昨年の研究集会からのアップデート

水木 敬明
東北大学サイバーサイエンスセンター

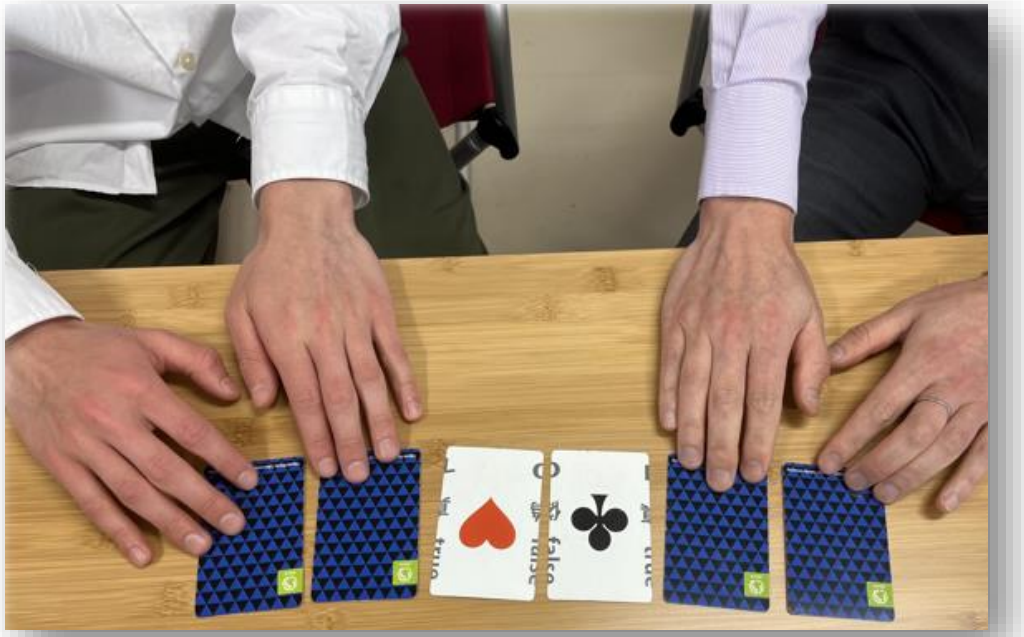
産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地｜2024a035
九州大学 伊都キャンパス ウエスト1号館 D棟 4階 IMIオーディトリアム（W1-D-413）
5月22日（水）【公開】10:00-17:45

昨年度

主催：九州大学マス・フォア・インダストリ研究所
種別・種目：一般研究-短期共同研究
研究計画題目：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
研究代表者：水木 敬明（東北大学）

組織委員	須賀 祐治（株式会社インターネットイニシアティブ） 縫田 光司（九州大学） 品川 和雅（茨城大学）

カードベース暗号は、物理的なカード組を用いて秘密計算やゼロ知識証明等の暗号機能を実現する技術である。その特徴は、カードを並べることによりプロトコルを視覚的・体験的に実行できることであり、暗号技術に関する教育的効果が期待されていることに加えて、非専門家が日常生活において利用できる実用的な暗号技術であるといえる。

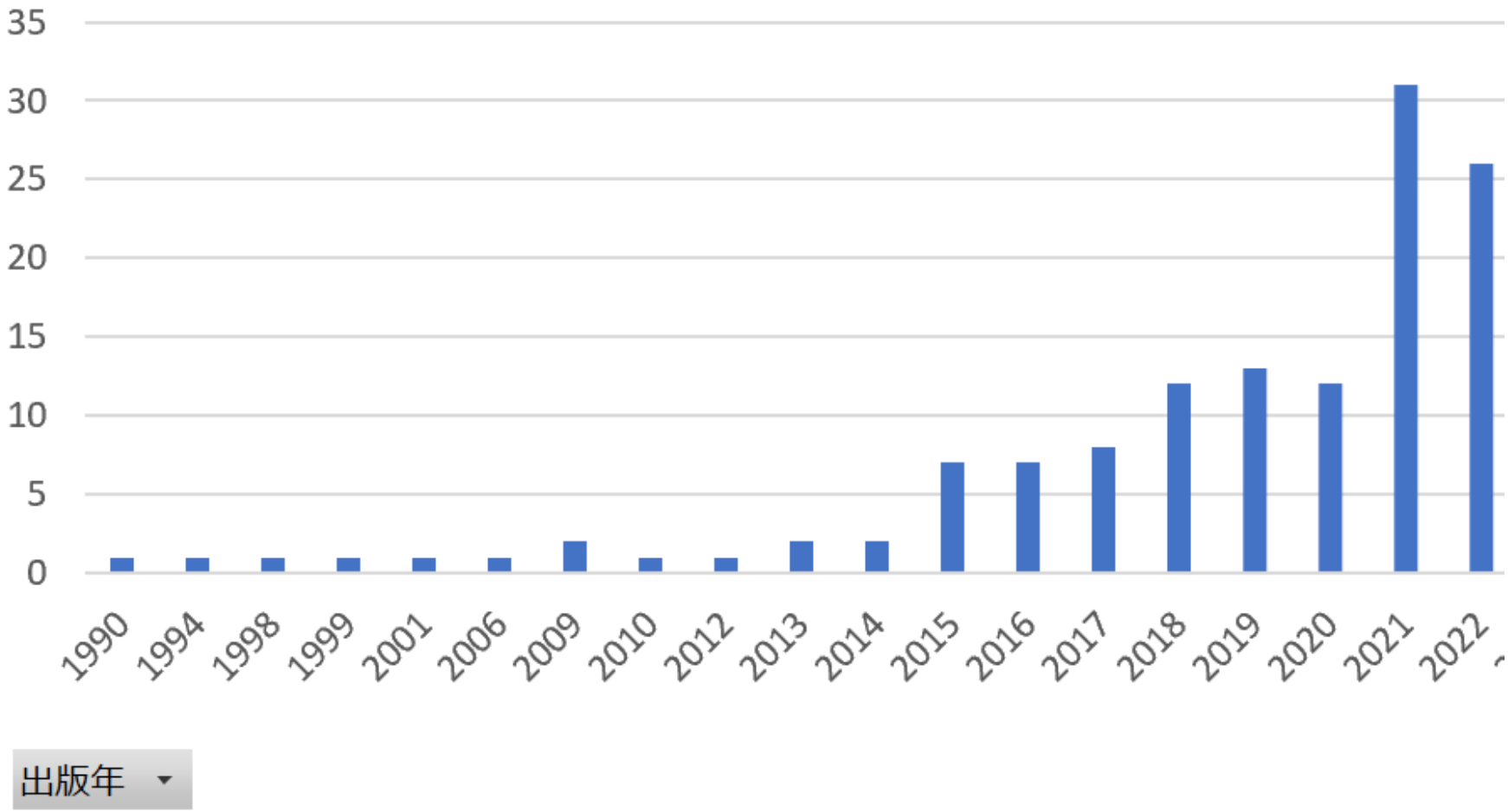


昨年度

カードベース暗号は1990年代に萌芽的研究が提案されたが、2010年代に本研究代表者らのグループが計算モデルを抽象機械によって数理的に定式化したことを皮切りに、複数の研究グループが活発に論文成果を発表するようになり、特にここ数年論文数が急増している。また同分野の近年の研究には、有限群論、アソシエーションスキーム、形式検証系などの数理科学的な題材との関連についての新しい研究テーマも現れてきており、研究分野として急成長を遂げる転換点にあると考えられる。このようにカードベース暗号分野が急速に拡大する状況において、この分野の未解決問題を把握すること自体のコストが高くなっており、新規参入のハードルは年々上がっている。

昨年度

カードベース暗号分野の Scopus掲載論文数の推移



昨年度

本共同研究では、さらなる分野の発展のため、新規に参入する研究者の増加を目標とし、この分野を先導する産業界と学術界の研究者が集中的に議論し、潜在的な研究者の参入のガイドになるような、未解決問題や新課題の整理を行う。そして、得られた整理の結果を未解決問題リストのような形で公表することにより、新規参入研究者の増大に資する。

昨年度

組織委員（講演者）
水木 敬明（東北大学 サイバーサイエンスセンター）
須賀 祐治（株式会社インターネットイニシアティブ）
縫田 光司（九州大学マス・フォア・インダストリ研究所）
品川 和雅（茨城大学 理工学研究科）

