LETTER Special Section on Information Theory and Its Applications

A Construction Method of an Isomorphic Map between Quadratic Extension Fields Applicable for SIDH

Yuki NANJO†a), *Student Member*, Masaaki SHIRASE††b), Takuya KUSAKA†c), *and* Yasuyuki NOGAMI†d), *Members*

SUMMARY A quadratic extension field (QEF) defined by $F_1 = \mathbb{F}_p[\alpha]/(\alpha^2+1)$ is typically used for a supersingular isogeny Diffie-Hellman (SIDH). However, there exist other attractive QEFs F_i that result in a competitive or rather efficient performing the SIDH comparing with that of F_1. To exploit these QEFs without a time-consuming computation of the initial setting, the authors propose to convert existing parameter sets defined over F_1 to F_i by using an isomorphic map $F_1 \to F_i$.
key words: *post-quantum cryptography, SIDH, quadratic extension field*

1. Introduction

Background and motivation. Shor's algorithm made that post-quantum cryptography occupies a major place in the current research of security. In 2011, Jao and De Feo proposed a Diffie-Hellman key exchange protocol based on the difficulty of computing a kernel of isogenies between supersingular elliptic curves, which is called supersingular isogeny Diffie-Hellman (SIDH) [1]. At this time, the best-known algorithms which against the SIDH have an exponential time complexity for both classical and quantum attackers. Thus, a family of key encapsulation mechanisms based on the SIDH named supersingular isogeny key encapsulation (SIKE) [2] is expected as one of the candidates of NIST standardization of post-quantum cryptography.

The isogenies required for the SIDH are efficiently computable since it can be decomposed into low-degree isogenies involving a point multiplication on the supersingular elliptic curves defined over a quadratic extension field (QEF). Besides, Costello et al. [3] proposed efficient formulas for the low-degree isogenies with a projective point associated with fast arithmetic on the Montgomery curve. Since arithmetic operations in the QEF also need to be particularly efficient, it is typically constructed by using an irreducible binomial, i.e., $F_1 = \mathbb{F}_p[\alpha]/(\alpha^2+1)$ where $\mathbb{F}_p$ is a prime field. As these optimizations, parameter sets for the SIDH on a fixed supersingular Montgomery elliptic curve defined over F_1, which are named as `SIKEp434`, `SIKEp503`, `SIKEp610`, and `SIKEp751`, are given in Chap. 1.6 of the specification of SIKE [4].

Although an efficient SIDH is realized by using QEF defined by F_1, there exist other attractive QEFs, e.g., $F_2 = \mathbb{F}_p[\beta]/(\beta^2+\beta+1)$ and $F_3 = \mathbb{F}_p[\gamma]/(\gamma^2-\gamma-1)$ of which multiplications have a better performance than that of F_1. According to [5], these QEFs F_i are also suggested for the SIDH since the performance of the SIDH with F_i has competitive or rather better than that of F_1. However, changing the QEF from F_1 to F_i involves a time-consuming computation for the parameter sets of the SIDH defined over F_i due to several initial points generation. Thus, the authors try to obtain the sets defined over F_i by exploiting the existing parameter sets defined over F_1, i.e., `SIKEp434`, `SIKEp503`, `SIKEp610`, and `SIKEp751`.

Our proposal. The authors propose to convert the existing parameter set defined over F_1 to F_i by using a low-computational complexity isomorphic map $F_1 \to F_i$. In this paper, the authors provide a construction method of the map with an arbitrary QEF defined by an irreducible monic polynomial of degree 2. As an example, the authors construct a map $F_1 \to F_2$ and provide a parameter set defined over F_2 associated with `SIKEp434`.

2. Preliminaries

The authors provide fundamentals of the isogeny and SIDH and describe the details of the QEFs suggested for a practical SIDH.

Notations. For a prime p, let $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ denote a prime field and its QEF with a characteristic p. Let K be a finite field. A set of rational points, which is denoted as $E(K)$, on an elliptic curve E defined over K with a point at infinity O_E forms an additive group where O_E acts as the unity. For a non-negative integer s and point $P \in E(K)$, a point multiplication by s is denoted as $[s]P$.

