2次元超特異非超特別同種写像グラフに関する予想に基づくLTZハッシュ関数への衝突攻撃

大橋 亮[1,a)]　小貫 啓史[1,b)]

概要：2023 年に LeGrow-Ti-Zobernig は有限体 $\mathbb{F}_{p^4}$ 上の超特異だが超特別でないアーベル曲面間に定まる $(2,2)$-同種写像グラフを利用した, 暗号学的ハッシュ関数 (以下 LTZ ハッシュ関数と呼ぶ) を提案した. 提案者らは LTZ ハッシュ関数に対しての衝突探索に必要となる時間計算量と空間計算量を, 共に $\widetilde{O}(p^3)$ と見積もっていた. 本稿ではまず LTZ ハッシュ関数で用いる同種写像グラフにおいて, より小さい体 $\mathbb{F}_{p^2}$ 上で定義される頂点数に関する予想を提示する. 次に我々の予想に基づき, 時間計算量は変わらず $\widetilde{O}(p^3)$ である一方, 必要なメモリを $O(\log(p)^2)$ に抑えた LTZ ハッシュ関数に対しての衝突探索アルゴリズムを提案する. このアルゴリズムを実際に Rust で実装した結果, 現在 35–37bit の安全性を有するとされるパラメータに対して, メモリ使用量は 26.2MB 以内で平均 20.2 時間で衝突を発見することに成功した.

キーワード：ハッシュ関数, 同種写像暗号, 超特異アーベル曲面

A collision attack on the LTZ hash function based on a conjecture on supersingular non-superspecial isogeny graphs of dimension 2

Ryo Ohashi[1,a)]　Hiroshi Onuki[1,b)]

Abstract: In 2023, LeGrow, Ti, and Zobernig proposed a cryptographic hash function (we refer to it as the LTZ hash function), based on a certain $(2,2)$-isogeny graph between supersingular non-superspecial abelian surfaces defined over $\mathbb{F}_{p^4}$. The authors estimated that both the time and space complexities required to find a collision in the LTZ hash function are $\widetilde{O}(p^3)$. In this paper, we first propose a conjecture on the number of vertices defined over the smaller field $\mathbb{F}_{p^2}$ in the isogeny graph used by the LTZ hash function. Based on our conjecture, we then propose a collision-finding algorithm for the LTZ hash function, which retains the same time complexity $\widetilde{O}(p^3)$, while reducing the required memory to $O(\log(p)^2)$. We implemented our algorithm in Rust and successfully found a collision for the parameters claimed to provide 35–37 bits of security within 26.2 MB of memory usage on average in 20.2 hours.

Keywords: Hash function, Isogeny-based cryptography, Supersingular abelian surfaces

1. 導入

耐量子計算機暗号の有力な候補の 1 つに**同種写像暗号**があり, 多くのプロトコルは, 与えられた超特異楕円曲線間の同種写像を求めることの困難性を安全性の根拠としている. 超特異楕円曲線を用いた最初の同種写像暗号プロトコルは Charles ら [4] が 2009 年に提案した暗号学的ハッシュ関数 (CGL ハッシュ関数) であり, 構成には超特異楕円曲線間の**同種写像グラフ**を利用する. 基礎体の標数 $p > 0$ に対して, この同種写像グラフの頂点数は約 $p/12$ であり, したがってグラフ内のサイクルを Pollard-ρ 法によって時間計算量と空間計算量が共に $\widetilde{O}(p^{1/2})$ で見つけることができる (なお, 本稿において全ての計算量は古典計算量で考える). 一方でこの同種写像グラフに対して Eisenträger ら [6] が提案した

[1] 東京大学大学院情報理工学系研究科
Graduate School of Inforation Science and Technology, The University of Tokyo
[a)] ryo-ohashi@g.ecc.u-tokyo.ac.jp
[b)] hiroshi-onuki@g.ecc.u-tokyo.ac.jp

より効率的なサイクル探索アルゴリズムも存在し, 彼らの手法を適用すると, 必要な時間計算量は $\widetilde{O}(p^{1/2})$ のままで, 空間計算量を $\log(p)$ の多項式に抑えられる. 以上のように得られたサイクルは CGL ハッシュ関数の衝突を与えるが, その結果として CGL ハッシュ関数の有する衝突困難性は, 現在 $\widetilde{O}(p^{1/2})$ と見積もられている.

また最近では楕円曲線の 2 次元版であるアーベル曲面を用いた同種写像暗号プロトコルも提案されている. 例えば Castryck ら [3] が 2020 年に提案した暗号学的ハッシュ関数 (CDS ハッシュ関数) では, 構成に**超特別アーベル曲面**間の同種写像グラフを用いる. また 2022 年に LeGrow ら [10] もアーベル曲面を用いたハッシュ関数を提案したが, 彼らは超特別ではない**超特異アーベル曲面**間の同種写像グラフを代わりに利用している. その利点として, グラフの頂点数が増大することに加え, 超特別アーベル曲面の場合に有効なサイクル探索アルゴリズム [5] が適用できないことにより, 結果として CDS ハッシュ関数と比べて高い衝突困難性を有する点が挙げられる. 具体的には, 基礎体の標数 $p > 0$ に対してこの同種写像グラフの頂点数は約 $p^6/2880$ であって, グラフ内のサイクルを Pollard-ρ 法によって時間計算量と空間計算量が共に $\widetilde{O}(p^3)$ で見つけられるが, これが最良の衝突攻撃であろうと提案者らは見積もっている. 表 1 では, 上述した三つのハッシュ関数の安全性, 及びセキュリティパラメータを λ とした場合の基礎体の大きさを纏めている. 表 1 が示す通り LTZ ハッシュ関数では, 扱う基礎体を最も小さく設定できるため, 効率的な計算が可能と考えられる.

表 1 同種写像グラフを利用する主要なハッシュ関数とその基礎体

略称	安全性	基礎体	標数
CGL ハッシュ関数	$\widetilde{O}(p^{1/2})$	$\mathbb{F}_{p^2}$	$p \sim 2^{2\lambda}$
CDS ハッシュ関数	$\widetilde{O}(p)$	$\mathbb{F}_{p^2}$	$p \sim 2^{\lambda}$
LTZ ハッシュ関数	$\widetilde{O}(p^3)$	$\mathbb{F}_{p^4}$	$p \sim 2^{\lambda/3}$

だが LTZ ハッシュ関数の構成に用いる同種写像グラフは超特別アーベル曲面の場合と比べて先行研究が少ないため, 十分な解析が進んでいるとは言えない.

そこで本稿では, まず LTZ ハッシュ関数の構成に用いる同種写像グラフに関してのある予想 (予想 4.3) を提示する. 具体的に言えば, この同種写像グラフの頂点は全て $\mathbb{F}_{p^4}$ 上で定義されるが, そのうち $\mathbb{F}_{p^2}$ 上定義される頂点数を与える. このような頂点を利用して先述の Eisenträger らの手法と似たアイデアに基づき, 我々は LTZ ハッシュ関数に対する衝突攻撃を構成する. 主結果は以下の通りである:

定理 1.1 仮定 4.10 の下で LTZ ハッシュ関数に対しての衝突を, 時間計算量 $\widetilde{O}(p^3)$, 空間計算量 $O(\log(p)^2)$ で求めるアルゴリズムが存在する (**Algorithm 2**).