講演者
真鍋 義文（工学院大学 情報学部情報科学科）
宮原 大輝（電気通信大学 情報理工学研究科）
中井 雄士（豊橋技術科学大学）

昨年度

10:00-11:30　オープニング、セッション1　（座長：縫田 光司）

水木 敬明（東北大学 サイバーサイエンスセンター）
ANDプロトコルにまつわる未解決問題

宮原 大輝（電気通信大学 情報理工学研究科）
カードベースZKPプロトコル

} 標準モデル等

13:00-14:30　セッション2　（座長：品川 和雅）

中井 雄士（豊橋技術科学大学）
秘匿置換を用いたカードベース暗号

真鍋 義文（工学院大学 情報学部情報科学科）
無開示性を持つカードベース暗号プロトコルについて

} 秘匿置換モデル

昨年度

15:00-17:15　セッション3、クロージング　（座長：水木 敬明）

品川 和雅（茨城大学 理工学研究科）
カードベース暗号に登場するさまざまなカード組と符号化

須賀 祐治（株式会社インターネットイニシアティブ）
デッキ分割法とアソシエーションスキーム

縫田 光司（九州大学マス・フォア・インダストリ研究所）
カードベース暗号に現れる数学

カード組と符号化

数学とのかかわり

水木 敬明（東北大学 サイバーサイエンスセンター）
ANDプロトコルにまつわる未解決問題　←このあとアップデートを

宮原 大輝（電気通信大学 情報理工学研究科）
カードベースZKPプロトコル　←セッション2で

中井 雄士（豊橋技術科学大学）
秘匿置換を用いたカードベース暗号★

真鍋 義文（工学院大学 情報学部情報科学科）
無開示性を持つカードベース暗号プロトコルについて★

品川 和雅（茨城大学 理工学研究科）
カードベース暗号に登場するさまざまなカード組と符号化★

須賀 祐治（株式会社インターネットイニシアティブ）
デッキ分割法とアソシエーションスキーム　←セッション3で

縫田 光司（九州大学マス・フォア・インダストリ研究所）
カードベース暗号に現れる数学★

★未解決問題は
フレッシュ

中井 雄士（豊橋技術科学大学）
秘匿置換を用いたカードベース暗号★

真鍋 義文（工学院大学 情報学部情報科学科）
無開示性を持つカードベース暗号プロトコルについて★

品川 和雅（茨城大学 理工学研究科）
カードベース暗号に登場するさまざまなカード組と符号化★

縫田 光司（九州大学マス・フォア・インダストリ研究所）
カードベース暗号に現れる数学★

スライドと動画は
昨年度のページでご覧ください：
https://joint.imi.kyushu-u.ac.jp/post-9009/

水木 敬明（東北大学 サイバーサイエンスセンター）
ANDプロトコルにまつわる未解決問題　←このあとアップデートを

宮原 大輝（電気通信大学 情報理工学研究科）
カードベースZKPプロトコル　←セッション2で

須賀 祐治（株式会社インターネットイニシアティブ）
デッキ分割法とアソシエーションスキーム　←セッション3で

以降も、昨年度のスライドです
未解決問題はフレッシュなままです

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

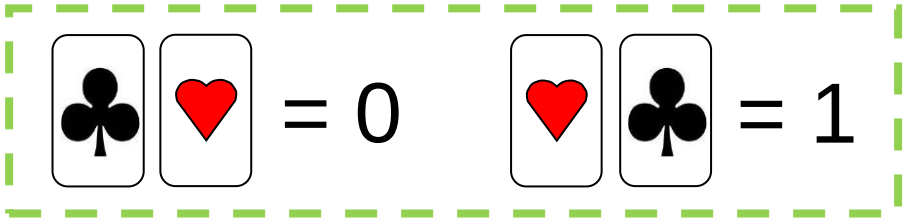
⇕ ひっくり返す

? ? ? ? ? 裏

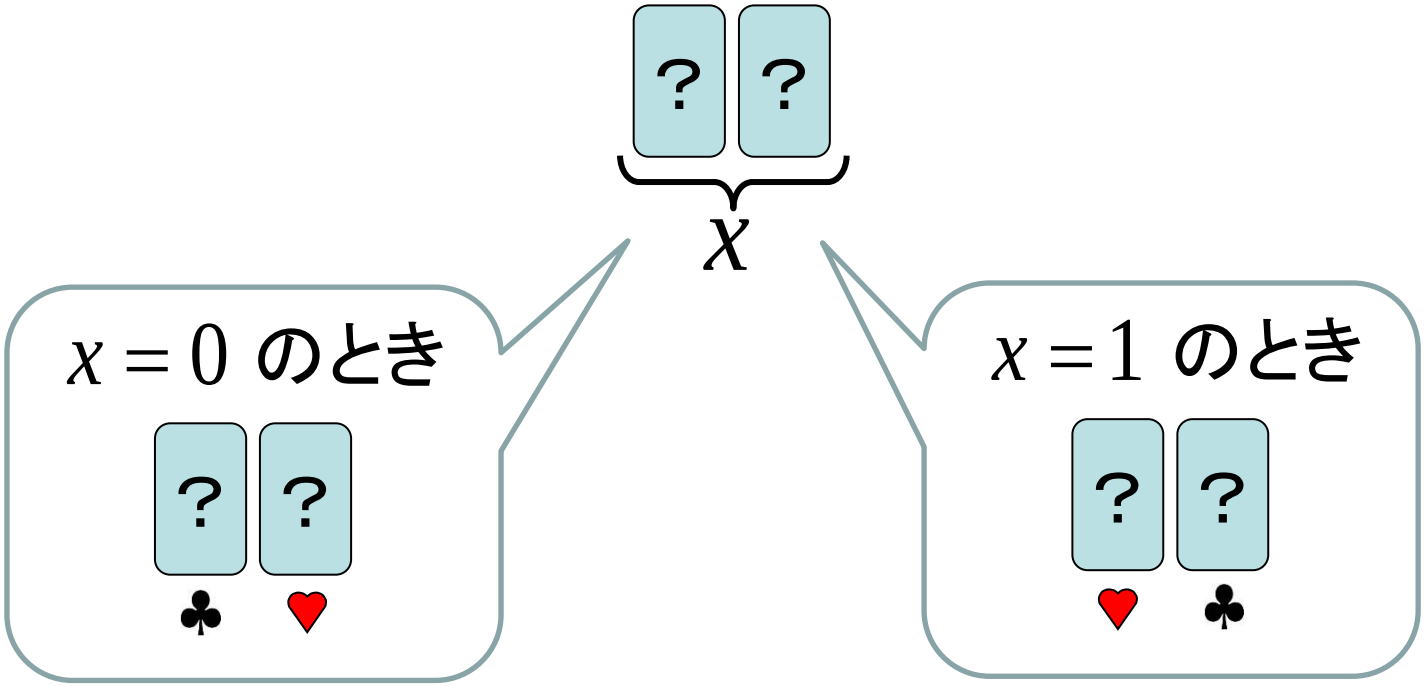
符号化

♣ ♥ = 0

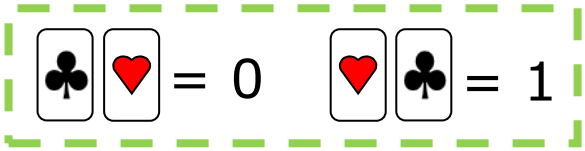
♥ ♣ = 1

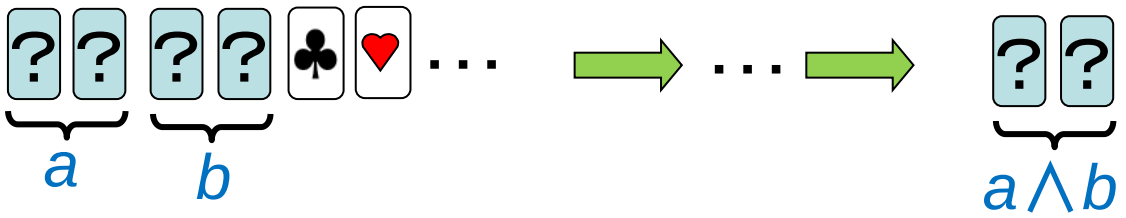


符号化に従う裏に置かれたカードを*コミットメント*と呼ぶ:



コミット型（2入力）ANDプロトコル

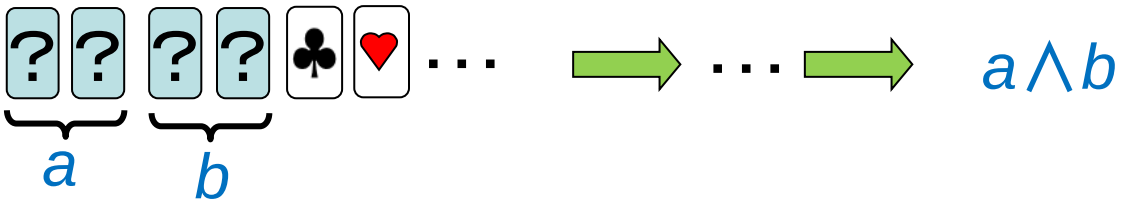




例：Mizuki-Sone ANDプロトコル [MS09]

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



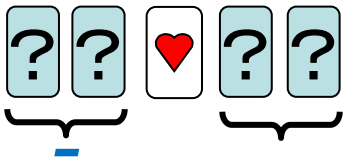
例：Five-Card Trick [DB90]

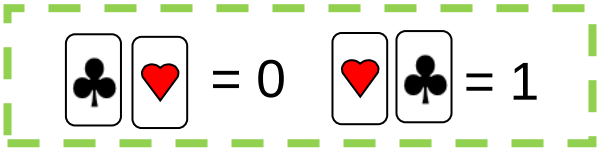
そうではない

[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.

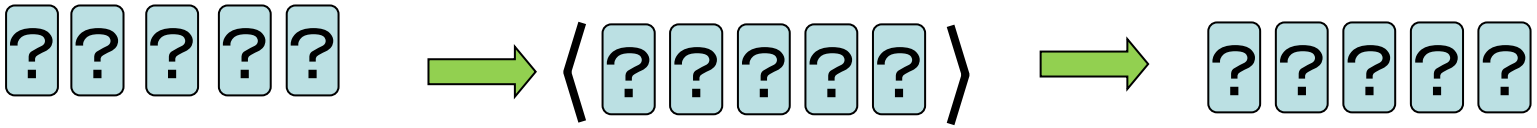
非コミット型ANDプロトコルの例：Five-Card Trick [DB90]

1. 5枚のカードを次のように置く:

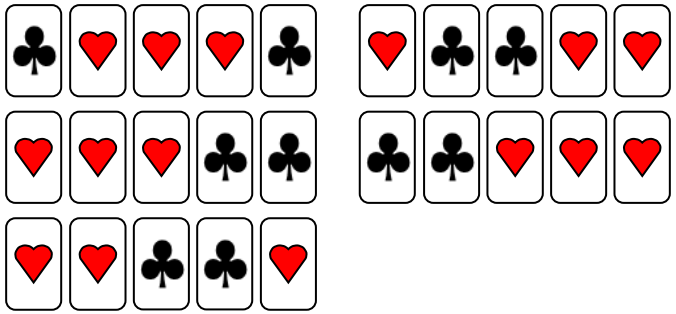




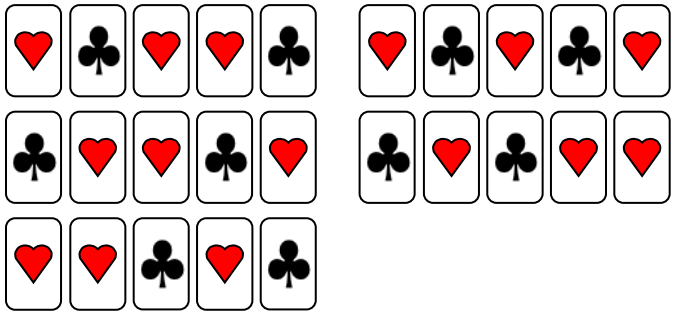
2. 真ん中のカードを裏にして，ランダムカットを適用する:



3. 5枚すべてのカードを表にする:



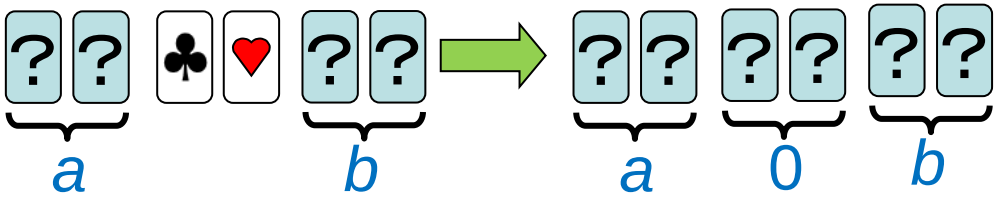
$a \wedge b = 1$

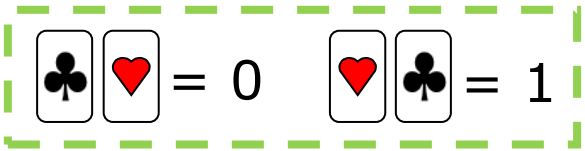


$a \wedge b = 0$

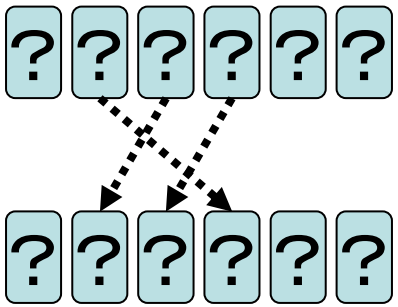
コミット型ANDプロトコルの例：Mizuki-Sone AND [MS09]

1. 初期配置:

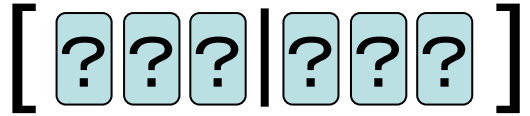




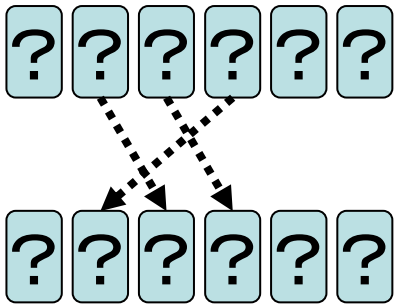
2. 並べ替え:



