Malaysian Journal of Mathematical Sciences 13(S) August: 67–76 (2019)
Special Issue: The 6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Construction of Endomorphisms for the ISD Method on Elliptic Curves with j-invariant 1728

Antony, S.N.F.M.A.*[1] and Kamarulhaili, H. [2]

[1,2]*School of Mathematical Sciences, Universiti Sains Malaysia*

E-mail: sitinoorfarwina@yahoo.com
**Corresponding author*

ABSTRACT

In this study, we construct the efficiently computable endomorphisms on elliptic curves with j-invariant 1728, to accelerate the computation of ISD method. The ISD method computed scalar multiplication on elliptic curves where it requires three endomorphisms to accomplish. However, the original ISD method only able to solve integer multiplications since their endomorphisms are defined over $\mathbb{Z}$. Besides, the endomorphisms defined in the original ISD method are not efficiently computable. We extend the study by defining the endomorphisms in the ISD method over the $\mathbb{Q}(\sqrt{-d})$, so that it can solve complex multiplications. Elliptic curves with j-invariant 1728 are defined over $\mathbb{Q}(i)$, where its discriminant is given as $D = -4$, with a unique maximal order. The maximal order satisfies a polynomial of degree two, which represents the minimal polynomial for the first efficiently computable endomorphism. Meanwhile, we choose the other two endomorphisms to belong to $\mathbb{Q}(i)$ as well.

Keywords: Efficient endomorphism, elliptic curve scalar multiplication, Integer Sub-Decomposition method, j-invariant 1728, quadratic field.

1. Introduction

$E(F_p)$ with $char(K) \neq 2, 3$ is an ordinary elliptic curve E defined over prime field, F_p, where

$$E : y^2 = x^3 + Ax + B$$

such that $A, B \in F_p$. The order of E, denoted as $\#E(F_p)$ is the number of points in $E(F_p)$ such that $\#E(F_p) = nh$, where n is a prime number and h is the cofactor. For cryptographic purpose, $h \leq 4$. These points form a group. It is clear that there exist a single prime subgroup of order n inside this group.

One of the most critical operation in elliptic curve cryptography (ECC) is scalar multiplication, kP, where $k \in [1, n]$ and a point, $P \in E(F_p)$ with order n. It remains to be the most dominant operation in ECC, see Park et al. (2002). To overcome the high computational cost problem, many researchers developed approaches such as the Gallant-Lambert-Vanstone (GLV) method and the Integer Sub-Decomposition (ISD) method.

Gallant et al. (2001) proposed the GLV method where they decomposed scalar k into two mini scalars; k_1 and k_2, which satisfy $k_1, k_2 \leq \sqrt{n}$. The general form of GLV method given as

$$kP = k_1 P + k_2 \Phi(P) \tag{1}$$

where $\Phi(P) = \lambda P$. They highlight that λ is the roots of the minimal polynomial of degree two for the endomorphism,Φ. This implies λ is an algebraic integer, see Ribenboim (2001). The GLV method allows complex multiplication since their efficiently computable endomorphism is defined over the complex quadratic field. The efficiently computable endomorphism helps to accelerate the scalar multiplication on elliptic curve via the GLV method by 50%, see Sica et al. (2002).

However, not all scalars k can be decomposed into scalars $k_1, k_2 \leq \sqrt{n}$. As an alternative, Ajeena and Kamarulhaili (2013) proposed the ISD method to fulfill the gap of GLV method. The ISD method further decomposed the GLV scalars $k_1, k_2 > \sqrt{n}$ into four different scalars $k_{1,1}, k_{1,2}, k_{2,1}, k_{2,2}$, where each scalars fall within $\sqrt{n}$, see Ajeena and Kamarulhaili (2014). The ISD method formulation is given as

$$kP = k_{1,1} P + k_{1,2} \Phi_1(P) + k_{2,1} P + k_{2,2} \Phi_2(P) \tag{2}$$

where three endomorphisms denoted by Φ, Φ_1, Φ_2 are needed. The ISD method increases the percentage of successful computations as compared to the GLV

method, however, their computational costs are expensive due to their inefficiently computable endomorphisms. They used trivial endomorphisms, defined by $X - \lambda = 0$, see Ajeena and Kamarulhaili (2015). As a result, they only able to solve integer multiplications. Hence, their method unable to solve complex multiplication on elliptic curves with j-invariant 1728.

In this paper, we extend the ISD method be defined over the imaginary quadratic field which allows it to solve complex multiplication on elliptic curves with j-invariant 1728. Section 2 discusses some definitions and essential theorems related to this study. Section 3 describes the efficiently computable endomorphisms acted on curves with j-invariant 1728 and their respective mapping. This section also discusses the upper and lower bound of the decomposed scalars. Other than that, the operation counts for each of the endomorphism are also being computed. Lastly, the last section concludes the paper.

2. Preliminaries

In this section, we give some important concepts which are used throughout this study which can refer to Washington (2008) and Cohen (1996).

Theorem 2.1. *Let E be an elliptic curve which allows complex multiplication. Then, $End(E)$ is isomorphic either to $\mathbb{Z}$ or an order in an imaginary quadratic field.*

Definition 2.1. *Let $E : y^2 = x^3 + Ax + B$ be an ordinary elliptic curve. Then, the only change of variables that preserves the structure of E is $x = u^2x', y = u^3y'$.*

Definition 2.2. *Let $d > 0$ be a square free integer and let*

$$K = \mathbb{Q}(\sqrt{-d}) = a + b\sqrt{-d} | a, b \in \mathbb{Q}.$$

Then, K is called an imaginary quadratic field.

Definition 2.3. *The discriminant of quadratic field, D is the discriminant of the quadratic polynomial where*

$$D = \begin{cases} -f^2d, & \text{if } d \equiv 3 \pmod 4 \\ -4f^2d, & \text{if } d \equiv 1, 2 \pmod 4 \end{cases}$$

where d is the square free integer and f is the conductor of the ring generated by an order in the complex or imaginary quadratic field,$K = \mathbb{Q}(\sqrt{-d})$.

Proposition 2.1. *Let $K = \mathbb{Q}(\sqrt{-d})$ with d a square free integer. Let $\{1, \mathcal{O}_K\}$ be the integral basis of K. Then, the largest subring of K denoted by $\mathcal{O}_K$, is finitely generated by an abelian group which is defined as*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right], & \text{if } d \equiv 3 \pmod 4 \\ \mathbb{Z}\left[\sqrt{-d}\right], & \text{if } d \equiv 1, 2 \pmod 4. \end{cases}$$

3. Curves with j-invariant 1728

The elliptic curves with j-invariant 1728 are curves which have the form of $E : y^2 = x^3 + Ax$, and it is defined over F_p. From Washington (2008), this curve is ordinary only when $p \equiv 1 \pmod 4$. This curve corresponds to unique discriminant of the complex quadratic field, $D = -4$ that is belong to class number one field, see Cohen (1996) where $K = \mathbb{Q}(i)$. Follow Proposition 2.1, the maximal order for this curve is given as $\mathbb{Z}(i)$, which is the largest ring in this field, with integral basis $\{1, i\}$. There exists a unique endomorphism that acted on the curve which is defined over $K = \mathbb{Q}(i)$. The following proposition describes the minimal polynomial and the mapping for the unique efficiently computable endomorphism acted on curves with j-invariant 1728.

Proposition 3.1. *Let $p \equiv 1 \pmod 4$ and $P \in E(F_p)$ with prime order n where $E : y^2 = x^3 + Ax$. Let $\beta \in F_p$ be an element of order four. Then, the endomorphism Φ satisfies $\Phi^2 + 1 = 0$, where $\Phi(P) = \lambda P$. Then, the map Φ is defined as*

$$\begin{array}{rccc} \Phi: & E(F_p) & \to & E(F_p) \\ & (x, y) & \mapsto & (-x, \beta y) \\ & \mathcal{O} & \to & \mathcal{O} \end{array}$$

is an endomorphism where $\beta^2 + 1 \equiv 0 \pmod p$.

