Improved supersingularity testing of elliptic curves

Yuji Hashimoto\(^1,2\) and Katsuyuki Takashima\(^3\)

\(^1\)Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8654, Japan
\(^2\)National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 135-0064, Japan
\(^3\)Faculty of Education and Integrated Arts and Sciences, Waseda University, 1-6-1 Nishi-Waseda, Shinjuku-ku, Tokyo 169-8050, Japan

*Corresponding author: hashimoto-yuji715@waseda.jp

Received December 29, 2020, Accepted March 29, 2021

Abstract

In protocols of isogeny-based cryptosystems, we send data of elliptic curves. Then it is necessary to identify supersingularity of the elliptic curves to guarantee the correctness of protocol. Among deterministic algorithms for the purpose, Sutherland proposed an efficient algorithm that utilizes sequences of 2-isogenies computed by using modular polynomials. In this paper, we improve the efficiency of the algorithm by using some properties of \(x\)-coordinates of 2-torsion points instead of modular polynomials. Our experimental result shows that our algorithm succeeded in reducing the computation time by 14 to 32 percent compared to Sutherland’s algorithm.

Keywords isogenies, supersingular elliptic curves, isogeny graphs, Sutherland’s algorithm, post-quantum cryptography

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

All conventional cryptosystems from discrete logarithm or factorization intractability assumption would be totally broken by the emergence of large quantum computers [1]. The National Institute of Standards and Technology has initiated a process to standardize quantum-resistant public-key cryptographic algorithms [2]. Recently key exchange (and key encapsulation) protocols based on the hardness of finding an isogeny between given two elliptic curves (called the isogeny problem) were proposed. Elliptic curves over finite fields are classified into ordinary and supersingular curves. While the isogeny problem on ordinary curves has a subexponential-time quantum algorithm [3], that on supersingular curves needs (quantum and classical) exponential time at present. Therefore, almost all proposed isogeny-based cryptosystems use supersingular curves.

Though such protocols are theoretically supposed to use supersingular curves, there may be possibilities that some practical implementations of the protocols improperly use ordinary curves. This can be either intentional (e.g., by malicious software engineers who want to compromise system security) or unintentional (e.g., by implementation errors). In this way, if the data sent in the cryptographic protocol contains a supersingular elliptic curve, an algorithm to determine whether it is a supersingular elliptic curve is needed to guarantee its correctness and to set the parameters of the protocol.

Therefore, it is desirable that users for the protocol are able to identify by themselves whether the given curve is supersingular or not. For this reason, the algorithms to identify supersingular elliptic curves have practical importance as well as purely mathematical interests. For the purpose, given an elliptic curve \(E\) over \(\mathbb{F}_{p^2}\), a practical probabilistic algorithm to test supersingularity of \(E\) is to randomly sample a rational point \(P \in E(\mathbb{F}_{p^2})\) and check if either \((p + 1)P = O_E\) or \((p - 1)P = O_E\) (where \(O_E\) is the infinity point of \(E\)), due to the structure of the group \(E(\mathbb{F}_{p^2})\) for supersingular \(E\) (see [4, Sec. 2.3] for the details). But this method cannot yield a deterministic polynomial-time algorithm. Among the deterministic algorithms, Sutherland proposed an efficient algorithm [4] by employing the fact that isogeny graphs associated with ordinary curves and with supersingular curves have very different structures. For this algorithm, there seems to be room to improve the efficiency further, especially for the case of larger primes \(p\). Such larger primes \(p\) are used in an isogeny-based key exchange protocol SIDH [5].

