数学者、暗号の野で遊ぶ

縫田 光司
九州大学 マス・フォア・インダストリ研究所
nuida@imi.kyushu-u.ac.jp
2023 年 2 月 22 日

概要

暗号分野と関係する数学としては素因数分解や楕円曲線が有名であるが、これらは氷山の一角にすぎない。本講演では、数学と暗号の二刀流に励む話者の研究を中心に、「数学者として楽しめた」暗号分野の題材をいくつか紹介する。（注意：本稿で取り扱う暗号分野の題材は「数学との面白い接点」という観点で選ばれており、暗号分野における主流の題材であるかとは無関係であることを断っておく。）

なお、本稿は 2022 年 12 月 17 日、18 日に開催された第 20 回岡シンポジウムにおける筆者の講演内容に基づいている。

記号の説明

本稿では、非負整数 n について $[n] := \{1, 2, \ldots, n\}$, $[0..n] := \{0\} \cup [n]$ とする。また $\equiv_n$ は「n を法として等しい」という関係を表す。素数 p について、有限素体 $\mathbb{F}_p$ を $\mathbb{Z}$ の部分集合 $[0..p-1]$ としばしば断りなしに同一視する。

1　公開鍵暗号化

暗号技術にはさまざまな種類があるが、その中で**暗号化技術**は非専門家にも比較的馴染みのある技術であろう。これは大まかに言えば、生のデータ（専門的には**平文**（ひらぶん）と呼ばれる）を**暗号文**へと変換する操作（**暗号化**）とその逆操作（**復号**）の組からなる技術である。ここで復号には「**鍵**」と呼ばれる秘密の補助情報が必要であり、平文の情報を得ようと企む攻撃者が鍵を持っていないならば暗号文から平文の情報を得ることができないように暗号化の方式を設計することが求められる。

暗号化技術は主に、暗号化操作の際にも復号用の鍵を必要とする**共通鍵暗号化**と、暗号化操作の際には復号用の鍵を必要としない**公開鍵暗号化**に分類される。後者においても、暗号化操作の際に、復号用の鍵と対になる何らかの補助情報を要することが多い。こうした補助情報は**公開鍵**（あるいは**暗号化鍵**）と呼ばれ、それとの対比として復号用の鍵は**秘密鍵**（あるいは**復号鍵**）と呼ばれる。公開鍵暗号化においては、公開鍵を（名称の通り）公開することで誰でも暗号文を作成できるようにすることが一般的であり、攻撃者が暗号文に加えて公開鍵をも入手したとしても平文の情報が得られないように方式を設計することが求められる。

以上を踏まえて、公開鍵暗号化の概念は以下のように定式化される。（定義の細部は文献によって異なる場合もある。以降の暗号技術に関する諸定義についても同様である。）

定義 1. 公開鍵暗号化方式とは、以下の仕様を満たす確率的多項式時間アルゴリズムの組 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

のことと定める[*1]。

鍵生成アルゴリズム $\mathsf{Gen}(1^\lambda)$　これは**セキュリティパラメータ**と呼ばれる正整数 λ を入力としてとる[*2]。その出力は、公開鍵 pk と秘密鍵 sk の組 $(\mathsf{pk}, \mathsf{sk})$ である。なお、pk はセキュリティパラメータ λ と、**平文空間**と呼ばれる有限集合 $\mathcal{M}$ および**暗号文空間**と呼ばれる有限集合 $\mathcal{C}$ を特定する情報を暗に含むものとする。また、表記の簡略化のため、sk は pk を（したがって、pk に含まれる平文空間 $\mathcal{M}$ や暗号文空間 $\mathcal{C}$ を特定する情報をも）暗に含むものと仮定する。

暗号化アルゴリズム $\mathsf{Enc}_{\mathsf{pk}}(m)$　これは公開鍵 pk と平文 $m \in \mathcal{M}$ を入力としてとる。その出力は暗号文 $c \in \mathcal{C}$ である。

復号アルゴリズム $\mathsf{Dec}_{\mathsf{sk}}(c)$　これは秘密鍵 sk と暗号文 $c \in \mathcal{C}$ を入力としてとる。その出力は平文 $m' \in \mathcal{M}$ もしくは「復号失敗」を意味する特別な記号 $\perp \notin \mathcal{M}$ である[*3]。

通常は、公開鍵暗号化方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ では、「正当性」$\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m)) = m$ が、$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ と $m \in \mathcal{M}$ について常に（確率 1 で）成り立つことを暗に要請する[*4]。また、公開鍵暗号化方式の安全性についてもいくつかの標準的な定義が知られているが、本稿では説明を割愛する。詳細については暗号理論の専門書を参照されたい。（啓蒙書の枠を超えた暗号理論の和書としては森山、西巻および岡本による著書 [21] が優れているが、残念ながら本稿の執筆時点では入手困難な状況である。筆者の著書 [24] の第 1 章でも公開鍵暗号分野の理論面での入門的事項をいくつか取り扱っている。また、暗号分野の広範な題材を扱っている比較的新しい和書としては、光成の著書 [17] や IPUSIRON の著書 [11] を挙げておく。）

例 1. 公開鍵暗号化は 1970 年代後半に提唱された [5] 概念である。ここでは比較的初期の代表的な方式の一つである**ElGamal**（エルガマル）**暗号** [7] を紹介する。

$\mathsf{Gen}(1^\lambda)$　ある適切な方法で、有限巡回群 G およびその生成元 g を選ぶ。s を $[0..|G|-1]$ から一様ランダムに（つまり、$[0..|G|-1]$ 上の一様分布に従って）選び、$h := g^s \in G$ とする。$\mathsf{pk} := (G, g, h)$ を公開鍵、$\mathsf{sk} := s$ を秘密鍵とする。平文空間は $\mathcal{M} = G$、暗号文空間は $\mathcal{C} = G^2$ である。

$\mathsf{Enc}_{\mathsf{pk}}(m)$　平文 $m \in G$ について、r を $[0..|G|-1]$ から一様ランダムに選び、$c_1 := g^r$, $c_2 := h^r m$ とする。$c := (c_1, c_2) \in G^2$ を暗号文とする。

$\mathsf{Dec}_{\mathsf{sk}}(c)$　暗号文 $c = (c_1, c_2) \in G^2$ について、$m' := c_2 {c_1}^{-s} \in G$ を復号結果とする。

この方式の正当性は（$G = \langle g \rangle$ の可換性より）$m' = c_2 {c_1}^{-s} = (h^r m) \cdot (g^r)^{-s} = g^{sr} m g^{-rs} = m$ と確かめられる。ElGamal 暗号の安全性は、巡回群 $G = \langle g \rangle$ とその元 $x \in G$ に対して $x = g^k$ を満たす $k \in [0..|G|-1]$ を特定する問題（**離散対数問題**）の計算困難性に基づいている[*5]が、詳細は割愛する。

[*1] なお、Dec については実際には出力が非確率的であることが多い。また、「多項式時間アルゴリズム」の概念に馴染みのない方は、本稿の範囲では「効率的に実行できる」ぐらいの意味合いと思っていただいて差し支えない。

[*2] セキュリティパラメータは、方式で用いられる数学的対象のサイズ（例えば素数 p の桁数など）をどの程度大きくするかを調整するためのパラメータであり、一般にはこれが大きいほど方式の安全性が向上する代わりに効率性が低下する。なお、理由は割愛するが、技術的な理由により、セキュリティパラメータ λ を入力に与える際には「1 を λ 個並べた列」1^λ の形で記述することが一般的である。

[*3] 後述する「正当性」が（確率 1 で）成り立つ状況では、正しく生成された暗号文を入力する限りは復号アルゴリズムが失敗することはないが、アルゴリズムの仕様としては不正な暗号文がうっかり入力される場合も想定しておく必要がある。

[*4] この性質が成り立たない確率が「無視できる」（後述する定義 3 を参照）、というやや緩和した性質で代替することもある。

[*5] 実際には、ElGamal 暗号の安全性は「離散対数問題の困難性」よりもやや弱い（直感的には、より成り立ちやすい）性質であると予想されているが、両者の正確な関係は本稿の執筆時点では未解明である。

2　準同型暗号

例 1 の ElGamal 暗号は、二つの平文 $m_i \in G$（$i = 1, 2$）の暗号文 $c_i = (c_{i,1}, c_{i,2}) = (g^{r_i}, h^{r_i} m_i) \in G^2$ が与えられたとき、それらの直積群 G^2 における積

$$c_1 c_2 = (c_{1,1} c_{2,1}, c_{1,2} c_{2,2}) = (g^{r_1} g^{r_2}, h^{r_1} m_1 h^{r_2} m_2) = (g^{r_1+r_2}, h^{r_1+r_2} m_1 m_2)$$

が平文の積 $m_1 m_2$ の（乱数 $r_1 + r_2 \bmod |G|$ による）暗号文となる、という特徴をもつ。つまり、暗号文の積を計算することで、暗号文を復号することなしに中身の平文に対する積を計算できる、ということである。このような「暗号文のままで中身の平文の演算ができる」性質をもつ（公開鍵）暗号化方式を**準同型暗号**と呼ぶ。また、その平文の演算に対応する暗号文の演算（ElGamal 暗号の例でいえば、群 G^2 上の積演算）のことを**準同型演算**と呼ぶ。準同型暗号には、ElGamal 暗号のように平文空間の単一の演算にのみ対応するものもあれば、複数の演算に同時に対応するものもある。特に、平文空間 $\mathcal{M}$ が環の構造をもち、平文に対する加法と乗法の両方を暗号文のまま計算できる方式を**環準同型暗号**と呼ぶ。なお、環 $\mathcal{M}$ が特に有限体 $\mathbb{F}_q$ である場合には、「あらゆる関数 $(\mathbb{F}_q)^N \to \mathbb{F}_q$ は $\mathbb{F}_q$ 上の和と積（とスカラー倍）の組み合わせで表せる」という事実[*6]から、環準同型暗号において（効率面はさておき、少なくとも原理的には）平文に対する任意の演算を暗号文のまま実現可能である。このことから、平文空間が有限体である環準同型暗号のことを**完全準同型暗号**と呼ぶ[*7]。