我々の衝突攻撃は, 従来手法の時間計算量は改善しないが, 空間計算量を $\log(p)$ の多項式に抑えることに成功している.

また実際に我々の衝突攻撃を Rust により実装した結果, 現在 35–37bit 安全だと考えられているパラメータ設定においてメモリ使用量 26.2MB 以内, 平均 20.2 時間で衝突を発見することに成功した. この実験結果の詳細については, 表 4 とそれに続く説明を参照のこと.

2. 数学的な準備

この節では LTZ ハッシュ関数の構成の際に必要となる, 超特異アーベル曲面及びその間に定まる同種写像グラフの性質を簡単に復習する. 以降, 基礎体 k の標数は $p > 5$ とし, その上の曲線やアーベル曲面について考える.

2.1 主偏極付きアーベル曲面と同種写像

群構造を備えた 2 次元射影多様体を**アーベル曲面**という. アーベル曲面 A からその双対 $\hat{A}$ への同型 $A \to \hat{A}$ であり, 豊富な直線束から定まるものを A 上の**主偏極**という. また, アーベル曲面とその上の主偏極 $\mathcal{L}$ の組 $(A, \mathcal{L})$ を**主偏極付きアーベル曲面**とよび, 本稿ではしばしば PPAS と略記する. 任意の PPAS は, 次のいずれかに $\bar{k}$ 上同型である:

- 二つの楕円曲線の直積に, 直積偏極を備えたもの.
- 種数 2 曲線のヤコビ多様体に, 標準偏極を備えたもの.

特に断りのない限り, アーベル曲面 A に対してこのような標準的な主偏極を暗黙に考える. その場合, 主偏極の記述を省略して単に A を PPAS と表記する. 種数 2 曲線 C, C' に対して, それらのヤコビ多様体を $\mathrm{Jac}(C)$, $\mathrm{Jac}(C')$ と書けば Torelli の定理より

$$\mathrm{Jac}(C) \cong \mathrm{Jac}(C') \text{ over } \bar{k} \iff C \cong C' \text{ over } \bar{k}$$

が成立する. 更に, 種数 2 曲線 C, C' が $\bar{k}$ 上同型となるのは, それらの absolute invariants $\in k^3$ が組として一致するとき, かつそのときに限る.

注 2.1 特に k が有限体であれば, 種数 2 曲線が k 上で定義されることと, その absolute invariants が k^3 に属することは同値である. また, この場合に absolute invariants は, 素体 $\mathbb{F}_p$ 上の $O(\log(p))$ 回の加法と乗法で計算可能である.

以降では, 基礎体の標数 p と互いに素な自然数 $N > 1$ を固定して 1 の N 乗根全体の集合を $\mu_N \subset \bar{k}$ と書く. 任意のアーベル曲面 A に対してその N-torsion 部分群を $A[N]$ と書けば $A[N] \cong (\mathbb{Z}/N\mathbb{Z})^4$ が成立する. このとき, 非退化かつ交代的な双線形写像 $A[N] \times \hat{A}[N] \to \mu_N$ が存在する. 特に, もし A が PPAS ならば, これは

$$e_N : A[N] \times A[N] \longrightarrow \mu_N$$

を誘導するが, この写像を A の N-Weil **ペアリング**と呼ぶ. また $A[N]$ の部分群 G であって, 任意の $P, Q \in G$ に対してそれらの Weil ペアリングが $e_N(P, Q) = 1$ を満たすものを等方的であるという. そのような部分群のうち, 包含関係に関して極大なものは $A[N]$ の**極大等方部分群**と呼ばれる.

定義 2.2　主偏極付きアーベル曲面 A に対して, $A[N]$ の基底 $(P_1, P_2; Q_1, Q_2)$ が symplectic であるとは

- $e_N(P_1, P_2) = e_N(Q_1, Q_2) = 1$,
- $e_N(P_1, Q_1) = e_N(P_2, Q_2) = \zeta_N$,
- $e_N(P_1, Q_2) = e_N(P_2, Q_1) = 1$

を満たす 1 の原始 N 乗根 $\zeta_N \in \mu_N$ が存在することをいう.

二つの PPAS 間の全射準同型 $\phi : A \to A'$ であって, その核が有限であるものを**同種写像**という. 基礎体の標数 p と互いに素な整数 $N > 1$ に対して $A[N]$ の極大等方部分群を核に持つ同種写像 ϕ は, 特に (N, N)**-同種写像**と呼ばれる. 核が等しい同種写像 $A \to A'$ は, 終域 A' の自己同型の差を除いて一致するので, これらは同一視される. 任意の A に対して, 始域を A に持つ異なる (N, N)-同種写像の個数は

$$S(N) \coloneqq N^3 \prod_{\text{primes } \ell \mid N} \left(1 + \frac{1}{\ell}\right)\left(1 + \frac{1}{\ell^2}\right) \qquad (2.1)$$

で与えられる (cf. [2], Lemma 2.1). 特に素数 ℓ に対しては, 式 (2.1) は $S(\ell) = (\ell + 1)(\ell^2 + 1)$ となる.

定義 2.3　三つの主偏極付きアーベル曲面 A, A', A'' 間の (N, N)-同種写像 $\phi : A \to A'$, $\phi' : A' \to A''$ に対して,

- $\ker \phi' = \phi(A[N])$ ならば ϕ' を ϕ の**双対拡大**,
- $\ker \phi' \cap \phi(A[N]) = \{0\}$ ならば ϕ' を ϕ の**良い拡大**,
- それ以外であれば ϕ' を ϕ の**悪い拡大**

と呼ぶ. 任意の (N, N)-同種写像 $\phi : A \to A'$ に対して, その異なる良い拡大の個数は N^3 である (cf. [2], Lemma 2.1).

また, 任意の (N^n, N^n)-同種写像 $\psi : A \to A'$ は次のように (N, N)-同種写像 $\phi_1, \ldots, \phi_n$ の合成に分解できる:

$$A = A_0 \xrightarrow{\phi_1} A_1 \longrightarrow \cdots \longrightarrow A_n \xrightarrow{\phi_n} A_{n+1} = A'.$$

但し, 各 $i \in \{1, \ldots, n-1\}$ に対して ϕ_{i+1} は ϕ_i の良い拡大. このような (N, N)-同種写像の列 $(\phi_1, \ldots, \phi_n)$ を, 本稿では長さ n の**良い** (N, N)**-拡大列**と呼ぶことにする.

2.2　超特異アーベル曲面と同種写像グラフ

楕円曲線 E に対して, 群 $E(\bar{k})$ が位数 p の元を持たない場合に E は**超特異**と呼ばれる. アーベル曲面 A に対しても次のように超特異楕円曲線の類似物が考えられる:

定義 2.4　体 k 上定義されたアーベル曲面 A に対して

- ある二つの超特異楕円曲線の直積に, 偏極を無視して $\bar{k}$ 上同種である A を**超特異**という.
- ある二つの超特異楕円曲線の直積に, 偏極を無視して $\bar{k}$ 上同型である A を**超特別**という.

