A Note on Point Multiplication on Supersingular Elliptic Curves over Ternary Fields

Kwang Ho Kim

Department of Algebra, Institute of Mathematics,
The State Academy of Sciences, D. P. R. of Korea
kimkhhj1980@yahoo.com.cn

Abstract: Recently, the supersingular elliptic curves over ternary fields are widely used in pairing based crypto-applications since they achieve the best possible ratio between security level and space requirement. We propose new algorithms for projective arithmetic on the curves, where the point tripling is field multiplication free, and point addition and point doubling requires one field multiplication less than the known best algorithms, respectively. The algorithms combined with DBNS can lead to apparently speed up scalar multiplications on the curves.

Keywords: supersingular elliptic curve, point addition, point doubling, point tripling, point multiplication, ternary field.

1. Introduction

For elliptic curve based cryptosystems, point multiplication(or scalar multiplication) on the curve is the most important but time-consuming operation. So the research on speeding up the operation continues to get increasing attraction since the origin of ECC.

The point multiplication is performed by curve arithmetic operations such as point addition, doubling and tripling which in turn are performed by field arithmetic operations such as addition, subtraction, multiplication, inversion and cubing in the field. Thus, it is important to decrease the number of field operations needed for the arithmetic on the curves.

A field inversion is much more costly than any other field operation. In affine coordinates, while tripling on the curves is field multiplication free as well field inversion free so that it is very fast, but point addition and doubling require the costly field inversions. But, when using projective coordinates we can eliminate all the costly field inversions in point multiplication, except for a few (usually one or two) needed to return to affine coordinates at the end of computation, asking for more field multiplications.

Thus, algorithms for projective arithmetic on elliptic curves have been proposed in many literatures(see e.g. [2], [3], [5], [12], [14], [15], [16], [17], [18], [25]), especially for characteristic 3 in [16] by N. Koblitz, in [5] by P. Barreto et al. and in [12] by K. Harrison et al..

N. Koblitz[16] has employed the ordinary projective coordinates, on which the point tripling is field multiplication free as is in affine coordinates. In the same coordinates, P. Barreto et al.[5] have proposed new point addition algorithm which requires 9 field multiplications that is one less than required for the algorithm by N. Koblitz. On the other hand, in [12] K. Harrison et al. have proposed algorithms for the curve arithmetic in Jacobian projective coordinates, where they also have proposed an algorithm for point doubling. The point addition algorithm proposed by K. Harrison et al. requires 8 field multiplications and so it is more efficient than P. Barreto et al.'s. But, for point tripling which is more important than point addition(in practice of scalar multiplication), K. Harrison et al.'s algorithm requires one field multiplication and thus the scalar multiplication based on their algorithms results in inefficient compared with one based on P. Barreto et al.'s algorithms.

This paper is organized as follows. Basic concepts and previous work on arithmetic on supersingular elliptic curves over ternary fields are summarized in section 2. In section 3, new algorithms are proposed, using the type of projective coordinates which was proposed in [15] by the first author et al. to give efficient algorithms on non-supersingular elliptic curves over the fields. In section 4, the performance of scalar multiplication using proposed algorithms is briefly discussed.

2. Curve Arithmetic

In this paper we consider following supersingular elliptic curves:

$$E(F_{3^m}):\ y^2 = x^3 - x + b\ (b = \pm 1)\ \ , \tag{1}$$

which recently are most attracting for efficient implementation of pairing-based cryptosystems (see e. g. [4], [5], [6], [9], [11], [12], [13],[20], [21], [22], [23]).

In affine coordinates (x, y), arithmetic operations on the curves can be performed by below formulae. [5]

-Point tripling: $(x_3, y_3) = [3](x, y)$

$$x_3 = x^9 - b,\ \ y_3 = -y^9 \tag{2}$$

- Point doubling: $(x_3, y_3) = [2](x, y)$:

$$x_3 = x + \lambda^2,\ \ y_3 = -(y + \lambda^3),\ \ \lambda = 1/y \tag{3}$$

- Point addition: $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$

$$x_3 = \lambda^2 - (x_1 + x_2),\ \ y_3 = (y_1 + y_2) - \lambda^3,\ \ \lambda = (y_1 - y_2)/(x_1 - x_2) \qquad (4)$$

Let us denote the costs of an inversion, a multiplication, a squaring, a cubing in the field as $1I$, $1M$, $1S$ and $1C$, respectively. According to [1], it holds that when using the polynomial base representation of the field, $1I \geq 7M$, $1M \geq 10C$ and if we use the normal base representation, $1I \geq 15M$, $1M \geq 300C$, independently on compilers used, in all practical sizes of the base field. The costs of a field addition and subtraction are much cheaper than $1C$ (see [1]) and so it will be ignored in the cost evaluations of this paper.

