Vol.2021-CSEC-95 No.8
Vol.2021-SPT-45 No.8
Vol.2021-EIP-94 No.8
2021/11/8

# ランダム二等分割カットのみを用いる5枚コミット型ANDプロトコル

豊田　航大[1,a)]　宮原　大輝[2,3]　水木　敬明[1,3]

**概要**：物理的なカード組を用いて秘密計算等を実現する手法をカードベース暗号と呼ぶ．カードベース暗号において，人間の手で実行可能なシャッフル操作としてランダムカットとランダム二等分割カットが知られている．近年シャッフル操作をこれらに限定したプロトコルの研究が進んでおり，コミット型 AND プロトコルに関しては，これらの 2 種類のシャッフルを両方用いた場合，5 枚で実現でき，その枚数は最適である（APKC 2018）．また，シャッフルをランダムカットのみに限定した場合は，6 枚のカードで構成されている（Natural Computing, 2021）．一方，ランダム二等分割カットのみを用いるコミット型 AND プロトコルは 2009 年に Mizuki と Sone によって 6 枚のカードを用いるプロトコルが初めて提案されて以来，このカード枚数を 5 枚に減らすことができるかどうかは未解決であった．そこで本稿ではこの問題を解決し，シャッフル操作としてランダム二等分割カットのみを用いるプロトコルを 5 枚のカードで構成する．このプロトコルは，必要なカード枚数が最小という意味で最適である．

# Five-card Committed-format AND Protocol Using Only Random Bisection Cuts

## 1. はじめに

トランプのようなカード組を用いて秘密計算を行う手法を**カードベース暗号**という．カードベース暗号では，表面が $\boxed{\clubsuit}$ または $\boxed{\heartsuit}$ であり，裏面が $\boxed{?}$ で区別のつかない 2 種類のカードを用いる．これらのカードを用いて次のようにブール値を表す．

$$\boxed{\clubsuit}\boxed{\heartsuit} = 0,\ \boxed{\heartsuit}\boxed{\clubsuit} = 1 \qquad (1)$$

ビット $x \in \{0,1\}$ がこの符号化ルールに従って符号化され，2 枚のカードが裏返しに置かれる時，この 2 枚のカードを $x$ の**コミットメント**と呼び，次のように書く．

$$\underbrace{\boxed{?}\boxed{?}}_{x}$$

カードベース暗号では通常，コミットメントで入力を行い秘密計算を実現する．例えば，論理積の秘密計算をする場合には，2 つの入力ビット $a, b \in \{0,1\}$ のコミットメント

$$\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}$$

を入力とする．コミットメントで出力をするプロトコルを**コミット型プロトコル**と呼び，そうでないプロトコルを**非コミット型プロトコル**と呼ぶ．

カードベース暗号において，人間の手で実行可能なシャッフル操作としてランダムカット（2.2 節）とランダム二等分割カット（2.3 節）が知られている．近年シャッフル操作をこれらに限定したプロトコルの研究が進んでおり，本稿では論理積を計算するプロトコルであるコミット型 AND プロトコルを取り扱う．

### 1.1 既存研究

既存のランダムカットまたはランダム二等分割カットのみを用いるプロトコルを表 1 に示す．コミット型 AND プロトコルは 1993 年に Crépeau–Kilian によって初めて提案され，必要となるカードは 4 色 10 枚であった [4]．それ

[1] 東北大学
Tohoku University
[2] 電気通信大学
The University of Electro-Communications
[3] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)
[a)] kodai.toyoda.p1@dc.tohoku.ac.jp

Vol.2021-CSEC-95 No.8
Vol.2021-SPT-45 No.8
Vol.2021-EIP-94 No.8
2021/11/8

**表 1** 既存のランダムカットまたはランダム二等分割カットのみを用いるコミット型 AND プロトコル

| | カード色数 | カード枚数 | シャッフル回数 | 使用するシャッフル | 有限 |
|---|---|---|---|---|---|
| Crépeau–Kilian, 1993 [4] | 4 | 10 | 8 | ランダムカット | |
| Niemi–Renvall, 1998 [10] | 2 | 12 | 7.5 | ランダムカット | |
| Stiglic, 2001 [11] | 2 | 8 | 2 | ランダムカット | |
| Mizuki–Sone, 2009 [9] | 2 | 6 | 1 | ランダム二等分割カット | ✓ |
| Abe et al., 2018 [1] | 2 | 5 | 7 | ランダムカット & ランダム二等分割カット | |
| Abe et al., 2021 [2] | 2 | 5 | 4.5 | ランダムカット & ランダム二等分割カット | |
| Abe et al., 2021 [3] | 2 | 6 | 2 | ランダムカット | ✓ |
| **本稿（3 節）** | **2** | **5** | **7** | **ランダム二等分割カット** | |