定義より直ちに, 超特別アーベル曲面は超特異である.

Deligne-Ogus-Shioda の定理より, 偏極を無視すれば全ての超特別アーベル曲面は互いに $\bar{k}$ 上同型である. 固定された超特別アーベル曲面 A の主偏極の個数は, A の自己同型の差を除いて約 $p^3/2880$ である (cf. [9]).

種数 2 曲線 C のヤコビ多様体が超特異/超特別か否かは, その曲線の Hasse-Witt 行列により判定可能である. 例えば, 種数 2 曲線 $C : y^2 = x^5 - 1$ の Hasse-Witt 行列を具体的に計算することで, 次の命題が得られる:

命題 2.5 ([9], Proposition 1.13)　標数 $p > 5$ の体上の種数 2 曲線 $C : y^2 = x^5 - 1$ に対して

(1) $p \equiv 1 \pmod 5$ ならば $\mathrm{Jac}(C)$ は超特異でない.
(2) $p \equiv 2, 3 \pmod 5$ ならば $\mathrm{Jac}(C)$ は超特異であるが, 超特別でない.
(3) $p \equiv 4 \pmod 5$ ならば $\mathrm{Jac}(C)$ は超特別である.

また, 曲線 C の自己同型群は $\mathbb{Z}/10\mathbb{Z}$ である.

注 2.6　二つの楕円曲線の直積 $E_1 \times E_2$ が超特異となるのは E_1, E_2 が共に超特異であるとき, かつそのときに限る. すると定義 2.4 より $E_1 \times E_2$ は自動的に超特別になるので, このようなアーベル曲面 (二つの楕円曲線の直積) が超特異かつ非超特別となることはない.

次に $\bar{k}$ 上の超特異楕円曲線 E を固定して, 加法群 $\mathbb{G}_a$ 上の Frobenius 自己準同型の核として得られる群スキーム α_p を考えよう. このとき, 任意の超特異アーベル曲面 A に対して次の短完全系列が存在する:

$$0 \longrightarrow \alpha_p \xrightarrow{\iota_t} E \times E \longrightarrow\!\!\!\!\rightarrow A \longrightarrow 0.$$

ここで, 埋め込み $\iota_t : \alpha_p \to E \times E$ は変数 $t \in \mathbb{P}^1(\bar{k})$ によりパラメータ付けされており, これを embedding parameter とよぶ. 超特異アーベル曲面 $A = (E \times E)/\iota_t(\alpha_p)$ が超特別であることは $t \in \mathbb{P}^1(\mathbb{F}_{p^2})$ に必要十分である (cf. [11]). そこで本稿では $t \in \mathbb{F}_{p^4} \smallsetminus \mathbb{F}_{p^2}$ の場合について議論する. このような超特異アーベル曲面について, 次の主張が知られている:

命題 2.7 ([8], Proposition 2.3)　体 $\bar{k}$ 上で定義された超特異アーベル曲面であり, その embedding parameter が $\mathbb{F}_{p^4} \smallsetminus \mathbb{F}_{p^2}$ に属するものは, 互いに $\bar{k}$ 上同型である.

定理 2.8 ([8], Theorems 1.1 and 1.2)　標数 $p > 5$ の体上の超特異アーベル曲面 A で embedding parameter が $\mathbb{F}_{p^4} \smallsetminus \mathbb{F}_{p^2}$ に属するものを一つ固定する. このとき,

(1) $p \equiv 1, 4 \pmod 5$ ならば A の主偏極の個数は, A の自己同型の差を除いて
$$\frac{p^2(p^2-1)^2}{2880}$$
で与えられる. また A の任意の主偏極 $\mathcal{L}$ に対して, その自己同型群は $\mathrm{Aut}(A, \mathcal{L}) = \{\pm 1\}$ となる.
(2) $p \equiv 2, 3 \pmod 5$ ならば A の主偏極の個数は, A の自己同型の差を除いて
$$1 + \frac{(p+3)(p-3)(p^2-3p+8)(p^2+3p+8)}{2880}$$
で与えられる. また $\mathrm{Aut}(A, \mathcal{L}) = \mathbb{Z}/10\mathbb{Z}$ を満たす A の主偏極 $\mathcal{L}$ が A の自己同型の差を除いて唯一存在して, それ以外の $\mathcal{L}$ に対しては $\mathrm{Aut}(A, \mathcal{L}) = \{\pm 1\}$ となる.

さて, 後の議論では embedding parameter が $\mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$ に属する超特異アーベル曲面 A_0 を固定しよう (命題 2.7 より, そのような A_0 の $\bar{k}$-同型類は一意である). このとき, A_0 の任意の主偏極 $\mathcal{L}$ に対して, 注 2.6 から $(A_0, \mathcal{L})$ は標準偏極を備えたある種数 2 曲線のヤコビ多様体に $\bar{k}$ 上で同型となる. このように $\mathcal{L}$ から標準的に定まる PPAS を $A_{\mathcal{L}}$ と表記してそれらのなす $\bar{k}$-同型類の集合を

$$\mathcal{V}_p \coloneqq \{A_{\mathcal{L}} \mid \mathcal{L} \text{ is a principal polarization on } A_0\}/\cong$$

と定義する. 定理 2.8 より $\mathcal{V}_p$ の要素数は

$$\begin{cases} \frac{p^2(p^2-1)^2}{2880} & \text{if } p \equiv \pm 1 \pmod 5, \\ 1 + \frac{(p+3)(p-3)(p^2-3p+8)(p^2+3p+8)}{2880} & \text{if } p \equiv \pm 2 \pmod 5 \end{cases}$$

で与えられる. 任意の $A \in \mathcal{V}_p$ は $\mathbb{F}_{p^4}$ 上で定義されることが知られている (cf. [10], Lemma 3).

定義 2.9 各素数 $\ell \neq p$ に対して, 次のように定義される多重グラフを $\mathcal{G}(\ell, p)$ と表記する:

- 頂点集合は $\mathcal{V}_p$ とする.
- 辺集合は, 頂点間の (ℓ, ℓ)-同種写像全体とする.

式 (2.1) により $\mathcal{G}(\ell, p)$ は $S(\ell) = (\ell+1)(\ell^2+1)$-正則である. 更に $\mathcal{G}(\ell, p)$ は連結である (cf. [10], Lemma 4).

3. LTZ ハッシュ関数

この節では, 定義 2.9 の超特異同種写像グラフ $\mathcal{G}(2, p)$ を利用して LeGrow ら [10] が構成した暗号学的ハッシュ関数 (**LTZ ハッシュ関数**) 及び, それに対する既存の攻撃手法の概要について説明する.

注 3.1 グラフ $\mathcal{G}(2, p)$ 上の辺 ϕ に対して, 定義 2.3 よりその良い拡大はちょうど 8 本存在する. それらに, 決定的な順序でラベル付けしたものを $\phi^{(0)}, \ldots, \phi^{(7)}$ と書く.

3.1 構成の概要

まず, グラフ $\mathcal{G}(2, p)$ 上の初期辺 $\phi_0 : A_{-1} \to A_0$ を適切に設定する (選び方については 3.2 節で説明する). このとき, 入力 $m \in \{0,1\}^*$ に対して, 次の手順を行う:

Step 1: 入力 m を $m = m_n \cdots m_2 m_1$ と 8 進数展開する. また $i \leftarrow 1$ と定める.

