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

SQISign の公開鍵の安全性
On the security of the public keys in SQISign

小貫 啓史 *
Hiroshi Onuki

キーワード 耐量子計算機暗号，電子署名，同種写像暗号，SQISign

あらまし

同種写像暗号は耐量子計算機暗号の候補の 1 つであり，鍵長および暗号文長が短いことから注目されている．実際，同種写像を用いた KEM である SIKE [4] は，アメリカ国立標準技術研究所 (NIST) の耐量子計算機暗号標準化プロジェクトの第 3 ラウンドの代替候補となっている．また，2020 年に提案された同種写像を用いた署名方式 SQISign [1] は，NIST 標準化候補の署名と比べて，公開鍵長と署名長の合計サイズが非常に小さいという利点を持つ．しかし，その安全性については未だ十分な議論がなされているとは言えない．

本研究では，SQISign の公開鍵の安全性について議論する．SQISign の設定は以下の通りである．p を $p \equiv 3 \pmod 4$ なる素数，E_0, E_A を $\mathbb{F}_{p^2}$ 上の超特異楕円曲線とする．さらに $j(E_0) = 1728$, 同種写像 $\varphi_s : E_0 \to E_A$ で $\deg(\varphi_s)$ が素数かつ $p^{1/4}$ 以下であるものが存在するとする．ここで p, E_0 が公開パラメータであり，φ_s が秘密鍵，E_A が公開鍵となる．$\deg(\varphi_s)$ が $p^{1/4}$ 以下であることは公開情報だが，その値は秘密情報である．ここで λ ビット安全性を満たす p のサイズは 2λ ビットであるとされている．公開鍵となりうる曲線は $O(p^{1/2})$ 個ある一方，$\mathbb{F}_{p^2}$ 上の超特異楕円曲線はおよそ $p/12$ 個存在する．つまり，公開鍵の候補全体の集合は全ての超特異楕円曲線の集合よりも遥かに小さいものとなる．しかし，$\deg(\varphi_s)$ が $p^{1/4}$ 以下であることを利用した攻撃は知られていない．また，中間一致攻撃 [3] および Delfs-Galbraith アルゴリズム [2] を適用した際の計算量は一般の超特異楕円曲線に対する攻撃同様 $O(p^{1/2})$ であり，鍵空間の全探索と同等であるというのが [1] の主張である．

これを検証するため，まず同種写像グラフにおける E_A の特徴を理論的に解析した．具体的には次を示した．

定理 1. $\varphi : E_0 \to E_A$ を φ_s と異なる同種写像とする．このとき，$\deg(\varphi) \geq p^{3/4}/4$.

この定理は公開パラメータ E_0 と公開鍵 E_A に中間一致攻撃を適用したときの計算量の下限が $O(p^{3/8})$ であることを示している．この下限は期待される計算量 $O(p^{1/2})$ よりも小さいが，一般の曲線では計算量の下限が 0 であることを考えれば，E_0, E_A への中間一致攻撃は最低難易度が保証されている分難しい可能性がある．

次に平均的なケースにおける攻撃の難易度を推定するため，小さな p に対して，2-同種写像グラフ上で中間一致攻撃および Delfs-Galbraith アルゴリズムの実験を行った．実験した範囲では公開鍵 E_A と一般の超特異楕円曲線で安全性に大きな違いは見られなかった．

参考文献

[1] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing.

[2] C. Delfs and S. D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016.

[3] S. D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999.

[4] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik. "SIKE - Supersingular isogeny key encapsulation", Submission to the NIST Post-Quantum Cryptography Standardization project; `https://sike.org`.

* 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
Graduate Shool of Information Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo