一种新的五元联合稀疏形式表示算法及其应用

王念平
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 提出了一种新的五元联合稀疏形式表示方法,并对其进行了详细的研究.对任一整数对,证明了该五元联合稀疏形式表示是惟一的;对任一二进制长度为 l 的整数对,证明了该五元联合稀疏形式表示的平均联合汉明重量是 $1/3l$;将该五元联合稀疏形式表示用于快速 Shamir 算法,与三元联合稀疏形式表示方法相比,该算法可节省 $0.167l$ 个点加运算;与已有的一种五元联合稀疏形式表示方法相比,该算法可节省 $0.054l$ 个点加运算.

关键词: 新五元联合稀疏形式表示; 平均联合汉明重量; 椭圆曲线密码; 标量乘法对
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0114-05

The Algorithm of New Five Elements Joint Sparse Form and Its Applications

WANG Nian-ping
(*Institute of Electronic Technology, The PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: A new five elements joint sparse form is proposed and is researched deeply in this paper. It is proved that every pair of integers has an unique five elements joint sparse form and average joint hamming weight of this five elements joint sparse form is $1/3l$ if the binary representations length of this pair of integers is l. We apply this five elements joint sparse form to fast Shamir algorithm. Comparing with three elements joint sparse form, this algorithm saves $0.167l$ addition operations. Comparing with existed five elements joint sparse form, this algorithm saves $0.054l$ addition operations.

Key words: new five elements joint sparse form; average joint hamming weight; elliptic curve cryptography; pairs of scalar multiplication

1 引言

椭圆曲线点群上的标量乘法运算 $kP = P + P + \cdots + P$ 是实现椭圆曲线密码体制的最主要的运算,其中 $k \in (0, n)$为正整数,n 为椭圆曲线点群的阶所包含的大素因子,P 为点群上的任意点.当 k 较小时,计算 kP 较容易,但如果 k 很大,计算 kP 就不那么容易了.此时,需要寻找一个速度更快的算法,目前关于这方面的讨论比较多[1~6].

在椭圆曲线密码的应用中,有一些体制需要计算两个标量乘法的和,即所谓的标量乘法对 $aP + bQ$ 的计算,其中 $a, b \in (0, n)$为正整数,n 为椭圆曲线点群的阶所包含的大素因子,a、b 的比特位数为 l,P、Q 是椭圆曲线点群上的任意两点.对于标量乘法对,当然可以分别计算两个标量乘法 aP 和 bQ,然后将它们做点加运算,但是能不能有更简单更直接的方法,是我们所关注的焦点.

Shamir 提出了一种计算乘法群中任意两个元素模指数的乘积的快速算法[7,8].具体地,设 G 是一个 n 阶乘法群,$g, h \in G$,即要计算形如 $g^a h^b$ 的表达式的值.考虑这个问题是因为在诸多常用的数字签名协议(除了 RSA)中,都需要通过计算 $g^a h^b$ 的值而达到认证的目的.一个最直接的方法就是分别计算两个模指数 g^a 和 h^b,然后再将所得的结果 g^a 和 h^b 相乘.运用二进制"平方—乘"方法,平均需要大约 $2l$ 个平方运算和 l 个乘法运算[9].

Shamir 认为并不需要分别计算两个模指数,而可以直接将两个指数合并为一个运算,从而提高其运算速度.一个最直接的方法就是将 a 和 b 同时用二进制表示,例如 $g^{37}h^{20}$可计算如下:

37	=	1	0	0	1	0	1
20	=	0	1	0	1	0	0
		1	g^2	g^4h^2	g^8h^4	$g^{18}h^{10}$	$g^{36}h^{20}$
$\times g$		g			g^9h^4		$g^{37}h^{20}$
$\times h$			g^2h		g^9h^5		

收稿日期:2008-03-06;修回日期:2010-06-20
基金项目:河南省信息安全重点实验室基金(No.9140C1102060702)

这种方法称为简单 Shamir 算法,显然这种方法平均需要大约 l 个平方运算和 l 个乘法运算.