例 2. 完全準同型暗号は Gentry の 2009 年の論文 [9] で初めて構成された。その方式はやや複雑なため、ここではより構造を説明しやすい完全準同型暗号の例として van Dijk, Gentry, Halevi, Vaikuntanathan による 2010 年の方式 [6] の概要を説明する。詳細は割愛するが、この方式では、p を秘密の素数（秘密鍵 sk の一部）、N を公開された p の倍数（公開鍵 pk の一部）として、平文 $m \in \mathcal{M} := \mathbb{F}_2$ の暗号文は

$$c = pq + 2r + m \bmod N \in (-N/2, N/2] \cap \mathbb{Z} \tag{1}$$

という形をしている（暗号文の生成方法については下記の注意 1 を参照されたい）。ここで N を法とする余りは（$[0..N-1]$ ではなく）0 を中心とする区間にとっており、q と r はランダムな整数である。暗号文 c の復号は、まず $c' := c \bmod p$ を計算して、次に $m' := c' \bmod 2$ を計算する、という手順で行われる。ここで、r **（の絶対値）が充分小さな値であれば、**$c' = 2r + m$ が成り立ち、したがって $m' = m$ が成り立つ。暗号化の際には、この性質が成り立つように、r の項（これを暗号文 c の**ノイズ**と呼ぶ）が充分小さな値となるよう暗号文 c を生成する。

この方式における平文 m_i（$i = 1, 2$）の暗号文 $c_i = pq_i + 2r_i + m_i$（以降では "$\bmod N$" を省略する）が与えられたとき、それらの和と積はそれぞれ

$$c_1 + c_2 = pq_{\mathrm{add}} + 2r_{\mathrm{add}} + m_1 + m_2 \ ,$$

$$c_1 c_2 = pq_{\mathrm{mult}} + 2r_{\mathrm{mult}} + m_1 m_2$$

という形に表せる。ここで

$$q_{\mathrm{add}} = q_1 + q_2 \, , \, r_{\mathrm{add}} = r_1 + r_2 \ ,$$

[*6] $(\mathbb{F}_q)^N$ 上の Kronecker のデルタ $\delta((a_1, \ldots, a_N), (b_1, \ldots, b_N))$ が多項式 $(1 - (a_1 - b_1)^{q-1}) \cdots (1 - (a_N - b_N)^{q-1})$ で表せる、という事実から導かれる。

[*7] 平文空間が体でない場合にも、環準同型暗号のことを完全準同型暗号と呼んでいる文献が少なくないことを注意しておく。

$$q_{\mathrm{mult}} = pq_1q_2 + 2q_1r_2 + 2q_2r_1 + q_1m_2 + q_2m_1\,,\; r_{\mathrm{mult}} = 2r_1r_2 + r_1m_2 + r_2m_1$$

である。このようにこの方式では、暗号文の和と積がそれぞれ平文の和と積の暗号文となっており、完全準同型暗号と同じ状況にある。

ただし一つ問題があり、和の準同型演算で得られる暗号文のノイズ r_{add} の大きさは元々のノイズの 2 倍程度、積の準同型演算で得られる暗号文のノイズ r_{mult} の大きさは元々のノイズの 2 乗程度（いずれも最悪時における評価）に増大してしまう。そのため、（特に積の）準同型演算を繰り返すことで、いずれは暗号文のノイズが大きすぎて正しい復号ができない状態に陥ってしまう。このようなノイズの増大に伴う復号失敗という現象は、既存の有効な完全準同型暗号方式のすべてに共通する問題点である[*8]。前述の Gentry の論文 [9] における最も重要な貢献は、準同型演算によって増大した暗号文のノイズを削減する**ブートストラップ**と呼ばれる一般的技法を導入した点である。このブートストラップについては次節で改めて述べる。

注意 1. 例 2 の方式において、秘密の素数 p を隠したまま式 (1) の形の暗号文を生成する方法の概要は以下の通りである。まず、公開鍵と秘密鍵の生成を行う際に、平文 1 の暗号文 $c_{\mathrm{org},1}$ と、平文 0 の暗号文からなる充分大きな集合 $\mathcal{C}_{\mathrm{org},0}$ を一緒に生成して公開鍵に含めておく。そして、平文 $m = 1$ に対する暗号化アルゴリズム $\mathsf{Enc}_{\mathsf{pk}}(1)$ では、$\mathcal{C}_{\mathrm{org},0}$ のランダムな部分集合を選び、それに属する暗号文すべてに和の準同型演算を施した上で、さらに暗号文 $c_{\mathrm{org},1}$ とも和の準同型演算を行う。$\mathcal{C}_{\mathrm{org},0}$ に属する暗号文はどれも平文 0 をもつため、和の準同型演算を行っても平文は不変であり、上記の手順で得られる暗号文の平文は確かに 1 である。同様に、平文 $m = 0$ の場合は、最後に $c_{\mathrm{org},1}$ を用いる部分を省略して上記の手順を行う。こうして得られる暗号文の平文は確かに 0 である。集合 $\mathcal{C}_{\mathrm{org},0}$ を充分大きく選んでおけば、そのランダムな部分集合の選び方の可能性が充分多数になり、暗号文 $c_{\mathrm{org},1}$ が準同型演算の対象に含められたかどうか（すなわち、平文 m が 0 と 1 のどちらであるか）を秘匿できる、というアイデアである。

3　ブートストラップと関数の多項式表示

前述の論文 [9] で導入されたブートストラップ操作の、最も素朴な実現方法は以下の通りである（図 1）。

1. ノイズを削減したい暗号文 c について、c を（ビット単位などに分割した上で）さらに暗号化する。
2. 上で得られた c の暗号文 $\widehat{c}$ について、「c を復号して平文を得る」という操作に対応する準同型演算を $\widehat{c}$ に施す。（直感的な説明としては、「暗号文 $\widehat{c}$ の内部で c の復号を行う」ということである。）
3. すると、暗号文 $\widehat{c}$ の内部で c がその平文 m へと変換され、結果として m の新たな暗号文が得られる。

このブートストラップの手順には二つの注意点がある。一つは、復号操作に対応する準同型演算を行うために、秘密鍵を暗号化した暗号文が必要となる。そのため鍵生成の際に公開鍵や秘密鍵と同時にブートストラップ用の鍵（秘密鍵の暗号文に相当する）を生成して、ブートストラップ鍵を公開しておくことが求められる。このように秘密鍵の暗号文を公開しても安全性に影響がないかどうか[*9]は慎重に検討する必要がある。もう一つは、例 2 で述べたような準同型演算の回数制限の存在を鑑みて、ブートストラップの過程で行われる復号操作に対応する準同型演算に必要な演算回数がこの回数制限を超えないようにする必要がある。ここで、可能な

[*8] こうしたノイズの増大が生じない完全準同型暗号の構成法がプレプリントとして発表された事例はいくつか存在するものの、いずれも安全性の解析が不充分であるとみなされている（もしくはより強く、具体的な攻撃方法が指摘されている）ため、暗号分野の専門家からは「完全準同型暗号の構成の成功例」とは認知されていない。

[*9] 専門的には “circular security” と呼ばれている。この概念については例えば [3] などを参照されたい。

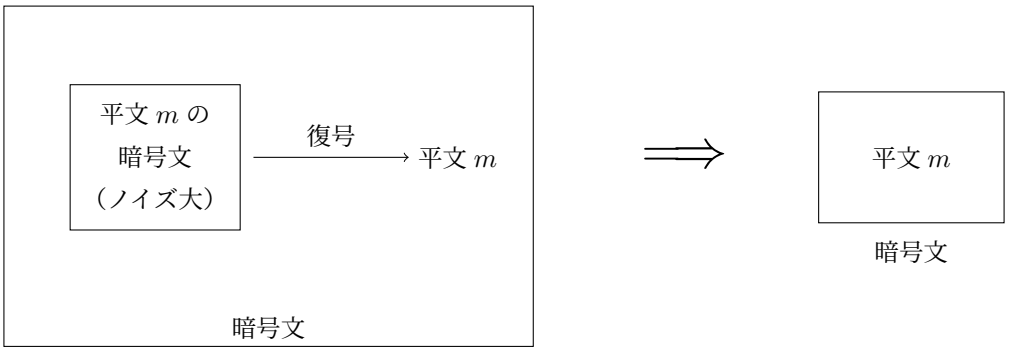

図 1　暗号文内部での準同型演算による復号操作（左側）とその結果得られる暗号文（右側）

準同型演算の最大回数を増やすためにはそれだけ方式のパラメータ（方式で用いられる整数の桁数など）を大きくする必要があり、効率の悪化を招くことから、復号（あるいはそれと等価な）操作をいかに少ない演算回数で実現できるかが完全準同型暗号の効率化に際しての重要な課題である。

