L-007

並列計算環境における同種写像暗号の最適計算法
Optimal strategies for parallel computing of SIDH

森 重義† 岩井 啓輔† 松原 隆† 黒川 恭一†
Shigeyoshi Mori Keisuke Iwai Takashi Matsubara Takakazu Kurokawa

1. はじめに

近年，量子計算機に耐性のある数学的問題を利用した暗号方式(耐量子暗号)の研究が盛んに行われている．耐量子暗号の候補の一つに同種写像の核計算問題を安全性の根拠とする同種写像暗号がある．2011 年に Jao らにより超特異楕円曲線間の同種写像を利用した 2 者間鍵共有(SIDH 鍵共有)方式が提案された[1]．本稿では，NIST の公募に提出されている安全性パラメータ[2][3]を用い，並列計算環境における SIDH 鍵共有で計算時間の多くを占める同種写像計算時間の向上率等を見積もり，計算に割り当てるべき効率の良いプロセッサ数について提案する．

2. 楕円曲線と同種写像

本章においては，SIDH 鍵共有で用いている楕円曲線や同種写像に関する数学的な定義等を準備する．

2.1 楕円曲線(モンゴメリー曲線)

素数 $p>3$ に対して， $n\in\mathbb{N}$ を用いて $q\coloneqq p^n$ とする．
$a,b\in\mathbb{F}_q, a^2\neq 4, b\neq 0$ に対し，

$$E/\mathbb{F}_q: by^2=x^3+ax^2+x \tag{1}$$

で表される曲線を $\mathbb{F}_q$ 上のモンゴメリー曲線と呼び，

$$E(\mathbb{F}_q)\coloneqq\left\{(x,y)\in(\mathrm{F}_q)^2\middle| by^2=x^3+ax^2+x\right\}\cup\{\mathrm{O}_E\} \tag{2}$$

をEの $\mathbb{F}_q$ −有理点群と呼ぶ．(O_EはEの無限遠点)

また，$E/\mathbb{F}_q: by^2=x^3+ax^2+x$ に対し，

$$j(E)=\frac{256(a^2-3)^3}{a^2-4} \tag{3}$$

を E の j −不変量と呼ぶ．

2.2 同種写像と Velu の公式

E,E'を$\mathbb{F}_q$上で定義された楕円曲線とする．このとき写像 $\phi: E\to E'$ が代数的射であり，O_E を $\mathrm{O}_{E'}$ に写すとき ϕ を同種写像と呼ぶ．そして $\ker(\phi)=\{P\in E|\phi(P)=\mathrm{O}\}$ は常に楕円曲線の有限部分群になる．さらに核の濃度が ℓ ならば，ϕ を $\ell-$ 同種写像と呼ぶ．

また，楕円曲線 E とその有限部分群 R が与えられたとき，$\ker(\phi)=R$ となる同種写像 $\phi: E\to E/R$ を明示的に計算することができる．これを$Velu$ の公式と呼び，この公式は ϕ の任意の次数 ℓ で成立する．

3. SIDH 鍵共有

本章では，超特異楕円曲線間の同種写像を利用した 2 者間鍵共有の構成について説明する．

†防衛大学校 National Defense Academy

3.1 パラメータ

$e_A,e_B\in\mathbb{Z},\ell_A,\ell_B$ を小素数$\left(\ell_A^{e_A}\approx\ell_B^{e_B}\right)$とし，素数 $p:=\ell_A^{e_A}\ell_B^{e_B}f\pm 1$を構成する（$f$ はpが素数となるように選択する）．E を位数が$\left(\ell_A^{e_A}\ell_B^{e_B}f\right)^2$ となる超特異楕円曲線とし，P_A,Q_A をE 上の互いに独立な位数$\ell_A^{e_A}$の点，P_B,Q_B をE 上の互いに独立な位数$\ell_B^{e_B}$の点とする．これらの，(p,E,P_A,Q_A,P_B,Q_B) の組をパラメータとする．

