次元 2 の同種写像を用いるハッシュ関数に対しての衝突発見アルゴリズム

大橋 亮 [1], 小貫 啓史 [1]
[1] 東京大学大学院情報理工学系研究科
e-mail : ryo-ohashi@g.ecc.u-tokyo.ac.jp

1　はじめに

耐量子計算機暗号の候補の 1 つである**同種写像暗号**が注目されており, 盛んに研究が行われている. その例として Charles-Lauter-Goren [1] は 2009 年に, 超特異楕円曲線間の同種写像グラフを用いて**ハッシュ関数**を構成した. また 2020 年に Castryck-Decru-Smith [2] はその 2 次元版として, 超特別アーベル曲面間の同種写像グラフを用いるハッシュ関数 (本稿では CDS ハッシュ関数と呼称する) を提案した. 彼らの構成において, その初期パス $\phi_0 : A_{-1} \to A_0$ は次のように設定されている.

設定. 基礎体の標数を $p \equiv 5 \pmod 6$ として, 超特異楕円曲線 $E_0 : y^2 = x^3 + 1$ を考える. このとき, ある決定的な $(2,2)$-同種写像の良い拡大列

$$E_0 \times E_0 \longrightarrow A_{-10} \longrightarrow A_{-9} \longrightarrow \cdots \longrightarrow A_{-1} \xrightarrow{\phi_0} A_0$$

を計算して $\phi_0 : A_{-1} \to A_0$ を初期パスに定める.

また, この設定における CDS ハッシュ関数の衝突困難性は, 次の数学問題に帰着される.

問題 (衝突困難性)**.** 種数 2 曲線 C および $(2,2)$-同種写像の良い拡大列 $\phi, \psi : A_0 \to \mathrm{Jac}(C)$ であって

1) 同種写像 ϕ, ψ の核は異なり, かつ

2) 同種写像 ϕ, ψ はいずれも楕円曲線の直積に対応する頂点を通らない

を満たすものを 1 つ見つけよ.

提案者らはこの問題を解くのに必要な計算量を $\widetilde{O}(p^{3/2})$ と見積もっていたが, 本稿ではそれよりも効率的に上記**問題**を解く方法を紹介する.

主結果. 多項式メモリでは時間計算量 $\widetilde{O}(p^{1/2})$ で, 指数メモリでは $\widetilde{O}(p^{3/10})$ で ϕ, ψ を構成できる.

2　衝突攻撃の概要

初めに, 基礎体の標数 p に対して, 次を満たすように自然数の組 (e, N_1, N_2) を定める:

$$N_1 + N_2 = 2^e, \quad \gcd(N_1, N_2) = 1, \quad \text{and} \quad N_1 N_2 > Mp.$$

なお $M > 0$ は標数 p に依らない定数である (詳細は後述する). このとき, 以降で必要になる $E_0[2^e]$ の定義体を大きくさせないために e は小さく取るのが望ましい.

Step 1: 次数が $N_1 N_2$ の自己準同型 $\alpha \in \mathrm{End}(E_0)$ を RepresentInteger アルゴリズム [3] を用いてランダムにサンプリングする. とり方より, ある超特異楕円曲線 E_1, E_2 に対して

$$\begin{array}{ccc} E_0 & \xrightarrow{f_2} & E_2 \\ {\scriptstyle f_1}\downarrow & \swarrow^{\alpha} & \downarrow{\scriptstyle g_1} \\ E_1 & \xrightarrow[g_2]{} & E_0 \end{array}$$

を可換にする N_1-同種写像 f_1, g_1 および N_2-同種写像 f_2, g_2 が存在する (これらは計算しない).

