Computer Security Symposium 2025
27-31 October 2025

最小枚数 AND プロトコルにおける 平均シャッフル回数の上界と下界

宮原 大輝[1,2,a)]

概要：カードベース暗号プロトコルの効率性は，主にカード枚数とシャッフル操作回数（ステップ数）によって評価される．カード枚数については必要十分条件の解析がある程度進み，特に 2014 年に Mizuki と Shizuya によって構築された計算モデルの下で，2 入力論理積（AND）の計算に必要なカード枚数のタイトな下界が明らかになった．しかし，必要なシャッフル回数の下界については未解明のままである．2021 年に Shinagawa と Nuida によって，カード枚数が十分に存在すれば 1 回のシャッフル操作で任意の関数を計算できることが示されているが，この最も基礎的な AND については，最小枚数の場合におけるシャッフル回数の下界は未解明である．そこで本研究では，シャッフル回数の下界を証明し，カード枚数とシャッフル回数にトレードオフがあることを示す．具体的には，4 枚・5 枚 AND プロトコルのシャッフル回数の限界を与える．特に 4 枚 AND プロトコルは必ずループを持つ，つまりラスベガス法に陥ることが証明されているため，本稿の結果はそのようなプロトコルに対して初めて下界を与えることになる．

キーワード：カードベース暗号，ラスベガス法，ステップ数，シャッフル回数

Upper and Lower Bounds on the Expected Number of Shuffles in Minimal-Card AND Protocols

Daiki Miyahara[1,2,a)]

Abstract: The efficiency of card-based cryptographic protocols has been primarily measured by the number of cards and the number of shuffling actions required. The minimal number of cards, especially for computing the two-input AND function, was completely determined under the computational model presented by Mizuki and Shizuya in 2014. However, nontrivial lower bounds on the number of shuffles remain open. In 2021, Shinagawa and Nuida showed that any function can be computed with a single shuffle given sufficiently many cards, but even for one of the most fundamental Boolean functions, namely the minimal-card two-input AND protocol, such a lower bound remains an entirely open problem. In this study, we present lower bounds on the number of shuffles for four- and five-card AND protocols, revealing a trade-off between the number of cards and the number of shuffles. In particular, our results provide the first lower bound for four-card AND protocols, which necessarily fall into the category of Las Vegas algorithms.

1. はじめに

カードベース暗号とは，物理的なカード組のみを用いて秘密計算を実現する暗号プロトコルであり，計算機を一切用いないという特性から，現代暗号とは一線を画す分野である．カードベース暗号（や他の物理的な道具を用いる暗号プロトコル）を対象とする国際会議論文は，Ruangwises 氏の Web サイト[*1]に全てまとまっている．更新速度も驚異的であり，国際会議の Accepted Papers にタイトルが掲載された瞬間に更新されるほどである[*2]．このサーベイリ

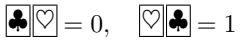
[1] 電気通信大学
The University of Electro-Communications
[2] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[a)] miyahara@uec.ac.jp

[*1] https://www.suthee.info/cbc-papers
[*2] あくまで著者の体感である．

ストによると，本稿執筆時点で 143 本の国際会議論文が存在し，情報セキュリティや理論計算機科学を対象とする幅広い国際会議に受け入れられていることが分かる．また，このリストには含まれていない国際論文誌についても，例えば TCS 誌や IEICE Trans. Fundamentals 誌などに多数掲載されている．特に NGCO 誌では，カードベース暗号に関する特集号がこれまでに 3 度組まれている [8].

1.1 モチベーション

本稿では 2 入力論理積を秘密計算する最も基礎的な AND プロトコルを対象とする．問題設定は次の通りである．ビットを黒と赤の 2 色のカードで次のように符号化する．



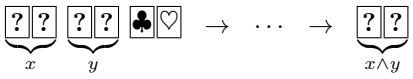
$$= 0, \quad = 1 \tag{1}$$

2 枚の裏になったカードがビット $x \in \{0,1\}$ を表すとき，その 2 枚を x の**コミットメント**といい，次のように表す．

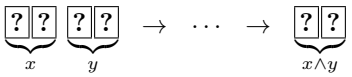
AND プロトコルは，$x, y \in \{0,1\}$ の入力コミットメントと追加カードが与えられ，$x \wedge y$ のコミットメントを出力する．

本稿ではコミットメントを出力する**コミット型**を対象とし，文脈上明らかな場合はコミット型の表記を省略する．

カードベース暗号は AND プロトコルに関する研究とともに発展してきたと言っても過言ではない．スペースの都合上，3 つに絞って研究を紹介する．1993 年に Crépeau と Kilian [1] によってコミット型 AND プロトコルが初めて提案され，カード組を用いて任意の関数を計算できることが示された．ただし追加カードを 6 枚使用し，プロトコルは **Las Vegas 法**，すなわち繰り返し構造を持つため，必要なステップ数は期待値で表される．特にシャッフル操作回数（以降では単に**シャッフル回数**と呼ぶ）の期待値は 8 回であり，実際に手で実行しようと思うまでには至らない．2009 年に Mizuki と Sone [11] によって，シャッフル操作 1 回で必ず終了する 6 枚 AND プロトコルが提案され，コミット型のプロトコルがデモ実演可能なレベルにまで効率化された．



このプロトコルをベースとして，対称関数といったより広い関数に特化して効率的なプロトコルが考案されている（cf. [12]）．2015 年に Koch ら [6] は，追加カード無しで AND を計算できることに加えて，追加カード無しの場合は必ず Las Vegas 法に陥ることを証明した．



ただしシャッフル回数の期待値は 8 回である．特筆すべきこととして，このプロトコルに用いられるシャッフル操作自体も実装が難しい（と思われている）が，この研究からシャッフル操作の実装に関する流れも生まれている（cf. [7]）．

1.2 貢献

本研究では，4 枚コミット型 AND プロトコルに必要なシャッフル回数（の期待値）の上界と下界を提示する．主要な結果は次の定理にまとめられる．

定理 1. シャッフル回数の期待値が約 3.57 回となるような 4 枚コミット型 AND プロトコルが存在する．

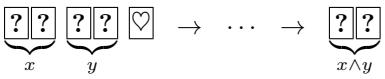
定理 2. 任意の 4 枚コミット型 AND プロトコルにおけるシャッフル回数の期待値は約 3.43 回が限界である．

これらの定理より，タイトな下界は得られなかったものの，ラスベガス法に必ず陥るカードベースプロトコルに必要な手順数の下界を初めて提示し，約 0.15 回まで狭められたことが主要な貢献である．また下界の証明により，4 枚 AND プロトコルに関する次の知られた結果に対する別証明も提示できる．

- 任意の 4 枚**非コミット型** AND プロトコルには，実用的なシャッフル操作が 2 回必要である [2].
- 任意の 4 枚コミット型 AND プロトコルは，非実用的なシャッフル操作を必要とする [5].