以降プロトコルの改良が進められており，1998 年 Niemi–Renvall によって 2 色 12 枚へとカードの色数を改良したプロトコルが提案され [10]，2001 年には Stiglic によって必要カード枚数が 8 枚に削減された [11]．これらのプロトコルはいずれもシャッフル操作としてランダムカットのみを使用していたが，2009 年に Mizuki–Sone によってランダム二等分割カットが考案され，カード枚数 6 枚のプロトコルが提案された [9]．このプロトコルのシャッフル回数は有限 1 回であり，シャッフル回数の面で最適である．2018 年にはランダムカットとランダム二等分割カットを両方用いたカード枚数 5 枚のプロトコルが Abe らによって提案され，これはカード枚数の面で最適なプロトコルとなっている [1]．また，Abe らは後にこのプロトコルのシャッフル回数を平均 7 回から平均 4.5 回に削減したプロトコルを提案している [2]．Abe らはさらに，2021 年にランダムカットのみを用いたプロトコルをカード枚数 6 枚で構成し，シャッフル回数についても有限 2 回と改良した [3]．

### 1.2 貢献

本稿ではランダム二等分割カットのみを用いるコミット型 AND プロトコルを 5 枚のカードで構成する．

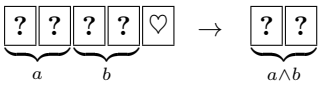



表 1 の通り, 既存のランダム二等分割カットのみを用いるコミット型 AND プロトコルに必要なカード枚数は Mizuki–Sone が提案したプロトコルの 6 枚が最小であったため，カード枚数を 1 枚削減することに成功したと言える．さらに，ランダムカットおよびランダム二等分割カットのみを用いたコミット型 AND プロトコルは 4 枚のカードで構成することができないことが 2017 年に Kastner らによって証明されている [5]．したがって，提案プロトコルはカード枚数の面で最適である．この提案プロトコルのシャッフル回数は平均 7 回である．

### 1.3 本稿の構成

本稿の構成は次の通りである．1 節ではランダムカットとランダム二等分割カットのみを用いたコミット型 AND プロトコルの既存研究について述べ，本稿の貢献について述べた．2 節ではカードベース暗号で用いられる操作について説明し，既存のランダム二等分割カットのみを用いたコミット型 AND プロトコルを紹介する．3 節で提案プロトコルについて説明し，4 節で結論を述べる．

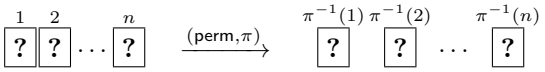
## 2. 準備

本節では，まずカードベース暗号の計算モデル [8] で用いられる操作について説明する．次にカードベース暗号における実用的なシャッフル操作である，ランダムカットとランダム二等分割カットについて説明する．さらに，既存のランダム二等分割カットのみを用いるコミット型 AND プロトコルとして，Mizuki–Sone のプロトコルを紹介する．