Step 2: 核が $\{([N_1]P, \alpha(P) \mid P \in E_0[2^e]\}$ である $(2^e, 2^e)$-同種写像 Φ は [4, Theorem 1] により直積 $E_0 \times E_0$ から直積 $E_1 \times E_2$ へのパスを与える. そこで, これの初めから 11 歩目までを計算して, 順に $A_{-10}, \ldots, A_{-1}, A_0$ を通らなければ *Step 1* に戻り $\alpha \in \mathrm{End}(E_0)$ をとり直す. この操作を

$$A_{-1} \xrightarrow{\phi_0} A_0 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_{e-13}} A_{e-13} \xrightarrow{\phi_{e-12}} A_{e-12} \longrightarrow E_1 \times E_2$$

なる $(2,2)$-同種写像の良い拡大列を得るまで繰り返す (但し, 各 A_i は楕円曲線の直積に分解しない). 先の定数 M は, この同種写像列が確率的に十分得られると考えられるように設定する.

Step 3: ある $(2,2)$-同種写像 $\psi_{e-11} : A_{e-12} \to A_{e-13}$ であって ϕ_{e-12} の良い拡大でもあるようなものが存在することが示せる. そこで

$$\phi := \phi_{e-13} \circ \cdots \circ \phi_1, \quad \psi := \psi_{e-11} \circ \phi_{e-12} \circ \phi_{e-13} \circ \cdots \circ \phi_1$$

と定めれば, これらは A_0 から A_{e-13} への異なるパスになる. これが求めるものであった.

証明は省略するが自然数 e の大きさを $\frac{1}{2}\log_2(p)$ 程度に設定する必要があり, したがって $E_0[2^e]$ の定義体の大きさを考慮に入れることで, 我々の手法の時間計算量は $\widetilde{O}(p^{1/2})$ と見積もることができる. さらに Meet-in-the-middle 法と組み合わせて時間計算量 $\widetilde{O}(p^{3/10})$ と空間計算量 $\widetilde{O}(p^{3/10})$ で衝突が見つかるように改良することも可能である. これにより, 先述の**主結果**が得られた.

3 実験結果

ここでは基礎体の標数を $p = 2^{125} \times 15 - 1$ に設定する (これは提案者らが 192-bit 安全と主張するパラメータであった). 我々の手法を計算代数システム Magma で実装の上, 異なる組 (e, N_1, N_2) やシード値に対して 128 並列で実行したところ $(e, N_1, N_2) = (86, 2^{85} - 49, 2^{85} + 49)$ に対して

$$m_1 = \texttt{40D66E465EFB9F2B16C17A8DED83564D67494E9717ED32EB58E893B},$$
$$m_2 = \texttt{CC0D66E465EFB9F2B16C17A8DED83564D67494E9717ED32EB58E893B}$$

なる衝突を約 10.84 時間で発見した (これに要した *Step 1–2* の繰り返し回数は 965,229 回であった). このように $E_0[2^e]$ が小さい有限体上で定義される場合には, 我々の手法は多項式時間アルゴリズムとなることを注意しておく.

謝辞 本研究は総務省の「電波資源拡大のための研究開発 (JPJ000254)」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」 の成果である.

参考文献

[1] D. X. Charles, K. E. Lauter and E. Z. Goren: *Cryptographic hash functions from expander graphs*, J. Cryptology **22**(1), 93–113, 2009.

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

[3] D. Kohel, K. Lauter, C. Petit and J. -P. Tignol: *On the quaternion ℓ-isogeny path problem*, LMS J. Comput. Math. **17A**, 418–432, 2014.

[4] E. Kani: *The number of curves of genus two with elliptic differentials*, J. Reine Angew. Math. **485**, 93–121, 1997.

2 次元同種写像を用いた Deuring 対応計算アルゴリズム

小貫 啓史 [1], 中川 皓平 [2]
[1] 東京大学大学院情報理工学系研究科, [2]NTT 社会情報研究所
e-mail : hiroshi-onuki@g.ecc.u-tokyo.ac.jp, kohei.nakagawa@ntt.com

1 概要

Deuring 対応により超特異楕円曲線間の同種写像は四元数代数の極大整環のイデアルと対応する. 与えられた極大整環とその左イデアルに対して, そのイデアルと対応する同種写像を計算するアルゴリズムは ideal-to-isogeny アルゴリズムと呼ばれる.

