An Innovative Scalar Multiplication Method Based on Improved m-ary

WenXue Tan , YiYan Fan , XiPing Wang and XiaoPing Lou

Institute of Network Technology
Hunan University of Arts and Science, Changde, 415000, Hunan, Mainland of P.R.China
College of Computer Science and Technology
Hunan University of Arts and Science, Changde, 415000, Hunan, Mainland of P.R.China
College of Economy and Management
Hunan University of Arts and Science, Changde, Hunan, 415000, Mainland of P.R.China
College of Computer Science and Technology
Hunan University of Arts and Science, Changde, Hunan, 415000, Mainland of P.R.China
Email: {papertwx}@163.com;{24045483,916284112,34197140}@qq.com

***Abstract*— On purpose to elevate the efficiency of elliptic curve scalar multiplication in the device with weak computation power and to improve computational security, in this paper we pioneer a novel algorithm named Improved-m-ary, which is based on the depth first addition chain scheme and the improved m-ary mechanism compatible with a flexible width window. At first, we research and analyze the advantages of addition-chain-method, m-ary and other algorithms respectively in terms of speeding computation by comparison. It is discovered that the proportion of atomic operation and window width are 2 key factors which keep the speed of scalar multiplication and its computation cost in a leash. Then, an innovative scalar-point-multiplication algorithm is designed by the project crew on the basis of findings of project research. At last, the results of theoretical analysis and experimentation statistics demonstrate that by this algorithm the average of hamming weight of the scalar as a multiplicator could be undercut and the computation cost of point-scalar-multiplication could be lowered to an amazing extent. In addition, because of its built-in scheme whereby the window width is randomized constantly it presents a favorable strong immunity against most attack methods hinged on power analysis . As a whole, it is potential that Improved-m-ary be a practical and promising fast scalar multiplication method alternative.**

***Index Terms*— Addition Chain; Scalar Multiplication; Flexible Window Width; ECC; Information Security.**

I. INTRODUCTION

Eclipse Curve Cryptograph (abbreviated by ECC) is a well-known public key encryption algorithm with a great future in the range of information security of E-Commerce based on Internet [1] and a host of Computerization Information System [2], [3]. It has been catching eyes of most scholars and researchers who are engaged in the research area of involving some better algorithms and attack algorithms. Considering the speeding crypto-operation, scalar multiplication has been playing an important role in Eclipse Curve Cryptograph. So, a list of fast scalar multiplication algorithms are designed in a heap of references.

A. Pending Questions Advanced in Ready-made References

[4] initiated a scalar multiplication algorithm named *NNAF*. That algorithm is able to reduce the scalar which as a multiplicator into a series of ones of shorter length, and by the information provided by theoretical analysis is only a fewer computation power in need. While, the related anti-attack performance and running speed demonstrated in reality faces a further survey, as a result of wanting a plenty of convincing experimentation statistics [5].

A method based a special addition-chain which was proposed in [6], and by which the proportion of point-addition-number and point-doubling-number can be optimized on the precondition of keeping the total of atomic operations stable basically. In other words, that is to decrease doubling operations and to increase addition operations. It is self-evident that addition often costs a fewer power than doubling operation, and a mediate result of which is a reduction of whole computation power-cost. However, the concerned algorithm based on the special addition-chain is only applicable to *Montgomery Ecliptic Curve* and a transformation is in demand before its being applied in the cases concerned the Ecliptic Curve of other forms. Certainly, extra computation is added in the course of transformation whereby the point-multiplication efficiency is discounted probably.

[7] designed a method of coordinate transformation, on Ecliptic Curves expressed by different reference frames, which can run at a faster speed on executing the addition-point and doubling-point. The cause is that the inverse-operations involved in point-multiplication is able to be

Submitted date: 2011-06-01;Revised date: 2012-04-04.
This work is funded by Project supported by Hunan Provincial Natural Science Foundation of China, No. 12JJ9020;Project of Hunan Provincial Science and Technology Plan, No. 2012GK3125; Project of the Education Department of Hunan Province No. 11C0900 and Project of Hunan University of Arts and Science ,No. JJYB201115.
Correspondences to: Western part of Dong-ting Road, No. 170,415000, Changde, Hunan, Mainland of P. R. China.

© 2012 ACADEMY PUBLISHER
doi:10.4304/jsw.7.11.2470-2477

decreased even canceled out by coordinate transformation, instead, some square-operations and multiplications are increased. In the end, computation power of every individual point-multiplication is cut down to a given extent. But some signals or high frequency electromagnetic wave which manifest a sharp difference in energy-consumption are eradiated on executing [8].

In response to the matter above, an attack mechanism so-called " bypassing-channel-attack " was machinated in [9]. By means of the power diversity mentioned above, bypassing-channel-attack can restructure some secret parameters of encryption communication and succeed in attacking ECC scheme. Accordingly, speed and security of point-multiplication are ranked as two key evaluation indexes which involve the security of encryption system in depth [10].

If only is speed concerned, undercutting the hamming weight of scalar, balancing the proportion of basic operations and reducing computation power-cost is a potential mainbody of technology of accelerating point-multiplication. It is convinced universally that proportion of atomic operation could be optimized through taking advantage of addition-chain. Window-method is effective to low hamming weight of scalar. But according to practice, the window width often is set to 2 or 2^r, which results in that when hamming weight downs to a certain limit the mechanism of addition-chain is excluded.

