一种用于加速椭圆曲线数量乘的 Signed-Binary 整数表示法

蒋苏立　陈　勇
（重庆大学计算机学院　重庆 400044）

摘　要　椭圆曲线公开加密系统已经得到了广泛的应用，其中最重要并且花费运行时间最多的运算就是计算数量乘。为了提高数量乘的运算度，本文提出了一种用于加速椭圆曲线数量乘的容易实现的 Signed-Binary 整数表示法，在不增加计算数量乘算法中预处理的复杂度的前提下，减少了点倍乘的次数，有效地提高了计算椭圆曲线点数量乘的速度。

关键词　椭圆曲线，数量乘，Signed-binary 整数表示法

A New Signed-Binary Representation for Speeding up Multiplication on Elliptic Curve

JIANG Su-Li　CHEN Yong
(The Department of Computer and Science, Chongqing University, Chongqing 400044)

Abstract　Scalar multiplication is the core operation in Elliptic curve cryptosystems (ECC). A novel recoding algorithm which products a new Signed-Binary representation for scalar multiplication is proposed in this paper. The analysis and the testing show that the algorithm can reduce the complexity while it is not increase the complexity of pre-computation to compute scalar multiplication on elliptic curve.

Keywords　Elliptic curve, Scalar multiplication, Signed-binary representation

椭圆曲线密码体制自 1985 年 N. Koblitz[1] 和 A. Menezes[2] 提出以来，由于其加密、解密的密钥短，运算速度比其他公钥算法（如 RSA、离散对数）快，受到各国安全专家和密码学专家的高度重视。在实际应用中，椭圆曲线密码体制分为两大类：

（1）建立在有限域 $GF(p)$ 上的椭圆曲线密码体制，其椭圆曲线为：

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

其中 $a,b\in GF(p)$，$4a^3+27b^2\neq 0$

（2）建立在有限域 $GF(2^n)$ 上的椭圆曲线密码体制，其椭圆曲线为：

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

其中 $a,b\in GF(2^n)$，$b\neq 0$

从研究情况来看，椭圆曲线离散对数问题（ECDLP）的难度远超过了乘法群上的离散对数问题。定义在椭圆曲线上的公钥密码体制可以使用较短的密钥获得与其它公钥体制相同的加密强度，而且拥有更快的执行速度。基于椭圆曲线上的密码体制使用 160 位的密钥提供的安全强度相当于 RSA 使用 1024 位密钥提供的安全强度[3]，而且在签名和解密方面，椭圆曲线上的密码体制要比 RSA 快很多。但相对于传统的对称加密算法（如 DES），速度还是较慢。其核心操作数量乘是主要的时间耗费。这里数量乘 KP 可以定义为

$$\underbrace{P+P+\cdots+P}_{k\text{个}P} \tag{1}$$

其中 P 是椭圆曲线上的一个有理数点，K 是一个正整数。

椭圆曲线上点的数量乘是实现椭圆曲线密码体制的基本操作，正是因为数量乘时间耗费大，目前椭圆曲线加解密的速度不能满足实际应用的需要。因此，加快计算数量乘的速度，对于椭圆曲线密码方案的实施及应用有着重要的意义。本文提出一种新的表示 K 的 Signed-binary 表示法并与 slide-window 算法相结合，提高了预处理点的利用效率，从而减少了计算椭圆曲线点数量乘的点倍乘次数，加快了算法运行速度。

1　数量乘的符号整数表示法

正如引言中所提到的那样，点的数量乘是椭圆曲线密码体制最基本、最耗时的运算。如何高效地实现数量乘运算，一直是椭圆曲线密码系统的一个研究热点。到目前为止，已经有了很多不同的算法用于加快计算椭圆曲线的数量乘[4,5]。理论上，所有适用于模指运算的算法都适用于数量乘运算。常用的算法有：Left-to-Right Binary 算法、Right-to-Left Binary 算法、m-ary 算法、滑动窗口算法。除此之外，椭圆曲线又有自身的特点，计算点加法和计算点减法的时间复杂度相同[6]，可以用由符号整数表示法（NAF）来表示 K，降低运算次数，也就是加法减法链。以下是符号整数表示法的定义：