これは，下界の証明において適用可能なシャッフル操作を全て数え上げているために得られる副産物である．

本研究ではさらに，5 枚コミット型 AND プロトコルに関する上界も求める．既存プロトコルとして Koch ら [6] は，確率 $2/3$ で 4 回，確率 $1/3$ で 6 回のシャッフル操作で終了する有限時間プロトコルを提案している．



これに対し本研究では次の上界を提示する．

定理 3. 2 回のシャッフル操作で終了する 5 枚コミット型 AND プロトコルが存在する．

この定理より，5 枚におけるシャッフル回数の下界は 2 回以下であることがいえる．しかし 4 枚のときと同じように下界を得ようとすると，他に確率 $1/2$ で 1 回で終了するプロトコルが見つかり，さらに終了しない場合の構造が複雑であったため，詳細な検討が必要である．

2. 準備

本節でコミット型プロトコルの形式的な定義を与える．カードベース暗号の計算モデルは 2014 年に Mizuki と Shizuya [10] によって構築され，このモデルの下で AND

プロトコルの枚数に関する下界が証明されてきた．

2.1 計算モデル

Σ を**シンボル**（絵柄）集合[*3]とする．Σ 上の有限多重集合を $\mathcal{D}$ とし，**デッキ**という．$c \in \mathcal{D}$ に対して，テーブル上に置かれる表面のカードを $^{c}/_{?}$，裏面のカードを $^{?}/_{c}$ で表す．ここで “?” はカードの裏面を表す特殊な記号であり，これらを総称して**カード**という．カード $\alpha = {}^{u}/_{v}$ に対して，次の関数を定義する．

- $\mathsf{swap}({}^{u}/_{v}) \coloneqq {}^{v}/_{u}$
- $\mathsf{vis}({}^{u}/_{v}) \coloneqq u$
- $\mathsf{symb}({}^{u}/_{v}) \coloneqq \begin{cases} u & \text{if } u \in \mathcal{D} \\ v & \text{if } v \in \mathcal{D} \end{cases}$

デッキ $\mathcal{D}$ に対して，$d \coloneqq |\mathcal{D}|$ とする．カードの順序付き d 組 $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ が以下を満たすとき，Γ を d 枚の**カード列**という．

$$\mathcal{D} = [\mathsf{symb}(\alpha_1), \mathsf{symb}(\alpha_2), \ldots, \mathsf{symb}(\alpha_d)\,]$$

カード列 Γ に対して，関数 $\mathsf{vis}(\cdot)$ を自然に拡張して適用させ，$\mathsf{vis}(\Gamma) = ((\mathsf{vis}(\alpha_1), \ldots, \mathsf{vis}(\alpha_d))$ を Γ の**可視列**という．$\mathcal{D}$ 上の全てのカード列を含む集合を $\mathsf{Seq}^{\mathcal{D}}$ と表す．

$$\mathsf{Seq}^{\mathcal{D}} \coloneqq \{\Gamma \mid \Gamma \text{ is a sequence from } \mathcal{D}\}$$

全ての可視列を含む集合を $\mathsf{Vis}^{\mathcal{D}} \coloneqq \{\mathsf{vis}(\Gamma) \mid \Gamma \in \mathsf{Seq}^{\mathcal{D}}\}$ とする．

プロトコルは，4 つ組 $\mathcal{P} = (\mathcal{D}, U, Q, A)$ で表される．ここで $\mathcal{D}$ はデッキ，$U \subseteq \mathsf{Seq}^{\mathcal{D}}$ は入力集合，Q は開始状態 q_0 と終了状態 q_{f} を含む状態集合，$A\colon Q \times \mathsf{Vis}^{\mathcal{D}} \to Q \times \mathsf{Action}$ は動作関数である．ここで Action は次の動作を含む動作集合であり，カード列 $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathsf{Seq}^{\mathcal{D}}$ に対して次のように動作する．

- (turn, T)．これは集合 $T \subseteq [\![1, d]\!]$ で示されるカードを裏返す．ここで 2 重ブラケットは整数区間を表し，以降でも同様に表記する．

$$\mathsf{turn}_T(\Gamma) = (\beta_1, \beta_2, \ldots, \beta_d),$$
$$\text{s.t. } \beta_i = \begin{cases} \mathsf{swap}(\alpha_i) & \text{if } i \in T \\ \alpha_i & \text{otherwise} \end{cases}$$

- (perm, π)．d 次の対称群を S_d とする．これは置換 $\pi \in S_d$ に従ってカード列を並び替える．

$$\mathsf{perm}_\pi(\Gamma) = (\alpha_{\pi^{-1}(1)}, \alpha_{\pi^{-1}(2)}, \ldots, \alpha_{\pi^{-1}(d)})$$

- $(\mathsf{shuf}, \Pi, \mathcal{F})$．これは置換集合 $\Pi \subseteq S_d$ 上の確率分布 $\mathcal{F}$ に従って置換 $\pi \in \Pi$ が選ばれ，カード列に適用する．$\mathcal{F}$ が一様分布の場合は $\mathcal{F}$ を省略して (shuf, Π) と書き，**一様**シャッフルと呼ぶ．Π が群を成すとき，**閉**シャッフルと呼ぶ．

$$\mathsf{shuf}_{\Pi,\mathcal{F}}(\Gamma) = \mathsf{perm}_{\pi \leftarrow \mathcal{F}}(\Gamma)$$

- $(\mathsf{result}, p_1, p_2)$．これは最終状態 q_{f} においてのみ現れる動作であり，$p_1, p_2 \in [\![1, d]\!]$ で指定されるコミットメントを出力してプロトコルは終了する．