Shamir 进一步观察发现,如果能够预计算并存储 gh,当 a 和 b 的二进制表示在相同位置上都为 1 时,则可以直接乘以 gh 而不必分别乘以 g 和 h,例如 $g^{37}h^{20}$可计算如下:

37	=	1	0	0	1	0	1
20	=	0	1	0	1	0	0
		1	g^2	g^4h^2	g^8h^4	$g^{18}h^{10}$	$g^{36}h^{20}$
$\times g$		g					$g^{37}h^{20}$
$\times h$			g^2h				
$\times gh$					g^9h^5		

这种方法称为快速 Shamir 算法.因为在相同位置上两个随机比特位都为 1 的概率为 1/4,所以与以上简单 Shamir 算法相比约节省了 $l/4$ 个乘法运算,从而这种方法平均需要大约 l 个平方运算和 $3l/4$ 个乘法运算.

以上的快速 Shamir 算法完全可以平移至计算标量乘法对.只不过此时平方运算变成了倍点运算,乘法运算变成了点加运算.基于椭圆曲线点群的逆运算不费时的优势,Solinas 将整数的 NAF 表示引入快速 Shamir 算法,这时平均需要大约 l 个倍点运算和 $5l/9$ 个点加运算[10],使快速 Shamir 算法得到优化.

但纵观以上各种算法,倍点运算次数都是 l 次不变,能减少的只是点加运算次数.事实上,我们关心的是标量乘法对中的整数对的非全零列——联合汉明重量,即要使联合汉明重量尽可能小.据此,Solinas 提出了整数对的三元联合稀疏形式表示[10].经证明,任一整数对有惟一的三元联合稀疏形式表示,且在所有取 0, ±1 三个值的联合汉明重量中是最小的,其平均联合汉明重量为 $l/2$.如果将三元联合稀疏形式表示引入快速 Shamir 算法,平均需要大约 l 个倍点运算和 $l/2$ 个点加运算.

因三元联合稀疏形式表示具有最小的联合汉明重量,故若要继续减小联合汉明重量,可以试图选择 $u_{i,j}=0,\pm1,\pm3$ 五个值,得到所谓的五元联合稀疏形式表示.问题是将这样的五元联合稀疏形式表示用于快速 Shamir 算法后,需要做一定数量的预计算,而减少的联合汉明重量所节省的点加运算计算量,是否多于预计算所需的计算量.文献[11]提出了一种五元联合稀疏形式表示方法,将该表示用于 Shamir 算法,需要大约 l 个倍点运算和 $0.387l$ 个点加运算.

本文经过深入的研究和分析,提出了一种新五元联合稀疏形式表示,其平均联合汉明重量仅为 $1/3l$.

2　一种新的五元联合稀疏形式表示

2.1　预计算量

在椭圆曲线点群中,计算任意点的三倍点运算需要基域的两个乘逆运算和四个乘法运算($2I+4M$).如果整数对用 $u_{i,j}=0,\pm1,\pm3$ 五个值表示,则采用快速 Shamir 算法就需要预计算 $3P,3Q,3P+3Q,3P-3Q,3P+Q,3P-Q,P+3Q,P-3Q,P+Q,P-Q$,总共需要 12 个乘逆运算和 24 个乘法运算($12I+24M$).

2.2　新五元联合稀疏形式表示的定义

定义 1　设整数对 x,y 表示为

$$x=<x_l,x_{l-1},\cdots,x_1,x_0>=\sum_{i=0}^{l}x_i\cdot2^i$$

$$y=<y_l,y_{l-1},\cdots,y_1,y_0>=\sum_{i=0}^{l}y_i\cdot2^i$$

其中 $x_j,y_j=0,\pm1,\pm3,0\leqslant j\leqslant l$.如果称之为新五元联合稀疏形式表示,必须满足:

(NWJS-1)　对 $\forall j,0\leqslant j\leqslant l-2$,若 $x_jy_j\neq0$,则 $x_{j+1}=y_{j+1}=x_{j+2}=y_{j+2}=0$.

(NWJS-2)　对 $\forall j,0\leqslant j\leqslant l-1$,若 x_j,y_j 中一个为零一个非零,则 $x_j+y_j=\pm1$ 且 x_{j+1},y_{j+1}同时为零或同时非零.