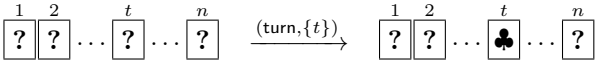
### 2.1 カードベース暗号で使用する操作

カードベース暗号では，カード列に対して主に 3 つの操作を行う．

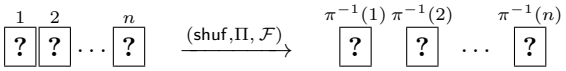
**並べ替え** カード列に対し置換 $\pi$ を適用する．




**めくる** カード列の左から $t$ 枚目のカードをめくってカードの色を確認する．



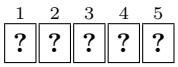

**シャッフル** カード列に対し置換集合 $\Pi$ から確率分布 $\mathcal{F}$ に従って得られる置換 $\pi$ を適用する．




ただし，$\Pi$ に含まれるどの置換が適用されたのかは誰も知り得ない．確率分布が一様である場合は，確率分布 $\mathcal{F}$ を省略する場合がある．

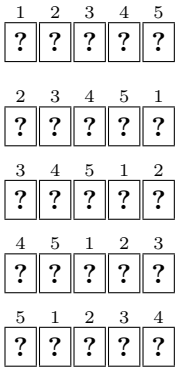
### 2.2 ランダムカット

ランダムカットとは，誰も並びが分からなくなるようにカード列を巡回的にランダムにシフトさせるシャッフル操作である．説明のために 5 枚のカード列に次のように番号を振る．



Vol.2021-CSEC-95 No.8
Vol.2021-SPT-45 No.8
Vol.2021-EIP-94 No.8
2021/11/8

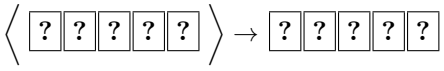
ランダムカット後のカード列は次の 5 通りのいずれかになり，生起確率はそれぞれ 1/5 である．




このランダムカットは，巡回置換 $\pi = (1\,2\,3\,4\,5)$ を用いて

$$(\mathsf{shuf}, \{\mathsf{id}, \pi, \pi^2, \pi^3, \pi^4\})$$

と書くことができる．ここで id は恒等置換である．ランダムカットは操作が簡単で，人間が安全に実行できることが実験的に確認されている [12]．ランダムカットは $\langle\cdot\rangle$ と表記する．例えば 5 枚のカードにランダムカットを適用する場合は，

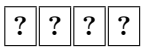


と書く．

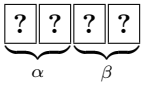
### 2.3 ランダム二等分割カット

ランダム二等分割カットは 2009 年に Mizuki–Sone [9] によって考案されたシャッフルである．以下では，4 枚のカードにランダム二等分割カットを適用する場合を例として説明する．

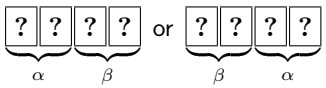
(1) 4 枚のカードを並べる．



(2) カード列を半分に分け，左半分を $\alpha$，右半分を $\beta$ とする．

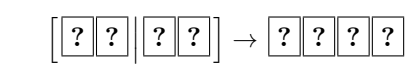



(3) $\alpha$ と $\beta$ の位置をランダムに入れ替える．




$\alpha$ と $\beta$ の位置はそのままであるか入れ替わることになり，その確率はそれぞれ 1/2 である．

以上がランダム二等分割カットの操作であり，$[\cdot|\cdot]$ と表記する．例えば 4 枚のカードにランダム二等分割カットを適用する場合は，

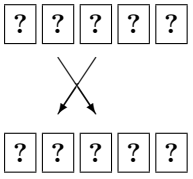


と書く．また，このランダム二等分割カットは，

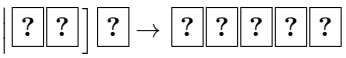
$$(\mathsf{shuf}, \{\mathsf{id}, (1\,3)(2\,4)\})$$

と書くことができる．また，$(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,4)\})$ のようなシャッフルについては，並び替えとランダム二等分割カットを組み合わせることで実現できる．以下に $(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,4)\})$ の場合を例として説明する．

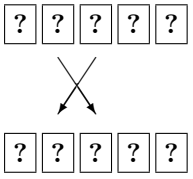
(1) 次のように並び替えを行う．



(2) 次のようにランダム二等分割カットを行う．



(3) 次のように並び替えを行う．



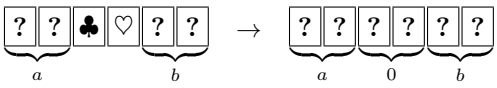
以上により，$(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,4)\})$ が適用される．

