A fast addition algorithm for elliptic curve arithmetic in $GF(2^n)$ using projective coordinates

Akira Higuchi and Naofumi Takagi

Department of Information Engineering, Nagoya University

Nagoya 464-8603, Japan

email: ntakagi@nuie.nagoya-u.ac.jp

Abstract

A new fast addition algorithm on an elliptic curve over $GF(2^n)$ using the projective coordinates with $x = X/Z$ and $y = Y/Z^2$ is proposed.

Keywords:

Algorithms; arithmetic; cryptography; elliptic curve

1 Introduction

Elliptic curve public-key cryptosystems over finite field $GF(2^n)$ [1, 2] have been coming into wide use. It is known that these cryptosystems with $n = 160$ have equivalent security to RSA cryptosystem with a 1024-bit modulus.

In elliptic curve cryptosystems, scalar multiplication mP, for P a point on the elliptic curve and m an integer, is the core operation. The scalar multiplication is performed by iterative additions and doublings on the elliptic curve. Therefore, performing addition and doubling on an elliptic curve fast is crucial for efficient implementation of these cryptosystems.

The addition and doubling on an elliptic curve are performed by field operations, i.e., additions, multiplications, squarings, and inversions in $GF(2^n)$. Among these field operations, inversion is relatively costly. It is reported that for normal basis representation, the cost ratio of inversion to multiplication is at least 7 for $n > 128$ [3]. Then, the use of projective coordinates is effective [1, 2, 4]. Using projective coordinates, we can remove inversions from the elliptic addition and doubling at the cost of increase in the other simpler operations, but need only one inversion at the end of the scalar multiplication for the coordinate transformation back into the affine coordinates. Note that field addi-

tion is very easy and that squaring can be performed by a cyclic shift in normal basis representation.

IEEE P1363 [2] has shown algorithms for the elliptic addition and doubling using the projective coordinates with $x = X/Z^2$ and $y = Y/Z^3$, which require less multiplications than those using the traditional projective coordinates with $x = X/Z$ and $y = Y/Z$ [1]. Lopez and Dahab [4] proposed algorithms using the projective coordinates with $x = X/Z$ and $y = Y/Z^2$, which require less multiplications than those in [2].

In this letter, we propose an elliptic addition algorithm using the same projective coordinates as [4], which requires one less multiplications than [4]. We can use the doubling algorithm in [4], since the same projective coordinates are used.

2 Elliptic curves over $GF(2^n)$

A non-supersingular elliptic curve E over $GF(2^n)$ is defined to be the set of solutions $(x, y) \in GF(2^n) \times GF(2^n)$ to the equation

$$y^2 + xy = x^3 + ax^2 + b \tag{1}$$

where a and $b \in GF(2^n)$, $b \neq 0$, together with the point at infinity denoted by O. E forms a commutative finite group, with O as the group identity, under the addition operation shown below. Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be points of E $(P \neq Q)$. Then, $P + Q = (x_2, y_2)$ is calculated as

$$x_2 = (\frac{y_0 + y_1}{x_0 + x_1})^2 + \frac{y_0 + y_1}{x_0 + x_1} + x_0 + x_1 + a, \tag{2}$$

$$y_2 = \frac{y_0 + y_1}{x_0 + x_1}(x_0 + x_2) + x_2 + y_0. \tag{3}$$

$2P = (x_2, y_2)$ is calculated as

$$x_2 = x_0^2 + \frac{b}{x_0^2},$$

$$y_2 = x_0^2 + (x_0 + \frac{y_0}{x_0})x_2 + x_2.$$

If we perform addition and doubling according to these formulae, each of them requires a field inversion.

3 A new addition algorithm

We use the same projective coordinates as [4], where $x = X/Z$ and $y = Y/Z^2$. Then, the elliptic curve E becomes the set of solutions $(X, Y, Z) \in GF(2^n) \times GF(2^n) \times GF(2^n)$ to the equation $Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4$. Note that the points with $Z = 0$ satisfying this equation, i.e., $(X, 0, 0)$, correspond to the point at infinity, O.

In order to obtain a new addition algorithm, we transform (2) as follows.

$$\begin{aligned} x_2 &= (\frac{y_0 + y_1}{x_0 + x_1})^2 + \frac{y_0 + y_1}{x_0 + x_1} + x_0 + x_1 + a \\ &= \frac{(y_0 + y_1)^2 + (y_0 + y_1)(x_0 + x_1) + (x_0 + x_1)^3 + a(x_0 + x_1)^2}{(x_0 + x_1)^2} \\ &= \frac{y_0^2 + y_1^2 + x_0y_0 + x_0y_1 + x_1y_0 + x_1y_1 + x_0^3 + x_0^2x_1 + x_0x_1^2 + x_1^3 + ax_0^2 + ax_1^2}{(x_0 + x_1)^2} \end{aligned}$$