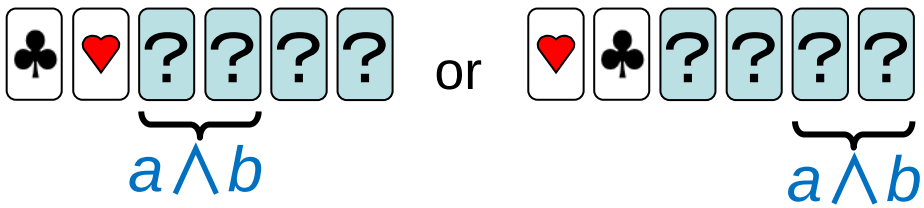
3. ランダム二等分割カット:



4. 並べ替え:



5. 左端の二枚をめくる:



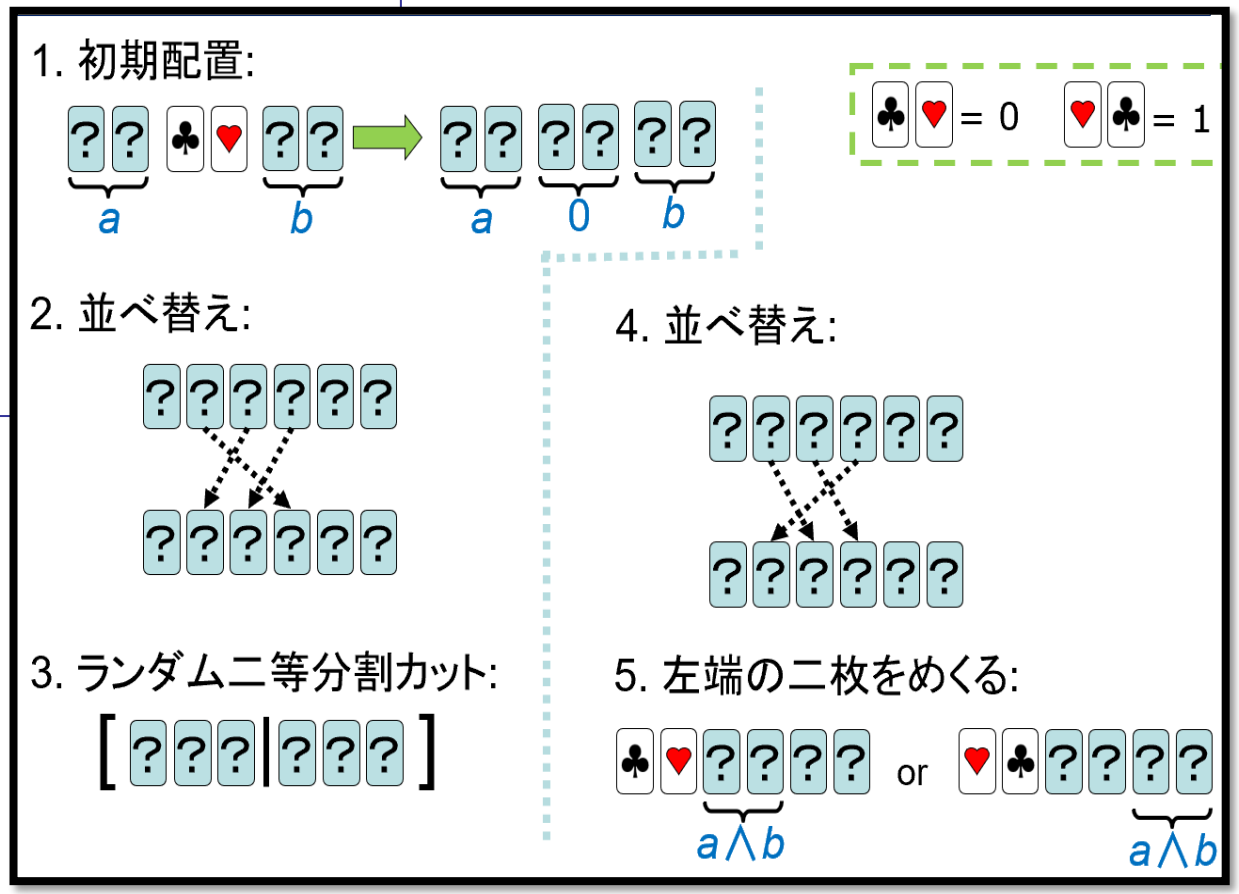
標準モデルにおけるプロトコル

- 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

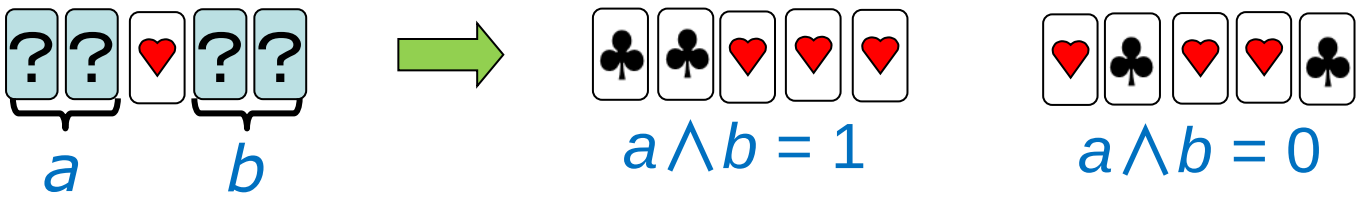
$(\mathrm{shuf}, \Pi, \mathcal{F})$: 分布$\mathcal{F}$ に従って, 置換 $\pi \in \Pi$ を適用

- $\mathcal{F}$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

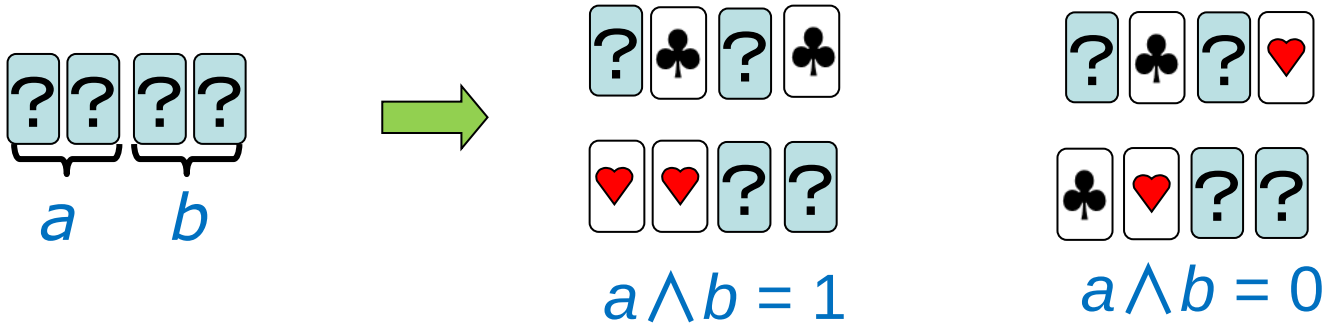
- ランダムカットやランダム二等分割カットは、どちらも一様で閉じているシャッフルである
- 一般に、一様で閉じているシャッフルは、人間が実装しやすいと考えられている

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:

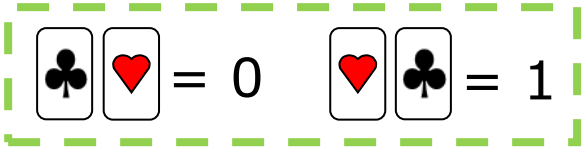


- ✓ ***4*** 枚の非コミット型ANDプロトコル [MKS12]:

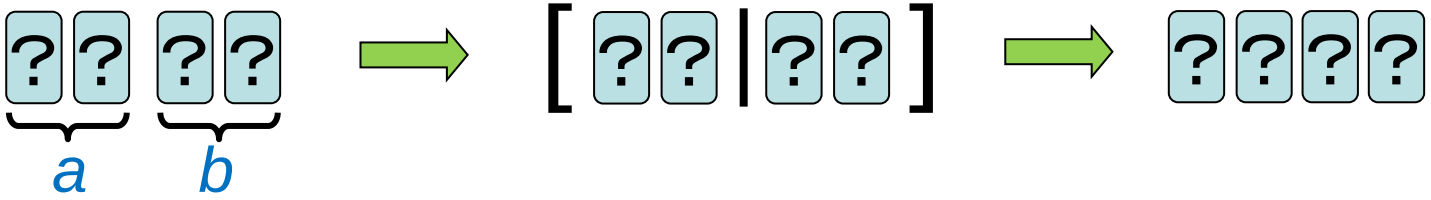


[MKS12] Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone. The five-card trick can be done with four cards. Advances in Cryptology—ASIACRYPT 2012, volume 7658 of LNCS, pages 598–606, Berlin, Heidelberg, 2012. Springer

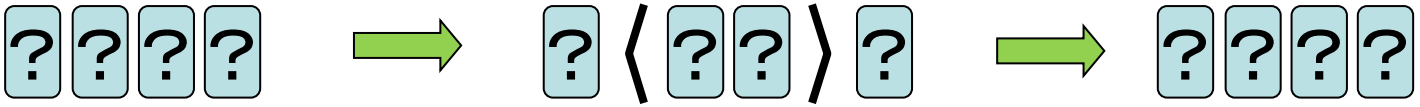
Mizuki-Kumamoto-Sone AND プロトコル[MKS12]



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：

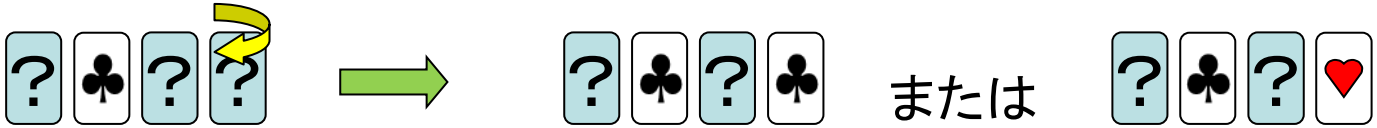


2. 中央の二枚に普通のシャッフルを適用する：

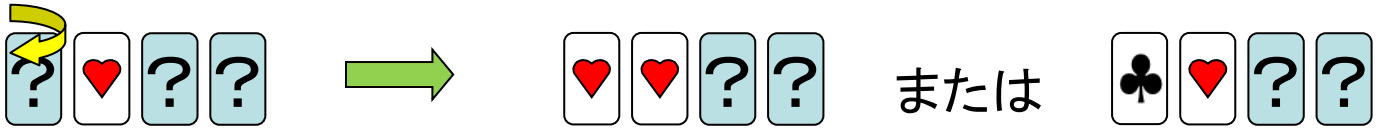


3. 2枚目をめくり，(1) 黒なら4枚目，(2) 赤なら1枚目をめくる：

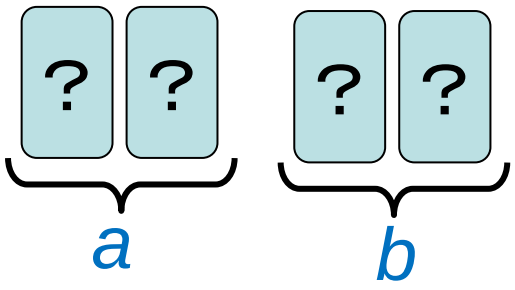
(1)