[*3] 本稿では $\Sigma = \{\clubsuit, \heartsuit\}$ となる．

2.2 既知の性質

計算モデル上でのプロトコルの表記を簡略化する性質として，シャッフルの**合成** [10] を紹介する．これは連続して適用される任意の 2 つのシャッフル操作は，1 つのシャッフル操作に合成して表記できることをいい，任意の置換集合と確率分布を許しているためである．より厳密には，2 つのシャッフル動作 $(\mathsf{shuf}, \Pi_1, \mathcal{F}_1)$ と $(\mathsf{shuf}, \Pi_2, \mathcal{F}_2)$ がこの順でカード列に適用されるとき，$\pi_1 \in \Pi_1$，$\pi_2 \in \Pi_2$ および $\pi' = \pi_2 \circ \pi_1$ に対して，これらは次を満たすシャッフル動作 $(\mathsf{shuf}, \Pi', \mathcal{F}')$ の適用と等しい．

$$\begin{aligned} \Pi' &= \Pi_2 \circ \Pi_1 \\ \mathcal{F}'(\pi') &= \mathcal{F}_1(\pi_1) \times \mathcal{F}_2(\pi_2) \end{aligned} \tag{2}$$

しかし 2 つのシャッフルの間にめくる動作 turn がある場合，これらは一般的には合成できない．なぜなら，カードをめくることによってどの置換が 1 つ目のシャッフルで適用されたか（ある程度）絞られるためである．

並び替え動作 (perm, π) は，置換集合の大きさが 1 の一様シャッフル (shuf, π) と見なせるため，これもシャッフルに合成できる．並び替え動作が（計算モデル上は）プロトコルの本質に影響しないことは自明である．

2.3 KWH 木：状態遷移図

プロトコルの正当性と安全性を図示する**状態遷移図** [6] を紹介する．開始状態から終了状態までの遷移は木構造となり，考案者の頭文字を取って **KWH 木**とも呼ばれる．例として図 1 を参照されたい．

あるプロトコル $\mathcal{P} = (\mathcal{D}, U, Q, A)$ の実行を考えよう．開始状態から終了状態までのカード列の遷移 $(\Gamma_0, \Gamma_1, \ldots, \Gamma_{\mathrm{f}})$ を**トレース**といい，$(\mathsf{vis}(\Gamma_0), \mathsf{vis}(\Gamma_1), \ldots, \mathsf{vis}(\Gamma_{\mathrm{f}}))$ を**可視列トレース**という．$\mathcal{P}$ の最初からある地点までの可視列トレース（つまり接頭部分）を v とするとき，v に対する**状態**は，v に条件付けられた $\mathsf{Seq}^{\mathcal{D}}$ 上の確率分布とされる．これはすなわち，ある地点におけるテーブル上のカード列は，実際には入力の値に応じて複数の可能性があり，さらにシャッフル動作によって確率的に変化するため，それを確率分布として表記することでプロトコルの確率遷移を捉える方法である．さらにめくる動作はカード列を一部確定させるため，v が与えられたときの条件付き確率分布となる．この確率分布の遷移を図示したものが KWH 木とな

り，図 1 に示すように，各状態が “箱” として表され，各動作によって変化していきながら最終的にコミットメントを出力する．ここで各箱内には本来はカード列を表記する必要がある（$\mathsf{Seq}^{\mathcal{D}}$ 上の確率分布であるため）が，カードではなくシンボルのみを記載することによって，視認性を高めている [6]．

より厳密な定義を与える．まず 2 入力のブール関数 $f\colon \{0,1\}^2 \to \{0,1\}$ に対して，入力が $b \in \{0,1\}^2$ である確率を表す記号を $X_b \in (0,1)$ とする．これらの記号を変数としたときの一次斉次多項式の集合を $\mathbb{R}[X_b \mid b \in \{0,1\}^2]$ とする．v に対する状態は，次を満たす写像 $\mu_v\colon \mathsf{Seq}^{\mathcal{D}} \to \mathbb{R}[X_b \mid b \in \{0,1\}^2]$ とされる．

- $\Sigma_{s \in \mathsf{Seq}^{\mathcal{D}}} \mu_v(s) = \Sigma_{b \in \{0,1\}^2} X_b = 1$.
- 全ての $s \in \mathsf{Seq}^{\mathcal{D}}$ に対して，$\mu_v(s)$ の各係数は $[0,1]$ の範囲に収まる．
- $\mu_v(s) \neq 0$ である全ての $s \in \mathsf{Seq}^{\mathcal{D}}$ に対して，$\mathsf{vis}(s)$ は v の末尾に一致する．このとき μ_v は s を**含む**という．

各動作の定義を踏まえ，状態 μ_v が各動作によってどのように変化するか記述する．まずシャッフル動作 $(\mathsf{shuf}, \Pi, \mathcal{F})$ によって μ_v が $\mu_{v'}$ に遷移したとする．ここでシャッフル動作を適用するカード列は全て裏面であるため，μ_v はただ一つの状態に遷移する．各 $s \in \mathsf{Seq}^{\mathcal{D}}$ に対して $\mu_{v'}(s)$ は以下のように計算できる．

$$\mu_{v'}(s) = \sum_{\pi \in \Pi} \mathcal{F}(\pi) \cdot \mu_v(\pi^{-1}(s))$$

めくる動作 (turn, T) については，状態 μ_v は複数に遷移する[*4]．めくる動作を適用した結果現れる可視列を v^+ とし，その地点までの可視列トレースを v' とすると，$v' = v \,\|\, v^+$ である．このとき μ_v が $\mu_{v'}$ に遷移する確率は，めくる位置 $t \in T$ のカードの絵柄が v^+ に合致するようなカード列が μ_v に含まれる確率である．すなわち $\mathsf{vis}(\mathsf{turn}_T(s)) = v^+$ である全ての $s \in \mathsf{Seq}^{\mathcal{D}}$ について，$\mu_v(s)$ の和がその確率である．ここでその確率を定数 $\lambda \in (0,1)$ とすると，次が成り立つ．

$$\sum_{\substack{s \in \mathsf{Seq}^{\mathcal{D}} \\ \mathsf{vis}(\mathsf{turn}_T(s)) = v^+}} \mu_v(s) = \lambda \sum_{b \in \{0,1\}^2} X_b = \lambda \tag{3}$$

これは入力がどの $b \in \{0,1\}^2$ であったとしても同じ確率 λ で遷移することを意味するため，後で定義するように λ の存在が安全性の条件となる．この λ を用いることにより，各 $s \in \mathsf{Seq}^{\mathcal{D}}$ に対する $\mu_{v'}(s)$ を以下のように計算できる．

$$\mu_{v'}(s) = \frac{\mu_v(s)}{\lambda}, \quad \text{where } \mathsf{vis}(\mathsf{turn}_T(s)) = v^+$$

