Computer Security Symposium 2019
21 - 24 October 2019

ランダムカットのみを用いるコミット型ANDプロトコルの改良と枚数削減不可能性

阿部 勇太[1,a)]　水木 敬明[2]　曽根 秀昭[2]

概要：カードベース暗号において，コミット型 AND プロトコルを設計することが主要なテーマの一つである．本研究では，ランダムカットと呼ばれるシャッフルのみを用いたコミット型 AND プロトコルについて考える．著者らは先行研究として，6 枚のカードで行えるプロトコルを提案した．このプロトコルでは，シャッフルが平均 8 回必要であった．本稿では，これを改良し，有限 2 回のプロトコルを新たに提案する．また，カード枚数について，4 枚のプロトコルは存在しないことが証明されているが，5 枚のプロトコルが存在するか否かについては，未解決問題である．そこで，5 枚での構成の不可能性を証明することで，この問題を解決する．

Improved Committed AND Protocol Using Only Random Cut and Impossibility of Reducing the Number of Cards

Yuta Abe[1,a)]　Takaaki Mizuki[2]　Hideaki Sone[2]

Abstract: In card-based cryptography, designing AND protocols in committed format is a major topic. In this study, we focus on committed AND protocols using only random cuts as shuffles. In our previous study, we proposed a protocol that can be executed with six cards. This protocol needs eight shuffles on average. To improve this, we propose a new protocol that uses exactly two shuffles. In addition, regarding the number of cards, it was proved that a committed AND protocol using only random cuts with four cards does not exist. However, it is an open problem whether there is a protocol with five cards. We solve this problem by proving the impossibility of designing a five-card protocol.

1. はじめに

身近な道具を用いて秘密計算を実現する方法として，カードベース暗号プロトコルがある．カードベース暗号では，裏面が ? であり，表面が ♣ または ♡ である 2 種類のカードを用いる．このカードを用いて次のようにブール値を表す．

$$\boxed{\clubsuit}\boxed{\heartsuit} = 0,\ \boxed{\heartsuit}\boxed{\clubsuit} = 1$$

この符号化ルールに従って，裏返しに置かれたカード 2 枚を，コミットメントと呼ぶ．

[1] 東北大学大学院情報科学研究科
Graduate School of Information Sciences, Tohoku University
[2] 東北大学サイバーサイエンスセンター
Cyberscience Center, Tohoku University
[a)] yuta.abe.r6@dc.tohoku.ac.jp

$$\underbrace{\boxed{?}\boxed{?}}_{\text{コミットメント}}$$

コミットメントで入出力を行い，論理積を秘密計算するプロトコルをコミット型 AND プロトコルという．

1.1 ランダムカット

カードベース暗号プロトコルを構築するうえで，カードをシャッフルする操作を取り入れることが必要不可欠である．その場合，“ランダムカット” と呼ばれるシャッフルがしばしば用いられる．ランダムカットとは，対象のカード列を，ランダムな回数だけ巡回的にシフトさせるシャッフルである．厳密にいえば，次のように定義できる．

定義 1 σ を $\{1, 2, \cdots, n\}$ 上の巡回置換とする．巡回群

$$\Pi = \langle\sigma\rangle = \{\sigma^i | 1 \leqq i \leqq n\}$$

から一様ランダムに選ばれる置換 π をカード列に対し適用する操作のことを，ランダムカットと呼び，RC_σ と表記することにする．

実際に，人間がランダムカットを実装するための手順は次のとおりである．以下，生成元を $\sigma = (i_1\, i_2\, \ldots\, i_n)$ として，RC_σ を実装したいとする．

(1) カード列の左から i_1 枚目，i_2 枚目，・・・，i_n 枚目の順にカードを取って積み上げていく．

(2) 出来たカード束に対し，Hindu cut [1] を適用する．すなわち，次の操作を十分なランダム回数素早く行う．
- 下から何枚かを抜き出し，上に重ねる．

(3) カード束の上から順に，左から i_n 枚目，i_{n-1} 枚目，・・・，i_1 枚目に戻す．

ランダムカットは人間が手で簡単に行える．さらに，人間が安全に実現できることが実験的に確認されている [1]．

本研究では，ランダムカットのみを用いたコミット型 AND プロトコルに焦点を当てる．

1.2 既存の研究と本稿の貢献

ランダムカットのみを用いたコミット型 AND プロトコルは，表 1 に記載する通り過去にいくつも提案されてきた．1993 年に Crépeau らが考案したもの [2] は 4 色 10 枚

表 1 シャッフルとしてランダムカットのみを使ったコミット型 AND プロトコルと存在不可能性

	カード		シャッフル	有限
	色数	枚数	回数（期待値）	
Crépeau–Kilian, 1993 [2]	4	10	8	
Niemi–Renvall, 1998 [3]	2	12	7.5	
Stiglic, 2001 [4]	2	8	2	
阿部・水木・曽根, 2019 [5]	2	6	8	
本稿（3 節）	2	6	2	✓
存在しない（4 節）	2	5	*	*
存在しない, Koch ら, 2017 [6]	2	4	*	*

ものカードを必要としたが，それを減らしていく研究がなされ，最近著者らが提案したプロトコル [5]（表 1 の上から 4 行目）では 2 色 6 枚のカードで行えるまでになった．

しかし，そのプロトコルは平均 8 回のシャッフルを必要とし，一つ前のもの [4] と比べ大きく増えてしまっている．本稿では，このプロトコル [5] を改良することで，シャッフル回数を 2 回まで減らす（表 1 の上から 5 行目）．

表 1 の既存プロトコルは全て非有限，つまりラスベガスアルゴリズムであった．今回提案するプロトコルは初めての有限プロトコルであり，必ずシャッフル 2 回で終了する．

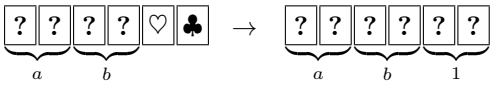
さらに，必要カード枚数を 6 枚から削減することが不可能であることを証明する（表 1 の下から 2 行目）．なお，4 枚では不可能なことは知られていた [6]（表 1 の下から 1 行目）ので，5 枚で不可能なことを本稿で初めて示したことになる．