备注 1:若 x_j,y_j 中一个为零一个非零,则 $x_j=\pm1,y_j=0$ 或 $x_j=0,y_j=\pm1$.

备注 2:若 x_j,y_j 中至少有一个非零,则 $x_{j+1}\equiv y_{j+1}\pmod 2$.

备注 3:对 $\forall j,0\leqslant j\leqslant l-2$,若 $x_jx_{j+1}\neq0(y_jy_{j+1}\neq0)$,则 $x_{j+2}=0(y_{j+2}=0)$,即任意连续的三项不能全部非零.

2.3　新五元联合稀疏形式表示算法

对给定的整数对 x,y,以下的算法输出其新五元联合稀疏形式表示

$$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x_l&\cdots&x_1&x_0\\y_l&\cdots&y_1&y_0\end{pmatrix}$$

为方便,以下约定 $x \overline{\bmod}\ 8$ 表示满足 $x=q\cdot8+r$ 和 $-4<r\leqslant4$ 的惟一的整数 r,这里 q 是一个整数.$x\bmod a$ 表示通常的 x 模 a 所得的非负余数,$x\equiv y\pmod 2$表示 x 和 y 关于模 2 同余,$x\not\equiv y\pmod 2$表示 x 和 y 关于模 2 不同余.

以下算法的基本思想是:若 x,y 都为偶数,则输出 $\begin{pmatrix}x_j\\y_j\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$.若 x,y 都为奇数,则输出 $\begin{pmatrix}x_j\\y_j\end{pmatrix}=\begin{pmatrix}x \overline{\bmod}\ 8\\y \overline{\bmod}\ 8\end{pmatrix}$.若 x,y 一奇一偶,则选择合适的 $\delta_j,\delta_j'\in\{1,-1\}$,使得$(x-\delta_jx_j)/2\equiv(y-\delta_j'y_j)/2\pmod 2$成立,这里 $x_j=x\bmod 2,y_j=y\bmod 2$.

算法 1　新五元联合稀疏形式表示算法

输入:整数对 x,y.

输出:x,y 的新五元联合稀疏形式表示 $\begin{pmatrix}x_l&\cdots&x_1&x_0\\y_l&\cdots&y_1&y_0\end{pmatrix}$.

(1)$j\leftarrow0$;

(2)While $x\neq0$ or $y\neq0$ do

```
(2.1) x_j ← x mod 2, y_j ← y mod 2;
(2.1.1) if x_j y_j ≠ 0 then
        x_j ← x mod 8, y_j ← y mod 8;
    end if
  (2.1.2) if x_j x_j = 0 and x_j + x_j ≠ 0 then
      (2.1.2.1) if (x − x_j)/2 ≠ (y − y_j)/2 (mod 2) then
          x_j ← − x_j, y_j ← − y_j;
      end if
    end if
(2.2) x ← (x − x_j)/2, y ← (y − y_j)/2;
(2.3) j ← j + 1;
Endwhile
```

2.4 新五元联合稀疏形式表示的惟一性

定理 1 任一整数对 x, y 的新五元联合稀疏形式表示是惟一的.

证明 由新五元联合稀疏形式表示的定义知,只需证明满足条件(NWJS-1)和(NWJS-2)的联合表示形式是惟一的即可.