数量乘由式（1）确定，其中 $K=(k_l,k_{l-1}\cdots k_1k)_{SD}$ 为 K 的符号整数表示法，l 为符号整数表示法的长度。我们可以将数量乘 KP 表示成：

$$kP=k_l2^{l-1}P+k_{l-1}2^{l-2}P+\cdots+k_1P,$$

其中 $k_i\in(0,-1,1)$，$i\in(1,2,\cdots,l)$

用于计算椭圆曲线数量乘比较出名的符号整数表示法有以下几种。1960 年，在文[7]中，Reitwiesner 提出一种符号整数表示法，也就是 NAF 表示法。他已经证明这种表示方法的非零位的比例是表示法长度的 1/3。在文[8]中，K. Koyama 和 Yukio Tsuruoka 提出了 KT 符号整数表示法。这种表示法的转换规则是将整数 K 的二进制表示法中的子串 $B(1\cdots b_i\cdots 1)$ 转换成 $T(10\cdots t_i\cdots\bar{1})$，其中 $\bar{1}$ 表示 -1。T 中 $t_i=b_i-$

蒋苏立　硕士研究生，主要研究方向是计算机密码学。

1。在文[9]中，Marc Joye 和 Sung-Ming Yen 提出了一种 left-to-right 的符号整数表示法，这种方法可以达到与 NAF 表示法一样的汉明权值(符号整数表示法中非零位的个数)和平均零子串长度，但是因为它是从左到右地转换二进制数串的，与 Reitwiesner 从右到左的转换法有很大的不同，后者需要更大的内存，用于存放要转换的字符串；前者只需要几个 bit 的内存单元，用于存放正在转换中的子字符串的临时地址空间。因此这种表示法在内存大小限制很多的环境中有很好的应用。例如，Smart Card 等。在文[10]中，Katti 提出了一种比 KT 表示法更为有效的表示法，它的平均零子串长度的大小更大。平均零子串长度越大，计算点数量乘的点加法也少，算法效率越高。2005 年，在文[11]中，Majid Khabbazian 提出了一种从左到右的 W-NAF 表示法，经过证明，这种表示法用于计算椭圆曲线的标量乘，点加法的次数最少。如果需要证明，可见文[11]。

2 新型 Signed-binary 整数表示法

下面我们将介绍一种新型 Signed-binary 整数表示法。设整数 K 的二进制表示为 $B(b_l b_{l-1}\cdots b_1)$，$kP=b_l 2^{l-1}P+b_{l-1}2^{l-2}P+\cdots+b_1 P$，其中 $b_i\in(0,1)$，$i\in(1,2,\cdots,l)$；W-NAF 表示为 $T(t_{l+1}t_l\cdots t_1)$，$kP=t_{l+1}2^l P+t_l 2^{l-1}P+\cdots+t_1 P$，其中 $t_i\in(0,-1,1)$，$i\in(1,2,\cdots,l)$。新型 Signed-binary 整数表示法表示为 $K(k_l k_{l-1}\cdots k_1)$，$kP=k_l 2^{l-1}P+k_{l-1}2^{l-2}P+\cdots+k_1 P$，其中 $k_i\in(0,-1,1)$，$i\in(1,2,\cdots,l)$。

具体的实现过程如下：

(1)利用算法 1 将整数 K 从二进制表示法 B 转换为 W-NAF 的表示形式 T。

(2)利用算法 2 将整数 K 从 NAF 的表示形式 T 根据下面两个转换规则转换成新型 Signed-binary 整数表示法 K。

规则 1：将串 T 中的子串 $1\underbrace{0\cdots0}_{n}\bar{1}$ 从左到右由子串 $1\underbrace{0\cdots0}_{n}\bar{1}1$ 代替。

规则 2：将串 T 中的子串 $\bar{1}\underbrace{0\cdots0}_{n}1$ 从左到右由子串 $\bar{1}\underbrace{0\cdots0}_{n-1}\bar{1}1$ 代替，其中 n 的大小由预处理点的多少来决定。在 W-NAF 表示法算法中[14]，预处理点为 4 个(1P，3P，…，$(2^{w-1}-1)$P)，其中 P 是椭圆曲线上的点，窗口大小 $W=4$，所以 $n=3$。如果预处理点为 8 个，窗口大小为 5，$n=5$。例如，如果窗口大小为 4，$1000\bar{1}$ 将转换为 $100\bar{1}1$。

