第 35 卷 第 8 期 计 算 机 工 程 2009 年 4 月
Vol.35 No.8 Computer Engineering April 2009
·安全技术· 文章编号：1000—3428(2009)08—0169—02 文献标识码：A 中图分类号：TN918.2

椭圆曲线密码标量乘的ϕ-NAF$_w$分解

丁 勇[1,2]
(1. 桂林电子科技大学数学与计算科学学院，桂林 541004；2. 西安电子科技大学计算机网络与信息安全国家重点实验室，西安 710071)

摘 要：对于$GF(p)$上的椭圆曲线的标量乘计算，Ciet通过引入特征多项式为$\phi^2+2=0$的自同态ϕ，提出一种整数k的ϕ-NAF分解。对ϕ-NAF分解使用窗口技术得到k的ϕ-NAF$_w$分解，通过一定量的存储可以获取更快的计算速度。对该分解的长度和Hamming密度进行较为准确的估计。

关键词：椭圆曲线密码；标量乘；窗口技术；自同态

ϕ-NAF$_w$ Decomposition of Scalar Multiplication of ECC

DING Yong[1,2]
(1. School of Mathematics and Computational Science, Guilin University of Electronic and Technology, Guilin 541004;
2. National Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071)

【Abstract】For fast computation of scalar multiplication of the elliptic curve over GF(p), with the utilization of the endomorphism ϕ whose characteristic polynomial is $\phi^2+2=0$, ϕ-NAF expansion of the integer k is proposed by Ciet in order to speed up the computation of scalar multiplication kP. In this paper, a window technic is applied to the ϕ-NAF representation, which gets the ϕ-NAF$_w$ decomposition of k and can obtain better result than ϕ-NAF representation with the cost of some quantities of storages. The length and the density of the expansion is accurately estimated.

【Key words】Elliptic Crypty Curves(ECC); scalar multiplication; window technic; endomorphism

1 概述

椭圆曲线密码(Elliptic Crypty Curves, ECC)由于相对于RSA具有长度短和速度快的优势，因此越来越多地被安全标准采用，逐步取代RSA成为实用公钥密码算法的主流。在ECC的优化实现中，最核心的问题就是如何有效地计算标量乘kP，这里k为一个大的正整数而P为椭圆曲线群上的一点。

对于标量乘，文献[1-2]总结了很多方法用于快速计算。对于$GF(p)$上的曲线，通过定义特征多项式为$\phi^2+2=0$的自同态ϕ[3]，由于在射影坐标下$\phi(p)$比$2P$计算快，因此结合GLV方法[4]，Ciet提出了整数k的ϕ-NAF分解[5]，获得了较快的计算速度。

本文将对ϕ-NAF分解使用窗口技术ϕ-NAF$_w$，在使用一定数量的存储的条件下，降低分解的Hamming密度，从而减少运算以达到更快的计算kP的目的，其中，w为窗口大小的参数。本文在详尽的数学分析基础上，精确地估计该分解的长度和Hamming密度，从理论上证明了本方法的高效性。

2 ϕ-NAF分解

令$p>3$为一个正素数，且-2为模p的平方剩余。令E: $y^2=4x^3-30x-28$为$GF(p)$上的椭圆曲线，再令ϕ：$\phi(x,y)=(\frac{2x^2+4x+9}{4(x+2)},-\frac{2x^2+8x-1}{4\sqrt{-2}(x+2)^2}y)$为$E$上的自同态，很容易验证任取$P(x,y)\in E$，都有$\phi^2(P)+2P=0$。即$\phi^2+2=0$为其特征多项式。在射影坐标系下，由于使用了计算量更小的ϕP来替代二进制表示k时的$2P$计算，因此达到加速kP计算的目的。定义记号$c=a$ mods b表示$c\equiv a(\text{mod } b)$且$(-b/2)\leqslant c<(b/2)$，ϕ-NAF分解算法如下。

算法1 ϕ-NAF分解

输入 正整数k，素数n。

输出 $(u_{m-1},u_{m-2},\cdots,u_1,u_0)$满足$k=\sum_{i=0}^{m-1}u_i\phi^i$且$u_iu_{i+2}$(对所有$0\leqslant i<m-2$)。

处理流程

(1)分解$k=k_1+k_2\phi(\text{mod } n)$(通过GLV方法)，转(2)；

(2)若$k_1==0$且$k_2==0$，转(5)；否则转(3)；

(3)若k_1为偶数，则$u_i=0$，转(4)；否则$u_i=k_1$ mods 4，转(4)；

(4) $t=-(k_1-u_i)/2, k_1=k_2, k_2=t$，转(2)；

(5)输出$(u_{m-1},u_{m-2},\cdots,u_1,u_0)$，结束。

3 ϕ-NAF$_w$窗口技术

本文对ϕ-NAF分解使用窗口技术得到k的ϕ-NAF$_w$分解，在长度基本不变的基础上，使分解的Hamming密度由ϕ-NAF的1/3下降到1/(w+1)，从而达到加速kP计算的目的。其中，w为窗口大小参数。对于任给一个正整数k，可由算法2得到其ϕ-NAF$_w$分解。