Isogeny. Let E and $\tilde{E}$ be elliptic curves defined over K. An isogeny $\phi : E \to \tilde{E}$ defined over K is a surjective morphism such that $O_E \mapsto O_{\tilde{E}}$, which induces a group homomorphism $E(K) \to \tilde{E}(K)$. If a cyclic subgroup $G \subset E(K)$ is given, there is a unique isogeny $\phi : E \to \tilde{E} \cong E/G$ with $\ker(\phi) = G$, which is called $\#G$-isogeny. The isogeny ϕ and $\tilde{E}$ can be made explicit by using Vélu's formulas [6] once E and G are known. If a degree of isogeny is a power of l, the isogeny is

Manuscript received January 23, 2020.
Manuscript revised May 20, 2020.
Manuscript publicized July 6, 2020.
†The authors are with Okayama University, Okayama-shi, 700-8530 Japan.
††The author is with Future University Hakodate, Hakodate-shi, 041-8655 Japan.
a) E-mail: yuki.nanjo@s.okayama-u.ac.jp
b) E-mail: shirase@fun.ac.jp
c) E-mail: kusaka-t@okayama-u.ac.jp
d) E-mail: yasuyuki.nogami@okayama-u.ac.jp
DOI: 10.1587/transfun.2020TAL0002

efficiently computable by decomposed into l-isogenies.

SIDH. The steps for the SIDH key exchange between the two-person, Alice and Bob, are given as follows:

Setup. Let p be a prime given as $p = l_A^{e_A} l_B^{e_B} f \pm 1$ where l_A and l_B are small integers, e_A and e_B are positive integers, and f is a small cofactor. The prime is called as a *SIDH-friendly prime* and is typically chosen as $p = 2^{e_A} 3^{e_B} f - 1$. Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve such that $\#E(\mathbb{F}_{p^2}) = (p \mp 1)^2$ given by the Montgomery form $by^2 = x^3 + ax^2 + x$ of which j-invariant is $j(E) = 256(a^2-3)^3/(a^2-4)$. And let P_A, Q_A, P_B, Q_B are rational points in $E(\mathbb{F}_{p^2})$ such that $\langle P_A, Q_A\rangle \cong \mathbb{Z}/l_A^{e_A}\mathbb{Z} \times \mathbb{Z}/l_A^{e_A}\mathbb{Z}$ and $\langle P_B, Q_B\rangle \cong \mathbb{Z}/l_B^{e_B}\mathbb{Z} \times \mathbb{Z}/l_B^{e_B}\mathbb{Z}$. A public parameter set of the SIDH is given as $\{p, l_A, l_B, e_A, e_B, E, P_A, Q_A, P_B, Q_B\}$.

Key generation. Alice chooses a secret key as $s_A \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$ and computes a secret subgroup $G_A = \langle P_A + [s_A]Q_A\rangle$. Alice also computes a $l_A^{e_A}$-isogeny $\phi_A : E \to E_A \cong E/G_A$ and images $\phi_A(P_B)$ and $\phi_A(Q_B)$, and sets her public key as $\{E_A, \phi_A(P_B), \phi_A(Q_B)\}$. Similarly, Bob chooses a secret key $s_B \in \mathbb{Z}/l_B^{e_B}\mathbb{Z}$ and obtains his public key $\{E_B, \phi_B(P_A), \phi_B(Q_A)\}$ by computing a $l_B^{e_B}$-isogeny $\phi_B : E \to E_B \cong E/G_B$ with $G_B = \langle P_B + [s_B]Q_B\rangle$ and images $\phi_B(P_A)$ and $\phi_B(Q_A)$. Finally, they send their public key to each other.

Shared secret. Alice computes a subgroup $G'_A = \langle \phi_B(P_A) + [s_A]\phi_B(Q_A)\rangle$ from the received Bob's public key. Then Alice computes a $l_A^{e_A}$-isogeny $\phi'_A : E_B \to E_{BA} \cong E_B/G'_A$ and obtains a shared key as a j-invariant $j(E_{BA})$. Bob also computes a $l_B^{e_B}$-isogeny $\phi'_B : E_A \to E_{AB} \cong E_A/G'_B$ with $G'_B = \langle \phi_A(P_B) + [s_B]\phi_A(Q_B)\rangle$ and obtains a shared key as $j(E_{AB})$. They can share the same j-invariant since $E_{BA} \cong E/\langle P_A + [s_A]Q_A, P_B + [s_B]Q_B\rangle \cong E_{AB}$, which means that E_{BA} and E_{AB} are isomorphic.

