DOCTORAL THESIS

Proposals on Efficient Software Implementation of Pairing-Based Cryptographic Primitives

Author:
Md. Al-Amin KHANDAKER

Supervisor:
Dr. Yasuyuki NOGAMI

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the

Information Security Lab.
Graduate School of Natural Science and Technology

OKAYAMA UNIVERSITY

September 15, 2018

Declaration of Authorship

I, Md. Al-Amin KHANDAKER, declare that this thesis titled, "Proposals on Efficient Software Implementation of Pairing-Based Cryptographic Primitives" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: _____

Date: _____

"Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism."

Dave Barry

OKAYAMA UNIVERSITY

Abstract

Faculty of Engineering
Graduate School of Natural Science and Technology

Doctor of Philosophy

Proposals on Efficient Software Implementation of Pairing-Based Cryptographic Primitives

by Md. Al-Amin KHANDAKER

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

Contents

List of Figures

List of Tables

List of Abbreviations

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

Physical Constants

Speed of Light $c_0 = 2.997\,924\,58 \times 10^8\,\mathrm{m\,s{-}1}$ (exact)

List of Symbols

a	distance	m
P	power	W (J s-1)
ω	angular frequency	rad

For/Dedicated to/To my…

Chapter 1

Introduction

1.1 Background

With the development of the information and communication technology, a social utilization of a computer network has advanced at a rapid pace. As a r esult, several services associated with the society and our daily life such as e-commerce and e-government are provided on the computer network. These services, however, transmit highly-confidential informations such as financial or privacy informations via the network. In order to protect these informations, cryptosystems are indispensable that provides the secret communication and authentication for the current information and communication services. In the modern cryptographies, public key cryptography that provides authentication, data integrity, and non-repudiation is one of the most important cryptosystems.

Recently, new cryptographic schemes that relax the restriction on use of the modern public key cryptosystems are proposed. Among these innovative cryptographies, pairing-based cryptographies such as ID-based cryptographies**ID** and group signature authentications **BBS nakanisi** have received much attentions. For example, in ID-based cryptographies, some unique information about the identity of the user such as e-mail address, name and telephone number can be used as the public key of user. In addition, group signature authentications allow the service vendor to verify that a signature is signed by a valid user, but they can not know who is the signer. Therefore, group signatures can protect user's privacy while preventing illegal accesses.

These cryptographic schemes allow us to use the advanced cryptosystems that can not be constructed by the conventional cryptographic technologies. However, they have a problem with processing time because a fairly complex calculation is required for their processing. Due to this problem, these sophisticated cryptographies have not yet led to practical use. In order to make these cryptographic applications practical, this thesis proposes efficient methods to calculate operations required for pairing-based cryptographies.

1.2 Motivation

Pairing is a bilinear map from two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a group $\mathbb{G}_3$, where they have respectively same prime order r. In detail, $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively becomes a subgroup in an elliptic curve group $E(\mathbb{F}_q)$ and $E(\mathbb{F}_{q^k})$, and $\mathbb{G}_3$ becomes a subgroup in $\mathbb{F}_{q^k}$, where q is a power of p and an extension degree k is especially called the *embedding degree*.

In pairing-based cryptography, not only pairing calculation but also scalar multiplications in $\mathbb{G}_1$ and $\mathbb{G}_2$, and exponentiations in $\mathbb{G}_3$ are carried out. Among these

operations, since pairing is the highest cost operation, a lot of improvements for pairing such as η_T pairing over super singular curves and Ate **Hess** *twisted* Ate**Hess** *optimized* Ate **TAte** optimized *twisted* Ate**TAte** *R*-ate**Rate** *Optimal***OptAte** Xate **Xate** pairings over ordinary curves, have been proposed in the recent years. Among these pairings, the fastest pairing is η_T pairing. However, η_T pairing has a disadvantage that supersingular curves are restricted to *embedding degree* $k \leq 6$. Since the *embedding degree* is important parameter that determines the security level of pairing-based cryptographies, efficient pairings on ordinary curves whose *embedding degree* are flexibly selectable are required. This thesis targets Ate and *twisted* Ate pairings because they are efficiently calculated on ordinary curves.

On the other hand, in addition to pairing, pairing-based cryptographies need to carry out a lot of scalar multiplications in $\mathbb{G}_1$ and $\mathbb{G}_2$ in proportion to the number of users. Therefore, efficient scalar multiplications in $\mathbb{G}_1$ and $\mathbb{G}_2$ can reduce the total cost of pairing-based cryptography.

In this thesis, we propose efficient scalar multiplications in $\mathbb{G}_1$ and $\mathbb{G}_2$, and pairings based on Ate and *twisted* Ate pairings.

Let P be a rational point in an elliptic curve group, a scalar multiplication $[s]P$ by scalar $s \in \mathbb{Z}$ means $(s-1)$-times elliptic curve additions of P. General approach to accelerate a scalar multiplication is a binary method. Note that a scalar s is at most the order r. Using a binary method, we can calculate $[s]P$ by $\lfloor \log_2 s \rfloor$-times elliptic curve doublings and $\mathrm{Hw}(s)$-times elliptic curve additions, where $\mathrm{Hw}(s)$ means the number of 1s' in the binary representation of s and it is generally called a *hamming weight* of s.

To accelerate a scalar multiplication, it is important that the scalar multiplication of an intrinsic scalar λ is calculated by efficiently computable endomorphisms. If the scalar λ is smaller than the order of an elliptic curve group, we can decompose a target scalar by λ-adic expansion. By using multi-scalar multiplication techniques, we can reduce the number of elliptic curve doublings to the bit-size of the scalar λ corresponding to the endomorphism. For example, when the elliptic curve is defined over an extension field, Frobenius endomorphism ϕ will efficiently work. Note that a Frobenius endomorphism is free from arithmetic operations. In the case of $\mathbb{G}_2$ of Ate and *twisted* Ate pairings, let t be a Frobenius trace of elliptic curve, a scalar multiplication by $\lambda = (t-1)$ corresponds to $\phi(P)$. Since $t \approx \sqrt{r}$ from Hasse's theorem, the number of elliptic doublings are reduced by about half. This relation $\phi(P) = [t-1]P$ has been considered optimal because the trace is the smallest among parameters construct an elliptic curve.