B. Main Contributions of this work

In this paper, we pioneer to introduce depth first addition chain into point-multiplication whereby to determine an optimal addition-chain by which scalar may be decomposed into a pretty proposition of basic operation after a list of preprocess measures. At the same time, a flexible-width window is embedded into the computation of point-multiplication when multiplications of the composites of scalar are extracted.

On the basis of m-ary method and improvements made in [11], we initiate an innovative scalar-point-multiplication method so-called Improved m-ary, which is abbreviated by I-m-ary. In terms of bypassing-attack, we advise to discard the ideal pursuit for the maximum computation speed, and try to shade the energy difference of signals eradiated from computation device through a mechanism of using a lot of random-flexible-width windows in turn. It is practical that selecting a best window with a moderate computation consumption in random, and shifting its width in turn in a pool of width candidates when running on precondition of keeping the total cost of computation stable by and large.

At last, the proposed algorithm is programmed and experimented in a simulation background through a horde of scalars and curves, and the gleaned statistics is systematically analyzed and compared with some up-to-date point-multiplication algorithms in parallel as to speeding performance, security, other aspects and so on.

II. Preliminaries of ECC and Traditional Scalar Algorithms

A. Preliminaries of ECC and Scalar Point Multiplication

The so-called elliptical curve we refer is a 2-dimension curve which originates from Weierstrass equation denoted by (1). Shift the focus to the integer field, and let a prime $p > 3$, define a set denoted by S, which covers all points (x, y) satisfy (2) which subject to $a, b \in GF(p)\ and\ 4a^3 + 27b^2 \neq 0 \bmod p$ and the infinite far point $\mathcal{O}$. On S, an addition operation denoted by $\oplus$ is defined [12]. From the angle of group theory,$E < \oplus, S >$ forms an Abelian group, which is often named by Ecliptic Curve group on Finite Field, denoted by E. On ecliptic curve E, let P_1 be point (x_1, y_1),and let P_2 be point (x_2, y_2), P_1 is added to P_2 and as a result, P_3 is returned which is defined by (3), (4) and (5).

$$y^2 a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (1)$$

$$y^2 \equiv x^3 + ax + b \bmod p \quad (2)$$

$$P_1(x_1, y_1) \oplus P_2(x_2, y_2) = P_3(x_3, y_3) \quad (3)$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = (x_1 - x_3) - y_1 \end{cases} \quad (4)$$

Here, slope λ is extracted as (3)

$$\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1} & if\ x_1 = x_2\ and\ y_1 = y_2 \\ \frac{y_1 - y_2}{x_1 - x_2} & if\ other\ cases \end{cases} \quad (5)$$

If $P_1 = P_2$, point-addition is renamed doubling-point operation, computing the slope of doubling point needs two times of square-operation which is denoted by $\hat{S}$, one time of inverse-operation which is denoted by $\hat{I}$ and two times of multiplication-operation which is denoted by $\hat{M}$. Relatively, point-addition costs one time of inverse-operation, two times of multiplication and one time of square.

Therefore, the computation cost totals of two cases are $1\hat{I} + 2\hat{S} + 2\hat{M}$,$1\hat{I} + 1\hat{S} + 2\hat{M}$ respectively. Given a certain hardware setting, three sorts of instruction present an approximate linear relationship as respect to time-cost as follows, $\hat{I} = 6\hat{M}$, $\hat{S} = 0.8\hat{M}$. Accordingly, both equivalent sum of cost are $T_{P \oplus P} = 9.6\hat{M}$, $T_{P_1 \oplus P_2} = 8.8\hat{M}$ respectively. A certain point $P(x, y)$ is added k times to $\mathcal{O}$ and point Q is returned, which is defined as point-scalar-multiplication, denoted by $Q = kP$.

B. Sliding-Window Algorithm

In Sliding-Window algorithm, if meet the " 0 " digit then slide the cache window across r bits [13]. However, because in each step there are s bits in demand of process, if treat it as a window, the algorithm regresses to a fix-length window mechanism. Sliding-window algorithm which is shown as Figure 1 makes a good use of the high digits of k in a system of binary number, thus efficiency of pre-computation is elevated to a great extent. By means

© 2012 ACADEMY PUBLISHER

```
R1)  Input: a Scalar k ,its m-ary
         decomposition form expressed by an
         Integer Array digit[d],Point P on E.
R2)  Output:Q = kP.
R3)  Q = O;
R4)  Point p[m + 1];
R5)  p[0] = O, p[1] = P,p[2] = 2P;
R6)  For (i = 1;i < 2^{r-1};i++)
R7)      p[i] = iP;
R8)  For (i = d - 1;i > -1;i--)
R9)      p[2i + 1] = p[2i - 1] + p[2];
R10) temp = m;r = 0;i = d - 1;
R11) while(temp >>= 1) r++;
R12) while(i > -1)
R13)     if(digit[i] == 0)
R14)         Q = 2Q;i--;
R15)     else
R16)         t = i - (r - 1);
R17)         while(digit[t] == 0) t++;
R18)         w = 1;h = 0;temp = t;
R19)         for(;t < i + 1;t++)
R20)         h+ = (digit[t] * w);w* = 2;
R21)         for(int n = 1;n < i - temp + 2;n++)
R22)             Q = 2Q;
R23)             Q = Q + p[h];i = temp - 1;
R24) Output Q.
```

Figure 1. Sliding-Window Algorithm.

of analysis course mentioned above, computation cost of Sliding-Window could be expressed by (6).