ランダム二等分割カットは身近な道具を用いて安全に実装できることが知られ [13]，カードの裏面が上下非対称の場合はランダムカットを用いて実装できる [12]．

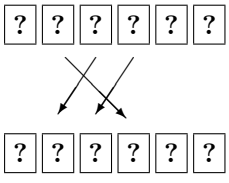
### 2.4 既存のランダム二等分割カットのみを用いるコミット型 AND プロトコル

既存のランダム二等分割カットのみを用いるコミット型 AND プロトコルとして Mizuki-Sone が提案したプロトコル [9] を紹介する．このプロトコルは，2 枚の追加カード ♣ ♡ を使用し，合計 6 枚のカードを用いる．

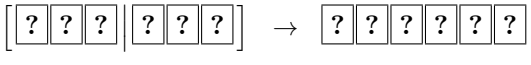
(1) 2 つの入力コミットメントの間に追加カードを置き，裏返す．




(2) 次のように並べ替えを行う．

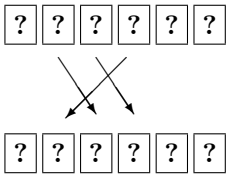


(3) 次のようにランダム二等分割カットを行う．

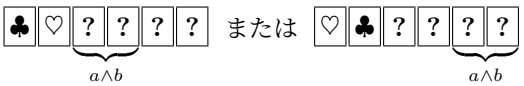


Vol.2021-CSEC-95 No.8
Vol.2021-SPT-45 No.8
Vol.2021-EIP-94 No.8
2021/11/8

(4) 次のように並べ替えを行う.

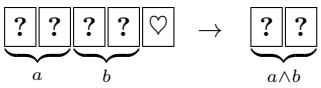


(5) 左側の 2 枚を表にし, ♣ と ♡ の並びによって $a \wedge b$ のコミットメントが得られる.




## 3. 提案プロトコル

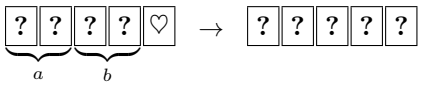
本節では, ランダム二等分割カットのみを用いるコミット型 AND プロトコルを提案する.




### 3.1 提案プロトコルの手順

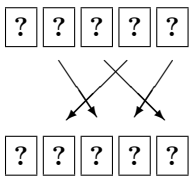
以下に提案プロトコルの手順を示す.

(1) $a, b$ の入力コミットメントと追加の ♡ のカードを並べ, 追加の ♡ を裏返す.

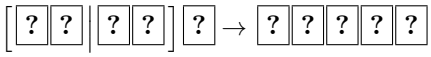



(2) $(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(4\,5)\})$ を適用する.

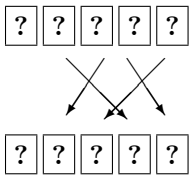
(a) 次のように並び替えを行う.



(b) 次のようにランダム二等分割カットを行う.

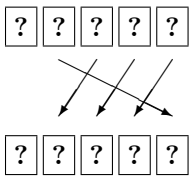


(c) 次のように並び替えを行う.



(3) $(\mathsf{shuf}, \{\mathsf{id}, (1\,4)(3\,5)\})$ を適用する.

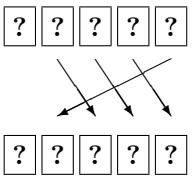
(a) 次のように並び替えを行う.



(b) 次のようにランダム二等分割カットを行う.



(c) 次のように並び替えを行う.



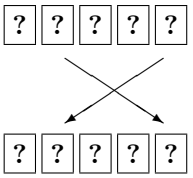
(4) 左から 2 枚目のカードをめくる.

(a) 黒のカード ♣ が出た場合, ステップ 11 に進む.

(b) 赤のカード ♡ が出た場合, ステップ 5 に進む.

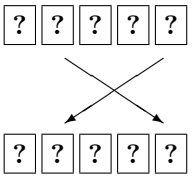
(5) $(\mathsf{shuf}, \{\mathsf{id}, (1\,5)\})$ を適用する.

(a) 次のように並び替えを行う.



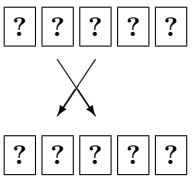
(b) 次のようにランダム二等分割カットを行う.

(c) 次のように並び替えを行う.



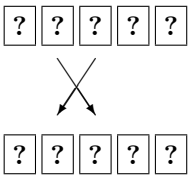
(6) $(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,4)\})$ を適用する.