1.1 Our Results

In this paper, we propose an improved supersingularity testing algorithm by applying an efficient computation technique in 2-isogeny sequence computation (proposed by Yoshida and Takashima [6]) to Sutherland’s algorithm. We note that the work by Yoshida and Takashima just supposed that the underlying elliptic curve is supersingular, and they did not consider applications to supersingularity testing as in our paper. When the characteristic \(p\) of the field \(\mathbb{F}_{p^2}\) satisfies \(p \equiv 1 \pmod{12}\), our deterministic algorithm improves existing methods. Then, we compare the theoretical computational complexity of our proposed algorithm and Sutherland’s algorithm. In iterated computation step domi-
nating the computational time, Sutherland’s algorithm requires 9 multiplications, 3 square root computations, and 15 constant multiplications, whereas our proposed algorithm requires 3 multiplications, 3 square root computations, and 0 constant multiplication.

We also investigate the actual computation time of the proposed algorithm and compare the proposed algorithm with Sutherland’s algorithm. In our experimental result, our algorithm succeeded in reducing the computation time by 14 to 32 percent compared to the existing algorithm.

2. Preliminaries

In this section, we explain elliptic curves, isogenies and isogeny graphs (especially of ordinary curves) as preliminaries for describing isogeny computation.

2.1 Elliptic Curves

In this subsection, we explain elliptic curves. For the details, refer to [7]. Let \( p \) be a prime with \( p \geq 5 \). Let \( \mathbb{F}_p \) be the finite field with \( p \) elements of characteristic \( p \) and \( \overline{\mathbb{F}}_p \) be an algebraic closure of \( \mathbb{F}_p \). An elliptic curve \( E \) over \( \mathbb{F}_q \) is given by the Weierstraß normal form

\[
E : y^2 = x^3 + Ax + B \quad (A, B \in \mathbb{F}_q).
\]

Here, the discriminant of the right hand side \( 4A^3 + 27B^2 \) is supposed to be non-zero. We denote the infinity point of the curve \( E \) by \( \mathcal{O} \). For the above curve, \( j \)-invariant is given as \( j(A, B) = 1728(4A^3/(4A^3 + 27B^2)) \). Conversely, for \( j_0 \in \mathbb{F}_q \) with \( j_0 \neq 0, 1728 \), there exists an elliptic curve \( E \) such that \( j(E) = j_0 \), which is given by \( A = A(j_0) = 3j_0/(1728 - j_0), B = B(j_0) = 2j_0/(1728 - j_0) \) in \( (1) \). For two elliptic curves \( E, E' \) over \( \mathbb{F}_q \), their \( j \)-invariants are equal if and only if these curves are isomorphic over \( \mathbb{F}_p \). We write \( E/\mathbb{F}_q \) to mean that the coefficients of \( E \) are all \( \mathbb{F}_q \). The \( \mathbb{F}_q \)-rational points of \( E/\mathbb{F}_q \) is denoted by \( E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + Ax + B \} \cup \{ \mathcal{O} \} \). Let \( \ell \neq p \) be a prime. The group of \( \ell \)-torsion points is \( E[\ell] = \{ P \in E(\mathbb{F}_q) \mid \ell P = \mathcal{O} \} \). It holds that \( E[\ell] \cong \mathbb{Z}/[\ell] \times \mathbb{Z}/[\ell] \). Then, there exist \( (\ell^2 - 1)/(\ell - 1) = \ell + 1 \) cyclic subgroups of order \( \ell \) in \( E[\ell] \). On the other hand, \( E[p] \) is isomorphic to \( \{ 0 \} \) or \( \mathbb{Z}/p\mathbb{Z} \). If \( E[p] \cong \{ 0 \} \), then \( E \) is called supersingular and if \( E[p] \cong \mathbb{Z}/p\mathbb{Z} \), then \( E \) is called ordinary.

