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

数体篩法実装は双子 smooth 素数の探索に役立つか?
Can NFS Implementation Find Twin Smooth Primes?

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

Keywords: B-SIDH, twin smooth prime, NFS, line sieve

実用的な量子計算機でも解読が困難とされる耐量子計算機暗号の研究が今世紀に入ってから急速に進んでいる。耐量子計算機暗号研究に特化した国際会議 PQCypto も 2008 年より始まり 2016 年からは毎年開催されている [1]。暗号技術の標準に強い影響力のある米国 NIST も 2016 年より耐量子計算機暗号の標準化 [2] を検討しはじめた。世界中に方式提案を呼びかけ、順調に行けば 2024 年ぐらいまでには標準の草案が出来るとされている。

耐量子計算機暗号として有力なものは格子、符号、多次多変数、同種写像をベースに作られている (例えば [2])。中でも同種写像ベースの方式、すなわち同種写像暗号は、鍵長を短くできる利点があり注目されている。NIST の公募にも SIKE[3] という同種写像暗号が応募されており、Round 3 の alternate candidates にも選ばれている。この SIKE に対して、さらに鍵長を短くする B-SIDH [1] という方式が提案されている。

効率的な B-SIDH を実装する上で、定義体の標数 p について $p\pm1$ が smooth であることが求められており、[6] ではより詳細な条件が出されている。SQISign [4] でも似た条件が必要な素数が必要なことから B-SIDH でも使える素数の探索が行なわれている。ここでは GMP[3] を利用し、6CPU·年を使った探索が行なわれている。一方、smooth な数の探索では、エラトステネスの篩をもとにした素因数分解アルゴリズムに一日の長がある。篩を利用する素因数分解アルゴリズムはいくつかあるが、中でも数体篩法 [5] は 100 桁程度以上の一般的な形の合成数の分解では最も高速であり、いくつかの実装は自由に入手可能である。さらに、篩範囲として、2 つの多項式から得られる値が同時に smooth かどうかの判定を行なうことから、B-SIDH で必要な $p\pm1$ の双方が smooth であるという形に似ている。

本稿では NFS 実装のうちの一つである `msieve`[4] を利用し、B-SIDH にふさわしい素数の探索を行なった結果を報告する。

* 文教大学 情報学部,
〒 253-8550 神奈川県茅ヶ崎市行谷 1100
Faculty of Information and Communications,
Bunkyo University,
Namegaya 1100, Chigasaki-shi, Kanagawa, 253-8550 Japan
(Email: `maro-bunkyo-ac-jp` (適宜「-」を「@」や「.」に変換))
† 東京大学大学院 情報理工学系研究科,
〒 113-8656 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, 113-8656 Japan

[1] `https://pqcrypto.org/conferences.html`

[2] `https://csrc.nist.gov/projects/post-quantum-cryptography`

[3] `https://gmplib.org/`

[4] `https://sourceforge.net/projects/msieve/`

参考文献

[1] Craig Costello. B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology — ASIACRYPT 2020, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 440–463. Springer-Verlag, Berlin, Heidelberg, 2020.

[2] CRYPTREC 暗号技術調査 WG(暗号解析評価). 耐量子計算機暗号の研究同行調査報告書. CRYPTREC TR-2001-2018 (`https://www.cryptrec.go.jp/tech_reports.html`, visited December 9, 2021), 2017.

[3] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8:209–247, 2014. (A preliminary version was presented at PQCrypt 2011.).

[4] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology — ASIACRYPT 2020, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 64–93. Springer-Verlag, Berlin, Heidelberg, 2020.

[5] Arjen Klaas Lenstra and Hendrik Willem Lenstra, Jr., editors. *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, 1993.

[6] Saki Otsuki, Kazumaro Aoki, Hiroshi Onuki, and Tsuyoshi Takagi. Computational estimation of B-SIDH by experiments and condition of good prime number. In *2022 Symposium on Cryptography and Information Security*, SCIS 2022, Osaka, Japan & Online, 2022. Technical Group on Information Security (IEICE). (in Japanese).