(a) 次のように並び替えを行う.



(b) 次のようにランダム二等分割カットを行う.

(c) 次のように並び替えを行う.

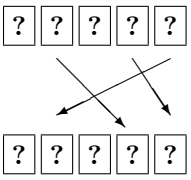


(7) 左から 5 枚目のカードをめくる.

(a) 黒のカード ♣ が出た場合, 次のように並び替え

Vol.2021-CSEC-95 No.8
Vol.2021-SPT-45 No.8
Vol.2021-EIP-94 No.8
2021/11/8

てステップ 11 に進む.



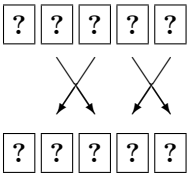
(b) 赤のカード $\boxed{\heartsuit}$ が出た場合，ステップ 8 に進む.

(8) $(\mathsf{shuf}, \{\mathsf{id}, (1\,3)(2\,4)\})$ を適用する.

$$\left[\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\right]\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

(9) $(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,5)\})$ を適用する.

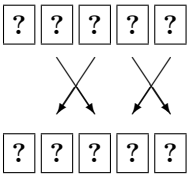
(a) 次のように並び替えを行う.



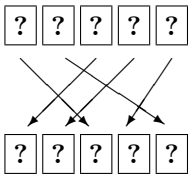
(b) 次のようにランダム二等分割カットを行う.

$$\left[\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\right]\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

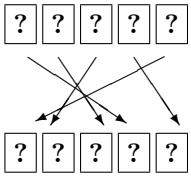
(c) 次のように並び替えを行う.



(10) 左から 4 枚目のカードをめくる．黒のカード $\boxed{\clubsuit}$ が出た場合，次のように並び替えてステップ 11 に進む.



赤のカード $\boxed{\heartsuit}$ が出た場合，次のように並び替えてステップ 8 に戻る.

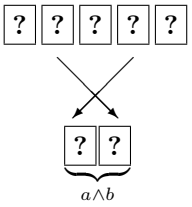


(11) $(\mathsf{shuf}, \{\mathsf{id}, (1\,3)(2\,4)\})$ を適用する.

$$\left[\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\right]\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

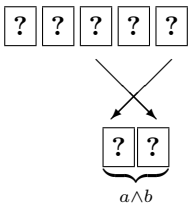
(12) 左から 1 枚目のカードをめくる.

(a) 黒のカード $\boxed{\clubsuit}$ が出た場合，次のようにして $a \wedge b$ のコミットメントが出力として得られる.



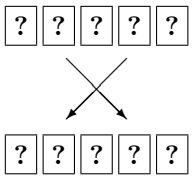

(b) 赤のカード $\boxed{\heartsuit}$ が出た場合，2 枚目のカードをめくる.

(i) 赤のカード $\boxed{\heartsuit}$ が出た場合，次のようにして $a \wedge b$ のコミットメントが出力として得られる.




(ii) 黒のカード $\boxed{\clubsuit}$ が出た場合，$(\mathsf{shuf}, \{\mathsf{id}, (1\,4)\})$ を適用してステップ 11 に戻る.

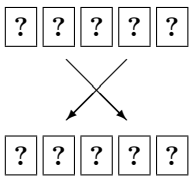
(A) 次のように並び替えを行う.



(B) 次のようにランダム二等分割カットを行う.

$$\left[\boxed{?}\middle|\boxed{?}\right]\boxed{?}\boxed{?}\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

(C) 次のように並び替えを行う.



以上が提案プロトコルの手順である.

### 3.2 正当性と安全性

提案プロトコルの正当性と安全性を KWH-tree [6] を用いて証明する．KWH-tree とは，カードの状態を表すノードとそれらを結ぶ操作を表すエッジでプロトコルを表現する図であり，各ノードの確率分布の和が $X_{11} + X_{10} + X_{01} + X_{00}$ と等しいという条件を満たしつつ KWH-tree を描くことができれば，そのプロトコルの正当性と安全性が証明されるものである．提案プロトコルは，図 1 のように KWH-tree が描ける．したがって，このプロトコルは正当かつ安全である.