2. 既存プロトコル

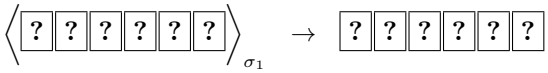
本節では，先行研究として，著者らが以前提案したランダムカットのみ用いたコミット型 AND プロトコル [5] を紹介する．a と b のコミットメント及び 2 枚の追加カードを入力として，$a \wedge b$ のコミットメント

を出力するものである．次の節で提案する新しいプロトコルの説明のために，細部を変更して紹介するが，大まかな流れは変わらない．

(1) 2 つの入力コミットメントの右に追加カードを置き，裏返す．

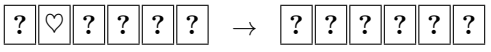


(2) 生成元 $\sigma_1 = (1\,2\,4\,6\,3\,5)$ として，ランダムカット RC_{σ_1}（$\langle\cdot\rangle_{\sigma^1}$ で表す）を，カード列に適用する．



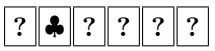
(3) 左から 2 枚目をめくる．

(a) ♡ が出たら，これを裏にし，



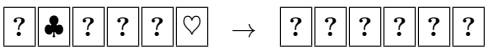
ステップ (2) へ戻る．

(b) ♣ が出たら，



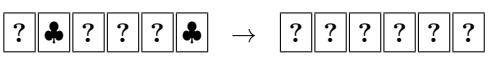
続けて，左から 6 枚目をめくる．（この ♣ が出る確率は 1/2 である．）

(i) ♡ が出たら，全て裏にし，



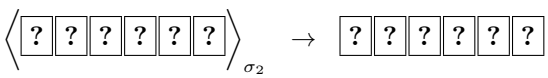
ステップ (2) へ戻る

(ii) ♣ が出たら，全て裏にし，



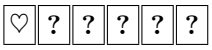
次のステップ (4) へ進む．（この ♣ が出る確率は 1/3 である．）

(4) 生成元 $\sigma_2 = (1\,2\,6\,3\,4\,5)$ として，ランダムカット RC_{σ_2} を，カード列に適用する．



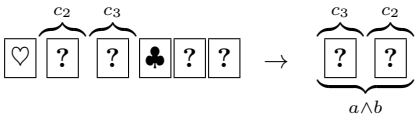
(5) 左から 1 枚目をめくる．

(a) ♡ が出たら，

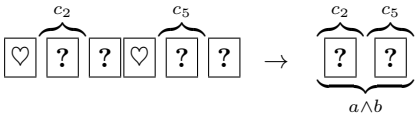


続けて，左から 4 枚目をめくる．（この ♡ が出る確率は 1/2 である．）

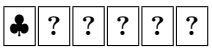
(i) ♣ が出たら，左から 3 枚目のカード c_3 を左側，2 枚目のカード c_2 を右側に配置した 2 枚のカードが，$a \wedge b$ のコミットメントである．（この ♣ が出る確率は 2/3 である．）



(ii) ♡ が出たら，左から 2 枚目，5 枚目のカードが，$a \wedge b$ のコミットメントである．

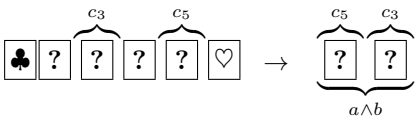


(b) ♣ が出たら，

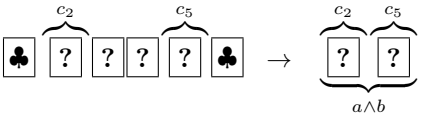


続けて，左から 6 枚目をめくる．

(i) ♡ が出たら，左から 5 枚目，3 枚目のカードが，$a \wedge b$ のコミットメントである．（この ♡ が出る確率は 2/3 である．）



(ii) ♣ が出たら，左から 2 枚目，5 枚目のカードが，$a \wedge b$ のコミットメントである．



以上が，以前著者らが提案した，ランダムカットのみ用いる 6 枚コミット型 AND プロトコル [5] である．

プロトコル中にループを含んでいるため，有限の回数のシャッフル（ランダムカット）では終了しないが，シャッフルの回数の期待値は 8 回と計算できる．

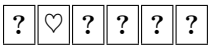
3. 提案プロトコル

本節では，2 節で紹介した既存プロトコルを改良し，より少ないシャッフル回数で実行できるプロトコルを新しく提案する．

2 節のプロトコルにおけるステップ (3)(a) とステップ (3)(b)(i) は，一つ前のステップに戻るという手順になっている．この二つのステップを，それぞれ次のように書き換える．

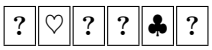
(3) 左から 2 枚目をめくる．

(a) ♡ が出たら，



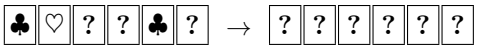
続けて，左から 5 枚目をめくる．（この ♡ が出る確率は 1/2 である．）

(i) ♣ が出たら，



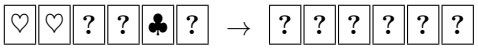
続けて，左から 1 枚目をめくる．（この ♣ が出る確率は 2/3 である．）

(A)♣ が出たら，全て裏にし，



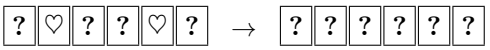
置換 (1 2 5 6 3 4) を適用して並び替え，次のステップ (4) へ進む．（この ♣ が出る確率は 1/2 である．）

(B)♡ が出たら，全て裏にし，



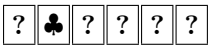
置換 (1 3 4)(2 6) を適用して並び替え，次のステップ (4) へ進む．