2.2 Isogenies and Vélu’s Formula

In this subsection, we explain isogenies. For the details, refer to [8]. For two elliptic curves \( E, E' \) over \( \mathbb{F}_q \), a homomorphism \( \phi : E \to E' \) which is given by rational functions (and sends \( \mathcal{O} \) to \( \mathcal{O} \)) is called an isogeny. In this paper, only non-zero \( \phi \) is considered. Let \( \phi : \mathbb{F}_q(E) \to \mathbb{F}_q(E') \) be the injective homomorphism between the corresponding function fields induced by \( \phi \). We call the isogeny \( \phi \) separable when the field extension \( \mathbb{F}_q(E)/\mathbb{F}_q(E') \) is a separable extension. For \( \ell \) with \( \ell \nmid p \), a separable isogeny is called \( \ell \)-isogeny if the kernel \( \ker \phi \) is isomorphic to the cyclic group \( \mathbb{Z}/\ell\mathbb{Z} \). For an \( \ell \)-isogeny, there exists an isogeny \( \phi : E' \to E \) such that \( \phi \circ \phi = [\ell] \) (\( \ell \)-multiplication on \( E \)). This isogeny \( \phi \) is called the dual isogeny of \( \phi \).

We next explain Vélu’s formula [9] for explicitly computing isogenies. Vélu’s formula takes as input an elliptic curve \( E \) and a finite cyclic subgroup \( C \subseteq E \) of order \( \ell \), and outputs an isogeny \( \phi \) with \( \ker \phi = C \) and the defining equation of the image curve \( E/C \). Here, we describe only Vélu’s formula for the case of \( \ell = 2 \).

Let \( i \) be a prime, and \( C = \langle \mathcal{O} \rangle \subseteq E[2] \). \( E/C \) is given as \( Y^2 = X^3 - (4A + 15\alpha^2)X + (8B - 14\alpha^3) \) and the 2-isogeny \( \phi = \phi_2 : E \to E/C \)

\[
\phi_2 : (x, y) \mapsto \left( x + \frac{3\alpha^2 + A}{x - \alpha}, y - \frac{(3\alpha^2 + A)y}{(x - \alpha)^2} \right).
\]

2.3 Isogeny Volcano Graphs of Ordinary Curves

In this subsection, we explain isogeny graphs. For the details, refer to [10].

In Sutherland’s algorithm [4], modular polynomials \( \Phi_{\ell}(X, Y) \in \mathbb{Z}[X, Y] \) [11] (of 2 variables \( X, Y \) with integral coefficients) play an important role. They are symmetric with respect to \( X \) and \( Y \), and of degree \( \ell + 1 \). In particular, when \( \ell \) is prime, all \( \ell \)-isogenies have cyclic group kernel, and the condition that \( E_1 \) and \( E_2 \) are \( \ell \)-isogenous is equivalent to \( \Phi_{\ell}(j(E_1), j(E_2)) = 0 \).

An isogeny graph \( G_{\ell}(\mathbb{F}_p) \) is a graph in which the vertices consist of isomorphism classes of elliptic curves over \( \mathbb{F}_p \) and the edges correspond to isogenies of degree \( \ell \) defined over \( \mathbb{F}_p \). From the above relation between the roots of modular polynomials and \( j \)-invariants of isogenous curves, the graph \( G_{\ell}(\mathbb{F}_p) \) can be identified with (the directed, non-simple) graph on vertex set \( \mathbb{F}_p \) in which \( (j_1, j_2) \in (\mathbb{F}_p)^2 \) is an edge if and only if \( \Phi_{\ell}(j_1, j_2) = 0 \). It is called the \( \ell \)-isogeny graph.

We denote by \( G_{\ell}(\mathbb{F}_p) \) the connected component of \( G_{\ell}(\mathbb{F}_p) \) containing the \( j \)-invariant \( j(E) \) of an elliptic curve \( E \) defined over \( \mathbb{F}_p \). We note that the vertex set of a connected component of \( G_{\ell}(\mathbb{F}_p) \) consists of either ordinary curves only or supersingular curves only. It is known that the connected component \( G_{\ell}(\mathbb{F}_p) \) of an isogenous graph at an ordinary elliptic curve \( E \) forms an \( \ell \)-volcano graph of height \( h \) for some \( h \), defined as follows (see Fig. 1 for an example of volcano graphs).