(反证法)假设整数对 x, y 有不同的五元联合稀疏形式表示 $\begin{pmatrix} x_l & \cdots & x_1 & x_0 \\ y_l & \cdots & y_1 & y_0 \end{pmatrix}$ 和 $\begin{pmatrix} x'_{l'} & \cdots & x'_1 & x'_0 \\ y'_{l'} & \cdots & y'_1 & y'_0 \end{pmatrix}$,则必然存在某个 $j, 0 \leqslant j \leqslant l$,使得 $\begin{matrix} x_j \\ y_j \end{matrix} \neq \begin{matrix} x'_j \\ y'_j \end{matrix}$. 假设 g 是使得 $\begin{matrix} x_j \\ y_j \end{matrix} \neq \begin{matrix} x'_j \\ y'_j \end{matrix}$ 的最小值,即对 $\forall k, 0 \leqslant k \leqslant g-1$,有 $\begin{matrix} x_k \\ y_k \end{matrix} = \begin{matrix} x'_k \\ y'_k \end{matrix}$,则 $u_{x,g-1} = \sum_{i=0}^{g-1} x_i \cdot 2^i = \sum_{i=0}^{g-1} x'_i \cdot 2^i$, $u_{y,g-1} = \sum_{i=0}^{g-1} y_i \cdot 2^i = \sum_{i=0}^{g-1} y'_i \cdot 2^i$. 令 $v_{x,g-1} = \dfrac{(x - u_{x,g-1})}{2^g} = \sum_{i=g}^{l} x_i \cdot 2^{i-g} = \sum_{i=g}^{l} x'_i \cdot 2^{i-g}$, $v_{y,g-1} = \dfrac{(y - u_{y,g-1})}{2^g} = \sum_{i=g}^{l} y_i \cdot 2^{i-g} = \sum_{i=g}^{l} y'_i \cdot 2^{i-g}$. 不失一般性,设 $x_g \neq x'_g$,则 $x_g x'_g \neq 0$(否则 x_g 和 x'_g 一个为零一个非零,将导致 $v_{x,g-1} = \dfrac{(x - u_{x,g-1})}{2^g} = \sum_{i=g}^{l} x_i \cdot 2^{i-g} = \sum_{i=g}^{l} x'_i \cdot 2^{i-g}$ 既是奇数又是偶数,矛盾!),此时由定义 1 后面的备注 2 知 $x_{g+1} \equiv y_{g+1} \pmod 2$, $x'_{g+1} \equiv y'_{g+1} \pmod 2$.

(1)若 $x_g, x'_g \in \{1, -1\}$,则由 $x_g \neq x'_g$ 知 $x_g x'_g = -1$,即 x_g 和 x'_g 中一个为 1,另一个为 -1,此时由 $v_{x,g-1} = 2\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} + x_g = 2\sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} + x'_g$ 知 $2(\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} - \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1}) = x'_g - x_g = \pm 2$,故 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} - \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} = \pm 1$,从而 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} \not\equiv \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} \pmod 2$,进而 $x_{g+1} \not\equiv x'_{g+1} \pmod 2$.

若 2 能整除 $v_{y,g-1}$,则 $y_g = y'_g = 0$,再由 $v_{y,g-1} = \dfrac{(y - u_{y,g-1})}{2^g} = \sum_{i=g}^{l} y_i \cdot 2^{i-g} = \sum_{i=g}^{l} y'_i \cdot 2^{i-g}$ 知 $y_{g+1} \equiv y'_{g+1} \pmod 2$,故 $x_{g+1} \equiv x'_{g+1} \pmod 2$,矛盾!

若 2 不能整除 $v_{y,g-1}$,则 $y_g \neq 0, y'_g \neq 0$,而 $x_g = 1$ 或 -1,从而 $x_g y_g \neq 0$,故由新五元联合稀疏形式表示的定义知 x_{g+1}, y_{g+1} 必同时为零. 同理由 $x'_g y'_g \neq 0$ 知 x'_{g+1}, y'_{g+1} 也必同时为零,故 $x_{g+1} \equiv x'_{g+1} \pmod 2$,矛盾!

(2)若 $x_g, x'_g \in \{3, -3\}$,则 $x_g x'_g = -9$,即 x_g 和 x'_g 中一个为 3,另一个为 -3,此时由 $v_{x,g-1} = 2\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} + x_g = 2\sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} + x'_g$ 知 $2(\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} - \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1}) = x'_g - x_g = \pm 6$,进而 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} - \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} = \pm 3$,故 $x_{g+1} \not\equiv x'_{g+1} \pmod 2$.

若 2 能整除 $v_{y,g-1}$,则 $y_g = y'_g = 0$,再由 $v_{y,g-1} = \dfrac{(y - u_{y,g-1})}{2^g} = \sum_{i=g}^{l} y_i \cdot 2^{i-g} = \sum_{i=g}^{l} y'_i \cdot 2^{i-g}$ 知 $y_{g+1} \equiv y'_{g+1} \pmod 2$,故 $x_{g+1} \equiv x'_{g+1} \pmod 2$,矛盾!

