A Consideration of an efficient calculation over the extension field of degree 3 and 4 for elliptic curve pairing cryptography

Author
Okayama University
Akihiro Sanada
Yuta Kadera
Yasuyuki Nogami

Future University Hakodate
Masaaki Shirase

University Rennes 1
Sylvain Duquesne

Acknowledgement
This work was partially supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan.

Introduction
Recently, pairing-based cryptography has been paid much attention since it realizes many innovative security applications. Since recent pairings are defined over extension fields \( F_{p^k} \) and \( F_{p^m} \), the efficiency of pairing depends on the arithmetic in these extension fields. Thus, this work considers multiplication, squaring, Frobenius mapping, and inversion over \( F_{p^k} \) and \( F_{p^m} \) in order to make them more efficient by using CVM and then evaluates these calculation costs with Karatsuba-based method.

Figure 1. Overview of security on ECC

Example over \( F_{p^2} \)
Karatsuba based method

\[
\begin{align*}
(a_1, a_2, a_3, b_1, b_2, b_3) &\rightarrow (a_1 + b_1 + a_2 + b_2 + a_3 + b_3)^2 \\
&= a_1b_1 + 2(a_1a_2b_1 + a_1b_2) + a_1b_3 + a_1b_2 + a_2b_3 + a_3b_3
\end{align*}
\]

CVM based (Cyclic Vector Multiplication Algorithm)

\[
\begin{align*}
(a_1, a_2, a_3, b_1, b_2, b_3) &\rightarrow (a_1 + b_1)(a_2 + b_2 + a_3 + b_3)
\end{align*}
\]

Table 1. Comparison of calculation costs

<table>
<thead>
<tr>
<th>Operation</th>
<th>CVM-based</th>
<th>Cyclic-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplication</td>
<td>9M+27A</td>
<td>6M+24A</td>
</tr>
<tr>
<td>Squaring</td>
<td>2M+5A</td>
<td>2M+3A</td>
</tr>
<tr>
<td>Frobenius mapping</td>
<td>3M</td>
<td>0</td>
</tr>
<tr>
<td>Inversion</td>
<td>17M+164A</td>
<td>31M+252A</td>
</tr>
</tbody>
</table>

Conclusions
Most of CVM-based arithmetic is superior to those of the Karatsuba-based method. It is noted that the modular prime number \( p \) for each condition needs to satisfy a certain condition. When \( p \) satisfies both of them, our proposed method has better costs.

Future work
We will apply the proposed methods in pairing-based Cryptosystem (ex. Figure 4) to evaluate the efficiency of the proposed methods.

Figure 4. Cryptosystem based on Math

Result of degree 3
As a construction, the Karatsuba-based multiplication over \( F_{p^2} \)

\[
\begin{align*}
(a_1, a_2, a_3, b_1, b_2, b_3) &\rightarrow (a_1 + b_1 + a_2 + b_2 + a_3 + b_3)^2 \\
&= a_1b_1 + 2(a_1a_2b_1 + a_1b_2) + a_1b_3 + a_1b_2 + a_2b_3 + a_3b_3
\end{align*}
\]

CVMA based method's multiplication over \( F_{p^2} \)

\[
\begin{align*}
(a_1, a_2, a_3, b_1, b_2, b_3) &\rightarrow (a_1 + b_1)(a_2 + b_2 + a_3 + b_3)
\end{align*}
\]

Vector space \( \mu \) is a point over the characteristic equation of the \( \mu \) is a degree over \( \mu \) is a degree.

Comparison of Calculation Cost over \( F_{p^2} \)

\[
\begin{align*}
\text{addition} &\rightarrow 18 \\
\text{multiplication} &\rightarrow 13 \\
\text{squaring} &\rightarrow 2 \\
\text{inversion of scalar} &\rightarrow 20
\end{align*}
\]

Result of degree 4
Efficient extension field \( F_{p^2} \) with Karatsuba-based method is constructed by towerings such as \( F_{p^2} \). Modular polynomial are \( f(x) = x^2 + 1 \) and \( g(x) = x^2 + (w + 1) \), where \( w \) is the zero of \( f(x) \). Then, \( F_{p^2} \) is constructed by the basis \( \{1, w\} \), where \( w \) is the zero of \( g(x) \) for this construction needs to satisfy \( w^2 = -w - 1 \) (mod \( f(x) \)).

The proposed method uses the basis \( \{1, w^2, w^3\} \) defined by modular polynomial \( g(x) = x^2 + (w + 1) \) and its zero \( w \in F_{p^2} \). In this case, \( p \equiv 1 \pmod{2} \) such that \( \{1, w\} \) becomes a basis. It is noted that our method is available for more prime numbers as \( p \) that conventional method; moreover it realizes efficient multiplication, squaring, and Frobenius mapping as shown in Figure 3.

Comparison of Calculation Cost over \( F_{p^2} \)

\[
\begin{align*}
\text{addition} &\rightarrow 18 \\
\text{multiplication} &\rightarrow 13 \\
\text{squaring} &\rightarrow 2 \\
\text{inversion of scalar} &\rightarrow 20
\end{align*}
\]