Because the difference of computation consumption and energy-cost is embodied with respect to both doubling-point and point-addition, it directly mirrors distribution of " 0 " and " 1 ", i.e. structure of scalar digit. This phenomena is extra universal in the environment with a weak computation power or thin client. If the eradiated signal is sniffed and the profile of energy is restored by means of a certain technology, it is possible to restructure and find scalar k,which provides an entry accessible to power-attack.

$$N(n,r) = 2^{r-1} + n + \frac{n}{r+1} - 2 \tag{6}$$

C. m-ary method of multiplication

Let $m = 2^r, r \geq 1$,a scalar k is represented in a system of numbers which includes m number-symbols as (7). As to a scalar composite i subject to $1 \leq i \leq 2^r$,point-multiplication iP is computed at first, which is name pre-computation, then extract kP. If $r = 1$,it regresses to binary method [14].

the word of English, " unary " expresses a system of numbers which includes one number symbol, and the English word " binary " connotates a system of numbers which includes two number symbols. Analogously, a system of numbers which includes m number symbols is expressed by the word " m-ary ". In the step of pre-computation, there are m scalars to compute point-multiplication at most. So this method is often referred by " m-ary " method, which is exhibited as Figure 2.

$$k = \sum_{j=0}^{d-1} digit[j]m^j, 0 \leq digit[j] \leq m-1 \tag{7}$$

```
R1)  Input: a Scalar k ,its m-ary
         decomposition form expressed by an
         Integer Array digit[d],Point P on E.
R2)  Output:Q = kP.
R3)  R = O;
R4)  Point p[m];
R5)  For(i = m - 1;i > -1;i--)
R6)      p[i] = iP;
R7)  For (i = d - 1;i > -1;i--)
R8)      R = mR;
R9)      R = R + p[digit[i]];
R10) Output R.
```

Figure 2. m-ary Scalar Point-Multiplication.

```
R1) Input:k
R2) Output NAF(k)=(b_{L-1}, b_{L-2}, ..., b_2, b_1, b_0).
R3) i = 0; n = k;
R4) while(n > 0)
R5)     if(n mod 2) b_i = 2 - n mod 4; n- = b_i;
R6)     else b_i = 0;
R7)     n = n/2;i++;
R8) Output(b_{L-1}, b_{L-2}, ... b_2, b_1, b_0).
```

Figure 3. Non-Adjacent Form Decomposition of Scalar.

m-ary method is simple and easy to implement. It requires $(d-1)r$ doubling-point operations. Let l denote the length of array $digit$, and represent k in a system number with 2^r symbols, then $d = \lceil l/r \rceil$, which is the number of digits. Suppose w denotes the number of non-zero symbols in k, that is to say that w represents Hamming weight. According to m-ary method, scalar-point-multiplication needs w point-addition operations and pre-computation costs $2^r - 2$ point operations.

The total computation cost of m-ary may be described by (8),which suggests that an aptitude adjustment of magnitude of r could vary the total computation consumption toward the decreasing tendency.

$$N(n,r) = (d-1)r + W + 2^r - 3 \tag{8}$$

D. NAF Algorithm

In the course of Sliding-Window algorithm, if some bit is " 0 ",on which point-addition operation is omitted. Suppose " 0 " bits could be increased, meantime " 1 " bits could be decreased on condition that magnitude of scalar is kept invariable. That is to say Hamming weight of scalar is lowered. Hinted by this idea, someone pioneers a decomposing method of scalar based on the system of binary numbers [15], i.e. Non-Adjacent Form, abbreviated by NAF. Denote the Non-Adjacent Form decomposition of scalar k $NAF(k)$,which is extracted by the algorithm exhibited by Figure 3.

NAF decomposition of scalar is characterized by follows. 1.The multiplication of adjacent 2 digits of decomposition always equals 0,i.e. $b_i \times b_{i+1} = 0$. In other words, there does not exist a phenomena that 2 non-zero digits is adjacent in $NAF(k)$,so it is named " Non-Adjacent Form ". 2.Hamming density of $NAF(k)$ is a third of that of regular binary decomposition of k, which means point-addition operations by NAF decomposition also is a third of scalar multiplication of binary-ladder algorithm.

As a result, energy cost reduces by a long way. For example,NAF of $k = 159$ is shown as Table I. NAF

© 2012 ACADEMY PUBLISHER

```
R1) Input:NAF(k)=(b_{L-1}, b_{L-2}, ..., b_2, b_1, b_0), Point
        P on E
R2) Output Q = kP.
R3) Q = O; R = P;
R4) For (i = 0; i < numbits(k); i++)
R5)     If(b_i ≠ 1) Q+ = b_i P;
R6)     Q+ = Q;
R7) Output Q;
```

Figure 4. Non-Adjacent Form Scalar Multiplication.

scalar multiplication algorithm is exhibited as Figure 4.

TABLE I.
NAF DECOMPOSITION OF $K = 159$

Weights	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary	1	0	0	1	1	1	1	1
NAF(159)	-1	0	0	0	0	1	0	1

However, energy-cost profile of NAF method is similar with Binary Ladder Algorithm. It isn't random irregular at all, which anchors its weakness against Side Channel analysis and Power-Attack.

III. RELATED DEFINITIONS & ALGORITHMS OF ADDITION-CHAIN

Improving the decomposition method of scalar k and decreasing the times of point-addition operation potentially save the power-cost of scalar point-multiplication to a certain extent. However, when the times of point-addition is reduced to a critical point where a further effort toward that direction difficultly makes progress.