算法2 ϕ-NAF$_w$分解

输入 正整数k，素数n(为ECC基点G的阶)，窗口大小为w。

基金项目：广西壮族自治区教育厅基金资助项目(ZT5800)
作者简介：丁 勇(1975－)，男，副教授、博士，主研方向：密码学，网路安全
收稿日期：2008-09-26 **E-mail：**stone_dingy@126.com

输出 $(u_{m-1},u_{m-2},\cdots,u_1,u_0)$ 满足 $k=\sum_{i=0}^{m-1}u_i\phi^i$，且若 $u_i\neq 0$，则所有 $t\leqslant(w-1)$ 都有 $u_{i\pm t}=0$。

处理流程

(1)分解 $k=k_1+k_2\phi \pmod n$ (通过 GLV 方法)，转(2)；

(2)若 $k_1==0$ 且 $k_2==0$，转(6)，否则转(3)；

(3)若 k_1 为偶数，则 $u_i=0, t=-(k_1/2), \quad k_1=k_2, k_2=t$，转(2)；若 k_1 为奇数，则转(4)；

(4)若 $w=2l$，则 $m_1=k_1 \bmod 2^l$, $m_2=k_2 \bmod 2^l$, $u_i=(m_1+m_2\phi)$，转(5)；若 $w=2l+1$，则 $m_1=k_1 \bmod 2^{l+1}$, $m_2=k_2 \bmod 2^l$, $u_i=(m_1+m_2\phi)$，转(5)；

(5)$t=-(k_1-m_1)/2, k_1=(k_2-m_2), k_2=t$，转(2)；

(6)输出$(u_{m-1},u_{m-2},\cdots,u_1,u_0)$，结束。

对于算法 2，需要解决如下 4 个问题：(1)对于 k 的 ϕ-NAF$_w$ 表示，是否满足若 $u_i\neq 0$，则所有 $t\leqslant(w-1)$ 都有 $u_{i\pm t}=0$；(2)该分解长度 m 为多少；(3)该分解的存在性和唯一性；(4)该分解的 Hamming 密度。为了解决这些问题，需要如下的引理和定理：

引理 1 任给一个元素 $a=a+b\phi$ 和正整数 k，有

(1) $(a+b\phi)/\phi^{2k+1}=(-1)^k(b/2^k-(a/2^{k+1})\phi)$

(2) $(a+b\phi)/\phi^{2k}=(-1)^k(a/2^k+(b/2^k)\phi)$

证明

因为 $\phi^2+2=0$，所以 $\phi^{-1}=-(\phi/2)$，从而 $(a+b\phi)/\phi=(b+a\phi^{-1})=(b-(a/2)\phi)$。

当 $m=0$ 时，则引理 1(1)显然成立。

假设对于 $m=k$ 时引理 1(1)成立，即

$$(a+b\phi)/\phi^{2m+1}=(-1)^m\left(\frac{b}{2^m}-\frac{a}{2^{m+1}}\phi\right)$$

当 $m=k+1$ 时，$(a+b\phi)/\phi^{2m+1}=((a+b\phi)/\phi^{2k+1})/\phi^2=((-1)^k(\frac{b}{2^k}-\frac{a}{2^{k+1}}\phi))/(-2)=(-1)^m(\frac{b}{2^m}-\frac{a}{2^{m+1}}\phi)$。

所以引理 1(1)成立。

同理，可以证明引理 1(2)成立。

引理 2 任给一个元素 $a=a+b\phi$ 和正整数 k，则

(1)当且仅当 $2^{k+1}|a$ 且 $2^k|b$ 时，$(a+b\phi)$能被 ϕ^{2k+1} 整除。

(2)当且仅当 $2^k|a$ 且 $2^k|b$ 时，$(a+b\phi)$能被 ϕ^{2k} 整除。

证明

由引理 1 显然可得。

定理 1 对于算法 2 的输出$(u_{m-1},u_{m-2},\cdots,u_1,u_0)$，若任取一个 $u_i\neq 0$，则对所有 $0<t\leqslant(w-1)$ 都有 $u_{i\pm t}=0$。

证明

若 $w=2l$，设 $u_i\neq 0$，则经过第 i 轮循环后，$k_1=k_2-(k_2 \bmod 2^l)$, $k_2=(k_1-k_1 \bmod 2^l)/2$。显然 $2^l|k_1$ 且 $2^{l-1}|k_2$。由引理 2(2)，有 $k_1+k_2\phi$ 能被 ϕ^{2l-1}。

所以，有 $u_{i+1}=u_{i+2}=\cdots=u_{i+2l-1}(=u_{i+w-1})=0$，对于所有的 $0<t\leqslant(w-1)$，有 $u_{i+t}=0$。

