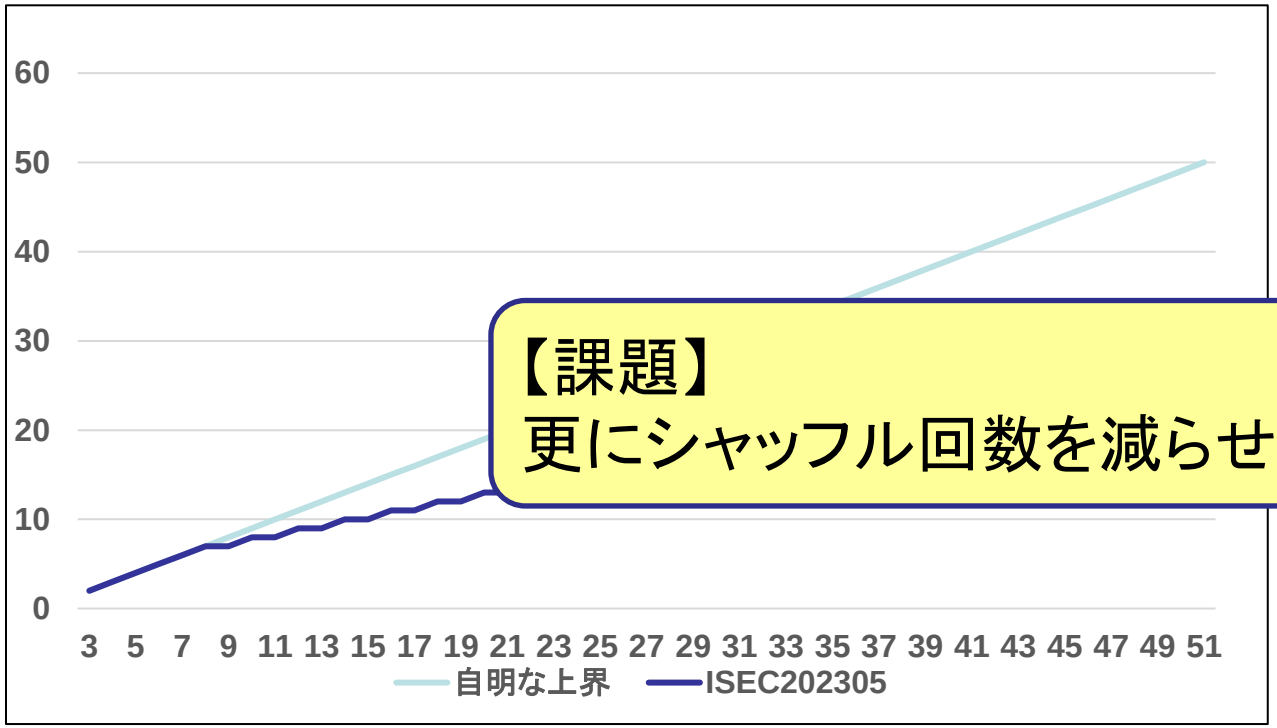
[SN21] Kazumasa Shinagawa and Koji Nuida. A single shuffle is enough for secure card-based computation of any Boolean circuit. Discrete Applied Mathematics, 289:248–261, 2021

[ISEC202305] 吉田拓叶, 中林佳祐, 田中滉大, 千田栄幸, 水木敬明,``2枚の追加カードを用いた多入力AND秘密計算におけるシャッフル回数の削減,'' 電子情報通信学会信学技報, Vol.123, No.26, ISEC2023-7, pp.35-42 (May 2023).

2016年に与えられた上界[Miz16]:

- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）

バッチングという技術 [SN21] を使うと、シャッフル回数を減らせることがわかっている [ISEC202305]



【課題】
更にシャッフル回数を減らせるか？

[SN21] Kazumasa Shinagawa and Koji Nuida. A single shuffle is enough for secure card-based computation of any Boolean circuit. Discrete Applied Mathematics, 289:248–261, 2021

[ISEC202305] 吉田拓叶, 中林佳祐, 田中滉大, 千田栄幸, 水木敬明,``2枚の追加カードを用いた多入力AND秘密計算におけるシャッフル回数の削減,'' 電子情報通信学会信学技報, Vol.123, No.26, ISEC2023-7, pp.35-42 (May 2023).