In order to avoid the costly inversions in (3) and (4), projective versions of (3)-(5) were proposed in [16], [5] and [12], separately.

There are many types of projective coordinates, including followings:

1. $Ordinary\ projective\ (X, Y, Z) \leftrightarrow Affine\ (x, y) = (X/Z, Y/Z)$ (5)

2. $Lopez - Dahab\ projective\,(X, Y, Z) \leftrightarrow Affine\ (x, y) = (X/Z, Y/Z^2)$ (6)

3. $Jacobian\ projective\,(X, Y, Z) \leftrightarrow affine\ (x, y) = (X/Z^2, Y/Z^3)$ (7)

4 $ML - projective\,(X, Y, Z, T)\ where\, T = Z^2 \leftrightarrow affine\ (x, y) = (X/T, Y/Z^3)$ (8)

For example, in ordinary projective coordinates, the curve equation (1) can be expressed as:

$$Y^2Z = X^3 - XZ^2 + bZ^3\,(b = \pm 1) \qquad (9)$$

Then point tripling $(X_3, Y_3, Z_3) = [3](X, Y, Z)$ on the curve (12) can be performed by:

$$Z_3 = Z^9, X_3 = X^9 - bZ_3, Y_3 = -Y^9 \qquad (10)$$

, consuming $6C$.(see [16])

For point addition, the mixed case where one point is affine and the other point is in projective representation is the most important in practice. So, in this paper we will restrict our consideration on point addition to the case.

Point addition $(X_3, Y_3, Z_3) = (X_1, Y_1, 1) + (X_2, Y_2, Z_2)$ on the curve (12) in ordinary projective coordinates can be obtained by:(see [5])

$$Z_3 = Z_2(X_1Z_2 - X_2)^3$$

$$X_3 = X_2(X_1Z_2 - X_2)^3 - (X_1Z_2 - X_2)[(X_1Z_2 - X_2)^3 - Z_2(Y_1Z_2 - Y_2)^2] \qquad (11)$$

$$Y_3 = (Y_1Z_2 - Y_2)[(X_1Z_2 - X_2)^3 - Z_2(Y_1Z_2 - Y_2)^2] - Y_2(X_1Z_2 - X_2)\,.$$

The formula requires $9M + 1C$ which is $1M$ less than the cost of N. Koblitz's formula[16].

On the other hand, K. Harrison et al. have proposed point tripling, addition and doubling algorithms which require $1M + 6C$, $8M + 3C$ and $7M + 2C$ respectively, in Jacobian projective coordinates.(see [12]) Although point addition is nearly by $1M$ more effective than (11), but the point tripling which is more frequent in the procedure of point multiplication is more expensive by $1M$ than (10). So, scalar multiplication based on their algorithms results in inefficient compared with one based on P. Barreto et al.'s algorithms.

3. New Algorithms

We use ML- projective coordinates (8), which is a slightly modified version of Jacobian projective coordinates and has been used to obtain efficient algorithms for non-supersingular elliptic curves over ternary fields, in [15]. In the coordinates, projective equation of the curve (1) can be expressed by:

$$Y^2 = X^3 - XT^2 + bT^3 \, (b = \pm 1) . \qquad (12)$$

[Theorem 1] In ML-projective coordinates, there exist algorithms that give the a point tripling, a point doubling and a point addition on the curve at the costs $8C$, $6M + 4C$ and $7M + 3C$, respectively.

Proof. Let us denote the affine points corresponding to projective points (X, Y, Z, T) , (X_i, Y_i, Z_i, T_i) $(i = 1,2,3)$ as (x, y) , (x_i, y_i) $(i = 1,2,3)$, respectively.

