Journal of Southeast University (English Edition) Vol. 24, No. 1, pp. 29 – 32 Mar. 2008 ISSN 1003—7985

Fast and secure elliptic curve scalar multiplication algorithm based on special addition chains

Liu Shuanggen[1, 2] Hu Yupu[1]

([1]Key Laboratory of Computer Network and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)
([2]College of Computer Information Engineering, Jiangxi Normal University, Nanchang 330022, China)

Abstract: To resist the side channel attacks of elliptic curve cryptography, a new fast and secure point multiplication algorithm is proposed. The algorithm is based on a particular kind of addition chains involving only additions, providing a natural protection against side channel attacks. Moreover, the new addition formulae that take into account the specific structure of those chains making point multiplication very efficient are proposed. The point multiplication algorithm only needs 1 719 multiplications for the SAC260 of 160-bit integers. For chains of length from 280 to 260, the proposed method outperforms all the previous methods with a gain of 26% to 31% over double-and add, 16% to 22% over NAF, 7% to 13% over 4-NAF and 1% to 8% over the present best algorithm—double-base chain.

Key words: scalar multiplication algorithm; special addition chains; side channel attacks; double base chain

Since the elliptic curve cryptography (ECC) was introduced by Miller and Koblitz[1-2], it has been the research subject of plenty of improvements and attacks. Various methods have been proposed to speed up and secure the computation of the scalar multiplication[3-4].

In this paper, we study a very particular kind of addition chains, special addition chains (SAC), which can lead to an exponentiation algorithm resistant natural side channel analysis. Moreover, the results show that it is suitable for general elliptic curves in prime fields and for giving rise to a fast and secure point multiplication. After some recall about ECC, we introduce SAC and the way that can be adapted to ECC. Finally, we compare them to other SCA resistant algorithms.

1 Background

An elliptic curve is the set of solutions for a Weierstrass equation over a field. For cryptographic purposes, this field is most frequently used as a finite field of the form GF(q). In these particular cases, the Weierstrass equation can be reduced to the following simple forms:

$$y^2 + xy = x^3 + ax^2 + b \text{ over GF}(q = 2^m), \text{ with } a, b \in \text{GF}(q) \text{ and } b \neq 0$$

$$y^2 = x^3 + ax + b \text{ over GF}(q = p^m), p > 3, \text{ with } a, b \in \text{GF}(q) \text{ and } 4a^3 + 27b^2 \neq 0$$

If the formal point at infinity ⊙ is added to the set of solutions, an addition operation can be defined over the elliptic curve, and the set of the points of the curve turns out to be a group. In Jacobian coordinates, the curve $E(p > 3)$ is given by $Y^2 = X^3 + aXZ^4 + bZ^6$, the point (X, Y, Z) on E corresponding to the affine point $\left(\frac{X}{Z^2}, \frac{X}{Z^3}\right)$ and the formulae are as follows:

Addition:

$$P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2), \quad P + Q = (X_3, Y_3, Z_3)$$
$$A = X_1 {Z_1}^2, B = X_2 {Z_1}^2, C = Y_1 {Z_2}^3, D = Y_2 {Z_1}^3, E = B - A$$
$$F = D - C, \quad X_3 = -E^3 - 2AE^2 + F$$
$$Y_3 = -CE^3 + F(AE^2 - X_3), Z_3 = Z_1 Z_2 E$$

Doubling:

$$2P = (X_3, Y_3, Z_3), A = 4X_1 {Y_1}^2, B = 3{X_1}^2 + A{Z_1}^4$$
$$X_3 = -2A + B^2, Y_3 = -8{Y_1}^4 + B(A - X_3), Z_3 = 2Y_1 Z_1$$

The computation costs are 12 multiplications (M) and 4 squarings (S) for the addition and 4M and 6S for the doubling.

Montgomery[5] proposed the following curves.

Definition 1 Let E be a prime field, an elliptic curve E_M/E is said to be in the Montgomery form if its equation is

$$By^2 = x^3 + Ax^2 + x$$

It is noted that curves in the Montgomery form can always be converted into a short classical form. However, such a conversion is false.

On such curves the addition and the doubling formulae are as follows:

Addition: $n \neq m$

$$X_{m+n} = Z_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2$$
$$Z_{m+n} = X_{m-n}((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n))^2$$

Doubling: $n = m$

$$4X_n Z_n = (X_n + Z_n)^2 - (X_n - Z_n)^2$$
$$X_{2n} = (X_n + Z_n)^2 (X_n - Z_n)^2$$
$$Z_{2n} = 4X_n Z_n((X_n - Z_n)^2 + ((A + 2)/4)(4X_n Z_n))$$

where (X_n, Y_n, Z_n) represent the point nP, for a given point P. Thus an addition takes 4M + 2S whereas a doubling needs 3M + 2S. It is well known that one needs to know the x- and z-coordinates of the points mP, nP and $mP - nP$ to compute the point $(m + n)P = mP + nP$. Finally, it is notable that there exists a formula to recover the y-coordinate at the end of a point multiplication[6].