Proof. An element $u \in F_p$ of order four is chosen such that $u^4 \equiv 1 \pmod p$. This implies $u^4 - 1 \equiv 0 \pmod p$ which can be reduced into $(u+1)(u-1)\left(u^2+1\right) \equiv 0 \pmod p$, where $u \equiv 1 \pmod p$,$u \equiv -1 \pmod p$ and $u \equiv \pm\sqrt{-1} \pmod p$. Clearly, the only algebraic number is $u \equiv \pm\sqrt{-1} \pmod p$, which satisfies a minimal polynomial of the form $u^2 + 1 = 0$. Note that, $\mathbb{Z}[u] \cong \mathcal{O}_K$. And from Theorem 2.1, Φ is isomorphic to and order in an imaginary quadratic field, $\Phi \cong u$, hence $\Phi^2 + 1 = 0$ which implies $\lambda^2 + 1 = 0$. From the Definition 2.1, the isomorphism that will preserve the equation from $E \to E$ is given by $x = u^2 x, y = u^3 y$. Since $u^2 \equiv -1 \pmod p$, we then have

$$\begin{aligned}\Phi\ (x,y) &= \left(u^2x, u^3y\right)\\ &= \left((-1)\,x, \beta y\right)\\ &= \left(-x, \beta y\right)\end{aligned}$$

Supposed $\beta \equiv u^3 \pmod p$, this implies $\beta^4 \equiv \left(u^3\right)^4 \equiv \left(u^4\right)^3 \equiv 1 \pmod p$. Thus, β is also an element of order four. Therefore, β satisfies the equation $\beta^2+1 \equiv 0 \pmod p$. □

ISD method needs two more endomorphisms so that it is applies on elliptic curve with j-invariant 1728. We choose the ring of the second endomorphism and the third endomorphism to be the subring of the endomorphism ring for the first endomorphism. The following lemma describes the existence of the other two non-maximal orders such that they belong to the same complex quadratic field as the maximal order.

Lemma 3.1. *Let $E : y^2 = x^3 + Ax$ defined over a field $K = \mathbb{Q}(i)$. Given the first endomorphism as $\Phi^2 + 1 = 0$, where the maximal order is given as $\mathcal{O}_K = \mathbb{Z}[i]$. Then, there exist two other non-maximal order which is given by $\mathbb{Z}[1-i]$ and $\mathbb{Z}[1+i]$ which belong to the same field.*

Proof. From Proposition 2.1, we have the maximal order for the imaginary quadratic field with discriminant, $D = -4$ given by $\mathcal{O}_K = \mathbb{Z}[i]$, where its integral basis given as $\{1, i\}$ from Proposition 2.1. This ring of integer generated by the maximal order is isomorphic to the endomorphism ring, which is an abelian group under addition. Any algebraic integer in this abelian group can be written as a linear combination of the basis 1 and i where $z = a(1) + b(i)$ with $a, b \in \mathbb{Z}$. By letting $a = 1, b = 1$, we have $z = 1 + i$. And by letting $a = -1, b = 1$, we have $z = -1 + i$. Both elements generated by the same generator, i, and they are belong to the same field $K = \mathbb{Q}[i]$. □

From Lemma 3.1, we have the second and third endomorphism in the second layer of decomposition as $\Phi_1^2 - 2\Phi_1 + 2 = 0$ and $\Phi_1^2 + 2\Phi_1 + 2 = 0$ where the endomorphism rings are isomorphic to $End(E) = \mathbb{Z}[\Phi_2] \cong \mathbb{Z}[1+i]$ and $End(E) = \mathbb{Z}[\Phi_2] \cong \mathbb{Z}[-1+i]$ respectively. The following theorem describes their respective mappings.

Theorem 3.1. *Let $p \equiv 1 \pmod 4$ and $P = (x, y)$ be a point in $E(F_p)$ with prime order n where $E : y^2 = x^3 + Ax$. Define $\Phi_1^2 - 2\Phi_1 + 2 = 0$ and $\Phi_2^2 + 2\Phi_2 + 2 = 0$ as the second and third endomorphism respectively. Then, their*

mapping is given by

$$\Phi_{1,2}(x,y) = \left(\frac{x^2 + A}{\epsilon_{1,2}^2 x}, y \left[\frac{x^2 - A}{\epsilon_{1,2}^3 x^2} \right] \right)$$

where $\epsilon_{1,2}$ *are the roots of the minimal polynomials for the endomorphisms.*

Proof. Since $E : y^2 = x^3 + Ax$, we can have the torsion point as $Q = (0,0)$, a point of order two. By using Velu's algorithm, see Galbraith (2012), we have

$$\begin{aligned} F(x,y) &= x^3 + Ax - y^2 = 0 \\ F_x &= 3x^2 + A \\ F_y &= -2y \\ u_Q &= 0 \\ v_Q &= (F_x(Q)) = A. \end{aligned}$$