According to [3], the isogeny computation and point multiplication in the Montgomery curve are efficiently computed without y-coordinates and a curve coefficient b. Thus, assuming x_P denotes a x-coordinate of a point P, the public parameter set is typically given as $\mathcal{P} = \{p, l_A, l_B, e_A, e_B, a, x_{P_A}, x_{Q_A}, x_{R_A}, x_{P_B}, x_{Q_B}, x_{R_B}\}$ with auxiliary x-coordinates of points $R_A = Q_A - P_A$ and $R_B = Q_B - P_B$.

QEFs. A QEF required for the SIDH is typically defined as $F = \mathbb{F}_p[\omega]/(f(\omega) = \omega^2 + c_1\omega + c_0)$ where $f(x)$ is an irreducible polynomial defined over $\mathbb{F}_p$ of which a primitive root is ω. Note that ω is denoted as $\omega = (-c_1 \pm \sqrt{D})/2$ where $D = c_1^2 - 4c_0$ is quadratic non-residue in $\mathbb{F}_p$. An arbitrary element in F is represented as $x = x_0 + x_1\omega$ where $x_0, x_1 \in \mathbb{F}_p$ and $\{1, \omega\}$ is a basis which is especially classified into a *polynomial basis*. If $c_1 \neq 0$, there exist the other basis representations $\{\omega, \omega^2\}$ and $\{\omega, \omega^p\}$, which are called as a *pseudo polynomial basis* and *normal basis*, respectively.

As one of the QEFs with efficient performing arithmetic operations, there are (i) $F_1 = \mathbb{F}_p[\alpha]/(f_1(\alpha) = \alpha^2 + 1)$ with a polynomial basis $\{1, \alpha\}$ based on an optimal extension field proposed by Bailey and Paar [7], (ii) $F_2 = \mathbb{F}_p[\beta]/(f_2(\beta) = \beta^2 + \beta + 1)$ with a pseudo polynomial basis $\{\beta, \beta^2\}$ based on an all-one polynomial extension field proposed by Nogami et al. [8], and (ii) $F_3 = \mathbb{F}_p[\gamma]/(f_2(\gamma) = \gamma^2 - \gamma - 1)$ with a normal basis $\{\gamma, \gamma^p\}$ of which multiplication can be efficiently computed by NTT method [9]. Let **M**, **S**, and **a** denote a calculation cost of the multiplication, squaring, and addition in $\mathbb{F}_p$, respectively. Then, the calculation costs of the multiplication and squaring in the above QEFs are given as Table 1. According to Table 1, the performance of the multiplication in F_2 and F_3 are better than that of F_1. The performance of the squaring in F_3 might be competitive to F_1, however, that of F_2 has a degradation.

Table 1 The calculation costs of the multiplication and squaring in the implementation-friendly QEFs.

QEFs	Mul.	Sqr.
F_1	3**M** + 5**a**	2**M** + 3**a**
F_2	3**M** + 4**a**	2**M** + 4**a**
F_3	3**M** + 4**a**	3**S** + 3**a**

In fact, the multiplications in $\mathbb{F}_{p^2}$ are typically more often used for the SIDH operations such that point multiplications and isogenies than squarings in $\mathbb{F}_{p^2}$ as shown in Table 1 of [3]. Thus, there is a possibility that the performances of the SIDH applied F_2 and F_3 are better than that of F_1, however, the typical SIDH implementations adopt F_1. In [5], Nanjo et al. confirmed the above possibility and found that F_2 and F_3 result in a slight performance improvement of SIDH comparing with F_1 by an implementation. Thus, in this paper, the authors consider a sensible way of changing the construction from F_1 to another attractive QEF F_i.

3. An Isomorphic Map from F_1 to an Arbitrary QEF F with a Characteristic of SIDH-Friendly Prime

To exploit the other attractive QEF F_i for the SIDH without a time-consuming computation of initial setting of a public parameter set $\mathcal{P}$ defined over F_i, the authors propose to convert the existing $\mathcal{P}$ defined over F_1 to F_i by using an isomorphic map $F_1 \to F_i$. In the following, the authors provide a construction method of an isomorphic map from F_1 to an arbitrary QEF F with the SIDH-friendly prime given as $p = 2^{e_A} 3^{e_B} f - 1$.

Lemma 1: If a field characteristic is $p = 2^{e_A} 3^{e_B} f - 1$, there exists a primitive cube root of unity defined over $\mathbb{F}_{p^2}$.