Vol.2021-CSEC-95 No.8
Vol.2021-SPT-45 No.8
Vol.2021-EIP-94 No.8
2021/11/8

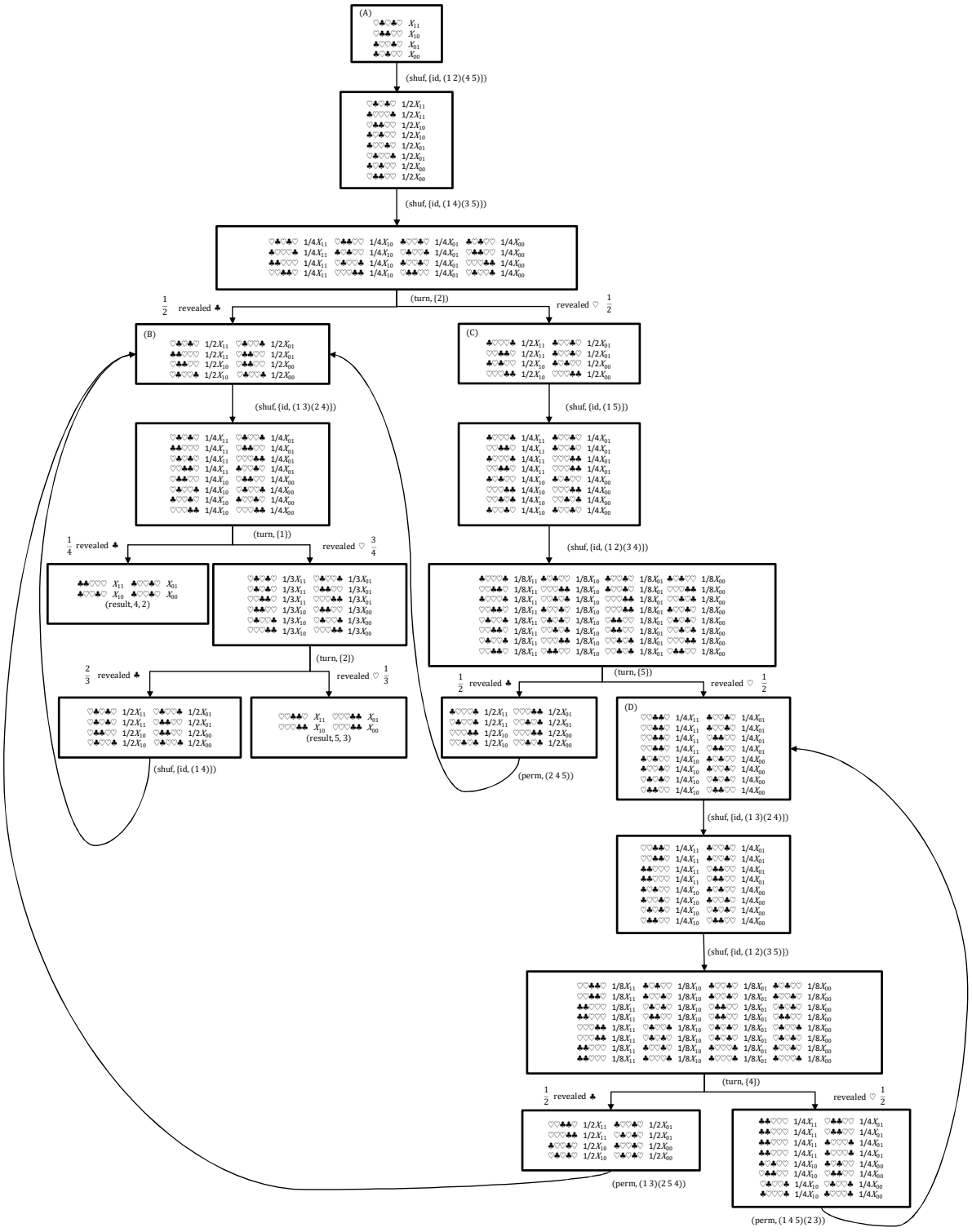



**図 1** 提案プロトコルの KWH-tree.

### 3.3 提案プロトコルのシャッフル回数

提案プロトコルのシャッフル回数について述べる．図 1 において，(A) から (B) または (C) に進むまでのシャッフル回数を $S_A$，(B) からプロトコル終了までのシャッフル回数を $S_B$，(C) から (B) または (D) に進むまでのシャッフル回数を $S_C$，(D) から (B) に進むまでのシャッフル回数を $S_D$ とする．このとき，プロトコル全体のシャッフル回数の期待値は (2) 式のようになる．

$$S_A + \frac{1}{2}S_B + \frac{1}{2}\left(S_C + \frac{1}{2}S_B + \frac{1}{2}(S_D + S_B)\right) \quad (2)$$