Then, the mapping for the isogeny is defined by $\phi : (x,y) = (X,Y)$ where

$$\begin{aligned} X &= x + \frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \\ &= x + \frac{A}{x} \\ &= \frac{x^2 + A}{x} \end{aligned}$$

and

$$\begin{aligned} Y &= y - u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} - v_Q \frac{a_1 (x - x_Q) + y - y_Q}{(x - x_Q)^2} - \frac{a_1 u_Q - F_x(Q) F_y(Q)}{(x - x_Q)^2} \\ &= y - A\left(\frac{y}{x^2}\right) \\ &= y \left[\frac{x^2 - A}{x^2} \right]. \end{aligned}$$

Then the map $\phi : (x,y) \to (X,Y)$ is a separable isogeny from E to

$$\tilde{E} : Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6$$

where

$$A_1 = a_1, A_2 = a_2, A_3 = a_3, A_4 = a_4 - 5v, A_6 = a_6 - \left(a_1^2 + 4a_2\right) v - 7w.$$

This implies $A_1 = 0, A_2 = 0, A_3 0, A_4 = a_4 - 5v = -4A, A_6 = 0$. Thus one have $\tilde{E} : y^2 = x^3 - 4Ax$ and $\phi(x,y) = \left(\frac{x^2 + A}{x}, y \frac{x^2 - A}{x^2} \right)$ as the isogeny $E_{1728} \to \tilde{E}_{1728}$.

Since $j(E) = j(\tilde{E})$, which preserve the structure of the curve, thus $E \cong \tilde{E}$. And it is clear that the mapping from E to $\tilde{E}$ satisfies the change of variable as stated in Definition 2.1, where $u^4 = -4 = 4(-1)$ which implies $u^2 = 2\sqrt{-1}$ that belongs to $\mathbb{Q}(-1)$. Thus, ϕ is applicable to define the endomorphism mapping defined over $\mathbb{Q}(-1)$.

Follow the concept of dual isogeny, there exist another isogeny $\tilde{E}$ to E such that it preserves the structure of the curves where $(X, Y) = (u^2x, u^3y)$ for $u \in K^*$. By letting $u = \epsilon_{1,2}$, the roots for second and third endomorphism, implies the mapping for the endomorphisms where $\Phi_{1,2} : (x, y) = (\frac{X}{\epsilon_{1,2}^2}, \frac{Y}{\epsilon_{1,2}^3})$ as

$$\Phi_{1,2}(x, y) = \left(\frac{x^2 + A}{\epsilon_{1,2}^2 x}, \frac{y}{\epsilon_{1,2}^3} \left[\frac{x^2 - A}{x^2} \right] \right)$$

where $\epsilon_1 \equiv 1 + \imath \pmod{p}$ and $\epsilon_2 \equiv -1 + \imath \pmod{p}$. □

Different endomorphisms will result in different lower and upper bounds. The following theorem explains the bounds for the mini scalars in the ISD method by using the endomorphisms defined earlier.

Theorem 3.2. *Let $E_{1728} : y^2 = x^3 + Ax$ defined over F_p such that $p \equiv 1 \pmod 4$. There exist point $P \in E_{1728}(F_p)$ with prime order n. Supposed that $kP = k_1P + k_2\Phi(P)$ be the the first layer of decomposition in ISD method such that $\Phi^2 + 1 = 0$. Then, the lower bound for k_1, k_2 are given as $max(|k_1|, |k_2|) \geq \sqrt{2}\sqrt{n}$. And supposed that $k_1P = k_{1,1}P + k_{1,2}\Phi_1(P)$ and $k_2P = k_{2,1}P + k_{2,2}\Phi_2(P)$ be the second decomposition layer of ISD where $\Phi_1^2 - 2\Phi_1 + 2 = 0$ and $\Phi_2^2 + 2\Phi_2 + 2 = 0$. Then, the upper bound for $k_{1,1}, k_{1,2}, k_{2,1}, k_{2,2}$ are given by $max(|k_{1,1}|, |k_{1,2}|, |k_{2,1}|, |k_{2,2}|) < \sqrt{5}\sqrt{n}$.*