On the other hand, recent elliptic curves for pairing need one more parameter in addition to parameters such as p, t, and r. Elliptic curves over which pairing can be defined are called pairing-friendly curves. In general, it is difficult to generate such pairing-friendly curves because they need to satisfy some strict conditions. However, several methods to easily generate pairing-friendly curves are proposed in recent years **Taxo** For example, *families* of pairing friendly curves whose parameters such as characteristic p, order r, and trace t are given by polynomials in terms of integer χ are easily constructed. Especially, since *complete families* can generate a lot of elliptic curves, we can select the optimal curve suitable for pairing calculations and scalar multiplications. Among *families* of pairing friendly curves, there is a curve whose trace t is given by polynomial that has larger degree than or equal to 2. In this case, χ becomes the smallest among parameters to construct curves. Therefore, it is possible that we can obtain the relation that joins Frobenius maps and an intrinsic scalar that is smaller than trace t. Thus, it is important to optimize the relation available for a scalar multiplication for *families* of pairing friendly curves. This thesis

targets *families* of pairing-friendly curves, and we mainly deal with Barreto-Naehrig (BN) curves of *embedding degree* equal to 12 that is one of the most important *complete families* of pairing-friendly curves.

In the case of BN curves, we can obtain the key relation that joins Frobenius maps and a certain smaller scalar than t. In detail, since the scalar becomes about χ and t is given by $(6\chi^2+1)$, its bit-size becomes a half of t.

In the case of $\mathbb{G}_2$, Frobenius endomorphism efficiently works for a scalar multiplication. However, Frobenius endomorphism does not work for a rational point $\mathbb{G}_1$ because a rational point applied Frobenius map becomes itself. Therefore, an efficiently computable endomorphism in $\mathbb{G}_1$ is required to apply the technique with Frobenius map as a scalar multiplication in $\mathbb{G}_2$. This thesis proposes a Frobenius-like endomorphism on $\mathbb{G}_1$. Using twist techniques, we can prepare the another group that is isomorphic to $\mathbb{G}_1$ over an extension field. Therefore, let the group be $\mathbb{G}_1'$, we can use Frobenius endomorphism on $\mathbb{G}_1'$. Focusing on this property, we derive a new endomorphism from the endomorphism on $\mathbb{G}_1'$. Then, we optimize a key relation available for a scalar multiplication in $\mathbb{G}_1$ that joins a new endomorphism and a certain scalar.

Furthermore, we apply the key relations available for scalar multiplications in $\mathbb{G}_1$ and $\mathbb{G}_2$ to accelerating pairing calculations.

The calculation costs of pairing are the highest among operations required for pairing-based cryptographies. Since pairing calculation is inherently sequential, it is difficult to apply the efficient parallelization technique using some recent processors have several computation cores. In general, pairing calculations consists of two calculation parts, one is Miller's algorithm and the other is *final exponentiation*. Since Miller's algorithm is slower than *final exponentiation*, several improvements for Miller's algorithm such as Ate and *twisted* Ate have been proposed. A structure of the algorithm is approximately same as that of a binary method for a scalar multiplication. Therefore, Miller's algorithm iterates a certain process $\lfloor \log_2 s \rfloor$-times as a binary method, where s is a parameter gives an loop iterations of Miller's algorithm. Since the process in Miller's algorithm needs several operations such as elliptic curve additions in elliptic curves and multiplications in extension fields, pairing becomes a fairly complex operation. Though a scalar multiplication uses a random number s, the number of calculations of Miller's algorithm is given by a specific number. For example, the number of calculation loops of Miller's algorithm for Ate pairing is given by $\lfloor \log_2(t-1) \rfloor$. That is, the calculation costs of Miller's algorithm is determined by the number of loop iterations. Therefore, we can reduce the calculation costs of Miller's algorithm by reducing its number of iterations. In addition, Hess shows that the lower bound of the number of iterations of Miller's algorithm for each pairing-friendly curve. In the case of BN curves, it becomes about $\lfloor \log_2 \chi \rfloor$, however Ate and *twisted* Ate pairing does not achieve.

In the case of a scalar multiplication, we can reduce the number of elliptic curve doublings by decomposing a scalar with the key relation. Using divisor theorem, a Miller's algorithm can be also decompose into several Miller's algorithm calculations whose the number of iterations are small. However, since there is no efficiently computable Miller's algorithm calculation for a certain number of iterations, the decomposition does not work. Rather, when we decompose Miller's algorithm, extra operations such as exponentiations in extension fields are required. This thesis shows that when we decompose a Miller's algorithm into several Miller's algorithms, some decomposed Miller's algorithms that has the bilinearity after applying *final exponenitaion* can be skipped by using the property of bilinearity. In the case of Ate pairing, Miller's algorithm has the bilinearity when a parameter that gives

the number of iteration is equal to $(t-1)$. Therefore, the key relation for a scalar multiplication in $\mathbb{G}_2$ is closely related to Ate pairing. In this thesis, Miller's algorithm is decomposed using the key relation, and then a new pairing whose number of iterations for Miller's algorithm is smaller than that of Ate pairing is proposed. As a result, the proposed pairing achieves the lower bound of the number of iterations for Miller's algorithm. Meanwhile, focusing on the decomposition technique for Miller's algorithm, Vercauteren, Lee et al. and the authors have respectively proposed Optimal, *R*-ate, and Xate pairings, independently. Optimal and *R*-ate pairings also achieve the lower bound of the number of iterations for Miller's algorithm. This thesis compares these pairings with our proposed pairing (Xate pairing).

On the other hand, the number of iterations for *twisted* Ate pairing is closely related to the key relation for a scalar multiplication in $\mathbb{G}_1$. That is, a new pairing based on *twisted* Ate pairing is derived, since its Miller's algorithm can be efficiently decomposed by the key relation. This pairing have been proposed by Lee et al. as *twisted R*-ate pairing, but the pairing does not achieve the lower bound of number of iterations for Miller's algorithm. In detail, the number of iterations is twice larger than that of the proposed pairing based on Ate pairing in the case of BN curves. This thesis first derives an another key relation that decomposes Miller's algorithm of *twisted* Ate pairing to two Miller's algorithm calculations whose maximum number of iterations is equal to that of the proposed pairing based on Ate pairing using the key relation available for a scalar multiplication in $\mathbb{G}_1$. Then, using a precomputed scalar multiplication, we propose a method to parallelize the two Miller's algorithm calculations with multi-pairing or *thread-computing*.

Since the proposed methods can substantially improve operations such as scalar multiplications and pairings required for pairing-based cryptographies, we can help to solve the problem on processing times. Therefore, our research contributes to promoting sophisticated cryptographies such as ID-based cryptographies and group signature authentications.

1.3 Outline

This thesis is organized as follows:

In Chapter 2, we briefly review the mathematical fact to define the pairing, and describe about the conventional pairing such as Tate, Ate, *twisted* Ate pairings. In addition, a target class of elliptic curves are shown. Ate and *twisted* Ate pairings improves Tate pairing by setting certain groups that have a special properties to $\mathbb{G}_1$ and $\mathbb{G}_2$. In this thesis, we target Ate and *twisted* Ate pairings, and accelerates scalar multiplications in their $\mathbb{G}_1$ and $\mathbb{G}_2$. In addition, new pairings respectively based on Ate and *twisted* Ate pairings are proposed. Chapter 3 proposes an efficient scalar multiplication in $\mathbb{G}_2$ that used by Ate and *twisted* Ate pairings. To accelerate a scalar multiplication, it is important that a certain scalar multiplication is calculated by efficiently computable endomorphisms. A target $\mathbb{G}_2$ has a property that a certain scalar multiplication is calculated by Frobenius endomorphism that is efficiently computable. Focusing on this property, we derive a key relation available for a scalar multiplication in $\mathbb{G}_2$ from the structural properties of target elliptic curves. Then, using the key relation, an efficient scalar multiplication is proposed. In addition, we show that the proposed scalar multiplication is about 40% faster than the conventional method from experimental results.