Obviously, the power-cost of doubling-point is more than that of point-addition. If on the condition that the sum of operation is kept stable and a certain number of doubling-point operations could be substituted by some equivalent point-addition operation, it is possible to save running-time of scalar point-multiplication. It is well known that any scalar k could be returned by a certain times of addition, subtraction, doubling of some base numbers which are membership of a given set. On the basis of that idea, we advise to introduce an improved addition-chain which is helpful to transforms scalar into a series of ordered additions and subtractions and etc, operations of a finite time. While subtraction and doubling operation may be unified into addition operation, accordingly name it addition-chain.

A. Chain Base

Given a certain odd integer m, define the set denoted by $B_m = \{\pm 1, \pm 2, \pm 3, \pm 5, \cdots, \pm(m-2), \pm m\}$ as the **Chain Base** of m, which includes the even primes, odds less than or equal to m and their additive inverses. m represents the window width of B.

B. Depth-First Addition-Chain

If n is an even which isn't a member of B_m, denote its chain node $N_m(n)$,which could be computed as (9). If

```
R1) Input:Integer k, B_m.
R2) Output: Depth denoted by h, Order of
        element posr.
R3) maxD = 0;
R4) for (i = 0; i < upbound(B_m); i++)
R5)     h = 0; temp = k + B_m(i);
R6) while(temp %2 == 0) {temp = temp/2; d++;}
R7)     if(h > maxD) maxD = h; posr = i;
R8) return maxD, posr;
```

Figure 5. Extraction Limit-Depth : $maxDepth(k, maxD, posr)$.

n is an odd which isn't a member of B_m,its chain node denoted by $N_m(n)$,then select a base element from B_m denoted by r which makes $n+r$ with a addition chain of maximum depth, and its chain-node could be computed as (10). Similarly,the step recurs uninterruptedly until that 1 is returned, and a series of nodes as $N_m(n)$ which consist of a addition-chain, so-called the **Depth-First-Addition-Chain**.

$$N_{\mathrm{m}}(n) : n = n \div 2 \tag{9}$$

$$N_{\mathrm{m}}(n) : n = (n + r) - r \tag{10}$$

C. Base Addition-Chain

If an integer n is an element of Addition-Chain Base B_m of which width is m,its addition-chain node denoted by $N_m(n)$,which may be computed as (11).

$$\begin{aligned} &N_{\mathrm{m}}(2) : 2 = 2(1) \\ &N_{\mathrm{m}}(3) : 3 = (2 + 1) \\ &N_{\mathrm{m}}(5) : 5 = (3 + 2) \cdots \\ &N_{\mathrm{m}}(m) : m = (m - 2 + 2) \end{aligned} \tag{11}$$

The computation chain consists of $(m+1)/2$ times of addition operation,which is named pre-computation process. In general, addition-chain of integer n is constructed on precondition of this pre-computation.

D. Construction of Addition-Chain

The limit depth of chain is denoted by $maxD$,which should be defined before computation of addition-chain. We design an algorithm to return the limit-depth $maxD$ and an element of B_m which satisfies $n + r$ with the addition chain of maximum depth. This algorithm is exhibited as Figure 5,which is used in computation of addition-chain.

For example,$m = 5, n = 326485$,let Addition-Chain Base be $N_5(326485)$,and its addition-chain is extracted as Figure 6.

This addition-chain only is in need of 3 times of point-addition operations and 16 times of doubling-point operations. While NAF method costs 4 times point-additions and 18 times of doubling-point operations. And 19 times of point-additions and 20 doubling-point operations are needed as to m-ary mechanism.

Thus it is accepted that a pretty proportion of atomic operation could be produced by an optimally singled addition-chain [16]. If substitute point-addition and

© 2012 ACADEMY PUBLISHER

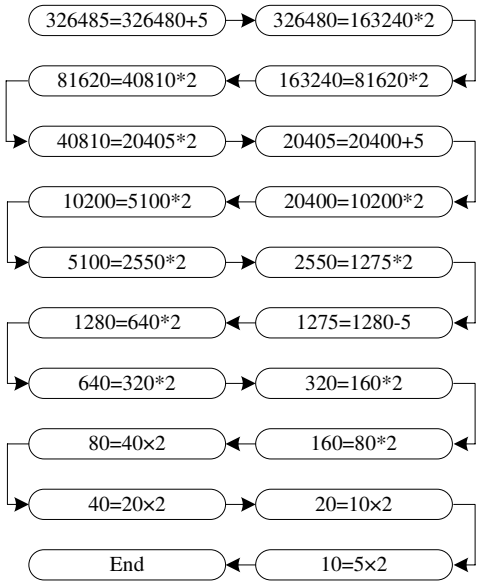

Figure 6. Addition-Chain of $N_5(326485)$.

```
R1) Input:Integer k,width m,B_m.
R2) Output: A list of N_m(k).
R3) while (k > m)
R4)     maxDepth(k, maxD, posr);
R5)     N_m(k) : k = k + B_m(posr);
R6)     While( k mod 2==0)
R7)         k = k/2;
R8)         N_m(k) : k = 2 × (k/2);
R9) Return;
```

Figure 7. Computation of Addition-Chain.

doubling-point for both addition and multiplication respectively, and compute by inverse-order, it is fit to be used for ECC scalar-point-multiplication kP, corresponding algorithm is depicted by Figure 7.

