Regular Ternary Algorithm for Scalar Multiplication on Elliptic Curves over Finite Fields of Characteristic Three

Chol-Sun Sin

Institute of Mathematics, State Academy of Sciences, DPR Korea

Abstract: In this paper we propose an efficient and regular ternary algorithm for scalar multiplication on elliptic curves over finite fields of characteristic three. This method is based on full signed ternary expansion of a scalar to be multiplied. The cost per bit of this algorithm is lower than that of all previous ones.

Keywords: elliptic curve, scalar multiplication, full signed expansion, SCA.

1 Introduction

Elliptic curve cryptosystems, proposed independently by Neal Koblitz [14] and Victor Miller [15] are more and more widespread in everyday-life applications. The core operation of elliptic curve cryptosystems is the scalar multiplication on elliptic curves. There are numerous investigations of fast and regular scalar multiplication on elliptic curves over large prime field or binary field.(See [1], [2] and [5])

Note that elliptic curves in characteristic three could be applied in cryptographic schemes. For example, Koblitz announced an implementation of the digital signature algorithm on special supersingular elliptic curves in characteristic three with great efficiency [12] and Boneh-Franklin used such curves in pairing-based cryptosystems [11].

Recently, the improved formulae for arithmetic on Weierstrass and Hessian forms with a point of order 3 over finite fields of characteristic three are given in [4, 7, 8, 10]. The new doubling , mixed addition and tripling formulae require 3M+2C, 8M+1C+1D and 4M+4C+1D, respectively, where M, C and D is the cost of a field multiplication, a cubing and a multiplication by a constant.

The goal of the present work is to make a fast and regular algorithm for scalar multiplication on elliptic curves in characteristic three by using an efficient ternary expansion of scalar.

The remainder of this paper is organized as follows. In section 2 we recall the necessary background for arithmetic on elliptic curves over finite fields of characteristic three. In section 3 we propose the fast and regular algorithm for scalar multiplication on elliptic curves over finite fields of characteristic three. Section 4 gives some comparison for scalar multiplication and in section 5 we give some conclusions.

2 Preliminaries

2.1 Ordinary elliptic curves over $\mathbf{F}_{3^m}$

Elliptic curves over any field can be broken down into two classes of ordinary and supersingular elliptic curves. Every ordinary elliptic curve over $\mathbf{F}_{3^m}$ with a point of order 3 can be written in the Weierstrass form

$$E_b : y^2 = x^3 + x^2 + b \quad \text{with} \quad b \neq 0,$$

or equivalently the Hessian form

$$E_d : x^3 + y^3 + 1 = dxy \quad \text{with} \quad d \neq 0.$$

The Weierstrass Form: In 2012, Farashahi et al. [4] presented a new explicit formulae for point doubling, tripling and addition with a cost of 3M+2C, 8M+1C+1D and 4M+4C+1D, respectively, using projective coordinate system(it is called scaled projective system) such as

$$\left(\frac{X}{aT}, \frac{Y}{aT} \right) \leftrightarrow (X, Y, T),$$

where $T = Z/a, \quad a = (-1/b)^{3^{m-1}}$. Using the scaled projective system, the Weierstrass curve can easily pass to the following

$$E_{-1/a^3} : Y^2 Z = X^3 + X^2 Z - Z^3/a^3 \quad \text{with} \quad a \in F_{3^m}.$$

Scaled Projective Point Doubling: $[2](X_1, Y_1, T_1) = (X_2, Y_2, T_2)$ where

$$\begin{gathered} A = X_1 + Y_1,\ B = X_1 - Y_1,\ D = (T_1 - A)^3, \\ E = (B - T_1)^3,\ F = B \cdot D,\ G = A \cdot E,\ H = T_1 \cdot (D + E), \\ X_2 = F + G,\ Y_2 = F - G,\ T_2 = H. \end{gathered}$$

Scaled Projective Point Addition: $(X_1, Y_1, T_1) + (X_2, Y_2, T_2) = (X_3, Y_3, T_3)$ where

$$\begin{aligned} & A_1 = X_1 + Y_1,\ B_1 = X_1 - Y_1, A_2 = X_2 + Y_2,\ B_2 = X_2 - Y_2, \\ & D = B_1 \cdot T_2,\ E = A_2 \cdot T_1,\ F = A_1 \cdot T_2,\ G = B_2 \cdot T_1, \\ & H = D \cdot E, I = F \cdot G,\ J = F \cdot I,\ K = E \cdot H, \\ & X_3 = D \cdot H + J - G \cdot I - K,\ Y_3 = X_3 + F \cdot I + E \cdot H,\ T_3 = (1/a)(D + F - E - G)^3. \end{aligned}$$

The cost of the mixed scaled addition formulae is 8M+1C+1D, by setting $T_1 = 1$.

