KMITL Sci. J. Vol. 5 No. 1 Feb. 2005

OVERVIEW OF ADDITION FORMULAS FOR ELLIPTIC CURVES OVER $GF(2^n)$ IN CRYPTOGRAPHY

IQBAL H. JEBRIL, ROSLI SALLEH , and Al-SHAWABKEH M.

Faculty of Computer Science and Information Technology, University of Malaya

ABSTRACT

There are several techniques for projective coordinate that can be used for speeding up the computation kP over $GF(2^n)$. In this paper we overview all this techniques method in projective coordinate and introduce a new efficient formula in projective coordinates. This formula used the idea of reducing the number of underlying field multiplication. Elliptic curve protocols and applications can be implemented with better performance using the suggested formula.

KEY WORDS. Elliptic Curves over $GF(2^n)$, Projective Coordinate, Cryptography.

E-mail: *Iqbal501@yahoo.com*

1-INTRODUCTION AND PRELIMINARIES.

Elliptic curve cryptography (ECC) has received considerable attention from mathematicians around the word ever since the original proposal by Victor Miller and Neal Koblitz in 1985 [1 and 5]. ECC is based on the Discrete Logarithm problem over the points on an elliptic curve.

Elliptic curve public-key cryptosystems over the finite field $GF(2^n)$ [3] have been coming into wide use. It is known that these cryptosystems wide n-160 have equivalent security to the RSA cryptosystem with a 1024-bit modulus.

Elliptic curve cryptosystem, scalar multiplication *mP*, *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 elliptic curve fast is crucial for efficient implementation of these cryptosystems.

Elliptic curves defined over *GF(p)* or $GF(2^n)$ are used in cryptography, the arithmetic of *GF(p)* is the usual mod p arithmetic, the arithmetic of $GF(2^n)$ is similar to that of *GF(p)*, however, there are some differences. Elliptic curves over $GF(2^n)$ are more popular due to the space and time-efficient algorithms for doing arithmetic in $GF(2^n)$. We proceed now to give a quick introduction to the fascinating theory of elliptic curves. For simplicity, we shall restrict our attention to elliptic curves over $GF(2^n)$.

Affine coordinates. Let E be an elliptic curve over $GF(2^n)$ (briefly, E ($GF(2^n)$)), given by the (affine) equation

$$y^2 + xy = x^3 + ax^2 + b,$$

where a and b in $GF(2^n), b \neq 0$.

The set of points on E($GF(2^n)$) also include point *O*, which is the point at infinity and which is the identity element under addition.

There is a rule for adding two points on elliptic curve E($GF(2^n)$)to give a third elliptic curve point. Together with this addition operation, the set of points E($GF(2^n)$) forms a group with *O* serving as its identity. It is this group that is used in the construction of elliptic curve cryptosy-stems.

The addition rule in E($GF(2^n)$), which can be explained geometrically is presented as a sequence of algebraic formulae.

1- $\exists\, O \in$ E($GF(2^n)$), such that $\forall$P $\in$ E($GF(2^n)$), P + *O* = *O* + P = P. (Identity element)

2- $\forall$P $\in$ E($GF(2^n)$), $\exists -$ P $\in$ E($GF(2^n)$), such that, P +(– P)=(– P)+P = *O*. (Inverse)

3- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on E with $P \neq -Q$. Then the

coordinates of $R = P + Q = (x_3, y_3)$ can be computed as follows:

(Point addition) **Formula (1)**	**(Point doubling)** **Formula (2)**
I- If $P_1 \neq P_2$,	II- If $P_1 = P_2$,
$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$,	$x_3 = \lambda^2 + \lambda + a$,
$y_3 = (x_1 + x_3)\lambda + x_3 + y_1$,	$y_3 = (x_1 + x_3)\lambda + x_3 + y_1$
where $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$	where $\lambda = \frac{y_1}{x_1} + x_1$

Thus we see that E($GF(2^n)$) forms an abelian group under addition.