例 2 の完全準同型暗号方式の場合、暗号文 c の復号には c を秘密の素数 p で割った余りの計算が必要であり、これは c/p を小数点以下切り捨てた値 $\lfloor c/p \rfloor$ の計算へと帰着される。原論文 [6] ではこの計算を、c の 2 進法表示と $1/p$ の（正確には、有限桁の小数による近似値の）2 進法表示の各桁のビットをそれぞれ暗号化して、準同型演算を通して両者の筆算式の掛け算を行う、という形で実現する方針を採用している。ここで、2 進法での掛け算においては各桁ごとの積では繰り上がりが生じないが、各桁ごとの積を足し合わせる際に上位桁への繰り上がりが生じる。これを和と積の準同型演算で処理するためには、足し算の繰り上がり関数を $\mathbb{F}_2$ 上の和と積の組み合わせ、すなわち多項式によって表示する必要がある。より正確には、入力の個数 n と正整数 i を指定したとき、自然な同一視 $\mathbb{F}_2 \tilde{\to} \{0,1\} \subseteq \mathbb{Z}$ を介して、和の i 桁上への繰り上がり関数を

$$\begin{array}{rccccc} \varphi_i \colon (\mathbb{F}_2)^n \tilde{\to} & \{0,1\}^n & \to & \{0,1\} & \tilde{\to} \mathbb{F}_2 \\ & \cup & & \cup & \\ (x_1, \ldots, x_n) \mapsto & \left\lfloor \dfrac{x_1 + \cdots + x_n}{2^i} \right\rfloor \bmod 2 & & & \end{array}$$

で定義する。この関数 φ_i の具体的な多項式表示については、以下の綺麗な結果が知られており、原論文 [6] のブートストラップでもこの関数が用いられている。

定理 1 ([2])**.** 上記の関数 $\varphi_i \colon (\mathbb{F}_2)^n \to \mathbb{F}_2$ は 2^i 次の基本対称式 $e_{2^i}(x_1, \ldots, x_n)$ と一致する。また、これは関数 φ_i に対する次数が最小の多項式表示である。

上記の方式では平文空間が $\mathcal{M} = \mathbb{F}_2$ に限定されていたが、筆者と黒澤の論文 [23] ではその平文空間を一般の素数 p（上記の構成に用いられている秘密の素数 p と記号が重複しているが、それとは別の値であることを注意しておく）に対する $\mathcal{M} = \mathbb{F}_p$ へと拡張する構成法を与えた。この方式のブートストラップでは、$\mathbb{F}_2$ の代わりに $\mathbb{F}_p$ 上で考えた上述の和の繰り上がり関数 $\varphi_i \colon (\mathbb{F}_p)^n \to \mathbb{F}_p$ のうち、$n = 2$ かつ $i = 1$ の場合の多項式表示を用いていた。この $\mathbb{F}_p$ 上での和の繰り上がり関数については、鍛冶、前野、筆者、沼田 [12] により、一般の場合に対する下記の結果を与えている。なお、有限体上の関数の最小次数の多項式表示の一意性により、下記の結果における $p = 2$ の場合は定理 1 と一致することを注意しておく。

定理 2 ([12])**.** 素数 p について、前述の関数 φ_i は下記の（最小次数の）多項式表示をもつ。

$$\varphi_i(x_1,\dots,x_n) = \sum_{\substack{d_1,\dots,d_n\in\{0,1,\dots,p-1\}\\ d_1+\cdots+d_n=p^i}} \prod_{j=1}^{n} \left(\frac{1}{d_j!} \bmod p\right) x_j(x_j-1)\cdots(x_j-d_j+1)$$

ここでは詳細は割愛するが、定理 2 は下記の Lucas の定理を用いて証明される。

命題 1 (Lucas の定理 [14])**.** p を素数とし、$a=(a_{\ell-1}\cdots a_1a_0)_p$ および $b=(b_{\ell-1}\cdots b_1b_0)_p$ をそれぞれ ℓ 桁で p 進法表示された非負整数とする（上位桁が 0 になることも許す)。このとき

$$\binom{a}{b} \equiv_p \binom{a_{\ell-1}}{b_{\ell-1}}\cdots\binom{a_1}{b_1}\binom{a_0}{b_0}$$

が成り立つ。

さて、和の繰り上がりについての結果が得られたからには、次は積の繰り上がりを調べたくなるのが数学者の業である。積の繰り上がりを考えるときには $p=2$ の場合は自明になるため、p を奇素数とし、自然な同一視 $\mathbb{F}_p \overset{\sim}{\leftrightarrow} [0..p-1] \subseteq \mathbb{Z}$ を介して、積の i 桁上への繰り上がり関数を

$$\begin{array}{ccccc} \psi_i\colon (\mathbb{F}_p)^n & \overset{\sim}{\leftrightarrow} & [0..p-1]^n & \to & [0..p-1] \quad \overset{\sim}{\leftrightarrow} \mathbb{F}_p \\ & & \cup & & \cup \\ & & (x_1,\dots,x_n) & \mapsto & \left\lfloor \dfrac{x_1\cdots x_n}{p^i} \right\rfloor \bmod p \end{array}$$

で定義する。この関数について、前述のプレプリント [12] で $i=1$ の場合の多項式表示を与えたものの、実はその結果は既に知られていた [32] ことがプレプリントの公表後に判明した[*10]。その表示は以下の通りである。

定理 3 ([12, 32])**.** p を奇素数とすると、上記の関数の $i=1$ の場合 ψ_1 は下記の（最小次数の）多項式表示をもつ。

$$\psi_1(x_1,\dots,x_n) = x_1\cdots x_n\cdot\left(\Psi(x_1\cdots x_n) - \sum_{j=1}^{n}\Psi(x_j) + (n-1)\Psi(1)\right)$$

ここで

$$\Psi(t) := \sum_{i=1}^{p-2}\left(\frac{B_{p-1-i}}{p-1-i} \bmod p\right)t^i = \frac{p-1}{2}t^{p-2} + \sum_{i=1}^{(p-3)/2}\left(\frac{B_{p-1-2i}}{p-1-2i} \bmod p\right)t^{2i}$$

である。なお、B_m は Bernoulli 数を表し、

$$\frac{t}{e^t-1} = \sum_{m\geq 0}\frac{B_m}{m!}t^m$$

で定められる。また、

$$\Psi(1) = \left(\frac{(p-1)!+1}{p} \bmod p\right) = \left(B_{p-1} + \frac{1}{p} - 1 \bmod p\right)$$

が成り立つ。

なお、定理 3 については Bernoulli 数たちの関係式を用いた地道な証明に加えて、群のコホモロジーを用いた証明も考えられる。詳しくは [12, Appendix] を参照されたい。

[*10] 研究当時、思いがけず Bernoulli 数という意外な道具を用いた綺麗な表示が得られたので喜んでいたが、逆に「こんな綺麗な結果がまだ知られていないなんてことはあるだろうか」と疑っていたところ、懸念が的中したという次第である。

4　完全準同型暗号と有限群の「圧縮関数」

例 2 でも少し触れたように、本稿の執筆時点で知られている有効な完全準同型暗号の構成法はすべて上述のブートストラップの方法論に基づいている。一方で、ブートストラップの方法論に立脚しない完全準同型暗号の構成へのアプローチも研究されており、Ostrovsky と Skeith は（Gentry の論文よりも 1 年早い）2008 年の論文 [29] の中で下記のようなアプローチに言及している。

1. ビットの集合 $\{0,1\}$ 上の演算を、何らかの有限群 G 上で「実現」する。
2. G の元に対する暗号化方式で、G 上の群演算に関する準同型性をもつものを構成する。

例えば、有限群 G の空でなく互いに交わらない部分集合 $X_0, X_1 \subseteq G$ と、関数 $f_\vee \colon G^2 \to G$ で、以下の二つの条件を満たすものが与えられているとする（これが上記の条件 1 でいうところの、ビット演算 $\vee$ の群 G 上での「実現」に相当する）。

- $b_1, b_2 \in \{0,1\}$, $g_i \in X_{b_i}$（$i = 1, 2$）のとき常に $f_\vee(g_1, g_2) \in X_{b_1 \vee b_2}$ が成り立つ。ここで $\vee$ はビットに対する OR（論理和）演算を表す。
- G 上の変数 x_1, x_2 について、$f_\vee(x_1, x_2)$ は x_1, x_2 および定数である G の元たちの積で表される。

さらに、G の元 g から暗号文 $[[g]]$ を生成する暗号化方式と、暗号文に対する演算 $*$ で、$g_1, g_2 \in G$ のとき常に $[[g_1]] * [[g_2]] = [[g_1 g_2]]$ を満たすものが与えられているとする（上記の条件 2 に相当する）。このとき、ビット $b \in \{0,1\}$ に対する暗号文を、ある元 $\sigma_b \in X_b$ に対する $[[\sigma_b]]$ と定める。すると、$b_1, b_2 \in \{0,1\}$ の暗号文 $[[\sigma_{b_1}]], [[\sigma_{b_2}]]$ に対して、関数 $f_\vee$ を構成する入力 x_1, x_2 と G の元たちとの積に対応する形で、暗号文 $[[\sigma_{b_1}]], [[\sigma_{b_2}]]$ および G の元の暗号文たちに演算 $*$ を施すことで、論理和 $b_1 \vee b_2$ に対応する暗号文 $[[h]]$、ただし $h \in X_{b_1 \vee b_2}$、を得ることができる、という具合である。

