第35卷 第14期 计 算 机 工 程 2009年7月
Vol.35 No.14 Computer Engineering July 2009
·博士论文· 文章编号：1000—3428(2009)14—0001—03 文献标识码：A 中图分类号：TP309

$GF(3^m)$-ECC 算法及其软件实现

端木庆峰[1]，王衍波[1]，张凯泽[1]，雷凤宇[2]
(1. 解放军理工大学通信工程学院，南京 210007；2. 华中科技大学计算机科学与技术学院，武汉 430074)

摘 要：研究 $GF(3^m)$有限域算术、$GF(3^m)$上的椭圆曲线群算术和椭圆曲线密码协议。设计并实现椭圆曲线密码算法库，对各种 $GF(3^m)$-ECC 密码算法进行仿真和性能分析，结果表明 $GF(3^m)$-ECC 算法与 $GF(2^m)$和 $GF(p)$上的 ECC 算法效率相当，可以应用到基于 ECC 的各种安全协议设计中。

关键词：椭圆曲线密码体制；标量乘法；三元域

$GF(3^m)$-ECC Algorithm and Its Software Implementation

DUANMU Qing-feng[1], WANG Yan-bo[1], ZHANG Kai-ze[1], LEI Feng-yu[2]
(1. Institute of Communications Engineering, PLA University of Science and Technology, Nanjing 210007;
2. College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan 430074)

【Abstract】 This paper researches the arithmetic in $GF(3^m)$, the arithmetic on elliptic curve over $GF(3^m)$ and Elliptic Curve Cryptography(ECC) protocol. It designs and implements an EC cryptographic algorithm library, tests and analyzes $GF(3^m)$-ECC algorithms. Results show that $GF(3^m)$-ECC algorithms can provide the same performance as ECC algorithms on $GF(2^m)$ and $GF(p)$, and can be applied into ECC security protocols design.

【Key words】 Elliptic Curve Cryptography(ECC); scalar multiplication; finite field of characteristic three

1 概述

椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)[1]是针对椭圆曲线有理点群离散对数困难问题提出的一种公钥密码体制。由于其上不存在亚指数攻击算法，因此 ECC 能以较小密钥长度达到很高安全性。目前，针对二元域 $GF(2^m)$ 和大素数域 $GF(p)$ 上椭圆曲线密码体制的研究较多，而 $GF(3^m)$ -ECC 的相关研究较少。$GF(3^m)$ -ECC 具有类似 $GF(2^m)$ -ECC 的特点(如计算速度快)以及自身的特性，其上的算术运算效率很高，适合作为安全密码算法的载体。随着 Weil 对和 Tate 对理论研究的不断深入以及基于此设计的各种安全协议的广泛应用，人们开始越来越关注 $GF(3^m)$ 上的超奇异椭圆曲线。本文研究 $GF(3^m)$ 有限域算术运算和椭圆曲线群算术运算，实现 $GF(3^m)$ -ECC 密码算法。

2 椭圆曲线公钥密码体制

设 K 是一个域，K 上仿射坐标系下的 Weierstrass 方程[1]为

$$y^2+a_1xy+a_3=x^3+a_2x^2+a_4x+a_6,\ \ a_1,a_2,a_3,a_4,a_6\in K$$

椭圆曲线为仿射平面 $A^2(K)=K\times K$ 中所有满足方程点和无穷远点 O 的集合，E/K 在平面 $K^2=K\times K$ 中的点称为 K-有理点，E/K 全体 K-有理点(包括 O)记为 $E(K)$。$E(K)$ 及其关于椭圆曲线点“弦和切线”加法运算可以构成一个加法交换群。当 $K=GF(3^m)$ 时，$E(K)$ 称为定义在 $GF(3^m)$ 上的椭圆曲线，其非超奇异椭圆曲线方程为

$$E/GF(3^m): y^2=x^3+ax^2+b,\ a,b\in GF(3^m)$$

令 $P=(x_1,y_1)$，$Q=(x_2,y_2)$，$P\neq O$，$Q\neq O$，$P\neq\pm Q$。

(1)点加法。令 $R=P+Q=(x_3,y_3)$，则 $x_3=k^2-a-x_1-x_2$，$y_3=k(x_1-x_3)-y_1$，其中，$k=(y_2-y_1)/(x_2-x_1)$。