3.2 鍵生成

$Alice$ と Bob は各々秘密鍵の$m_A,n_A\in\left(\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}\right)^\times, m_B,n_B\in\left(\mathbb{Z}/\ell_B^{e_B}\mathbb{Z}\right)^\times$ をランダムに選ぶ．そして，それぞれ以下のような $\ell_A^{e_A}-$ 同種写像 ϕ_A , $\ell_B^{e_B}-$ 同種写像 ϕ_Bを計算する．

$$\phi_A: E\to E/<m_AP_A+n_AQ_A>=E_A \tag{4}$$

$$\phi_B: E\to E/<m_BP_B+n_BQ_B>=E_B \tag{5}$$

ここで$Alice$は$(E_A,\phi_A(P_B),\phi_A(Q_B))$を，$Bob$は$(E_B,\phi_B(P_A),\phi_B(Q_A))$を各自の公開鍵とする．

3.3 共有鍵生成

$Alice$ と Bob は互いの公開鍵より以下のような $\ell_A^{e_A}-$ 同種写像 ϕ'_A , $\ell_B^{e_B}-$ 同種写像 ϕ'_Bを計算する．

$$\phi'_A: E_B\to E_B/<m_A\phi_B(P_A)+n_A\phi_B(Q_A)>=E_{AB} \tag{6}$$

$$\phi'_B: E_A\to E_A/<m_B\phi_A(P_B)+n_B\phi_A(Q_B)>=E_{BA} \tag{7}$$

ここで，$E_{AB}\simeq E_{BA}$ より $j(E_{AB})=j(E_{BA})$ を共通鍵とする．

4. 同種写像計算部のアルゴリズムについて

E を楕円曲線，R をE 上の位数ℓ^e の点とし，ℓ^e-同種写像$\phi: E\to E/<R>$ とする．ϕ は e 個の$\ell-$同種写像に分解でき，$E_0=E, R_0=R$ とし，$0\le i\le e$ に対し $\phi_i: E_i\to E_{i+1}=E_i/<\ell^{e-i-1}R_i>, R_{i+1}=\phi_i(R_i)$ とすると，合成写像 $\phi=\phi_{e-1}\circ\cdots\circ\phi_0$ が計算できる．各$\ell-$同種写像ϕ_i は，位数ℓの部分群を得た後，$Velu$ の公式より計算できる．

ℓ^4-同種写像の計算構造は図 1 のような Tree で表せる．

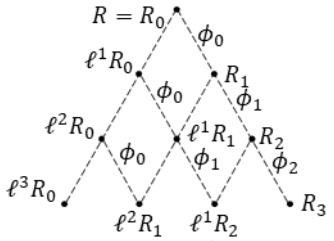

図 1 ℓ^4-同種写像ϕの Tree

図 1 の Tree の各点は楕円曲線上の点を表し，同じ高さの点は全て同じ位数を表す．左下方向の破線の上から下への点の動きは ℓ 倍写像，右下方向の破線の上から下への点の動きは $\ell-$同種写像を意味する．また，同種写像ϕを計算することは右端最下段に到達することと同値である．

この Tree においての最短経路が，最も計算時間の短くなる同種写像計算のアルゴリズムとなる．

4.1 Multiplication based Strategy

先ず，計算時間はかかるものの最も単純なアルゴリズムである Multiplication based Strategy [1]について説明する．

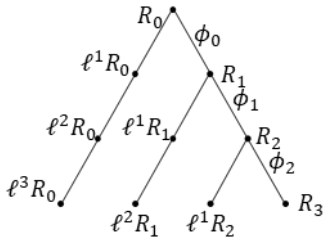

図 2 Multiplication based Strategy の Tree

図 2 の計算構造は，位数ℓ^4 の点$R_0 \in E_0$に対し，ℓ^3倍し，ker $(\phi_0) =< \ell^3R_0 >$ を計算し，$\phi_0(R_0) = R_1 \in E_1$ を計算する．得られたR_1 に対し，ℓ^2倍し，位数ℓ の点を計算し，ϕ_1 を計算する．これを繰り返し，各ℓ −同種写像ϕ_iを合成し，ℓ^4 −同種写像ϕ を計算する．

4.2 Parallelization Strategy

次に A. Hutchison らが提案した SIMD 型並列計算環境における同種写像計算のアルゴリズム[4]を説明する．

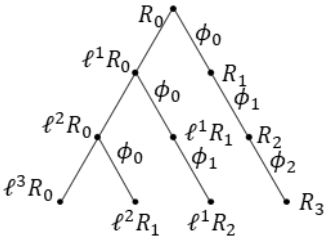

図 3 Parallelization Strategy の Tree

図 3 の計算構造は，計算時間がかかる左下方向のℓ 倍写像演算の回数を減らし，右下方向へのℓ −同種写像演算をプロセッサ数に応じて並列処理したものである．プロセッサ数を K, n を Tree の葉の数とし，$C^K(n) = C^{K/K}(n)$ を Parallelization Strategy での計算時間とすると，

$$C^{k/K}(n) \quad (1 \le k \le K)$$
$$= \begin{cases} \min_{1 \le i < n} (C^{k-1/K}(i) + C^{k/K}(n-i) + (n-i)p + q) & (if\ k > 1) \\ \min_{1 \le i < n} (C^{K/K}(i) + C^{k/K}(n-i) + (n-i)p + iq) & (if\ k = 1) \end{cases} \quad (8)$$