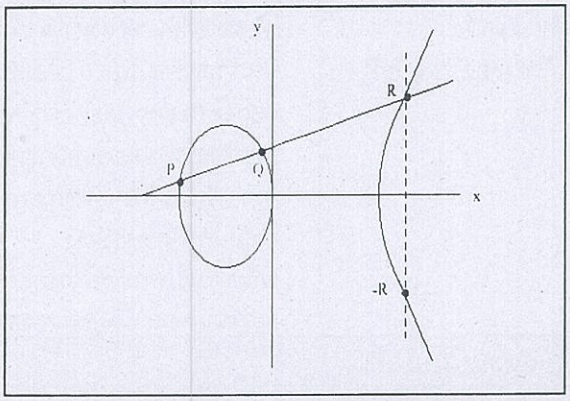

Figure (1): Adding two points on an Elliptic Curve

4-∀P, Q ∈ E($GF(2^n)$), if R = P + Q, then R ∈ E($GF(2^n)$). (Closure)
(see Figure (1))

5- ∀P, Q ∈ E($GF(2^n)$), P + Q = Q + P. (Commutative)

6- P + (Q + R) = (P + Q) + R, ∀P, Q, R ∈ E($GF(2^n)$). (Associative)

We can notice that addition over E($GF(2^n)$) requires one inversion, two multiplications, one squaring and eight additions. Similarly, doubling a point on E($GF(2^n)$) requires one inversion, two multiplication, one squaring and six additions.

The following algorithm implements the addition of two points on E($GF(2^n)$) in terms of affine coordinates.

Algorithm1: Addition on E($GF(2^n)$) (affine coordinates)

INPUT: An elliptic curve E($GF(2^n)$)with parameters $a, b \in GF(2^n)$, and points

$P = (x_1, y_1)$ and $Q = (x_2, y_2)$

OUTPUT: $R=P+Q$.

If $P= O$ then $R \leftarrow Q$ and stop

If $Q= O$ then $R \leftarrow P$ and stop

If $x_1 = x_2$ then

If $y_1 + y_2 = x_2$ then $R \leftarrow O$ and stop

else

$\lambda \leftarrow x_2 + y_2 / x_2$, $x_3 \leftarrow \lambda^2 + \lambda + a$, $y_3 \leftarrow x_2^2 + (\lambda + 1)x_3$,

else

$\lambda \leftarrow (y_1 + y_2)/(x_1 + x_2)$, $x_3 \leftarrow \lambda^2 + \lambda + x_1 + x_2 + a$,

$y_3 \leftarrow (x_2 + x_3)\lambda + x_3 + y_2$,

Output $R \leftarrow (x_3, y_3)$.

2- ADDITION FORMULAS IN PROJECTIVE COORDINATES FOR ECC OVER $GF(2^n)$.

When filed inversion in $GF(2^n)$ is expensive relative to multiplications it may be more efficient to represent points in projective coordinates since a field division is more expensive than 10 multiplications we use projective coordinates as proposed in [9], then it may pay to keep track of numerators and denominators separately. In this way, one can replace division by α with multiplication of the denominator by α.

In standard projective coordinates, the projective point (X, Y, Z), $Z \neq 0$, corresponds to the affine point $(X/Z, Y/Z)$ The projective equation of the elliptic curve is $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$

Given the distinct points P and Q expressed in projective coordinates $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$ we compute the projective coordinates of the elliptic sum $P + Q = (X_3, Y_3, Z_3)$, the addition formulae for computing 2P are given as multiplications. The projective addition formula is:

(Point addition)	**Formula (3)**
$A = X_2Z_1 + X_1$,	$1M$
$B = Y_2Z_1 + Y_1$,	$1M$
$C = A + B$,	
$D = A^2(A + aZ_1) + Z_1BC$,	$4M$
$X_3 = AD$,	$1M$

$Y_3 = CD + A^2(BX_1 + AY_1)$, 4M

$Z_3 = A^3 Z_1$, 2M

13M

This computation requires 13 field multiplications.