Step 2: 辺 $\phi_{i-1} : A_{i-2} \to A_{i-1}$ の良い拡大 $\phi_{i-1}^{(m_i)}$ を選びそれを $\phi_i : A_{i-1} \to A_i$ とする. もし $i < n$ ならば, 変数 i をインクリメントして *Step 2* を繰り返す.

Step 3: 最終的に計算された辺 ϕ_n の終域 A_n は $\mathbb{F}_{p^4}$ 上のある種数 2 曲線 C_n のヤコビ多様体に同型である. そこで, 曲線 C_n の absolute invariants $\in (\mathbb{F}_{p^4})^3$ を出力する.

注 3.2 もし *Step 2* で双対拡大や悪い拡大も選ぶことを許すと, 長さが 2 や 4 の**自明なサイクル**が存在してしまう (cf. [3], §7.1). すると, 終域が一致するような異なる経路が容易に得られるため, 構成したハッシュ関数の衝突困難性が満たされなくなる.

3.2 初期辺の設定方法

原論文 [10] で初期辺 ϕ_0 の選び方は明示されていないが, 自明な衝突を避けるため慎重に ϕ_0 を設定する必要があり, 我々はその方法を議論する. 以降では基礎体 k の標数 p の条件として $p > 5$ かつ $p \equiv 2, 3 \pmod 5$ を課すものとする. すると命題 2.5 によって種数 2 曲線 $C_{\mathrm{start}} : y^2 = x^5 - 1$ のヤコビ多様体 $A_{\mathrm{start}} \coloneqq \mathrm{Jac}(C_{\mathrm{start}})$ は超特異であって, かつ超特別ではない. また A_{start} の自己同型群は $\mathbb{Z}/10\mathbb{Z}$ であり, 定理 2.8 から $A_{\mathrm{start}} \in \mathcal{V}_p$ を得る (cf. [10], Proposition 1).

注 3.3 素朴に $A_0 \coloneqq A_{\mathrm{start}}$ と設定するのは適切でない. なぜなら A_{start} に隣接する頂点は 3 個であり (cf. [7], §4.15) どのように初期辺 $\phi_0 : A_{-1} \to A_0$ を選んでも, ϕ_0 の異なる良い拡大であり終域が一致するものが存在するためである. これは 3.3 節で述べるように自明な衝突を引き起こす.

そこで, 我々は CDS ハッシュ関数 [3] と同様の解決策で初期辺 ϕ_0 を設定する. 具体的には, 非負整数 $d \geq 0$ に対して決定的に A_{start} を始域とする $(2^{d+1}, 2^{d+1})$-同種写像

$$A_{\mathrm{start}} \longrightarrow A_{-d} \longrightarrow \cdots \longrightarrow A_{-1} \xrightarrow{\phi_0} A_0$$

を計算して $\phi_0 : A_{-1} \to A_0$ を初期辺に設定する.

注 3.4 このような ϕ_0 の選び方は CDS ハッシュ関数においては, もはや安全でないことに注意せよ (cf. [1], §5.4). この衝突攻撃は, 超特異楕円曲線の直積から A_0 への経路を利用するため, 自明には LTZ ハッシュ関数に適用できない. とは言え ϕ_0 の選び方は依然として重要な問題であり, より保守的に何らかの手段を用いて A_{start} から A_0 への経路を秘匿して ϕ_0 を設定する方法も考えられる.

以上のように設定した初期辺 $\phi_0 : A_{-1} \to A_0$ を用いて, 具体的な LTZ ハッシュ関数のアルゴリズムを記述する.

Algorithm 1 $\mathsf{LTZ}(m)$

Input: A message $m \in \{0,1\}^*$.
Output: The hash value of the input m.

1: Let $\phi_0 : A_{-1} \to A_0$ be the initial isogeny defined as above.
2: Write $m = m_n \cdots m_2 m_1$ in octal.
3: **for** $i = 1, \ldots, n$ **do**
4: $\quad \phi_i \leftarrow \mathsf{GoodExtension}(\phi_{i-1}, m_i)$.
5: **end for**
6: **return** $\mathsf{AbsoluteInvariant}(\phi_n) \in (\mathbb{F}_{p^4})^3$.

ここで **Algorithm 1** では, 次のような関数を使用した:

- $\mathsf{GoodExtension}(\phi, j)$: グラフ $\mathcal{G}(2, p)$ 上の辺 ϕ に対してその j 番目の良い拡大 $\phi^{(j)}$ を出力する関数.
- $\mathsf{AbsoluteInvariant}(\phi)$: グラフ $\mathcal{G}(2, p)$ 上の辺 ϕ に対してその終域 (と同型なヤコビ多様体を持つ種数 2 曲線) の absolute invariants を出力する関数.

注 3.5 これらの関数は Mumford 表現や Theta 関数を用いて $\log(p)$ の多項式時間アルゴリズムとして実装できる (詳細は省略するが, 例えば [3] を参照のこと).

3.3 安全性と既存の攻撃手法

上記のように構成された LTZ ハッシュ関数の安全性は, それぞれ次の数学的な問題に帰着される:

問題 3.6 (原像困難性) 与えられた頂点 $A \in \mathcal{V}_p$ に対し, それを終域とする良い $(2,2)$-拡大列

$$A_{-1} \xrightarrow{\phi_0} A_0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n \longrightarrow A$$

を見つけよ.

問題 3.7 (衝突困難性) ある頂点 $A \in \mathcal{V}_p$ を終域とする, 相異なる良い $(2,2)$-拡大列

$$A_{-1} \xrightarrow{\phi_0} A_0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n \longrightarrow A,$$
$$A_{-1} \xrightarrow{\phi_0} A_0 \longrightarrow B_1 \longrightarrow \cdots \longrightarrow B_{n'} \longrightarrow A$$

を見つけよ.

また問題 3.7 は問題 3.6 への帰着が可能であり, したがって結局 LTZ ハッシュ関数の安全性解析のためには問題 3.7 を解くのに必要な計算量を見積もる必要がある. 原論文では, 問題 3.7 を解く最良のアルゴリズムは Pollard-ρ 法, つまり次のような手法であろう, と主張している:

Step 1: 自然数 $N \leftarrow \lfloor \log_8(p^3) \rfloor$ と定める.

Step 2: 初期頂点 A_0 を始域とするような長さ $m \leq N$ の良い $(2,2)$-拡大列 $(\phi_1, \ldots, \phi_m)$ を全て保存する (但し ϕ_1 は初期辺 ϕ_0 の良い拡大の中から選ぶ).

Step 3: *Step 2* で保存された二つの良い $(2,2)$-拡大列の組であって, それらの終域が同型であるものを出力する.