これは λ によって，各確率の和が 1 になるように正規化しているとも捉えられる．

[*4] ただ一つの状態に遷移することは考えない．なぜならその場合は現れる色が確定的であり，めくることによって何も情報が得られないためである．

KWH 木を用いてプロトコルの正当性と安全性を定義する．

定義 1 (正当性)．プロトコル $\mathcal{P} = (D, U, Q, A)$ は，$\mathcal{P}$ の KWH 木が以下を満たすとき，2 入力 AND 関数を計算するという．

- 各入力 $b \in \{00, 01, 10, 11\}$ に対して，開始状態 μ_0 は唯一のカード列 $s = (\alpha_1, \ldots, \alpha_d) \in U$ を含み，$\mu_0(s) = X_b$ である．ここで各 $i \in [\![1, 2]\!]$ に対して，次を満たす．

$$(\alpha_{2i-1}, \alpha_{2i}) = \begin{cases} (?/\clubsuit, ?/\heartsuit) & \text{if } b[i] = 0 \\ (?/\heartsuit, ?/\clubsuit) & \text{if } b[i] = 1 \end{cases}$$

  ここで $b[i]$ は i 番目のビットを表し，インデックスは 1 から始まる．
- 各最終状態 μ_ℓ は，動作 $(\mathsf{result}, p_1, p_2)$ によって出力コミットメントを決定する．すなわち μ_ℓ に含まれる各 $s = (\beta_1, \ldots, \beta_{|\mathcal{D}|}) \in \mathsf{Seq}^{\mathcal{D}}$ に対して，p_1, p_2 は次を満たす．

$$(\beta_{p_1}, \beta_{p_2}) = \begin{cases} (?/\heartsuit, ?/\clubsuit) & \mu_\ell(s) \text{ が } X_{11} \text{ を含む} \\ (?/\clubsuit, ?/\heartsuit) & \mu_\ell(s) \text{ が他 3 つを含む} \end{cases}$$

上の定義はすなわち，コミット型 AND プロトコルの入力・出力カード列を各入力に対して定めている．この定義より，任意の AND プロトコルにおいて，$\mu(s)$ が X_{11} を含む場合，他に変数は含まないことがいえる．すなわち任意の $s \in \mathsf{Seq}^{\mathcal{D}}$ と状態 μ に対して，次式が成り立つ．

$$\mu(s) \in \{\lambda_{00} X_{00} + \lambda_{01} X_{01} + \lambda_{10} X_{10}, \lambda_{11} X_{11} \mid \lambda_b \in [0,1], b \in \{0,1\}^2\} \tag{4}$$

定義 2 (安全性)．プロトコル $\mathcal{P} = (D, U, Q, A)$ は AND 関数を計算するとする．$\mathcal{P}$ の KWH 木における任意のめくる動作において，式 (3) を満たす定数 $\lambda \in (0,1)$ が存在するとき，$\mathcal{P}$ は安全である．

KWH 木を用いない場合，コミット型プロトコルの安全性は可視列トレースから入力が漏れないこと，すなわち可視列トレースの確率変数と入力の確率変数が互いに独立であると定義される [10]．可視列トレースはめくる動作によってのみ変化するため，結局はそこに注目する．[*5]

3. シャッフル回数の上界

本節で定理 3 を証明し，5 枚コミット型 AND プロトコルに必要なシャッフル回数の上界を与える．4 枚における上界である定理 1 については，スペースの都合上証明を省略する．

提案する 5 枚コミット型 AND プロトコルの KWH 木

[*5] コミット型の出力は各入力に対して一意に定まるが，非コミット型の場合は定まらないため，追加で “出力安全性” を考慮する必要がある [3]．

を図 1 に示す．ここで $X_0 \coloneqq X_{00}+X_{01}+X_{10}, X_1 \coloneqq X_{11}$ とする．この図より，初期状態から終了状態に至るまで，2.3 節で示した遷移規則に沿って状態が正しく遷移し，終了するまでにシャッフル操作が 2 回行われていることが分かる．正当であり（定義 1）かつ安全である（定義 2）ことも，この図から簡単に確認できる．正当性については，各終了状態 μ_ℓ において $\mu_\ell(s)$ が X_0 を含むならば $(?/\clubsuit, ?/\heartsuit)$ が出力され，X_1 を含むならば $(?/\heartsuit, ?/\clubsuit)$ が出力されている．安全性については，各めくる動作において遷移する確率がどの入力 $b \in \{0,1\}^2$ においても一定である．例えば上から 2 番目の箱（状態）を μ とすると，最初のめくる動作 $(\mathsf{turn}, \{3\})$ によって ♣ が見える確率は，$\mathsf{symb}(s[3]) = \clubsuit$ であるようなカード列を s とすると，$\mu(s)$ の和であり，以下のように計算される．

$$\begin{aligned}&\mu(\clubsuit\heartsuit\clubsuit\heartsuit\heartsuit)+\mu(\heartsuit\clubsuit\clubsuit\heartsuit\heartsuit)+\mu(\heartsuit\heartsuit\clubsuit\heartsuit\clubsuit)\\ =&1/2 X_{00}+1/4(X_{01}+X_{10})+1/4(X_{01}+X_{10})+1/2 X_{11}\\ =&1/2(X_{00}+X_{01}+X_{10}+X_{11})=1/2\end{aligned}$$

既存プロトコル [4, 図 8.2] では赤の追加カードを途中から活用することで有限時間となるが，提案プロトコルでは追加カードを最初から有効に活用することにより，シャッフル回数が抑えられている．用いられるシャッフル操作は $(\mathsf{shuf}, \{\mathsf{id}, (1\,4\,5\,2\,3)\} \circ \{\mathsf{id}, (1\,3)(2\,4)\})$ と $(\mathsf{shuf}, \Pi_1, \mathcal{F})$ であるが，どれも一様閉シャッフルではなく，非実用的である．ここで id は恒等置換である．

$$\begin{aligned}\Pi_1 &= \{\mathsf{id}, (1\,3\,2\,4\,5)\} \circ \{\mathsf{id}, (1\,2)\}\\ &= \{\mathsf{id}, (1\,2), (1\,3\,2\,4\,5), (1\,4\,5)(2\,3)\}\\ F_1\colon \mathsf{id} &\to 1/3, (1\,2) \to 1/3,\\ &(1\,3\,2\,4\,5) \to 1/6, (1\,4\,5)(2\,3) \to 1/6\end{aligned}$$