ただし、前述の論文 [29] では、上記の条件 1 を満たす「実現」の構成法については議論されているものの、条件 2 を満たす暗号化方式の構成法については述べられていない。実のところ、条件 2 を満たす暗号化方式の構成が上記のアプローチの特に難しい点であり、筆者も以前そのような暗号化方式の構成法について検討した [25] ものの、具体的な構成を得るには至っていない状況である。その難しさの主な要因の一つとして、条件 1 を満たす群 G は必然的に非可換群となる点が挙げられる。大まかな説明としては、従来の暗号分野では、平文空間や暗号文空間に用いられる群は基本的に可換群であり、非可換群を用いた暗号技術の構成や安全性解析のノウハウが未だ乏しいと言うことができる。

ここでは条件 2 の実現方法はひとまず気にせず、条件 1 を実現する良い関数の構成という問題に着目する。前述の論文 [29] では、G が非可換な有限単純群である場合に、交換子の性質を用いた（非構成的な）存在証明を与えている。一方で、前述の筆者の研究 [25] では、下記のような 2 段階の構成方法を考案している。例えば、上でも例に挙げた論理和 $\vee$ の場合、G を 5 次対称群 S_5 とし、$\sigma_0 := 1$ をその単位元として、$\sigma_1 := \sigma := (1\ 2\ 3) \in G$ について $X_b := \{\sigma_b\}$（$b = 0, 1$）と定める。構成のアイデアとして、G 上の積 $x_1 x_2$ について、$b_1, b_2 \in \{0,1\}$ に対応する積 $\sigma_{b_1}\sigma_{b_2}$ を考えると、$(b_1, b_2) = (1,1)$ のときは $\sigma_1\sigma_1 = \sigma^2$ となり所望の X_1 の元とはならないものの、それ以外の (b_1, b_2) については $\sigma_{b_1}\sigma_{b_2} = \sigma_{b_1 \vee b_2} \in X_{b_1 \vee b_2}$ が成り立つことがわかる。（これは $b_1, b_2 \in \{0,1\}$ の整数としての和 $+$ が、$(b_1, b_2) \neq (1,1)$ のとき $b_1 + b_2 = b_1 \vee b_2$ を満たすことと対応する。）ここで、$(b_1, b_2) = (1,1)$ の場合に正しい集合 X_1 からはみ出た元 σ^2 を正しい元 $\sigma_1 = \sigma$ へと（X_0 および X_1 の元は固定したままで）戻すことができれば所望の関数が得られる。より詳しくは、S_5 上の

積で実現される関数 $F\colon S_5 \to S_5$ で、条件

$$F(1) = 1 \text{ および } F(\sigma) = F(\sigma^2) = \sigma \tag{2}$$

を満たすものを構成できれば、合成関数 $(x_1, x_2) \mapsto F(x_1 x_2)$ が上記の関数 $f_\vee$ の条件を満たす。

この条件 (2) を満たす関数 F として、前述の [25] では

$$F(y) := (1\ 5)(2\ 3\ 4)y(2\ 3\ 4)y(3\ 4)y^2(2\ 3)(4\ 5)y(2\ 3\ 4)y(3\ 4)y^2(1\ 4\ 2\ 5)$$

を与えているが、その構成方法は「上手くいきそうな関数の候補を与えて、計算機で条件の成否を確認して、上手くいかなければ微調整して再度計算機に尋ねる」という場当たり的なものであった。そこで筆者はその後、S_5 以外の有限非可換群 G も視野に入れて、条件 (2) を満たす関数 F の（非）存在性や構成に関するより系統的な研究を行った。そうして（まだプレプリントの段階ではあるが）以下の結果を得た。

定理 4 ([27])**.** 1. 群 $G = A_5$（5 次交代群）、$\sigma = (1\ 2\ 3) \in G$ および以下の関数

$$F\colon A_5 \to A_5\,,\ F(y) := (1\ 2\ 4\ 3\ 5)y(1\ 3\ 5)y(1\ 4\ 3)y(1\ 5)(2\ 3)y(1\ 4\ 3\ 5\ 2)$$

は条件 (2) を満たす。またこの F が、所望の条件を満たす A_5 上の関数のうち、表示に現れる y の個数が最小となるものの一つである。

2. 位数が $60 = |A_5|$ 以下である群 G のうち A_5 と同型でない群 G については、位数 3 の元 $\sigma \in G$ および G 上の積で実現される関数 $F\colon G \to G$ で条件 (2) を満たすものは存在しない。

5 楕円曲線の群構造の証明

1 節の例 1 で紹介した ElGamal 暗号の安全性は、構成に用いられている巡回群 G 上の離散対数問題の計算困難性に基づいているのであった。ここで、一般に、互いに同型な巡回群であっても、その群における離散対数問題の計算の難度は群の具体的な構成法に大きく依存する。例えば、群 G として加法群 $\mathbb{Z}/n\mathbb{Z}$ を用いる（この場合は累乗の代わりにスカラー倍を考えることになる）と、$\mathbb{Z}/n\mathbb{Z}$ の生成元 g とそのスカラー倍 $h := a \cdot g$ が与えられたとき、g の乗法に関する逆元 $g^{-1} \in \mathbb{Z}/n\mathbb{Z}$（これはいわゆる拡張 Euclid の互除法を用いて効率的に計算できる）を用いて離散対数 a を $a = h \cdot g^{-1}$ と容易に計算できる。なお、一般の位数 n の巡回群 G については、G から $\mathbb{Z}/n\mathbb{Z}$ への同型写像 φ が常に存在するものの、φ およびその逆写像 φ^{-1} が効率的に計算可能とは限らないため、$\mathbb{Z}/n\mathbb{Z}$ 上の離散対数問題の解法を直ちに G 上の場合に転用できるわけではない。

現代の暗号分野では、ElGamal 暗号のような暗号方式の設計に用いる（離散対数問題が計算困難であることが求められる）有限巡回群 G としては、有限体 K 上の楕円曲線 E の有理点集合 $E(K)$ がなす群（の適切な巡回部分群）を用いるのが、効率性と安全性のバランスが最も優れていると考えられている。こうした楕円曲線の有理点群を用いる暗号技術は**楕円曲線暗号**と総称されている [13, 16]。楕円曲線暗号は現代の暗号分野の中で知名度が最も高い暗号技術の一つである。一方で、（一般の体 K について）$E(K)$ が群をなすという事実（特に、有理点の間に定義された演算 $+$ が結合法則を満たすこと）の良く知られた証明は、数学の専門家以外にとってかなり高度な数学的予備知識を必要とする[*11]。そこで筆者は、$E(K)$ 上の演算 $+$ が結合法則を満

[*11] この演算 $+$ が結合法則を満たすことの「自然な」証明方針の一つは、E の定義体 K をその代数閉包 $\overline{K}$ まで拡大し、$E(\overline{K})$ から E の Picard 群 $\mathrm{Pic}^0(E)$ への単射 φ で演算 $+$ を保つものを構成するというものである。この φ を用いると、$P, Q, R \in E(\overline{K})$ について $P + (Q + R)$ と $(P + Q) + R$ のいずれも φ で $\mathrm{Pic}^0(E)$ の同一の元に写る（$\mathrm{Pic}^0(E)$ は群であり演算の結合法則が成り立つため）ことから、φ の単射性より $E(\overline{K})$ においても $P + (Q + R) = (P + Q) + R$ が成り立つ、というものである。

たすという事実について、数学の専門家以外にも手が届き得るようにすべく、高度な数学的予備知識をできるだけ排した証明に取り組み、線型代数の範囲の予備知識で完結する証明[*12]を考案した。なお、$E(K)$ 上の演算 $+$ の結合法則を直接（初等的）計算で証明する既存研究も存在し、例えば Friedl [8] による証明の大部分は手計算による直接的議論で構成されているが、一部の補題の成立が計算機を用いてしか確認されていない。計算機の援用を完全に排した初等的計算による証明を記した文献は筆者の知る限りではまだ存在しない。

ここでは上述の証明の大まかな方針を紹介する。（詳細は論文 [28] を参照されたい。なお、この証明の日本語版が筆者の著書 [24] の付録に掲載されている。）大元のアイデアは、Silverman と Tate の著書 [31] で述べられている Cayley–Bacharach の定理を用いた証明と同様である。まず、有理点 $P, Q \in E(K)$ について、（直感的には）「P と Q を結ぶ直線と E とのもう一つの交点」を $P * Q$ で表す。より正確には、件の加法 $P + Q$ について $P * Q = -(P + Q)$ を満たすように演算 $*$ を定義している。このとき、証明すべき結合法則は、$P, Q, R \in E(K)$ について

$$(-P) * (Q * R) = (-R) * (Q * P) \tag{3}$$

が成り立つことと同値であることが直接計算によりわかる。ここで、「O, P, $-P$ を通る直線」「Q, R, $Q * R$ を通る直線」「$Q * P$, $-R$, $(-R) * (Q * P)$ を通る直線」の定義式の積として得られる斉次 3 次多項式を F_1 とし、その P と R を交換して得られる「O, R, $-R$ を通る直線」「Q, P, $Q * P$ を通る直線」「$Q * R$, $-P$, $(-P) * (Q * R)$ を通る直線」の定義式の積として得られる斉次 3 次多項式を F_2 とする。（O は E の無限遠点を表す。）すると、射影平面において F_1 と F_2 の各々が定める 3 次曲線は、それらの定義に現れた点たちのうち $(-P) * (Q * R)$ と $(-R) * (Q * P)$ を除いた 8 点を共有する。[31] における証明は、上記の状況に Cayley–Bacharach の定理を適用することで、これらの 3 次曲線たちが残る 1 点も共有することが示され、したがって式 (3) が導かれる、という具合に進められる。