(2) 倍点。令 $R=2P=(x_3,y_3)$，则 $x_3=k^2-a+x_1$，$y_3=k(x_1-x_3)-y_1$，其中，$k=ax_1/y_1$。

(3) $3P$。令 $R=3P=(x_3,y_3)$，则 3 倍点计算公式为 $A=a^{-2}$，$B=a^{-3}$ 和 $C=ab$ (预先计算)，$x_3=A\cdot(x_1^3+b)-C\cdot x_1^3\cdot(x_1^3+b)^{-2}$，$y_3=B\cdot(y_1^3)^3(x_1^3+b)^{-3}-y_1^3(x_1^3+b)^{-1}$。

给定 $E(GF(p^m))$，n 阶点 P 生成的子群为 $\langle P\rangle$，Q 为 $\langle P\rangle$ 中任意一点。椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)就是在已知点 P 和点 Q 的条件下，求满足 $Q=kP$ 的整数 k，$0\leq k\leq n-1$。目前没有有效的多项式和亚指数时间算法可以解决 ECDLP 问题。椭圆曲线公钥密码体制是基于 ECDLP 困难问题构建的。ECC 域参数由 7 元组 $D=(q,FR,a,b,P,n,h)$ 表示，其中，$q=p$ 或 $q=p^m$；FR 为 $GF(q)$ 元素表示方法；域元素 a 和 b 定义 $GF(q)$ 具体椭圆曲线方程 E；P 为 $E(GF(q))$ 子群基点 (x_P,y_P)；n 为点 P 的阶；整数 h 为余因子，$h=\#E(GF(q))/n$；n 为 ECC 主要安全参数，ECC 的密钥长度定义为 n 的比特数。根据域参数 D 可以生成 ECC 的公私钥对。ECC 私钥 d 为区间 $[1,n-1]$ 内的整数，公钥 $Q=(x_Q,y_Q)$ 满足 $Q=dP$，其中，D 和 Q 公开；d 秘密保存。

椭圆曲线 Menezes-Vanstone 加密方案(ECMV)是 ElGamal 系统椭圆曲线版本。假定 Alice 和 Bob 域参数为 D，Alice 的密钥对为 (Q_A,d_A)，Bob 欲向 Alice 发送消息 m。Bob 先将消息 m 编码为 $M=(m_1,m_2)\in Z_p^*\times Z_p^*$，随机选择整数

基金项目：国家自然科学基金资助项目(60703048)
作者简介：端木庆峰(1980－)，男，博士研究生，主研方向：信息安全，密码学，信息隐藏；王衍波，教授；张凯泽，副教授；雷凤宇，博士研究生
收稿日期：2009-02-27 **E-mail：**duanmuziyun@126.com

$k \in [1, n-1]$，确保 $kQ_A = (c_1, c_2) \neq (0,0)$，计算 $R = kP$，$y_1 = c_1 m_1 \bmod p$ 和 $y_2 = c_2 m_2 \bmod p$，则 (R, y_1, y_2) 为加密后的消息。Alice 收到密文后，计算 $H = d_A R = kQ = (c_1, c_2)$，$m_1 = y_1 c_1^{-1} \bmod p$ 和 $m_2 = y_2 c_2^{-1} \bmod p$，则 $M = (m_1, m_2)$，反编码为消息 m。该算法消息扩张率为 2，与一般 ElGamal 系统相当。

椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)由 Scott Vanstone 于 1992 年提出，是数字签名算法(DSA)的椭圆曲线版本。假定签名者 Alice 的域参数 D 和公钥 Q_A 已由标准算法生成，签名验证者 Bob 已知 D 和 Q_A。SHA-1 为 160 bit 的杂凑函数。为对消息 m 签名，Alice 随机选择整数 $k \in [1, n-1]$，计算 $kP = (x_1, y_1)$，$r = x_1 \bmod n$，$e = \text{SHA-1}(m)$ 和 $s = k^{-1}(e + dr) \bmod n$，则消息 m 的签名为 (r, s)。如果 $r = 0$ 或 $s = 0$，就需要重新产生签名，否则会降低签名的安全性。若 $r = 0$，则签名信息 $s = k^{-1}(e + dr) \bmod n$ 不含有私钥 d。若 $s = 0$，则 s^{-1} 不存在(验证时需要)。Bob 收到签名 (r, s) 后对其进行验证，先检查参数 r 和 s 是否位于区间 $[1, n-1]$ 内，然后计算 $e = \text{SHA-1}(m)$，$w = s^{-1} \bmod n$，$u_1 = ew \bmod n$，$u_2 = rw \bmod n$，$u_1 P + u_2 Q_A = (x_1, y_1)$ 和 $v = x_1 \bmod n$，则仅当 $v = r$ 时签名正确。若 $u_1 P + u_2 Q_A = (u_1 + xu_2)P = kP$，$k = s^{-1}(e + dr) \bmod n$，则 $v = r$。为达到与标准数字签名 DSA 同等安全级别，参数 n 至少应达到 160 bit。

3 $GF(3^m)$-ECC 算法研究

椭圆曲线密码方案包括有限域算术运算、椭圆曲线算术运算和高层密码协议 3 个部分。有限域算术运算是 ECC 的基础，包括有限域各种基础运算，如加法、乘法、约减和逆等。椭圆曲线算术运算是 ECC 的核心，包括椭圆曲线群各种基本点和标量乘法运算。高层密码协议是 ECC 的应用，包括各种加密方案、签名方案和密钥协商方案等。上述 3 个部分相互依赖，椭圆曲线算术建立在有限域算术的基础上，ECC 高层协议依赖椭圆曲线算术的高效执行。

3.1 $GF(3^m)$有限域算术

$GF(3^m)$ 元素采用多项式基表示，即 $GF(3^m) = GF(3)[x] / f(x)$，$\forall a \in GF(3^m), a = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0, a_i \in GF(3)$，$f(x)$ 为 $GF(3)$ 上 m 次不可约多项式。

$GF(3^m)$ 中元素的加法和减法较简单，按位进行即可。$GF(3^m)$ 中乘法运算(普通乘法和平方)可以先使用行列扫描算法计算乘积，然后进行多项式约减以求得最终结果，计算过程中可以应用 Karatsuba 和 Ofman 技术进行优化。$GF(3^m)$ 中元素算术运算结果多项式的次数若高于 $m-1$，则需要对其进行约减，即 $\bmod f(x)$。为提高 $GF(3^m)$ 上约减运算的性能，一般选择域多项式 $f(x)$ 为不可约 3 项式 $f(x) = x^m + ax^k + b$，$a, b \in GF(3), m, k \in Z$。$GF(3)$ 首一三项式具有以下 4 种类型：$x^m + x^k + 1$，$x^m + x^k - 1$，$x^m - x^k + 1$ 和 $x^m - x^k - 1$。其中，1 总是 $x^m + x^k + 1$ 的一个根，是可约的。其他 3 个多项式可约性的详细讨论见文献[2]。

类似二元域平方运算，$GF(3^m)$ 上 3 次方运算具有快速算法。$GF(3^m)$ 特征为 3，$\forall a \in GF(3^m), 3a = 0$，则

$\forall A(x) \in GF(3^m)$

$$A(x)^3 = A(x^3) \bmod f(x) = \sum_{i=0}^{m-1} a_i x^{3i} \bmod f(x) =$$

$$\sum_{i=0 \bmod 3}^{3(m-1)} a_{i/3} x^i \bmod f(x) == \left(\sum_{i=0 \bmod 3}^{m-1} a_{i/3} x^i \right) + \left(\sum_{i=0 \bmod 3}^{2m-1} a_{i/3} x^i \right) +$$

$$\left(\sum_{i=0 \bmod 3}^{3(m-1)} a_{i/3} x^i \right) \bmod f(x) = T + U + V \bmod f(x)$$