IV. Improved-m-ary Algorithm Based on Addition-Chain and Theoretical Analysis

A. Improved-m-ary Algorithm Based on Addition-Chain

As to m-ary algorithm,we find that if decompose scalar k by means of a system numbers with m symbols,not subject to 2^r symbols then the const array $\overline{p}$ could be omitted and some computation-load may be saved. In addition, substitute depth-first-chain method for point-multiplication of the power in a form of 2^r in the major loop of algorithm, this algorithm is defined as the Improved-m-ary algorithm,abbreviated by I-m-ary. It is exhibited by Figure 8.

B. Analysis of Improved-m-ary.

Lemma 1. Let $l(k)$ be the length of m-decomposition of k in the algorithm I-m-ary, then have (12) satisfied.

$$\lceil \log_m k \rceil \le l(k) \le \lceil \log_m k \rceil + 1 \tag{12}$$

Lemma 2. Given a positive integer scalar k, denote its average Hamming weight of m-decomposition $Aver_w$,

```
R1) Input:Integer array K[d] as (3),P on E.
R2) Output: Q = kP.
R3) R = O;
R4) For(j = 1; j <= d; j++)
R5)     If(digit[j]) Extract the node series of
        depth-first addition-chain N_w(digit[j];
R6) Point temp;
R7) For(j = d − 1; j > −1; j − −)
R8)     If(digit[j]0)
R9)         temp = digit[j]P;
R10)        Extract node series of depth-first
        addition-chain N_w(digit[j]
R11)        AddChain(N_w(digit[j]),&temp);
R12)        R+ = temp;
R13)    R = 2R;
R14) Output Q = R.
```

Figure 8. Improved-m-ary Algorithm of Scalar Multiplication.

then (13) could be satisfied.

$$Aver_w = \lceil \log_m k \rceil \frac{m-1}{m+1} \tag{13}$$

Theorem 1. Let $m = 2^r$,$Aver_c(2,m)$ denotes the average computation-load of point-multiplication kP per bit, then they are characteristic of as (14) to (16).

$$\begin{aligned} &if\ E\ on\ GF(p)\ and\ r \bmod 2 = 0 \\ &ave\_c(2,m) = (1/2 + \tfrac{2^r-1}{r(2^r+1)})\hat{I} \\ &+(9/2 - \tfrac{5\times 2^r-5}{r(2^r+1)})\hat{S} + (9/2 - \tfrac{2\times 2^r-2}{r(2^r+1)})\hat{M} \\ &= (11.1 + \tfrac{4\times 2^r-1}{r(2^r+1)})\hat{M} \end{aligned} \tag{14}$$

$$\begin{aligned} &if\ E\ on\ GF(p)\ and\ r \bmod 2 = 0 \\ &ave\_c(2,m) = (1/2 + \tfrac{1}{2r})\hat{I} \\ &+(9/2 - \tfrac{2.5}{r})S + (9/2 + \tfrac{4.5\times 2^r-9.5}{r(2^r+1)})\hat{M} \\ &= (11.1 + \tfrac{5.5\times 2^r-8.5}{r(2^r+1)})\hat{M} \end{aligned} \tag{15}$$

$$if\ E\ on\ GF(p)\ \lim_{r\to\infty} ave\_c(2,m) = 11.1\hat{M} \tag{16}$$

Proof. Let $GF(p)$ be a limit field and $r\ mod\ 2 = 0$. $c(4P)$ denotes the computation power to extract $4P$ and some similar symbols connotate the same implication and some midterm results are extracted as follows.

$$\begin{aligned} &\because c(4P) = \hat{I} + 9\hat{S} + 9\hat{M}. \\ &\therefore c(4P+Q) = 2\hat{I} + 4\hat{S} + 11\hat{M}. \\ &\therefore c(2^rP) = c(4^{r/2}P) = (r/2)\times c(4P) \\ &= (r/2)\hat{I} + (9\times r/2)\hat{S} + (9\times r/2)\hat{M}. \\ &\therefore c(2^rP+Q) = c(4(4^{r/2-1}P)+Q) \\ &= (r/2-1)\times c(4P) + c(4P+Q) \\ &= ((r+2)/2)\hat{I} + ((9\times r-1)/2)\hat{S} \\ &+((9\times r+13)/2)\hat{M}. \end{aligned}$$

According to **Lemma 2**,the average Hamming weight of m-decomposition $Aver_w$ satisfies (13). On the base of formula of base-substitution, we have (17).

$$\lceil \log_m k \rceil \frac{m-1}{m+1} = \lceil \log_2 k \rceil \frac{m-1}{(m+1)r} \tag{17}$$

© 2012 ACADEMY PUBLISHER

then as follows.

$$ave\_c(2,m) = (\lceil \log_2 k \rceil \frac{m-1}{(m+1)r} c(2^r P + Q) + \frac{2\lceil \log_2 k \rceil}{(m+1)r} c(2^r P))/\lceil \log_2 k \rceil \quad (18)$$

.

$$ave\_c(2,m) = (\frac{1}{2} + \frac{2^r - 1}{r(2^r+1)})\hat{I} + (\frac{9}{2} - \frac{5\times 2^r - 5}{r(2^r+1)})\hat{S} + (\frac{9}{2} - \frac{2\times 2^r - 2}{r(2^r+1)})\hat{M} = (11.1 + \frac{4\times 2^r - 1}{r(2^r+1)})\hat{M} \quad (19)$$

(19) is equivalent to (14).