ここで、上の議論に現れる点たちが重複をもたない場合には、その場合に限定した Cayley–Bacharach の定理が純粋に線型代数的な議論で証明できることから、式 (3) の証明の全体も線型代数的な議論に収まる。しかし、一般の場合におけるこの方針での証明では、F_1 や F_2 を構成する直線と楕円曲線 E との交点の「重複度」の定義が必要であり、通常はそれには局所環の概念を要することから、純粋に線型代数的な議論には収まらない。筆者による証明ではこの点に関して、まず、F_1 や F_2 を構成する直線と E が「重複度 3 で交わる」、すなわち上の議論に現れる点たちのうち 3 点が一致する場合については、初等的（組合せ論的）な議論により個別に証明できることを示している。次に、「重複度 3 で交わる」ことがない場合に限定すると、直線と E との交点が「重複度 1 をもつ」状況と「重複度 2 をもつ」状況を区別するだけであれば線型代数的な議論により可能であることを見出し、Cayley–Bacharach の定理の証明と類似の（線型代数的な）議論により式 (3) の証明を与えている。こうして全体として線型代数の範囲の予備知識で収まる証明を実現している。なお、この証明は確かに数学的予備知識は線型代数の範囲に収まる（かつ計算機の援用も要しない）ものの、議論自体は少々込み入っているため、「数学の専門家以外にも理解しやすい証明」という当初の目標が達成できているかどうかは悩ましい。より簡潔な議論に基づく証明は今後の研究課題である。

[*12] ただし、そもそも楕円曲線の（Weierstrass 標準形による）定義自体に射影平面の概念を用いており、その点だけは線型代数の範囲に収まっていないことを注意しておく。

6　疑似乱数と単純正規数と語の組合せ論

例えば例 1 の ElGamal 暗号において、その鍵生成アルゴリズムと暗号化アルゴリズムでは「ランダムな値」を選ぶ必要があった。「アルゴリズム」の概念の一般的な数理モデル化においては、「アルゴリズム」の本体は確定的、つまり同じ入力に対しては常に同じ出力を与える手順として定義され、アルゴリズムにおけるランダムな挙動は、ある確率分布に従う値（乱数）をアルゴリズムの補助入力として与えることで実現されるものと解釈する。さらに、現実の計算機において完全な（つまり、本来想定される確率分布と同じ分布をもつ）乱数を大量に生成することは容易ではないため、その代わりに、**種**と呼ばれるサイズの小さな乱数のみを生成し、それをある（確定的）アルゴリズムでサイズの大きな「乱数っぽい」値へと変換する、という二段構えの手法が標準的に用いられる。この手法で用いられるアルゴリズムのことを**疑似乱数生成器**と呼び、その出力を**疑似乱数**と呼ぶ。疑似乱数生成器の設計においては、計算効率とその出力の質（何らかの基準において、ランダムな種に対する出力の分布が所望の確率分布とどの程度近いか）とが一般にトレードオフの関係にあり、どちらをどの程度優先すべきかは疑似乱数の用途によって変化する。

疑似乱数生成器の構成法に関しては多数の研究が存在する。その中で一風変わった手法として、カオス的な挙動を示す写像の一つであるロジスティック写像（のパラメータ $\mu = 4$ の場合）

$$L(x) := 4x(1-x) \quad (0 < x < 1)$$

の出力を疑似乱数に転用する研究がある（例えば [30] など）。荒木、宮崎、上原 [1] は、このロジスティック写像の値をスケーリングした上で有限精度の整数区間に落とし込んでできる写像

$$L_n(x) := \left\lfloor \frac{x(2^n - x)}{2^{n-2}} \right\rfloor \quad (x \in X_n := [2^n - 1])$$

の疑似乱数への応用について研究を行った（ここで n は非負整数のパラメータである）。そこでは、集合 X_n 上の値をとる疑似乱数生成器の内部状態 s について、その値を $s \leftarrow L_n(s)$ と更新しつつ s から何らかの形で定まる出力値を得る、という手順を繰り返し、それらを連結したものを最終的な出力とする、という構成法が考えられていた。しかし、この構成法では、一旦内部状態の値が $s = 2^{n-1}$ となってしまうと、更新後の値が $L_n(s) = 2^n$ となり集合 X_n からはみ出てしまうし、もしそれを許容するとしても、さらに次の値は $L_n(2^n) = 0$ となり、以降は内部状態が $L_n(0) = 0$ と一定値をとるため、疑似乱数に求められるランダム性が失われてしまう。この問題を解決する安直な方法としては、入力となる種の範囲から 2^{n-1} を除外する方法が考えられる。しかし、$L_n(x) = 2^{n-1}$ を満たす別の入力値 $x \in X_n$ が存在する場合には、それらの入力値も除外する必要が生じるため、処理が煩雑になってしまうという問題がある。筆者はこの点について、2^{n-1} 以外に除外すべき入力が生じるようなパラメータ n の漸近的な割合に興味を持ち研究を行った [22]。

問題の定式化のために以下の定義を導入する。

定義 2. 整数のパラメータ $n \geq 2$ が**悪い**とは、$L_n(x) = 2^{n-1}$ を満たす $x \in X_n$ が存在することと定める。

ここで考える問題は、2 以上の整数全体の中に悪いパラメータ n がどの程度の割合で存在するかである。前述の論文 [22] の主結果を述べるためにいくつか記号を導入する。整数 $N \geq 2$ について、$2 \leq n \leq N$ を満たす悪いパラメータ n の個数を a_N で表す。また、可算無限長のビット列 $w = w_1 w_2 w_3 \cdots$, $w_i \in \{0, 1\}$ について

$$Z(w) := \{i \geq 1 \mid w_i = 0\}, \; r_{\inf}(w) := \liminf_{n\to\infty} \frac{|Z(w) \cap [n]|}{n}, \; r_{\sup}(w) := \limsup_{n\to\infty} \frac{|Z(w) \cap [n]|}{n}$$

と定める。さらに、$\sqrt{2}$ の 2 進法表示の小数点以下 k 桁目を $b_k \in \{0,1\}$ で表す。つまり

$$\sqrt{2} = (1.b_1b_2b_3\cdots)_2$$

である。このとき以下が成り立つ。ここで、実数 $x \in \mathbb{R}$ が基数 d で単純正規であるとは、x の d 進法表示（小数点以下有限桁で止まる場合には、その下に 0 が無限に続いているものとみなす）において 0 から $d-1$ までの各数字が漸近的に同じ割合 $1/d$ だけ現れることと定義される[*13]。

定理 5 ([22])**.** 上記の記号のもと、ビット列 $b = b_1b_2b_3\cdots$ について

$$\limsup_{N\to\infty} \frac{a_N}{N} \geq \frac{5r_{\sup}(b)-2}{3}\,,\ \liminf_{N\to\infty} \frac{a_N}{N} \geq \frac{5r_{\inf}(b)-2}{3}$$

が成り立つ。特に、$r_{\sup}(b) > 2/5$ であるならば、悪いパラメータ n は無限に存在する。さらに、$\sqrt{2}$ が基数 2 で単純正規であるならば、$\liminf_{N\to\infty} a_N/N \geq 1/6$ が成り立つ（つまり、悪いパラメータの割合は漸近的に $1/6$ 以上である）。

なお、$\sqrt{2}$ は基数 2 で単純正規であると予想されており、それが正しければ定理 5 のように悪いパラメータが漸近的に $1/6$ 以上の割合で存在することとなるが、上記の予想は本稿の執筆時点で未解決である。

以下では定理 5 の証明の概略を紹介する。まず定義より、$n \geq 2$ が悪いパラメータであることは

$$2^{n-1} \leq \frac{x(2^n-x)}{2^{n-2}} < 2^{n-1}+1$$

を満たす $x \in X_n$ が存在することと同値である。この不等式を変形すると

$$\sqrt{2^{2n-3}-2^{n-2}} < |2^{n-1}-x| \leq \sqrt{2^{2n-3}} \tag{4}$$

となる。さらに、式 (4) の左辺について

$$\sqrt{2^{2n-3}} - \sqrt{2^{2n-3}-2^{n-2}} = \frac{2^{n-2}}{\sqrt{2^{2n-3}}+\sqrt{2^{2n-3}-2^{n-2}}} > \frac{2^{n-2}}{2\cdot\sqrt{2^{2n-3}}} = \frac{\sqrt{2}}{4}$$

より $\sqrt{2^{2n-3}-2^{n-2}} < \sqrt{2^{2n-3}} - \sqrt{2}/4$ となるため、$x \in X_n$ が

$$\sqrt{2^{2n-3}} - \frac{\sqrt{2}}{4} < |2^{n-1}-x| \leq \sqrt{2^{2n-3}} \tag{5}$$

を満たせば式 (4) も成り立つ。この条件 (5) を満たす $x \in X_n$ が存在することは、左半開区間 $(\sqrt{2^{2n-3}} - \sqrt{2}/4, \sqrt{2^{2n-3}}]$ に整数点が含まれることと同値である。ここで、$\sqrt{2^{2n-3}} = 2^{n-2}\sqrt{2}$ および $\sqrt{2}/4$ の 2 進法表示は

$$\sqrt{2^{2n-3}} = (\cdots.b_{n-1}b_nb_{n+1}b_{n+2}b_{n+3}\cdots)_2\,,\ \frac{\sqrt{2}}{4} = (0.01011\cdots)_2$$