Scaled Projective Point Tripling: $[3](X_1, Y_1, T_1) = (X_3, Y_3, T_3)$ where

$$\begin{gathered} A = X_1 - T_1,\ B = (A + Y_1)(A - Y_1),\ D = A \cdot (B + T_1 \cdot A), \\ X_3 = D^3,\ Y_3 = (Y_1 \cdot B)^3,\ T_3 = -(1/a) \cdot A^9. \end{gathered}$$

The Hessian Form: With a substitution $x = X/Z,\ y = Y/Z$, the equation of Hessian curve can be expressed as

$$X^3 + Y^3 + Z^3 = dXYZ.$$

A mixed addition, doubling and tripling formulae presented in [4] and [10] require 8M+1C+1D, 3M+2C and 4M+4C+1D, respectively.

Mixed Addition: $(X_1, Y_1, 1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)$ where

$$C = X_1 \cdot Z_2,\ D = Y_1 \cdot Z_2,\ E = X_2 \cdot D,\ F = Y_2 \cdot C,$$
$$X_3 = D \cdot E - Y_2 \cdot F,\ Y_3 = C \cdot F - X_2 \cdot E,\ Z_3 = (1/d)(X_2 + Y_2 - C - D)^3.$$

Point Doubling: $[2](X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$ where

$$X_2 = Y_1 \cdot (Z_1 - X_1)^3,\ Y_2 = X_1 \cdot (Y_1 - Z_1)^3,\ Z_2 = Z_1 \cdot (X_1 - Y_1)^3.$$

Point Tripling: $[3](X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$ where

$$A = X_1 + Y_1 + Z_1,\ B = (X_1 - Z_1)(Y_1 - Z_1),\ D = A \cdot (B - Z_1 \cdot A),\ E = Y_1 \cdot B,$$
$$X_3 = (D + E)^3,\ Y_3 = (D - E)^3,\ Z_3 = -(1/a) \cdot A^9.$$

2.2 Scalar multiplication

In order to withstand Side Channel Analysis(SCA), one must render the scalar multiplication regular, namely such that it performs a constant operation flow whatever the scalar value.[16-21] There are some algorithms such as the Montgomery ladder and the double-and-add algorithm proposed by Joye in [7]. These algorithms are based on an invariant loop invariants the point registers R_0 and R_1. In the Montgomery ladder, the relation $R_1 - R_0 = P$ is satisfied at the and of every loop iteration, while in Joye algorithm the i th loop iteration yields $R_0 + R_1 = [2^i]P$.

Algorithm 1 (Montgomery ladder)

Input: $P \in E(F_q),\ k = (k_{n-1}, \ldots, k_1, k_0)_2 \in N$

Output: $Q = [k]P$

```
1. $R_0 \leftarrow O; R_1 \leftarrow P$
2. $For\ i = n-1\ downto\ 0\ do$
3.     $b \leftarrow k_i; R_{1-b} \leftarrow R_{1-b} + R_b$
4.     $R_b \leftarrow 2R_b$
5. $end\ for$
6. Return $R_0$
```

Algorithm 2 (Joye double-and-add)

Input: $P \in E(F_q),\ k = (k_{n-1}, \ldots, k_1, k_0)_2 \in N$

Output: $Q = [k]P$

```
1. $R_0 \leftarrow O; R_1 \leftarrow P$
2. $For\ i = n-1\ downto\ 0\ do$
3.     $b \leftarrow k_i$
4.     $R_{1-b} \leftarrow 2R_{1-b} + R_b$
5. $end\ for$
6. Return $R_0$
```

The Montgomery ladder was initially proposed as a scalar multiplication algorithm for a specific kind of elliptic curves with very efficient point arithmetic.

In general, ternary algorithms are faster than binary ones in finite fields of characteristic three, but it is less secure against SCA.

3 Regular Ternary Algorithm for Scalar Multiplication

3.1 Full signed ternary expansion

Let k be a scalar with ternary expansion $(k_{n-1},\ldots,k_1,k_0)_3$, where $k_i \in \{0,1,2\}$ for every $i < n-1$ and $k_{n-1} \neq 0$. There exists a unique full signed expansion $(k_{n-1},\ldots,k_1,k_0)$ of k such that

$$k = \sum_i k_i 3^i$$

with $k_i \in \{\pm1,\pm2\}$ for $i < n-1$ and $k_{n-1} > 0$. This expansion is obtained from the fact that for every $\omega > 1$, we have

$$1 = 3^{\omega} - \sum_{i=0}^{\omega-1} 2 \cdot 3^i \ .$$

It follows that any group of ω bits $00\ldots1$ in the ternary expansion of k can be replaced by the group of ω signed bits $1\overline{2}\overline{2}\ldots\overline{2}$ (where $\overline{2} = -2$).