Proof. Since the primitive cube root of unity is written as $\sqrt[3]{1} = (-1 \pm \sqrt{-3})/2$, it is defined over $\mathbb{F}_{p^2}$ if $\sqrt{-3} \in \mathbb{F}_{p^2}$. According to [10], if $3 \nmid (p-1)$ is satisfied, 3 and -1 are quadratic residue and non-residue in $\mathbb{F}_p$ which leads to -3 is quadratic non-residue in $\mathbb{F}_p$, i.e., $\sqrt{-3} \in \mathbb{F}_{p^2}$. Since $p = 2^{e_A} 3^{e_B} f - 1$ is satisfied the condition, $\sqrt[3]{1} \in \mathbb{F}_{p^2}$. □

From Lemma 1, there exists a primitive cube root of unity in F_1 and F with a SIDH-friendly characteristic given as $p = 2^{e_A} 3^{e_B} f - 1$. In the following, let $\delta = \delta_0 + \delta_1\alpha$ and $\zeta = \zeta_0 + \zeta_1\omega$ be a primitive cube root of unity in F_1 and F where $\delta_0, \delta_1, \zeta_0, \zeta_1 \in \mathbb{F}_p$, respectively. Indeed, these elements can be written as $\delta_0 = -1/2$, $\delta_1 = \pm\sqrt{3}/2$, $\zeta_0 = (-1 \pm c_1\sqrt{-3/D})/2$, and $\zeta_1 = \pm\sqrt{-3/D}$, respectively. Note that $\sqrt{3}$, $\sqrt{-3/D} \in \mathbb{F}_p$ from the quadratic residue property of 3, quadratic non-residue property of -3, and D in $\mathbb{F}_p$.

Proposition 1: If a field characteristic is $p = 2^{e_A}3^{e_B}f - 1$, an isomorphic map from F_1 to F is defined as follows:

$$\begin{aligned} M : & F_1 \to F, \\ & x = x_0 + x_1\alpha \mapsto (x_0 + mx_1) + nx_1\omega, \end{aligned} \tag{1}$$

where $m = (\zeta_0 - \delta_0)/\delta_1, n = \zeta_1/\delta_1 \in \mathbb{F}_p$.

Proof. Let a and b be elements in F_1 represented by $a = a_0 + a_1\omega$ with $a_0, a_1 \in \mathbb{F}_p$ and $b = b_0 + b_1\omega$ with $b_0, b_1 \in \mathbb{F}_p$, respectively. (i) Additive homomorphism. It is clearly satisfied that $M(a + b) = ((a_0 + b_0) + m(a_1 + b_1)) + n(a_1 + b_1)\omega = M(a) + M(b)$. (ii) Multiplicative homomorphism. It is obtained that $M(a \cdot b) = (a_0b_0 + m(a_0b_1 + a_1b_0) - a_1b_1) + n(a_0b_0 + a_1b_0)\omega$ and $M(a) \cdot M(b) = (a_0b_0 + m(a_0b_1 + a_1b_0) + d_0a_1b_1) + n(a_0b_1 + a_0b_1 - d_1a_1b_1)\omega$ where $d_0 = m^2 - c_0n^2$ and $d_1 = n(c_1n - 2m)$. Since $m = \pm c_1\sqrt{-1/D}$ and $n = \pm 2\sqrt{-1/D}$ with $D = c_1^2 - 4c_0 \in \mathbb{F}_p$, we have $d_0 = -1$ and $d_1 = 0$ which leads to $M(a \cdot b) = M(a) \cdot M(b)$. (iii) Monomorphism. Since $n \neq 0$, it is satisfied that $M(a) \neq M(b)$ if $a \neq b \in F$. From the above (i)–(iii), M is an isomorphism. □

From the above, the isomorphic map $M : F_1 \to F$ is easily constructed once the primitive cube root of unity $\delta \in F_1$ and $\zeta \in F$ are obtained. The elements δ and ζ are obtained without square root computation by computing a cubic non-residue element to the power of $(p^2 - 1)/3$ in F_1 and F, respectively. The calculation cost to compute an image of $x \in F_1$ is enough low since it requires only 2 multiplications and 1 addition in $\mathbb{F}_p$.