- The point tripling $(X_3, Y_3, Z_3, T_3) = [3](X, Y, Z, T)$ can be obtained by:

$$X_3 = (X - bT)^9, \;\; Y_3 = -Y^9, \;\; Z_3 = Z^9, \;\; T_3 = T^9 . \qquad (13)$$

In fact, from (13), it follows that $x_3 = (X - bZ^2)^9 / Z^{18} = (x - b)^9 = x^9 - b$ and

$y_3 = -Y^9 / Z^{27} = -y^9$, which satisfy (2). Moreover, $T_3 = (Z^2)^9 = Z_3{}^2$.

- The point doubling $(X_3, Y_3, Z_3, T_3) = [2](X, Y, Z, T)$ can be obtained by:

$$\begin{aligned} &Z_3 = -Y_1 Z_1{}^3, \;\; T_3 = Z_3{}^2 , \\ &X_3 = (T^3)^2 + (X^3 - Y^2)Y^2 + bT_3 , \qquad (14) \\ &Y_3 = (T^3)^3 + Y^2 T_3 . \end{aligned}$$

In fact, from (14) and the curve equation (12), it follows that

$$x_3 = [Z^{12} + (X^3 - Y^2)Y^2 + bY^2Z^6]/Y^2Z^6$$

$$= [Z^{12} + (X^3 - Y^2 + bZ^6)Y^2]/Y^2Z^6$$
$$= (Z^{12} + XZ^4Y^2)/Y^2Z^6 = (1/y)^2 + x\,,$$

$y_3 = -(Z^{18} + Y^4Z^6)/Y^3Z^9 = -[(1/y)^3 + y]$, which satisfy (4).

- The point addition $(X_3, Y_3, Z_3, T_3) = (X_1, Y_1, 1, 1) + (X_2, Y_2, Z_2, T_2)$ $(Z_1 = 1)$ can be obtained by: $Z_3 = Z_2(X_1T_2 - X_2)$, $T_3 = {Z_3}^2$,

$$X_3 = (Y_1{Z_2}^3 - Y_2)^2 + (X_1T_2 - X_2)^3 + X_1T_3\,, \tag{15}$$

$$Y_3 = (Y_1{Z_2}^3 + Y_2)(X_1T_2 - X_2)^3 - (Y_1{Z_2}^3 - Y_2)^3\ .$$

In fact, from (15) it follows that

$$x_3 = [(Y_1{Z_2}^3 - Y_2)^2 + (X_1T_2 - X_2)^3 + X_1T_3]/T_3$$

$$= [(Y_1{Z_2}^3 - Y_2)^2 + (X_1{Z_2}^2 - X_2)^3]/[{Z_2}^2(X_1{Z_2}^2 - X_2)^2] + x_1$$

$$= [(y_1 - y_2)/(x_1 - x_2)]^2 - (x_1 + x_2)\,,$$

$$y_3 = [(Y_1{Z_2}^3 + Y_2)(X_1{Z_2}^2 - X_2)^3 - (Y_1{Z_2}^3 - Y_2)^3]/[{Z_2}^3(X_1{Z_2}^2 - X_2)^3]$$

$= (y_1 + y_2) - [(y_1 - y_2)/(x_1 - x_2)]^3$, which satisfy (5).

It is clear that the costs of (13), (14), (15) are $8C$, $6M + 4C$ and $7M + 3C$, respectively. The theorem was proven. ∎

Algorithm	Coordinates	Tripling	Addition	Doubling
Classic	Affine	$4C$	$1I + 2M + 1C$	$1I + 1M + 1C$
N. Koblitz[16]	Ordinary projective	$6C$	$10M + 1C$	
P. Barreto et al.[5]	Ordinary projective	$6C$	$9M + 1C$	
K. Harrison et al.[12]	Jacobian Projective	$1M + 6C$	$8M + 3C$	$7M + 2C$
Proposed	ML-projective	$8C$	$7M + 3C$	$6M + 4C$

Table 1. Comparing costs for arithmetic operations on supersinguar curves over ternary fields

4. Point multiplication

In [10], M. Ciet et al. showed that use of the double base number system(DBNS) results in sublinear algorithm for scalar multiplication on supersingualr elliptic curves over ternary fields, using the fact that a point tripling is performed in a negligible fraction of the time costs of an addition and doubling.