**Definition 1** ([10, Def. 1], [12, Def. 1]) A connected, undirected, and simple graph \( V \) is an \( \ell \)-volcano graph of height \( h \) if there exist \( h + 1 \) disjoint subgraphs \( V_0, \ldots, V_h \) (called level graphs) such that any vertex of \( V \) belongs to some \( V_0, \ldots, V_h \) and the following conditions hold.

1. The degree of vertices except for \( V_h \) is \( \ell + 1 \) and the degree of vertices in \( V_h \) is 1 when \( h > 0 \) and at most 2 when \( h = 0 \) (the degree in this case depends on the form \( V_0 \)).

2. The \( V_0 \) is one of the following: a cycle (of at least three vertices), a single edge (with two vertices), or a single vertex. Moreover, if \( h > 0 \), then all the other outgoing edges from a vertex in \( V_0 \) are joined to vertices in \( V_1 \).

3. In the case of \( h > i > 0 \), each vertex in the level \( i \) graph \( V_i \) is adjacent to only one vertex in the level \( i - 1 \) graph \( V_{i-1} \) and all the other outgoing edges are joined to vertices in \( V_{i+1} \).

4. If \( h > 0 \), then each vertex of \( V_h \) has only one outgoing edge and it is joined to a vertex in \( V_{h-1} \).
The graph $G_\ell(\mathbb{F}_{p^2})$ has a connected component of all the $j$-invariants of supersingular curves over $\mathbb{F}_p$ [13]. Therefore, other connected components in $G_\ell(\mathbb{F}_{p^2})$ consist of $j$-invariants of ordinary curves. For the ordinary components, Sutherland obtained the following result about the upper bound of the height of the components, Sutherland obtained the following result about the upper bound of the height of the $\ell$-volcano.

**Corollary 2** ([10]) Heights of $\ell$-volcano connected components of $G_\ell(\mathbb{F}_{p^2})$ are less than or equal to $\log_\ell(2p)$.

### 3. Sutherland’s Test of Supersingular Curves

In this section, we describe Sutherland’s algorithm [4] of supersingular elliptic curves. Sutherland’s algorithm outputs true if and only if the input is supersingular.

Precisely, the input is an elliptic curve $E$ over $\mathbb{F}_{p^2}$ of characteristic $p \geq 5$ and the algorithm is given below.

1. If $j(E) \notin \mathbb{F}_{p^2}$, output false.
2. If the cubic polynomial $\Phi_2(j(E), X)$ with respect to $X$ does not have three roots in $\mathbb{F}_{p^2}$, then output false. Otherwise, let the roots be $j_0, j_1, j_2 \in \mathbb{F}_{p^2}$.
3. For $\mu = 0, 1, 2$, set $j_\mu' \leftarrow j(\mu)$.
4. Let $m := \lceil \log_2 p \rceil + 1$, and iterate the following from $i = 1$ to $m$: For $\mu = 0, 1, 2$,
   a. Calculate the quadratic polynomial $f_\mu(X) \leftarrow \Phi_2(j_\mu, X) / (X - j_\mu')$.
   b. If $f_\mu(X)$ has no root in $\mathbb{F}_{p^2}$, output false. Otherwise, let $j_\mu$ be one of the two roots.
5. (If false is not outputted, output true).

If $E$ is ordinary, the $2$-isogeny graph is of $2$-volcano.

In step 4, we construct three non-backtracking paths whose initial points are $j_0, j_1, j_2$ in step 2, respectively. Therefore, at least one of the paths is descending on the volcano. Moreover, the descending path cannot have length $m + 1 \geq \log_2(2p) + 1$ by Corollary 2, and the algorithm outputs false in step 4 if $E$ is ordinary.

Sutherland gives the following time estimate in [4].