本稿では, [1] により提案された 2 次元同種写像と楕円曲線の自己準同型環への虚二次体の埋め込みを用いた ideal-to-isogeny アルゴリズム IdealToIsogenyIQO [*1] を概説する. IdealToIsogenyIQO は既存の 1 次元同種写像のみを用いるアルゴリズムに比べて, 楕円曲線の標数に課される条件が弱い. さらに適切に標数を選択することとにより, IdealToIsogenyIQO は既存のものよりも高速となる.

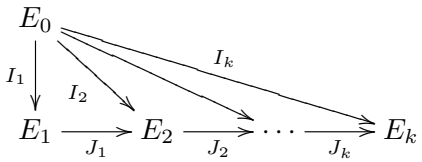
2 提案アルゴリズム

Smooth な整数 m_1, m_2 および整数 f を $p := m_1 m_2 f - 1$ が素数となるように選ぶ. さらに $m_2 > \sqrt{p}$ を仮定する. R を判別式の小さな p が分解しない虚二次体の整数環, $\mathcal{O}_0$ を $\mathcal{B}_{p,\infty}$ の極大整環で R を含むもの, E_0 を $\mathbb{F}_{p^2}$ 上の超特異楕円曲線で自己準同型環が $\mathcal{O}_0$ と同型なものとする. 同型写像 $\iota : \mathcal{O}_0 \to \mathrm{End}(E_0)$ を 1 つ固定し, $\mathcal{O}_0$ と $\mathrm{End}(E_0)$ を同一視する. 以下のアルゴリズムでは, これらは暗黙的に入力として与えられているものとする.

I_1 を $\mathcal{O}_0$ の左イデアルであって, $\mathrm{n}(I_1)$ が m_1 と互いに素なものとし, E_1 を φ_{I_1} の終域とする. このとき, ι と φ_{I_1} が導く同型 $\iota_1 : \mathcal{O}_1 \to \mathrm{End}(E_1)$ が存在する. J を $\mathcal{O}_1$ の左イデアルとし, ι_1 により対応する同種写像を φ_J とする.

2.1 アルゴリズムの概要

IdealToIsogenyIQO は E_1, I_1, $\varphi_{I_1}|_{E_0[m_1 m_2]}$, J を入力とし, φ_J の終域を計算するアルゴリズムである. Generalized KLPT アルゴリズム [2] を用いることにより $\mathrm{n}(J) = m_1^k$ $(k \in O(\log p))$ として良い. $J = J_1 \cdots J_k$ とノルム m_1 のイデアルに分解する. このとき, J_i により対応する同種写像の終域を E_i とする. $\mathcal{O}_0$ の左イデアル $I_1 J_1 \cdots J_{i-1}$ と同等なイデアルであってノルムが m_1 と互いに素なものを I_i とする. イデアルと楕円曲線は以下のように対応する. 矢印は対応する同種写像を表す.



まず, E_i, I_i, $\varphi_{I_i}|_{E_0[m_1 m_2]}$, J_i を入力とし, $I_{i+1}, \varphi_{I_{i+1}}|_{E_0[m_1 m_2]}, E_{i+1}$ を計算するアルゴリズム ShortIdealToIsogenyIQO を構成する. これを繰り返し用いることで φ_J の終域 E_k が計算できる.

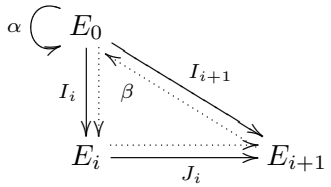
[*1] IQO は Imaginary Quadratic Order の略である.

2.2 ShortIdealToIsogenyIQO

ShortIdealToIsogenyIQO は以下の手順で構成される.