2016年に与えられた上界[Miz16]:

- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）
- 追加カード1枚 → シャッフル $n-1$ 回（非コミット型）
- 追加カードなし →
  - $n=3$ のとき、シャッフル 5 回（非コミット型）
  - $n \geq 4$ のとき、シャッフル $n+1$ 回（非コミット型）

【課題】
追加カード1枚の場合のシャッフル回数については未検討

追加カード枚数を固定するのではなく、シャッフルを1回に固定すると？

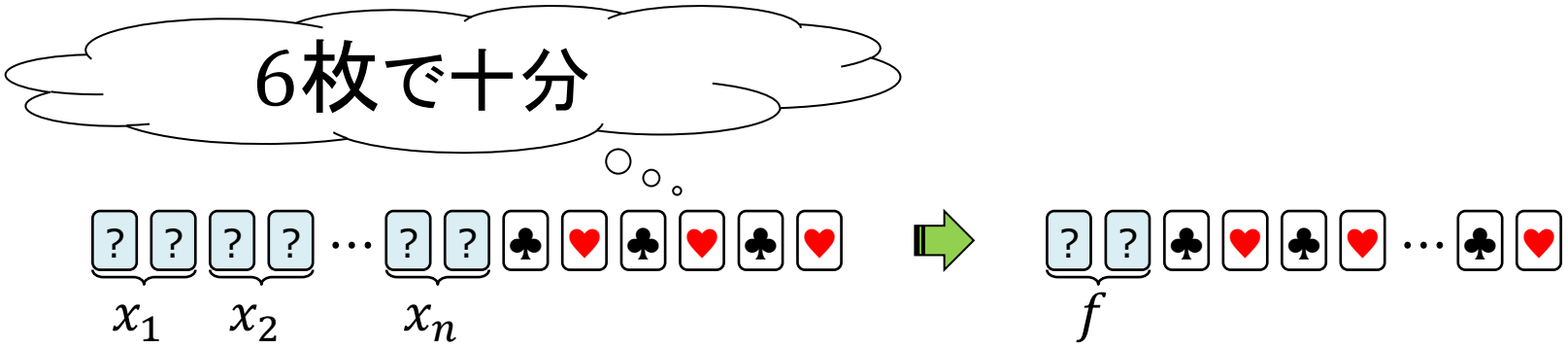
Shinagawa-Nuida [SN21] のカードベースのガーブルドサーキットの考えを応用すると、追加カード$2n-2$枚でシャッフル1回のn入力コミット型ANDプロトコルを構成できる [KTMM22]（ただし、このときのシャッフルは閉じていない）。

【未解決問題】
更に追加カード枚数を減らせるか？

[SN21] Kazumasa Shinagawa and Koji Nuida. A single shuffle is enough for secure card-based computation of any Boolean circuit. Discrete Applied Mathematics, 289:248–261, 2021
[KTMM22] Tomoki Kuzuma, Kodai Toyoda, Daiki Miyahara, and Takaaki Mizuki. Card-based single-shuffle protocols for secure multiple-input AND and XOR computations. In ASIA Public-Key Cryptography, pages 51–58, NY, 2022. ACM.

目次

任意のn入力論理関数（$n \geq 4$）に対して、追加カード6枚でコミット型プロトコルを構成できる [NHMS15a]



【未解決問題】
6枚から追加カード枚数を減らせるか？

[NHMS15a] Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Card-based protocols for any Boolean function. Theory and Applications of Models of Computation, volume 9076 of LNCS, pages 110–121, Cham, 2015. Springer.

おわりに

ANDプロトコルにまつわる未解決問題

- 2色カード組、1ビット2枚符号化
- 標準モデル（パブリックモデル、シャッフルモデル）[MS14]
- 2入力や多入力のANDを秘密計算するプロトコル
- コミット型、非コミット型

カードベース暗号の研究分野にはたくさんの未解決問題や課題があります

皆様の参入を期待しています

本研究は九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点の支援を受けた.（2023年度短期共同研究「産学連携によるカードベース暗号の数理的未解決問題と新課題の整理」（2023a020）

追加情報：XORについて

	枚数	色数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	14	4	✔		10
Mizuki, et. al [MUS06]	10	2	✔		7
Mizuki-Sone [MS09]	4	2		✔	1
Toyoda, et. al [TMMS20]	6	2	✔		2

[MUS06] Takaaki Mizuki, Fumishige Uchiike, and Hideaki Sone. Securely computing XOR with 10 cards. The Australasian Journal of Combinatorics, 36:279–293
[TMMS20] Kodai Toyoda, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. Six-card finite-runtime XOR protocol with only random cut. In ACM Workshop on ASIA Public-Key Cryptography, APKC '20, pages 2–8, New York, ACM

追加情報：XORについて

	枚数	色数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	14	4	✔		10
Mizuki, et. al [MUS06]	10	2	✔		7
Mizuki-Sone [MS09]	4	2		✔	1
Toyoda, et. al [TMMS20]	6	2	✔		2

【未解決問題】
ランダムカットのみを用いて、5枚以下でコミット型XORプロトコルを構成できるか？