(ii) ♡ が出たら，全て裏にし，



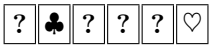
置換 (2 6 5 3) を適用して並び替え，次のステップ (4) へ進む．

(b) ♣ が出たら，



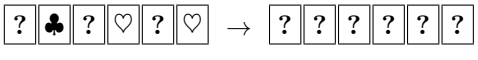
続けて，左から 6 枚目をめくる．

(i) ♡ が出たら，



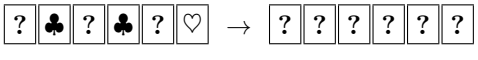
続けて，左から 4 枚目をめくる．

(A)♡ が出たら，全て裏にし，



置換 (1 4 3)(2 5) を適用して並び替え，次のステップ (4) へ進む．（この ♡ が出る確率は 1/2 である．）

(B)♣ が出たら，全て裏にし，



置換 (1 4 6 5 3) を適用して並び替え，次

のステップ (4) へ進む．

以上のように改良することで，プロトコルからループをなくし，シャッフル回数を平均 8 回から有限の 2 回に減らすことに成功した．

このプロトコルは，図 1 のような KWH-tree で描ける．KWH-tree [7] とは，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る．提案プロトコルは既存プロトコルに図 1 の状態 L〜状態 S を加えたプロトコルである．

4. カード枚数の削減不可能性

3 節ではシャッフル回数に注目したが，本節では必要なカード枚数について議論する．以降，“シャッフルとしてランダムカットのみを用いたコミット型 AND プロトコル”を “RC 限定コミット型 AND プロトコル” と呼ぶことにする．

表 1 で示されているように，現在最も少ないカード枚数で実行できる RC 限定コミット型 AND プロトコルは，著者らが提案した 6 枚のプロトコルである．よって，次の定理が成立する．

定理 1 6 枚の RC 限定コミット型 AND プロトコルが存在する．

では，必要カード枚数を 5 枚以下に削減することは可能なのだろうか．この疑問の一部を解決する定理が，Koch ら [6] によって次のように示されている．

定理 2（[6]） シャッフルとして一様で closed なもののみを用いる場合，4 枚のコミット型 AND プロトコルは存在しない．

ランダムカットは一様で closed なシャッフルであるため，定理 2 より，次の系を導くことができる．

系 1 4 枚の RC 限定コミット型 AND プロトコルは存在しない．

すなわち，定理 2 が示された時点で，4 枚で構成できないことは判明している．しかし，5 枚の RC 限定コミット型 AND プロトコルが存在するか否かは未解決問題である．

以上をふまえ，本節では，5 枚の RC 限定コミット型 AND プロトコルが存在しないことを証明する．なお，計算モデルは文献 [8] で定式化されたものを使う．

4.1 準備

図 1 から分かるように，状態はカード列 s とその発生確率 p のペア (s,p) がいくつか集まって構成されている．秘密計算では入力情報が洩れてはいけないため，次の定義を考える．

定義 2 状態内の発生確率の和が $X_{11}+X_{10}+X_{01}+X_{00}$ であるならば，その状態は安全であると言う．

この定義に基づき，次の補題が成り立つ．

補題 1 コミット型のカードベース暗号プロトコルは，プロトコル上で発生する全ての状態が安全である．

カード列 s の左から i 枚目のカードの表の模様を $s[i] \in \{\clubsuit, \heartsuit\}$ と書くことにする．これを使って，コミット型 AND プロトコルにおける終了状態を次のように定義する．

定義 3 q を安全な状態とする．ある整数 i,j があり，任意のカード列 s とその発生確率 p のペア $(s,p) \in q$ について，次の命題がともに真であるとき，q を終了状態と呼ぶ．

- p が X_{11} を含むならば $(s[i],s[j]) = (\heartsuit,\clubsuit)$
- p が X_{11} 以外の変数 (X_{10}, X_{01}あるいは X_{00}) を含むならば $(s[i],s[j]) = (\clubsuit,\heartsuit)$

X_{ab} は入力が (a,b) である確率を表しており，$X_{11}+X_{10}+X_{01}+X_{00}=1$ である．終了状態は結果のコミットメントを出力できる状態のことであるため，初期状態から終了状態へ遷移できなければプロトコルは存在しないということになる．よって，次の補題が成り立つ．

補題 2 シャッフルとしてランダムカットのみを用いた場合に，カード列が d 枚である初期状態の最終的な遷移先が全て終了状態になる，ということがないならば，d 枚の RC 限定コミット型 AND プロトコルは存在しない．

次に，準終了状態を以下のように定義する．

定義 4 q を安全な状態とする．ある確率変数 $Y \in \{X_{11}, X_{10}, X_{01}, X_{00}\}$ とある整数 i,j があり，任意のカード列 s とその発生確率 p のペア $(s,p) \in q$ について，次の命題がともに真であるとき，q を準終了状態と呼ぶ．

- p が Y を含むならば $(s[i],s[j]) = (\heartsuit,\clubsuit)$
- p が Y 以外の変数を含むならば $(s[i],s[j]) = (\clubsuit,\heartsuit)$

$Y = X_{11}$ であるような準終了状態が，終了状態となる．準終了状態の条件は終了状態の条件より弱い条件であるので，次の補題が成り立つ．

補題 3 q を状態とする．q が準終了状態でないならば，q は終了状態ではない．

また，終了状態への遷移について，次の補題が成り立つ．

補題 4 q を状態とする．任意の確率変数 $Y \in \{X_{11}, X_{10}, X_{01}, X_{00}\}$ に対して，q 内の Y を含む全ての発生確率 p が，Y 以外の変数を含むならば，q からの最終的な遷移先が全て終了状態になる，ということはない．