Let $n = \log_2(p)$ from now on.

**Proposition 3** ([4, Prop. 5]) Sutherland’s algorithm can be implemented as a deterministic algorithm with running-time $O(n^3)$ and space complexity $O(n)$ when quadratic and cubic non-residues are given as auxiliary inputs.

### 4. Key Observation for Constructing the Proposed Algorithm

Sutherland’s algorithm [4] is designed based on whether the roots of the modular polynomial ($j$-invariant of the elliptic curve) are in $\mathbb{F}_{p^2}$. The proposed algorithm using the Yoshida-Takashima method [6] is designed based on whether the $x$-coordinates of 2-torsion points of supersingular elliptic curves are in $\mathbb{F}_{p^2}$.

The Yoshida-Takashima method efficiently computes the $x$-coordinates of the images of the 2-torsion points under a 2-isogeny. Let $\phi_0 : E_0 \to E_1$ be a 2-isogeny and $P$ be a 2-torsion points of $E_1$. If $P$ satisfies that $E_1/(P) \cong E_0$, then it is called a backtracking point of $E_1$ (with respect to $\phi_0 : E_0 \to E_1$). There exists a unique backtracking point and we denote such a backtracking point by $\beta_{E_1} \in E_1$. Since $E_1$ has three 2-torsion points, there are two non-backtracking points of $E_1$, which are denoted by $\alpha_{E_1}, \gamma_{E_1}, \beta_{E_1}$. For simplicity, we denote the $x$-coordinates of $\alpha_{E_1}, \beta_{E_1}, \gamma_{E_1}$.

**Proposition 4** Let $\phi_1 : E_1 \to E_2 := E_1/(\alpha_{E_1})$ be a 2-isogeny.

1. ([6, Prop. 1]) The $x$-coordinate $\beta_{E_2}$ of the backtracking point of $E_2$ is given by $\beta_{E_2} = -2\alpha_{E_1}$.
2. ([6, Thm. 1]) The $x$-coordinates $\alpha_{E_2}, \gamma_{E_2}$ of the other 2-torsion points of $E_2$ are given by
   \[
   \alpha_{E_2}, \gamma_{E_2} = \alpha_{E_1} \pm 2[\beta_{E_1} - \alpha_{E_1}](\gamma_{E_1} - \alpha_{E_1})^{1/2}.
   \]

The following proposition guarantees that it is possible to construct our proposed algorithm by using the Yoshida-Takashima method.

**Proposition 5** A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $p \equiv 1 \pmod{12}$ satisfies that $E[2] \subset E(\mathbb{F}_{p^2})$.

**Proof** Since $p \equiv 1 \pmod{12}$, the trace $t$ of the supersingular curve $E/\mathbb{F}_{p^2}$ satisfies that $t = \pm 2\sqrt{p^2 - 2p}$ by [14, Theorem 4.1]. Then, $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p - 1)\mathbb{Z} \oplus \mathbb{Z}/(p + 1)\mathbb{Z}$ by [15, Lem. 4.8]. Since $p$ is an odd prime, i.e., $2|p \pm 1$, we have that $E[2] \subset E(\mathbb{F}_{p^2})$.

(QED)

### 5. Proposed Algorithm

We assume that $p \equiv 1 \pmod{12}$ throughout this section. In this section, we improve Sutherland’s algorithm [4] by using the Yoshida–Takashima efficient 2-isogenies computation [6]. Instead of directly using modular polynomials in Sutherland’s algorithm, the proposed algorithm uses the Yoshida–Takashima method. The proposed algorithm based on the Yoshida–Takashima method is given as follows: an input is an elliptic curve $E : y^2 = f(x) = x^3 + Ax + B$ ($A, B \in \mathbb{F}_q$) over a finite field $\mathbb{F}_q$ of characteristic $p \geq 5$.