Let $GF(p)$ be a limit field and $r \ mod \ 2 = 0$.

$\because c(4P) = \hat{I} + 9\hat{S} + 9\hat{M}.w(2P) = \hat{I} + 2\hat{S} + 2\hat{M}.$
$c(2P+Q) = \hat{I} + 2\hat{S} + 9\hat{M}.$

$\therefore$ as follows.

$$\begin{aligned} &c(2^r P) = c(2(4^{(r-1)/2}P)) \\ &= ((r-1)/2) \times c(4P) + c(2P) \\ &= ((r+1)/2)\hat{I} + (\tfrac{(9r-5)}{2})\hat{S} + (\tfrac{(9r-5)}{2})\hat{M} \end{aligned} \quad (20)$$

$$\begin{aligned} &c(2^r P + Q) = c(2(4^{(r-1)/2}P)) \\ &= ((r-1)/2)c(4P) + c(2P+Q) \\ &= ((r+1)/2)\hat{I} + (\tfrac{(9r-5)}{2})\hat{S} + (\tfrac{(9r+9)}{2})\hat{M} \\ &= (11.1 + \tfrac{5.5\times 2^r - 8.5}{r(2^r+1)})\hat{M} \end{aligned} \quad (21)$$

(21) is equivalent to (15).

Given r,$r \ mod \ 2 = 1$ or $r \ mod \ 2 = 0$,either always exists. then (20) and (21), either is always satisfied.

$$\lim_{r\to\infty} \frac{4\times 2^r - 1}{r(2^r+1)} = 0 \quad (22)$$

$$\lim_{r\to\infty} \frac{5.5\times 2^r - 8.5}{r(2^r+1)} = 0 \quad (23)$$

If some part of (14) and (15) is replaced by it,(24) is returned, which also is (16).

$$\lim_{r\to\infty} ave\_c(2,r) = 11.1\hat{M} \quad (24)$$

Proof ends.

It is made clear that on the condition of extra memory units over 2^r,scalar multiplication could be improved more efficiently by means of NAF mechanism with the window width of 2^r. Contrarily,NAF method does not contribute to the efficient of scalar multiplication.

Theorem 1 points it out that as to the limit field $GF(p)$ based on prime,the computation power of I-m-ary method could be estimated by (14) and (15) on condition that its window width is a power of 2.While the power nears to ∞ the average of computation power nears to a certain limit. In other words, when the power increases to some critical point, it has no immediate effect on the reduction of computation load of scalar multiplication.

However, substitute flexible window width of m for 2^r, the average Hamming weight of scalar can be lowered in a large scale on precondition that the length of scalar integer is not changed nearly, which is demonstrated in the I-m-ary method. In addition, beside the mechanism of flexible window width, addition-chain is introduced into I-m-ary algorithm, which can save computation cost of scalar multiplication from different angles by taking advantages of both above.

V. Experimentation and Contrast of Performance

In this section, computation cost of scalar multiplication demonstrated in experimentation is compared in detail as to I-m-ary algorithm and some algorithms proposed heretofore. Algorithm subjects are implemented on the basis of program library so-called NTL [17].Take an example of some 160-bits ecliptic curve and compute a certain number of scalar-point multiplication randomly. The number of scalar sample k is in condition that their bit total approximates 400 Kb, and computation cost of multiplication is collected in unit $\hat{M}$. On this condition, computation consumption per bit($\hat{M}$/Bit,unit of Y-coordinate) is computed and analyzed in parallel.

A. Comparison of I-m-ary and Montgomery-Ladder on Binary Curve

3 cases of I-m-ary with different window width are singled out and denoted respectively by I-m-ary-32, I-m-ary-256 and I-m-ary-1024. In a certain range, they are representatives of the maximum cost, the minimum cost and a moderate cost respectively, details of cost are exhibited in Figure 9.

Statistics and the illustration establish it clear that the minimum cost of I-m-ary is about 58% of Montgomery-Ladder, and a moderate cost is 59 % or so of Montgomery-Ladder. As a result, they save 42% and 41% computation cost respectively.

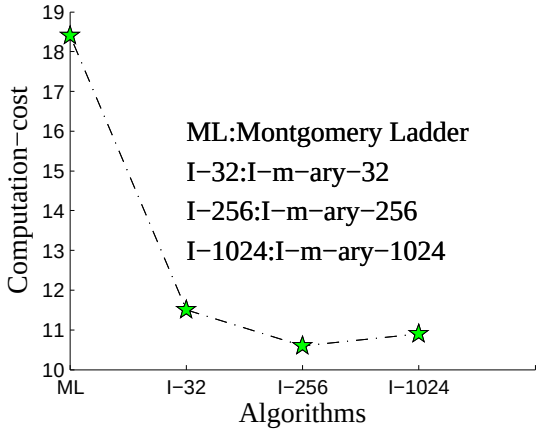

Figure 9. Comparison of I-m-ary and Montgomery.

© 2012 ACADEMY PUBLISHER

B. Speed Comparison Based on Prime Field Curve

Take an example of an average ecliptic curve E on $GF(p)$, which is expressed by (1). Its parameters a, b, base (B_x, B_y) and order $\#(E)$ are listed in Table II in a hex form. By means of the same analysis course, the window width of I-m-ary is chosen at random every time. The recorded statistics is exhibited by Figure 10 in detail.

It has been accepted that both double base-chain and m-ary are two scalar-point multiplication algorithms with a rather high speed. By comparison, the speed of double-base-chain is 84.8% of I-m-ary and 83.4% one of m-ary is 83.4% that of I-m-ary, while 15.2% and 16.3% are elevated respectively.