4.2 証明

まずは，5 枚の初期状態から遷移可能な安全な状態をすべて挙げる．

初期状態は

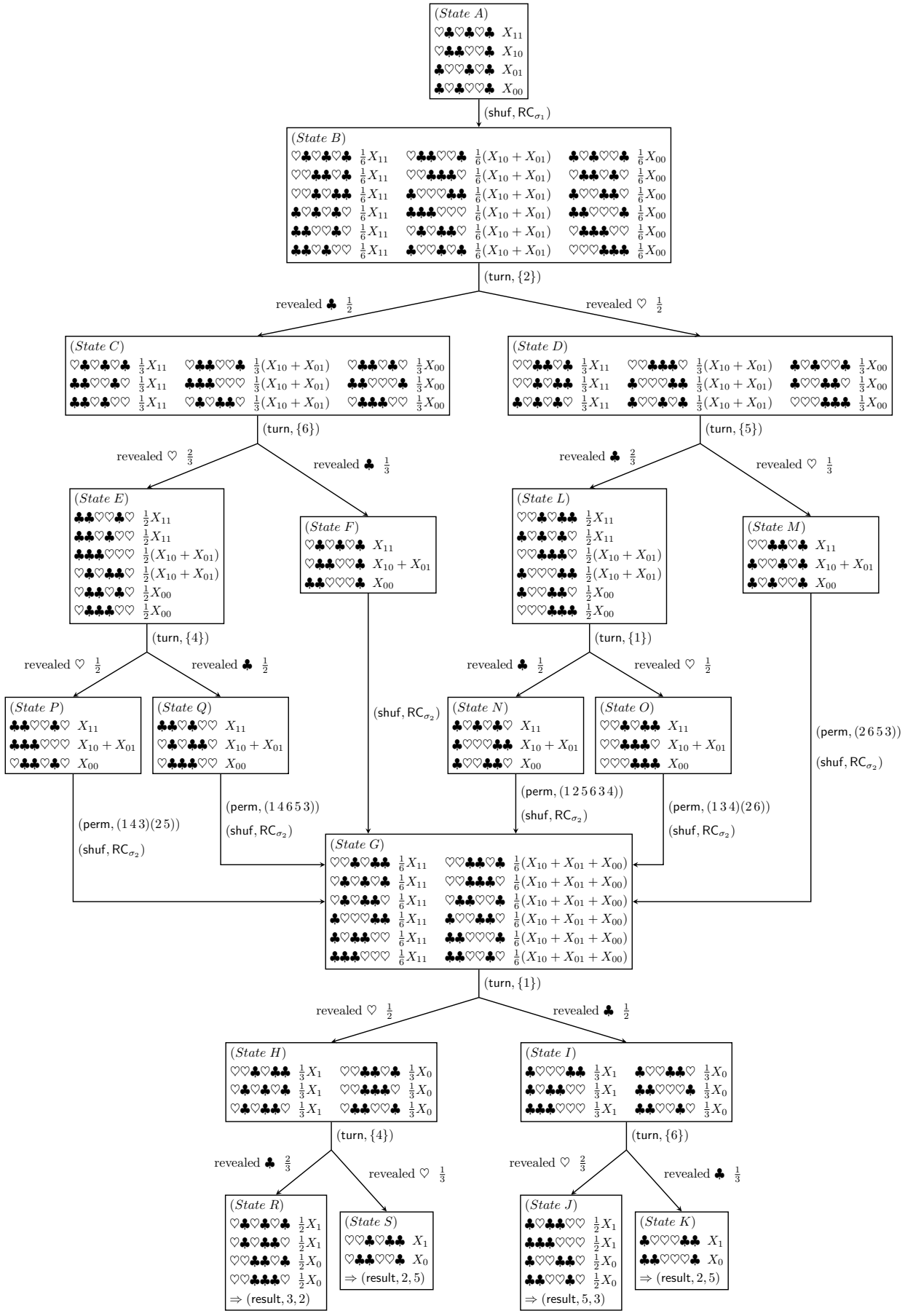


図 1 提案するランダムカットのみを用いた 6 枚コミット型 AND プロトコルの KWH-tree

$$q_1 = \{(\heartsuit\clubsuit\heartsuit\clubsuit\heartsuit, X_{11}), (\heartsuit\clubsuit\clubsuit\heartsuit\heartsuit, X_{10}),$$
$$(\clubsuit\heartsuit\heartsuit\clubsuit\heartsuit, X_{01}), (\clubsuit\heartsuit\clubsuit\heartsuit\heartsuit, X_{00})\}$$

とする．入力カード列は

$$\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}\boxed{\heartsuit} \tag{1}$$

である．

カード列の並びに関しては，次の補題が成り立つ．

補題 5 上記の状態 q_1 から準終了状態へ遷移することが不可能ならば，どんな入力カード列に対しても準終了状態に遷移しない．

すなわち，カードの並びを任意に決めても，それに対しランダムカットの生成元やめくる位置，出力とする位置を自由に設定すれば，一般性は失われない．

カード列に適用する操作としては，“シャッフル” と “めくる” だけ考える．[8] のモデルにおいては “並び替える” という操作も存在するが，補題 5 と同様の考え方により，“並び替える” 操作を行わなくてもすべての状態遷移を本質的に網羅できる．よって “並び替える” 操作は考えない．

また，状態 q と q に置換操作を加えてできる状態 q' がどちらも現れるとき，補題 5 と同様の考え方により，q' は q としても扱えるので，q' へ遷移する状態はかわりに q へ遷移することとする．

以上を踏まえて，初期状態 q_1 からの状態遷移は図 2 のように描ける．ノード Q_2〜Q_{33} は状態の集合を表し，そこへ遷移する場合には集合のいずれかの要素に遷移する．Q_2〜Q_{33} が具体的にどのような集合かは付録 A.1 にて記す．

上に数字が書かれているエッジは，その番号に対応するランダムカットを適用したときの遷移を表している．5 枚のカードに対するランダムカットは恒等置換を除いて 84 種類あり，それぞれに 1 から 84 の番号を振っている．具体的にどの番号がどんなランダムカットを表しているかは付録 A.2 で記す．$i \in \{1,2,3,4,5\}, f \in \{\heartsuit, \clubsuit\}$ なる $s[i] = f$ が書かれているエッジは，i 枚目をめくって模様 f が出たときの遷移を表している．

図 2 のどの状態を見ても，全ての操作が適用されているわけではない．これは，補題 1 より，安全でない状態へ遷移する操作は省略しているからである．また，補題 4 の条件を満たす状態も省略している．

図 2 で描かれている状態はすべて準終了状態でないので，補題 3 より，初期状態 q_1 の最終的な遷移先が全て終了状態になる，ということはない．よって，補題 2 より，5 枚の RC 限定コミット型 AND プロトコルは存在しないことが示される．したがって，6 枚の RC 限定コミット型 AND プロトコルから，さらにカード枚数を減らすことは不可能である．

5. おわりに

本稿では，著者らが以前提案したプロトコル [5] を改良し，シャッフル回数を有限の 2 回に減らすことに成功した．さらに，必要なカード枚数を 5 枚以下に削減することが不可能であり，カード枚数において 6 枚使う著者らの提案プロトコルが最適であることを証明した．

参考文献

[1] I. Ueda, A. Nishimura, Y. Hayashi, T. Mizuki and H. Sone, “How to Implement a Random Bisection Cut,” Theory and Practice of Natural Computing, Lecture Notes in Computer Science, Vol. 10071, p.58–69, 2016.

