カードベース暗号に現れる数学

縫田 光司

九州大学マス・フォア・インダストリ研究所

IMI 共同利用ワークショップ　2023 年 5 月 31 日

Contents

- 出力の確率分布と必要なカード枚数
- 一様閉シャッフルと巡回群シャッフル
- カードベースゼロ知識証明と秘密計算

Contents

- 出力の確率分布と必要なカード枚数
- 一様閉シャッフルと巡回群シャッフル
- カードベースゼロ知識証明と秘密計算

ランダムな対象を生成するプロトコル

- 不動点のない置換の一様ランダム生成 [Crépeau and Kilian, CRYPTO 1993]
- 秘匿グループ分け [Hashimoto et al., ICITS 2017]
- …

不動点のない置換の一様ランダム生成

- Las Vegas プロトコル [CK93; Ishikawa–Chida–Mizuki, UCNC 2015; Ibaraki–Manabe, MCIS 2016]
  - 有限時間で終わるとは限らない
  - 有限時間で打ち切る（固定の値を出力する）と、分布がわずかに偏る
- [Hashimoto et al., IEICE Trans. 2018] **有限時間プロトコル**（かつ分布が正確）のときに必要な**カード枚数**の評価
  - 一様シャッフルを仮定（後述）

Kőnig の補題とプロトコル木

定理（Kőnig の補題）

どの頂点の次数も有限である木が長さ無限の道を持たないならば、その頂点は有限個しかない。

- この補題を（各状態での分岐が有限な）プロトコル木に適用すると：
  有限時間プロトコルには**状態が有限個**しか存在しない

有限なプロトコル木での出力確率

- 有限なプロトコル木で、ある特定の出力 y が得られる確率 p_y は以下の形：

$$p_y = \sum_{\rho} \frac{n_{\rho,1}}{d_{\rho,1}} \cdot \frac{n_{\rho,2}}{d_{\rho,2}} \cdots \frac{n_{\rho,\ell_\rho}}{d_{\rho,\ell_\rho}}$$

  ここで ρ は y が出力されるような経路、$\dfrac{n_{\rho,i}}{d_{\rho,i}}$ は経路 ρ の i 番目の分岐での分岐確率（既約分数）
  - 分岐確率は有理数と仮定（後述）
- 上記は**有限和**なので、P を p_y の既約分数表示の分母の素因数とすると、ある $d_{\rho,i}$ は P を約数にもつ必要がある（**特に $d_{\rho,i} \geq P$**）

用いるシャッフルに関する仮定

- 仮定：プロトコル中の状態遷移の分岐はどれも「カード（の一部）のどれか1枚を一様ランダムに選ぶ」ことで実現される
  - ランダムカット（RC）、パイルシフティングシャッフル（PSS）、$\cdots$
  - 完全シャッフル（n 枚 RC $\to$ $n-1$ 枚 RC $\to \cdots \to$ 2 枚 RC、で実現可能）
- カード枚数 N 枚のとき、前ページの確率 $\dfrac{n_{\rho,i}}{d_{\rho,i}}$ は、ある $k \le N$ について $\dfrac{1}{k}$ の形
- $\to$ **出力確率の分母の素因数 P は常に $P \le N$** を満たす必要がある

不動点のない置換のプロトコルのカード枚数

- d_n：不動点のない n 文字の置換の総数
  - 出力の確率は $1/d_n$
- d_n の最大の素因数を P_n とすると、
  前ページの仮定を満たす有限時間プロトコルのカード枚数は P_n 以上
- P_n の漸近的評価：$P_{n-1} + P_n = \Omega(n \log n)$ [H+18, Theorem 2]
  - 方針：漸化式 $d_n = nd_{n-1} + (-1)^n$ に **abc 予想**を適用

不動点のない置換の総数の素因数の評価

- abc 予想（の特殊形）：a, b, c が互いに素な正整数で $a + b = c$ のとき、ある定数 $\gamma > 0$ について、$c \le \gamma \mathrm{rad}(abc)^2$（$\mathrm{rad}(k)$ は k の異なる素因数すべての積）
- 漸化式 $d_n = n d_{n-1} + (-1)^n$ と合わせて、$d_n \le \gamma \mathrm{rad}(n d_{n-1} d_n)^2 \le \gamma (n \cdot \mathrm{rad}(d_{n-1}) \mathrm{rad}(d_n))^2$
- $\mathrm{rad}(d_n) \le {P_n}^{\pi_{P_n}} = e^{\pi_{P_n} \log P_n} \in e^{O(P_n)}$
（素数定理より：π_k は k 以下の素数の個数）
- $\therefore \log d_n \in O(\log n + \log_{P_{n-1}} + \log_{P_n})$
- $\therefore P_{n-1} + P_n \in \Omega(\log d_n) = \Omega(n \log n)$
（Stirling の公式より）