Chapter 4 proposes an efficient scalar multiplication in $\mathbb{G}_1$ that used by Ate and *twisted* Ate pairings. A target $\mathbb{G}_1$ does not have a property that Frobenius endomorphism is available for a scalar multiplication. Therefore, it is difficult to apply the method proposed in chapter 3 to a scalar multiplication in $\mathbb{G}_1$. In order to solve this problem, we propose a new endomorphism available for a scalar multiplication in $\mathbb{G}_1$. Using the endomorphism, a key relation is derived in a same manner of $\mathbb{G}_2$. Then, using the key relation, an efficient scalar multiplication is proposed. In addition, this chapter shows that the proposed method is about 30% faster than the conventional method from experimental results.

In chapter 5, how to decompose the Miller's algorithm calculation is described, and it is shown that the approach for accelerating scalar multiplications is also applied to pairing calculations. Then, we proposes a new pairing based on Ate pairing using the key relation available for a scalar multiplication in $\mathbb{G}_2$. This is because the property of $\mathbb{G}_2$ is closely related to Ate pairing. In addition, we show that the proposed pairing is about two times faster than Ate pairings from experimental results.

Chapter 6 proposes an efficient pairing based on *twisted* Ate pairing using the key relation proposed in chapter 4. In addition, the pairing can be efficiently applied the parallelizing technique that can not be applied to the conventional pairings. From the experimental results, we show that the proposed method can reduce the calculation times of *twisted* Ate pairing by up to about 70%.

Chapter 7 concludes this thesis.

Chapter 2

Fundamentals

2.1 Introduction

This chapter briefly review the mathematical fact to define the pairing, and shows a target class of elliptic curves. In addition, we describe the conventional pairings such as Tate, Ate, *twisted* Ate pairings.

2.2 Finite Field

2.2.1 Group

A group is an algebraic system defined as follows.

Definition 1 (Group) *A group* $\langle \mathbb{G}, \circ \rangle$ *is a nonempty set with a binary operations* $\circ$ *that satisfies the following group axioms:*

G1 : (Closure) *For all* $a, b \in \mathbb{G}$*, the result of* $a \circ b$ *is also in* $\mathbb{G}$*.*

G2 : (Associativity) $(a \circ b) \circ c = a \circ (b \circ c) \qquad a, b, c \in \mathbb{G}.$

G3 : (Unit Element) *For* $\forall a \in \mathbb{G}$*, there exists an element* $e \in \mathbb{G}$ *such that* $a \circ e = e \circ a = a$*, where e is called unit element.*

G4 : (Inverse Element) *For* $\forall a \in \mathbb{G}$*, there exists an element* $x \in \mathbb{G}$ *such that* $a \circ x = x \circ a = e$*, where x is called inverse element of a.*

■

Definition 2 (Commutative Group)

AG5 : (Commutativity) *A group* $\mathbb{G}$ *is said to be commutative (or abelian), if* $a \circ b = b \circ a$ *for* $^{\forall} a, b \in \mathbb{G}$*.*

■

For example, the algebraic system $\langle \mathbb{Z}, + \rangle$ is an infinite commutative group, where $\mathbb{Z}$ is the integer set and $+$ means the ordinary addition for integers. For a finite group, its order is defined as follows.

Definition 3 (Order of Group) *The order* $\#\mathbb{G}$ *is the number of elements in finite group* $\mathbb{G}$*.*

■

Let us consider an example of finite groups. An algebraic system $\langle \mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}, + \rangle$ is not a group because it does not satisfy the group axioms. Therefore, in order to construct a group from $\mathbb{Z}_n$, it is necessary to modify the addition. We will define a new sum as

$$a + b \equiv c \mod n \qquad a, b \in \mathbb{Z}_n, \tag{2.1}$$

where the notation "mod n" means that c is assigned to a remainder on division by n when $a + b = c \notin \mathbb{Z}_n$. Therefore, c certainly belongs to $\mathbb{Z}_n$ and then $\langle \mathbb{Z}_n, + \rangle$ forms a group.

There is a convenient way of presenting a finite group. A table displaying the group operation is referred to as *Cayley table*. For example, the group $\mathbb{Z}_4$ is presented as follows.

Example 2.1 *The Cayley table for the group $\mathbb{Z}_4$ is:*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

In what follows, we will use the notation of ordinary addition such that $a + a = 2a$ and $a + a + a = 3a$ (in multiplicative notation, these are denoted by a^2,a^3).

Definition 4 (Cyclic Group) *A group $\mathbb{G}$ is said to be* cyclic *if there is an element $g \in \mathbb{G}$ such that for any $a \in \mathbb{G}$ there is some integer j with $a = g^j$. Such an element g is called a generator of the cyclic group.* ■

From the definition, we can see that any elements in cyclic group are generated with iterative operations of generator g. **Figure**. 2.1 shows it schematically.

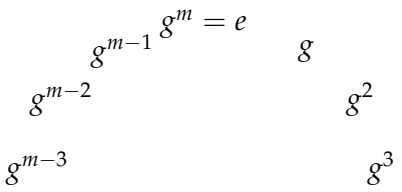

FIGURE 2.1: Cyclic group

In general, for an element $a \in \mathbb{G}$, the least positive integer m such that $a^m = e$ is called the order of a, where e is the unit element in $\mathbb{G}$.

2.2.2 Field

Field is an algebraic system defined as follows.

Definition 5 (Field) *A field $\langle \mathbb{F}, +, \cdot \rangle$ has two binary operations denoted by $+$ and $\cdot$, such that:*

F1 : (Additive Group) $\mathbb{F}$ *is a commutative group with respect to* $+$.

F2 : (Multiplicative Group) $\mathbb{F}^*$*is a group with respect to* $\cdot$*, where* $\mathbb{F}^*$*is the set that consists of every element distinct from the unit element (zero element) with respect to* $+$.

F3 : (Distributive law) *For all* $a, b, c \in \mathbb{F}$ *we have* $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$.

■

In general, the elements 0 and 1 denote the unit elements regarding to addition $+$ and multiplication $\cdot$, respectively.