若 2 不能整除 $v_{y,g-1}$,则 $y_g \neq 0, y'_g \neq 0$,而 $x_g = 3$ 或 -3,从而 $x_g y_g \neq 0$,故由新五元联合稀疏形式表示的定义知 x_{g+1}, y_{g+1} 必同时为零. 同理由 $x'_g y'_g \neq 0$ 知 x'_{g+1}, y'_{g+1} 也必同时为零,故 $x_{g+1} \equiv x'_{g+1} \pmod 2$,矛盾!

(3)若 x_g 和 x'_g 中一个为 1 或 -1,另一个为 3 或 -3,则 $x_g x'_g = \pm 3$. 由 $v_{x,g-1} = 2\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} + x_g = 2\sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} + x'_g$ 知 $2(\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} - \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1}) = x'_g - x_g = \pm 2$ 或 ± 4,进而 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} - \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} = \pm 1$ 或 ± 2,故 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} \not\equiv \sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} \pmod 4$.

若 2 能整除 $v_{y,g-1}$,则 $y_g = y'_g = 0$,由 $x_g x'_g \neq 0$ 及定义 1 后面的备注 1 知,此时必有 $x_g, x'_g \in \{1, -1\}$,这与 $x_g x'_g = \pm 3$ 矛盾!

若 2 不能整除 $v_{y,g-1}$,则 $y_g \neq 0, y'_g \neq 0$,从而 $x_g y_g \neq 0, x'_g y'_g \neq 0$,故由新五元联合稀疏形式表示的定义知 $x_{g+1} = y_{g+1} = x_{g+2} = y_{g+2} = 0$, $x'_{g+1} = y'_{g+1} = x'_{g+2} = y'_{g+2} = 0$,进而 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} \equiv 0 \pmod 4$, $\sum_{i=g+1}^{l} x'_i \cdot 2^{i-g-1} \equiv 0$

$(\mathrm{mod}\ 4)$,于是 $\sum_{i=g+1}^{l} x_i \cdot 2^{i-g-1} \equiv \sum_{i=g+1}^{l} x_i' \cdot 2^{i-g-1} (\mathrm{mod}\ 4)$,矛盾!

综上可知,不论哪种情形都将导致矛盾,从而任一整数对 x, y 的新五元联合稀疏形式表示必是惟一的.

证毕

2.5 新五元联合稀疏形式表示的平均联合汉明重量

定义 2 设 $\begin{pmatrix} x_l & \cdots & x_1 & x_0 \\ y_l & \cdots & y_1 & y_0 \end{pmatrix}$ 是整数对 x, y 的新五元联合稀疏形式表示,$x = < x_l, x_{l-1}, \cdots, x_1, x_0 >$, $y = < y_l, y_{l-1}, \cdots, y_1, y_0 >$,称 $l_x = \max_i \{ i+1 \mid x_i \neq 0, 0 \leqslant i \leqslant l \}$ 和 $l_y = \max_i \{ i+1 \mid y_i \neq 0, 0 \leqslant i \leqslant l \}$ 分别为 x 和 y 在新五元联合稀疏形式表示中的长度,称 $l_{x,y} = \max_i \left\{ i+1 \middle| \begin{pmatrix} x_i \\ y_i \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 0 \leqslant i \leqslant l \right\}$ 为整数对 x, y 的新五元联合稀疏形式表示的长度.这里定义 $l_0 = 0$.

显然 $x = < x_{l_x-1}, \cdots, x_1, x_0 >$, $y = < y_{l_y-1}, \cdots, y_1, y_0 >$, $l_{x,y} = \max\{ l_x, l_y \}$.特别地,$l_{x,0} = l_x$, $l_{0,y} = l_y$.

为计算整数对 x, y 的新五元联合稀疏形式表示的平均联合汉明重量,引入以下三个引理.

引理 1 设 $\begin{pmatrix} x_l & \cdots & x_1 & x_0 \\ y_l & \cdots & y_1 & y_0 \end{pmatrix}$ 是整数对 x, y 的新五元联合稀疏形式表示,$l_{x,y} = l+1$,则

(1) $l_y < l_x$ 时必有 $x_l \neq 0, x_{l-1} = 0$.