Proof. Let λ and μ be the roots of $\Phi^2 + r'\Phi + s' \equiv 0 \pmod n$. Define the transformation T as $T : (x_1, x_2)\, x \mapsto x_1 + x_2\lambda \pmod n$ and $T : (x_1, x_2)\, x \mapsto x_1 + x_2\mu \pmod n$. For any point $P \in Ker(T) - \{0\}$, one have

$$0 \equiv (x + \lambda y)(x + \mu y) \equiv x^2 + (\lambda + \mu)\, xy + (\lambda\mu)\, y^2.$$

As the minimal polynomial for the first endomorphism is a polynomial of degree two and any polynomial of degree two will satisfy $\Phi^2 - (sumofroots)\Phi + (productofroots) = 0$ where the sum of roots is given as $\lambda + \mu = -r'$ and the product of roots as $\lambda\mu = s'$, where $0 \equiv x^2 + (-r')\, xy + (s')\, y^2 \pmod n$. Since $\Phi^2 + r'\Phi + s' = 0$ is irreducible in $\mathbb{Z}[\Phi]$, then $x^2 + (-r')\, xy + s'y^2 \geq n$. And

this implies

$$\begin{aligned} n \leq x^2 + (-r')\, xy + s'y^2 &\leq x^2 + |-r'|\, xy + s'y^2 \\ &\leq max\left\{x^2 + |-r'|\, x^2 + s'x^2, y^2 + |-r'|\, y^2 + s'y^2\right\} \\ &\leq [1 + |-r'| + s']\, max\left\{x^2, y^2\right\}. \end{aligned}$$

Then, $max\left\{x^2, y^2\right\} \geq \frac{n}{[1+|-r'|+s']}$ which implies $max\left\{x, y\right\} \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$. Hence, one can have $|v_1| \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$ where $|v_1| = |(r_{m+1}, -t_{m+1})|$ which it can be either $r_{m+1} \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$ or $|t_{m+1}| \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$. This can be divided into two cases:

1. $r_{m+1} \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$.
   From Lemma 1 in Gallant et al. (2001),$r_{m+1}\,|t_{m+2}| + r_{m+2}\,|t_{m+1}| = n$ implies $r_{m+1}\,|t_{m+2}| < n$ and $r_{m+2}\,|t_{m+1}| < n$. Since $r_{m+1} \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$, then $|t_{m+2}| < \sqrt{n}\sqrt{[1 + |-r'| + s']}$ and thus result $|v_2| = |(r_{m+2}, -t_{m+2})| < \sqrt{[1 + |-r'| + s']\, n}$.
2. $|t_{m+1}| \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$
   From Lemma in Gallant et al. (2001), $r_m\,|t_{m+1}| + r_{m+1}\,|t_m| = n$ implies $r_m\,|t_{m+1}| < n$ and $r_{m+2}\,|t_{m+1}| < n$. Since $|t_{m+1}| \geq \sqrt{\frac{n}{[1+|-r'|+s']}}$, then $r_m < \sqrt{n}\sqrt{[1 + |-r'| + s']}$ and thus result $|v_2| = |(r_m, -t_m)| < \sqrt{[1 + |-r'| + s']\, n}$.

The upper bound for k_1 and k_2 depend on the upper bound for generator vectors, where the upper bound for k_1 and k_2 in the GLV method are given as $max\left\{|k_1|, |k_2|\right\} < \sqrt{[1 + |-r'| + s']\, n}$. Since the first endomorphism is defined as $\Phi^2 + 1 = 0$ where $r' = 0$ and $s' = 1$, this implies $max\left\{|k_1|, |k_2|\right\} < \sqrt{2n}$ as the upper bound for GLV method. Thus, the lower bound for the ISD method is given by $min\left\{|k_1|, |k_2|\right\} \geq \sqrt{2n}$. By using same approach, the upper bound for the subdecomposed scalar using the second and third endomorphism are given as $\max(|k_{1,1}|, |k_{1,2}|, |k_{2,1}|, |k_{2,2}|) < \sqrt{5}\sqrt{n}$. □

Next, we discuss the operation counts for the efficiently computable endomorphism defined on elliptic curves with j-invariant 1728. The first endomorphism is defined by $\Phi^2 + 1 = 0$ where it maps $\Phi : (x, y) \mapsto (-x, \beta y)$. It suffices to know that $\Phi(P)$ requires one multiplication. The following theorem explains

the operation counts for the endomorphism's mapping defined in the second layer of decomposition.