Definition 6 (Order of Finite Field) *The order is the number of elements in* $\mathbb{F}$. *If the order of* $\mathbb{F}$ *is finite,* $\mathbb{F}$ *is called finite field.* ■

Definition 7 (Characteristic of Finite Field) *The least positive number* n *such that* $na = 0$ *for every* $a \in \mathbb{F}$ *is called characteristic.* ■

This paper treats only finite fields. Finite fields have the following property, which is often used in cryptographic area.

Theorem 1 *For every finite field* $\mathbb{F}$*, the multiplicative group* $\mathbb{F}^*$*is cyclic.* ■

For example, ElGamal encryption **multi** can be defined over multiplicative group of $\mathbb{F}$. Its security depends on the difficulty of a problem in $\mathbb{F}$ related to computing *discrete logarithms*. A subset $\mathbb{K}$ of a field $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ will be called a *subfield* of $\mathbb{F}$. In this case, $\mathbb{F}$ is called an *extension (field)* of $\mathbb{K}$. If $\mathbb{K} \neq \mathbb{F}$, we say that $\mathbb{K}$ is a *proper subfield* of $\mathbb{F}$. Then, *prime field* is defined as follows.

Definition 8 (Prime Field) *A field containing no proper subfield is called prime field.* ■

Moreover, the following theorem is given.

Theorem 2 *Every finite field has a prime field as a subfield.* ■

Therefore, finite fields are classified into two types, which are prime field and its extension field. Prime field $\mathbb{F}_p$ has a prime number p as the order and characteristic. In the same way as Eq.(2.1), we can define fundamental operations of $\mathbb{F}_p = \{0, 1, 2 \cdots, p-1\}$ by using remainder of integer as follows,

$$a + b \equiv c \mod p, \tag{2.2a}$$

$$a \cdot b \equiv c \mod p \qquad a, b \in \mathbb{F}_p. \tag{2.2b}$$

In order to understand it easily, following examples are shown.

Example 2.2 *The Cayley table for the two operations* $+$ *and* $\cdot$ *for elements in* $\mathbb{F}_5$ *are as follows:*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

As described above, we can define arithmetic operations in $\mathbb{F}_p$ by modular operations (mod p) for integers. However, it does not work in an extension field $\mathbb{F}_{p^m}$. In the next section, arithmetic operations in extension field $\mathbb{F}_{p^m}$ is described in detail.

2.2.3 Extension Field

A subset $\mathbb{F}_0$ of a field $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ will be called a *subfield* of $\mathbb{F}$. In this case, $\mathbb{F}$ is called an *extension field* of $\mathbb{F}_0$. An extension field of a prime field $\mathbb{F}_p$ can be represented as m-dimensional vector space that has m elements in $\mathbb{F}_p$. Let the vector space be the m-th extension field, it is denoted by $\mathbb{F}_{p^m}$. The order of extension fields $\mathbb{F}_{p^m}$ is given as p^m. In what follows, let q be the power of p, the extension field of a prime field $\mathbb{F}_p$ is denoted by $\mathbb{F}_q$.

There are several methods to represent an element in extension fields, such as polynomial basis and normal basis. In this thesis, we use normal basis. Let ω be a root of m-th irreducible polynomial over $\mathbb{F}_q$, we consider the following m elements.

$$\omega,\ \omega^q,\ \omega^{q^2},\ \cdots,\ \omega^{q^{m-1}}$$

All elements in this set are conjugate to each other. When the set of the conjugates become linearly independent, this is called *normal basis*. Using normal basis, an element $\alpha \in \mathbb{F}_q$ is expressed as a polynomial by

$$\alpha = a_1\omega + a_2\omega^q + a_3\omega^{q^2} + \cdots + a_m\omega^{q^{m-1}}, \tag{2.3}$$

where $a_1,\ a_2,\ a_3, \cdots,\ a_m \in \mathbb{F}_q$.

Arithmetic operations in $\mathbb{F}_{q^m}$ are carried out with ordinary addition and multiplication for polynomial and modular reduction by irreducible polynomial.

2.2.4 Frobenius Map

For any element $\alpha \in \mathbb{F}_{q^m}$, let us consider the following map $\pi_q : \alpha \to \alpha^q$.

$$\begin{aligned}
\pi_q(\alpha) &= \left(a_1\omega + a_2\omega^q + a_3\omega^{q^2} + \cdots + a_m\omega^{q^{m-1}}\right)^q \\
&= a_1\omega^q + a_2\omega^{q^2} + a_3\omega^{q^3} + \cdots + a_m\omega^{q^m} \\
&= a_m\omega + a_1\omega^q + a_2\omega^{q^2} + \cdots + a_{m-1}\omega^{q^{m-1}}
\end{aligned} \tag{2.4}$$

Note that the order of $\mathbb{F}^*_{q^m}$ is given by $q^m - 1$, that is, $\omega^{q^m} = \omega$ is satisfied. Furthermore, a^q is equal to a for each coefficients a.

Therefore, the map $\pi_q(\alpha)$ is efficiently calculated by cyclic shift operations among its basis coefficients, which is free from arithmetic operations. From the computational efficiency, the map π_q is especially called Frobenius map.

In ElGamal Encryption, many exponentiations are executed in encryption and decryption processes. When the exponent is equal to p, its calculation cost can be reduced by using Frobenius map. Therefore, Frobenius map is widely used in the cryptographic application.

2.2.5 Quadratic Residue/Quadratic Non-residue, and Cubic Residue/Cubic Non-residue

For any non-zero element $d \in \mathbb{F}_q$, d is called a Quadratic Residue (QR) when x such that $x^2 = d$ exists in $\mathbb{F}_q$. On the other hand, when such an x does not exist in $\mathbb{F}_q$, d is called a Quadratic Non-Residue (QNR). We can identify whether or not d is a QR by following test.

$$d^{(q-1)/2} = \begin{cases} 1 & : \text{QR} \\ -1 & : \text{QNR} \end{cases} \tag{2.5}$$

All elements in finite fields $\mathbb{F}_q$ of odd characteristics become QR in extension fields $\mathbb{F}_{q^{2j}}$. On the other hand, quadratic non-residues also become QNR in $\mathbb{F}_{q^i}$, where i is not divisible by 2.

2.3 Elliptic Curve

In this section, we review elliptic curves and pairings.

2.3.1 Additive Group over Elliptic Curves

In general, let $p > 3$, an elliptic curve $E/\mathbb{F}_p$ over a finite field $\mathbb{F}_p$ is defined as

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b,\ 42a^3 + 27b^2 \neq 0,\ a, b \in \mathbb{F}_p. \tag{2.6}$$

The field that x and y belong to is called the definition field. The solutions (x, y) of Eq.(2.6) is called rational points. $E(\mathbb{F}_q)$ that is the set of rational points on the curve, including the *point at infinity* $\mathcal{O}$, forms an additive abelian group. The *point at infinity* works as an unity element in $E(\mathbb{F}_q)$. When the definition field is $\mathbb{F}_{q^m}$, we denote the additive group by $E(\mathbb{F}_{q^m})$.