Side channel attacks were discovered by Kocher et al. [7-8]. They aim at recovering secret information, the bits

Received 2006-11-30.

Biographies: Liu Shuanggen (1979—), male, graduate; Hu Yupu (corresponding author), male, doctor, professor, yphu@ mail. xidian. edu. cn.

Foundation item: The National Natural Science Foundation of China (No. 60473029, 60673072).

Citation: Liu Shuanggen, Hu Yupu. Fast and secure elliptic curve scalar multiplication algorithm based on special addition chains[J]. Journal of Southeast University (English Edition), 2008, 24(1): 29 – 32.

of the exponent in a point multiplication, by not only analyzing the amount of time required to perform secret operations, but also power consumption or electromagnetic radiation. However, the methods have weaknesses. It mainly depends on the fact that additions are more expensive than doublings during a point multiplication. Thus a side channel attack allowing one to deduce what kinds of operations are computed and so guess the bits of the exponent. Several countermeasures have been proposed against this threat. One example is the use of dummy operations during the process in order to make the group operations look identical and another example is the side channel atomicity[9] which consists of splitting the curve operations into identical atomic blocks.

In this paper, in order to avoid side channel attacks, we propose to perform the point multiplication using only point additions. This can be done by special addition formulae in Jacobian coordinates.

2 Scalar Multiplication Algorithm without Doubling

In this section, a new exponentiation method is presented and it can be adapted to elliptic curve scalar point multiplication.

2.1 Special addition chains

Some classical definitions are used in the addition chain study.

Definition 2 An addition chain computing an integer k is given by two sequences v and w such that

$$v = (v_0, \dots, v_s) \qquad v_0 = 1, v_s = k$$
$$v_i = v_{i_1} + v_{i_2} \qquad 1 \leqslant i \leqslant s$$
$$w = (w_1, \dots, w_s), w_i = (i_1, i_2) \qquad 0 \leqslant i_1, i_2 \leqslant i - 1$$

The length of the addition chain is s.

Definition 3 A star addition chain is an addition chain. It satisfies

$$\forall\, i, w_i = (i-1, j)$$

for some j such that $0 \leqslant j \leqslant i-1$. That is to say, for all i, we have $v_i = v_{i-1} + v_j$.

In this case we can omit $i-1$ and just write $w_i = j$.

Research about addition chains and how they are used in exponentiation problems can be referenced in Ref. [10]. In the remainder of this paper, a particular kind of star addition chain is defined as follows.

Definition 4 A special addition chain is a star addition chain with

$$w_i = \begin{cases} i-2 \\ w_{i-1} \end{cases}$$

As w_i can take only two different values, we rewrite w as

$$w = (w_3, \dots, w_s) \in \{0, 1\}^{s-2}$$

Satisfying

$$v_0 = 1, v_1 = 2, v_2 = 3$$
$$v_i = v_{i-1} + v_j \Rightarrow v_{i+1} = v_i + \begin{cases} v_{i-1} & \text{if } w_{i+1} = 0 \\ v_j & \text{if } w_{i+1} = 1 \end{cases}$$

Finally, in order to lighten the notations, we note $k = (w_3, \dots, w_s)$.

Example 1 $34 = (1, 0, 0, 0, 1, 0)$

$$v_2 = v_1 + v_0 = 2 + 1\ ,\ w_3 = 1 \Rightarrow v_3 = v_2 + v_0 = 4$$
$$w_4 = 0 \Rightarrow v_4 = 4 + 3, w_5 = 0 \Rightarrow v_5 = 7 + 4$$
$$w_6 = 1 \Rightarrow v_6 = 11 + 4, w_7 = 1 \Rightarrow v_7 = 15 + 4$$
$$w_8 = 0 \Rightarrow v_8 = 19 + 15 = 34$$

Given a point P on E, an integer k and $k = (w_3, \dots, w_s)$, it is easy to deduce the following exponentiation algorithm.

Algorithm 1

```
Input: $P$ in $E$ and $k = (w_3, \dots, w_s)$;
Output: $kP$ in $E$.
$(U_1, U_2, U_3) \leftarrow (P, 2P, 3P)$
for $i = 3$ to $s$ do
    if $w_i = 0$ then
        $U_1 \leftarrow U_2$
    end
    $U_2 \leftarrow U_3$
    $U_3 \leftarrow U_1 + U_2$
end
return $U_3$
```

This algorithm is particularly good for elliptic curves in the Montgomery form. As at each step, we have the points $U_1 = k_1 P$, $U_2 = k_2 P$ and $U_3 = U_1 + U_2 = (k_1 + k_2) P = k'P$, that is, we have exactly what we need to compute $U_3 + U_i = k'P + k_i P$, $i \in \{1, 2\}$.