TABLE II.
PARAMETERS OF THE ECLIPTIC CURVE

a	0X 39860000726400005FFC0000134000007959
b	0X 0FF800007B63000066590000502B0000707E
B_x	0X 153C000012DB00002EA600000BB3000001EB
B_y	0X 12950AEBB4F005A80C506272FC9A2F94F794326D
$\#(E)$	0X 0100000000000000000000003D292A9AE0C99D9C2937

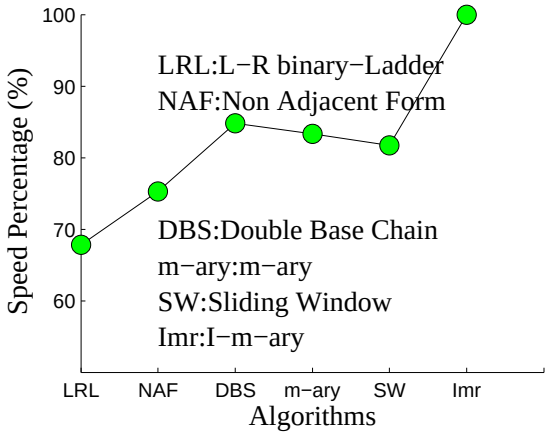

Figure 10. Comparison Based on Prime Field Curve.

C. Security Performance Analysis

Power attack is one of major bypassing attack methods, which has been a destructive threat against the security of ECC applied in device with weak computation power [18], [19]. Nowadays, mainstream of power-analysis are the Simple Energy-Analysis and the Differential-Power Analysis, and corresponding counteractant measures are demonstrated in evening and randomizing scalar multiplication cost [20], [21].

I-m-ary algorithm which introduces a randomizing-mechanism to determine the window-width and makes use of some width of which the density is rather big in parallel with other most window width and which makes a moderate power-consumption and inclines to be accepted by computation environment, is discussed and analyzed systematically in the paper. As to " 0 " bit and " 1 " bit of scalar k, the same instruction series are executed, which shades the difference of energy-cost of both.

In addition, the width like the mentioned above has a large number and can be picked out easily, in the meantime window width may be altered timely in the course of running which keeps power-cost graph in a random profile from beginning to end on precondition that the total power cost is invariable by and large. Accordingly, I-m-ary is capable of establishing a strong immunity against bypassing attack [22]–[24].

VI. CONCLUSIONS

In this work, we design an innovative scalar-point-multiplication algorithm so-called I-m-ary based on depth-first-addition and flexible window width, and it is applicable to the Ecliptic curve in Montgomery form and the curve defined on prime field $GF(p)$.

The theoretical analysis elucidates it clear that it could effectively decrease the average Hamming weight of scalar and computation consumption. Related experimentation and statistics analysis demonstrates that its computation cost is about 59% of one of Montgomery method and 75.3% of one of NAF algorithm, 84.8% of one of Double-Base-Chain,and that it is of a better efficiency in parallel with other similar algorithms.

As to security performance, because its window width can be adjusted at random on executing, the power-cost difference of point-addition and point-doubling is screened effectively, and the profile of energy-cost is evened. As a result, it can put an effective damper to bypass analysis and power-attack.

To summarize the text above, if a farther detail validation research is unfolded smoothly, I-m-ary is a potential of practical and predominant scalar-point-multiplication algorithm to be introduced in the information security application of Ecliptic Curve Cryptography.

ACKNOWLEDGMENT

This work is funded by Project supported by Hunan Provincial Natural Science Foundation of China, No. 12JJ9020;Project of Hunan Provincial Science and Technology Plan, No. 2012GK3125; Project of the Education Department of Hunan Province No. 11C0900 and Project of Hunan University of Arts and Science ,No. JJYB201115.

The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the paper.

REFERENCES

[1] WANG Xi-ping, TAN Wen-xue, PAN Mei-sen;Fast ECC scalar multiplication algorithm based on random-window-width for E-commerce security,*J. Computer Engineering and Design*,Vol.32,No.9,pp.2957-2960, 2011.

[2] Tan WenXue,Wang XiPing,Xi JinJu;An intelligent diagnosing system by the uncertainty reason based on key-associative certainty forecast,*J. Communications in Computer and Information Science*,Vol.217,No.4,pp.215-220, 2011.

