SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

同種写像暗号 B-SIDH の実験による計算量評価と効率的な素数 p の条件

Computational Estimation of B-SIDH by Experiments and Condition of Good Prime Number

大槻 紗季 * 青木 和麻呂 † 小貫 啓史 * 高木 剛 *
Saki Otsuki Kazumaro Aoki Hiroshi Onuki Tsuyoshi Takagi

キーワード 耐量子計算機暗号，同種写像暗号，超特異楕円曲線，B-SIDH

あらまし

同種写像暗号は，量子計算機に対する耐性を持つ暗号の中で鍵長が小さいという特長を持つ一方，計算の効率化が課題になっている．特に，計算コストが支配的である同種写像計算の高速化が研究されている．代表的な同種写像暗号として，有限体 $\mathbb{F}_{p^2}$ 上で定義された超特異曲線間の同種写像問題の困難性を基にした鍵交換方式 SIDH [4] がある．また，SIDH をベースとした KEM である SIKE [3] は，NIST の耐量子暗号標準化プロジェクト第 3 ラウンドの候補となっている．

SIDH より更に小さな鍵長を達成する同種写像暗号として B-SIDH [1] が提案された．しかし，B-SIDH は高次の同種写像計算を行うため，計算量が SIDH より大きくなる問題がある．B-SIDH の高速化には，同種写像計算の次数を小さくする定義体の標数 p の構成が研究課題である．具体的には $p\pm1$ がともに smooth であることが望まれ，素数 p の探索法として，拡張ユークリッド法 [1]，$p = 2x^n - 1$ 型 [1]，PTE 法 [2] が提案されてきた．

本研究では，上記の三手法で得られる素数 p に対する鍵交換方式 B-SIDH の計算量を考察する．B-SIDH を Python により実装し，主要な計算コストとなる秘密鍵生成，公開鍵生成，共有鍵生成に対して，$\mathbb{F}_{p^2}$ 上の乗算の演算回数を数えた．実験は，論文 [1] [2] に記載された 128 ビット程度の安全性を実現する 237〜256 ビットの 14 個の素数 p に対して行った．その結果，鍵交換全体の演算回数は，$p\pm1$ の素因数分解に現れる因子の総和の約 17 倍である結果を得た（図 1）．この比率 17 倍の内訳は，同種写像の核計算 (6 倍)，点計算 (10 倍)，係数計算 (1 倍) であり，B-SIDH の計算コストの大部分を占めることが確かめられた．これにより，B-SIDH の計算コストの指標として，定義体の標数 p の $p\pm1$ の因子の総和を用いることができる．

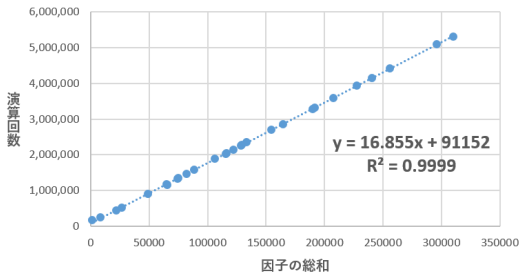

図 1: $p\pm1$ の因子の総和と B-SIDH の演算回数

参考文献

[1] C. Costello. B-SIDH : supersingular isogeny Diffie-Hellman using twisted torsion. ASIACRYPT 2020, LNCS 12492, pp.440-463, 2020.
[2] C. Costello, M. Meyer and M. Naehrig. Sieving for twin smooth integers with solutions to the Prouhet-Tarry-Escott problem. EUROCRYPT 2021, LNCS 12696, pp.272-301,2021.
[3] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik. SIKE: Supersingular Isogeny Key Encapsulation, NIST Post-Quantum Cryptography Project, 2017.
[4] D. Jao, L. De Feo, and J.Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Journal of Mathematical Cryptology, vol.8(3), pp.209-247, 2014.

* 東京大学大学院　情報理工学系研究科, 東京都文京区本郷 7-3-1, The Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, Japan
† 文教大学　情報学部, 神奈川県茅ヶ崎市行谷 1100, Faculty of Information and Communications, Bunkyo University, 1100, Namegaya, Chigasaki-shi, Kanagawa, Japan