A New Method for Speeding Up ECC Operations

*The authors are working at the Institute of Mathematics in The Academy of Sciences of DPR Korea.

**Address : Un Jong district Kwahakdong Number 1 Pyongyang DPR Korea

Abstract: Now, the best costs of elliptic doubling and addition on binary fields are believed to be 4M+5S(namely, four finite field multiplications and five field squarings) and 8M+5S respectively.

In this paper we reduce these costs to less than 3M+3S and 8M+1S respectively by using a new so-called ML-coordinate and rewriting the elliptic curve doubling formula. Combining a little programming skill, this method speeds up elliptic scalar multiplication by about 15～20 percent.

1. Survey of results

As well known, elliptic curve cryptosystem(ECC) is recognized to be strongest among modern cryptographic systems.

Nevertheless in practice the amount of operations needed for it is still too large. So, the investigation for speeding up the cryptographic system by reducing the cost has been steadily working since ECC was appeared.[1-7]

The elliptic operation means the elliptic curve addition(Ep) and the elliptic curve doubling(Ed).

In the case of characteristic 2 the fastest elliptic operation algorithm which was introduced to the international standard was designed in 1999, consuming $15M+5S$, i.e. 15 multiplications and 5 squarings in finite field, per Ep.[1]

Not far from the time, a new algorithm has occurred, which requires $14M+6S$ per Ep operation.[2]

Also, a new Ep-algorithm which required $13M+4S$ was announced, in 2000.[3]

But all these algorithms reach to at most $9M+4S$ in the case of $a=1$ and $z=1$ which is most fundamental in the cryptographic practice[1,4]

After these, in 2002, an Ep algorithm of the case $a=1$ and $z=1$ was proposed, which require $8M+5S$.[4] Since the weight of M is bigger than of S, it turns out that this is in advance of [2].

On the other hand, during all these time the Ed-algorithm had not been improved any more than $4M+5S$ which is primal.

It is a reason enough for it that the less the cost, the greater the increase of operation speed is caused by the decrease by 1M(now, 12% and 25%, respectively, in Ep and Ed), but simultaneously the more difficult the compression of the cost must be.

Another reason for it is referred to the requirement of the cryptographic practice that we can compress Ed and Ep not separatively, but surely in a coordinate.

Because the possibility, with which we can change the coordinates, is restricted by it.

In sum, the best costs for Ed and Ep attained by now are $4M+5S, 8M+5S$ respectively.[1-5]

Now in this paper we propose a new method to reduce these costs to less than $3M+3S$ and $8M+1S$ respectively. Combining a little programming skill, this method gives a speed-enhancement by 15~20 percent.

2. Algorithm

In a binary finite field $\mathbf{F} = GF(2^n)$ the modulation (by the definition polynomial) of a element $a \in \mathbf{F}$ is denoted by $[a]$ and the multiplication of a by b without the modulation – by $a*b$.

Then obviously

$$ab = [a*b].$$

By tradition $W(ab) = 1M$ and $W(a^2) = 1S$ are taken as the units of operation cost in $\mathbf{F} = GF(2^n)$.

$W(a*b) = 1M - 1S$ is evident.

Since the characteristic of the field is two , $W(a*a)$ is fell to the cost for two finite field additions by usual table-looking-up.

Since the binary field addition is so cheap that is always negligible in the considerations of cost,, $W([a]) = 1S$.

Below these values are used as the foundation of the estimation of operation cost.

In this paper we employ 4-D coordinate $P = (X, Y, Z, T)$ to projectivizate an affine point $P = (x, y)$ on an elliptic curve $E \subseteq \mathbf{F}^2$,as following.

$$x = X/Z, y = [Y]/T, T = Z^2$$

As shown , the difference of this coordinate from the traditional Lopez-Dahab coordinate is that an expansion variable T is added and the output Y is without modulation.

In this paper the transformed coordinate is called a ML-coordinate.

Lets consider in this coordinate the Ed of elliptic curve E of standard type with $a = 1$:

$$E = E(1,b) : y^2 + xy = x^3 + x^2 + b$$

[THEOREM 1]

The result (X_1, Y_1, Z_1, T_1) of an Ed-operation on a point (X, Y, Z, T) in the ML-coordinate is obtained as following.

Order	Operation	Cost
1	$A = X^2, B = [Y]^2$	$3S$
2	$Z_1 = TA, \quad T_1 = Z_1^2$	$1M + 1S$
3	$X_1 = [A*A + b*T^2]$	$1M + 1S$
4	$Y_1 = B*(B + X_1 + Z_1) + b*T_1 + T_1$	$2M - 2S$
Total		$4M + 3S$

(proof)

By the definition of elliptic operation, the doubling point (x_1, y_1) of affine point (x, y) is following:

$$\lambda = y/x + x$$
$$x_1 = \lambda^2 + \lambda + 1$$
$$y_1 = x_1(\lambda + 1) + x^2$$

Applying to here equalities from the curve equation :

$$y^2 + b = x^2(\lambda + 1)$$
$$x^6 = (y^2 + xy + x^2 + b)^2,$$

then

$$x_1 = y^2/x^2 + x^2 + (y^2+b)/x^2 = x^2 + b/x^2$$
$$y_1 = (x^4+b)(y^2+b)/x^4 + x^2 = [y^2(y^2+x^2+x^4+b) + x^4(b+1)]/x^4 .$$

In the ML-coordinate

$$x_1 = (X^4 + bZ^4)/X^2Z^2$$
$$y_1 = ([Y]^2([Y]^2 + X^2Z^2 + X^4 + bZ^4) + X^4Z^4(b+1))/X^4Z^4 .$$

Consequently, it can be easily checked that the result is obtained by putting $Z_1 = X^2Z^2$.