U 和 V 需要约减域多项式 $f(x)$。由有限域算术理论可知，选择域多项式为不可约 3 项式 $f(x) = x^m + p_t x^t + p_0$，$t < m/3$，$U$ 和 V 只需要 1 次约减就可以使得次数小于 m [3]。

有限域最费时的运算为域逆运算，根据三元域特点推广小素数扩域上各种求逆算法，可以得到 $GF(3^m)$ 上域的逆算法。在实际执行中，可以根据 $GF(3^m)$ 的特点和编程环境进一步优化算法。

3.2 $GF(3^m)$-ECC 标量乘法运算

标量乘法运算是 ECC 最核心的运算，其定义为 $Q = kP = P + \cdots + P$，其中，点 P 为 n 阶基点；k 为满足 $1 \leq k \leq n-1$ 的整数。椭圆曲线标量乘可以分解为椭圆曲线群上一系列基本点的运算组合，因此，提高性能的关键在于如何减少基本点运算数量以及加快基本点运算速度等。不同底域和椭圆曲线选择使椭圆曲线群算术具有不同特点，据此可以优化设计快速标量乘算法。

与 $GF(2^m)$ 类似，$GF(3^m)$-ECC 标量乘 $Q = kP$ 可以采用经典倍点加算法计算。文献[4]推广倍点加，提出 3 倍点加标量乘算法，将整数 k 以基 3 进行展开，即

$$k = \sum_{i=0}^{m-1} k_i 3^i, k_i \in GF(3), k_{m-1} \neq 0$$

其中，$m = \lfloor \log_3 k \rfloor + 1$ 为 k 基 3 展开的位数。k 基 3 展开长度比基 2 展开短，据此设计的 3 倍点加标量乘算法需要 $m-1$ 次 3 倍点和 $H(k)-1$ 次点加运算，$H(k)$ 表示 k 的汉明距离。在整数 k 基 3 展开式中，其非零数字平均密度为 $2/3$，因此，算法平均需要 $2m/3$ 次点加。为了减少点加数量，需进一步减少 k 基 3 展开式中非零数字密度。称有符号基 r 表示 $k = (k_{m-1}, k_{m-2}, \cdots, k_0)$ 为基 r 的非邻接表示型(rNAF)，若满足条件：(1) $k_j \cdot k_{j-1} = 0, j = 0, 1, \cdots, m$，定义 $k_m = k_{-1} = 0$；(2)最左端非零数字为正整数；(3) $d_j \in D_r = \{0, \pm 1, \pm 2, \cdots, \pm(r^2 - 1)/2\} \setminus \{\pm 1r, \pm 2r, \cdots, \pm\lfloor (r-1)/2 \rfloor r\}$，整数 k 基 3 rNAF 展开型，$k = \sum_{i=0}^{m-1} k_i 3^i, k_i \in D$，其展开数字集为 $D = \{0, \pm 1, \pm 2, \pm 4\}$。整数 k 基 3rNAF 展开式中非零系数的密度为 $(r-1)/(2r-1) = 2/5$。据此可以设计整数 k 基 3rNAF 标量乘算法，进一步提高 $GF(3^m)$-ECC 标量乘效率。算法需要预计算 $2P$ 和 $4P$，因此，该算法平均需要 2 次倍点、$\lfloor \log_3 k \rfloor + 1$ 次 3 倍点运算和 $2(\lfloor \log_3 k \rfloor + 1)/5$ 次点加运算。

算法 1 计算整数 k 基 3rNAF 展开算法

输入 正整数 k

输出 3rNAF(k) = (k_{m-1}, k_{m-2},⋯,k_0)

i=0

当 k≥1 时，重复执行

　若 k mod 3 = = 0，则 k_i = 0；否则 k_i = k mod 9；

　若 k_i > 4，则 k_i = k_i–9，k =k-k_i；

　k = k/3，i = i + 1

返回 (k_{m-1}, k_{m-2},⋯,k_0)