Since $y_0^2 + x_0y_0 = x_0^3 + ax_0^2 + b$ and $y_1^2 + x_1y_1 = x_1^3 + ax_1^2 + b$ from (1), $y_0^2 + y_1^2 + x_0y_0 + x_1y_1 + x_0^3 + x_1^3 + ax_0^2 + ax_1^2 = 0$. Therefore,

$$x_2 = \frac{x_0y_1 + x_1y_0 + x_0^2x_1 + x_0x_1^2}{(x_0 + x_1)^2} \tag{4}$$

Let $P = (X_0, Y_0, Z_0)$ and $Q = (X_1, Y_1, Z_1)$ be points of E $(P \neq Q)$. Then, $P + Q = (X_2, Y_2, Z_2)$ is calculated as

$$X_2 = X_0Z_1(Y_1Z_0^2 + (X_1Z_0)^2) + X_1Z_0(Y_0Z_1^2 + (X_0Z_1)^2), \tag{5}$$

$$\begin{aligned} Y_2 &= (X_0Z_1(Y_0Z_1^2 + Y_1Z_0^2)(X_0Z_1 + X_1Z_0) + Y_0Z_1^2((X_0Z_1)^2 + (X_1Z_0)^2))((X_0Z_1)^2 + (X_1Z_0)^2) \\ &\quad +((Y_0Z_1^2 + Y_1Z_0^2)(X_0Z_1 + X_1Z_0) + Z_2)X_2, \end{aligned} \tag{6}$$

$$Z_2 = Z_0Z_1((X_0Z_1)^2 + (X_1Z_0)^2). \tag{7}$$

We can derive these formulae as follows. First, we determine (7) so that no inversion is required for the calculations of X_2 and Y_2. Then, we obtain (5) and (6) by substituting $x = X/Z$ and $y = Y/Z^2$ to (4) and (3), and transforming them using (7), respectively. Note that $(X_0Z_1 + X_1Z_0)^2 = (X_0Z_1)^2 + (X_1Z_0)^2$ in $GF(2^n)$.

Therefore, we can perform the addition by the following calculations.

$$\begin{aligned} A_0 &= X_0Z_1 \\ A_1 &= X_1Z_0 \\ B_0 &= A_0^2 \end{aligned}$$

$$
\begin{aligned}
B_1 &= A_1^2 \\
C &= A_0 + A_1 \\
D &= B_0 + B_1 \\
E_0 &= Y_0 Z_1^2 \\
E_1 &= Y_1 Z_0^2 \\
F &= E_0 + E_1 \\
G &= FC \\
Z_2 &= Z_0 Z_1 D \\
X_2 &= A_0(E_1 + B_1) + A_1(E_0 + B_0) \\
Y_2 &= (A_0 G + E_0 D)D + (G + Z_2)X_2
\end{aligned}
$$

The proposed addition algorithm requires 13 multiplications and 4 squarings. When $Z_1 = 1$, it requires 10 multiplications and 3 squarings.

Table 1 shows a comparison of elliptic addition algorithms with respect to the number of required field operations. When one of the two coefficients defining the elliptic curve, a, is 0 or 1, the addition algorithms of [2] and [4] require one less multiplications than in the other cases. The proposed addition algorithm is the fastest when a is not 0 nor 1.

Table 1: The number of field operations for elliptic addition (( ): when $a = 0$ or 1)

algorithm	projective coordinates	$Z_1 \neq 1$		$Z_1 = 1$	
		#mul.	#sqr.	#mul.	#sqr.
IEEE [2]	$X/Z^2, Y/Z^3$	15 (14)	5	10 (9)	4
Lopetz [4]	$X/Z, Y/Z^2$	14 (13)	6	10 (9)	4
proposed	$X/Z, Y/Z^2$	13	4	10	3

Since the same projective coordinates are used, we can use the known fastest doubling algorithm proposed in [4] which requires 5 multiplications (4 when a is 0 or 1) and 5 squarings.

When we use the simple double-and-add method for scalar multiplication, mP, we need $\log_2 m$ doublings and on an average $\frac{1}{2}\log_2 m$ additions. Therefore, when a is not 0 nor 1, using the proposed addition algorithm, we obtain an improvement of about 4.2 %

compared with [4].

4 Conclusion

We have proposed a fast addition algorithm on an elliptic curve over $GF(2^n)$ using the projective coordinates with $x = X/Z$ and $y = Y/Z^2$. It requires one less multiplications than the known fastest algorithm. We can use the known fastest doubling algorithm proposed in [4], since the same projective coordinates are used.

References

[1] A. Menezes: Elliptic curve public key cryptosystems, Kluwer Academic Publishers, 1993.

[2] IEEE P1363, Standard Specifications for Public Key Cryptography, http://grouper.ieee.org/groups/1363/, 1999

[3] J. Guajardo and C. Paar: 'Efficient algorithms for elliptic curve cryptosystems,' Advances in Cryptology, Proc. CRYPT'97, LNCS 1294, Springer-Verlag, pp. 342–356, 1997.

[4] J.Lopez and R.Dahab: 'Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$,' Selected Areas in Cryptography, Proc. SAC'98, LNCS 1556, Springer-Verlag, pp. 201–212, 1998