図 1 の “右側” では $(\mathsf{shuf}, \Pi_1, \mathcal{F}_1)$ の前に $(\mathsf{perm}, (2\,5)(3\,4))$ を適用することで，右側と左側の遷移が同一となるように工夫し，それら 2 つを合成している．

4. シャッフル回数の下界

本節で定理 2 を証明する．この証明は 2 つの定理から導かれ，まず任意の 4 枚コミット型 AND プロトコルは終了するために少なくとも 2 回のシャッフル操作が必要であること（定理 4）を示し，次に終了確率は 1/2 を超えないこと（定理 5）を示す．

4.1 シャッフル回数は 2 より大きい

定理 4. 任意の 4 枚コミット型 AND プロトコルは少なくとも 2 回のシャッフル操作を必要とする．

証明. $\mathcal{P} = (\mathcal{D}, U, Q, A)$ を安全な 4 枚 AND プロトコル，つまり $\mathcal{D} = [\clubsuit, \clubsuit, \heartsuit, \heartsuit]$ とし，$\mathcal{P}$ の KWH 木における初期状態を μ_0 とする．$\mathcal{P}$ が 1 回のシャッフル操作で終了すると仮定し，矛盾を導く．任意の AND プロトコルがシャッフル操作を 1 回必要とすることは自明であり，ある $\Pi \subseteq S_4$ に対して μ_0 が $(\mathsf{shuf}, \Pi, \mathcal{F})$ によって μ_1 に遷移すると仮定する．ここで各入力 $b \in \{0,1\}^2$ に対して，$s_b \in U$ は $\mu_0(s_b) = X_b$ を満たすカード列とする．すなわち次の通りである．

$$\begin{aligned}s_{00} &\coloneqq \clubsuit\heartsuit\clubsuit\heartsuit\\ s_{01} &\coloneqq \clubsuit\heartsuit\heartsuit\clubsuit\\ s_{10} &\coloneqq \heartsuit\clubsuit\clubsuit\heartsuit\\ s_{11} &\coloneqq \heartsuit\clubsuit\heartsuit\clubsuit\end{aligned} \tag{5}$$

ここで s_b と $s_{\bar{b}}$ は色に関して**対称**である．また μ_0 に含まれないカード列は $s \coloneqq \clubsuit\clubsuit\heartsuit\heartsuit$ と $s' \coloneqq \heartsuit\heartsuit\clubsuit\clubsuit$ の 2 つであり，これらも互いに対称である．

可能性のある Π を全て数え上げる．μ_1 にはめくる動作が適用されるため，式 (3) より，μ_1 は X_{11} に対応するカード列を少なくとも 2 つ含む．ここでまず Π は恒等置換 id を含むと固定すると，μ_1 は s_{11} を含み，もう一方を s' とする．（後で示すように，一般性を失わずに Π は id を含むと仮定でき，また μ_1 が s を含むとしても同様の議論が導かれる．）式 (4) より，各 $\pi \in \Pi$ は s_{11} を s_{11} もしくは s' に置換する必要があり，これより Π は高々 8 つの置換から成る．

$$\Pi \subseteq \{\underbrace{\mathsf{id}, (1\,3), (2\,4), (1\,3)(2\,4)}_{s_{11} \mapsto s_{11}}, \underbrace{(2\,3), (1\,2\,3), (1\,2\,4\,3), (2\,4\,3)}_{s_{11} \mapsto s'}\}$$

さらに s_{01} と s_{10} は s_{11} に置換されないため，Π はさらに絞られる．

$$\Pi \subseteq \{\mathsf{id}, (1\,3)(2\,4), (2\,3), (1\,2\,4\,3)\}.$$

$\mathcal{F}\colon \mathsf{id} \mapsto p_1, (1\,3)(2\,4) \mapsto p_2, (2\,3) \mapsto p_3, (1\,2\,4\,3) \mapsto p_4$ とし，$p_1+p_2+p_3+p_4 = 1$ を満たすとする．このシャッフルを初期状態に適用した KWH 木を図 2 に示す．ここで μ_1 は 2,3 番目をめくると式 (3) を満たすことができ，一般性を失わずに $(\mathsf{turn}, \{2\})$ を適用すると，次式を得る．

$$p_1+p_2 = p_1+p_3 = p_2+p_4 = p_3+p_4 \Rightarrow p_1+p_2 = 1/2.$$

この式より，μ_1 の各係数は 0 にならず，6 個のカード列を全て含む．そして $(\mathsf{turn}, \{2\})$ によって遷移する 2 つの状態はどれもコミットメントを出力できず，前提に矛盾する．以上の議論は Π を絞るにあたって最初に含むと固定した置換によらず，任意の $\pi \in S_4$ を Π に合成すれば同様に成り立つ．したがって以降では任意のシャッフル操作は id を含むと固定する． □