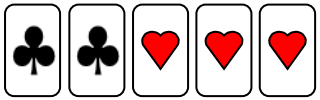
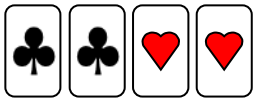
(2)



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

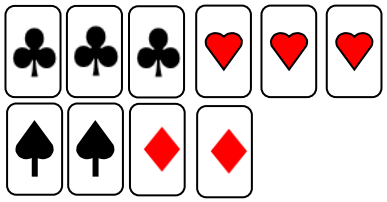
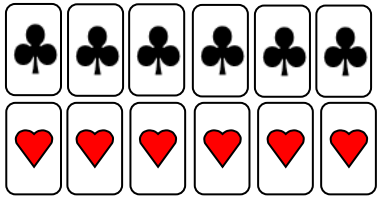
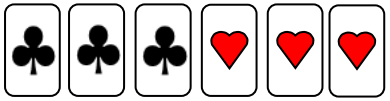
これらは1つのシャッフルに結合できる:
(shuf, {id, (1 3)(2 4),(2 3),(1 3 4 2)})

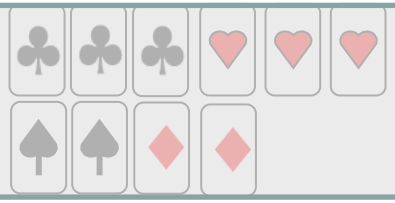
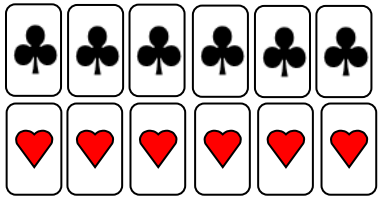
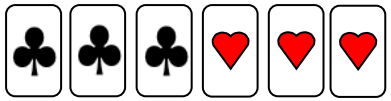
しかし、この置換の集合は閉じていない（部分群になっていない）

【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？

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.

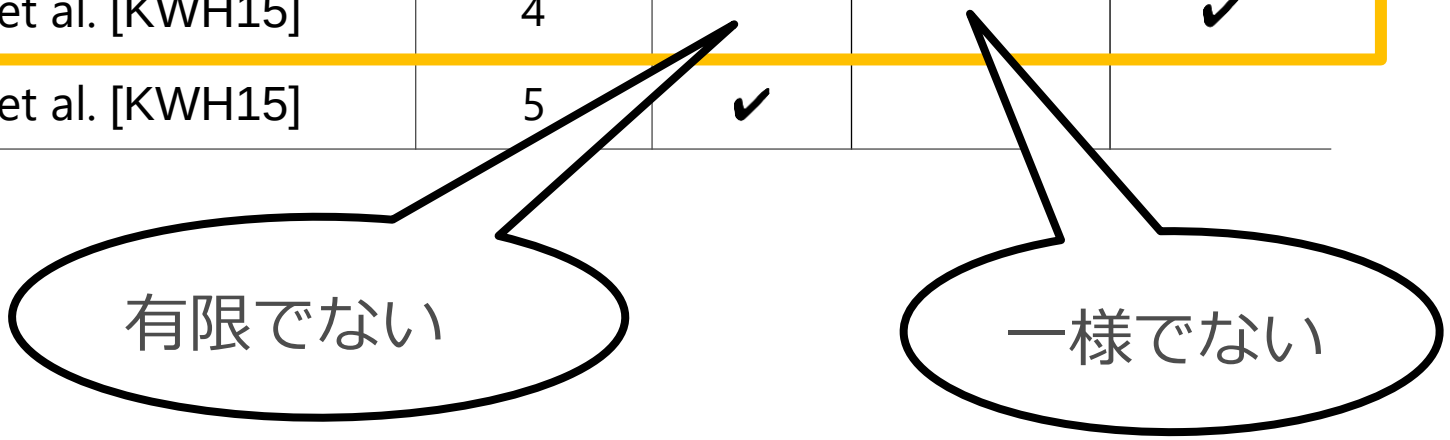
Protocols	# of cards	shuffle		
		finite	uniform	closed
Niem-Renvall [NR98]	12		✔	✔
Stiglic [Sti01]	8		✔	✔
Mizuki-Sone [MS09]	6	✔	✔	✔

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	✔		

閉じていない

(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	✔	✔	

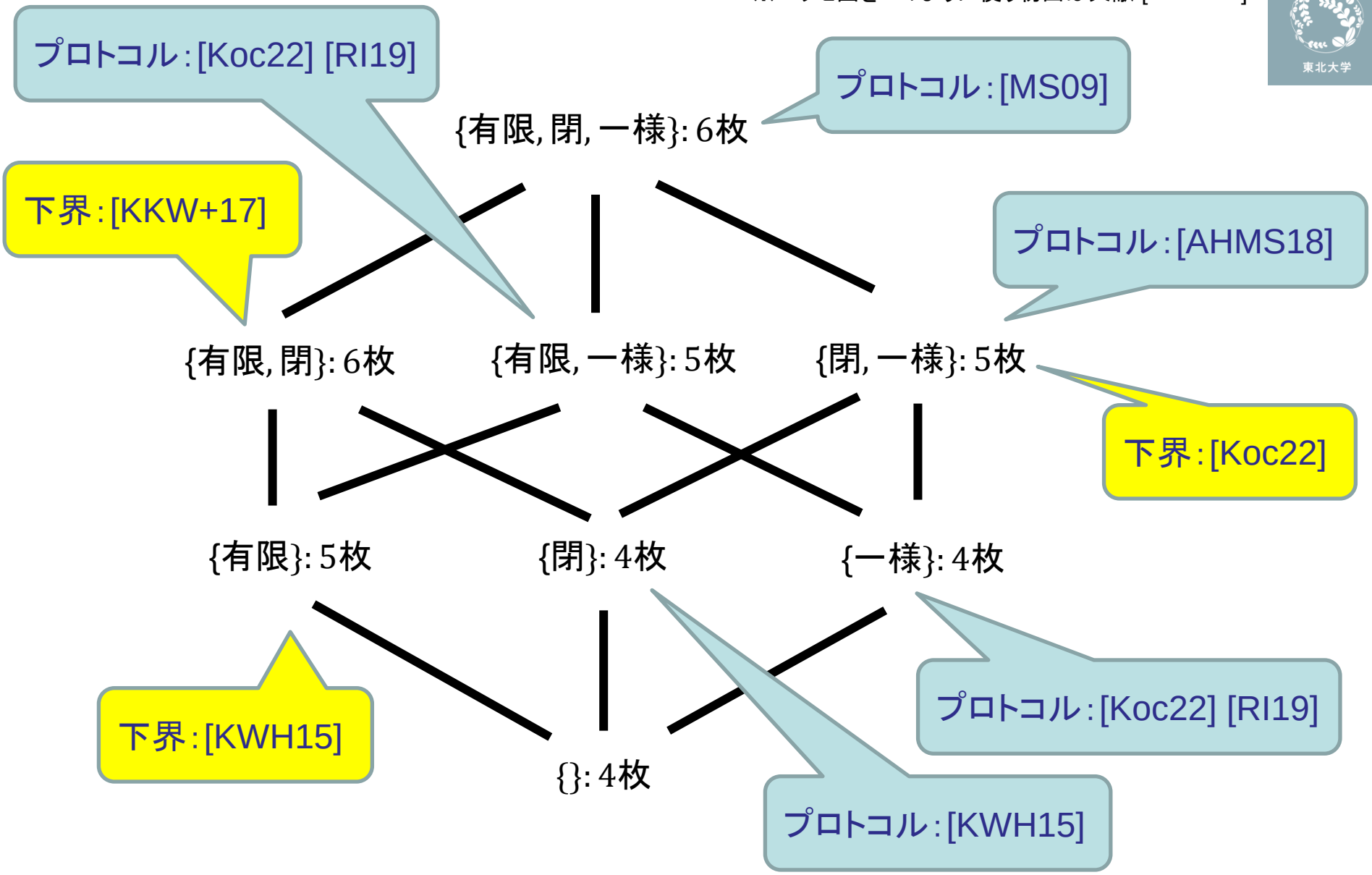
Koch et al., [KWH15]のをベースに，uniformへ

[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		✔	✔

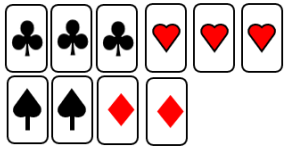
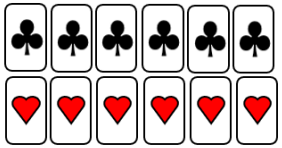
ランダムカットとランダム二等分割カットを計7回（期待値）使う

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.

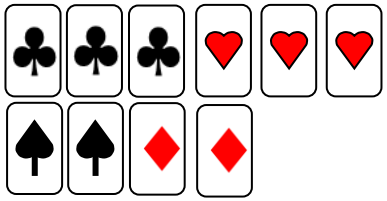
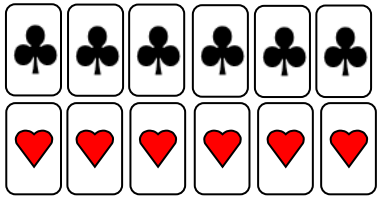
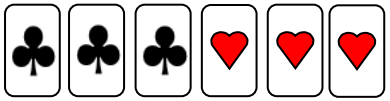
シャッフルをランダムカットのみに限定すると、

	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.

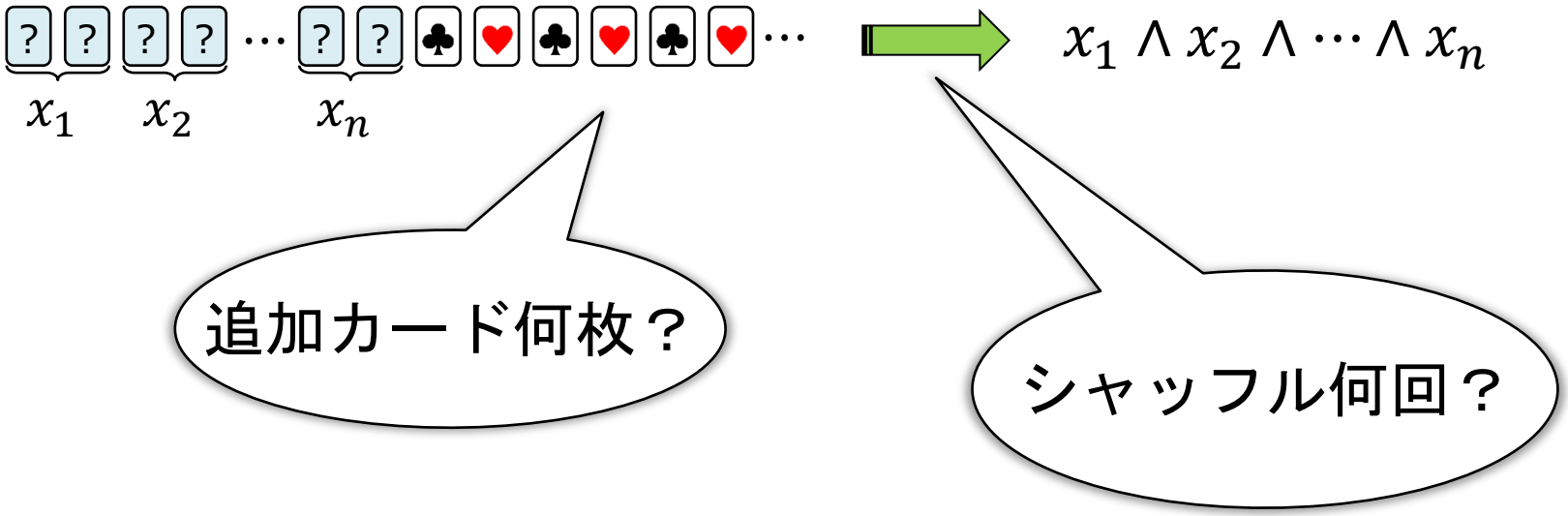
	枚数等	ランダムカット	シャッフル回数
Crépeau-Kilian [CR94]	10 	✔	8 有限でない
Niemi-Renvall [NR98]	12 	✔	7.5 有限でない
Stiglic [Sti01]	8 	✔	2 有限
Abe et. al [AMS21]	6 	✔	2 有限