で与えられることから、上の性質はさらに、$\sqrt{2^{2n-3}}$ の小数点以下の部分 $(0.b_{n-1}b_nb_{n+1}b_{n+2}b_{n+3}\cdots)_2$ が、$\sqrt{2}/4 = (0.01011\cdots)_2$ よりも小さいことと言い換えられる。特に、$b_{n-1}b_n = 00$, $b_{n-1}b_nb_{n+1}b_{n+2} = 0100$, $b_{n-1}b_nb_{n+1}b_{n+2}b_{n+3} = 01010$ のいずれかが成り立てば上記の性質が成り立つことがわかる。以上を踏まえて、ビット列 w について

$$P(w) := \{k \geq 2 \mid w_{k-1}w_k = 00 \text{ or } w_{k-1}w_kw_{k+1}w_{k+2} = 0100 \text{ or } w_{k-1}w_kw_{k+1}w_{k+2}w_{k+3} = 01010\}$$

[*13] 例えば 10 進法における $1.000\cdots = 0.999\cdots$ のように 2 通りの無限小数表示をもつ実数も存在するが、その場合はどちらの表示を選んでも「単純正規でない」という結論には影響しない。

と定めると、これまでの議論より、整数 $N \geq 1$ について

$$\frac{a_N}{N} \geq \frac{|P(b) \cap [N]|}{N} \tag{6}$$

が成り立つ。この集合 $P(w)$ について、論文 [22] では以下の性質を示している。

命題 2. どの可算無限ビット列 w についても、

$$\frac{5r_{\inf}(w) - 2}{3} \leq \liminf_{n\to\infty} \frac{|P(w) \cap [n]|}{n} \leq r_{\inf}(w)\,,\ \frac{5r_{\sup}(w) - 2}{3} \leq \limsup_{n\to\infty} \frac{|P(w) \cap [n]|}{n} \leq r_{\sup}(w)$$

が成り立つ。

定理 5 は命題 2 の不等式それぞれの左側の部分と式 (6) を合わせることで得られる。命題 2 の不等式それぞれの（右側の部分は容易に得られるため、左側の部分の）証明では、w の有限部分列に対して、その中に現れる 0 および 1 の個数を変えずに、3 種類のパターン 00, 0100, 01010 の個数が減るような変形を考える。そして、そうした変形をそれ以上施せないようなビット列の「標準形」を特定した上で、標準形であるビット列に対して所望の不等式を確かめることで、一般の w に対しても同じ不等式が成り立つことを導いている。

7　暗号学的疑似乱数と「病的な反例」

前節で扱った疑似乱数生成器の構成法は、計算効率と出力の質のトレードオフにおいて計算効率を特に重視したものであった。そうした疑似乱数生成器は効率的ではあるものの、暗号技術のように強固な安全性が求められる応用に適しているとは言い難い。一方、計算効率はやや劣るものの、暗号技術の実装にも使用できるような良質な出力をもつ疑似乱数生成器も多く研究されている。そのような疑似乱数生成器は**暗号学的**疑似乱数生成器と呼ばれている。

暗号学的疑似乱数生成器の概念の定式化を述べるために、定義をいくつか準備する。

定義 3. 非負整数全体の集合 $\mathbb{Z}_{\geq 0}$ から非負実数全体の集合 $\mathbb{R}_{\geq 0}$ への関数 $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ が**無視できる**とは、どの正の整数 k についても、それに応じて $N \in \mathbb{Z}_{\geq 0}$ を適切に選ぶと、$n \geq N$ のとき常に $f(n) < n^{-k}$ が成り立つことと定める。（Landau の記号を用いると、この条件は $f(n) \in n^{-\omega(1)}$ と表すこともできる。）

定義 4. パラメータ $\lambda \in \mathbb{Z}_{\geq 0}$ によって定まる有限集合 S_λ 上の確率分布 D^0_λ, D^1_λ が**計算量的に識別不可能**であるとは、ビットを出力するどの確率的多項式時間アルゴリズム A（つまり、その実行ステップ数が λ に関して多項式オーダーに収まるということ）についても、D^0_λ に従う値 r を入力として A が値 1 を出力する確率と、D^1_λ に従う値 r を入力として A が値 1 を出力する確率の差

$$\mathsf{Adv}(A) := \left|\Pr[1 \leftarrow A(r) \mid r \leftarrow D^0_\lambda] - \Pr[1 \leftarrow A(r) \mid r \leftarrow D^1_\lambda]\right|$$

（これを A の**優位度**と呼ぶ）が λ に関して無視できることと定める。

定義 4 で導入された A の優位度については

$$\begin{aligned}\mathsf{Adv}(A) &= \left|(1 - \Pr[0 \leftarrow A(r) \mid r \leftarrow D^0_\lambda]) - \Pr[1 \leftarrow A(r) \mid r \leftarrow D^1_\lambda]\right| \\ &= 2\left|\frac{\Pr[0 \leftarrow A(r) \mid r \leftarrow D^0_\lambda] + \Pr[1 \leftarrow A(r) \mid r \leftarrow D^1_\lambda]}{2} - \frac{1}{2}\right|\end{aligned}$$

が成り立つ。すなわち A の優位度は、$b \in \{0,1\}$ について A に D_λ^b の値を入力した際にビット b を出力する確率の平均値と $1/2$ との差と（定数倍を除いて）等しく、これは直感的には、A が D_λ^0 と D_λ^1 のどちらの確率分布に従う値を与えられたかを正しく推測する確率が、単にランダムに推測した場合の正答率 $1/2$ からどれだけ離れているか、という値と一致する。つまり定義 4 は直感的には、確率的多項式時間アルゴリズムを用いて二つの確率分布の値を識別しようとしても、ランダムな推測と比べて無視できる程度の正答率の上昇しか実現できない（すなわち、二つの確率分布はそれだけ類似している）、ということを意味している。この概念を用いると、疑似乱数生成器の出力が理想的な（一様な）分布と、暗号技術に利用できるほどの高い精度で似ている、という状況を定式化できる。具体的には以下のように定義される。

定義 5. $\mathcal{R}\colon X \to Y$ を疑似乱数生成器、X をその種の空間、Y をその出力の空間とする。（これらはあるパラメータ $\lambda \in \mathbb{Z}_{\geq 0}$ に応じて定まっているものと暗に仮定する。）$\mathcal{R}$ が**暗号学的**疑似乱数生成器である、もしくは**安全である**、とは、X 上の一様分布に従う種 s から得られる出力 $\mathcal{R}(s) \in Y$ の分布が、Y 上の一様分布と計算量的に識別不可能であることと定める。

暗号分野においては古くから、「何らかの暗号技術の方式 Π が、理想的な（一様な）乱数の使用を仮定したときに安全であり、かつ疑似乱数生成器 $\mathcal{R}$ が安全であれば、Π の内部で用いられる乱数を $\mathcal{R}$ の出力に置き換えた実装もやはり安全である」と認識されてきた[*14]。これは、そもそも定義 5 のような暗号学的疑似乱数生成器の安全性の概念が、さまざまな暗号技術の安全性の定義と相性の良い形で定められていることによるものであり、多くの場合には、具体的な暗号技術の安全性の定義に当てはめて上記「…」部の性質をきちんと証明することも可能である。しかしながら、暗号分野におけるありとあらゆる安全性の定義に対して上記「…」部の性質が実際に確認されたわけではないため、理論上は、件の性質が成り立たないような「方式 Π の安全性」の定義が現存する可能性は一概に否定できないはずである。筆者はこの点に着目した研究を行い、「秘密計算」という種類の暗号技術（次節も参照されたい）の標準的な安全性定義の一つについて、上記「…」部の性質が成り立たないような秘密計算の方式 Π と暗号学的疑似乱数生成器 $\mathcal{R}$ の具体例を構成した。（暗号分野の専門的な内容すぎるためここではその説明は割愛する。詳細は論文 [28] を参照されたい。）この結果は、直感的には成り立つと期待される性質が成り立たない具体例を（かなり人為的に）与えたものであり、数学におけるいわゆる「病的な反例」に近いものである。「病的な反例」の探索は数学者に特徴的な営みにも思われるが、本件は暗号分野の研究でもそうした数学者の特性が役立つ場合があるという実例の一つと言えるであろう。

8 カードを用いた暗号技術と abc 予想

本稿でこれまでに扱ってきた暗号技術は、どれも基本的には電子的な計算機上での利用を想定したものである。一方、暗号分野においては、電子的な計算機を用いる代わりに、トランプのようなカードの列に対して、カードを伏せる・めくる・シャッフルするなどの操作を施すことで暗号的な何らかの計算を行う手法も研究されている。こうした手法は**カードベース暗号**や**カードプロトコル**などと総称されている。

カードプロトコルの具体例として、以下の問題を考える。A さんと B さんの二人の登場人物がおり、A さんがトランプのカードを 2 枚、B さんに中身が見えないように持っているとする。ここで、トランプのカードの裏面の模様はどれも同一で見分けがつかないものと仮定する。この状況において、

[*14] より正確には、これは暗号方式 Π の安全性が計算量的安全性、すなわち攻撃者を確率的多項式時間アルゴリズムとしてモデル化した際の安全性である場合に限定されており、攻撃者のアルゴリズムの計算複雑度と無関係な安全性（情報理論的安全性）をもつ暗号方式についてはその限りではない（情報理論的安全性は保たれず、計算量的安全性に低下する）ことを注意しておく。

- B さんは A さんのカードのどちらか 1 枚（左側または右側）の中身を見たいと思っているが、どちらを見たいと思っているのかを A さんには秘密にしたい。
- 一方で A さんは、B さんが選んだ方のカードの中身を見せることは構わないが、もう片方のカードの中身は秘密のままにしたい。