For rational points $P_1(x_1, y_1), P_2(x_2, y_2) \in E(\mathbb{F}_q)$, the elliptic curve addition $P_3(x_3, y_3) = P_1 + P_2$ is defined as follows.

$$\begin{aligned} \lambda &= \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P_1 \neq P_2,\ x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & P_1 = P_2 \end{cases} \\ x_3 &= \lambda^3 - x_1 - x_2 \\ y_3 &= (x_1 - x_3)\lambda - y_1 \end{aligned}$$

In the case of $P_1 = P_2$, the addition is especially called elliptic curve doubling.

Let a rational point $P(x, y)$, an inverse point $-P$ is given by $-P(x, -y)$. Elliptic curve cryptographies is constructed on elliptic curve groups $E(\mathbb{F}_q)$.

Let $\#E(\mathbb{F}_p)$ be the order of $E(\mathbb{F}_p)$, it is given as

$$\#E(\mathbb{F}_p) = p + 1 - t, \tag{2.7}$$

where t is the Frobenius trace of $E(\mathbb{F}_p)$.

From Hasse's theorem, t satisfies

$$|t| \leq 2\sqrt{p}. \tag{2.8}$$

Let $[s]P$ denote the $(s-1)$-times addition of a rational point P as,

$$[s]P = \sum_{i=0}^{s-1} P. \tag{2.9}$$

This operation is called a scalar multiplication. As a general approach for accelerating a scalar multiplication, the binary method is the most widely used. **Algorithm 2.1** shows the binary method. The binary method iterates elliptic curve doublings

and elliptic curve additions using binary representation of scalar. A scalar multiplication needs $\lfloor \log_2 s \rfloor$ elliptic curve doublings and $\lfloor \log_2 s \rfloor / 2$ elliptic curve additions on average.

Algorithm 2.1 : Binary method

Input :	P, n-bit integer $s = \sum_{i=0}^{\ell-1} s_i 2^i$, $s_i \in \{0, 1\}$
Output :	$R = [s]P$
1.	$R \leftarrow \mathcal{O}$
2.	For $i = \ell - 1$ to 0 by -1 do:
3.	$R \leftarrow R + R$
4.	If $s_i = 1$ then $R \leftarrow R + P$
5.	Return R

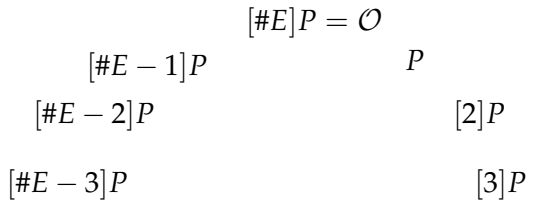

FIGURE 2.2: An image of elliptic curve group

2.3.2 Frobenius Map on Elliptic Curve Groups

In this section, we introduce Frobenius map for a rational point in $E(\mathbb{F}_q)$. For any rational point $P = (x, y)$, Frobenius map ϕ is given by $\phi : P(x, y) \rightarrow (x^q, y^q)$. Then, the following relation holds for any rational points in $E(\mathbb{F}_q)$ with regard to Frobenius map.

$$\left(\phi^2 - [t]\phi + [q]\right) P = \mathcal{O}.$$

Thus, we have

$$[q]P = \left([t]\phi - \phi^2\right) P. \tag{2.10}$$

From Hasse's theorem, note the bit-size of Frobenius trace t is about a half of the characteristic p. Using Eq.(2.10), we can efficiently calculate scalar multiplication **frobexp**

Chapter 3

ICCE-TW 2016

In elliptic curve cryptography (ECC), a scalar multiplication for rational point is the most time consuming operation. This paper proposes an efficient calculation for a scalar multiplication by applying Frobenious Mapping. Particularly, this paper deals with Barreto-Naehrig curve defined over extension field $\mathbb{F}_{q^2}$, where $q = p^6$ and p is a large prime.

3.1 Introduction

In cryptography research, elliptic curve cryptography (ECC) has gained a wide acceptance due to its smaller key size and greater security. In ECC, scalar multiplication (SM) is carried out at the encryption and decryption phases. SM is the major operation in ECC. Let us denote a scalar and rational point by s and P, respectively. Then, the SM is denoted by $[s]P$. In real cases s is significantly large number less than the order of rational point group. Since SM needs a complicated calculation over the definition field such as prime field, an efficient algorithm for SM is needed. Recently, ECC defined over extension field $\mathbb{F}_{q^2}$ with a large prime number p such as more than 2000 bits is used in some ECC based protocols. On the other hand, pairing based cryptography realizes some innovative application protocol. Pairing based cryptography requires pairing friendly curve which is difficult to generate. Barreto-Naehrig (BN) **BN** curve is one of the well known pairing friendly curve**BN_def** whose parameters are able to be systematically given. BN curve is mostly used due to its efficiency to realize pairing based cryptography. Thus, this paper proposes an efficient approach for calculating SM on BN curve particularly defined over extension field $\mathbb{F}_{q^2}$, where $q = p^6$ and p is a prime number by using Frobenious Mapping (FM) for the rational points.

3.2 Preliminaries

This section briefly discusses the fundamental arithmetic operations required for elliptic curve cryptography defined over prime field $\mathbb{F}_p$ and its extension field $\mathbb{F}_{q^2}$. In addition, this paper focuses on BN curve defined over $\mathbb{F}_{q^2}$, $q = p^6$.

3.2.1 BN curve over prime field $\mathbb{F}_p$

BN curve is a non super-singular (*ordinary*) pairing friendly elliptic curve of embedding degree 12**BN_def** The equation of BN curve defined over $\mathbb{F}_p$ is given by

$$E : y^2 = x^3 + b, \quad (b \in \mathbb{F}_p). \tag{3.1}$$

where $b \neq 0$. Its characteristic p, Frobenius trace t and order r are given by using an integer variable χ as follows:

$$p(\chi) = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, \tag{3.2}$$
$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1, \tag{3.3}$$
$$t(\chi) = 6\chi^2 + 1. \tag{3.4}$$

From Eq.(3.3) and Eq.(3.4) we find that the bit size of r is two times larger than t. Thus, these parameters generally satisfy $t \ll p \approx r$ and the following relation.

$$r = p + 1 - t. \tag{3.5}$$

Point addition

Let $E(\mathbb{F}_p)$ be the set of all rational points on the curve defined over $\mathbb{F}_p$ and it includes the point at infinity denoted by $\mathcal{O}$. Let us consider two rational points $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, and their addition $R = P + Q$, where $R = (x_R, y_R)$ and $P, Q, R \in E(\mathbb{F}_p)$. Then, the x and y coordinates of R is calculated as follows.