と表せる．全ての分割の計算時間を求めて最も計算時間が小さくなるような分割を行って計算することにより，並列計算環境における効率の良い同種写像計算が行える．

5. 同種写像計算における効率の良いプロセッサ数

米国標準技術研究所(NIST) の公募にも提出されている SIDH 鍵共有ベースの暗号方式である SIKE の安全性パラメータ[2]での，Parallelization Strategy(SIMD 構造)を用いて同種写像計算時間及び向上率を見積もり，計算に割り当てるべき効率の良いプロセッサ数について考察した．

先ずは，NIST の公募にも提出されている SIDH 鍵共有の安全性パラメータについて説明する．

5.1 安全性パラメータ

表 1 は各安全性レベルを満たすパラメータである．SIKEp434 の様な p 後方の値は，パラメータである素数 p のビット長を表す．特に SIKEp503 は古典計算機で 128bit, 量子計算機で 64bit の安全性レベルであり，SIKEp751 は古典計算機で 192bit, 量子計算機で 96bit の安全性レベルである．

表 1 各安全性レベルのパラメータ

Security Level	ℓ_A	e_A	ℓ_B	e_B
SIKEp434	2	216	3	137
SIKEp503	2	250	3	159
SIKEp610	2	305	3	192
SIKEp751	2	372	3	239

5.2 プロセッサ数と計算時間の関係

図 4 は，5.1 のパラメータに則り，$4^{108}(= 2^{216})$ −同種写像及び$4^{125}(= 2^{250})$ −同種写像の計算に要する時間とプロセッサ数との関係である．計算時間の見積りには，CPU:Intel Corei7 3.20GHz で実測したℓ −同種写像を 1.00 とした際の比率を用いた．

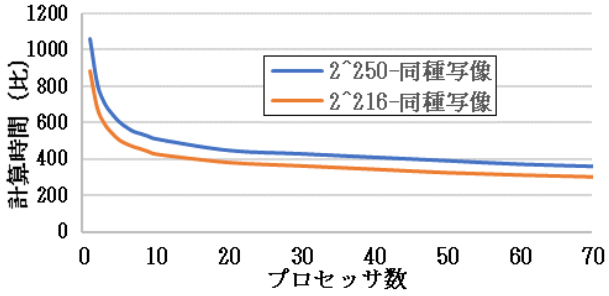

図 4 プロセッサ数と計算時間の関係

5.3 考　察

2^{216} −同種写像，及び2^{250} −同種写像どちらの場合もプロセッサ数を増加させることで計算時間の向上は図れるものの，一定のプロセッサ数からの向上率は効果的でないことがわかった．

6. まとめ

SIMD 型並列計算環境における同種写像に要する最適な計算時間とプロセッサ数の関係について調べ，リソース投入に対する限界について調べた．

本結果より，一定のプロセッサ数からは計算時間の向上率が，著しく鈍い反応になることがわかった．また，プロセッサ数と計算時間の関係は，他の安全性パラメータでもほぼ同様な結果となった．

今後は SIDH 鍵共有方式全体でのプロセッサ数に応じた計算時間を実測し，向上率を調査する．

参考文献

[1] D. Jao, L. DeFeo, “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies,” PQCRYPT2011, pp.19-34, 2011.
[2] D. Jao, “Supersingular Isogeny Key Encapsulation,” Post-Quantum Cryptography Round 2 Submissions, 2019.
[3] C. Costello, P. Longa, M. Naehrig, “Efficient algorithms for supersingular isogeny Diffie-Hellman,” CRYPTO 2016, pp.572-601, 2016.
[4] A. Hutchinson, K. Karabina, “Constructing Canonical Strategies for Parallel Implementation of Isogeny Based Cryptography,” INDOCRYPT2018, pp.169-89, 2018.