For $i\,(0 \le i < n-1)$, the full signed ternary expansion of k is obtained as follows.

$$k_i = \begin{cases} k_i\,, & k_{i+1} \neq 0,\ k_i \neq 0 \\ k_i - 3, & k_{i+1} = 0,\ k_i \neq 0 \\ -2, & k_{i+1} = 0,\ k_i = 0 \\ 1\,, & k_{i+1} \neq 0,\ k_i = 0. \end{cases}$$

3.2 Regular algorithm for scalar multiplication

We perform the scalar multiplication $Q \leftarrow [k]P$ with a left-to-right ternary algorithm by using the full signed representation of k, namely we iterate $Q \leftarrow [3]Q + [k_i]P$. In every iteration, we use the point operations in [4,10]. Our algorithm is depicted in the next algorithm.

Algorithm 3 (signed ternary)

Input: $P \in E(F_q),\ k = (k_{n-1},\ldots,k_1,k_0) \in N$

Output: $Q = [k]P$

```
1. $R_1 \leftarrow O; R_2 \leftarrow [2]P$
2. $l \leftarrow k_{n-1}; Q \leftarrow R_l$
3. $For\ i = n-2\ downto\ 0\ do$
4.     $Qb \leftarrow [3]Q$
5.     $b \leftarrow sign(k_i); l = |k_i|$
6.     $Q \leftarrow Q + (-1)^b R_l$
7. $end\ for$
8. Return $Q$
```

Algorithm 3 involves $n-1$ tripling and add operation, and the initial doubling point.

Table 1. Cost of algorithm 3 on ordinary curves

Form	Cost per bit	Additional cost	#Field registers
Weierstrass	8M+3.3C+1.3D	1I+3M	8/9
Hessian	8M+3.3C+1.3D	1I+5M+2C	8/9

As known above, the algorithm 3 is fast and regular low-memory ternary algorithm for scalar multiplication on ordinary curves over finite fields of characteristic three.

We now look at the context where more memory is available. In that case one can use following window techniques for scalar multiplication.

Let k be a scalar with full signed ternary expansion $(k_{n-1},\ldots k_1,k_0)$, where $k_i \in \{\pm 1, \pm 2\}$ for every $i < n-1$ and $k_{n-1} > 0$.

We can replace the signed ternary expansion of k by the following signed 3^{ω}-radix expansion by the group of ω

$$k = (K_{t-1},\ldots,K_1,K_0)$$

such that

$$K_i = \sum_{j=0}^{\omega-1} k_{i\cdot\omega+j} 3^j,$$

where ω is window size , $t = \lceil n/\omega \rceil$ and $K_i \neq 0$.

In the above representation, the digits K_i lie in a basis B which is different from the simple 3^{ω} - radix basis $\{1,\ldots,3^{\omega}-1\}$ and includes negative integers.

The use of the above signed window expansion yields the following algorithm, where B^+ denotes the set $\{|d| : d \in B\}$.

Algorithm 4 (signed window ternary)

```
Input: $P \in E(F_q),\ k = (K_{t-1},\ldots,K_1,K_0) \in N$
Output: $Q = [k]P$
1. for all $d \in B^+$ do $R_d \leftarrow [d]P$
2. $l \leftarrow K_{t-1}; Q \leftarrow R_l$
3. For $i = t-2$ downto $0$ do
4.     $Q \leftarrow [3^{\omega}]Q$
5.     $b \leftarrow sign(K_i); l = |K_i|$
6.     $Q \leftarrow Q + (-1)^b R_l$
7. end for
8. return $Q$
```

The signed window ternary algorithm with $\omega > 1$ involves less point additions than general ternary versions, while it requires more memories as it requires $m = \# B^+$ point registers and precomputation $[d]P$ for all $d \in B^+$. This precomputation is similar to the schemes presented in [9], hence it requires only one field inverse operation.

4 Comparison

In this section we compare the performances of different scalar multiplication for ordinary curves over finite fields of characteristic three.

In particular, we consider the previous regular binary algorithms including the Montgomery ladder and double-and-add algorithm.