[2] C. Crépeau and J. Kilian, “Discreet Solitary Games,” CRYPTO ’93, Lecture Notes in Computer Science, Vol. 773, p.319–330, 1994.

[3] V. Niemi and A. Renvall, “Secure multiparty computations without computers,” In Theoretical Computer Science, Vol. 191, p.173–183, 1998.

[4] A. Stiglic, “Computations with a deck of cards,” In Theoretical Computer Science, Vol. 259, p.671–678, 2015.

[5] 阿部 勇太，水木 敬明，曽根 秀昭，“ランダムカットのみ用いる 6 枚コミット型 AND プロトコル”，2019 年電子情報通信学会ソサイエティ大会，2019.

[6] J. Kastner, A. Koch, S. Walzer, D. Miyahara, Y. Hayashi, T. Mizuki and H. Sone, “The Minimum Number of Cards in Practical Card-Based Protocols,” ASIACRYPT 2017, Lecture Notes in Computer Science, vol 10626, pp 126–155, 2017.

[7] A. Koch, S. Walzer, and K. Härtel, “Card-based cryptographic protocols using a minimal number of cards,” ASIACRYPT 2015, Lecture Notes in Computer Science, Vol. 9452, p.783–807, 2015.

[8] T. Mizuki and H. Shizuya, “A formalization of card-based cryptographic protocols via abstract machine,” International Journal of Information Security, Vol. 13, p.15–23, 2014.

付　　録

A.1 状態集合 Q_2〜Q_{33} について

4 節で出てきた Q_2〜Q_{33} は次のような状態集合である．ここで，4 次の対称群 S_4 の要素 $\pi \in S_4$ と任意の 4 項組 (Z_1, Z_2, Z_3, Z_4) に対して $\pi(Z_1, Z_2, Z_3, Z_4) = (Z_{\pi^{-1}(1)}, Z_{\pi^{-1}(2)}, Z_{\pi^{-1}(3)}, Z_{\pi^{-1}(4)})$ とする．

$$Q_t = \bigcup_{(Y_0,Y_1,Y_2,Y_3)=\pi(X_{11},X_{10},X_{01},X_{00}),\pi\in S_4} q_t(Y_0, Y_1, Y_2, Y_3)$$

ただし

$$\alpha = \heartsuit\heartsuit\heartsuit\clubsuit\clubsuit,\ \beta = \heartsuit\heartsuit\clubsuit\heartsuit\clubsuit,\ \gamma = \heartsuit\heartsuit\clubsuit\clubsuit\heartsuit,\ \delta = \heartsuit\clubsuit\heartsuit\heartsuit\clubsuit$$
$$\epsilon = \heartsuit\clubsuit\heartsuit\clubsuit\heartsuit,\ \zeta = \heartsuit\clubsuit\clubsuit\heartsuit\heartsuit,\ \eta = \clubsuit\heartsuit\heartsuit\heartsuit\clubsuit,\ \theta = \clubsuit\heartsuit\heartsuit\clubsuit\heartsuit$$
$$\iota = \clubsuit\heartsuit\clubsuit\heartsuit\heartsuit,\ \kappa = \clubsuit\clubsuit\heartsuit\heartsuit\heartsuit$$

とする．また，Y_0, Y_1, Y_2, Y_3 をパラメータとして $2 \leqq i \leqq 33$ なる $q_i(Y_0, Y_1, Y_2, Y_3)$ を次のように定義する．

$$q_2 = \{\{(\gamma, Y_0/2), (\epsilon, Y_1), (\zeta, Y_2/2), (\theta, Y_0/2), (\iota, Y_3), (\kappa, Y_2/2)\}\}$$
$$q_3 = \{\{(\alpha, Y_0/2), (\beta, Y_1/2), (\epsilon, Y_2), (\zeta, Y_3), (\theta, Y_0/2), (\iota, Y_1/2)\}\}$$
$$q_4 = \{\{(\alpha, Y_0/3), (\beta, Y_1/3), (\gamma, Y_0/3), (\delta, Y_2/3), (\epsilon, Y_3),$$
$$(\zeta, Y_2/3), (\eta, Y_1/3), (\theta, Y_0/3), (\iota, Y_1/3), (\kappa, Y_2/3)\}\}$$