算法 2 基于整数 k 基 3rNAF 标量乘算法

输入 $k = (k_{m-1}, \cdots, k_1, k_0)_3$，$P$

输出 kP

对于 i∈{1,2,4}，预计算 P_i = iP；

Q = P

当 k≥1 时，重复执行

　若 k mod 3 = = 0，则 k_i = 0，

否则 k_i=k mod 9；如果 k_i>4，

则 $k_i = k_i$–9，k = k - k_i；

若 $k_i > 0$，则 $Q = Q + P_k$ ；

若 $k_i < 0$，则 $Q = Q–P_{-k}$ ；

k = k/3，Q = 3Q，i = i + 1

返回 Q

4 软件实现和性能分析

椭圆曲线密码方案的实现较复杂，包括从有限域算术运算到高层密码协议的一系列函数和许多辅助功能模块。因此，需要设计一套椭圆曲线密码算法库，该算法库能灵活地定制 ECC 参数以适应不同应用和测试需要，并能方便地进行各种 EC 协议开发。本文以 NTL[5]算法库为基础，使用标准 C++ 语言对 ECC 算法库进行实现。整个库按椭圆曲线密码系统划分为 3 个层次，即底层有限域算术层、ECC 算术层和高层协议层，其系统结构见图 1。分层次模块化的设计使该算法库独立于特定有限域和曲线，能方便地实现任意类型 ECC 密码系统，并可以根据需要修改任意层功能而不影响其他层，因此，具有较高可扩展性和灵活性。

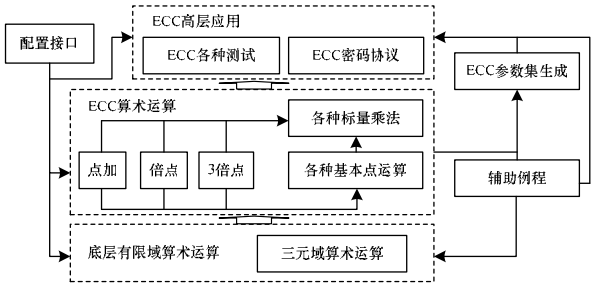

图 1 ECC 系统软件结构

以 ECC 算法库为测试平台，分别测试和分析 $GF(3^m)$ 有限域算术运算、$GF(3^m)$ 椭圆曲线群算术运算和基于 $GF(3^m)$ 椭圆曲线密码协议的性能。测试平台为 Pentium 4 2.66 GHz 处理器，256 MB 内存，Windows XP 操作系统，编程环境为 VC++6.0。考虑到客观性，对每个算法的计时采用平均分摊法，即随机产生 100 000~500 000 个测试样本，计算算法每次执行所需平均时间。

先测试 $GF(3^m)$ 有限域各种算术运算。根据低、中、高 3 个安全强度分别选择有限域 $GF(3^{97})$, $GF(3^{239})$ 和 $GF(3^{353})$ 作为测试对象，其上域多项式分别选择不可约 3 项式 $x^{97}+x^{12}-1$, $x^{239}+x^{24}-1$ 和 $x^{353}+x^{142}-1$。测试算法为加减法、乘法、平方、3 次方以及几乎可逆求逆算法。各种算术的运算性能见表 1，其中，乘法(K-O)表示采用 Karatsuba-Ofman 技术的域乘法，逆运算使用经典几乎可逆算法。可以看出，$GF(3^m)$ 上 3 次方运算比乘法和平方运算的效率高很多，平方运算约为普通乘法的 4/5，设计算法时应尽量使用 3 次方运算。与其他有限域类似，域逆运算虽采用了优化技术，但仍然是有限域最费时的运算。

表 1 $GF(3^m)$算术运算性能 μs

有限域运算	$GF(3^{97})$	$GF(3^{239})$	$GF(3^{353})$
加法	0.04	0.06	0.07
乘法	10.45	39.30	77.10
乘法(K-O)	9.24	30.10	61.30
平方	7.24	27.60	56.20
3 次方	0.67	2.45	4.14
逆运算	33.59	115.35	198.12