このとき, *Step 2* で保存される良い $(2,2)$-拡大列の全ての個数は $O(p^3)$ で, 一方で $\mathcal{V}_p$ の要素数は $O(p^6)$ だったから, 無視できない確率で上記のアルゴリズムは問題 3.7 の解の出力に成功する. また, 上記のアルゴリズムでは $O(p^3)$ 個の $(2,2)$-同種写像を計算して保存するので, その時間計算量と空間計算量は共に $\widetilde{O}(p^3)$ である. したがって, 原論文では, LTZ ハッシュ関数が λ-bit セキュリティを達成するために用いる基礎体の標数を $p \approx 2^{\lambda/3}$ 程度に設定すれば良い, と述べられている.

なお原論文 [10] で明示的な記述はないが, 暗黙のうちに上述した議論では次のヒューリスティック仮定が置かれていることに注意されたい:

仮定 3.8 十分大きい $m \in \mathbb{N}$ に対して良い $(2,2)$-拡大列 $(\phi_0, \phi_1, \ldots, \phi_m)$ の終域は, 集合 $\mathcal{V}_p$ でほぼ一様に分布する.

仮定 3.8 は, 以下で述べるより弱い予想に基づくものである (cf. 超特別アーベル曲面の場合は Conjecture 3 in [3]).

予想 3.9 任意の頂点 $A \in \mathcal{V}_p$ に対してそれを終域とする良い $(2,2)$-拡大列

$$A_{-1} \xrightarrow{\phi_0} A_0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n \longrightarrow A$$

が存在する.

我々が知る限り予想 3.9 の証明は知られておらず, これの証明及び仮定 3.8 の解析は今後の研究課題である.

4. 主結果

この節の目標は, LTZ ハッシュ関数に対する衝突攻撃を提示することである. そこで, 初めに 4.1 節で攻撃の概要を説明し, 続く 4.2 節で攻撃の根拠となる数学的事実と予想を述べる. 攻撃の具体的なアルゴリズムと, その計算量評価については 4.3 節で与える.

4.1 衝突攻撃の概要

以降で述べる我々の攻撃は, CGL ハッシュ関数に対する Eisenträger ら [6] による攻撃のアイデアに基づく. 以降ではアーベル曲面 A の p^2-Frobenius 共役を $A^{(p^2)}$ と書き, また, 同種写像 ψ の p^2-Frobenius 共役を $\psi^{(p^2)}$ と表記する:

$$\begin{array}{ccc} A & \longrightarrow & A^{(p^2)} \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi^{(p^2)}} \\ A' & \longrightarrow & A'^{(p^2)} \end{array}$$

このとき, 問題 3.7 における相異なる良い $(2,2)$-拡大列を, 次の方針で見つけることを考える:

Step 1: 初期頂点 A_0 を始域とする良い $(2,2)$-拡大列で, その終域 A が $\mathbb{F}_{p^2}$ 上で定義される $(\phi_1, \ldots, \phi_n)$ を見つける (但し ϕ_1 は初期辺 ϕ_0 の良い拡大の中から選ぶ). このとき, これらの合成を $\psi \leftarrow \phi_n \circ \cdots \circ \phi_1 : A_0 \to A$ とする.

Step 2: 初期頂点 A_0 を始域とする良い $(2,2)$-拡大列で, その終域 B が $\mathbb{F}_{p^2}$ 上で定義される $(\phi'_1, \ldots, \phi'_{n'})$ を見つける (但し ϕ'_1 は初期辺 ϕ_0 の良い拡大の中から選ぶ). このとき, これらの合成を $\psi' \leftarrow \phi'_{n'} \circ \cdots \circ \phi'_1 : A_0 \to B$ とする.

Step 3: もし $\psi'' \leftarrow \psi^{(p^2)} \circ \hat{\psi}'^{(p^2)} \circ \psi'$ が $(2^{n+2n'}, 2^{n+2n'})$-同種写像でなければ *Step 2* に戻り ψ' をとり直す. 最後に, 各 ψ, ψ'' に対応する良い $(2,2)$-拡大列の組を出力する.

ここで *Step 1* と *Step 2* で得られた各 ψ, ψ' の終域 A, B は $\mathbb{F}_{p^2}$ 上で定義されていることから $A^{(p^2)} = A$, $B^{(p^2)} = B$ を満たす. したがって $\psi'' := \psi^{(p^2)} \circ \hat{\psi}'^{(p^2)} \circ \psi'$ は図 1 のように初期頂点 A_0 から A への同種写像であることに注意せよ:

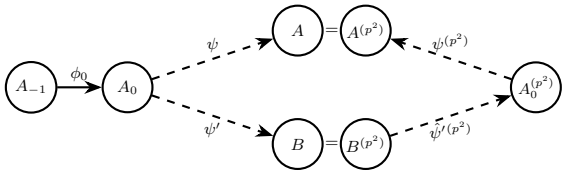

図 1 衝突攻撃の概念図

以上により, *Step 3* で得られる $\psi, \psi'' : A_0 \to A$ に対応する相異なる良い $(2,2)$-拡大列は問題 3.7 の解を与え, すなわち LTZ ハッシュ関数の求める衝突を引き起こす. 残る問題は, このような同種写像 ψ, ψ'' を構成することである. そのため続く 4.2 節では $\mathcal{G}(2,p)$ 内の $\mathbb{F}_{p^2}$ 上定義される頂点に関するいくつかの主張 (と予想) を用意する.

4.2 グラフ内の特殊な頂点に関する主張

引き続き基礎体の標数は $p > 5$ かつ $p \equiv 2, 3 \pmod 5$ を満たすと仮定する. このとき $\mathcal{G}(2,p)$ 内の $\mathbb{F}_{p^2}$ 上定義される頂点に対して, 次のような命題が成立する:

命題 4.1 超特異アーベル曲面 $A \in \mathcal{V}_p$ が有限体 $\mathbb{F}_{p^2}$ 上で定義されるならば, 次の条件 (1)(2) を共に満たす $A[2]$ のある symplectic 基底 $(P_1, P_2; Q_1, Q_2)$ が存在する.

(1) 点 $P_1, P_2 \in A[2]$ は $\mathbb{F}_{p^2}$ 上定義されている.

(2) p^2-Frobenius 自己準同型 $\pi \in \mathrm{End}(A)$ に対して

i. $\pi(Q_1) = Q_1 + P_1$ かつ $\pi(Q_2) = Q_2 + P_2$,

ii. $\pi(Q_1) = Q_1 + P_2$ かつ $\pi(Q_2) = Q_2 + P_1$,

のいずれかを満たす.

更に, 条件 (2) で i. または ii. のいずれが満たされるかは, 超特異アーベル曲面 A の $\bar{k}$-同型類のみに依存する.

紙面の都合上, 命題 4.1 の証明は省略する.

定義 4.2 有限体 $\mathbb{F}_{p^2}$ 上の超特異アーベル曲面 $A \in \mathcal{V}_p$ に対して, 命題 4.1 の条件を満たす $A[2]$ の symplectic 基底を $(P_1, P_2; Q_1, Q_2)$ とする. このとき

- 条件 (2) の i. を満たすならば A を Type I,
- 条件 (2) の ii. を満たすならば A を Type II,

と呼ぶことにする.

なお $\mathbb{F}_{p^2}$ 上の超特異アーベル曲面 $A \in \mathcal{V}_p$ が Type II であることと任意の $P \in A[2]$ に対して $e_2(P, \pi(P)) = 1$ を満たすことは同値である.