For every algorithm, we give the cost per bit, additional cost and number of required field registers.

The result of comparison is summarized in the table 2.

Table 2. Cost of regular scalar multiplication algorithms for Weierstrass (Hessian) form

Method	Cost per scalar bit	Additional cost	#field reg.
Montgomery ladder	11M+3C+1D		8/9
Joye’s double-add	11M+3C+1D		8/9
Signed ternary	8M+3.3C+1.3D	1I+3M(1I+5M+2C)	8/9
Signed window ternary($\omega = 2$)	5.3M+3C+1D	1I+61M+8C+6D	22/23

5 Conclusion

In this paper we presented a regular scalar multiplication based on a full signed ternary expansion of scalar on ordinary curves over $\mathbf{F}_{3^m}$. The cost of the algorithm is 8M+3.3C+1.3D per bit and only 2 registers are needed for points.

This method is more efficient than all the previous regular algorithms for ordinary elliptic curves over $\mathbf{F}_{3^m}$, which can be also used for supersingular elliptic curves over $\mathbf{F}_{3^m}$.

References

[1] I. F. Blake, G. Seroussi, and N. P. Smart. Advance in elliptic curve cryptography. Cambridge University Press, 2005.

[2] D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to elliptic curve cryptography. Springer-Verlag,2003.

[3] I. F. Blake, G. Seroussi, and N. P. Smart. Elliptic curves in cryptography. Vol.265. Cambridge University Press, New York, 1999.

[4] R. R. Farashahi, H. Wu, and C. Zhao. Efficient arithmetic on elliptic curves over fields of characteristic three. Cryptology ePrint Archive, Report 2012/122, 2012.

[5] M. Rivain. Fast and regular algorithms for scalar multiplication over elliptic curves. Cryptology ePrint Archive, Report 2011/338, 2011.

[6] H. Wu, C. Zhao. Faster scalar multiplication on ordinary Weierstrass elliptic curves over fields of characteristic three. Cryptology ePrint Archive, Report 2011/468, 2011.

[7] R. R. Goundar, M. Joye, and A. Miyaji. Co-z addition formulae and binary ladders on elliptic curves. Cryptology ePrint Archive, Report 2010/309, 2010.

[8] R. M. Avanzi, C. Heuberger, and H. Prodinger. Arithmetic of supersingular Kobliz curves in characteristic three. Cryptology ePrint Archive, Report 2010/436, 2010.

[9] P. Longa, A. Miri. New composite operations and precomputation scheme for elliptic curve cryptosystems over prime fields. Public Key Cryptography,11th International Workshop-PKC’2008, Springer, LNCS 4939, 229-247, 2008.

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

[11] D. Boneh and M. Franklin. Identity-based encryption form the Weil pairing. In Advances in Cryptology-CRYPTO 2001, Springer, LNCS 2139, 213-229,2001.

[12] N. Koblitz. An elliptic curve implementation of the finite field digital signature algorithm. In Advances in Cryptology-CRYPTO’ 98, Springer, LNCS 1462, 327-337,1998.

[13] N. P. Smart. The Hessian form of an elliptic curve. In Cryptographic Hardware and Embedded Systems-CHES 2002, Springer, LNCS 2162, 118-125, 2001.

[14] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48, 203-209, 1987.

[15] V. S. Miller. Uses of elliptic curves in cryptography, In Advances in Cryptology-CRYPTO ‘85, Springer, LNCS 218, 417-426,1986.

[16] A. Chilikov and O. Taraskin. New fault attack on elliptic curve scalar multiplication. Cryptology ePrint Archive, Report 2009/528, 2009.

[17] M. K. Lee. SPA-resistant simultaneous scalar multiplication. Computational Science and Its Applications-ICCSA 2005, Springer, LNCS 3481, 463-512,2005.

[18] T. Akishita and T. Takagi. Zero- Value point attacks on elliptic curve cryptosystem. Information Security 6th Infernational Conference-ISC 2003, Springer, LNCS 2851, 218-233, 2003.

[19] E. Brier and M. Joye. Weierstrass elliptic curves and side-channel attacks. Public Key Cryptography-PKC 2002, Springer, LNCS 2274, 335-345, 2002.

[20] M. Joye and J. J. Quisquater. Hessian elliptic curves and side-channel attacks. In Cryptographic Hardware and Embedded Systems-CHES 2001, Springer, LNCS 2162, 402-410, 2001.

[21] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. Advances in Cryptography 19th Annual International Cryptography Conference-CRYPTO’99， Springer, LNCS 1666, 388-397,1999.