1. (1) Output false if $j(E) \notin \mathbb{F}_{p^2}$.
2. (2) Output false if all the three roots of the cubic equation $f(X) = 0$ are not in $\mathbb{F}_{p^2}$. Otherwise, let the three roots be $\lambda_0, \lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$.
3. (3) For $\mu = 0, 1, 2$, let initial values $(\alpha_{0,\mu}, \beta_{0,\mu}, \gamma_{0,\mu})$ be
   \[
   (\alpha_{0,0}, \beta_{0,0}, \gamma_{0,0}) \leftarrow (\lambda_0, \lambda_1, \lambda_2),
   (\alpha_{0,1}, \beta_{0,1}, \gamma_{0,1}) \leftarrow (\lambda_1, \lambda_2, \lambda_0),
   (\alpha_{0,2}, \beta_{0,2}, \gamma_{0,2}) \leftarrow (\lambda_2, \lambda_0, \lambda_1).
   \]
4. (4) Let $m := \lceil \log_2 p \rceil + 1$ and iterate the following from $i = 1$ to $m$. 

### Fig. 1. An example of 2-volcano graphs of height 2.
For $\mu = 0, 1, 2$, determine whether the discriminant
\[ \Delta_{i-1,\mu} \leftarrow (\beta_{i-1,\mu} - \alpha_{i-1,\mu})(\gamma_{i-1,\mu} - \alpha_{i-1,\mu}) \]
has a square root in $\mathbb{F}_{p^2}$ or not. If not, output false. Otherwise, let $\delta_{i-1,\mu}$ be a square root of $\Delta_{i-1,\mu}$ and calculate the $x$-coordinates $(\alpha_{i,\mu}, \beta_{i,\mu}, \gamma_{i,\mu})$ of $2$-torsion points on the $i$-th elliptic curve $E_{i,\mu}$ as follows:
\[ \alpha_{i,\mu} \leftarrow \alpha_{i-1,\mu} + 2\delta_{i-1,\mu}, \quad \beta_{i,\mu} \leftarrow -2\alpha_{i-1,\mu}, \quad \gamma_{i,\mu} \leftarrow \alpha_{i-1,\mu} - 2\delta_{i-1,\mu}. \]
(5) Output true if false is not output in the above.

**Proposition 6** Let $p$ be a prime such that $p \equiv 1 \pmod{12}$. Given an elliptic curve, then our proposed algorithm determines whether or not the elliptic curve is supersingular.

**Proof** We have $E[2] \subset E(\mathbb{F}_{p^2})$ for supersingular $E$ from Proposition 5. As a result, our proposed algorithm satisfies correctness for supersingular $E$. Given ordinary $E$, if a curve $E_{i,\mu}$ in step 4 in our algorithm belongs to $V_0$, then $E_{i,\mu}$ has only one edge from Definition 1. In other words, if $E$ is ordinary, then there exists no non-backtracking points $\alpha_i, \gamma_i$ on $E_{i,\mu}$. Whether $\alpha_i, \gamma_i$ are elements in $\mathbb{F}_{p^2}$ depends on whether $\Delta_i$ is an element in $\mathbb{F}_{p^2}$. As a result, our proposed algorithm also satisfies correctness for ordinary $E$.

(QED)

### 6. Comparison

We compare Sutherland’s algorithm [4] in Section 3 and our proposed algorithm in Section 5. For both algorithms, the most time-consuming step, i.e., step 4, iterates computation step including square root computation $m := \lceil \log_2 p \rceil + 1$ times. In iterated computation step dominating the computational time, Sutherland’s algorithm requires 9 multiplications, 3 square root computations, and 15 constant multiplications, whereas our proposed algorithm requires 3 multiplications, 3 square root computations, and 0 constant multiplication.

### 7. Experimental Result

We compare the performance of Sutherland’s algorithm [4] with the performance of our proposed algorithm based on 2-isogenies using Magma computational algebra system. All tests were run on a platform: Magma V2.23-10 on 2.10 GHz Intel Xeon Skylake Gold 6130 Processor. In experiment of Sutherland’s algorithm, we used Magma code provided by Sutherland himself.