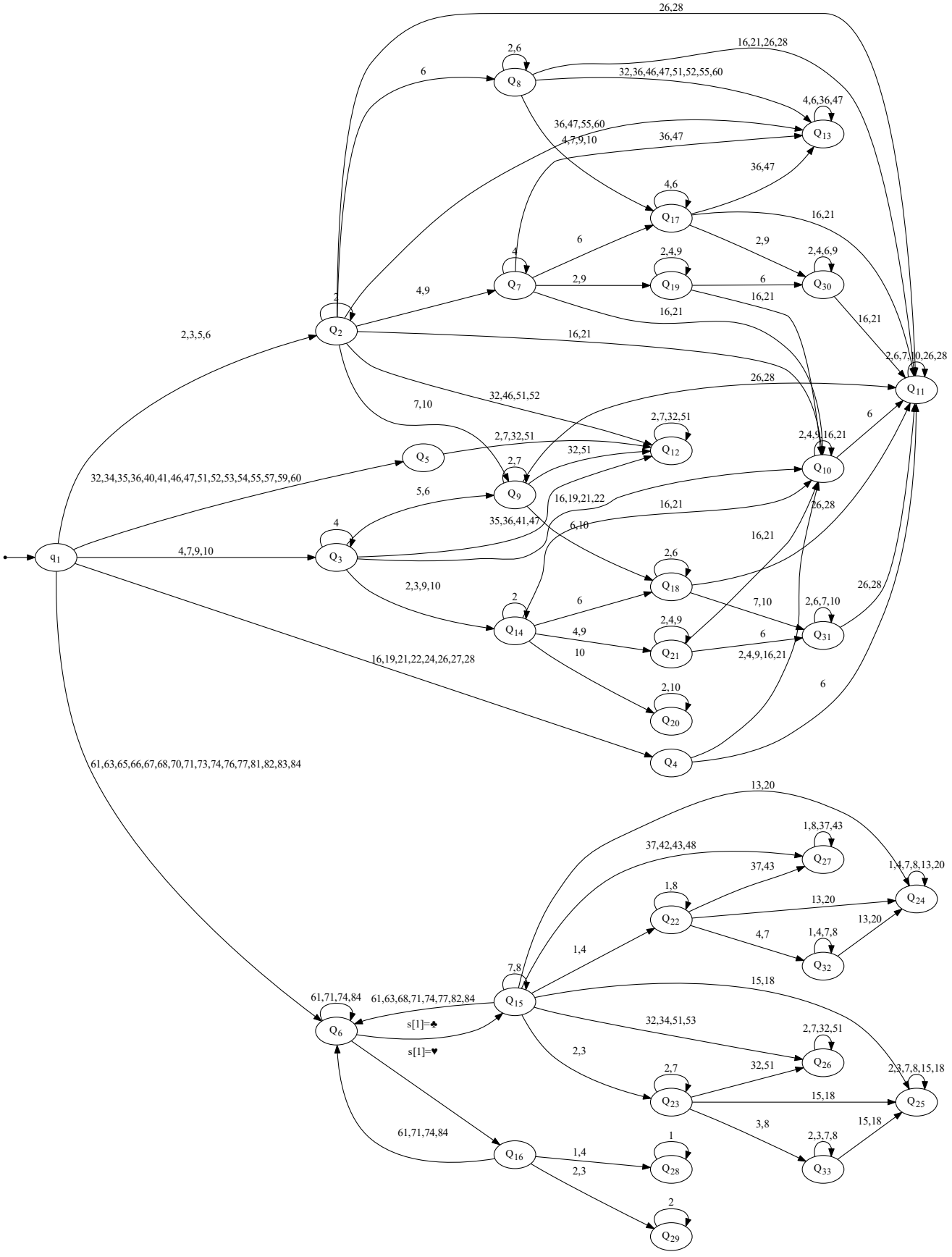


図 2　初期状態 q_1 からの状態遷移

$$
\begin{aligned}
q_5 =&\{\{(\alpha,(Y_0+Y_1)/4),(\beta,Y_2/4),(\gamma,(Y_0+Y_1)/4),\\
&(\delta,Y_3/2),(\epsilon,(Y_0+Y_1)/4),(\zeta,Y_2/4),(\eta,Y_2/4),\\
&(\theta,(Y_0+Y_1)/4),(\iota,Y_3/2),(\kappa,Y_2/4)\}\}\\
q_6 =&\{\{(\alpha,Y_0/5),(\beta,(Y_1+Y_2+Y_3)/5),(\gamma,Y_0/5),\\
&(\delta,(Y_1+Y_2+Y_3)/5),(\epsilon,(Y_1+Y_2+Y_3)/5),\\
&(\zeta,Y_0/5),(\eta,Y_0/5),(\theta,(Y_1+Y_2+Y_3)/5),\\
&(\iota,(Y_1+Y_2+Y_3)/5),(\kappa,Y_0/5)\}\}\\
q_7 =&\{\{(\alpha,Y_0/4),(\beta,Y_1/2),(\gamma,Y_0/2),(\delta,Y_2/4),(\epsilon,Y_3),\\
&(\zeta,Y_2/2),(\theta,Y_0/4),(\iota,Y_1/2),(\kappa,Y_2/4)\}\}\\
q_8 =&\{\{(\gamma,(Y_0+Y_1)/4),(\epsilon,Y_2),(\zeta,(Y_0+Y_1)/4),\\
&(\theta,(Y_0+Y_1)/4),(\iota,Y_3),(\kappa,(Y_0+Y_1)/4)\}\}\\
q_9 =&\{\{(\alpha,Y_0/2),(\beta,Y_1/4),(\gamma,Y_2/2),(\epsilon,Y_0/2),\\
&(\zeta,Y_1/4),(\eta,Y_1/4),(\theta,Y_2/2),(\iota,Y_3),(\kappa,Y_1/4)\}\}\\
q_{10} =&\{\{(\alpha,Y_0/3),(\beta,Y_1/3),(\gamma,Y_0/3),(\delta,Y_2/3),(\epsilon,Y_3),\\
&(\zeta,Y_2/3),(\eta,Y_1/3),(\theta,Y_0/3),(\iota,Y_1/3),(\kappa,Y_2/3)\}\}\\
q_{11} =&\{\{(\alpha,Y_0/3),(\beta,(Y_1+Y_2)/6),(\gamma,(Y_1+Y_2)/6),\\
&(\delta,Y_0/3),(\epsilon,Y_0/3),(\zeta,(Y_1+Y_2)/6),(\eta,(Y_1+Y_2)/6),\\
&(\theta,(Y_1+Y_2)/6),(\iota,Y_3),(\kappa,(Y_1+Y_2)/6)\}\}\\
q_{12} =&\{\{(\alpha,(Y_0+Y_1)/4),(\beta,Y_2/4),(\gamma,(Y_0+Y_1)/4),\\
&(\delta,Y_3/2),(\epsilon,(Y_0+Y_1)/4),(\zeta,Y_2/4),(\eta,Y_2/4),\\
&(\theta,(Y_0+Y_1)/4),(\iota,Y_3/2),(\kappa,Y_2/4)\}\}\\
q_{13} =&\{\{(\alpha,(Y_0+Y_1)/8),(\beta,(Y_0+Y_1+2Y_2)/8),\\
&(\gamma,(Y_0+Y_1+2Y_2)/8),(\delta,(Y_0+Y_1)/8),(\epsilon,Y_3/2),\\
&(\zeta,(Y_0+Y_1+2Y_2)/8),(\eta,Y_3/2),(\theta,(Y_0+Y_1)/8),\\
&(\iota,(Y_0+Y_1+2Y_2)/8),(\kappa,(Y_0+Y_1)/8)\}\}\\
q_{14} =&\{\{(\alpha,Y_0/2),(\beta,Y_1/4),(\gamma,Y_0/4),(\epsilon,Y_2),(\zeta,Y_3/2),\\
&(\eta,Y_1/4),(\theta,Y_0/4),(\iota,Y_1/2),(\kappa,Y_3/2)\}\}\\
q_{15} =&\{\{(\eta,Y_0/2),(\theta,(Y_1+Y_2+Y_3)/2),\\
&(\iota,(Y_1+Y_2+Y_3)/2),(\kappa,Y_0/2)\}\}\\
q_{16} =&\{\{(\alpha,Y_0/3),(\beta,(Y_1+Y_2+Y_3)/3),(\gamma,Y_0/3),\\
&(\delta,(Y_1+Y_2+Y_3)/3),(\epsilon,(Y_1+Y_2+Y_3)/3),(\zeta,Y_0/3)\}\}\\
q_{17} =&\{\{((\alpha,(Y_0+Y_1)/8),(\beta,Y_2/2),(\gamma,(Y_0+Y_1)/4),\\
&(\delta,(Y_0+Y_1)/8),(\epsilon,Y_3),(\zeta,(Y_0+Y_1)/4),\\
&(\theta,(Y_0+Y_1)/8),(\iota,Y_2/2),(\kappa,(Y_0+Y_1)/8)\}\}\\
q_{18} =&\{\{(\alpha,Y_0/4),(\beta,Y_1/4),(\gamma,(Y_1+2Y_2)/8),(\delta,Y_0/4),\\
&(\epsilon,Y_0/2),(\zeta,(Y_1+2Y_2)/8),(\eta,Y_1/4),\\
&(\theta,(Y_1+2Y_2)/8),(\iota,Y_3),(\kappa,(Y_1+2Y_2)/8)\}\}\\
q_{19} =&\{q(i,j,k)|i,j,k\geqq 0,\\
&q(0,0,0)=\{(\alpha,Y_0/4),(\beta,Y_1/4),(\gamma,3Y_0/8),(\delta,Y_2/4),(\epsilon,Y_3),\\