上の証明において $\mathcal{F}$ が一様分布となるのは，各 p_i が次の 3 通りの値を取るときである．

$$p_1 = p_3 = 1/2, p_1 = p_4 = 1/2, p_1 = p_2 = p_3 = p_4 = 1/4$$

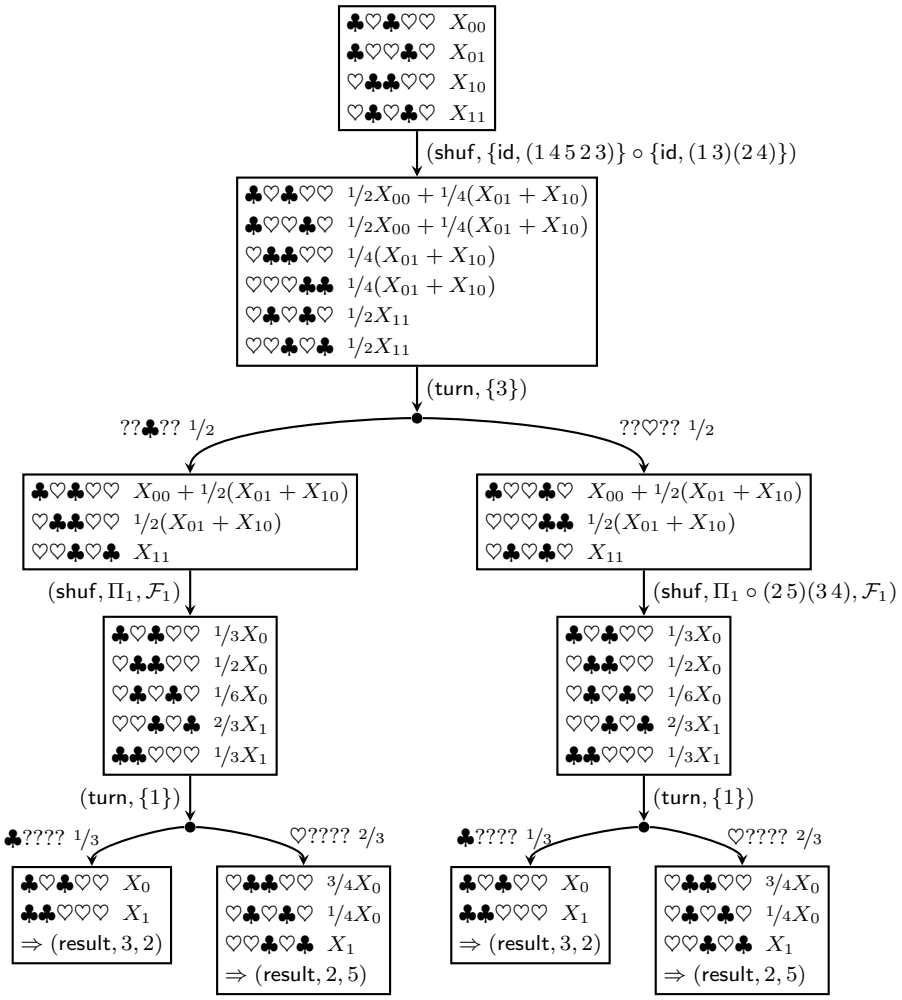


図 1 提案 5 枚コミット型 AND プロトコル．ここで $\Pi_1 = \{\mathsf{id}, (1\,3\,2\,4\,5)\} \circ \{\mathsf{id}, (1\,2)\} = \{\mathsf{id}, (1\,2), (1\,3\,2\,4\,5), (1\,4\,5)(2\,3)\}$, $F_1\colon \mathsf{id} \to 1/3, (1\,2) \to 1/3, (1\,3\,2\,4\,5) \to 1/6, (1\,4\,5)(2\,3) \to 1/6$ および $X_0 = X_{00} + X_{01} + X_{10}, X_1 = X_{11}$ である．2 回のシャッフル操作で必ず終了する．

ただしどの場合でも，Π は群となり得ない．これはすなわち，1 回のシャッフル操作によって正当性と安全性を満たしながらプロトコルを進める場合は，シャッフル操作は閉シャッフルとは成り得ず，これは非コミット型でも同様[*6]である．Iino ら [2] の証明では，全ての閉シャッフルを 30 個数え上げ，その内のどれを適用しても式 (4) もしくは式 (3) に反することが示されている．

4.2 終了確率は 1/2 を超えない

定理 5. 任意の 4 枚コミット型 AND プロトコルがループを抜け出す確率は $1/2$ を超えない．

本定理の証明は 2 つの補題から成る．1 つ目（補題 1）は，任意のプロトコルにおけるループ構造は図 3 として一般化されることである．2 つ目（補題 2）は，図 3 において，置換集合 Π は 6 個に限定されかつ $|\Pi| \leq 4$ となる．これらを踏まえ，6 個の可能性を全て試すことで定理 5 を証明する．

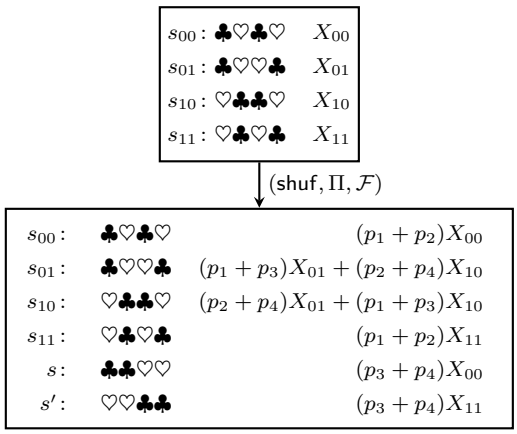


図 2 4 枚 AND プロトコル KWH 木における初期状態からシャッフル操作による遷移の一般化．ここで $\mathcal{F}\colon \mathsf{id} \mapsto p_1, (1\,3)(2\,4) \mapsto p_2, (2\,3) \mapsto p_3, (1\,2\,4\,3) \mapsto p_4$, $p_1 + p_2 + p_3 + p_4 = 1$ である．

補題 1. 任意の 4 枚コミット型 AND プロトコルのループ

[*6] 非コミット型の場合は，(turn, {2}) で出た色に応じて再度 1 枚めくることで論理積の値を求めることができ，これはまさに Mizuki ら [9] の 4 枚 AND プロトコル（のシャッフル合成版）である．

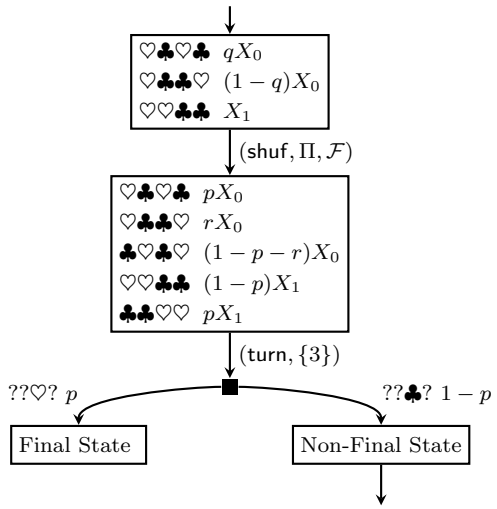


図 3 任意の 4 枚コミット型 AND プロトコルにおけるループの一般化

は図 3 として一般化される．

証明. 任意の 4 枚コミット型 AND プロトコルにおける KWH 木を考える．ここで定理 4 の証明より，図 2 は初期状態に対して任意のシャッフル操作を適用した際の KWH 木の一般化であり，これにめくる動作によって遷移する 2 つの状態に注目する．2 つの内，♡ が見えた方を μ_2 とし，一般性を失わずに 1 番目の位置に ♡ が見えたとする．（♣ が見えた際の議論は対称的であり省略できる．）このとき，μ_2 に含まれる 3 つのカード列は一意に定まり，$\mathsf{supp}(\mu_2) = \{♡♣♡♣, ♡♣♣♡, ♡♡♣♣\}$ である．図 3 に示すように，$\mu_2(♡♡♣♣) = X_1$ と仮定し，$q \in (0,1)$ を X_0 の係数とする．（X_1 を含むカード列を他の 2 つに仮定しても同様の議論となる．）