$S_A$ について考えると，図 1 の通り，(A) からスタートして最初にシャッフルを 2 回行っているため $S_A = 2$ である．$S_B$ についてはシャッフルを 1 回行い，カードをめくる操作を最大 2 回行った結果 1/2 の確率でプロトコルが終了し，1/2 の確率でシャッフルを 1 回行って (B) に戻るため $S_B = 3$ である．$S_C$ は，(B) または (D) に進むまでにシャッフルを 2 回行うため $S_C = 2$ であり，$S_D$ についてはシャッフルを 2 回行ったあと 1/2 の確率で (B) に進み，1/2 の確率で (D) に戻るため $S_D = 4$ である．以上より提案プロトコルのシャッフル回数の期待値はこれらの値を (2) 式に代入することで，7 回となる．

## 4. おわりに

本稿ではランダム二等分割カットのみを用いるコミット型 AND プロトコルを 5 枚のカードで構成し，既存の 6 枚から 1 枚削減することに成功した．よって次の定理が成立する．

**定理 1** カード枚数 5 枚のランダム二等分割カットのみを用いるコミット型 AND プロトコルが存在する．

また，Kastner [5] らによって次の定理が示されている．

**定理 2 ( [5])** シャッフルとして一様で closed なもののみを用いる場合，カード枚数 4 枚のコミット型 AND プロトコルは存在しない．

ランダム二等分割カットは一様で closed なシャッフルであるため，定理 1 と定理 2 より提案プロトコルが必要なカード枚数が最小という意味で最適であることが導かれる．

本稿のプロトコルでは，カード枚数を削減した一方でシャッフル回数が大幅に増加している．このシャッフル回数を削減することが可能かどうか，あるいはシャッフル回数を有限とすることが可能かどうかは今後の課題である．近年カードベース暗号の研究が盛んであり（例 [7,14–19]），この問題を含め様々な魅力的な未解決問題が残されているので多くの研究者のこの分野への参入を期待したい．

**謝辞** 提案プロトコルの発見に協力頂いた阿部勇太氏に感謝します．本研究は JSPS 科研費 JP19J21153 と JP21K11881 の助成を受けたものです．

### 参考文献

[1] Abe, Y., Hayashi, Y., Mizuki, T. and Sone, H.: Five-Card AND Protocol in Committed Format Using Only Practical Shuffles, *5th ACM on ASIA Public-Key Cryptography Workshop*, APKC '18, New York, ACM, pp. 3–8 (online), available from ⟨https://doi.org/10.1145/3197507.3197510⟩ (2018).

[2] Abe, Y., Hayashi, Y., Mizuki, T. and Sone, H.: Five-Card AND Computations in Committed Format Using Only Uniform Cyclic Shuffles, *New Gener. Comput.*, Vol. 39, No. 1, pp. 97–114 (online), available from ⟨https://doi.org/10.1007/s00354-020-00110-2⟩ (2021).

[3] Abe, Y., Mizuki, T. and Sone, H.: Committed-format AND protocol using only random cuts, *Natural Computing*, (online), DOI: 10.1007/s11047-021-09862-2 (2021).

[4] Crépeau, C. and Kilian, J.: Discreet Solitary Games, *Advances in Cryptology—CRYPTO' 93* (Stinson, D. R., ed.), LNCS, Vol. 773, Berlin, Heidelberg, Springer, pp. 319–330 (online), available from ⟨https://doi.org/10.1007/3-540-48329-2_27⟩ (1994).