© 2012 ACADEMY PUBLISHER

[3] Tan WenXue,Wang XiPing,Xi JinJu;Expert system of goat disease diagnosis with dual-reasoning-kernel,*J. Nongye Gongcheng Xuebao/Transactions of the Chinese Society of Agricultural Engineering*,Vol.25,No.10(SUPPL),pp.218-222, October 2009.
[4] Zhao Chang-an, Zhang Fang-Guo. Research and Development on Efficient Pairing Computations ,*J.Journal of Software*,vol.20, No.11,pp.3001-3009, 2009.
[5] Tan WenXue,Wang XiPing; A novel practical Certificate-Less digital signing system based on super-elliptic bilinear map parings,*J. Journal of Software*,Vol.6,No.8,pp.1403-1408, August 2011.
[6] Liu Shuang-genHu Yu-pu. Fast and secure elliptic curve scalar multiplication algorithm based special addition chains,*J.Journal of Southeast University (English Edition)*,vol.24,No.1.pp.29-32,2008.
[7] Pang Liao-Jun, Li Hui-Xian, Jiao Li-Cheng, et.al. Design and Analysis of a Provable Secure Multi-Recipient Public Key Encryption Scheme, *J.Journal of Software*,vol.20, No.10, pp. 2907-2914, 2009.
[8] Tan WenXue,Pan MeiSen,Wang XiPing,Shu XiaoHe; A method of security gradation against RSA IEA,*Proc. 2010 1st ACIS International Symposium on Cryptography, and Network Security, Data Mining and Knowledge Discovery, E-Commerce and Its Applications, and Embedded Systems, CDEE 2010*,Vol.1,pp.170-174,2010.
[9] Douglas Stebila and Nicolas Theriault. Unified Point Addition Formula and Side-Channel Attacks,*M. CHES, Springer-Verlag*, Berlin,pp.354-368, 2006.
[10] Tan WenXue,Wang XiPing; An innovative certificate-free signature algorithm by bilinear parings on elliptic curve,*J. ICIC Express Letters*,Vol.5,No.7,pp.2319-2325,2011.
[11] Wang xue-liPei ding-yi. Theory & Implementation On Elliptic and super-Elliptic Curve Cryptography,*M.Bei Jing-Science Press*,pp. 448-475,2006.
[12] F.Morain and J.olivos. Speeding up the computations on an elliptic curve using Addition subtraction chains,*J.Informatique Theorique et at Applications*,Vol.24,No.(7),pp.531-544,2010.
[13] Ning Zhang,Zhi-xiong Chen,Guo-zhen Xiao. Efficient elliptic curve scalar multiplication algorithms resistant to power analysis,*J. Information Sciences*,vol.177, No.10, pp.2119-2129, 2007.
[14] Tan WenXue,Wang XiPing,Xu XiaoRong; An intelligent system of diagnosis based on associative factor uncertainty speculation inference,*J. Advances in Intelligent and Soft Computing*,Vol.104,pp.51-56,2011.
[15] Marc Joye. Highly Regular Right-to-Left Algorithms for Scalar Multiplication ,*C.CHES, LNCS 4727,Springer-Verlag,Berlin*, pp.135-147,2007.
[16] Ding Xiao-Fei, Ma Chuan-gui.The Three-Party Password-Authenticated Key Exchange Protocol with Stronger Security,*J. Chinese Journal of Computers*,Vol.33,No.1,pp. 111-118,2010.
[17] Tan WenXue,Pan MeiSen,Xu XiaoRong; An intelligent disease diagnosis system by fuzzy similarity distance,*J. Applied Mechanics and Materials*,Vol.71-78,pp.2218-2221,2011.
[18] Tan WenXue,Wang XiPing; Research on intelligent diagnosing model based similarity distance,*J. Advanced Materials Research*,Vol.308-310,pp.432-435,2011.
[19] Liu Duo, Dai Yi-Qi. A New Algorithm of Elliptic Curve Multi-Scalar Multiplication, *J.Chinese Journal of Computers*,Vol.31,No.7,pp. 1113-1137, 2008.
[20] Chen Jing, Jiang Jun-Jie,Dun can,.et.al.High Performace Architecture for Elliptic Curve Scarlar Multiplication Base on FPGA*J. Chinese Journal of Computer Research and Development*,Vol.45,No.11,pp.1947-1954, 2008.
[21] Yvo Desmed, Rosario Gennaroy Kaoru. A new and improved paradigm for hybrid encryption secure against chosen-cipher-text attack,*J. Journal of cryptology*,Vol.23,no.1,pp.91-120, 2010.
[22] Tan WenXue,Wang XiPing,Lou XiaoPing,Pan MeiSen; Analysis of RSA based on quantitating key security strength,*J. Procedia Engineering*,Vol.15,pp.1340-1344,2011.
[23] Tan WenXue,Xi JinJu,Wang XiPing; A RSA key security gradating algorithm based on threshold attack time,*J. Journal of Software*,Vol.6,No.9,pp.1873-1880,2011.
[24] WenXue Tan,YiYan Fan and XiaoPing Lou; Research on a Novel Point Multiplication Method Based on Addition-Chain of Flexible-Window-Width,*J. ICIC Express Letters, Part B: Applications*,Vol.3,No.2,pp.297-304,2012.

WenXue Tan (1973-). He graduated with Master's of Science in Information technology and Earth Exploring from East China Institute of technology, Jiang-xi, Mainland of P. R. China,2003. In 2004, he joined Hunan university of Art and Science as a lecturer,being approved and authorized as computer software System Analyst by Ministry of Personnel,Mainland of P. R. China in 2005,and being promoted to Associate professor and Senior Engineer in 2008. His current research interests include Computer Science and Technology, Network and Information Security.

YiYan Fan (1978-). He is a Senior Engineer engaging in teaching in Computer Science , College of Computer Science and Technology,Hunan University of Arts and Science. His current research interests include Network Security and Web service.

Xiping Wang (1980-). She graduated with Bachelor's of Marketing from East China Institute of Technology, Jiangxi, China, 2004. She is an Instructor of Hunan University of Arts and Science. Her current research interests include Electronic Commerce and Information Security.

XiaoPing Lou (1982-). She graduated with Master's of Science in Computer Application and Technology from Center South University , Hunan, Mainland of P. R. China, 2009.She is a lecturer engaging in teaching in Hunan University of Arts and Science. Her research interests include: Quantum Secure Communication.

© 2012 ACADEMY PUBLISHER