1) $\ker \varphi_{J_i} = \varphi_{I_i}(E_0[I_iJ_i] \cap E_0[m_1])$ を計算する.
2) Velu's の公式を用いて E_{i+1}, $(\varphi_{J_i} \circ \varphi_{I_i})|_{E_0[m_2]}$ を計算する.
3) $\beta \in I_iJ_i$ と $\alpha \in R$ であって, $\mathrm{n}(\beta)/\mathrm{n}(I_iJ_i)$ が m_1m_2 と互いに素であり, $\mathrm{n}(\alpha)+\mathrm{n}(\beta)/\mathrm{n}(I_iJ_i) = m_2$ を満たすものを見つける. ここで $I_{i+1} = \xi_{I_iJ_i}(\beta)$ とする.
4) $\varphi_{I_{i+1}}|_{E_0[m_2]}$ を計算する.
5) $\hat{\varphi}_{I_{i+1}}|_{E_{i+1}[m_1m_2]}$ を計算する.
6) 離散対数問題を解くことで $\varphi_{I_{i+1}}|_{E_{i+1}[m_1m_2]}$ を計算する.

イデアルと楕円曲線は以下のように対応する. ここで $\beta = \hat{\varphi}_{I_{i+1}} \circ \varphi_{J_i} \circ \varphi_{I_i}$ である.



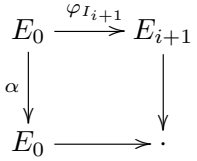
手順 3. 格子 I_iJ_i に格子点列挙を行うことで $\mathrm{n}(\beta)/\mathrm{n}(I_iJ_i) \approx \sqrt{p}$ となる β を複数見つける. その中で $m_2 - \mathrm{n}(\beta)/\mathrm{n}(I_iJ_i)$ が R の元のノルムとなるものを Cornacchia アルゴリズムを用いて求める.

手順 4. 以下の等式により計算される.

$$m_1\varphi_{I_{i+1}} = \frac{1}{\mathrm{n}(I_i)}\varphi_{J_i} \circ \varphi_{I_i} \circ \hat{\beta}.$$

右辺により $E_0[m_1m_2]$ の基底を評価することで $\varphi_{I_{i+1}}|_{E_0[m_2]}$ が計算できる.

手順 5. 以下の図式に Kani の定理 [3] を適用することで計算される.



ここで $\deg(\alpha) + \deg(\varphi_{I_{i+1}}) = m_2$ であることから (m_2, m_2)-同種写像を計算することで $\hat{\varphi}_{I_{i+1}}$ が計算できる.

参考文献

[1] Onuki, H., Nakagawa, K.: Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign, Cryptology ePrint archive 2024/778, 2024.

[2] De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. ASIACRYPT 2020, Part I. LNCS, vol. 12491 (2020), pp. 64–93.

[3] Kani, E.: The number of curves of genus two with elliptic differentials. Journal für die reine und angewandte Mathematik **485** (1997), 93–122.

Gröbner 基底の計算量理論の定式化 — 暗号の安全性解析に向けて

工藤 桃成 [1], 横山 和弘 [2]
[1] 福岡工業大学情報工学部情報通信工学科, [2] 立教大学理学部数学科
e-mail : m-kudo@fit.ac.jp, kazuhiro@rikkyo.ac.jp

1　概要

Gröbner 基底の計算量を厳密に評価することは一般には難しい問題であり, 暗号の安全性解析などにおいても重要な課題となっている. Gröbner 基底の計算量は入力となる生成系のデータの大きさの関数として表され, その計算量を測る指標として**求解次数 (solving degree)** がよく利用される. しかし, 求解次数には定義が 3 種類 (実際には 4 種類) も存在し, 混同されるだけでなく数学的に誤った議論がなされていることも少なくない. 本講演ではまず, これらの異なる定義を正確かつ厳密な形で与えた上で, 大小関係や一致する条件などの基本的性質を示す. 次に, 2024 年春の研究部会連合発表会 (JANT セッション) で紹介した著者による求解次数の評価に関する結果に基づいた, Gröbner 基底の計算量の漸近評価式を明示的に与える. さらに, 暗号の安全性解析 (特に MQ 問題の求解計算量評価) において屡々用いられる (暗号学的) 半正則性仮定を取り上げ, 同仮定下での計算量の漸近評価式を正しい形で述べる. また,「入力多項式系が半正則ではないが半正則である場合と同様の計算挙動になる」という仮定について, 従来の半正則性の定義を拡張することで理論的な定式化が得られたので, これについても紹介するとともに, Fröberg 予想のある種の一般化を提示し, 暗号の安全性解析への応用可能性を示す. 以下では, 上記の講演予定内容のうち主要なもののみ記す.