μ_2 があるシャッフル操作 $(\mathsf{shuf}, \Pi, \mathcal{F})$ によって遷移した先の状態を μ_3 とする．先述したように Π は id を含み，μ_3 は μ_2 に含まれる 3 つのカード列を少なくとも含む．ここで μ_3 は $(\mathsf{turn}, \{3\})$ によって最終状態に遷移すると仮定すると，μ_3 には 2 つの可能性が存在し，図 3 に示すように ♡ が見えて最終状態に遷移するか，もしくは ♣ が見えて遷移するかの 2 通りが考えられる．しかし以降では，前者の図 3 しか起こり得ないことを示す．

後者の場合を仮定し，矛盾を導く[*7]．ここで以下の記号を導入する．

- $c \in \{♣, ♡\}$ とする．Π に含まれる置換で，μ_2 に含まれる ♡♡♣♣ を，μ_3 に含まれる $s_♣ \coloneqq ♡♡♣♣$ もしくは $s_♡ \coloneqq ♣c♡\bar{c}$ に置換する全ての置換の集合を，それぞれ $\Pi_♣ \subset \Pi$ と $\Pi_♡ \subset \Pi$ とする．すなわち，

$$\Pi_{♣(♡)} \coloneqq \{\pi \mid \pi^{-1}(s_{♣(♡)}) = ♡♡♣♣, \pi \in \Pi\}$$

であり，$\Pi_♣ \sqcup \Pi_♡$ は Π の分割である．さらに

$$\sum_{\pi \in \Pi_♣} \mathcal{F}(\pi) = p, \quad \sum_{\pi \in \Pi_♡} \mathcal{F}(\pi) = 1 - p \qquad (6)$$

として p を定める．すなわち $\mu_3(s_♣) = pX_1$ かつ $\mu_3(s_♡) = (1-p)X_1$ とする．

- Π に含まれる置換で，μ_2 に含まれる ♡♣♡♣ もしくは ♡♣♣♡ を μ_3 に含まれる $s_0 \coloneqq ♡♣♣♡$ に置換する全ての置換の集合を $\Pi_0 \subset \Pi$ とする．すなわち，

$$\Pi_0 \coloneqq \{\pi \mid \pi^{-1}(s_0) = ♡♣♡♣, ♡♣♣♡, \pi \in \Pi\} \qquad (7)$$

とする．μ_3 に含まれる 5 つのカード列の内，$s_0[3] = s_♣[3] = ♣$ であるため，式 (3) より，$\mu_3(s_0) + \mu_3(s_♣)$ は定数となり，特に $\mu_3(s_0) = pX_0$ である．

ここで $\Pi_0 \cap \Pi_♡ = \emptyset$ かどうかの 2 通りが存在するが，どちらの場合も以下のように矛盾が導かれる．

(1) $\Pi_0 \cap \Pi_♡ = \emptyset$ とすると，$\Pi = \Pi_♣ \sqcup \Pi_♡$ より $\Pi_0 \subseteq \Pi_♣$ である．これと式 (6) より，以下が得られる．

$$\sum_{\pi \in \Pi_0} \mathcal{F}(\pi) \leq \sum_{\pi \in \Pi_♣} \mathcal{F}(\pi) = p$$

しかしながらこれは以下の矛盾を導く．

$$\begin{aligned} \mu_3(s_0) = pX_0 &= \sum_{\pi \in \Pi_0} \mathcal{F}(\pi) \cdot \mu_2(\pi^{-1}(s_0)) \\ &< \sum_{\pi \in \Pi_0} \mathcal{F}(\pi) \cdot X_0 \\ &\leq \sum_{\pi \in \Pi_♣} \mathcal{F}(\pi) \cdot X_0 = pX_0 \end{aligned}$$

これはすなわち，例え $q = 1$ かつ $1 - q = 1$ だとしても，$\mu_3(s_0)$ に含まれる X_0 の係数，すなわち p は，p より小さいことを意味し，矛盾する．

(2) $\Pi_0 \cap \Pi_♡ \neq \emptyset$ とすると，これは $\pi \in \Pi_0 \cap \Pi_♡$ を満たすような π が存在することを意味する．ここで $\pi(s_♣) = s_♣$ であるため，$\pi(1) = 3$ もしくは $\pi(2) = 3$ であるが，どちらも以下のように矛盾する．

- $\pi(1) = 3$ とすると，$\pi(♡♣♡♣)[3] = ♡$ かつ $\pi(♡♣♣♡)[3] = ♡$ であるが，式 (7) に示したように $\pi(♡♣♡♣) = s_0$ もしくは $\pi(♡♣♣♡) = s_0$ であるため，$\pi(♡♣♡♣)[3] = ♣$ もしくは $\pi(♡♣♣♡)[3] = ♣$ となり，矛盾する．
- $\pi(2) = 3$ とすると，これは μ_3 が X_0 に対応するカード列について，3 番目の位置が ♣ となるようなカード列を 2 つ含むことを意味する．しかし μ_3 はそのようなカード列を 1 つしか含まないと仮定していたため，矛盾する．

以上より図 3 に示すように，一般性を失わずに ♡ が見えて最終状態に遷移すると一般化できるが，最後に $s_♡ = ♣♣♡♡$ を示す．$\pi(2) = 3$ としたときの議論と同様に，μ_3 が X_0 に対応するカード列について，4 番目の位置が ♡ である

[*7] 本来は後者の場合を表す KWH 木を準備していたが，スペースの都合上省略する．

ようなカード列を 2 つ既に持っていることに注目する．これは任意の $\pi \in \Pi$ に対して，$\pi(1) = 4$ もしくは $\pi(1) = 1$ が成り立つことを意味する．したがって $s_{\heartsuit}$ はただ一つの ♣♣♡♡ に定まり，本補題は証明される．（これにより μ_3 には ♣♡♡♣ が含まれないと一般性を失わずに仮定でき，次の Π の数え上げで効力を発揮する．） □