すべてランダムカットしか使わない

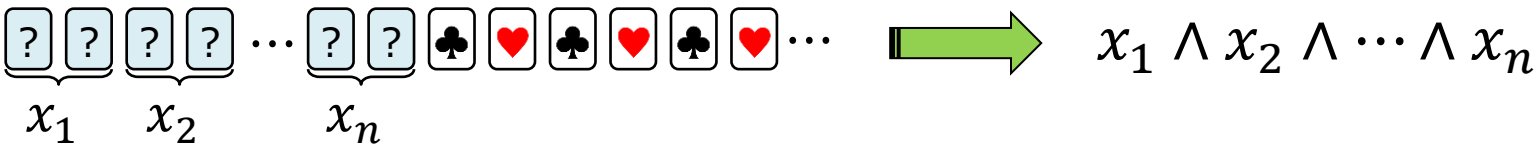
【未解決問題】
シャッフルはランダムカットしか使えないという条件のもと、5枚コミット型ANDプロトコルは構成できるか？（有限ではない）

目次

多入力ANDプロトコル



多入力ANDプロトコル

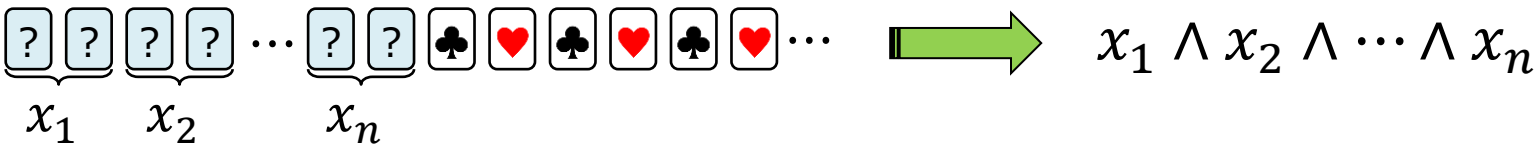


2016年に与えられた上界[Miz16]:

- 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



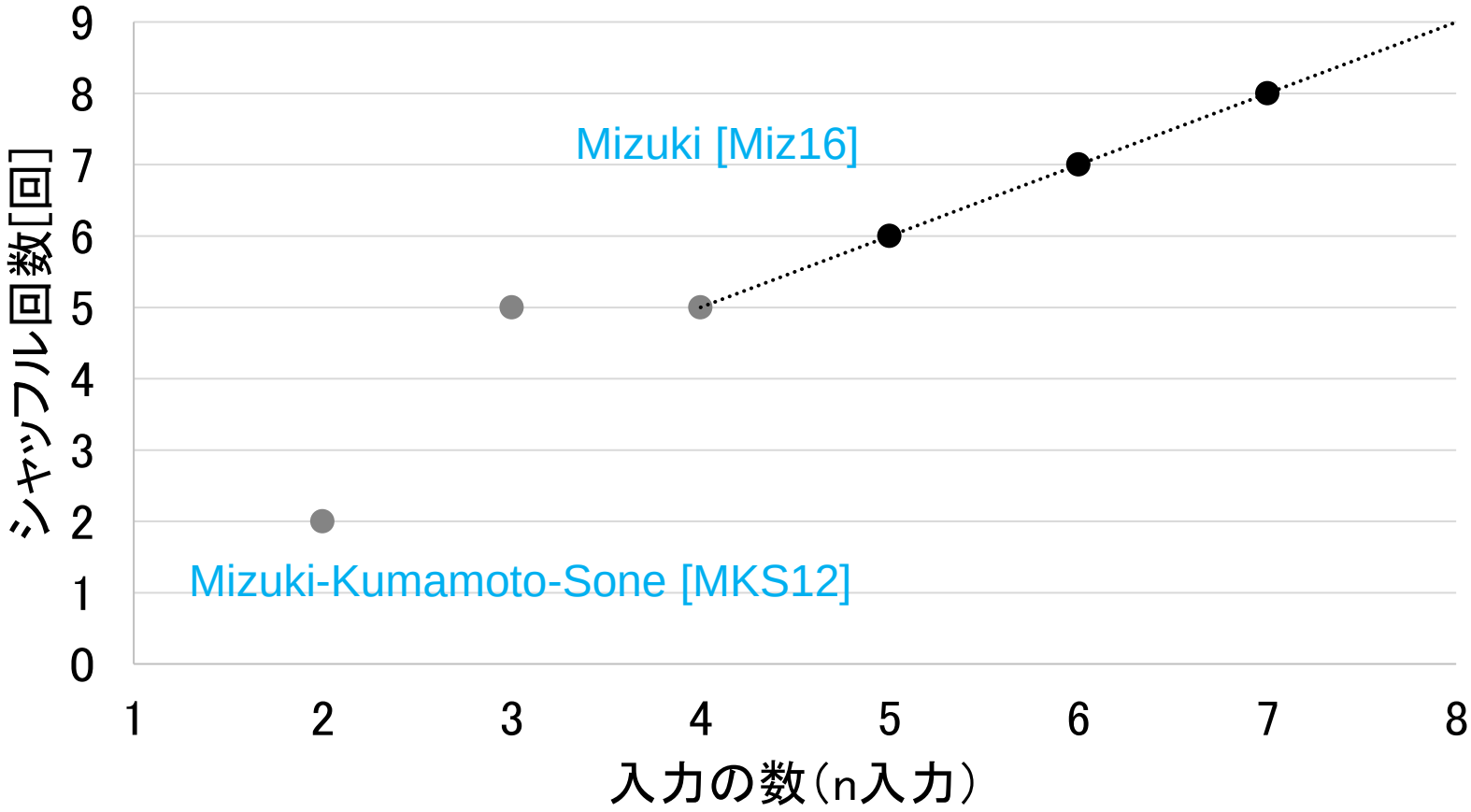
2016年に与えられた上界[Miz16]:

- 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）

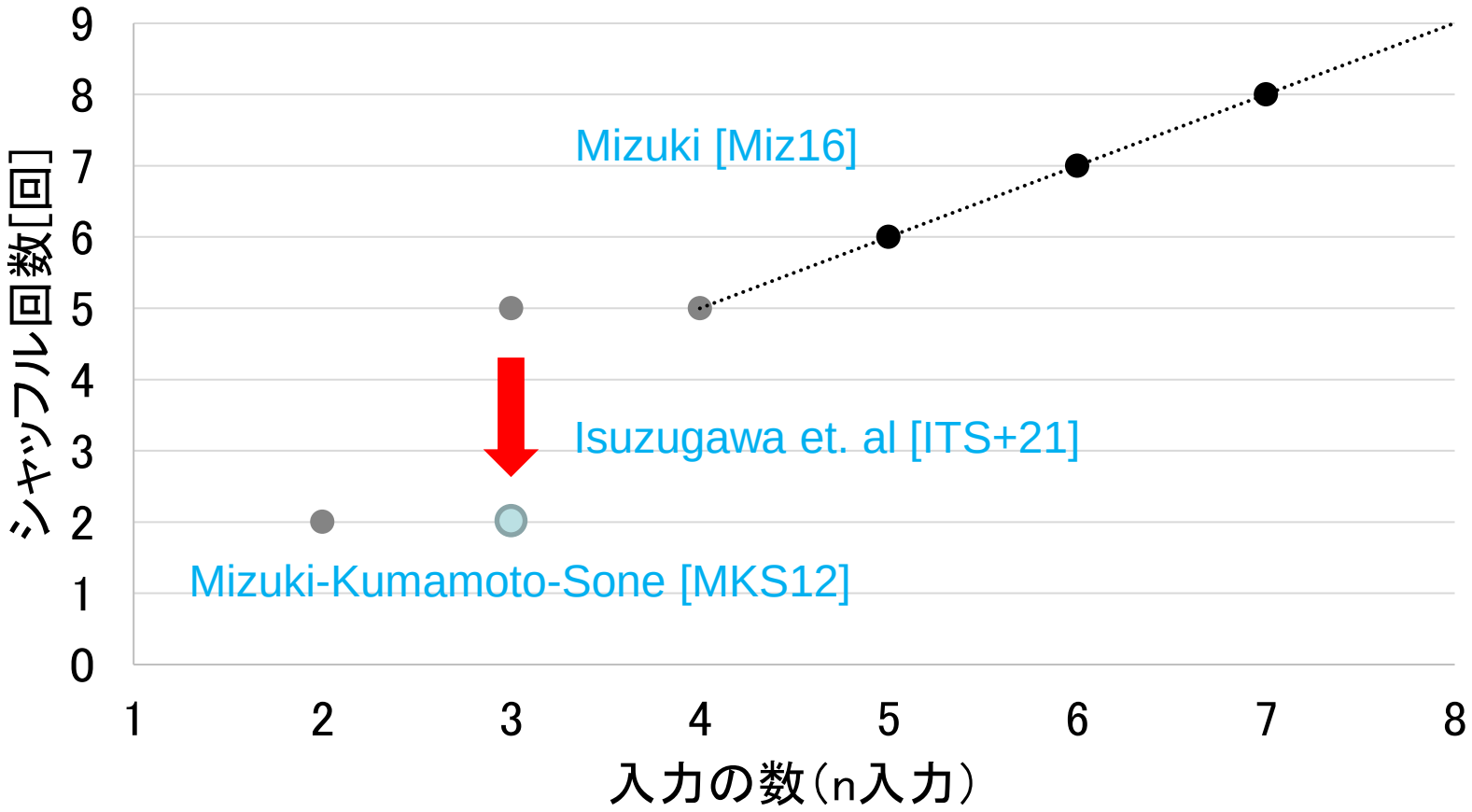
[Miz16] Takaaki Mizuki. Card-based protocols for securely computing the conjunction of multiple variables. Theor. Comput. Sci., 622(C):34–44, 2016.

