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 Kodera

Yasuyuki Nogami

Future University Hakodate

Masaaki Shirase

University Rennes 1

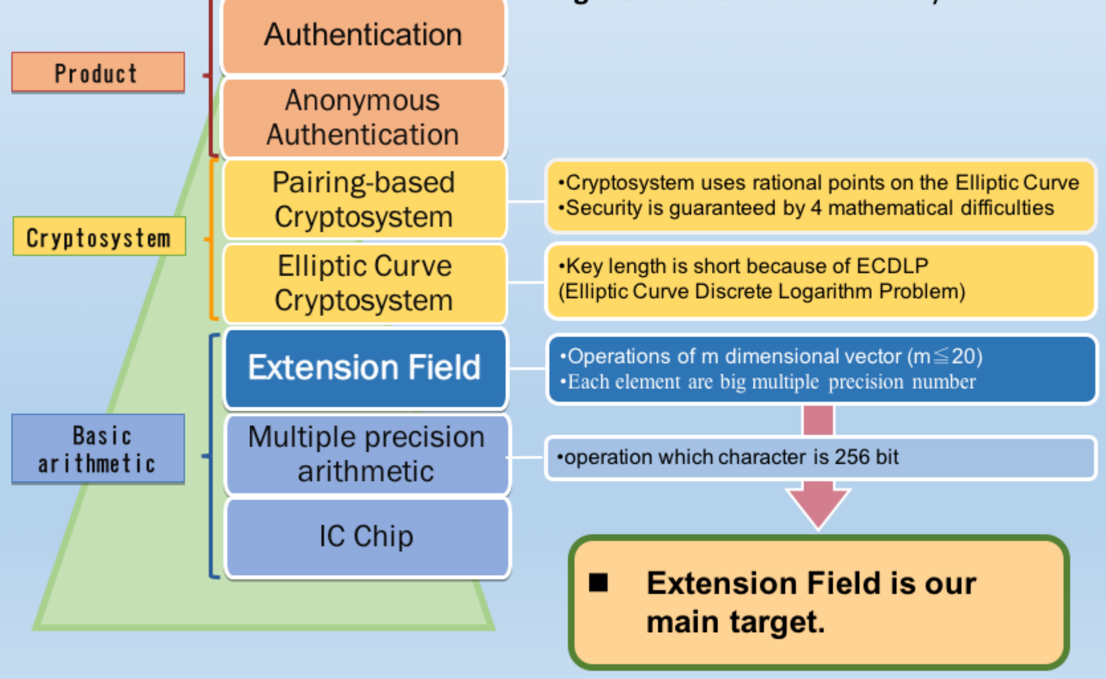
Sylvain Duquesne

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 $F_{p^{18}}$ and $F_{p^{24}}$, the efficiency of pairing depends on the arithmetic in these extension field.

Thus, this work considers multiplication, squaring, Frobenius mapping, and inversion over F_{p^3} and F_{p^4} as the base of $F_{p^{18}}$ and $F_{p^{24}}$ in order to make them more efficient by using CVMA and then evaluate these calculation costs with Karatsuba-based method.

Figure 1. Overview of security on ECC



Example over F_{p^2}

Karatsuba based method

let $X = a + b\omega, Y = c + d\omega$

base$\{1,\omega\}$: $\omega^2 = -1$

$$
\begin{aligned}
XY &= (a + b\omega)(c + d\omega) \\
&= ac + (ad + bc)\omega + bd\omega^2 \\
&= ac - db + [(a + b)(c + d) - ac - bd]\omega
\end{aligned}
$$

CVMA based (Cyclic Vector Multiplication Algorithm)

let $X = a\omega + b\omega^2, Y = c\omega + d\omega^2$

base $\{\omega,\omega^2\}$: $\omega^3 = 1 = -\omega - \omega^2$

$$
\begin{aligned}
XY &= (a\omega + b\omega^2)(c\omega + \omega^2) \\
&= ac\omega^2 + (ad + bc)\omega^3 + bd\omega^4 \\
&= \{(a - b)(c - d) - ac\}\omega + \{(a - b)(c - d) - bd\}\omega^2
\end{aligned}
$$

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.

Result of degree 3

As a competitive construction, Karatsuba-based method uses polynomial basis $\{1, \alpha, \alpha^2\}$ defined by method uses polynomial $f(x) = x^3 - 2$ and its zero $\alpha \in F_{p^3}$. In this case, it needs to satisfy $2^{\frac{p-1}{3}} \not\equiv 1 (mod\ p)$ so that $f(x)$ becomes irreducible overF_p.