さて, 各素数 p に対して有限体 $\mathbb{F}_{p^2}$ 上で定義される超特異アーベル曲面 $\in \mathcal{V}_p$ のうち

- Type I に分類されるものの個数を $N_{1,p}$,
- Type II に分類されるものの個数を $N_{2,p}$

と書くことにする. 以上の表記の下で, 我々は $N_{1,p}, N_{2,p}$ に関する次の予想を提示する:

予想 4.3 任意の $p > 5$ かつ $p \equiv 2, 3 \pmod 5$ を満たす素数 p に対して $N_{1,p}, N_{2,p}$ は次の式で与えられる.

(1) $p \equiv 1 \pmod 4$ ならば

$$N_{1,p} = \left(\frac{p+1}{2}\right)\left(\frac{p-1}{4}\right)^2,$$
$$N_{2,p} = \frac{2}{3}\left(\frac{p+1}{2}\right)\left(\frac{p-1}{4}\right)^2.$$

(2) $p \equiv 3 \pmod 4$ ならば

$$N_{1,p} = \left(\frac{p-1}{2}\right)\left(\frac{p+1}{4}\right)^2,$$
$$N_{2,p} = 0.$$

予想 4.3 が $p \equiv 2, 3 \pmod 5$ を満たす素数 $5 < p < 100$ に対して真であることは計算機による実験で確認できている.

注 4.4 条件 $p \equiv 2, 3 \pmod 5$ が満たされない場合でも, 上記の範囲 $5 < p < 100$ においては, 命題 4.1 と予想 4.3 は成立している.

予想 4.3 はグラフ $\mathcal{G}(2,p)$ 内の $\mathbb{F}_{p^2}$ 上定義される頂点数について述べており, これにより 4.1 節の *Step 1* や *Step 2* で所望の ψ, ψ' が見つかるまでに必要な計算量が見積もれる. 一方で *Step 3* では, 合成 $\psi^{(p^2)} \circ \hat{\psi}'^{(p^2)} \circ \psi'$ における二つの接続部分が, いずれも良い拡大で結ばれている必要がある. より正確には, $\psi = \phi_n \circ \cdots \circ \phi_1$ 及び $\psi' = \phi'_{n'} \circ \cdots \circ \phi'_1$ に対して, 以下の条件が要求される:

- ${\phi_1}^{(p^2)}$ は $\hat{\phi}'_1{}^{(p^2)}$ の良い拡大であり, かつ
- $\hat{\phi}'_{n'}{}^{(p^2)}$ は $\phi'_{n'}$ の良い拡大である.

前者の条件は ϕ'_1 が $\hat{\phi}_1$ の良い拡大であることに同値である. したがって *Step 2* において ϕ'_1 を ϕ_0 の良い拡大であって, かつ $\hat{\phi}_1$ の良い拡大でもあるように選ぶ必要がある. これは次の補題により, 常に可能である.

補題 4.5 主偏極付きアーベル曲面間の $(2,2)$-同種写像で終域 A_0 を共有する $\phi_0, \hat{\phi}_1$ に対して, ϕ_0 の良い拡大であり, かつ $\hat{\phi}_1$ の良い拡大でもある $(2,2)$-同種写像が存在する.

証明. 定義 2.3 より $\phi_0, \hat{\phi}_1$ の良い拡大は各 8 本存在する. 一方で (2.1) より A_0 を始域とする異なる $(2,2)$-同種写像の個数は 15 だから, 鳩ノ巣原理より直ちにしたがう. □

次に, 後者の条件について考察する.

定義 4.6 有限体 $\mathbb{F}_{p^2}$ 上の主偏極付きアーベル曲面 A を始域とする $(2,2)$-同種写像 ϕ が**良い p^2-共役**を持つことを, それが $\hat{\phi}^{(p^2)}$ の良い拡大であることと定義する.

補題 4.7 有限体 $\mathbb{F}_{p^2}$ 上の超特異アーベル曲面 $A \in \mathcal{V}_p$ に対して, 次の主張が成立する:

(1) もし A が Type I ならば, それを始域とする $\mathbb{F}_{p^2}$ 上定義されない $(2,2)$-同種写像の個数は 12 である. うち, 良い p^2-共役を持つものは 8 個である.

(2) もし A が Type II ならば, それを始域とする $\mathbb{F}_{p^2}$ 上定義されない $(2,2)$-同種写像の個数は 8 であって, 全て良い p^2-共役を持つ.

証明. 命題 4.1 の条件を満たす $A[2]$ の symplectic 基底を $(P_1, P_2; Q_1, Q_2)$ とする. また $A[2]$ の極大等方部分群 G を核に持つ $(2,2)$-同種写像を ϕ と書く. このとき

- ϕ が $\mathbb{F}_{p^2}$ 上で定義されない $\iff G \neq \pi(G)$,
- ϕ が良い p^2-共役を持つ $\iff G \cap \pi(G) = \emptyset$

が成立する. 全ての $A[2]$ の極大等方部分群を列挙して π による作用を計算すれば(表 2 及び表 3), 主張を得る. □

表 2 超特異アーベル曲面 $A \in \mathcal{V}_p$ が Type I の場合

G	$\pi(G)$	$G \cap \pi(G)$
$\langle P_1, P_2 \rangle$	$= G$	G
$\langle P_1 + P_2, Q_1, Q_2 \rangle$	$= G$	G
$\langle P_1 + P_2, P_1 + Q_1 + Q_2 \rangle$	$= G$	G
$\langle P_1, Q_2 \rangle$	$\langle P_1, P_2 + Q_2 \rangle$	$\langle P_1 \rangle$
$\langle P_2, Q_1 \rangle$	$\langle P_2, P_1 + Q_1 \rangle$	$\langle P_2 \rangle$
$\langle Q_1, Q_2 \rangle$	$\langle P_1 + Q_1, P_2 + Q_2 \rangle$	$\emptyset$
$\langle Q_1, P_2 + Q_2 \rangle$	$\langle P_1 + Q_1, Q_2 \rangle$	$\emptyset$
$\langle P_1 + Q_2, P_1 + P_2 + Q_1 \rangle$	$\langle P_1 + P_2 + Q_2, P_2 + Q_1 \rangle$	$\emptyset$
$\langle P_1 + Q_2, P_2 + Q_1 \rangle$	$\langle Q_1 + Q_2, P_1 + P_2 + Q_1 \rangle$	$\emptyset$

表 3 超特異アーベル曲面 $A \in \mathcal{V}_p$ が Type II の場合

G	$\pi(G)$	$G \cap \pi(G)$
$\langle P_1, P_2 \rangle$	$= G$	G
$\langle P_1 + P_2, Q_1, Q_2 \rangle$	$= G$	G
$\langle P_1 + P_2, P_1 + Q_1 + Q_2 \rangle$	$= G$	G
$\langle P_1, Q_2 \rangle$	$= G$	G
$\langle P_2, Q_1 \rangle$	$= G$	G
$\langle P_1, P_2 + Q_2 \rangle$	$= G$	G
$\langle P_2, P_1 + Q_1 \rangle$	$= G$	G
$\langle Q_1, Q_2 \rangle$	$\langle P_2 + Q_1, P_1 + Q_2 \rangle$	$\emptyset$
$\langle Q_1, P_2 + Q_2 \rangle$	$\langle P_2 + Q_1, P_1 + P_2 + Q_2 \rangle$	$\emptyset$
$\langle P_1 + Q_1, Q_2 \rangle$	$\langle P_1 + P_2 + Q_1, P_1 + Q_2 \rangle$	$\emptyset$
$\langle P_1 + Q_1, P_2 + Q_2 \rangle$	$\langle Q_1 + Q_2, P_1 + P_2 + Q_1 \rangle$	$\emptyset$

補題 4.7 によって, *Step 2* で見つかった ψ' が後者の条件を満たす確率は $2/3$ 以上である, と見積もれる.