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）

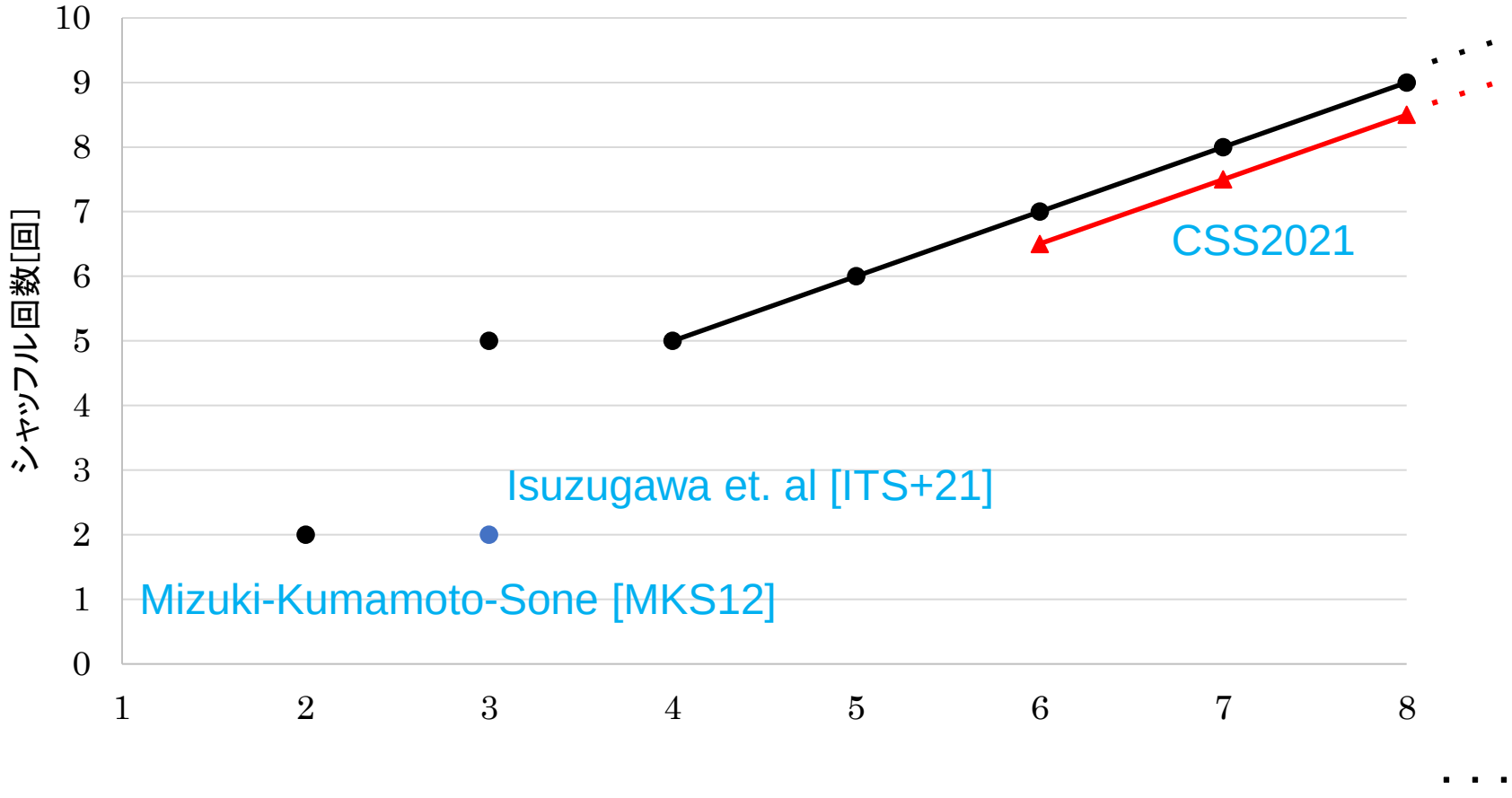


追加カードなしの2回シャッフルの3入力AND [ITS+21]：



[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。

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)})

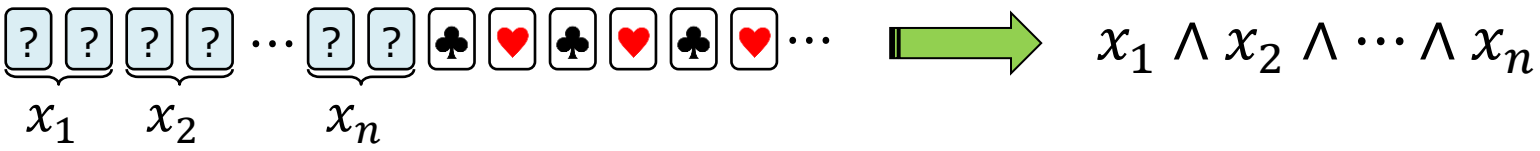
どちらも一様で
閉じている

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]:

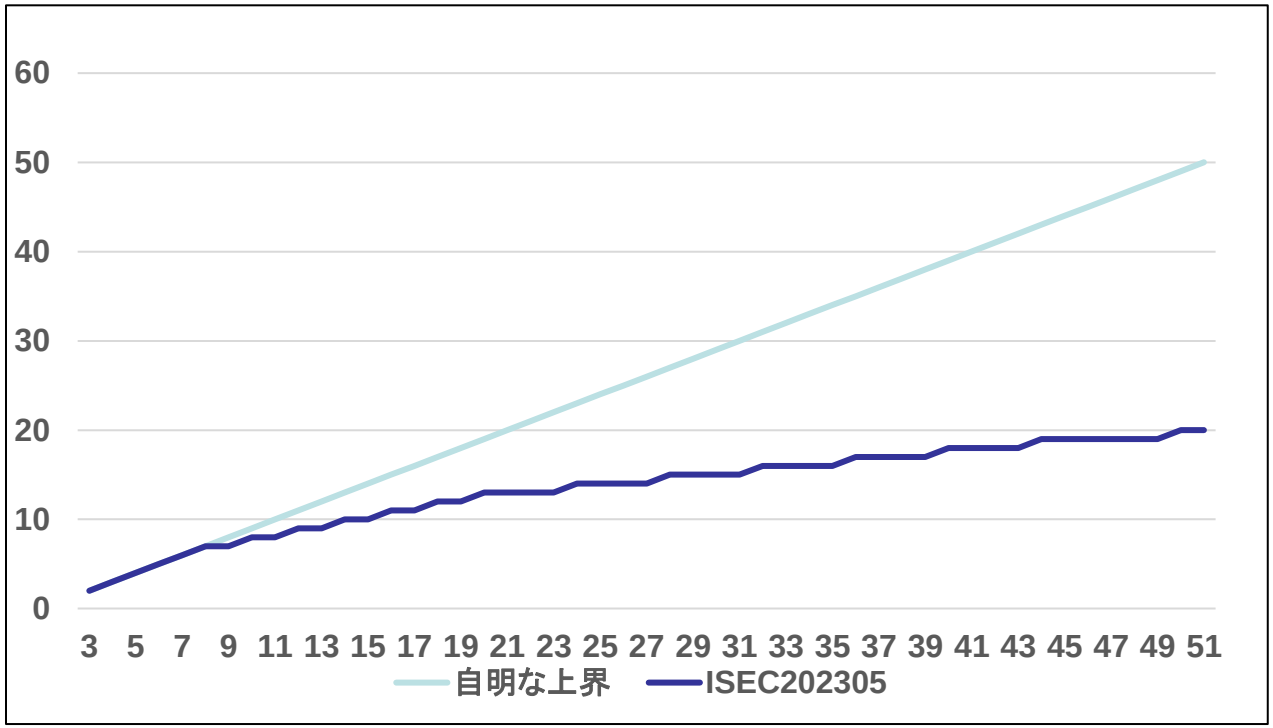
- 追加カード2枚 → シャッフル $n-1$ 回（コミット型）
- 追加カード1枚 → シャッフル $n-1$ 回（非コミット型）
- 追加カードなし →
  - $n=3$ のとき、シャッフル 5 回（非コミット型）
  - $n \geq 4$ のとき、シャッフル $n+1$ 回（非コミット型）

[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]



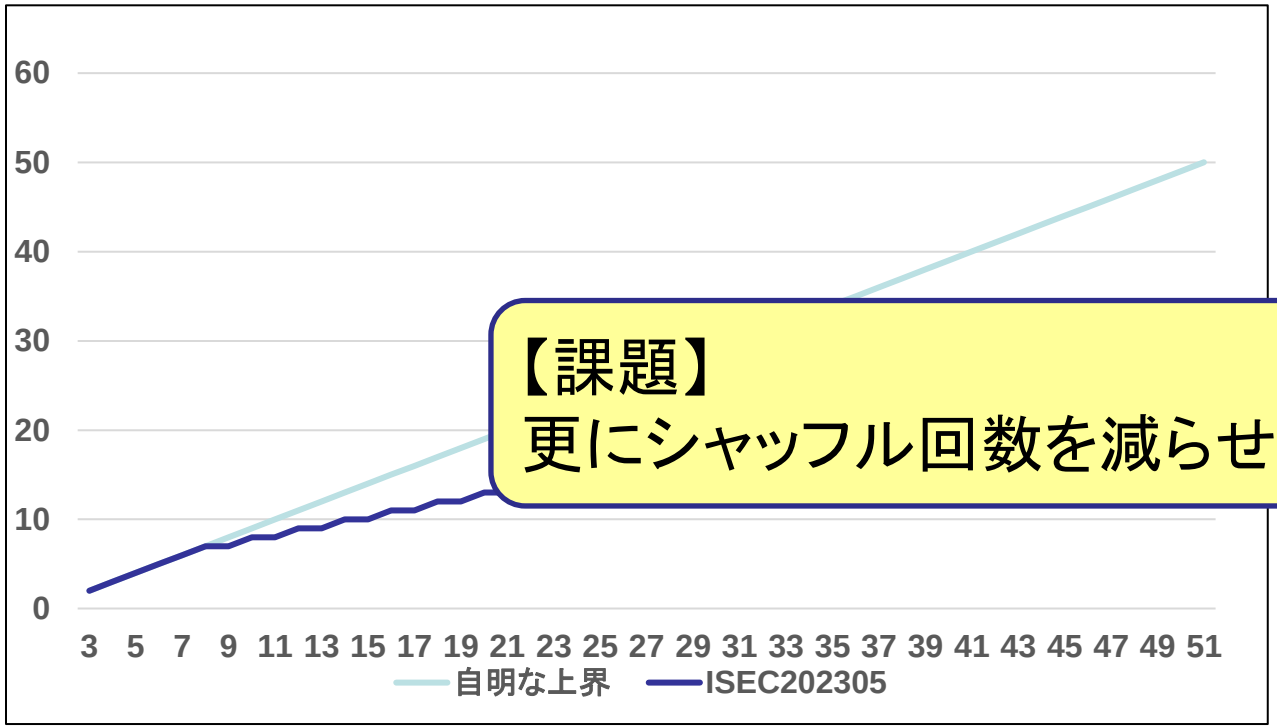
[SN21] Kazumasa Shinagawa and Koji Nuida. A single shuffle is enough for secure card-based computation of any Boolean circuit. Discrete Applied Mathematics, 289:248–261, 2021