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & (P \neq Q \text{ and } x_Q \neq x_P), \\ \frac{3x_P^2}{2y_P} & (P = Q \text{ and } y_P \neq 0), \\ \phi & \text{otherwise.} \end{cases} \tag{3.6a}$$

$$(x_R, y_R) = ((\lambda^2 - x_P - x_Q), \\ (x_P - x_R)\lambda - y_P), \text{ if } \lambda \neq 0. \tag{3.6b}$$
$$(x_R, y_R) = \mathcal{O} \quad \text{if } \lambda = 0. \tag{3.6c}$$

λ is the tangent at the point on EC and $\mathcal{O}$ it the additive unity in $E(\mathbb{F}_p)$. When $P = -Q$ then $P + Q = \mathcal{O}$ is called elliptic curve addition (ECA). If $P = Q$ then $P + Q = 2R$, which is known as elliptic curve doubling (ECD).

3.2.2 Elliptic curve over extension field $\mathbb{F}_{q^2}$

At first, let us consider arithmetic operations in $\mathbb{F}_{q^2}$, which is the degree 2 extension field over $\mathbb{F}_q$. In other words extension field $\mathbb{F}_{q^2}$ is the two dimensional vector space over $\mathbb{F}_q$. Let $\{v_0, v_1\}$ be a basis of $\mathbb{F}_{q^2}$, an arbitrary element $\mathbf{x} \in \mathbb{F}_{q^2}$ is represented as

$$\mathbf{x} = x_0 v_0 + x_1 v_1, \text{ where } x_i \in \mathbb{F}_q. \tag{3.7}$$

When we implicitly know the basis vectors v_0 and v_1, Eq.(3.7) is simply expressed as

$$\mathbf{x} = (x_0, x_1). \tag{3.8}$$

Addition and subtraction in $\mathbb{F}_{q^2}$

For vectors, addition, subtraction, and multiplication by a scalar in $\mathbb{F}_q$ are carried out by coefficient wise operations over $\mathbb{F}_q$. Let us consider two vectors $\mathbf{x} = (x_0, x_1)$

and $\mathbf{y} = (y_0, y_1)$. Then,

$$\begin{aligned} \mathbf{x} \pm \mathbf{y} &= (x_0 \pm y_0, x_1 \pm y_1), & (3.9) \\ k\mathbf{x} &= (kx_0, kx_1),\ k \in \mathbb{F}_q. & (3.10) \end{aligned}$$

Vector multiplication in $\mathbb{F}_{q^2}$

For a vector multiplication, we simply consider a polynomial basis representation. Let $f(x)$ be an irreducible polynomial of degree 2 over $\mathbb{F}_q$. Particularly, an irreducible binomial is efficient for calculations. In order to obtain an irreducible binomial, Legendre Symbol $\left(c/q\right)$ is useful. Consider a non-zero element $c \in \mathbb{F}_q$. If c does not have square roots, $f(x) = x^2 - c$ becomes an irreducible binomial over $\mathbb{F}_q$. In order to judge it, Legendre symbol is generally applied. Then, let its zero be ω, $\omega \in \mathbb{F}_{q^2}$, the set $\{1, \omega\}$ forms a polynomial basis in $\mathbb{F}_{q^2}$. Using this polynomial basis, the multiplication of two arbitrary vectors is performed as follows:

$$\begin{aligned} \mathbf{xy} &= (x_0 + x_1\omega)(y_0 + y_1\omega) \\ &= x_0y_0 + (x_0y_1 + x_1y_0)\omega + x_1y_1\omega^2 \\ &= (x_0y_0 + cx_1y_1) + (x_0y_1 + x_1y_0)\omega. & (3.11) \end{aligned}$$

In this calculation, we have substituted $\omega^2 - c = 0$, since ω is a zero of the irreducible binomial $f(x) = x^2 - c$.

Vector inversion in $\mathbb{F}_{q^2}$

For calculating the multiplicative inverse vector of a non-zero vector $\mathbf{x} \in \mathbb{F}_{q^2}$, first we calculate the conjugate of $\mathbf{x}$ that is given by Frobenius mapping (FM) $\pi_q(\mathbf{x}) = \mathbf{x}^q$. In detail, $\pi_q(\mathbf{x}) = \mathbf{x}^q$ is the conjugate of $\mathbf{x}$ to each other. Then the inverse $\mathbf{x}^{-1}$ of $\mathbf{x}$ is calculated as follows.

$$\mathbf{x}^{-1} = n(\mathbf{x})^{-1}(\mathbf{x}^q), \quad (3.12)$$

where $\mathbf{x}$, $\mathbf{x}^q$ are the conjugates and $n(\mathbf{x}) \in \mathbb{F}_q^*$ is their product. FM of $\mathbf{x}$, $\pi_q(\mathbf{x}) = (x_0 + x_1\omega)^q$ can be easily calculated using an irreducible binomial as follows:

$$\begin{aligned} (x_0 + x_1\omega)^q &= \sum_{i=0}^{q} \binom{q}{i} x_0^{(q-i)} (x_1\omega)^i \\ &= x_0 + x_1\omega^q \\ &= x_0 + x_1(\omega^2)^{\frac{q-1}{2}}\omega \\ &= x_0 + x_1(c)^{\frac{q-1}{2}}\omega \\ &= x_0 - x_1\omega, & (3.13) \end{aligned}$$

where we substituted the modular relation $\omega^q = -\omega$. In other words, the conjugate of $\mathbf{x}$ is given as $x_0 - x_1\omega$. Therefore, the calculation procedure for $n(\mathbf{x}) = \mathbf{x}\pi_q(\mathbf{x})$ is as follows:

$$\begin{aligned} n(\mathbf{x}) &= (x_0 + x_1\omega)(x_0 - x_1\omega) \\ &= x_0^2 - x_1^2\omega^2 \\ &= x_0^2 - cx_1^2. & (3.14) \end{aligned}$$

Since $n(\mathbf{x})$ is given without ω, it is found that $n(\mathbf{x})$ is a scalar. Finally, the inversion Eq.(3.12) is efficiently calculated.