In Jacobian projective coordinates [4], the projective point (X, Y, Z), $Z \neq 0$, corresponds to the affine point $(X/Z^2, Y/Z^3)$ and the projective equation of the curve is $Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6$. The projective form of the adding formula on the curve $y^2 + xy = x^3 + ax^2 + b$ over $GF(2^n)$ is $(X_0, Y_0, Z_0) + (X_1, Y_1, 1) = (X_2, Y_2, Z_2)$, where,

(Point addition)	**Formula (4)**
$W = X_1 Z_0^2 + X_1$,	1M
$R = Y_1 Z_0^3 + Y_1$,	2M
$Z_2 = WZ_0$,	1M
$V = RX_1 + Z_2 Y_1$,	2M
$T = R + Z_2$,	
$X_2 = aZ_2^2 + TR + W^3$,	3M
$Y_2 = TX_2 + VZ_2^2$,	2M
	11M

In [10], a set of projective coordinates was introduced. Here, a projective point (X, Y, Z), $Z \neq 0$, corresponds to the affine point $(X/Z, Y/Z^2)$ and the projective equation of the curve is $Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4$. Formulas for addition in mixed coordinates are: $(X_0, Y_0, Z_0) + (X_1, Y_1, 1) = (X_2, Y_2, Z_2)$, where

(Point addition)	**Formula (5)**
$A = Y_1 Z_0^2 + Y_0$,	1M
$B = X_1 Z_0 + X_0$,	1M
$C = Z_0 B$,	1M
$D = B^2(C + aZ_0^2)$,	2M
$Z_2 = C^2$,	
$E = AC$,	1M
$X_2 = A^2 + D + E$,	
$F = X_2 + X_1 Z_2$,	1M

$G = X_2 + Y_1 Z_2$ $1M$

$Y_2 = EF + Z_2 G$ $2M$

$10M$

In a new general set of projective coordinates was introduced. Here, a projective point (X, Y, Z), $Z \neq 0$ corresponds to the affine point $(X / Z^i, Y / Z^{2i})$ and the projective equation of the curve is $Y^2 + XYZ^i = X^3 Z^i + aX^2 Z^{2i} + bZ^{4i}$. Formulas for addition in mixed coordinates are: $(X_1, Y_1, Z_1) + (X_2, Y_2, 1) = (X_3, Y_3, Z_3)$, where

(Point addition) **Formula (6)**

$K = Z_2^i$,

$A = X_1 K$, $1M$

$B = A^2$,

$E = Y_1 K^2$, $1M$

$U = A + X_2$,

$D = U^2$,

$Z_3^i = KD$, $1M$

$F = Z_3^i$,

$R = X_1 F$, $1M$

$T = E + Y_2$,

$X_3 = A(Y_2 + X_2^2) + X_2(E + B)$, $2M$

$Y_3 = (R + X_3)(TU + Z_3^i) + F^2(Y_1 + X_1)$, $3M$

$9M$

Now we are going to prove that the previous formula(6), let $P_1 = (X_1 / Z_1^i, Y_1 / Z_1^i)$ and $P_2 = (X_2 / Z_2^i, Y_2 / (Z_2^i)^2)$ be two points on the elliptic curve E. Assume that $X_1 / Z_1^i = x_1$, $Y_1 / (Z_1^i)^2 = y_1$, $X_2 / Z_2^i = x_2$, $Y_2 / (Z_2^i)^2 = y_2$, and $Z_1 = 1$, now we are going to show $X_3 / Z_3^i = x_3$ and $Y_3 / (Z_3^i)^2 = y_3$, where (x_3, y_3) is generated by (x_1, y_1) and (x_2, y_2) by using the standard addition formula of affine coordinates, then the addition formula is $P_1 + P_2 = (X_3 / Z_3^i, Y_3 / (Z_3^i)^2)$.