On the other hand, the proposed method uses the basis $\{\tau_1, \tau_2, \tau_3\} = \{\omega - \omega^{-1}, \omega^2 - \omega^{-2}, \omega^3 - \omega^{-3}\}$ defined by modular polynomial $\Phi_7(x) = (x^7 - 1)/(x - 1)$ and its zero $\omega \in F_{p^3}$. In this case, $p \not\equiv 1,6\ (mod\ p)$ such that $\{\tau_1, \tau_2, \tau_3\}$ becomes a basis. It is noted that our method is available for more prime numbers as p than conventional method, moreover it realizes efficient multiplication, squaring, and Frobenius mapping as shown in Figure 2.

Karatsuba based method's multiplication over F_{p^3}

$$
\begin{aligned}
&(a_0 + a_1\alpha + a_2\alpha^2)(b_0 + b_1\alpha + b_2\alpha^2) \\
&= a_0b_0 + 2[(a_1 + a_2)(b_1 + b_2) - a_1b_1 - a_2b_2] \\
&\quad +[(a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1 + 2a_2b_2]\alpha \\
&\quad +[(a_0 + a_2)(b_0 + b_2) - a_0b_0 - a_2b_2 + a_1b_1]\alpha^2
\end{aligned}
$$

1: $a_0b_0 + 2[(a_1 + a_2)(b_1 + b_2) - a_1b_1 - a_2b_2]$

α: $(a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1 + 2a_2b_2$

α^2: $(a_0 + a_2)(b_0 + b_2) - a_0b_0 - a_2b_2 + a_1b_1$

CVMA based method's multiplication over F_{p^3}

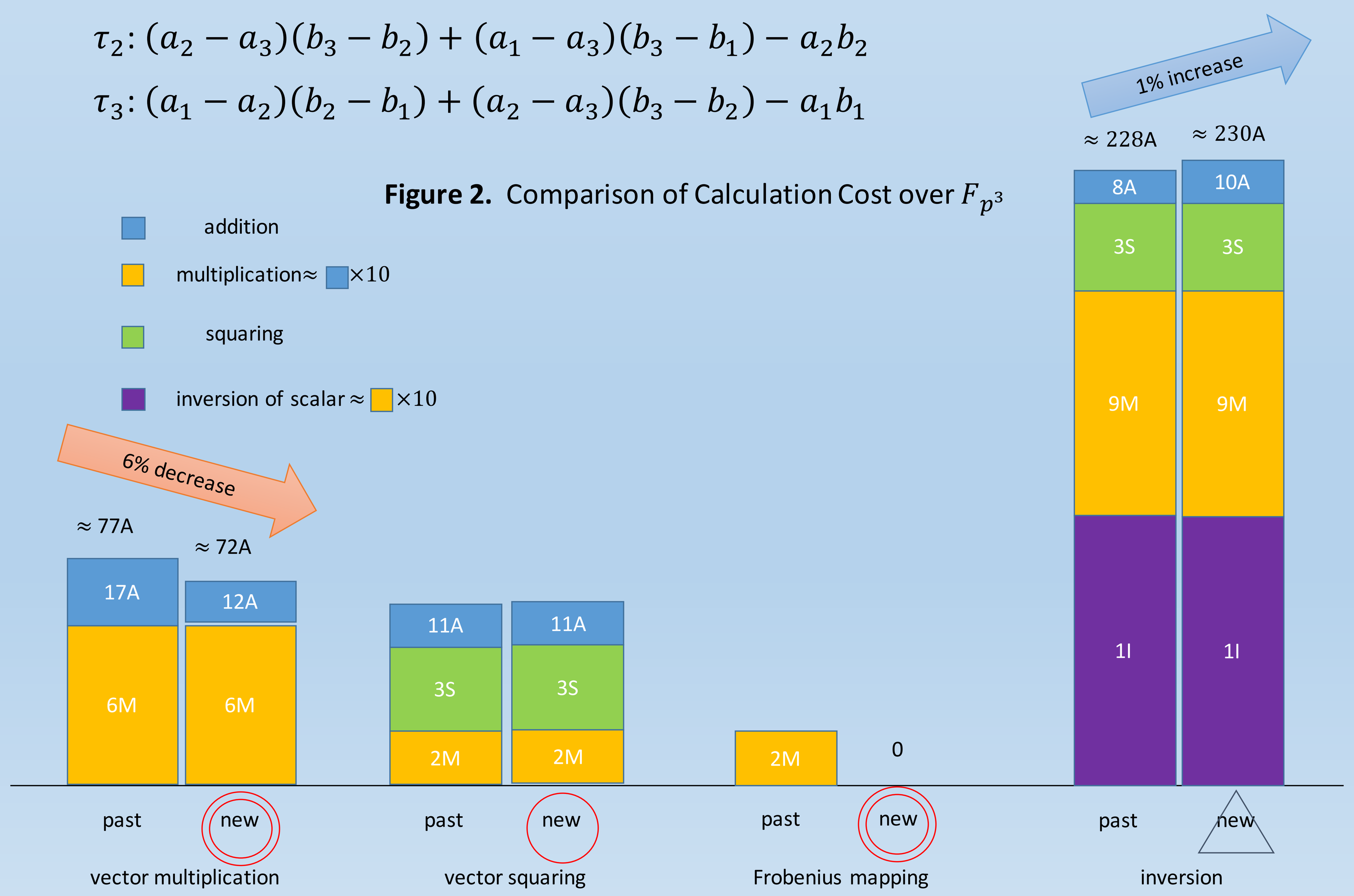
$(a_1\tau_1 + a_2\tau_2 + a_3\tau_3)(b_1\tau_1 + b_2\tau_2 + b_3\tau_3)$