2　求解次数 (solving degree) と Gröbner 基底の計算量

以下, K を体, $R = K[x_1, \ldots, x_n]$, $F = \{f_1, \ldots, f_m\} \subset R$ とし, $\prec$ を R 上の次数付き項順序とする. また, アルゴリズムの計算量は K における四則演算の回数で評価する. F の $\prec$ に関する Gröbner 基底の計算量を評価するための特徴量の 1 つに求解次数があり, 3 種類 (実際には 4 種類) の定義が存在する. 第 1 の定義として, 正規戦略により Gröbner 基底を計算するアルゴリズム $\mathcal{A}$ を実行した際の step degree の最大値を求解次数と呼び, $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ と表す. $\mathcal{A}$ の実行中に最も計算時間のかかる step degree を求解次数と呼ぶ場合もあるが, そのように定義すると求解次数は $\mathcal{A}$ の実装方法にも依存し得るため, 本稿では考えない. 第 2・3 の定義による求解次数は **Macaulay 行列**を用いて定義され, それぞれ $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$, $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ と表される (mut は **mutant** の略). 第 2・3 の定義による求解次数は採用するアルゴリズムに依存せず F と $\prec$ にのみ依存し, $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ が成り立つ. もし F が斉次なら, $\mathcal{A}$ に適切な設定を施すことで $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) = \mathrm{sd}_{\prec}^{\mathrm{mac}}(F) = \mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ が成り立ち, これは F の $\prec$ に関する簡約 Gröbner 基底の最大総次数 $\mathrm{max.GB.deg}_{\prec}(F)$ に等しい. 一方, F が非斉次の場合, これら 3 つの求解次数は $\mathrm{max.GB.deg}_{\prec}(F)$ 以上となり, その評価は一般には難しい. ただし暗号の分野では, 多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m)$ が**暗号学的半正則**であると仮定し, F の求解次数を**正則性次数** $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ で近似することがあるが, これらは一般には等しくない (ここで F^{top} は F の最大斉次部分). 著者は 2024 年春の JANT において, 同仮定下で $\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 1$ を示した. 今回, この上界評価に基づき, F の Gröbner 基底の計算量に関する評価式を得た：

定理 1　記号は上の通りとし, 非斉次多項式列 $\boldsymbol{F}$ は暗号学的半正則であるものとする. このとき,

1) [1, Theorem 3] ある正規戦略アルゴリズム $\mathcal{A}$ が存在して $\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D-1$, かつ $\mathcal{A}$ の実行中に計算される S 多項式の総次数は $2D-2$ を超えない.

2) さらに, $\mathcal{A}$ の計算量オーダーは次式で上から評価される：

$$m\binom{n+D}{D}^{\omega} + \frac{1}{2}\binom{n+D}{D}^{2}\binom{n+D-1}{D-1}^{2}\binom{n+2D-2}{2D-2}.$$