算法 1 将二进制串转换为 W-NAF 表示法

```
    INPUT:(r_{l-1}r_{l-2}…r_0)_2
OUTPUT:(r'_l r'_{l-1}…r'_0)_{W-NAF}
j=0;r'_l=r_{l-1}-j;i=l-1;
    while i>0
        r'_i=r_{i-1}-r_i;i=i-1;
    end
    r'_0=j-r_0;
```

算法 2 将 W-NAF 表示法转换为新型 signed-binary 整数表示法

```
INPUT:(r'_l r'_{l-1}…r'_0)_{W-NAF}
OUTPUT:(k_{l-1}k_{l-2}…k_0)_{NewSD}
i=l
While i>4
If r'_i=1 and r'_{i-1}=0 and r'_{i-2}=0 and r'_{i-3} and r'_{i-4}=-1
   k_{i-3}=-1;k_{i-4}=1
end
If r'_i=-1and r'_{i-1}=0 and r'_{i-2}=0 and r'_{i-3}=0 and r'_{i-4}=1
   k_{i-3}=1;k_{i-4}=-1
end
i=i-4;
end
```

3 新型 Signed-Binary 整数表示法的算法分析

第 2 节介绍的几种整数表示法，其共同的特点是对于预处理点的利用不是很好。例如：滑动窗口大小为 4，如果 W-NAF 表示法为 10001，则在计算数量乘的运算中，需要 2 个加法以及 3 个点的倍乘。但是经过算法 2 的转换后，变为 $1001\bar{1}$，计算数量乘的运算只需要 2 个加法。下面将给出几个定理来分析本文提出的新型 Signed-Binary 整数表示法如何提高计算数量乘的性能。

定理 1 新型 signed-binary 整数表示法对于每一个整数 K 是唯一的。

证明：W-NAF 表示法对于每一个整数 K 均是唯一的，且规则 1，2 是一种双射函数映射。所以规则 1，2 这种确定性变化后得到的新型 Signed-Binary 整数表示法也是唯一对应一个整数 K。

证毕。

定理 2 新型 Signed-Binary 整数表示法不会增加计算标量乘的点加法数量。

证明：(数学归纳法证明)很明显，窗口大小为 2 时，$x0\bar{x}$ 变为 $x\bar{x}x$ 后，窗口数量仍为 2，没有增加窗口数量。设当窗口大小为 n 时，仍然满足。当窗口大小为 $n+1$ 时，由规则 1，2 可以明显知道，$x\underbrace{0\cdots0}_{n}\bar{x}$ 经过唯一变换成为 $x\underbrace{0\cdots0}_{n-1}\bar{x}x$ 后，窗口数量仍然是 2，没有增加窗口数量。

证毕。

定理 3 新型 signed-binary 整数表示法减少了点倍乘的数量，同时不增加预处理的点加法数量。

证明：(数学归纳法证明)在证明前将给出与本文提出的新型 signed-binary 整数表示法相结合的滑动窗口算法。

算法 3：滑动窗口算法

```
INPUT (k_{l-1}k_{l-2}…k_0)_{NewSD}
OUTPUT Q=KP
Precompute:(1P,3P,…,(2^{w-1}-1)P)，其中 P 是椭圆曲线上的点，w 是窗口大小
Q=P; i=l
Main Loop: while i>0
  If k_i=0 then
  Q=2Q, i=i-1;
  Else
    i-t+1≤w and k_i≠0,k_t≠0
    h_j=(k_i k_{i-1}…k_t)
    Q=2^{i-t+1}Q+h_j P;
  j=t-1;
end
```