Eventually, the costs of this algorithm are one initial doubling and an $s-1$ addition, that is, $(4s-1)$M and $(2s+1)$ S. Next we show that this approach can be generalized as non-Montgomery curves.

2.2 New elliptic curve point addition formulae over prime fields

Let $p > 3$ be a prime number and E/F_p an elliptic curve. If $P = (X_1, Y_1, Z)$, $Q = (X_2, Y_2, Z)$ and $P + Q = (X_3, Y_3, Z)$ are three points of E given in Jacobian coordinates, then we have

$$X_3 = ((Y_2 - Y_1)^2 - (X_1 + X_2)(X_2 - X_1)^2)\ Z^6 = X_3{}'Z^6$$
$$Y_3 = (-Y_1(X_2 - X_1)^3 + (Y_2 - Y_1)(X_1(X_2 - X_1)^2 - X'_3))Z^9 = Y'_3 Z^9$$
$$Z_3 = Z(X_2 - X_1)\ Z^3 = Z'_3 Z^3$$

Thus we have $(X_3, Y_3, Z_3) = (X'_3 Z^6, Y'_3 Z^9, Z'_3 Z^3) \sim (X'_3, Y'_3, Z'_3)$. So when P and Q have the same z-coordinate, $P + Q$ can be obtained using the following formulae.

Addition:

$$P = (X_1, Y_1, Z), Q = (X_2, Y_2, Z)\ ,\ P + Q = (X'_3, Y'_3, Z'_3)$$
$$A = (X_2 - X_1)^2, B = X_1 A, C = X_2 A, D = (Y_2 - Y_1)^2$$
$$X'_3 = D - B - C,\ Y'_3 = (Y_2 - Y_1)(B - X_3) - Y_1(C - B)$$
$$Z'_3 = Z(X_2 - X_1)$$

This addition requires 5M and 5S.

It seems to be infrequent that both P and Q share the same z-coordinate. However, if we look at the quantities $X_1 A = X_1(X_2 - X_1)^2$ and $Y_1(C - B) = Y_1(X_2 - X_1)^3$ computed during the addition, they can be seen as the x- and y-coordinates of the point $(X_1(X_2 - X_1)^2), Y_1(X_2 - X_1)^3, Z(X_2 - X_1)) \sim$

(X_1, Y_1, Z). Thus, it is possible to add P and $P+Q$ with our new formulae.

The same remark can be conducted from the doubling formulae. Indeed the quantities $A = X_1(2Y_1)^2$ and $8Y_1^4 = Y_1(2Y_1)^3$ are the x- and y-coordinates of the point $(X_1(2Y_1)^2, Y_1(2Y_1)^3, 2Y_1Z_1) \sim (X_1, Y_1, Z_1)$ allowing us to compute $P+2P$ without additional computation. Using these formulae, the computational costs of algorithm 1 become $(5s-1)$M and $(2s+4)$S.

Some cryptographic protocols only require the x-coordinate of the point kP. In this case, it is possible to save one multiplication by algorithm 1 noticing that Z does not appear during the computation of X_3' and Y_3'; thus, it is not necessary to compute Z_3' during the process. Thus, we propose new addition point addition formulae taking advantages of the specificity of special addition chains.

3 Comparisons to Other SCA Protected Algorithms

In this section we compare the proposed algorithm to the Montgomery ladder when it is used on Montgomery curves, and to the classical double-and add, NAF and 4-NAF methods, plus the recent double-base chain proposed in Ref. [11] when used on general curves.

3.1 Montgomery curves

The Montgomery ladder is a classical algorithm naturally side-channel-attack resistant. Indeed, for each bit (except the last) of the exponent k, one addition and one doubling are computed, which gives a complexity of $(7\text{M}+4\text{S})(|k|-1)$ over prime fields (where $|k|$ is the bit length of k). So if we consider that the ratio of squarings to multiplications is about 0.8 in F_P and then 160-bit integers, we obtain Tab. 1.

Tab. 1 Comparison between Montgomery ladder and SAC in F_P for a 160-bit exponent

Algorithms	Cost/M
Montgomery	1 622
SAC300	1 680
SAC280	1 568
SAC260	1 456

With chains of lengths 280 and 260, we obtain a gain of 3% and 10%, respectively.