ここで ω は行列積の指数であり, $2 \leq \omega < 3$ を満たす. また, もし $\mathcal{A}$ の実行中に 0-reduction が一度も起きないと仮定すると, $\mathcal{A}$ の計算量オーダーは次式で上から評価される：

$$m\binom{n+D}{D}^{\omega} + \binom{n+D-1}{D-1}^{2}\binom{n+2D-2}{2D-2}.$$

3　正則性次数および半正則性の拡張

定理 1 の評価式は最悪の評価であり, 実用的にはよりタイトな評価が望まれる. ここでは, 従来の正則性次数および半正則性の定義を拡張することで, より実用的な評価式を導く. 以下では, $\prec$ は次数付き逆辞書式順序とする. また, F^h, $\boldsymbol{F}^h$, $\prec^h$ をそれぞれ F, $\boldsymbol{F}$, $\prec$ の斉次化とし ([1, Section A.2]), $\boldsymbol{F}^{\mathrm{top}}$ を $\boldsymbol{F}$ の最大斉次部分列とする. 有限生成次数付き R-加群 M の Hilbert 関数を HF_M と表す.

定義 2（[1, Definition 2.3.1]）　斉次イデアル $I \subset R$ の**一般化された正則性次数** $\widetilde{d}_{\mathrm{reg}}(I)$ を次で定義する：ある d_0 が存在して, 任意の $d \geq d_0$ に対して $\mathrm{HF}_{R/I}(d) = \mathrm{HF}_{R/I}(d_0)$ が成り立つとき, そのような d_0 の最小値を $\widetilde{d}_{\mathrm{reg}}(I)$ と定める. そのような d_0 が存在しないとき, $\widetilde{d}_{\mathrm{reg}}(I) = \infty$ と定める.

定理 3（[1, Proposition 2.3.4]）　$f_1, \ldots, f_m \in R$ は斉次とは限らない 1 次以上の多項式とする. もし $R/\langle F^{\mathrm{top}}\rangle$ が Artin 的で, かつ $\boldsymbol{F}^{\mathrm{top}}$ が暗号学的半正則であれば, $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) - 1$ および $\max.\mathrm{GB}.\deg_{\prec^h}(F^h) \leq \max\{d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle), \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\}$ が成り立つ.

定義 4（[1, Definition 2.3.3]）　$f_1, \ldots, f_m \in R$ が全て斉次のとき, $\boldsymbol{F}$ が**一般化された暗号学的半正則列**であるとは, $\boldsymbol{F}$ が $\widetilde{d}_{\mathrm{reg}}(\langle F\rangle)$-正則のときをいう. $f_1, \ldots, f_m \in R$ が斉次とは限らない場合, $\boldsymbol{F}$ が一般化された暗号学的半正則列であるとは, $\boldsymbol{F}^h$ が一般化された暗号学的半正則列であるときをいう.

定理 5（[1, Section 4.3]）　$m \geq n$ とし, 非斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m)$ に次の 2 条件：

1) $\boldsymbol{F}^h$ は一般化された暗号学的半正則列, すなわち $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$-正則.

2) $\boldsymbol{F}^{\mathrm{top}}$ は暗号学的半正則, すなわち $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$-正則.

を仮定する (これらの仮定は generic に成り立つことが予想される [1, Conjecture 4.3.4].) このとき,

$$D_{\mathrm{new}} := \begin{cases} \deg\left(\left[\frac{\prod_{i=1}^{m}(1-z^{\deg(f_i)})}{(1-z)^{n+1}}\right]\right) + 1 & (m > n), \\ \sum_{i=1}^{n}(\deg(f_i) - 1) + 1 & (m = n) \end{cases}$$

とおくと, $\max\{d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle), \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\} \leq D_{\mathrm{new}}$ が成り立つ. 従って定理 3 より, F^h の $\prec^h$ に関する Gröbner 基底の (よって F の $\prec$ に関する Gröbner 基底の) 計算量は $O\left(m\binom{n+D_{\mathrm{new}}}{D_{\mathrm{new}}}^{\omega}\right)$ となる.

本節で述べた内容の, 暗号の安全性解析への応用可能性については, 講演内で説明する.

参考文献

[1] M. Kudo and K. Yokoyama, The solving degrees for computing Gröbner bases of affine semi-regular polynomial sequences, MEGA2024 (arXiv:2404.03530 or eprint/2024/52).