3.3 Efficient scalar multiplication

In the context of pairing-based cryptography especially on BN curve, three groups $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ are considered. Among them, $\mathbb{G}_1, \mathbb{G}_2$ are rational point groups and $\mathbb{G}_T$ is the multiplicative group in the extension field. They have the same order r. Let us consider a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{q^2})$ as $Q(\mathbf{x}, \mathbf{y}) = (x_0 + x_1\omega, y_0 + y_1\omega)$. In the case of BN curve, it is known that Q satisfies the following relations:

$$\begin{aligned} [p+1-t]Q &= \mathcal{O} \\ [t-1]Q &= [p]Q. \end{aligned} \tag{3.15}$$

$$\begin{aligned} [\pi_p - p]Q &= \mathcal{O} \\ \pi_p(Q) &= [p]Q. \end{aligned} \tag{3.16}$$

Thus, these relations can accelerate a scalar multiplication in $\mathbb{G}_2$. From Eq.(3.16) $\pi_p(Q) = [p]Q$. Substituting $[p]Q$ in Eq.(3.15) we find $[t-1]Q = \pi_p(Q)$. Next, let us consider SM $[s]Q$, where $0 \leq s \leq r$. From Eq.(3.3) we know r is the order of BN curve where $[r]Q = \mathcal{O}$. Here, the bit size of s is nearly equal to r. As previously said, in BN curve r is two times larger than the bit size of t. It means that s is two times larger than the bit size of $t-1$. Therefore, let us consider $[t-1]$-adic representation of s as $s = s_0 + s_1(t-1)$, where s will be separated into two coefficients s_0 and s_1 whose size will be nearly equal to or less than the size of $[t-1]$. Then SM $[s]Q$ is calculated as follows:

$$\begin{aligned} [s]Q &= [s_0]Q + [s_1(t-1)]Q \\ &= [s_0]Q + s_1\pi_p(Q). \end{aligned} \tag{3.17}$$

Then, applying a multi-scalar multiplication technique, the above calculation will be efficiently carried out.

3.4 Conclusion and future work

In this paper, we have introduced an acceleration of scalar multiplication on Barreto-Naehrig (BN) curve defined over 2 degree extension field $\mathbb{F}_{q^2}$, $q = p^6$. We have showed that $[t-1]$-adic representation of large scalar number along with Frobenius mapping (FM) on rational points accelerates SM operation significantly, where t is the Frobenius trace of BN curve. As a future work, we would like to evaluate its computational time with a large prime characteristic as a practical situation.

Bibliography

[1] Paulo S. L. M. Barreto and M. Naehrig, “Pairing-friendly elliptic curves of prime order," Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers, pages 319-331, 2005. Springer LNCS 3897 (2006).

[2] D. Freeman, M. Scott, and E. Teske, “A taxonomy of pairing-friendly elliptic curves," Cryptography ePrint Archive, Report 2006/372 (2006), http://eprint.iacr.org/2006/372

[3] Y. Nogami, M. Akane, Y. Sakemi, H. Katou, and Y. Morikawa, “Integer Variable chi-Based Ate Pairing," Pairing- Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings, pages 178-191, 2008. Springer LNCS 5209 (2008).

Appendix A

Frequently Asked Questions

A.1 How do I change the colors of links?

The color of links can be changed to your liking using:

`\hypersetup{urlcolor=red}`, or
`\hypersetup{citecolor=green}`, or
`\hypersetup{allcolor=blue}`.

If you want to completely hide the links, you can use:

`\hypersetup{allcolors=.}`, or even better:
`\hypersetup{hidelinks}`.

If you want to have obvious links in the PDF but not the printed text, use:

`\hypersetup{colorlinks=false}`.

Research Activities

- Journal Papers (Peer-Reviewed)

1. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. “An Improvement of Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E100.A, no. 9, Sep. 2017, pp. 1838-1845, 2017. https://doi.org/10.1587/transfun.E100.A.1838
2. **Md. Al-Amin Khandaker**, Taehwan Park, Yasuyuki Nogami, and Howon Kim. “A Comparative Study of Twist Property in KSS Curves of Embedding Degree 16 and 18 from the Implementation Perspective." KIICE Journal of Information and Communication Convergence Engineering, vol. 15, no. 2, Jun. 2017, pp. 93-103, 2017. https://doi.org/10.6109/jicce.2017.15.2.97
3. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami, “Efficient Pairing-Based Cryptography on Raspberry Pi." Journal of Communications, vol. 13, no. 2, pp. 88-93, 2018. https://doi.org/10.12720/jcm.13.2.88-93
4. Yuta Hashimoto, **Md. Al-Amin Khandaker**, Yuta Kodera, Taehwan Park, Takuya Kusaka, Howon Kim, Yasuyuki Nogami, “An Implementation of ECC with Twisted Montgomery Curve over 32nd Degree Tower Field on Arduino Uno." International Journal of Networking and Computing (IJNC), vol. 8, no. 2, pp. 341-350, 2018. https://doi.org/10.15803/ijnc.8.2_341
5. Yuta kodera, Takeru miyazaki, **Md. Al-Amin Khandaker**, Md. Arshad ali, Takuya kusaka, Yasuyuki nogami and Satoshi uehara. “Distribution of Digit Patterns in Multi-Value Sequence over the Odd Characteristic Field." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E101.A, no. 9, Sep. 2018, pp. 1525-1536, 2018. https://doi.org/10.1587/transfun.E101.A.1525
6. Shunsuke Ueda, Ken Ikuta, Takuya Kusaka, **Md. Al-Amin Khandaker**, Ali Md. Arshad, Yasuyuki Nogami. “An Extended Generalized Minimum Distance Decoding for Binary Linear Codes on a 4-Level Quantization over an AWGN Channel." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E101.A, no. 8, Aug. 2018, pp. 1235-1244, 2018. https://doi.org/10.1587/transfun.E101.A.1235
7. Shoma Kajitani, Yasuyuki Nogami, Shunsuke Miyoshi, Thomas Austin, **Md. Al-Amin Khandaker**, Nasima Begum, Sylvain Duquesne, “Web-based Volunteer Computing for Solving the Elliptic Curve Discrete Logarithm Problem." International Journal of Networking and Computing (IJNC), vol. 6, no. 2, pp. 181-194, 2016. https://doi.org/10.15803/ijnc.6.2_181

- International conferences (Peer-Reviewed)