Theorem 3.3. *Let $p \equiv 1 \pmod 4$ and $P \in E(F_p)$ be a prime order point where $E : y^2 = x^3 + Ax$. Given the second and third endomorphisms' mapping as $\lambda_{1,2}P = \left(\frac{x^2+A}{\epsilon_{1,2}^2 x}, y\left[\frac{x^2-A}{\epsilon_{1,2}^3 x^2}\right]\right)$, such that λ_1, λ_2 and ϵ_1, ϵ_2 are the roots of minimal polynomial for the second and third endomorphism modulo n and p respectively. Then, the cost of computing $\Phi_{1,2}P$ consists of one multiplication, one squaring and two inversion operations.*

Proof. The second and third endomorphisms define by $\Phi_1^2 - 2\Phi_1 + 2 = 0$ and $\Phi_2^2 + 2\Phi_2 + 2 = 0$ respectively. The cost of computing the operation counts involve in that mapping is calculated in the table below:

Multiplication	Squaring	Inversion
$y \cdot \left[\frac{x^2-A}{\epsilon_{1,2}^3 x^2}\right]$	x^2	$\frac{x^2+A}{\epsilon_{1,2}^2 x}$
		$\frac{x^2-A}{\epsilon_{1,2}^3 x^2}$
1M	1S	2I

□

4. Conclusion

We extended the original ISD method on the imaginary quadratic field so that it is applicable on elliptic curves with j-invariant 1728. Elliptic curves with j-invariant 1728 are defined over a unique imaginary quadratic field, $K = \mathbb{Q}(i)$ with discriminant, $D = -4$. We constructed the endomorphisms needed to carry out the ISD method on this curves. All these endomorphisms are defined over the same imaginary quadratic field as the curve itself. The first endomorphism is given as $\Phi^2 + 1 = 0$, where its ring is isomorphic to the largest ring of integer defined in this field, $\mathbb{Z}(i)$. Its mapping requires only one multiplication. We choose the second and third endomorphism as $\Phi_1^2 - 2\Phi_1 + 2 = 0$ and $\Phi_2^2 + 2\Phi_2 + 2 = 0$, where their endomorphism rings are isomorphic to the subrings in $\mathbb{Z}(i)$. The cost of computing the second and third endomorphism mapping is one multiplication, one squaring and two inversions, regardless of how large the field might be. Instead of using repeated doublings and additions,

the existence of efficiently computable endomorphisms will reduce the cost of computing scalar multiplication kP.

References

Ajeena, R. and Kamarulhaili, H. (2013). Analysis on the elliptic scalar multiplication using integer sub decomposotion method. *International Journal of Pure and Applied Mathematics*, 87(1):95–114.

Ajeena, R. and Kamarulhaili, H. (2014). Glv-isd method for scalar multiplication on elliptic curves. *Australian Journal of Basic and Applied Sciences*, 8(15):1–14.

Ajeena, R. and Kamarulhaili, H. (2015). On the distribution of scalar k for elliptic scalar multiplication. *AIP Conf. ProcJournal of Applied Mathematics and Information Sciences*, 1682(020052):1–9.

Cohen, H. (1996). *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, Heidelberg, London.

Galbraith, S. (2012). *Mathematics of Public Key Cryptography.* Cambridge University Press, UK.

Gallant, R., Lambert, R., and Vanstone, S. (2001). Faster point multiplication on elliptic curve with efficient endomorphism. *CRYPTO 2001,Advances in Cryptology*, 2139:190–200.

Park, Y., Jeong, S., Kim, C., and Lim, J. (2002). An alternative decomposition of an integer for faster point multiplication on certain elliptic curves. *PKC,LNCS*, 2274:323–334.

Ribenboim, P. (2001). *Classical Theory of Algebraic Numbers.* Springer-Verlag, New York, Berlin, Heidelberg.

Sica, R., Ciet, M., and Quisquater, J.-J. (2002). Analysis of the gallant-lambert-vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves. *SAC 2002,Selected Areas in Cryptography,9th Annual International Workshop*, 2595:21–36.

Washington, L. C. (2008). *Elliptic Curves Number Theory and Cryptography.* CRC Press, London, New York, 2nd edition.