We denote by $b$ the bit-length of $p$. For each value $b$ of bit-length in Table 1 we randomly selected five $b$-bit prime numbers $p$. For each prime $p$ we generated one hundred supersingular elliptic curves over $\mathbb{F}_{p^2}$. These supersingular elliptic curves were randomly generated by using 2-isogenies sequence computation starting from initial supersingular elliptic curve. To generate the initial elliptic curve we used SupersingularEllipticCurve function provided by Magma computational algebra system. Table 1 gives the average execution times of the 500 trials for each bit-length. The table shows that the execution times for our proposed algorithm are about 20.4 percent (in average) shorter than Sutherland’s algorithm.

### Acknowledgments

We thank Andrew V. Sutherland for kindly sending us the Magma code of Sutherland’s algorithm. We thank Koji Nuida for his helpful comments. This work was supported by JSPS KAKENHI Grant Number JP19J23395.

### References

[1] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput., 26 (1997), 1484–1509.
[2] NIST, Post-quantum cryptography standardization, 2016, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. (accessed 22 Dec. 2020)
[3] A. Childs, D. Jao and V. Soukharev, Constructing elliptic curve isogenies in quantum exponential time, J. Math. Cryptol., 8 (2014), 1–29.
[4] A. Sutherland, Identifying supersingular elliptic curves, LMS J. Comput. Math., 15 (2012), 317–325.
[5] L. De Feo, D. Jao and J. Plut, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, J. Math. Cryptol., 8 (2014), 209–247.
[6] R. Yoshida and K. Takashima, Computing a sequence of 2-isogenies on supersingular elliptic curves, IEICE Trans. Fundamentals, E96.A (2013), 158–165.
[7] L. Washington, Elliptic Curves : Number Theory and Cryptography, 2nd edn., CRC Press, New York, 2008.
[8] S. Galbraith, Mathematics of Public Key Cryptography, Cambridge Univ. Press, 2012.
[9] J. Vélu, Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris, Sérés A, 273 (1971), 238–241.
[10] A. V. Sutherland, Isogeny volcanoes, in: Proc. of the Tenth Algorithmic Number Theory Symposium, pp.507–530, Open Book Series volume 1, 2013.
[11] A. V. Sutherland, On the evaluation of modular polynomials, in: Proc. of the Tenth Algorithmic Number Theory Symposium, pp.531–555, Open Book Series volume 1, 2013.
[12] A. V. Sutherland, Computing Hilbert class polynomials with the Chinese Remainder Theorem, Math. Comp., 80 (2011), 501–538.
[13] D. Kohel, Endomorphism rings of elliptic curves over finite fields, PhD thesis, University of California at Berkeley, 1996.
[14] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Math. Sc. Éc. Norm. Supér. (4), 2 (1969), 521–560.
[15] R. Schoof, Nonsingular plane cubic curves over finite fields, J. Combin. Theory Ser. A, 46 (1987), 183–208.

| $b$ | Sutherland’s algorithm | Our algorithm |
|-----|------------------------|---------------|
| 64  | 137                    | 104           |
| 128 | 732                    | 631           |
| 192 | 1467                   | 1425          |
| 256 | 2140                   | 2120          |
| 320 | 5150                   | 4100          |
| 384 | 5711                   | 4721          |
| 448 | 8334                   | 7066          |
| 512 | 12865                  | 10472         |
| 576 | 17153                  | 14653         |
| 640 | 25735                  | 21578         |
| 704 | 33032                  | 31370         |
| 768 | 42132                  | 36132         |
| 832 | 47533                  | 39007         |
| 896 | 71306                  | 53930         |
| 960 | 77907                  | 68208         |
| 1024| 121396                 | 103023        |