(2) $l_x = l_y$ 时,$x_l \neq 0, x_{l-1} = 0$ 和 $y_l \neq 0, y_{l-1} = 0$ 至少有一种情形出现.

引理 2 设 $\begin{pmatrix} x_l & \cdots & x_1 & x_0 \\ y_l & \cdots & y_1 & y_0 \end{pmatrix}$ 是整数对 x, y 的新五元联合稀疏形式表示,$x = < x_{l_x-1}, \cdots, x_1, x_0 >$, $y = < y_{l_y-1}, \cdots, y_1, y_0 >$, $l_x \geqslant 1$, $l_y \geqslant 1$,则 $x > 0 (y > 0)$ 当且仅当 $x_{l_x-1} > 0 (y_{l_y-1} > 0)$.

引理 3 设 $\begin{pmatrix} x_l & \cdots & x_1 & x_0 \\ y_l & \cdots & y_1 & y_0 \end{pmatrix}$ 是整数对 x, y 的新五元联合稀疏形式表示,则

(1) 对 $\forall j$, $0 \leqslant j \leqslant l-2$, $\left| \sum_{i=j}^{j+2} x_i \cdot 2^{i-j} \right| \leqslant | < 310 > | = 3 \cdot 2^2 + 1 \cdot 2 + 0 = 14$.

(2) 对 $\forall j$, $0 \leqslant j \leqslant l-1$, $\left| \sum_{i=j}^{j+1} x_i \cdot 2^{i-j} \right| \leqslant | < 31 > | = 3 \cdot 2 + 1 = 7$.

(3) 对 $\forall j, 0 \leqslant j \leqslant l$, $|x_j| \leqslant |3| = 3$.

引理 3 说明,在新五元联合稀疏形式表示中,连续三位数字对应数值的绝对值以 310 对应的绝对值 14 为最大,连续两位数字对应数值的绝对值以 31 对应的绝对值 7 为最大,一位数字对应数值的绝对值以 3 对应的绝对值 3 为最大.

定理 2 设 $\begin{pmatrix} x_l & \cdots & x_1 & x_0 \\ y_l & \cdots & y_1 & y_0 \end{pmatrix}$ 是整数对 x, y 的新五元联合稀疏形式表示,若 x, y 的传统二进制表示分别有 m_x 和 m_y 位,则 $l_{x,y} \leqslant \max\{ m_x, m_y \} + 1$.

利用引理 1 ~ 3 可证得以下定理.

定理 3 任一二进制长度为 l 的整数对的新五元联合稀疏形式表示的平均联合重量是 $\frac{1}{3}l$.

由定理 3 知,将新五元联合稀疏形式表示用于快速 Shamir 算法,需要大约 l 个倍点运算和 $\frac{1}{3}l$ 个点加运算,而文献[10]中的三元联合稀疏形式表示的平均联合汉明重量为 $\frac{1}{2}l$,从而与文献[10]中的算法相比,可节省 $\frac{1}{2}l - \frac{1}{3}l = \frac{1}{6}l (\approx 0.167l)$ 个点加运算,即 $\frac{1}{6}lI + \frac{1}{3}lM$ 个基域运算.而预计算需要 12 个乘逆运算和 24 个乘法运算,即 $12I + 24M$ 个基域运算,所以,与文献[10]中的三元联合稀疏形式表示方法相比,快速 Shamir 算法总共可以减少 $(\frac{1}{6}l - 12)I + (\frac{1}{3}l - 24)M$ 个基域运算.文献[11]中的五元联合稀疏形式表示的平均联合汉明重量为 $0.387l$,从而与文献[11]中的算法相比,可节省 $0.387l - \frac{1}{3}l \approx 0.054l$ 个点加运算,即 $0.054lI + 0.108lM$ 个基域运算,而本文中的算法和文献[11]中的算法需要相同的预计算,所以,与文献[11]中已有的一种五元联合稀疏形式表示方法相比,快速 Shamir 算法总共可以减少 $0.054lI + 0.108lM$ 个基域运算.表 1 是本文中的算法和文献[10]、[11]中相应算法的比较.