不動点のない置換の総数の素因数

- $P_{n-1} + P_n \in \Omega(n \log n)$
- 例：$P_6 = 53$, $P_{12} = 1456321$, $P_{13} = 139241$, $P_{74} = 103086877872015343362237075543609027902253313357$
- P_n のより良い評価は？

発展：カード枚数とシャッフル回数の関係

- 例：確率 2^{-10} と $1-2^{-10}$ で1または0を出力
- カード枚数5枚以下
- シャッフルはRCとPSSと完全シャッフルのみ
  - RCとPSSでの分岐確率の分母で、素因数2の指数は2以下（$4=2^2$）
  - 完全シャッフルでは、2の指数は3以下（$5!=2^3\cdot 15$）
- このとき、シャッフルは最低4回必要
  - 3回以下だと、確率の積 $\frac{n_{\rho,1}}{d_{\rho,1}}\cdots\frac{n_{\rho,\ell_\rho}}{d_{\rho,\ell_\rho}}$ の分母には2を9個以下しか入れられない
- **こうした評価手法の応用は？**

非一様シャッフルの難しさの評価

- 不動点のない置換のプロトコルについて、一様分布でないシャッフルを用いればカード枚数を減らせるかもしれない
- **非一様シャッフルの「難しさ」をどう評価・比較するか？**

Contents

- 出力の確率分布と必要なカード枚数
- 一様閉シャッフルと巡回群シャッフル
- カードベースゼロ知識証明と秘密計算

元ネタの紹介

- Kazuki Kanai, Kengo Miyamoto, Koji Nuida, Kazumasa Shinagawa: “Uniform Cyclic Group Factorizations of Finite Groups”, arXiv:2302.02831
- または SCIS 2022, 2F5-3

一様閉シャッフル

- 一様：置換の分布がある集合上一様
- 閉：その集合が合成に関して閉じている
- 両方を満たすシャッフルは比較的実装がしやすいとされている

巡回群シャッフル

- 置換の集合が複雑な場合にどう実装する？
- シャッフルが「一定の置換の繰り返し」であれば比較的実行しやすそう
  - 置換の集合が巡回群である、ということ（巡回群シャッフルと呼ぶ）
- **問題：任意の一様閉シャッフルを巡回群シャッフルたちに分解できるか？**
  - 数学的には：任意の有限群を巡回群たちに「分解」できるか？

- 有限群 G の部分集合 $H_1, \ldots, H_k$ について、$(H_1, \ldots, H_k)$ が G の重複度 t の**一様分解**
$\overset{def}{\Leftrightarrow}$ どの $g \in G$ についても、$g = h_1 \cdots h_k$ となる $h_i \in H_i$ たちの組の個数が t 個
- **一様群分解** $\overset{def}{\Leftrightarrow}$ さらに H_i たちが G の部分群
- **一様巡回群分解** $\overset{def}{\Leftrightarrow}$ さらに H_i たちが G の巡回部分群
- 注：重複度 1 の一様分解は logarithmic signature と等価

例

- n 次対称群 S_n の一様巡回群分解：
  $H_i = \langle (1\ 2\ \cdots\ (i+1)) \rangle$ $(1 \le i \le n-1)$
- S_5 の別の一様巡回群分解：$H_1 = \langle (1\ 2\ 3\ 4\ 5) \rangle$,
  $H_2 = \langle (1\ 2\ 4\ 3) \rangle$, $H_3 = \langle (1\ 2\ 3)(4\ 5) \rangle$
- 5 次交代群 A_5 の一様巡回群分解：
  $H_1 = \langle (1\ 2\ 3\ 4\ 5) \rangle$, $H_2 = \langle (1\ 2)(3\ 4) \rangle$,
  $H_3 = \langle (1\ 3)(2\ 4) \rangle$, $H_4 = \langle (1\ 2\ 3) \rangle$
  - 一般の A_n も一様巡回群分解をもつ
- これらはすべて重複度 1 の例

いくつかの結果

- 任意の有限群が一様巡回群分解をもつことを示すには、任意の有限非可換単純群が非自明な一様群分解をもつことを示せばよい
- 可換または可解ならば一様巡回群分解をもつ
- H_1, H_2 が G の部分群であり、どの $g \in G$ も $g = h_1 h_2$, $h_i \in H_i$ と表せるならば、(H_1, H_2) は G の一様群分解である
  - 注：いくつかの散在型単純群では上記のような分解 (H_1, H_2) が知られている [Liebeck–Praeger–Saxl, Mem. Amer. Math. Soc 1990]