&(\zeta,3Y_2/8),(\eta,Y_1/4),(\theta,3Y_0/8),(\iota,Y_1/2),(\kappa,3Y_2/8)\},\\
&q(i,j,k)=\mathsf{RC}_{(1\,3)}(q(i-1,j,k)),\\
&q(i,j,k)=\mathsf{RC}_{(1\,5)}(q(i,j-1,k)),\\
&q(i,j,k)=\mathsf{RC}_{(3\,5)}(q(i,j,k-1))\}\\
q_{20} =&\{\{(\alpha,Y_0/2),(\beta,(Y_0+Y_1)/8),(\gamma,(Y_0+Y_1)/8),(\delta,Y_2/2),\\
&(\epsilon,Y_2/2),(\zeta,Y_3/2),(\eta,(Y_0+Y_1)/8),\\
&(\theta,(Y_0+Y_1)/8),(\iota,Y_1/2),(\kappa,Y_3/2)\}\}\\
q_{21} =&\{q(i,j,k)|i,j,k\geqq 0,\\
&q(0,0,0)=\{(\alpha,3Y_0/8),(\beta,3Y_1/8),(\gamma,Y_0/4),(\delta,Y_2/4),(\epsilon,Y_3),\\
&(\zeta,Y_2/2),(\eta,Y_1/4),(\theta,3Y_0/8),(\iota,3Y_1/8),(\kappa,Y_2/4)\},\\
&q(i,j,k)=\mathsf{RC}_{(1\,3)}(q(i-1,j,k)),\\
&q(i,j,k)=\mathsf{RC}_{(1\,5)}(q(i,j-1,k)),\\
&q(i,j,k)=\mathsf{RC}_{(3\,5)}(q(i,j,k-1))\}\\
q_{22} =&\{\{(\delta,Y_0/4),(\epsilon,(Y_1+Y_2+Y_3)/4),(\zeta,(Y_1+Y_2+Y_3)/4),\\
&(\eta,Y_0/4),(\theta,(Y_1+Y_2+Y_3)/4),(\iota,(Y_1+Y_2+Y_3)/4),\\
&(\kappa,Y_0/2)\}\}\\
q_{23} =&\{\{(\beta,Y_0/4),(\gamma,(Y_1+Y_2+Y_3)/4),(\zeta,Y_0/4),(\eta,Y_0/4),\\
&(\theta,(Y_1+Y_2+Y_3)/4),(\iota,(Y_1+Y_2+Y_3)/2),(\kappa,Y_0/4)\}\}\\
q_{24} =&\{\{(\alpha,(Y_0+Y_1+Y_2)/6),(\beta,(Y_0+Y_1+Y_2)/6),(\delta,Y_3/3),\\
&(\epsilon,(Y_0+Y_1+Y_2)/6),(\zeta,(Y_0+Y_1+Y_2)/6),(\eta,Y_3/3),\\
&(\theta,(Y_0+Y_1+Y_2)/6),(\iota,(Y_0+Y_1+Y_2)/6),(\kappa,Y_3/3)\}\}\\
q_{25} =&\{\{(\alpha,Y_0/6),(\beta,Y_0/6),(\gamma,(Y_1+Y_2+Y_3)/3),(\epsilon,Y_0/6),\\
&(\zeta,Y_0/6),(\eta,Y_0/6),(\theta,(Y_1+Y_2+Y_3)/3),\\
&(\iota,(Y_1+Y_2+Y_3)/3),(\kappa,Y_0/6)\}\}\\
q_{26} =&\{\{(\alpha,(Y_0+Y_1+Y_2)/8),(\beta,Y_3/4),(\gamma,(Y_0+Y_1+Y_2)/8),\\
&(\delta,(Y_0+Y_1+Y_2)/4),(\epsilon,(Y_0+Y_1+Y_2)/8),(\zeta,Y_3/4),\\
&(\eta,Y_3/4),(\theta,(Y_0+Y_1+Y_2)/8),(\iota,(Y_0+Y_1+Y_2)/4),\\
&(\kappa,Y_3/4)\}\}\\
q_{27} =&\{\{(\alpha,Y_0/8),(\beta,Y_0/8),(\gamma,Y_0/4),(\delta,Y_0/8),\\
&(\epsilon,(Y_1+Y_2+Y_3)/4),(\zeta,(Y_1+Y_2+Y_3)/4),(\eta,Y_0/8),\\
&(\theta,(Y_1+Y_2+Y_3)/4),(\iota,(Y_1+Y_2+Y_3)/4),(\kappa,Y_0/4)\}\}\\
q_{28} =&\{\{(\alpha,Y_0/3),(\beta,(Y_1+Y_2+Y_3)/3),(\gamma,Y_0/3),\\
&(\delta,(Y_1+Y_2+Y_3)/6),(\epsilon,(Y_1+Y_2+Y_3)/6),(\zeta,Y_0/6),\\
&(\eta,(Y_1+Y_2+Y_3)/6),(\theta,(Y_1+Y_2+Y_3)/6),(\iota,Y_0/6)\}\}\\
q_{29} =&\{\{(\alpha,Y_0/3),(\beta,(Y_1+Y_2+Y_3)/6),(\gamma,Y_0/6),\\
&(\delta,(Y_1+Y_2+Y_3)/3),(\epsilon,(Y_1+Y_2+Y_3)/3),(\zeta,Y_0/6),\\
&(\eta,(Y_1+Y_2+Y_3)/6),(\theta,Y_0/6),(\kappa,Y_0/6)\}\}\\
q_{30} =&\{q(i,j,k,l)|i,j,k,l\geqq 0,\\
&q(0,0,0,0)=\{(\alpha,(Y_0+Y_1)/8),(\beta,Y_2/4),(\gamma,(3Y_0+3Y_1)/16),\\
&(\delta,(Y_0+Y_1)/8),(\epsilon,Y_3),(\zeta,(3Y_0+3Y_1)/16),\\
&(\eta,Y_2/4),(\theta,(3Y_0+3Y_1)/16),(\iota,Y_2/2),\\