4.3 アルゴリズムと計算量評価

我々の衝突攻撃の具体的なアルゴリズムを提示する前に良い拡大の木構造を次のように定義する:

定義 4.8 グラフ $\mathcal{G}(2,p)$ 内の任意の辺 ϕ に対して, ϕ の**良い拡大の木**を次のように定義する.

- 根ノードは ϕ である.
- 各ノードは, その親ノードの良い拡大である.

このとき, 次のような関数を定義する:

– DFS-GoodExt$(\phi, B, \texttt{bool})$: グラフ $\mathcal{G}(2,p)$ 上の辺 ϕ に対して長さ $\leq B$ の良い $(2,2)$-拡大列 $(\phi, \phi_2, \ldots, \phi_n)$ で終域が $\mathbb{F}_{p^2}$ 上で定義されるものを, ϕ の良い拡大の木を深さ優先探索して見つける. もし bool が true ならば最後の同種写像 ϕ_n が良い p^2-共役を持つまで探索する. 出力はこれらの合成 $\psi := \phi_n \circ \cdots \circ \phi_2 \circ \phi$ とする.

以上の表記の下で, LTZ ハッシュ関数に対する衝突攻撃の具体的なアルゴリズムは次のように記述される.

Algorithm 2 Finding a collision in LTZ hash function

Input: The initial edge ϕ_0 of the LTZ hash function.
Output: Two different chains of good extensions of ϕ_0.

1: $\phi_1 \leftarrow \mathsf{GoodExtension}(\phi_0, 0)$.
2: $i \leftarrow 1$.
3: $\phi_1' \leftarrow \mathsf{GoodExtension}(\phi_0, i)$.
4: **while** ϕ_1' is not a good extension of $\hat{\phi}_1$ **do**
5: $\quad i \leftarrow i + 1$.
6: $\quad \phi_1' \leftarrow \mathsf{GoodExtension}(\phi_0, i)$.
7: **end while**
8: $B \leftarrow \lfloor \log_2(p) \rfloor + 1$.
9: $\psi \leftarrow \mathsf{DFS\text{-}GoodExt}(\phi_1, B, \texttt{false})$.
10: $\psi' \leftarrow \mathsf{DFS\text{-}GoodExt}(\phi_1', B, \texttt{true})$.
11: $\psi'' \leftarrow \psi^{(p^2)} \circ \hat{\psi}'^{(p^2)} \circ \psi'$
12: **return** ψ, ψ''.

出力された同種写像 ψ, ψ'' に対応する $m \neq m'' \in \{0,1\}^*$ を復元することで, 我々は所望の LTZ ハッシュ関数における衝突 $\mathsf{LTZ}(m) = \mathsf{LTZ}(m'')$ を得る.

注 4.9 なお 9 行目で $\hat{\psi}^{(p^2)} \circ \psi$ が良い拡大の合成だった場合は 10 行目を $\psi' \leftarrow \mathsf{DFS\text{-}GoodExt}(\phi_1', B, \texttt{false})$ として, 得られた ψ と ψ' を交換しても良い.

最後に **Algorithm 2** の実行に必要な計算量を見積もる. まず, 予想 4.3 に基づき, 我々は次のヒューリスティックな仮定を置く:

仮定 4.10 超特異アーベル曲面 $A \in \mathcal{V}_p$ とそれを終域に持つ $(2,2)$-同種写像 ϕ に対して, 長さが $n \leq \log_2(p) + 1$ の良い $(2,2)$-拡大列 $(\phi, \phi_2, \ldots, \phi_n)$ で, 最後の同種写像 ϕ_n が良い p^2-共役を持つようなものが, 少なくとも一つ存在する.

以降では, この主張が成り立つと考える理由を説明する. 定理 2.5 より, 集合 $\mathcal{V}_p$ の要素数は約 $p^6/2880$ であった. また予想 4.3 に基づけば, うち $\mathbb{F}_{p^2}$ 上で定義されるものの個数は約 $p^3/32$ であり, その割合は全体の

$$\frac{p^3}{32} \cdot \frac{2880}{p^6} = \frac{90}{p^3}$$

に相当する. 長さ n の良い $(2,2)$-拡大列 $(\phi, \phi_2, \ldots, \phi_n)$ は, 定義 2.3 より 8^{n-1} 個存在する (最初の ϕ が固定されていることに注意せよ) ので, 長さ $n = \lfloor \log_2(p) \rfloor + 1$ では

$$8^{\lfloor \log_2(p) \rfloor} > 8^{\log_2(p)-1} = \frac{p^3}{8}$$

個となる. これらの終域は集合 $\mathcal{V}_p$ でほぼ一様に分布すると仮定でき, したがって $\mathbb{F}_{p^2}$ 上で定義される終域 $\in \mathcal{V}_p$ を持つ長さ $n = \lfloor \log_2(p) \rfloor + 1$ の良い $(2,2)$-拡大列 $(\phi, \ldots, \phi_n)$ は, 約 $90/8 = 11.25$ 個存在すると見積もられる. 補題 4.7 より, 最後の同種写像 ϕ_n が, 良い p^2-共役を持つ確率は $2/3$ 以上なので, 少なくとも一つは所望の $(\phi, \ldots, \phi_n)$ が存在すると考えられる.

いよいよ, 定理 1.1 の証明を行う.

定理 1.1 の証明. まず **Algorithm 2** の正当性から示す. 出力された ψ, ψ'' が同種写像として異なることは対応する良い $(2,2)$-拡大列の長さが異なることから明らか. 以降では出力される直前の ψ, ψ' に対応する良い $(2,2)$-拡大列を

$$(\phi_1, \phi_2, \ldots, \phi_n), \quad (\phi_1', \phi_2', \ldots, \phi_{n'}')$$

としておく. このとき ϕ_n の終域は $\mathbb{F}_{p^2}$ 上で定義されるのでその共役 $\phi_n^{(p^2)}$ の終域と一致する. 同様に, $\phi_{n'}'$ と $\phi_{n'}'^{(p^2)}$ の終域は一致する. また $\hat{\phi}_1^{(p^2)}$ 及び $\hat{\phi}_1'^{(p^2)}$ の終域は, 共に ϕ_0 の終域の共役に一致する. 次に ϕ_1' は $\hat{\phi}_1$ の良い拡大であるが, これは, $\phi_1^{(p^2)}$ が $\hat{\phi}_1'^{(p^2)}$ の良い拡大となることを意味する. 更に 10 行目で $\hat{\phi}_{n'}'^{(p^2)}$ が $\phi_{n'}'$ の良い拡大であるように ψ' が選ばれる. したがって

$$(\phi_1', \ldots, \phi_{n'}', \hat{\phi}_{n'}'^{(p^2)}, \ldots, \hat{\phi}_1'^{(p^2)}, \phi_1^{(p^2)}, \ldots, \phi_n^{(p^2)})$$

は良い $(2,2)$-拡大列であり, これは ψ'' に対応する. 以上より **Algorithm 2** の出力は正しい.