この条件をどうすれば達成できるだろうか？ 例えば、失敗例として、単に B さんが A さんのカードの一方を（指差すなどの形で）指定して A さんがそのカードを見せるのでは、上記の前者の条件に合致しない。一方、A さんがカードを両方とも B さんに渡して、B さんが自分の見たい側のカードの中身を（どちらのカードを見ているかを隠しつつ）覗き見るのでは、A さんの立場ではもう片方のカードの中身を B さんに覗き見られない保証がないため、上記の後者の条件に合致しない。

この問題については例えば以下の解決法（図 2）が存在する（これは水木と曽根による AND 関数に対するカードプロトコル [18] のアイデアを応用したものである）。

1. A さんはカードを 2 枚とも裏向きに伏せて置く。
2. B さんは、中身を見たいカードの上に〇印のカードを伏せて置き、もう片方のカードの上に × 印のカードを伏せて置く[*15]。
3. 重なった 2 枚のカードの束を保ったまま、それらの束どうしをシャッフルして、元々どちらの束がどちらに置いてあったのかがわからないようにする。
4. 各々の束の上側の（つまり、元々 B さんが置いた）カードをめくり、〇印が書かれたカードの下側にあるカードを B さんが受け取って、A さんに見られないようにそのカードの中身を見る[*16]。

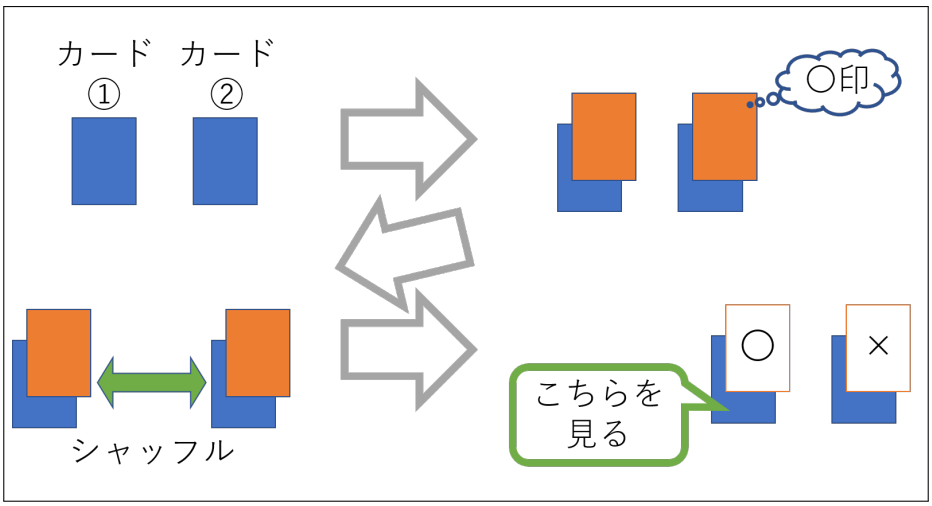

図 2　カードプロトコルの具体例

厳密な議論は割愛するが、この方式では「〇印のカードと B さんが見たいカードが束になっている」という性質がシャッフルしても変わらないため、B さんは確かに所望のカードの中身を見ることができる。一方で、〇印のカードが元々どちらに置かれていたか（つまり、B さんがどちらのカードを見たいのか）はシャッフルの

[*15] 直感的な理解のために「〇印」「× 印」と呼んでいるが、両者の区別が付きさえすればよいので、例えば「ハートの A」と「クラブの A」などでも構わない。
[*16] B さんが見たカードの中身を A さんも見てしまうと、B さんがどちらのカードを見たのかがわかってしまい不適切である。

効果で特定できなくなっており、また B さんはカードの中身を 1 枚だけしか見ないので、前述の二つの条件がどちらも満たされる。こうして上記の問題が確かに解決されていることがわかる。一般に、上記の方式のように「複数の参加者が、各自の入力情報（この例では、B さんがどちらのカードの中身を見たいのか、および A さんのもう片方のカードの中身が何なのか）をお互いに秘匿したままで、協力して所望の出力だけを得る」ための暗号技術を**秘密計算**という。秘密計算については、電子的な計算機で実行する方式が多数研究されているだけでなく、秘密計算を実現するカードプロトコルもいろいろと研究されている。カードプロトコルについては、日本語での概説論文も水木 [19] により記されている。

以降では、Crépeau と Kilian による 1993 年の論文 [4] で提起されている、不動点のない秘密の置換を一様ランダムに生成するカードプロトコルの構成という問題を取り扱う。整数 $n \geq 2$ について、不動点のない n 文字の置換の集合を D_n で表す。すなわち

$$D_n := \{\sigma \in S_n \mid \text{どの } i \in [n] \text{ についても } \sigma(i) \neq i\}$$

である。$d_n := |D_n|$ とおく。問題は、一様ランダムな $\sigma \in D_n$ を何らかの形で符号化したカード列[*17]を、出力のカードがすべて裏向きであり σ についての情報が秘匿された状態で生成するというものである。この問題を素朴に解決しようとすると、D_n ではなく S_n 全体から一様ランダムに σ を（秘密計算のカードプロトコルを適宜用いて、どの置換が選ばれたかを秘匿した状態で）選び、$\sigma \in D_n$ かどうかを（同様に、σ を秘匿したままで）判定し、$\sigma \notin D_n$ であれば σ を選ぶ段階からやり直す、という方法が考えられる[*18]。しかしこの方法では、運が悪いと毎回 $\sigma \notin D_n$ となる σ が選ばれてしまい、いつまで経っても手順が終わらない可能性がある[*19]。それを避けるために、一定の回数だけ失敗した場合には予め選んでおいた何らかの元 $\sigma \in D_n$ を出力する、という代替案も考えられるが、その場合には出力の確率分布が D_n 上の一様分布からわずかながら外れるという別の問題が生じる。こうした問題を防止し、有限回のステップで必ず終了し、かつ出力の分布が D_n 上一様であるような手順を考えたい。素朴な方法としては、予め D_n の元（を符号化したカード列）を列挙しておき、それらの中から一様ランダムに出力を選ぶ、という方法が考えられる。しかし、D_n は $n \to \infty$ のとき $|S_n|/e = n!/e$ 程度の個数の要素を持つため、D_n の元の列挙に必要なカード枚数が膨大になってしまい、とても現実的な手法とはいえない。

この問題について、橋本、筆者、品川、稲村、花岡による論文 [10] では、（出力の秘匿はひとまず不問として、）カードを用いた有限の長さの手順で D_n の元を一様ランダムに生成するのに必要なカード枚数の下界について研究を行った。ここで「カードを用いた手順で」という点がやや曖昧であるが、上記の論文では

> 手順中のランダムな選択はすべて、「ある枚数のカードの中から 1 枚を一様ランダムに選ぶ」操作の組み合わせにより実現される

という仮定を導入している。この仮定はそれほど強い仮定ではなく、例えば、S_n の元 τ を一様ランダムに選ぶ操作は、「$\tau(1)$ の値を（n 枚のカードを用いて）一様ランダムに選ぶ」「残る候補から、$\tau(2)$ の値を（$n-1$ 枚のカードを用いて）一様ランダムに選ぶ」…「残る候補から、$\tau(n-1)$ の値を（2 枚のカードを用いて）一様ランダムに選ぶ」「残った値を $\tau(n)$ の値とする」という一連の操作で、上記の仮定の範疇で実現できる。この設定のもと、上記の論文 [10] では以下の結果を与えている。

[*17] 例えば、ハートとクラブの 2 種類のカードを用いて、ハートが 1、クラブが 0 を表すとして、値 $\sigma(i)$（$i \in [n]$）の各々を 2 進法表示したカード列によって σ を表す、といった方法が考えられるが、以下の議論はそうした特定の符号化の方法には依存しない。

[*18] D_n から直接選ぶのではなく S_n からの選択を介している理由は、後述のように S_n の元については効率的な方法で一様ランダムな生成が可能だからである。

[*19] より正確には、手順の終了までのステップ数に有限な上界が存在しない、ということである。

定理 6 ([10])**.** 正整数 k の最大の素因数を $P(k)$ で表す。このとき、上記の設定のもとで D_n の元を有限のステップ数で一様ランダムに生成する手順には $P(d_n)$ 枚以上のカードが必要である。また、漸近的に

$$P(d_{n-1}) + P(d_n) \in \Omega(n \log n) \quad (n \to \infty)$$

が成り立つ。

定理 6 の証明の概略は以下の通りである。まず、この手順（Σ で表す）における状態の分岐を根付き木 T として表示したとき、手順 Σ 中の各段階では高々有限通りの分岐しか存在しないことから、T の各頂点から出る辺は有限個である。また、手順 Σ が有限回のステップで常に終了するという条件から、T は長さ無限の道をもたない。ここで、グラフ理論における Kőnig の補題を用いる。

命題 3 (Kőnig の補題)**.** 木 T が無限個の頂点をもち、各頂点から出る辺の個数が有限であるとき、T は長さ無限の道をもつ。

命題 3 を上記の木 T に適用すると、T の頂点数が有限であることがわかる。すなわち、手順 Σ における状態の総数も有限である。このことと上記の仮定から、手順 Σ で用いるカードの枚数を ℓ とするとき、手順 Σ においてある事象が起こる確率の値は、正整数 $\ell' \leq \ell$ について $1/\ell'$ という形の値（つまり、ℓ' 枚のカードを使ったランダムな選択であるカードが選ばれる確率）たちの有限個の和と積で作れる値に限られることがわかる。このときに用いられる値が有限個であることから、得られる値の分母 m は 1 から ℓ までの整数たちの積によって作れる値に限られる。特に $P(m) \leq \ell$ が成り立つ。手順 Σ は D_n の元を一様ランダムに、つまり各々確率 $1/d_n$ で選ぶものであるから、$m = d_n$ について上記の性質が成り立つ。すなわち

$$\ell \geq P(d_n)$$

である。よって定理 6 の前半が成り立つ。

定理 6 の後半の評価式について、d_n が満たす漸化式 $d_n = nd_{n-1} + (-1)^n$ を変形すると

$$\begin{cases} nd_{n-1} + 1 = d_n & (n \text{ が偶数のとき}) \\ d_n + 1 = nd_{n-1} & (n \text{ が奇数のとき}) \end{cases}$$