The estimation of the cost is obvious. □

To be remarked in this theorem is that two among four field multiplications is without modulations , by a fixed constant b .

Since the multiplication by a constant b is a linear transformation which is invariant under the shift operation , in the end this multiplication be away to a certain fixed MA filter operation.

Therefore the cost can be much reduced on the computer by block control using the MMX command and on the hardware by the filter operation of dsp.

In either case the cost is easily fell to less than half of 1M which is primal.

Therefore the cost $4M+3S$ in above theorem is reduced to less than $3M+3S$ in the actual cryptographic practice.

On the other hand, the Ep-operation needed for the realization of ECC is of the case $Z=1$ in either side of adders, as mentioned previously. Namely, in our case, this is corresponding to the Ep-operation of ML-projective points and we show a algorithm for this operation below.

[THEOREM 2]

A elliptic addition (X_2,Y_2,Z_2,T_2) of an affine point (x,y) and a ML-projective point (X_1,Y_1,Z_1,T_1) is obtained as follows.

Order	Operation	Cost
1	$A = X_1 + xZ_1$	$1M$
2	$B = [Y_1 + y*T_1]$	$1M$
3	$C = AZ_1$	$1M$
4	$D = C(B+C)$	$1M$
5	$Z_2 = C^2, \quad T = {Z_2}^2$	$2S$
6	$X_2 = [B*B + C*A^2 + D]$	$1M+1S$
7	$Y_2 = (X_2 + xZ_2)*D + (x+y)*T_2$	$3M-2S$
Total		$8M+1S$

We abbreviate the proof of this theorem for the proof is quite similar to one of theorem 1. □

As known in communication practice, in the transmission all Ed-operations can be eliminated. In this case we can eliminate the modulation of the X -component as well as the one of the Y -component in the ML-coordinate. It can be easily checked that this makes also reduce by 1S in the estimation of the cost in above theorem.

Therefore the cost of the Ep-operation in the transmission is estimated to be 8M.

In sum, theorems 1 and 2 show that ,using the ML- coordinate , the costs for Ed and Ep come to reduce to less than $3M+3S$ and $8M+1S$ respectively.

3. Where have we came to ?

Here we will discuss the highest speed of ECC generation by usual PC.

Lets be given the extension degree N of $GF(2^n)$ i.e. the length of keys. At this time, using the algorithms proposed above, the up-bound of cost needed to generate one elliptic key by using the window method with width 4 which is usually used is estimated as follows.

Case of transmission : $W_1 = Ep * N/16 = N * 8M/16 = N * 0.5M$

Case of reception : $W_2 = Ed * N + Ep * N/4 = N * (3M + 3S + 2M + 0.25S)$

$= N * (5M + 3.25S)$

Total : $W = W_1 + W_2 = N * (5.5M + 3.25S)$

If the key length N is about 200 bit (namely around 1500 bit , turning into RSA-strength), a usual P4-2.4GHz computer can proceed four million of finite field multiplications per second by using the method for speeding-up proposed in [7]. Thereby, according to the discussion above we can generate three thousand ECC keys of 200 bit long per second. Consequently by only one percent of this ability we can cover the real time course of passing zone 6 Kbps, only by series of elliptic keys which would be generated purely physically, without any stream propagation of keys. This shows that we can realize the conversation which make the statistical correlation attack principally improbable, by covering such a course for the real time speech conversation with usual quality as a phone by a complete physical random series, only by software on usual PC without adding any hardware. Then the saving residue 99 percent of computational ability discussed above is enough to no matter that use the high quality protocol of standard mp3 type in the real time compression of speech conversation within 4Kbps.

4. References

[1] I. Blake, G. Seroussi, and N. P. Smart, Elliptic Curves in cpyptography, pp. 60-72, Cambridge, U.K.: Cambridge Univ. Press, 1999.

[2] J. Lopez and R. Dahab, "Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$", Proc. Selected Areas in Cryptography-SAC`98, pp. 201-212, 1998.

[3] A. Higuchi and N. Takagi, "A Fast Addition Algorithm for Elliptic Curve Arithmetic in $GF(2^n)$ Using Projective Coordinates", Information Processing Letters, vol. 76, pp. 101-103, 2000.

[4] E. Al-Daoud, R. Mahmed, M. Rushdan, and A. Kilioman, "A New Addition Formula for Elliptic Curves over $GF(2^n)$", IEEE Transactions on computers, vol. 51, no. 8, pp. 972-975, 2002.

[5] A. Satoh and K. Takano, "A Scalable Dual –Field Elliptic Curve cryptographic processor", IEEE Transactions on Computers, vol. 52, no. 4, pp. 449-460, 2003.

[6] M. Aydos, T. Yanik and Ç. K. Koç, "High -Speed Implementation of an ECC-based Wireless authentication protocol on an ARM Microprocessor", IEE Proc. Commun., vol. 148, no. 5, pp. 273-279, 2001.

[7] Kim So In and Kim Gwang Ho, "A Method for high-speed implementation of multiplication operations in binary field $GF(2^k)$", Bulletin of the Academy of Sciences, the DPR Korea, no.1, pp.1-4, 2005.