τ_1: $(a_1 - a_2)(b_2 - b_1) + (a_2 - a_3)(b_3 - b_2) - a_1b_1$

τ_2: $(a_2 - a_3)(b_3 - b_2) + (a_1 - a_3)(b_3 - b_1) - a_2b_2$

τ_3: $(a_1 - a_2)(b_2 - b_1) + (a_2 - a_3)(b_3 - b_2) - a_1b_1$

Figure 2. Comparison of Calculation Cost over F_{p^3}



Result of degree 4

Efficient extension field F_{p^4} with Karatsuba-based method is constructed by towering technique such as $F_{(p^2)^2}$.Modular polynomial are $f(x) = x^2 + 1$ and $g(x) = x^2 - (\omega + 1)$, where ω is zero of $f(x)$ .Then, $F_{(p^2)^2}$ is constructed by the basis $\{1, \omega\}\times\{1, \theta\}$, where θ is a zero of $g(x)$.For this construction,p needs to satisfy $p \equiv 3\ (mod\ 8)$.

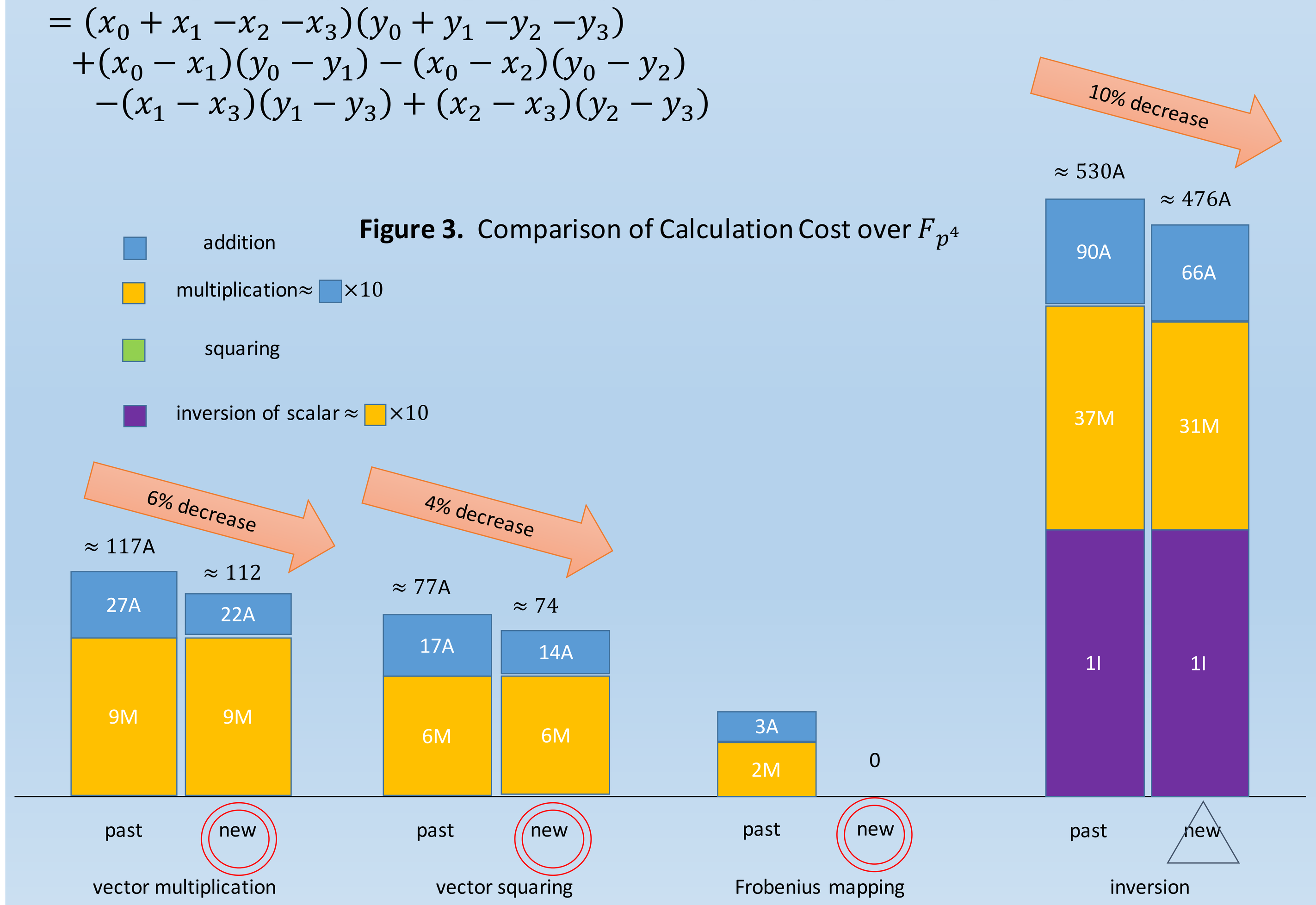
The proposed method uses the basis $\{\omega, \omega^2, \omega^3, \omega^4\}$ defined by modular polynomial $\Phi_5(x) = (x^5 - 1)/(x - 1)$ and its zero $\omega \in F_{p^4}$. In this case, $p \equiv 2,3\ (mod\ 5)$ such that $\Phi_5(x)$ becomes irreducible over F_p. The proposed CVMA-based method provides an efficient calculation as shown in Figure 3.