となる。この関係式に abc 予想 [15, 20] を適用する。abc 予想の主張には表面上は微妙に異なるいくつかの表現方法があるが、ここでは以下の形を用いる。

定理 7 (abc 予想 [15, 20])**.** ε を正の実数とすると、以下を満たす正の定数 K_ε が存在する：a, b, c が互いに素な正整数で $a + b = c$ を満たすとする（特に $a, b \leq c$ である）と、

$$c < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon}$$

が成り立つ。ここで正整数 m について、m の相異なる素因数すべての積を $\mathrm{rad}(m)$ で表す。

特に $\varepsilon = 1$ の場合を考えると、n の偶奇にかかわらず、定理 7 の関係式より

$$d_n < K_1 \cdot \mathrm{rad}(d_n \cdot nd_{n-1} \cdot 1)^2$$

が成り立つ。ここで正の整数 m について、m 以下のすべての素数の積を Π_m で表すと、上の式より

$$d_n < K_1 \cdot \mathrm{rad}(nd_{n-1}d_n)^2 \leq K_1 \cdot n^2 \cdot \mathrm{rad}(d_{n-1})^2 \cdot \mathrm{rad}(d_n)^2 \leq K_1 \cdot n^2 \cdot (\Pi_{P(d_{n-1})})^2 (\Pi_{P(d_n)})^2$$

となり、$n \to \infty$ において

$$\log n + \log \Pi_{P(d_{n-1})} + \log \Pi_{P(d_n)} \geq \frac{\log d_n - \log K_1}{2} \in \Omega(\log d_n)$$

が成り立つ。漸近的に $d_n \sim n!/e$ であることと、階乗 $n!$ に対する Stirling の公式を用いると、右辺は

$$\Omega(\log d_n) = \Omega(\log(n!)) = \Omega(n \log n)$$

となり、したがって

$$\log \Pi_{P(d_{n-1})} + \log \Pi_{P(d_n)} \in \Omega(n \log n)$$

となる。さらに、m 以下の素数の個数を π_m で表すと、

$$\begin{aligned} \log \Pi_{P(d_{n-1})} + \log \Pi_{P(d_n)} &\leq \log \left(P(d_{n-1})^{\pi_{P(d_{n-1})}}\right) + \log \left(P(d_n)^{\pi_{P(d_n)}}\right) \\ &= \pi_{P(d_{n-1})} \log P(d_{n-1}) + \pi_{P(d_n)} \log P(d_n) \end{aligned} \tag{7}$$

となる。ここで素数定理より漸近的に $\pi_m \sim m/\log m$ であり、したがって、ある正の定数 α について、$\pi_m \leq \alpha m/\log m$ が常に成り立つ。このことから、式 (7) の右辺は

$$\leq \alpha \frac{P(d_{n-1})}{\log P(d_{n-1})} \log P(d_{n-1}) + \alpha \frac{P(d_n)}{\log P(d_n)} \log P(d_n) = \alpha(P(d_{n-1}) + P(d_n))$$

となる。以上を合わせると

$$P(d_{n-1}) + P(d_n) = \Omega(n \log n)$$

となり、定理 6 の後半の評価式が導かれる。

謝辞

本稿は 2022 年 12 月 17 日、18 日に開催された第 20 回岡シンポジウムにおける筆者の講演内容に基づいています。この場をお借りして、講演の貴重な機会をくださりました、松澤淳一先生をはじめとする奈良女子大学理学部数学コースの先生方に深く御礼申し上げます。

参考文献

[1] Shunsuke Araki, Takeru Miyazaki, Satoshi Uehara, “Analysis for Pseudorandom Number Generators Using Logistic Map”, in: Proceedings of ISITA 2006 (2006)

[2] Joan Boyar, René Peralta, Denis Pochuev, “On the Multiplicative Complexity of Boolean Functions over the Basis (cap, +, 1)”, Theoretical Computer Science **235**(1), pp.43–57 (2000)

[3] David Cash, Matthew Green, Susan Hohenberger, “New Definitions and Separations for Circular Security”, in: Proceedings of PKC 2012, pp.540–557 (2012)

[4] Claude Crépeau, Joe Kilian, “Discreet Solitary Games”, in: Proceedings of CRYPTO 1993, pp.319–330 (1993)

[5] Whitfield Diffie, Martin E. Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory **22**(6), pp.644–654 (1976)

[6] Marten van Dijk, Craig Gentry, Shai Halevi, Vinod Vaikuntanathan, “Fully Homomorphic Encryption over the Integers”, in: Proceedings of EUROCRYPT 2010, pp.24–43 (2010)

[7] Taher El Gamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, in: Proceedings of CRYPTO 1984, pp.10–18 (1985)

[8] Stefan Friedl, “An Elementary Proof of the Group Law for Elliptic Curves”, Groups Complexity Cryptology **9**(2), pp.117–123 (2017)

[9] Craig Gentry, “Fully Homomorphic Encryption Using Ideal Lattices”, in: Proceedings of STOC 2009, pp.169–178 (2009)

[10] Yuji Hashimoto, Koji Nuida, Kazumasa Shinagawa, Masaki Inamura, Goichiro Hanaoka, “Toward Finite-Runtime Card-Based Protocol for Generating a Hidden Random Permutation without Fixed Points”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E101-A**(9), pp.1503–1511 (2018)

[11] IPUSIRON、『暗号技術のすべて』、翔泳社、2017 年

[12] Shizuo Kaji, Toshiaki Maeno, Koji Nuida, Yasuhide Numata, “Polynomial Expressions of Carries in p-ary Arithmetics”, arXiv:1506.02742 (2015)

[13] Neal Koblitz, “Elliptic Curve Cryptosystems”, Mathematics of Computation **48**(177), pp.203–209 (1987)

[14] Édouard Lucas, “Théorie des Fonctions Numériques Simplement Périodiques”, American Journal of Mathematics **1**(3), pp.197–240 (1878)

[15] David William Masser, “Open Problems”, in: Proceedings of the Symposium on Analytic Number Theory, Imperial College London (1985)

[16] Victor S. Miller, “Use of Elliptic Curves in Cryptography”, in: Proceedings of CRYPTO 1985, pp.417–426 (1986)

[17] 光成滋生、『クラウドを支えるこれからの暗号技術』、秀和システム、2015 年

[18] Takaaki Mizuki, Hideaki Sone, “Six-Card Secure AND and Four-Card Secure XOR”, in: Proceedings of FAW 2009, pp.358–369 (2009)

[19] 水木敬明、「カード組を用いた秘密計算」、電子情報通信学会基礎・境界ソサイエティ Fundamentals Review **9**(3), pp.179–187 (2016)

[20] Shinichi Mochizuki, “Inter-Universal Teichmüller Theory IV: Log-Volume Computations and Set-Theoretic Foundations”, Publications of the Research Institute for Mathematical Sciences **57**(1/2), pp.627–723 (2021)

[21] 森山大輔、西巻陵、岡本龍明、『公開鍵暗号の数理』、共立出版、2011 年

[22] Koji Nuida, “Pattern Occurrence in the Dyadic Expansion of Square Root of Two and an Analysis of Pseudorandom Number Generators”, INTEGERS: Electronic Journal of Combinatorial Number Theory **10**, pp.111–127 (2010)

[23] Koji Nuida, Kaoru Kurosawa, “(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces”, in: Proceedings of EUROCRYPT 2015 (Part I), pp.537–555 (2015)

[24] 縫田光司、『耐量子計算機暗号』、森北出版、2020 年

[25] Koji Nuida, “Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory”, in: International Symposium on Mathematics, Quantum Theory, and Cryptography, Mathematics for Industry book series vol.33, Springer, pp.57–78 (2021)

[26] Koji Nuida, “Cryptographic Pseudorandom Generators Can Make Cryptosystems Problematic”, in:

Proceedings of PKC 2021 (Part II), pp.441–468 (2021)

[27] Koji Nuida, "On Compression Functions over Small Groups with Applications to Cryptography", arXiv:2208.02468 (2022)

[28] Koji Nuida, "An Elementary Linear-Algebraic Proof without Computer-Aided Arguments for the Group Law on Elliptic Curves", International Journal of Mathematics for Industry **13**(1), article no.2150001 (2022)

[29] Rafail Ostrovsky, William E. Skeith III, "Communication Complexity in Algebraic Two-Party Protocols", in: Proceedings of CRYPTO 2008, pp.379–396 (2008)

[30] Shashikant C. Phatak, Sumathi Suresh Rao, "Logistic Map: A Possible Random-Number Generator", Physical Review E **51**(4), pp.3670–3678 (1995)

[31] Joseph H. Silverman, John Tate, "Rational Points on Elliptic Curves" (2nd ed.), Springer (2015)

[32] Carl Sturtivant, Gudmund Skovbjerg Frandsen, "The Computational Efficacy of Finite-Field Arithmetic", Theoretical Computer Science **112**(2), pp.291–309 (1993)