表 1　不同的联合稀疏形式表示算法之间的比较

算法名称	平均联合汉明重量	需要的点加运算数量	本文中的算法减少的点加运算	本文中的算法减少的基域运算
三元联合稀疏形式表示[10]	$1/2l$	$1/2l$	$1/6l$ 个	$1/6lI + 1/3lM$ 个
五元联合稀疏形式表示[11]	$0.387l$	$0.387l$	$0.054l$ 个	$0.054lI + 0.108lM$ 个
本文中的算法	$1/3l$	$1/3l$	—	—

3 结论

本文提出了一种新的五元联合稀疏形式表示方法,将该新五元联合稀疏形式表示用于快速 Shamir 算法,与文献[10]中的三元联合稀疏形式表示方法相比,可节省 $(\frac{1}{6}l - 12)I + (\frac{1}{3}l - 24)M$ 个基域运算;与文献[11]中的五元联合稀疏形式表示方法相比,可节省 $0.054lI + 0.108lM$ 个基域运算,从而与同类算法相比,

具有很大的优势.由于目前很多椭圆曲线密码体制需要计算标量乘法对,从而本文的研究是非常有意义的.

参考文献:

[1] D M Gordon. A survey of fast exponentiation methods[J]. Journal of Algorithms, 1998, 27: 129 – 146.

[2] K Koyama, Y Tsuruoka. Speeding up elliptic cryptosystems by using a signed binary windows method[A]. Proc. Advances in Cryptology-Crypto'92[C]. Berlin: Springer-Verlag, 1993. 345 – 357.

[3] M Joye, S M Yen. Optimal left-to-right binary signed-digit recoding[J]. IEEE Transactions on Computers, 2000, 49(7): 740 – 748.

[4] Y Sakai, K Sakurai. Efficient scalar multiplications on elliptic curves with direct computations of several doublings[J]. IEICE Transactions on Fundamentals, 2001, E84-A(1): 120 – 129.

[5] R M Ayanzi, M Ciet, F Sica. Faster scalar multiplication on koblitz curves combining point halving with the frobenius endomorphism[A]. Proc. Public Key Cryptography 2004[C]. Berlin: Springer-Verlag, 2004. 28 – 40.

[6] V S Dimitrov, L Imbert, P K Mishra. Fast elliptic curve point multiplication using double-base chains[OL]. http://eprint.iacr.org/069.pdf, November, 2005.

[7] H Ong, C P Schnorr, A Shamir. An efficient signature scheme based on quadratic equations[A]. Proc. 16th ACM Symposium on Theoretical Computer Science[C]. New York: ACM, 1984. 208 – 216.

[8] T ElGamal. A public-key cryptosystems and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(14): 469 – 472.

[9] D E Knuth. The Art of Computer of Programming[M]. Vol.2: Seminumerical Algorithms (2nd ed), USA: Addison-Wesley, 1981.

[10] A Solinas. Low-weighr Binary Representations for Pairs of Integers[OL]. http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps, December, 2001.

[11] 张晓丹,肖晓强.椭圆曲线密码的一种合适的对算法[J].湖南文理学院学报(自然科学版),2007,19(4):83 – 85.
Zhang Xiao-dan, Xiao Xiao-qiang. A fast algorithm on pairs for elliptic curve cryptosystems[J]. Journal of Hunan University of Arts and Science (Natural Science Edition), 2007, 19(4): 83 – 85. (in Chinese)

[12] 唐文,唐礼勇,陈钟.基于 Markov 链的椭圆曲线标量乘法算法性能分析[J].电子学报,2004,32(11):1778 – 1781.
Tang Wen, Tang Li-yong, Chen Zhong. A Markov-chain based performance analysis method for scalar multiplication on elliptic curve[J]. Acta Electronica Sinica, 2004, 32(11): 1778 – 1781. (in Chinese)

作者简介:

王念平 男,1973 年 6 月出生于河南洛阳,现为解放军信息工程大学电子技术学院副教授,博士,硕士生导师,主要研究方向为密码学和应用数学.

E-mail: wwnnpp@126.com