So our algorithms combined with DBNS lead to very efficient scalar multiplications on supersingular elliptic curves over ternary and binary fields, because besides the efficient tripling comparable with the affine case, the point addition and doubling does not require field inversions and so is much faster compared with the affine case. The detailed discussion on the implementation of scalar multiplication is abbreviated.

5. References

[1] O. Ahmadi, D. Hankerson and A. Menezes. Software implementation of arithmetic in F_{3^m}. WAIFI 2007. to appear.

[2] E. Al-Daoud, R. Mahmed, M. Rushdan and A. Kilioman. A new addition formula for elliptic curves over $GF(2^n)$. IEEE Trans. on Comp., 51, 972-975, 2002.

[3] M. Barbosa, A. Moss and D. Page. Compiler assisted elliptic curve cryptography. Technical Report 2007/053, Cryptology ePrint Archive, 2007.

[4] P. S. L. M. Barereto, S. Galbraith, C. hEigeartaigh and M. Scott. Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography, 42, 239-271, 2007.

[5] P. S .L. M. Baretto, H. Y. Kim, B. Lynn and M. Scott. Efficient algorithms for pairing-based cryptosystems. CRYPTO'2002, LNCS 2442. 354-368, 2002.

[6]] P. S .L. M. Baretto, B. Lynn and M. Scott. Efficient implementation of pairing-based cryptosystems. J. Cryptology, 17(4), 17-25, 2004.

[7] I. F. Blake, G. Seroussi and N. P. Smart. "Advances in Elliptic Curve Cryptography". LMLNS 317, Cambridge Univ. Press, 2005.

[8] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. SIAM J. on Computing, 32, 586-615, 2003.

[9] X. Boyen and L. Martin. Identity-based cryptography standard(IBCS) #1: Supersingular curve implementation of the BF and BB1 cryptosystems. IETF Internet Draft, December 2006.

[10] M. Ciet and F. Sica. An analysis of double base number systems and a sublinear scalar

multiplication algorithm. Proceedings of Mycrypt2005, LNCS 3715, 171-182, 2005.

[11] R. Granger, D. Page and M. Stam. Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three. IEEE Trans. on Comp., 54, 852-860, 2005.

[12] K. Harrison, D. Page and N. P. Smart. Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems. LMS J. Comput. Math., 5, 181-193, 2002.

[13] T. Kerins, W. Marmane, E. Popovici and P. S. L. M. Barreto. Efficient Hardware for the Tate pairing calculation in characteristic three. CHES 2005, LNCS 3659, 412-426, 2005.

[14] K. H. Kim, S. I. Kim. A new method for speeding up arithmetic on elliptic curves over binary fields. Technical Report 2007/181, Cryptology ePrint Archive, 2007.

[15] K. H. Kim, S. I. Kim and J. S. Choe. New fast algorithms for arithmetic on elliptic curves over finite fields of characteristic three. Technical Report 2007/179, Cryptology ePrint Archive, 2007.

[16] N. Koblitz. An elliptic curve implementation of the finite field digital signature algorithm. CRYPTO'98, LNCS 1462, 327-337, 1998.

[17] J. Lopez and R. Dahab. Improved Algorithms for elliptic curve arithmetic in $GF(2^n)$, SAC'98, 201-212, 1998.

[18] C. Negre. Scalar multiplication on elliptic curves defined over fields of small odd characteristic. INDOCRYPT 2005, LNCS 3797, 389-402, 2006.

[19] D. Page and N. P. Smart. Hardware implementation of finite fields of characteristic three. CHES 2002, LNCS 2523, 529-539, 2003.

[20] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Technical Report 2003/054, Cryptology ePrint Archive, 2003.

[21] M. Scott. Computing the Tate pairing. CT-RSA 2005, LNCS 3376, 293-304, 2005.

[22] M. Scott. Implementing cryptographic pairings. Preprint, 2006.

[23] M. Scott, N. Costigan and W. Abdulwahab. Implementing cryptographic pairings on smartcards. CHES 2006, LNCS 4249, 134-147, 2006.

[24] N. P. Smart. The Hessian form of an elliptic curve. CHES 2002, LNCS 2162, 118-125, 2002.

[25] N. P. Smart and E. J. Westwood. Point multiplication on ordinary elliptic curves over fields of characteristic three. AAECC, 13, 485-497, 2003.