1. **Md. Al-Amin Khandaker**, Yuki Nanjo, Loubna Ghammam, Sylvain Duquesne, Yasuyuki Nogami, and Yuta Kodera. "Efficient optimal ate pairing at 128-bit security level." In: Patra A., Smart N. (eds) Progress in Cryptology (INDOCRYPT), 2017. Lecture Notes in Computer Science, vol 10698. Springer, Cham. https://doi.org/10.1007/978-3-319-71667-1_10.
2. **Md. Al-Amin Khandaker**, Hirotaka Ono, Yasuyuki Nogami, Masaaki Shirase, and Sylvain Duquesne. "An Improvement of Optimal Ate Pairing on KSS Curve with Pseudo 12-Sparse Multiplication." In: Hong S., Park J. (eds) Information Security and Cryptology (ICISC), 2016. Lecture Notes in Computer Science, vol 10157. Springer, Cham. https://doi.org/10.1007/978-3-319-53177-9_11.
3. **Md. Al-Amin Khandaker**, Yasuyuki Nogami, Hwajeong Seo, and Sylvain Duquesne. "Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18." In: Choi D., Guilley S. (eds) Information Security Applications (WISA), 2016. Lecture Notes in Computer Science, vol 10144. Springer, Cham. https://doi.org/10.1007/978-3-319-56549-1_19.
4. **Md. Al-Amin Khandaker**, and Yasuyuki Nogami. "Isomorphic Mapping for Ate-Based Pairing over KSS Curve of Embedding Degree 18." Fourth International Symposium on Computing and Networking (CANDAR), 2016. IEEE. https://doi.org/10.1109/CANDAR.2016.0113.
5. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "An improvement of scalar multiplication on elliptic curve defined over extension field Fq2." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2016. IEEE. https://doi.org/10.1109/ICCE-TW.2016.7520894.
6. **Md. Al-Amin Khandaker**, and Yasuyuki Nogami. "Frobenius Map and Skew Frobenius Map for Ate-based Pairing over KSS Curve of Embedding Degree 16 ." 32nd International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC), 2017. IEIE.
7. Yuki Nanjo, **Md. Al-Amin Khandaker**, Masaaki Shirase, Takuya Kusaka and Yasuyuki Nogami. "Efficient Ate-Based Pairing over the Attractive Classes of BN Curves." Information Security Applications (WISA), 2018. To appear Lecture Notes in Computer Science. Springer, Cham. (Acceptance Ratio 22/44 = 50%)
8. Yuta Hashimoto, **Md. Al-Amin Khandaker**, Yuta Kodera, Taehwan Park, Takuya Kusaka, Howon Kim and Yasuyuki Nogami. "An ECC Implementation with a Twisted Montgomery Curve over Fq32 on an 8-Bit Microcontroller." Fifth International Symposium on Computing and Networking (CANDAR), 2017. IEEE. https://doi.org/10.1109/CANDAR.2017.90.
9. Taehwan Park, Hwajeong Seo, **Md. Al-Amin Khandaker**, Yasuvuki Nogami, Howon Kim. "Efficient Parallel Simeck Encryption with GPGPU and OpenCL." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2018. IEEE. https://doi.org/10.1109/ICCE-China.2018.8448768.

10. Yuta Kodera, Takeru Miyazaki, **Md. Al-Amin Khandaker**, Ali Md Arshad, Yasuyuki Nogami, and Satoshi Uehara. "Distribution of bit patterns on multi-value sequence over odd characteristics field." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2017. IEEE. https://doi.org/10.1109/ICCE-China.2017.7991033
11. Ken Ikuta, Takuya Kusaka, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, and Thomas H. Austin. " Estimation of computational complexity of Pollard's rho method based attack for solving ECDLP over Barreto-Naehrig curves." 32nd International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC), 2017. IEIE.
12. Ken Ikuta, Sho Joichi, Kazuya Kobayashi, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. "A Study on the Parameter Size of the Montgomery Trick for ECDLP." International Symposium on Information Theory and its Applications (ISITA), 2018. IEICE. (To appear in IEEE Xplore).
13. Ken Ikuta, Sho Joichi, Kazuya Kobayashi, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. "A Study on the Parameter of the Distinguished Point Method in Pollard's Rho Method for ECDLP." International Symposium on Information Theory and its Applications (ISITA), 2018. IEICE. (To appear in IEEE Xplore).
14. Takuya Kusaka, Sho Joichi, Ken Ikuta, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, Satoshi Uehara, Nariyoshi Yamai and Sylvain Duquesne. "Solving 114-Bit ECDLP for a Barreto-Naehrig Curve." In: Kim H., Kim DC. (eds) Information Security and Cryptology (ICISC), 2017. Lecture Notes in Computer Science, vol 10779. Springer, Cham. https://doi.org/10.1007/978-3-319-78556-1_13.
15. Taehwan Park, Hwajeong Seo, Garam Lee, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, Howon Kim. "Parallel Implementations of SIMON and SPECK, Revisited." In: Kang B., Kim T. (eds) Information Security Applications (WISA), 2017. Lecture Notes in Computer Science, vol 10763. Springer, Cham. https://doi.org/10.1007/978-3-319-93563-8_24. (Acceptance Ratio $27/53 \approx 50\%$)
16. Yuta Kodera, Takuya Kusaka, Takeru Miyazaki, **Md. Al-Amin Khandaker**, Yasuyuki Nogami and Satoshi Uehara. "An Efficient Implementation of Trace Calculation over Finite Field for a Pseudorandom Sequence." Fifth International Symposium on Computing and Networking (CANDAR), 2017. IEEE. https://doi.org/10.1109/CANDAR.2017.86.
17. Akihiro Sanada, Yasuyuki Nogami, Kengo Iokibe, **Md. Al-Amin Khandaker**. "Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2017. IEEE. https://doi.org/10.1109/ICCE-China.2017.7991108

- Domestic conferences

1. **Md. Al-Amin Khandaker**, Hirotaka Ono, Yuki Nanjo, Takuya Kusaka and Yasuyuki Nogami. "Efficient Optimal-Ate Pairing on BLS-12

Curve Using Pseudo 8-Sparse Multiplication." Computer Security Symposium (CSS), 2017, CD-ROM (3E1-4).

2. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. “Efficient Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve." Symposium on Cryptography and Information Security (SCIS), 2017, CD-ROM (B1-3).
3. Hirotaka Ono, **Md. Al-Amin Khandaker**, Yuki Nanjo, Toshifumi Matsumoto, Takuya Kusaka and Yasuyuki Nogami. “An Implementation and Evaluation of ID-based Authentication on Raspberry Pi with Pairing Library." Symposium on Cryptography and Information Security (SCIS), 2018, CD-ROM (4D2-1).
4. Yuki Nanjo, **Md. Al-Amin Khandaker**, Yuta Kodera and Yasuyuki Nogami. “Implementation method of the pairing over BN curve using two type of extension fields." Symposium on Cryptography and Information Security (SCIS), 2018, CD-ROM (4D2-3).
5. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami. “The relation between the efficient sextic twist and constant of the modular polynomial for BN curve." Computer Security Symposium (CSS), 2017, CD-ROM (3E1-3).
6. Norito Jitsui, Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. “ Efficient Elliptic Scalar Multiplication for Pairing-Based Cryptography over BLS48." Symposium on Cryptography and Information Security (SCIS), 2018, CD-ROM (3B4-1).

Biography

Md. Al-Amin Khandaker was born on September 11, 1990, in a beautiful village of Bangladesh. He completed his high school in 2007 and in 2008, admitted to Jahangirnagar University, Bangladesh. In 2012, he graduated majoring in Computer Science and Engineering. After that, he joined in a Holland-based off-shore software development company in Dhaka. In 2015 he awarded Japan Govt. Scholarship (MEXT) to pursue Doctor's course in the field of cryptography in Okayama University under the supervision of Professor Yasuyuki NOGAMI. His main fields of research are optimization and efficient implementation techniques for the elliptic curve, pairing-based cryptography and it's application for IoT security. He is a graduate student member of IEEE.