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

SIKE に対する vOW 法の内部関数の新計算手法
A new method for computing internal functions of the vOW algorithm for SIKE

神戸 祐太 * 高橋 康 * 相川 勇輔 † 工藤 桃成 ‡
Yuta Kambe Yasushi Takahashi Yusuke Aikawa Momonari Kudo
安田 雅哉 * 高島 克幸 § 横山 和弘 *
Masaya Yasuda Katsuyuki Takashima Kazuhiro Yokoyama

キーワード 超特異楕円曲線暗号，同種写像問題，SIKE，vOW アルゴリズム，Elkies 多項式

あらまし

超特異楕円曲線間の同種写像を用いた鍵カプセル化メカニズム SIKE に対する攻撃法として，van Oorschot-Wiener（vOW）アルゴリズム [1] と呼ばれる衝突探索による中間一致攻撃がある．本稿では，vOW アルゴリズムにおける衝突判定を，従来の j-不変量計算と，Elkies 多項式の計算で行った場合の実験結果を紹介し，両者の計算時間を比較する．

vOW 法の概要 vOW の中間一致攻撃では，標数 $p = k \cdot 2^{e_2} \cdot 3^{e_3} - 1$ を固定したとき，次数 $\ell = 2, 3$ の長さ $e = e_2, e_3$ の $\mathbb{F}_{p^2}$ 上の同種写像パス $E_0 \to E_1$ に対して，位数 $e/2$ の E_0, E_1 の巡回群全体の集合に対応した有限集合 S を考える．S の元に対応した巡回群 $G = \langle R \rangle \subset E_i$ に対して $h(G) = j(E_i/G)$ で定まる関数 $h : S \to \mathbb{F}_{p^2}$ と，ランダムな関数 $g : \mathbb{F}_{p^2} \to S$ を合成して得られる関数 $f = g \circ h : S \to S$ に vOW 法を適用することで，$f(x) = f(x')$ だが $x \neq x'$ となる元が得られる．このとき $h(x) = h(x')$ であれば x, x' が同種写像パス $E_0 \to E_1$ に対する中間衝突に対応する．このように，vOW 法による中間一致攻撃では同種写像の衝突判定に $h : S \to \mathbb{F}_{p^2}$ の反復計算を行うため，h の計算効率が攻撃全体の効率に関わっている．

内部関数の新計算法 野呂-安田-横山 [2] は，同種写像の値域の定義方程式は Elkies 多項式の第 1〜3 係数 t_1, t_2, t_3 によって計算できることを示した．Elkies 多項式は同種写像の核 $G = \langle R \rangle$ について，R のスカラー倍の x 座標を根としてもつ多項式として特徴付けられるため，衝突判定関数 $h : S \to \mathbb{F}_{p^2}$ を $h(G) = (t_1(R), t_2(R), t_3(R))$ に置き換えることができる．

実装比較と今後の課題 本稿では，vOW 法における衝突判定を，従来の j 不変量計算と Elkies 多項式の係数 t_1, t_2, t_3 の計算で行った場合の実験結果を紹介し，両者の計算時間を比較する．標数 $p = 31 \cdot 2^{36} \cdot 3^{22} - 1$，$\ell = 3$ の場合，sage の組み込み関数による $j(E/\langle R \rangle)$ の計算に比べ $t_1(R)$, $t_2(R)$, $t_3(R)$ の平均計算時間は約 10 倍高速であった．しかし，$E \to E/\langle R \rangle$ を次数 3 のパスに分解する逐次的な j 不変量計算に比べると，現状では $t_1(R)$, $t_2(R)$, $t_3(R)$ の平均計算時間は約 127 倍も遅い．今後は t_1, t_2, t_3 を逐次的に計算する手法や，R のスカラー倍計算に SIMD 演算を導入することで効率化を図る．

参考文献

[1] P. C. van Oorschot and Michael J. Wiener, Parallel Collision Search with Cryptanalytic Applications, Journal of Cryptology, Vol. 12, pp. 1–28, 1999.

[2] M. Noro, M. Yasuda and K. Yokoyama, Symbolic Computation of Isogenies of Elliptic Curves by Vélu's Formula, Commentarii Mathematici Universitatis Sancti Pauli, Vol. 68, pp. 93–130, 2021.

* 立教大学 Rikkyo University
† 三菱電機 Mitsubishi Electric Corporation
‡ 東京大学 The University of Tokyo
§ 早稲田大学 Waseda University