CVMA based method's multiplication over F_{p^4}

$$
\begin{aligned}
&(x_0\omega + x_1\omega^2 + x_2\omega^3 + x_3\omega^4)(v_0\omega + y_1\omega^2 + y_2\omega^3 + y_3\omega^4) \\
&= (x_2y_2 + x_1y_3 - x_3y_1 - x_0y_3 - x_1y_2 + x_2y_1 - x_3 y_0)\omega \\
&\quad +(x_0y_0 + x_2y_3 - x_3y_2 - x_0y_3 - x_1y_2 + x_2y_1 - x_3 y_0)\omega^2 \\
&\quad +(x_3y_3 + x_0y_1 - x_1y_0 - x_0y_3 - x_1y_2 + x_2y_1 - x_3 y_0)\omega^3 \\
&\quad +(x_1y_1 + x_0y_2 - x_2y_0 - x_0y_3 - x_1y_2 + x_2y_1 - x_3 y_0)\omega^4 \\
&= \{U - (x_1 - x_3)(y_1 - y_3) - x_0y_0\}\omega \\
&\quad +\{U - (x_2 - x_3)(y_2 - y_3) - x_1y_1\}\omega^2 \\
&\quad +\{U - (x_0 - x_1)(y_0 - y_1) - x_2y_2\}\omega^3 \\
&\quad +\{U - (x_0 - x_2)(y_0 - y_2) - x_3y_3\}\omega^4
\end{aligned}
$$

$$
\begin{aligned}
&U \\
&= (x_0 - x_3)(y_0 - y_3) + (x_1 - x_2)(y_1 - y_2) \\
&= (x_0 + x_1 - x_2 - x_3)(y_0 + y_1 - y_2 - y_3)\{(x_0 - x_3)(y_1 - y_2) + (x_1 - x_2)(y_0 - y_3)\} \\
&= (x_0 + x_1 - x_2 - x_3)(y_0 + y_1 - y_2 - y_3) \\
&\quad +(x_0 - x_1)(y_0 - y_1) - (x_0 - x_2)(y_0 - y_2) \\
&\quad -(x_1 - x_3)(y_1 - y_3) + (x_2 - x_3)(y_2 - y_3)
\end{aligned}
$$

Figure 3. Comparison of Calculation Cost over F_{p^4}



Conclusions

Most of CVMA-based arithmetic are 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.

Table 1. Comparison of calculation costs

Operation	Karatsuba-based	CVMA-based
Comparison over F_{p^3}		
Multiplication	6M+17A	6M+12A
Squaring	2M+3S+11A	2M+3S+11A
Frobenius mapping	2M	0
Inversion	9M+3S+8A+I	9M+3S+10A+I
Comparison over F_{p^4}		
Multiplication	9M+27A	9M+22A
Squaring	6M+17A	6M+14A
Frobenius mapping	2M+3A	0
Inversion	37M+90A+I	31M+66A+I

Literature cited

N. Nekado, Y. Nogami, H. Kato, and Y. Morikawa
"Cyclic vector multiplication algorithm and existence probability of gauss period normal basis"
IEICE Trans. Fundamentals, vol.E94-A, no.1, pp. 172-179, 2011

Y. Sakemi, H. Kato, Y.Nogami, and Y.Morikawa
"An improvement of twiste ate pairing with barreto-naehring curve by using frobenius mapping"
Convergence and Hybrid Information Technologies, Intech, pp. 335-342,2005

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