[5] Kastner, J., Koch, A., Walzer, S., Miyahara, D., Hayashi, Y., Mizuki, T. and Sone, H.: The Minimum Number of Cards in Practical Card-Based Protocols, *Advances in Cryptology—ASIACRYPT 2017* (Takagi, T. and Peyrin, T., eds.), LNCS, Vol. 10626, Cham, Springer, pp. 126–155 (online), available from ⟨https://doi.org/10.1007/978-3-319-70700-6_5⟩ (2017).

[6] Koch, A., Walzer, S. and Härtel, K.: Card-Based Cryptographic Protocols Using a Minimal Number of Cards, *Advances in Cryptology—ASIACRYPT 2015* (Iwata, T. and Cheon, J. H., eds.), LNCS, Vol. 9452, Berlin, Heidelberg, Springer, pp. 783–807 (online), available from ⟨https://doi.org/10.1007/978-3-662-48797-6_32⟩ (2015).

[7] Mizuki, T.: Preface: Special Issue on Card-Based Cryptography, *New Gener. Comput.*, Vol. 39, No. 1, pp. 1–2 (2021).

[8] Mizuki, T. and Shizuya, H.: Practical Card-Based Cryptography, *Fun with Algorithms* (Ferro, A., Luccio, F. and Widmayer, P., eds.), LNCS, Vol. 8496, Cham, Springer, pp. 313–324 (online), available from ⟨https://doi.org/10.1007/978-3-319-07890-8_27⟩ (2014).

[9] Mizuki, T. and Sone, H.: Six-Card Secure AND and Four-Card Secure XOR, *Frontiers in Algorithmics* (Deng, X., Hopcroft, J. E. and Xue, J., eds.), LNCS, Vol. 5598, Berlin, Heidelberg, Springer, pp. 358–369 (online), available from ⟨https://doi.org/10.1007/978-3-642-02270-8_36⟩ (2009).

[10] Niemi, V. and Renvall, A.: Secure multiparty computations without computers, *Theor. Comput. Sci.*, Vol. 191, No. 1–2, pp. 173–183 (online), available from ⟨https://doi.org/10.1016/S0304-3975(97)00107-2⟩ (1998).

[11] Stiglic, A.: Computations with a deck of cards, *Theor. Comput. Sci.*, Vol. 259, No. 1–2, pp. 671–678 (online), available from ⟨https://doi.org/10.1016/S0304-3975(00)00409-6⟩ (2001).

[12] Ueda, I., Miyahara, D., Nishimura, A., Hayashi, Y., Mizuki, T. and Sone, H.: Secure implementations of a random bisection cut, *Int. J. Inf. Secur.*, Vol. 19, No. 4, pp. 445–452 (online), available from ⟨https://doi.org/10.1007/s10207-019-00463-w⟩ (2020).

[13] Ueda, I., Nishimura, A., Hayashi, Y., Mizuki, T. and Sone, H.: How to Implement a Random Bisection Cut, *Theory and Practice of Natural Computing* (Martín-Vide, C., Mizuki, T. and Vega-Rodríguez, M. A., eds.),

LNCS, Vol. 10071, Cham, Springer, pp. 58–69 (online), available from ⟨https://doi.org/10.1007/978-3-319-49001-4_5⟩ (2016).
[14] 土井アナスタシヤ, 中井雄士, 品川和雅, 渡邉洋平, 岩本貢：カードを用いた秘匿共通集合プロトコル, コンピュータセキュリティシンポジウム 2021（CSS2021）(2021).
[15] 中林佳祐，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 2021（CSS2021）(2021).
[16] 須賀祐治：手の内だけで簡単に実行可能な Six Card Trick とカード入力後の置換に関する考察，第 92 回 CSEC 研究発表会，7 (2021).
[17] 中井雄士，徳重佑樹，　岩本貢，太田和夫：秘匿置換を用いたカードベースしきい値関数プロトコル，暗号と情報セキュリティシンポジウム SCIS2021，2F1-3 (2021).
[18] 須賀祐治：三人寄ればチーズの知恵，マルチメディア，分散協調とモバイルシンポジウム 2021 論文集，Vol. 2021, No. 1, pp. 173–178（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/170000185498/⟩ (2021).
[19] 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 2021（CSS2021）(2021).