$$\frac{X_3}{Z_3^i} = \frac{A(Y_2 + X_2^2) + X_2(E + B)}{KD} = \frac{X_1 Z_2^i (Y_2 + X_2^2) + X_2 (Y_1 Z_2^{2i} + X_1^2 Z_2^{2i})}{Z_2^i (X_1 Z_2^i + X_2)^2}$$

$$= \frac{X_1 Y_2 + X_1 X_2^2 + X_2 Y_1 Z_2^i + X_1^2 X_2 Z_2^i}{(X_1 Z_2^i + X_2)^2} = \frac{x_1 y_2 + x_1 x_2^2 + x_2 y_1 + x_1^2 x_2}{(x_1 + x_2)^2}$$

$$= \frac{y_1^2 + y_2^2 + x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2}{(x_1 + x_2)^2} + \frac{x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3 + a x_1^2 + a x_2^2}{(x_1 + x_2)^2}$$

$$= \frac{(y_1 + y_2)^2 + (y_1 + y_2)(x_1 + x_2)}{(x_1 + x_2)^2} + \frac{(x_1 + x_2)^3 + a(x_1 + x_2)^2}{(x_1 + x_2)^2}$$

$$= \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a = x_3,$$

$$\frac{Y_3}{(Z_3^i)^2} = \frac{(R + X_3)(TU + Z_3^i) + F^2(Y_1 + X_1)}{(KD)^2}$$

$$= \frac{(X_1 Z_3^i + X_3)(TU + Z_3^i) + Y_1 Z_3^i + X_1 Z_3^i}{Z_2^{2i}(X_1 Z_2^i + X_2)^4}$$

$$= \frac{TUZ_3^i X_1 + TUX_3 + X_3 Z_3^i + Y_1 Z_3^{2i} + 2X_1 Z_3^{2i}}{Z_2^{2i}(X_1 Z_2^i + X_2)^4}$$

$$= \frac{TU(Z_3^i X_1 + X_3) + X_3 Z_3^i + Y_1 Z_3^{2i}}{Z_2^{2i}(X_1 Z_2^i + X_2)^4}$$

$$= \frac{Y_1 Z_2^{2i} + Y_2}{Z_2^i (X_1 Z_2^i + X_2)^2} \times \frac{X_1 Z_3^i + X_3}{Z_3^i} + \frac{X_3}{Z_3^i} + Y_1$$

$$= \frac{\left(Y_1 + \frac{Y_2}{Z_2^{2i}}\right)}{\left(X_1 + \frac{X_2}{Z_2^i}\right)} \times \left(X_1 + \frac{X_3}{Z_3^i}\right) + \frac{X_3}{Z_3^i} + Y_1$$

$$= \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1 = y_3,$$

In formula (6), if $i=1$ hen $P_1 + P_2 = (X_3 / Z_3,\ Y_3 / Z_3^2)$ and the number of field multiplication is nine, and the number of squaring is five. If $i=2$ then $P_1 + P_2 = (X_3 / Z_3^2,\ Y_3 / Z_3^4)$ and the number of field multiplication is also nine, and the number of squaring is

increased from five to sex, however, the squaring is very cheap in $GF(2^n)$ and, there fore; negligible, the Table 1 show that . In general if i is even or equal one then the number of field multiplication is nine, but if i is odd and not equal 1 then the number of field multiplication is ten.

In table 3, we illustrate the expected number of ones in the binary representation of k is $t/2 \approx n/2$, whence the expected running time of Algorithm is approximately $n/2$ point additions and n point doublings, denoted $0.5nA+nD$. If affine coordinates are used, then the running time expressed in terms of field operations is $3nM+1.5nI$, where I denotes an inversion and M a field multiplication. If projective coordinates are used, then Q is stored in projective coordinates, while P can be stored in affine coordinates. The field operation count of Jacobian projective$(X/Z^2, Y/Z^3)$ is $8.5nM+(2M+ 1I)$ (1 inversion and 2 multiplications are required to convert back to affine coordinates).

4. DISCUSSION AND CONCLUSIONS

Elliptic curve cryptography offers two major benefits over RSA namely; it has more security per bit and a suitable key size for hardware and modern communication. Thus, this results to smaller public key certificates, lower power requirements and smaller hardware processors.

There are two necessary conditions to use a new group over $GF(q)$ for cryptography: one is the discrete logarithm problem for a candidate group has enough difficulty and the other its operations can be implemented efficiency. Using the new full addition projective coordinate formula, the elliptic curve group operations can be reduced.