Note that $M(x) \in F$ with a polynomial basis representation can also be deformed to the pseudo polynomial basis and normal basis representations as $M(x) = (x_0 + mx_1) + nx_1\omega = ((-c_1x_0 + (c_0n - c_1m)x_1)/c_0)\omega - ((x_0 + mx_1)/c_0)\omega^2 = ((-x_0 + (c_1n - m)x_1)/c_1)\omega - ((x_0 + mx_1)/c_1)\omega^p$ with a non-zero coefficient c_0 and c_1.

4. Sample Parameter Set

The authors focus on an existing public parameter set of the SIDH defined over F_1 such that $\mathcal{P}$ = `SIKEp434`, which consists of $p = 2^{216}3^{137} - 1$, $l_A = 2$, $l_B = 3$, $e_A = 216$, $e_B = 137$, $a = 6 + 0\alpha \in F_1$, and x-coordinates of initial points $x_{P_A}, x_{Q_A}, x_{R_A}, x_{P_B}, x_{Q_B}, x_{R_B} \in F_1$ (see Chap. 1.6.1 in [4]). In the following, the authors construct an isomorphic map $M_{12} : F_1 \to F_2$ and provide a public parameter set of the SIDH defined over F_2 which are computed as $M_{12}(\mathcal{P}) = \{p, l_A, l_B, e_A, e_B, M_{12}(a), M_{12}(x_{P_A}), M_{12}(x_{Q_A}), M_{12}(x_{R_A}), M_{12}(x_{P_B}), M_{12}(x_{Q_B}), M_{12}(x_{R_B})\}$.

From Proposition 1, the isomorphism map $F_1 \to F_2$ is obtained as $M_{12} : F_1 \to F_2, x_1 = x_0 + x_1\alpha \mapsto x_2 = (x_0 + mx_1) + nx_1\beta = (-x_0 + (n - m)x_1)\beta - (x_0 + mx_1)\beta^2$ where m and n are given as follows:

$m =$ `00db6794 b8c6558d e8372711 9cd51000 00000000`
`00000000 00000000`
$n =$ `01b6cf29 718cab1b d06e4e23 39aa2000 00000000`
`00000000 00000000`

When applying M_{12}, a curve coefficient $a \in F_1$ is mapped to $M_{12}(a) = -6\beta - 6\beta^2 \in F_2$. The x-coordinates of initial points $x_{P_A}, x_{Q_A}, x_{R_A}, x_{P_B}, x_{Q_B}, x_{R_B} \in F_1$ can be mapped to elements defined over F_2 by computing $M_{12}(x_{S_X}) = x_{S_{X2},0}\beta + x_{S_{X2},1}\beta^2 \in F_2$ where $x_{S_{X2},0}$ and $x_{S_{X2},1}$ are the following values for $S \in \{P, Q, R\}$ and $X \in \{A, B\}$.