从算法 3 明显可以知道，当窗口为 2 时，$x0\bar{x}$ 变为 $x\bar{x}x$ 后，中间的零就不用浪费一个点倍乘了，而且窗口仍然为 2。在第一个窗口中 $x\bar{x}$ 值为 ±1，仍然在 $2^{w-1}-1$ 内($w=2$)，仍然在预处理点的范围内，所以没有增加预处理中点加法的次数；设当窗口大小为 n 时，仍然满足。当 $w=n+1$ 时，$x\underbrace{0\cdots0}_{n}\bar{x}$ 经过唯一变换成为 $x\underbrace{0\cdots0}_{n-1}\bar{x}x$ 后，窗口数量没有变，在第一个窗口中 $x\underbrace{0\cdots0}_{n-1}\bar{x}$ 值为 $\pm2^{n-1}+1$，仍然在预处理点的范围内，所以没有增加预处理中点加法的次数。

证毕。

从上述 3 个定理我们可以看到，只要表示法中出现 $1\underbrace{0\cdots0}_{n}\bar{1}$，$\bar{1}\underbrace{0\cdots0}_{n}1$ 子串，就可以通过本文提出的转换的方法，结合滑动窗口算法，减少计算椭圆曲线数量乘中的点倍乘次数。下一节将仔细分析这种子串在不同的表示法位长度中出现的

数学期望，从而得出在不同的表示法长度下，可以减少点倍乘的次数。

4 减少点倍乘次数的分析

因为在计算椭圆曲线数量乘的实际应用中，一般整数的大小为100bit到300bit之间，所以根据文[12]，我们可以知道当窗口大小为4时是比较好的，计算的复杂度最低，预处理点的数量相对少，所消耗的内存相对少，利于在智能卡等对内存限制较多的环境中应用。所以在分析减少点倍乘次数时，我们将假定窗口大小为4。也就是说，本文将分析1000 $\bar{1}$，$\bar{1}$ 0001子串出现次数的数学期望。从算法1中，我们可以看到要出现上述两种子串，在二进制串中必须出现011110，100001这两种子串。于是我们就可以将问题转换为求在二进制串中出现011110，100001子串次数的数学期望。下面将建立一个概率模型来估计它。

设P是在6bit长的子串中出现011110，100001子串的概率。明显地，$P=1/32$。n是二进制串的长度，$100<n<300$。

在n bit二进制串中去随机抓取6bit子串，这个事件相当于做$n-6$次伯努利实验，每一次抓取事件都是独立的。所以可以用二项分布来分析它。但是要注意的是，当抓取到一个子串后，要抓取第二个子串平均只能再抓取$(n-6)/2$。依次类推，当确定了2个子串，要抓取第3个时，就只能再抓取$(n-6*2)/2$，所以求至少出现1次011110，100001这两种子串时，要做$n-6$次伯努利实验，至少出现2次$(n-6)/2$，依次类推。至少出现k次时，要做$(n-6*k)/2$。最多只能出现$\lfloor n/6 \rfloor$次子串，此时，只能做$\lceil n/6 \rceil$次伯努利实验。

P(至少出现一次)$=1-P$(一次都没有出现)$=1-(1-p)^n$；

P(至少出现两次)$=1-P$(一次都没有出现)$-P$(仅出现一次)

$$=1-\binom{0}{(n-6*1)/2}(1-p)^n-\binom{1}{(n-6*1)/2}p(1-p)^{n-6};$$

依次类推：

P(只少出现k次)$=1-P$(一次都没有出现)$-P$(仅出现一次)$-\cdots-P$(仅出现k次)

$$=1-\binom{0}{(n-6*k)/2}(1-p)^n-\cdots-\binom{k}{(n-6*k)/2}p^k(1-p)^{(n-6*k)/2}-k$$

在表1中可以看到，当$n=100,163,192,255$时，经过算法2转换后的新型signed-binary整数表示法与滑动窗口算法结合后具体减少的点倍乘次数。

表1 减少点倍乘次数(每出现一次子串均可以减少3次点倍乘的次数)

N大小	子串出现次数的数学期望(次)	减少点倍乘次数的数学期望(次)
100	3.5	10.5
163	6	18
192	9	27
255	13	39

结论 本文提出一种新的表示K的Signed-binary表示法，它是从左到右进行转换的，实现比较容易，能很好地应用到各种领域之中。在与slide-window算法相结合后，它提高了预处理点的利用效率，从而减少了计算椭圆曲线数量乘的点倍乘次数，加快了算法运行速度。因此，基于我们提出的Signed-binary表示法的椭圆曲线公开加密系统无论是在软件实现还是硬件实现上均能够拥有更好的性能。