Three major approaches are used in this paper to enhance the elliptic curve cryptosystems: reducing the number of the elliptic curve group arithmetic operations, speed up the underlying finite field operations and reducing the size of the transited parameters. A new full addition in the projective coordinate is introduced, where the analysis for this formula show that the number of multiplication over the finite field is reduced to nine general field element multiplication. Thus this reduction will be speed up the addition about 11 percent.

Table 1. Timings for one field operation.

Field operation	Time
Multiplication	4.41
Squaring	0.49
Division	38.01

Table 2. Operation counts for point addition.

Coordinate system	Field operation		
	M	I	Total *(M+10I)*
Affine	2	1	12
Standard projective*(X/Z, Y/Z)*	13	0	13
Jacobian projective$(X/Z^2, Y/Z^3)$	11	0	11
Projective $(X/Z, Y/Z^2)$	10	0	10
Projective$(X/Z^i, Y/(Z^i)^2)$			
i even or *i=1*	9	0	9
i odd	10	0	10

Table 3. Rough estimates of point multiplication costs for n=163.

Coordinate system	EC operations		Field operations		
Affine	*A*	*D*	*M*	*I*	*Total*[a]
Standard projective*(X/Z, Y/Z)*	82	163	490	245	2940
Jacobian projective$(X/Z^2, Y/Z^3)$	82	163	1390	1	1400
Projective$(X/Z^i, Y/(Z^i)^2)$ *i even* or *i=1*	82	163	1306	1	1316
i odd and *i≠1*	82	163	1348	1	1358

[a] Total cost in field multiplications assuming *1I=10M.*

REFERENCES:

1. http://www.certicom.com, Jan. **2001**.
2. De Win, E., Bosselaers, A., Vanderberghe, S., De Gersem P. and Vandewalle, J,**1996**. A fast software implementation for arithmetic operations in *GF*(2)," *Advances in Cryptology, Proc. Asiacrypt'96, LNCS 1163,* K. Kim and T. Matsumoto, Eds.,Springer-Verlag, , p.65-76.
3. Eberle, H., Gura, N., Chang Shantz S. and Gupta, V, **2003**. A Cryptographic Processor for Arbitrary Elliptic Curves over GF(2m), *Sun Microsystems Laboratories*, Inc. Printed in U.S.A.May.

4. Hankerson, D., Lopez, J. and Menezes, A, **2000**. Software Implementation of Elliptic Curve Cryptography over Binary Fields, *Proc. Cryptographic Hardware and Embedded Systems-CHES 2000,* pp. 1-24.
5. IEEE P1363, **2001**. Standard Specifications for Public Key Cryptography, *draft.*
6. Gutub, A. and Ibrahim, M, **2003**. Power-Time Flexible Architecture for GF (2^k)Elliptic Curve Cryptosystem Computation, GLSVLSI, Washington, DC, pp.237-240.
7. Kim, J. H. and Ho Lee, D, **2002**. A Compact Finite Field Processor over GF (2^m) for Elliptic Curve Cryptography, IEEE TRANSACTIONS ON COMPUTERS, pp. 340-343.
8. Konstantinov, E., Stamatiou, Y. and Zaroliagis, G, **2002**. A Software Library for Elliptic Curve Cryptography, Springer-Verlang, pp. 625- 637.
9. Lopez, J. and Dahab, R, **1999**. Fast multiplication on elliptic curve over GF(2^m) without Precomputation, *Proc. Cryptographic Hardware and Embedded Systems(CHES'99)*, pp.316-327, Springer-Verlag.
10. Lopez, J. and Dahab, R, **1998**. Improved algorithms for elliptic curve arithmetic in GF((2^n)^m), SAC'98, LNCS 1556, pp. 201-212, Springer-Verlag.
11. Lopez, J. and Dahab, R, **1998**. An Improvement of Guajardo-Paar Method for Multiplication on Non-Supersingular Elliptic Curve, Proc. I8th'l Conf. Chilean Computer Science Soc., vol. 1, pp. 1-10.