然后对 $GF(3^m)$ 椭圆曲线算法进行测试，选择 $GF(3^{97})$ 上椭圆曲线 $E: y^2 = x^3 + x^2 + b$，其中，b = 0x5C6A21D1BF0967068295B8EAA7253DD2BD7A72 。该椭圆曲线群的阶为 $\#E(GF(3^m))$ = 19088056323407827075424645001545815478748968937 = 3× 6362685441135942358474881667181938492916322979 ，最后一个因子为大素数。由于选择 $GF(3^m)$ 上适合密码应用的椭圆曲线很困难，因此本文使用文献[4]提出的椭圆曲线。测试的基本点运算包括普通点加、倍点、3 倍点和 kP 运算，其中，kP 运算分别采用倍点加标量乘算法；3 倍点加标量乘算法和 3rNAF 展开标量乘算法，执行效率见表 2。可以看出，在仿射坐标系下，$GF(3^m)$ 上椭圆曲线 3 倍点效率较高，接近 2 倍点，据此设计的 3 倍点加标量乘算法由于具有更短计算长度，因此效率明显高于 2 倍点加算法。3rNAF 展开标量乘采用整数基 3rNAF 展开，减少点加数量，其性能比 3 倍点加提高近 24%。

表 2 $GF(3^{97})$-ECC 算术运算性能 μs

$GF(3^{97})$-ECC 点运算	时间
点加法	50.21
倍点	52.61
3 倍点	64.45
kP (倍点加)	13 134.57
kP(3 倍点加)	11 498.36
kP(3rNAF 展开算法)	8 723.24

最后测试 $GF(3^m)$ -ECC 密码协议的执行效率，密码协议包括公钥对生成算法、ECMV 和椭圆曲线数字签名算法 ECDSA。协议使用的标量乘算法为仿射坐标系 3 倍点加标量乘算法。基于 $E(GF(3^m))$密码协议性能如表 3 所示。

表 3 基于 $E(GF(3^m))$的密码协议性能 ms

ECDSA 签名算法($E(GF(3^{97}))$	时间
ECC 公钥对生成	17.48
ECMV 加密	27.35
ECMV 解密	18.48
ECDSA 签名生成算法	19.25
ECDSA 签名验证算法	23.76

从上述测试数据可以看出，小素数扩域 $GF(3^m)$ 上椭圆曲线密码算法的效率较高，可以恰当地应用到 ECC 各种安全协议中。

5 结束语

小素数扩域椭圆曲线具有其他有限域不可比拟的优点，它能比传统有限域提供更多、更灵活的密码选择方案以及较高安全性。$GF(3^m)$ 作为 $GF(p^m)$ 的一种特殊类型，定义于其上的椭圆曲线密码算法更优越。$GF(3^m)$ -ECC 密码算法的效率能满足各类安全应用的需要，因此，可以作为 $GF(2^m)$ -ECC 和 $GF(p)$ -ECC 的替代方案。下一步工作将研究如何优化 $GF(3^m)$ -ECC 核心标量乘法运算的性能。

参考文献

[1] Menezes A J. Elliptic Curve Public Key Cryptosystems[M]. Boston, USA: Kluwer Academic Publishers, 1993.

[2] Loidreau P. On the Factorization of Trinomials over F3[EB/OL]. (2000-02-18). http://www.inria.fr/RRRT/RR-3918.html.

[3] Bertoni G, Guajardo J, Kumar S, et al. Efficient $GF(p^m)$ Arithmetic Architectures for Cryptographic Applications[C]//Proceedings of CTRSA'03. Berlin, Germany: Springer-Verlag, 2003: 158-175.

[4] Smart N P, Westwood E J. Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three[J]. Applicable Algebra in Engineering, Communication and Computing, 2003, 13(6): 485-497.

[5] Shoup V. NTL: A Library for Doing Number Theory[EB/OL]. (2003-09-01). http://shoup.net/ntl/.

编辑 陈 晖