参考文献

1 Koblitz N. Elliptic curve cryptosystems[J]. Mathematics of computation, 1987, 48(177): 203～209
2 Miller V S. Use of elliptic curve of cryptograhphy[C]. Advances in Cryptology-CRYPTO'85 Proceeding, Springer-verlag, 1986. 417～426
3 Lauter K. The Advantages of Elliptic Curve Cryptography for Wireless Security. IEEE Wireless Communication, February 2004
4 Blake I, Seroussy G, Smart N. Elliptic Curves in Cryptography. Cambridge, U. K.: Cambridge Univ Press, 1999. 67～70
5 Menezes A, van Oorschot P, Vanstone S. Handbook of Applied-Cryptography. CRC Press, 1997
6 Blake I, Seroussi G, Smart N, Elliptic Curves in Cryptography. Cambridge, U. K.: Cambridge Univ press, 1999. 62～63
7 Reitwiesner G W. Binary Arithmetic. In: Advances in Computers, 1960, 1: 231～308
8 Koyama K, Tsuruoka Y. Speeding up elliptic cryptosystems by using a signed binary window method. Advances in Cryptology-Crypto'92, LNCS740, Springer-Verlag, 1993
9 Joye M, Yen S M. Optimal Left-to-Right Binary Signed-Digit Recoding, IEEE Trans Computers, 2000, 49: 740～748
10 Katti R. Speeding up Elliptic Cryptosystems using a new Signed Binary Representation for Integers. In: Proceedings of the Euromicro Symposium on Digital System Design (DSD'02), 2002
11 Khabbazian M, Gulliver T A, Bhargava V K. A New Minimal Average Weight Representation for Left-to-Right Point Multiplication Methods. IEEE transactions on computers 2005, 54(11): 1454～1460
12 郝林，储颖，张雁. 椭圆曲线上点的数乘中窗口最佳长度的选取. 计算机工程与设计，2004, 25(1): 17～21

(上接第234页)

TPN的活性、有界性实际上是非常简单的。

寻找性质相对于传统Petri网保持不变的更广泛的网类，是我们将来进一步的研究内容。

参考文献

1 吴哲辉. 有界Petri网的活性和公平性的分析与实现. 计算机学报，1989, 12(4): 267～278
2 许安国，吴哲辉. 加权T-图的活性分析. 软件学报，1993, 4(6): 12～21
3 许安国，王培良. 加权T-图活性的进一步研究. 计算机学报，1998, 21(4): 92～96
4 翟正利，吴哲辉，杨扬. 时间Petri网模拟能力模拟能力的研究. 计算机科学，2006, 33(4)
5 Merlin P M, Farber D J. Recoverability of communication protocols - implications of a theoretical study. IEEE Trans. on Communications, 1976, 24(9): 1036～1049
6 Popova L. On Time Petri Nets. J. Inform. Process. Cybern. EIK 1991, 27(4): 227～244
7 Berthomieu B, Diaz M. Modeling and Verificatioon of Time Dependent Systems Using Time Petri Nets. IEEE Trans. On Software Engineering, 1991, 17 (3): 259～273
8 Berthomieu B, Menasche M. An enumerative approach for analyzing time petri nets. IEEE Trans. On Software Engineering, 1983, 17(3): 41～67
9 Menasche M, Berthomieu B. Time Petri Nets for Analyzing and Verifying Time Dependent Communication Protocols. In Protocol Specification, Testing, and Verification, III, Elsevier (North-Holland), 1983. 161～172
10 Murata T. Petri nets—properties, analysis, and applications. Proceedings of IEEE, 1989, 77(11): 541～580
11 袁崇义. Petri网原理. 北京：电子工业出版社，1998
12 Peterson J 著，吴哲辉译. Petri网理论与系统模拟. 徐州：中国矿业大学出版社，1989
13 Reisig W. Petri Nets -- An Introduction. Berlin: Springer Verlag, 1982