若对于某个 $0<t\leqslant(w-1)$，有 $u_{i-t}\neq 0$，则由上面结论必有 $u_i=0$，与 $u_i\neq 0$ 矛盾。

所以，对于所有的 $0<t\leqslant(w-1)$，有 $u_{i-t}=0$。因此，$w=2l$，定理成立。

同理可证 $w=2l+1$ 时定理成立。

综上，定理成立。

引理 3 对于一个元素 $a=a+b\phi$，定义其模 $N(a)=a^2+2b^2$，分别定义 $N_{\max}(d)$和 $N_{\min}(d)$为 ϕ-NAF$_w$ 表示长度为 d 的元素中模的最大值和最小值。则有 a 的 ϕ-NAF$_w$ 表示长度 m 满足：

$$\mathrm{lb}^{N(\alpha)}-\mathrm{lb}^{\left(\frac{N\max(d)}{(2^{d/2}-1)^2}\right)}<m<\mathrm{lb}^{N(\alpha)}+d-2\mathrm{lb}^{\left|\sqrt{N_{\min}(d)}-\frac{\sqrt{N_{\max}(d)}}{2^{d/2}-1}\right|}$$

证明

采用和文献[6]中证明 RTNAF 长度(定理 2)完全相同的方法，可以得到以上结果。证毕。

引理4 对于一个元素$a=a+b\phi$，定义其模$N(a)=a^2+2b^2$，则有a的ϕ-NAF$_w$表示长度m约为$\mathrm{lb}^{N(\alpha)}$。

证明

在引理 3 中，选取合适的 d，总可以使得$\mathrm{lb}^{\left(\frac{N\max(d)}{(2^{d/2}-1)^2}\right)}$以及$d-2\mathrm{lb}^{\left|\sqrt{N_{\min}(d)}-\frac{\sqrt{N_{\max}(d)}}{2^{d/2}-1}\right|}$相对于$\mathrm{lb}^{N(\alpha)}$非常小而可以忽略，从而引理 4 成立。

证毕。

定理 2 k 的 ϕ-NAF$_w$ 表示长度 m 约为 $\mathrm{lb}^n+2\mathrm{lb}^3$。

证明

由引理 4 可知 $m\approx \mathrm{lb}_2^{N(k_1+k_2\phi)}$。

又因为 $N(k_1+k_2\phi)=k_1^2+2k_2^2$ 且 $\max(|k_1|,|k_2|)\leqslant\sqrt{3}\sqrt{n}$ [4]，所以 $N(k_1+k_2\phi)\leqslant 9n, m\approx \mathrm{lb}_2^{N(k_1+k_2\phi)}\leqslant \mathrm{lb}_2^{9n}=\mathrm{lb}_2^n+2\mathrm{lb}_2^3$，定理 2 成立。

定理 3 对于任何一个正整数 k，其 ϕ-NAF$_w$ 表示有且仅有一个。

证明

由定理 2 知算法 2 的输出长度是有限的，因此，算法 2 是收敛的，总可得到 k 的 ϕ-NAF$_w$ 表示，从而证明了存在性。

又因为算法 2 的输出是唯一确定的，所以只要 k 取定，得到的 ϕ-NAF$_w$ 表示是唯一的，从而证明了其唯一性。综上，定理 5 成立。

定理 4 ϕ-NAF$_w$ 表示的 Hamming 密度为 $1/(w+1)$。

证明

显然 ϕ-NAF$_w$ 表示和 RTNAF$_w$ 表示的 Hamming 密度是完全一样的，由于 RTNAF$_w$ 表示的 Hamming 密度为 $1/(w+1)$ [5]，因此 ϕ-NAF$_w$ 表示的 Hamming 密度为 $1/(w+1)$。

定理 5 使用 k 的 ϕ-NAF$_w$ 表示来计算 kP，若 $w=2l$，则需要的存储的数目为 $2^{2l-2}+2^{l-2}-1$；若 $w=2l+1$，则需要的存储数目为 $2^{2l-1}+2^{l-2}-1$。

证明

所需存储的个数即为 u_i 除 0 和 ±1 外所有不互为相反数的值的个数。由算法 2 本身很容易得到定理 5 的结果。

4 结束语

对于 $GF(p)$上的椭圆曲线，通过引入特征多项式为 $\phi^2+2=0$ 的自同态 ϕ，Ciet 使用 ϕ-NAF 形式分解整数 k，利用在射影坐标系下 $\phi(p)$计算快于 $2P$ 而获得了标量乘的快速计算。本文对 ϕ-NAF 使用窗口技术，即使用 ϕ-NAF$_w$ 分解整数 k，使用较少的存储，可以获取更快的速度。同时证明分解的正确性(即满足任意 w 个连续的系数至多有一个非零)、存在性和唯一性，估计了分解长度并给出了分解的 Hamming 密度，最后分析了所需要的存储数目。通过以上分析可以发现，在 ϕ-NAF$_w$ 使用少量的存储和长度基本不变的条件下，

(下转第 173 页)