次に **Algorithm 2** の停止性を示す. 停止性が明らかでないのは 4–7 行目の **while** ループと 9–10 行目だけである. 補題 4.5 により, 前者は高々 6 回の反復で終了する. 後者の関数 DFS-GoodExt の停止性については仮定 4.10 から従う. 以上より **Algorithm 2** は必ず成功する.

最後に **Algorithm 2** の実行に必要な計算量を見積もる. 注 3.5 により関数 GoodExtension は $\log(p)$ の多項式時間で実行でき, 与えられた ϕ_1' が $\hat{\phi}_1$ の良い拡大であるか否かも同様 $\log(p)$ の多項式時間で判定可能である. また, これらは空間計算量 $O(\log(p))$ で実行できる. したがって, 支配的なステップは 9–10 行目の DFS-GoodExt の実行であり,

- 探索されるノードの個数は高々 8^B であり,
- 保存されるノードの個数は高々 B である.

各ノードでは関数 AbsoluteInvariants 及び GoodExtension が一度ずつ呼ばれる (特に `bool` が `true` の場合は良い拡大か否かの判定も行われる). よって DFS-GoodExt 全体では

- 時間計算量 $\widetilde{O}(8^B) = \widetilde{O}(p^3)$,
- 空間計算量 $O(B\log(p)) = O(\log(p)^2)$

となり, これがアルゴリズム全体の計算量に等しい. 以上で証明は完了した. □

5. 計算機による実験

この節では, 前節で提案した LTZ ハッシュ関数に対する衝突攻撃 (**Algorithm 2**) を Rust を用いて実装した結果を報告する.

本実験では $p \equiv 2, 3 \pmod 5$ かつ $35 \leq 3\log_2(p) \leq 37$ を満足する全ての素数 p に対して **Algorithm 2** を実行した. これらの素数は 35bit から 37bit のセキュリティレベルを達成すると期待されるパラメータである. また, この実験を行った環境は

- OS: Ubuntu 22.04.5 LTS,
- CPU: Intel Core i9-14900 (24 コア, 48 スレッド),
- メモリ: 128GB RAM,
- コンパイラ: Rust 1.88.0 (`--release`フラグ有効)

である. 実験の結果は表 4 のようになった.

表 4 LTZ ハッシュ関数に対する衝突攻撃の実験結果

		#(探索頂点)/p^3 1st	#(探索頂点)/p^3 2nd	注 4.9 の割合	所要時間 (秒)	使用メモリ (kB)
$p \equiv 1$ (mod 4)	平均	1.14%	1.48%	48/61	62,109	25,742
	最悪	5.66%	7.02%	—	256,715	26,152
$p \equiv 3$ (mod 4)	平均	1.65%	1.74%	40/57	83,787	25,807
	最悪	9.62%	9.57%	—	346,364	26,168

上記の表の第 2 列及び第 3 列では **Algorithm 2** の 9 行目及び 10 行目での深さ優先探索において, 探索された全部のノード数を p^3 で割った値を示している. 仮定 4.10 により, この値は 100%以下と予想される. 実際の値は 100%よりもかなり小さいが, このことは我々のヒューリスティックが妥当であることを示唆している. また第 4 列では, 注 4.9 の状況が起きた事例数を示している. 第 5 列では攻撃全体に掛かった時間を, 最終列では最大で使用した物理メモリのサイズ (RSS) を示している. 特に最終列の結果から, 我々の衝突攻撃はこの範囲で約 26MB の実用的なメモリサイズで動作していることが分かる.

注 5.1 もし 3.3 節で説明したような, 既存の攻撃手法を利用する場合には, 中間の頂点を全て保存する必要があり, その頂点数はグラフサイズに対して平方根, すなわち約

$$\sqrt{\frac{p^6}{2880}} \approx \frac{p^3}{54}$$

となる. 仮に各頂点の情報が 1byte で保存できたとしても, 既存の攻撃手法では, 我々と同じ実験範囲で 1GB を超える使用メモリになると考えられる.

6. まとめと今後の課題

本稿では, LTZ ハッシュ関数に対しての新たな衝突攻撃 (**Algorithm 2**) を提案した. この攻撃は既存の攻撃手法と比較して

- 時間計算量は $\widetilde{O}(p^3)$ に保ったまま,
- 空間計算量を $\widetilde{O}(p^3)$ から $O(\log(p)^2)$ に改善する.

一方, 本稿で我々が提示した予想 4.3 は未証明であり, その証明は今後の課題である. また CDS ハッシュ関数と同様に非常に特殊な超特異アーベル曲面から初期曲面への経路が秘匿されていないことを利用した更に効率的な攻撃手法が構成できないかについても検討したい.

謝辞 本研究は JST 経済安全保障重要技術育成プログラム JPMJKP24U2 の支援を受けたものである.

参考文献

[1] W. Castryck, T. Decru, P. Kutas, A. Laval, C. Petit, Y. B. Ti: *KLPT^2: Algebraic pathfinding in dimension two and applications*, Crypto 2025, to appear.

[2] W. Castryck, T. Decru: *Multiradical isogenies*, Comtemp. Math. **779**, 57–89, 2022.

[3] W. Castryck, T. Decru, B. Smith: *Hash functions from superspecial genus-2 curves using Richelot isogenies*, J. Math. Cryptol. **14**, 268–292, 2020.

[4] D. X. Charles, K. E. Lauter, E. Z. Goren: *Cryptographic hash functions from expander graphs*, J. Cryptology **22**, No. 1, 93–113, 2009.

[5] C. Costello, B. Smith: *The supersingular isogeny problem in genus 2 and beyond*, PQCrypto 2020, Lecture Notes in Comput. Sci. **12100**, 151–168, 2020.

[6] K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, J. Park: *Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs*, ANTS XIV, Open Book Series **4**, 215–232, 2020.

[7] E. Florit, B. Smith: *An atlas of the Richelot isogeny graph*, RIMS Kôkyûroku Bessatsu **90**, 195–219, 2022.

[8] T. Ibukiyama: *Principal polarizations of supersingular abelian surfaces*, J. Math. Soc. Japan **72**, No. 4, 1161–1180, 2020.

[9] T. Ibukiyama, T. Katsura, F. Oort: *Supersingular curves of genus two and class numbers*, Compos. Math. **57**, 127–152, 1986.

[10] J. LeGrow, Y. B. Ti, L. Zobernig: *Supersingular nonsuperspecial abelian surfaces in cryptography*, Mathematical Cryptology **3**, No. 2, 11–23, 2023.

[11] F. Oort: *Which abelian surfaces are product of elliptic curves?*, Math. Ann. **214**, 35–47, 1975.