[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

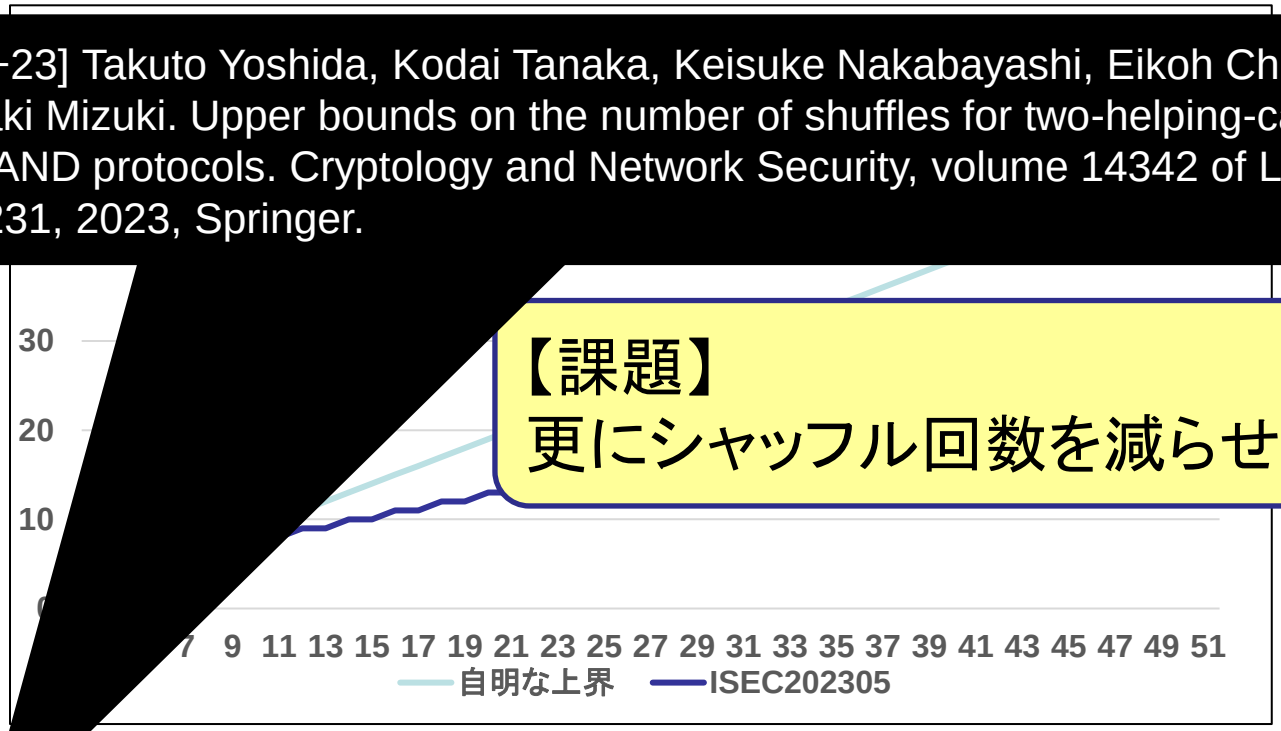
[ISEC202305] 吉田拓叶, 中林佳祐, 田中滉大, 千田栄幸, 水木敬明,``2枚の追加カードを用いた多入力AND秘密計算におけるシャッフル回数の削減,'' 電子情報通信学会信学技報, Vol.123, No.26, ISEC2023-7, pp.35-42 (May 2023).

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）

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]

[YTN+23] Takuto Yoshida, Kodai Tanaka, Keisuke Nakabayashi, Eikoh Chida, and Takaaki Mizuki. Upper bounds on the number of shuffles for two-helping-card multi-input AND protocols. Cryptology and Network Security, volume 14342 of LNCS, pages 211–231, 2023, Springer.



【課題】
更にシャッフル回数を減らせるか？

[SN21] K masa 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).

このページを追加しています

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 [IYTN+23]

【追記】
SCIS 2024において石崎と品川は、一般化パイルスクランブルシャッフルやブランチング技術を導入することで、シャッフル回数を減らせることを示している [SCIS2024]

[SCIS2024]石崎悠斗, 品川和雅,``追加カード 2 枚の多入力 AND 計算におけるシャッフル回数の新しい削減方法,'' SCIS2024 暗号と情報セキュリティシンポジウム, 3D1-1 (January 2024).

[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
[YTN+23] Takuto Yoshida, Kodai Tanaka, Keisuke Nakabayashi, Eikoh Chida, and Takaaki Mizuki. Upper bounds on the number of shuffles for two-helping-card multi-input AND protocols. Cryptology and Network Security, volume 14342 of LNCS, pages 211–231, 2023, Springer.

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？

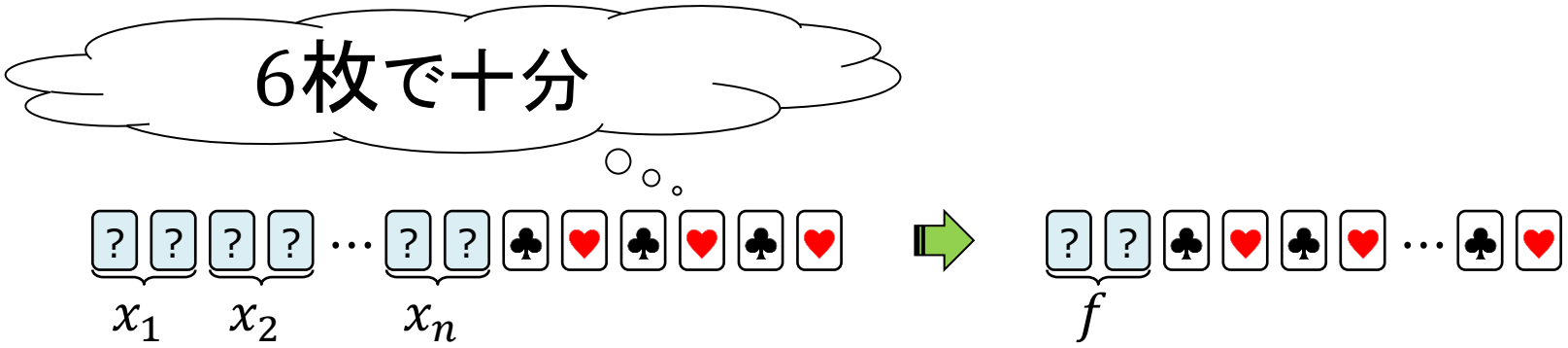
Shinagawa-Nuida [SN21] のカードベースのガーブルドサーキットの考えを応用すると、追加カード$2n-2$枚でシャッフル1回のn入力コミット型ANDプロトコルを構成できる [KTMM22]（ただし、このときのシャッフルは閉じていない）。

【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

昨年度のスライドここまで

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）

カードベース暗号の研究分野の俯瞰

カードベース暗号の計算モデル

プロトコル

抽象機械

$P = (D, U, Q, A)$

疑似コード

1 input …
2 perm …
⋮

自然言語

step1. 入力
step2. 並べ替え
⋮

計算モデルのリファイン

道具・操作を計算モデルに適用させる

計算限界の解明

カード枚数やシャッフル回数の下界の発見

・プロトコルの開発（=上界の発見）

現実世界

人間
カード組
操作

教育応用

・情報科学への興味の喚起
・暗号・セキュリティ教育
- パズルのゼロ知識証明
・抽象化の理解

実利用のプロトコルとして展開

ex.）・気まずくならない告白
・みんなで食事会を開くか決める
・金持ち比べ

（→socialな身近な問題への解決）

2023年以降に出版された論文（Scopusより）

著者名	タイトル	出版年	出版物名	会議名
Ruangwises S.	Verifying the first nonzero term: physical ZKPs for ABC End View, Goishi Hiroi, a	2024	Journal of Combinatorial Optimi	
Ono T., Shinagawa K., Nakai T., W	Single-Shuffle Card-Based Protocols with Six Cards per Gate	2024	LNCS	ICISC 2023
Hatsugai K., Asano K., Abe Y.	A Physical Zero-Knowledge Proof for Sumplete, a Puzzle Generated by ChatGPT	2024	LNCS	COCOON 2023
Robert L., Miyahara D., Lafourcad	Physical ZKP protocols for Nurimisaki and Kurodoko	2023	Theoretical Computer Science	
Shikata H., Miyahara D., Mizuki T.	Few-helping-card Protocols for Some Wider Class of Symmetric Boolean Functio	2023	Proceedir	APKC 2023
Ruangwises S.	An improved physical ZKP for nonogram and nonogram color	2023	Journal of Combinatorial Optimi	
Shinagawa K., Miyamoto K.	Automorphism Shuffles for Graphs and Hypergraphs and Its Applications	2023	IEICE Transactions on Fundame	
Abe Y., Nakai T., Watanabe Y., Iwa	A Computationally Efficient Card-Based Majority Voting Protocol with Fewer Car	2023	IEICE Transactions on Fundame	
Suga Y.	Relationship between AND extension and XOR extension of 3-valued input with 2	2023	2023 IEEE	ICCE-Asia 2023
Ruangwises S.	The Landscape of Computing Symmetric n-Variable Functions with 2n Cards	2023	LNCS	ICTAC 2023
Yoshida T., Tanaka K., Nakabayas	Upper Bounds on the Number of Shuffles for Two-Helping-Card Multi-input and I	2023	LNCS	CANS 2023
Manabe Y., Shinagawa K.	Free-XOR in Card-Based Garbled Circuits	2023	LNCS	CANS 2023
Suga Y.	A classification for commutative three-element semigroups with local XOR struct	2023	2023 Inter	ICCE-Taiwan 2023
Tanaka K., Mizuki T.	Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku	2023	LNCS	FCT 2023
Suga Y.	POSTER: A Card-Based Protocol that Lets You Know How Close Two Parties are	2023	LNCS	ACNS 2023
Ruangwises S.	Physical Zero-Knowledge Proofs for Five Cells	2023	LNCS	LATINCRYPT 2023
Tozawa K., Morita H., Mizuki T.	Single-Shuffle Card-Based Protocol with Eight Cards per Gate	2023	LNCS	UCNC 2023
Hand S., Koch A., Lafourcade P., M	Check Alternating Patterns: A Physical Zero-Knowledge Proof for Moon-or-Sun	2023	LNCS	IWSEC 2023
Nuida K.	Efficient Card-Based Millionaires' Protocols via Non-binary Input Encoding	2023	LNCS	IWSEC 2023
Ruangwises S.	Physically Verifying the First Nonzero Term in a Sequence: Physical ZKPs for AB	2023	LNCS	IJTCS-FAW 2023
Suga Y.	Security Considerations for the Fourth Data Over Non-Committed 3-Valued Card	2023	2023 Inter	ITC-CSCC 2023
Guillen L.	The Asymmetric five-card trick: working with variable encoding in card-based pr	2023	Journal of Cryptographic Engine	
Shimano M., Sakiyama K., Miyaha	Towards Verifying Physical Assumption in Card-Based Cryptography	2023	LNCS	SECITC 2022
Komano Y., Mizuki T.	Card-Based Zero-Knowledge Proof Protocol for Pancake Sorting	2023	LNCS	SECITC 2022
Ruangwises S.	Physical Zero-Knowledge Proof for Ball Sort Puzzle	2023	LNCS	CiE 2023

スペースの都合で切れている箇所があり申し訳ありません。機械的に抽出しているため漏れがあるかもしれません。

国際会議発表から今日のご講演

Tomoki Ono, Kazumasa Shinagawa, Takeshi Nakai, Yohei Watanabe, Mitsugu Iwamoto, Single-Shuffle Card-Based Protocols with Six Cards per Gate. ICISC 2023