&(\kappa,(3Y_0+3Y_1)/16)\},\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,3)}(q(i-1,j,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,5)}(q(i,j-1,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(2\,4)}(q(i,j,k-1,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(3\,5)}(q(i,j,k.l-1))\}\\
q_{31} =&\{q(i,j,k,l)|i,j,k,l\geqq 0,\\
&q(0,0,0,0)=\{(\alpha,3Y_0/8),(\beta,(3Y_1+2Y_2)/16),\\
&(\gamma,(Y_1+2Y_2)/8),(\delta,Y_0/4),(\epsilon,3Y_0/8),\\
&(\zeta,(3Y_1+2Y_2)/16),(\eta,(3Y_1+2Y_2)/16),\\
&(\theta,(Y_1+2Y_2)/8),(\iota,Y_3),(\kappa,(3Y_1+2Y_2)/16)\},\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,3)}(q(i-1,j,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(2\,4)}(q(i,j-1,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(2\,5)}(q(i,j,k-1,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(4\,5)}(q(i,j,k.l-1))\}\\
q_{32} =&\{q(i,j,k,l)|i,j,k,l\geqq 0,\\
&q(0,0,0,0)=\{(\alpha,(Y_0+Y_1+Y_2)/8),(\beta,(Y_0+Y_1+Y_2)/8),\\
&(\delta,3Y_3/8),(\epsilon,(Y_0+Y_1+Y_2)/4),\\
&(\zeta,(Y_0+Y_1+Y_2)/4),(\eta,Y_3/4),\\
&(\theta,(Y_0+Y_1+Y_2)/8),(\iota,(Y_0+Y_1+Y_2)/8),\\
&(\kappa,3Y_3/8)\},\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,2)}(q(i-1,j,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,5)}(q(i,j-1,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(2\,5)}(q(i,j,k-1,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(3\,4)}(q(i,j,k.l-1))\}\\
q_{33} =&\{q(i,j,k,l)|i,j,k,l\geqq 0,\\
&q(0,0,0,0)=\{(\alpha,Y_0/8),(\beta,Y_0/4),(\gamma,(3Y_1+3Y_2+3Y_3)/8),\\
&(\epsilon,Y_0/8),(\zeta,Y_0/4),(\eta,Y_0/8),\\
&(\theta,(Y_1+Y_2+Y_3)/4),(\iota,(3Y_1+3Y_2+3Y_3)/8),\\
&(\kappa,Y_0/8)\},\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,3)}(q(i-1,j,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(1\,4)}(q(i,j-1,k,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(2\,5)}(q(i,j,k-1,l)),\\
&q(i,j,k,l)=\mathsf{RC}_{(3\,4)}(q(i,j,k.l-1))\}
\end{aligned}
$$

とする．$\mathsf{RC}_\sigma(q)$ は状態 q に RC_σ を適用してできる状態を表す．

$q\in q_i$ が準終了状態でなければ，Q_i のいずれの要素も準終了状態でないことに留意する．$q_{19},q_{21},q_{30},q_{31},q_{32},q_{33}$ は，それぞれの $q(0,0,0)$ または $q(0,0,0,0)$ の発生確率の変数の係数が変化した状態の集合になるため，$q(0,0,0)$ または $q(0,0,0,0)$ が準終了状態でなければ，他の要素も準終了状態でない．

A.2 ランダムカット 1〜84 について

番号 i が割り振られているランダムカットは，次の Python3 コードで生成される sigma_list$[i-1]$ を生成元とするランダムカットである．

```
import itertools
def make_sigma_list():
  sigma_list = [ ]
  for i in range(2,6):
    lst = [list(lst) for lst in
                list(itertools.permutations(range(1,6),i))]
    for j in range(len(lst)):
      idx = lst[j].index(min(lst[j]))
      lst[j] = lst[j][idx:] + lst[j][:idx]
    seen = [ ]
    lst = [n for n in lst if n not in seen and not seen.append(n)]
    sigma_list += lst
  return sigma_list
```