補題 2. 図 3 における Π は 6 つに限定される．

証明. μ_2, μ_3 を補題 1 の証明の際と同様に定める．μ_2 に含まれる ♡♡♣♣ は，μ_3 に含まれる ♡♡♣♣ もしくは ♣♣♡♡ に $(\mathsf{shuf}, \Pi, \mathcal{F})$ によって置換されるため，Π は次のように絞られる．

$$\Pi \subseteq \{\underbrace{\mathsf{id}, (1\,2), (3\,4), (1\,2)(3\,4)}_{♡♡♣♣ \mapsto ♡♡♣♣}, \underbrace{(1\,3)(2\,4), (1\,3\,4\,2), (1\,4)(2\,3), (1\,4\,2\,3)}_{♡♡♣♣ \mapsto ♣♣♡♡}\}$$

さらに補題 1 の最後の方で示したように，任意の $\pi \in \Pi$ は $\pi(1) = 4$ もしくは $\pi(1) = 1$ であるため，$\Pi \subseteq \{\mathsf{id}, (3\,4), (1\,4)(2\,3), (1\,4\,2\,3)\}$ である．Π は必ず id を含み，また $(1\,4)(2\,3)$ もしくは $(1\,4\,3\,2)$ を含まなければ ♡♡♣♣ ↦ ♣♣♡♡ とならないため，Π は次の 6 つとなる．

$$\begin{aligned}\Pi = \{&\mathsf{id}, (1\,4)(2\,3)\}, \{\mathsf{id}, (1\,4\,2\,3)\},\\ &\{\mathsf{id}, (1\,4)(2\,3), (1\,4\,2\,3)\}, \{\mathsf{id}, (3\,4), (1\,4)(2\,3)\},\\ &\{\mathsf{id}, (3\,4), (1\,4\,2\,3)\}, \{\mathsf{id}, (3\,4), (1\,4)(2\,3), (1\,4\,2\,3)\} \quad (8)\end{aligned}$$

これより本補題は証明された． □

定理 5 を証明する準備が整った．

定理 5 の証明. 補題 1 と補題 2 より，任意の 4 枚コミット型 AND プロトコルにおけるループは，図 3 に一般化され，式 (8) より，$p_1 + p_2 + p_3 + p_4 = 1$ 満たす各記号を用いて $\mathcal{F}$ を次のように定める．

$$\mathcal{F}\colon \mathsf{id} \mapsto p_1, (3\,4) \mapsto p_2, (1\,4)(2\,3) \mapsto p_3, (1\,4\,2\,3) \mapsto p_4$$

これを適用した結果，次の状態が得られる．

♡♣♡♣	$(qp_1 + (1-q)p_2)X_0$
♡♣♣♡	$((1-q)p_1 + qp_2 + (1-q)p_3 + qp_4)X_0$
♣♡♣♡	$(qp_3 + (1-q)p_4)X_0$
♡♡♣♣	$(p_1 + p_2)X_1$
♣♣♡♡	$(p_3 + p_4)X_1$

ここで $p_3 + p_4$ がループを抜け出し終了状態に遷移する確率である．式 (3) より，次式が成り立つ．

$$\begin{aligned}&p_3 + p_4 = qp_1 + (1-q)p_2\\ \Rightarrow &1 - (p_1 + p_2) = qp_1 + (1-q)p_2\\ \Rightarrow &p_3 + p_4 < 1/2 \quad \because q \in (0,1)\end{aligned}$$

これより本定理は証明された． □

また式 (8) より，終了するためには非実用的なシャッフルを必要とすることを証明でき，これは [5] で得られた結果の別証明である．式 (8) を見ると，Π が群を成すのは $\Pi = \{\mathsf{id}, (1\,4)(2\,3)\}$ のみであり，$p_2 = p_4 = 0$ とすると，式 (3) より次式が得られる．

$$p_3 = qp_1 \Rightarrow p_3 \neq p_1$$

したがって非一様シャッフルとなり，実用的とされている一様閉シャッフルでは終了できないことが示される．

4.3 より詳細な検討

定理 4 と定理 5 より，任意の 4 枚コミット型 AND におけるシャッフル回数の期待値は 3 より大きいことが示される．定理 2 を証明するためには，2,3 回目のシャッフル操作で終了する確率を $1/2$ よりもタイトに抑えることが必要であるが，スペースの都合上証明は省略する．

謝辞 本研究は JSPS 科研費 JP23H00479 の助成を一部受けている．

参考文献

[1] C. Crépeau and J. Kilian. In *Advances in Cryptology—CRYPTO' 93*, volume 773 of *LNCS*, pages 319–330, Berlin, Heidelberg, 1994. Springer.
[2] S. Iino, S. Ikeda, K. Shinagawa, Y. Li, K. Sakiyama, and D. Miyahara. In *Cryptology and Network Security*, LNCS, Singapore, 2025. Springer.
[3] J. Kastner, A. Koch, S. Walzer, D. Miyahara, Y. Hayashi, T. Mizuki, and H. Sone. In *Advances in Cryptology—ASIACRYPT 2017*, volume 10626 of *LNCS*, pages 126–155, Cham, 2017. Springer.
[4] A. Koch. *Cryptographic Protocols from Physical Assumptions*. PhD thesis, Karlsruhe Institute of Technology, 2019.
[5] A. Koch. In *IEEE Information Theory Workshop*, pages 1–6, NY, 2021. IEEE.
[6] A. Koch, S. Walzer, and K. Härtel. In *Advances in Cryptology—ASIACRYPT 2015*, volume 9452 of *LNCS*, pages 783–807, Berlin, Heidelberg, 2015. Springer.
[7] K. Miyamoto and K. Shinagawa. Graph automorphism shuffles from pile-scramble shuffles. *New Gener. Comput.*, 40:199–223, 2022.
[8] T. Mizuki. Special issue on card-based cryptography 3. *New Generation Computing*, 42(3):303–304, 2024.
[9] T. Mizuki, M. Kumamoto, and H. Sone. In *Advances in Cryptology—ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 598–606, Berlin, Heidelberg, 2012. Springer.
[10] T. Mizuki and H. Shizuya. A formalization of card-based cryptographic protocols via abstract machine. *Int. J. Inf. Secur.*, 13(1):15–23, 2014.
[11] T. Mizuki and H. Sone. In *Frontiers in Algorithmics*, volume 5598 of *LNCS*, pages 358–369, Berlin, Heidelberg, 2009. Springer.
[12] T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone. In *Theory and Applications of Models of Computation*, volume 9076 of *LNCS*, pages 110–121, Cham, 2015. Springer.