問題

- 任意の有限非可換単純群は非自明な一様群分解をもつか？
  - 有限単純群の分類定理に依存しない証明は可能か？
- 任意の巡回群シャッフルをどう実装するか？
  - PSS＋追加カードで実現可能：効率化は？

Contents

- 出力の確率分布と必要なカード枚数
- 一様閉シャッフルと巡回群シャッフル
- カードベースゼロ知識証明と秘密計算

ペンシルパズルの答えのゼロ知識証明

- 数独などのパズルの答えを知っていることの、カードを用いたゼロ知識証明（[Gradwohl et al., FUN 2007] など）
  - パズルの答えそのものを秘匿しつつ「答えを知っている」ことを他者に納得させる技術
- 近年では、研究対象となる「数独っぽい」パズルの種類が多岐にわたっている
  - （そもそも、そういうパズルの種類自体が年々増殖している）

カードベースゼロ知識証明の基本方針

- 問題の答えをカード列に符号化する
- 答えのカード列を必要なだけコピーする
- 答えの条件を一つずつ、コピーした答えを用いて秘密計算で確認する
  - 例：数独の場合には
    「各行に重複なし」
    「各列に重複なし」
    「各小正方形に重複なし」

領域の連結性の条件

- ある種のパズルでは、盤面のいくつかのマスの集合が答えであり、「選んだマスの集合が連結であること」が条件の一つになっている
- 例：「数コロ」

	3		3	
	3		4	1
1				
			3	

$\rightarrow$

1	3	2	3	1
	2		2	
	3	2	4	1
1	2		2	
		1	3	1

（[佐々木-品川, SCIS 2023] より引用）

領域の連結性のゼロ知識証明

[佐々木-品川, SCIS 2023] の手法：

- 確定で選ばれるマス（「始点」）の一つに 1、それ以外のマスに 0 を（秘匿して）置く
- すべてのマスに対して順に「そのマスが答えで選ばれており、隣接するマスのどれかに 1 が置かれていれば、そのマスを 1 にする」操作を（カードプロトコルで）行う
- 上記を盤面のマスの個数と同じ回数行う
  $\rightarrow$ 始点を含む連結成分が 1、残りが 0 になる
- 計算量：盤面のマスの個数の 2 乗のオーダー
- より少ない計算量にできないか？

パズルのゼロ知識証明設計のモジュール化

- ペンシルパズルの解の条件には「典型的な条件」がいくつかある
  - 「各行（列）の数字に重複がない」
  - 「領域が連結である」
  - 「領域が 2×2 の正方形を含まない」
  - $\cdots$
- 典型的な条件に対する良いプロトコルを整理収集しておけば、新しいパズルに対するプロトコルの設計に便利なのでは？

Contents

- 出力の確率分布と必要なカード枚数
- 一様閉シャッフルと巡回群シャッフル
- カードベースゼロ知識証明と秘密計算

参考文献

CK93 C. Crépeau, J. Kilian: "Discreet Solitary Games", in: CRYPTO 1993, pp.319–330, 1994

H+17 Y. Hashimoto, K. Shinagawa, K. Nuida, M. Inamura, G. Hanaoka: "Secure Grouping Protocol Using a Deck of Cards", in: ICITS 2017, pp.135–152, 2017

ICM15 R. Ishikawa, E. Chida, T. Mizuki: "Efficient Card-Based Protocols for Generating a Hidden Random Permutation without Fixed Points", in: UCNC 2015, pp.215–226, 2015

IM16 T. Ibaraki, Y. Manabe: "A More Efficient Card-Based Protocol for Generating a Random Permutation without Fixed Points", in: MCSI 2016, pp.252–257, 2016

H+18 Y. Hashimoto, K. Nuida, K. Shinagawa, M. Inamura, G. Hanaoka: "Toward Finite-Runtime Card-Based Protocol for Generating a Hidden Random Permutation without Fixed Points", IEICE Trans. Fundamentals, E101-A(9), pp.1503–1511, 2018

G+07 R. Gradwohl, M. Naor, B. Pinkas, G. N. Rothblum: "Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles", in: FUN 2007, pp.166–182, 2007

SS23 佐々木駿、品川和雅、「数コロに対する物理的ゼロ知識証明プロトコル」、SCIS 2023、3D2-4、2023