3.2 General curve over F_P

In the case of general curves, protecting the classic algorithms against SCA implies the use of side channel atomicity, which implies that the ratio of squarings to multiplications is 1. However, the very structure of special addition chains is not allowed to resort to side channel atomicity(We keep the ratio of squarings to multiplications at 0.8). We refer to Ref. [11] for a precise study of double-and add, NAF, 4-NAF and double-base chain complexities. For 160-bit integers, we obtain Tab. 2.

We conclude that the use of special addition chains of length 300 already have a gain of 21% over double-and add and 10% over NAF. For chains of lengths from 280 to 260, the proposed method outperforms all the previous methods, with gains of 26% to 31% over double-and add, 16% to 22% over NAF, 7 to 13% over 4-NAF and 1% to 8% over double-base chain.

Tab. 2 Comparison of different elliptic curve exponentiation algorithms over F_P for a 160-bit exponent

Algorithms	Cost/M
Double-and add	2 511
NAF	2 214
4-NAF	1 983
Double-base chain	1 863
SAC300	1 983
SAC280	1 851
SAC260	1 719

4 Conclusion

In this paper, a new exponentiation method based on special addition chains is proposed. It is suitable for the application of Montgomery elliptic curves and general curves in prime fields. Besides, new formulae in the case of general curves that take advantage of the particular structures of special addition chains are presented. All of these lead to a very simple and efficient scalar multiplication algorithm. As a result, this kind of scalar multiplication algorithm directly provides a natural protection against side channel attacks.

References

[1] Miller Victor S. Uses of elliptic curves in cryptography[C]// *Advances in Cryptology—CRYPTO'85*, *Lecture Notes in Computer Sciences*. Springer-Verlag, 1986: 417 – 428.

[2] Koblitz Neal. Elliptic curve cryptosystems [J]. *Mathematics of Computation*, 1987, **48**(177): 203 – 209.

[3] Avanzi Roberto M, Cohen Henri, Doche Christophe, et al. *Handbook of elliptic and hyperelliptic curve cryptography* [M]. Boca Raton, FL, USA: Chapman and Hall/CRC Press, 2005.

[4] Hankerson Darrel, Menezes Alfred J, Vanstone Scott. *Guide to elliptic curve cryptography*[M]. Springer-Verlag, 2004.

[5] Montgomery P L. Speeding the Pollard and elliptic curve methods of factorization [J]. *Mathematics of Computation*, 1987, **48**(177): 143 – 264.

[6] Okeya Katsuyuki, Sakurai Kouichi. Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve[C]//*Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, *Lecture Notes in Computer Science*. Springer-Verlag, 2001, **2162**: 126 – 141.

[7] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems [C]//*Advances in Cryptology—CRYPTO'96*, *Lecture Notes in Computer Sciences*. Springer-Verlag, 1996: 104 – 113.

[8] Kocher P C, Jaffe J, Jun B. Differential power analysis[C]// *Advances in Cryptology—CRYPTO'99*, *Lecture Notes in Computer Sciences*. Springer-Verlag, 1999: 388 – 397.

[9] Chevallier-Mames Benoit, Ciet Mathieu, Joye Marc. Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity [J]. *IEEE Transactions on Computers*, 2004, **53**(6): 760 – 768.

[10] Knuth Donald E. *The art of computer programming*: *fundamental algorithms* [M]. Addison-Wesley, 1981.

[11] Dimitrov Vassil, Imbert Laurent, Mishra Pradeep Kumar. Ef-

ficient and secure elliptic curve point multiplication using double-base chains [C]//11*th International Conference on the Theory and Application of Cryptology and Information Security*, *Lecture Notes in Computer Sciences*. Springer-Verlag, 2005, **3788**: 59 − 78.

基于特殊加法链的快速安全椭圆曲线标量乘算法

刘双根[1,2]　　胡予濮[1]

([1] 西安电子科技大学计算机网络与信息安全教育部重点实验室,西安 710071)
([2] 江西师范大学计算机信息工程学院,南昌 330022)

摘要:为了抵抗椭圆曲线密码的边信道攻击,提出了一种新型快速安全的标量乘算法. 该算法是一种基于仅有点加运算的特殊加法链,可自然地抵抗边信道攻击. 此外,提出在一种新型点加运算公式中引进特殊结构的加法链,可以大大提高标量乘算法的运算效率. 对于长度为 160 比特的整数,其特殊加法链长度为 260 时,仅仅需要 1 719次乘法运算. 特殊加法链长度为 280 ~260 时,运行标量乘算法比倍点-点加算法效率上提高 26% ~31% ,比 NAF 算法快 16% ~22% ,比 4-NAF 算法快 7% ~13% ,比目前最好的方法双基链算法还要快 1% ~8% .

关键词:标量乘算法;特殊加法链;边信道攻击;双基链

中图分类号:TP301