$x_{P_{A2},0} =$ `0001b7ec 3cb83805 31034815 ffcce3b5 40693f5a`
`fb9bbd81 80395c7b 9cfbb4fb 30ad5bdd 3cba824f`
`73f213fe e7125ecc 8be39afc 2fcf4c60`
$x_{P_{A2},1} =$ `00000293 5e9b5a9f 35f24ff3 5de41dac a2843950`
`b9f07d05 b49cbb3b 12d96a45 d64a0409 5dceb9dd`
`ea4aaeaa 0c29fc7a df7a8ab4 a3a31d0f`
$x_{Q_{A2},0} =$ `0001bcec 6753b4d5 c8dd8561 a57eeca8 cc29930f`
`a7b9a009 d83cb9b5 a109001f 13c48a6a 2f9ff3c3`
`c6f7de48 67ad08b5 e671097a 225bc897`
$x_{Q_{A2},1} =$ `00011cc5 b86ac995 173a0084 4c1e862d b9733e81`
`129c3bd1 59924a7c 3ec1ba05 5ed21eb2 55da228c`
`b8565f38 ceee876b 1dd4a10d c1ce1e8f`
$x_{R_{A2},0} =$ `0000b936 ddd16a1e 503f960c 9c71a2fc 210958e0`
`306a79c0 573cb62c c04a31b8 462b666b acf65cb4`
`ccc79553 2d9ad510 582b7a6f 55726594`
$x_{R_{A2},1} =$ `0001c812 09c63acd 2e8f4126 ae76e1a3 7c4fd316`
`6921dcf9 d3f29fa4 559a7dac c167f8c0 08dcd073`
`b6c29408 5cb6fc9a cd8d5b69 1e93503e`
$x_{P_{B2},0} =$ `0001adba a0b8cb6c 560c24a4 9fa15de9 3b5c300b`
`6094d83c b7611fcf faa76a13 c8c97403 ff620503`
`4c26819c 609a161b a0b9a8c4 f9c84856`
$x_{P_{B2},1} =$ `0001adba a0b8cb6c 560c24a4 9fa15de9 3b5c300b`
`6094d83c b7611fcf faa76a13 c8c97403 ff620503`
`4c26819c 609a161b a0b9a8c4 f9c84856`
$x_{Q_{B2},0} =$ `0001059a 4fb24deb 8667a051 bfc945a6 e20e2135`
`ca957fdd a2b130ff 1806b39c 14f9c97e 174e18c6`
`73f4dbe3 e64699a0 2461ebf9 25c2c7b9`
$x_{Q_{B2},1} =$ `0001059a 4fb24deb 8667a051 bfc945a6 e20e2135`
`ca957fdd a2b130ff 1806b39c 14f9c97e 174e18c6`
`73f4dbe3 e64699a0 2461ebf9 25c2c7b9`
$x_{R_{B2},0} =$ `00004a01 53e81db2 b207c2d4 9cc9c890 c660622d`
`7785390f 637fa6d6 f44e6787 266dbc35 100f2130`
`c5c6f60b 3351c140 4ce94455 a3517d60`
$x_{R_{B2},1} =$ `000083ec 47621b2c 28213cd2 95cf9731 dc0d41f9`
`a79332cd 53df0535 e132f50e ddc026b7 66d32c9a`
`1ba4f05d 732eeed5 7e031f07 480913c6`

According to [5], the parameter set $M_{12}(\mathcal{P})$ obtained by the above computation is expected to lead in an efficient SIDH defined over F_2 of which performance is slightly better than that of F_1.

5. Conclusion

To obtain a public parameter set of the SIDH defined over an attractive QEF F_i without time-consuming computation, the authors propose to convert the existing parameter set defined over $F_1 = \mathbb{F}_p[\alpha]/(\alpha^2 + 1)$ to F_i by using a low-computational complexity isomorphic map $F_1 \to F_i$. In this paper, the authors provide a construction method of the isomorphic map and give a sample conversion associated with the existing parameter set `SIKEp434`.

Acknowledgments

This research was supported by JSPS KAKENHI Grant Numbers 19J2108611 and 19K11966.

References

[1] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," International Workshop on Post-Quantum Cryptography, pp.19–34, Springer, 2011.

[2] R.A. David Jao, M. Campagna, C. Costello, L.D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik, "Supersinglar isogeny key encapsulation." Round 1 submission, NIST Post-Quantum Cryptography Standardization, 2017. https://sike.org

[3] C. Costello, P. Longa, and M. Naehrig, "Efficient algorithms for supersingular isogeny diffie-hellman," Annual International Cryptology Conference, pp.572–601, Springer, 2016.

[4] M. Campagna, C. Costello, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, D. Urbanik, et al., "Supersingular isogeny key encapsulation," 2019. https://sike.org/files/SIDH-spec.pdf

[5] Y. Nanjo, M. Shirase, T. Kusaka, and Y. Nogami, "A performance analysis and evaluation of SIDH with implementation-friendly classes of quadratic extension fields," 2019 Seventh International Symposium on Computing and Networking (CANDAR), pp.178–184, IEEE, 2019.

[6] J. Vélu, "Isogénies entre courbes elliptiques," CR Acad. Sci. Paris, Séries A, vol.273, pp.305–347, 1971.

[7] D.V. Bailey and C. Paar, "Efficient arithmetic in finite field extensions with application in elliptic curve cryptography," J. Cryptol., vol.14, no.3, pp.153–176, 2001.

[8] Y. Nogami, A. Saito, and Y. Morikawa, "Finite extension field with modulus of all-one polynomial and representation of its elements for fast arithmetic operations," IEICE Trans. Fundamentals, vol.E86-A, no.9, pp.2376–2387, Sept. 2003.

[9] T. Kobayashi, "Oef using a successive extension," Proc. 2000 Symposium on Cryptography and Information Security, 2000.

[10] F. Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein, Springer Science & Business Media, 2013.