Kyosuke Hatsugai, Kyoichi Asano, Yoshiki Abe, Physical Zero-Knowledge Proof for Sumplete, a Puzzle Generated by ChatGPT. COCOON 2023

Yoshihiro Takahashi, Kazumasa Shinagawa, Hayato Shikata and Takaaki Mizuki, Efficient Card-Based Protocols for Symmetric Functions Using Four-Colored Decks, APKC 2024

Yuki Ito, Hayato Shikata, Takuo Suganuma and Takaaki Mizuki, Card-Based Cryptography Meets 3D Printer, UCNC 2024

10:40-11:20
小野 知樹(電気通信大学)
ゲートあたり6枚で実行できるカードベースガーブルド回路

11:20-12:00
高橋 由紘(茨城大学)
多色カードを用いた効率的な対称関数プロトコル

14:10-14:50
初貝 恭祐(電気通信大学)
Sumpleteに対する物理的ゼロ知識証明

15:45-16:25
伊藤 優樹(東北大学)
3Dプリンタのカードベース暗号への応用

おまけ（２つ宣伝）

真に高機能暗号の社会展開に資する物理・視覚暗号

科学研究費　基盤研究(A)　23H00479

研究代表者
花岡 悟一郎

研究分担者
品川 和雅、宮原 大輝、矢内 直人、
Attrapadung Nuttapong、渡邉 洋平、岩本 貢、
松田 隆宏、水木 敬明、宮本賢伍、山下 恭佑

真に高機能暗号の社会展開に資する物理・視覚暗号

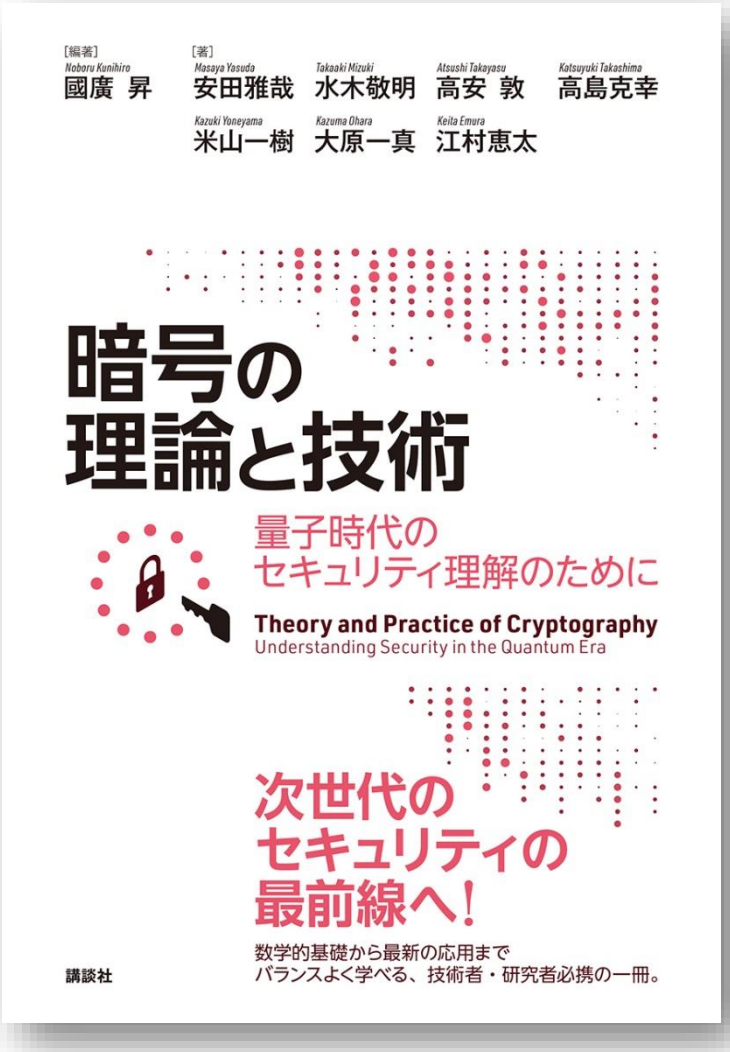
科学研究費　基盤研究(A)　23H00479

高機能暗号は安全なデータ利活用を可能とする技術として極めて有効であるが、機能や安全性の概念が複雑であり、潜在的な**利用者企業**が必ずしも十分に理解が出来ず社会展開があまり進んでいない。本研究では、高機能暗号の事業展開を検討している企業と連携し、高機能暗号技術について、潜在的利用者に対する機能や安全性の平易な説明を可能とする**物理・視覚暗号**の設計および実装を行う。

暗号の理論と技術
量子時代のセキュリティ理解のために

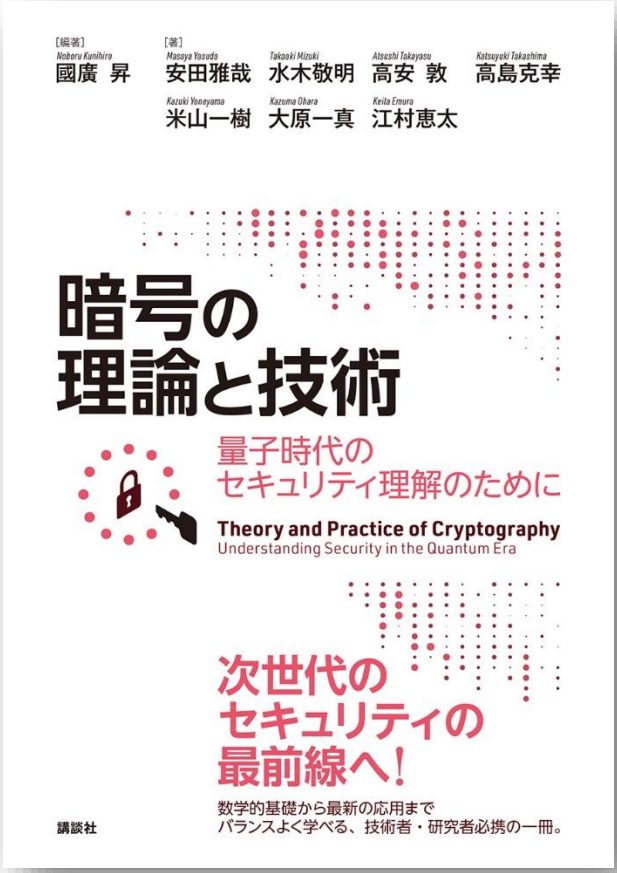
国廣昇・編著
安田雅哉／水木敬明／高安敦／
高島克幸／米山一樹／大原一真
／江村恵太・著

発行：2024/05/22
ISBN：978-4-06-53563



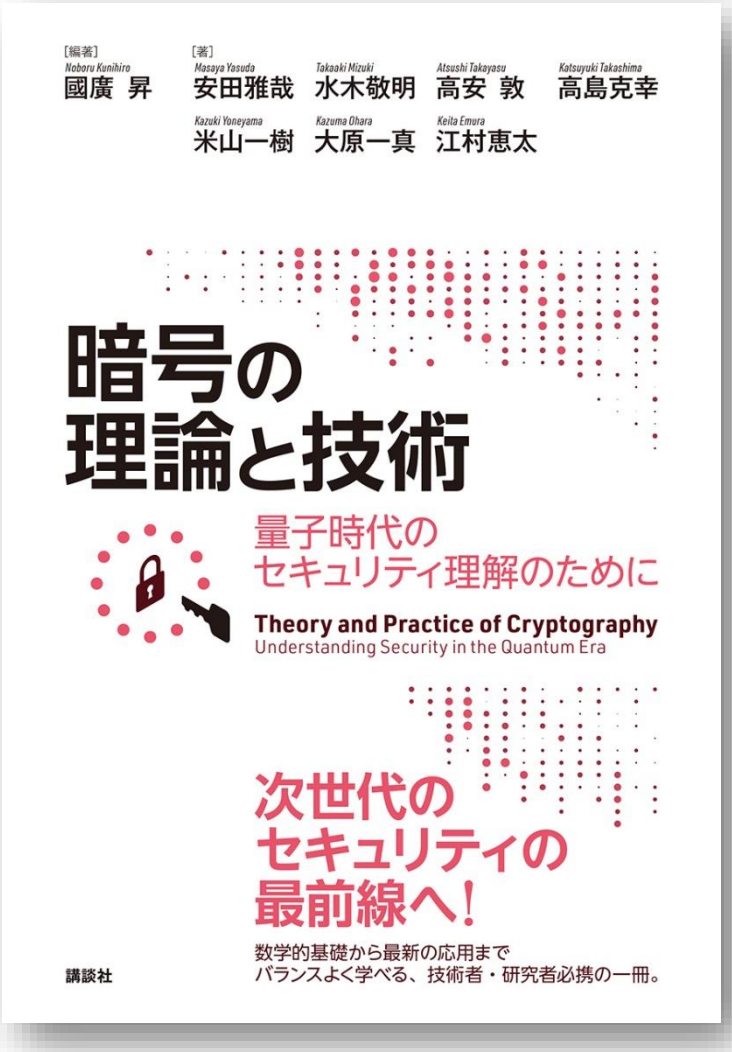
暗号の理論と技術
量子時代のセキュリティ理解のために

1章 暗号技術の基礎
2章 現代の暗号技術を支える数学
3章 カードベース暗号
4章 格子理論を用いた暗号攻撃
5章 量子計算基礎とその暗号への応用
6章 耐量子計算機暗号
7章 形式手法による安全性検証
8章 秘密計算
9章 証明可能安全性と高機能暗号



暗号の理論と技術
量子時代のセキュリティ理解のために

3章 カードベース暗号
- 3.1 カード組を用いた秘密計算
- 3.2 コミット型プロトコル
- 3.3 金持ち比べプロトコル
- 3.4 ゼロ知識証明プロトコル



10:00-12:00 オープニング・セッション1

10:00-10:10
須賀 祐治(株式会社インターネットイニシアティブ)
オープニング

10:10-10:40
水木 敬明(東北大学)
昨年の研究集会からのアップデート

10:40-11:20
小野 知樹(電気通信大学)
ゲートあたり6枚で実行できるカードベースガーブルド回路

11:20-12:00
高橋 由紘(茨城大学)
多色カードを用いた効率的な対称関数プロトコル

13:30-15:30 セッション2

13:30-14:10
安部 芳紀(電気通信大学 <現：セコム株式会社 IS研究所>)
数独に対する物理的ゼロ知識証明

14:10-14:50
初貝 恭祐(電気通信大学)
Sumpleteに対する物理的ゼロ知識証明

14:50-15:30
宮原大輝(電気通信大学)
月か太陽に対する物理的ゼロ知識証明

15:45-17:45 セッション3・クロージング

15:45-16:25
伊藤 優樹(東北大学)
3Dプリンタのカードベース暗号への応用

16:25-17:05
品川 和雅(茨城大学)
一様巡回群分解に基づく一様閉シャッフルの実現方法とその応用

17:05-17:35
須賀 祐治(株式会社インターネットイニシアティブ)
正則グラフでアクセス構造を表現する非コミットメント型カードプロトコル

17:35-17:45
須賀 祐治(株式会社インターネットイニシアティブ)
クロージング