

# GF(p)上安全椭圆曲线产生算法

侯爱琴<sup>1,3</sup>, 辛小龙<sup>2</sup>, 杨世勇<sup>3</sup>

(1. 西北大学信息科学与技术学院, 西安 710069; 2. 西北大学数学系, 西安 710069;

3. 西安电子科技大学 ISN 国家重点实验室, 西安 710071)

**摘要:** 研究素数域 GF(p)(p>3)上的椭圆曲线, 讨论阶为素数的椭圆曲线的产生算法, 在此基础上, 分析阶为 2 个素数之积的椭圆曲线产生问题, 并提出一种 GF(p)上安全椭圆曲线的产生算法, 给出椭圆曲线及其全体有理点的随机产生实例。仿真实验结果表明, 该算法是有效可行的。

**关键词:** 椭圆曲线群; 阶; 基点

## Secure Elliptic Curve Generating Algorithm over GF(p)

HOU Ai-qin<sup>1</sup>, XIN Xiao-long<sup>2</sup>, YANG Shi-yong<sup>3</sup>

(1. School of Information Science & Technology, Xi'an 710069; 2. Department of Mathematics, Northwest University, Xi'an 710069;

3. ISN National Key Lab, Xidian University, Xi'an 710071)

**【Abstract】** This paper analyzes the elliptic curves over prime field GF(p), while p is greater than 3. It discusses an algorithm to generate an elliptic curve with a prime order. On basis of this, the problems for generating an elliptic curve with an order which equals to the product of two prime numbers are studied. A secure elliptic curve generating algorithm over GF(p) is proposed. It gives some examples for producing an elliptic curve and all the points on this elliptic curve under these two circumstances. Simulation experimental results show this algorithm is effective and feasible.

**【Key words】** elliptic curve group; order; base point

### 1 概述

椭圆曲线参数的选择是椭圆曲线密码亟待解决的问题, 是实现椭圆曲线密码(ECC)的前提和关键。参数的选择要使得 ECC 能抵抗所有已知的攻击, 另外还要考虑实现的问题。

椭圆曲线的产生, 目前主要有 2 类方法: 随机法产生椭圆曲线和构造法产生椭圆曲线。为防止针对特殊类型椭圆曲线的攻击, 最好选择随机产生法。因为随机曲线满足已知的同构攻击条件的概率非常小且可忽略。文献[1]给出源于 ANSI X9.62 标准的在素域随机产生椭圆曲线的算法, 该算法安全性很高, 但实现也较复杂。

本文讨论素数域 GF(p)上椭圆曲线参数的产生问题, 给出阶为素数以及阶为 2 个素数乘积 2 种情况下随机产生安全的椭圆曲线上所有点的算法。

### 2 椭圆曲线参数

#### 2.1 安全的椭圆曲线

$T = \langle P, a, b, G, n, h \rangle$  为椭圆曲线参数组, 描述了  $p > 3$  的素数域 GF(p)上的椭圆曲线 E 上的点满足方程:  $y^2 = x^3 + ax + b \pmod{p}$ , 基点为 G, 基点的阶为 n, 余因子为 h。该椭圆曲线上所有的点构成加法阿贝尔群。

一条良好的适于构建密码体制的有限域上的椭圆曲线应当满足下面的安全性约束<sup>[1]</sup>:

(1)抵抗 Pohlig-Hellman 和 Pollard's rho 攻击。椭圆曲线 E 上的有理点数 N 必须能够被足够大的素数 n 整除( $n > 2^{160}$  且  $n > 4\sqrt{p}$ ), 并且 N 应为素数或近似素数,  $N = nh$ , 其中, n 为素数, h 非常小( $h = 1, 2, 3$ )。

(2)抵抗同构攻击。为避免攻击素域异常曲线, 应保证阶

$N \neq p$ ; 为避免 Weil 和 Tate 配对攻击, 应该保证对于所有的  $1 \leq k \leq C$ , n 不被  $q^k - 1$  整除, 其中 C 应足够大, 使  $GF(q^C)$  上的 DLP 不可解(若  $n > 2^{160}$ , 则  $C = 20$  就足够了)。

#### 2.2 椭圆曲线的阶

有限域 GF(p)上的椭圆曲线群的阶等于该椭圆曲线上点的数目 N。由 Hasse 定理:  $N = p + 1 - t$ , 其中,  $|t| \leq 2\sqrt{p}$ 。

当 N 与 p 满足该定理的不等式时就存在一条有 N 个点的模 p 椭圆曲线 E, 且 N 与 p 是同量级的<sup>[2]</sup>。

当 p 较小时, 可以利用穷举的方法求出所有点。但对于一般情况 p 很大时, 要确切计算椭圆曲线解点 N 的准确值比较困难, 目前能够有效计算 p 大到  $10^{409}$  的 GF(p)上的椭圆曲线解点数和 m 大到 601 的 GF(2<sup>m</sup>)上的椭圆曲线解点数<sup>[1]</sup>。

实际中确定椭圆曲线的阶, 通常用以下 3 种方法:

(1)子域曲线法: 先直接计算有限域的子域上的椭圆曲线点数, 进而可对其乘以一个因子, 若乘积在 Hasse 区间  $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$  内, 就可确定椭圆曲线的点数为该乘积。因为椭圆曲线的点数位于 Hasse 区间内且是子域上的椭圆曲线点数的倍数<sup>[1]</sup>。

(2)复乘(CM)方法: 该方法选择一个满足安全性约束的阶 N, 构造一个阶为 N 的椭圆曲线, 具体算法见文献[1]。

(3)SEA 点计数法: 是计算任意椭圆曲线 E 的点数的多项

**基金项目:** 陕西省自然科学基金资助项目(2007A19); 陕西省科技攻关计划基金资助项目(2005K04G10)

**作者简介:** 侯爱琴(1967—), 女, 讲师、硕士, 主研方向: 椭圆曲线密码, 信息安全; 辛小龙, 教授、博士; 杨世勇, 副教授、博士

**收稿日期:** 2009-08-10 **E-mail:** houaiqin@eyou.com

式时间算法。SEA 算法是已知最好的求解任意素域和 OEF 上椭圆曲线的点计数方法，对实际密码应用中的  $p$ ，该算法的运行时间只需要几分钟。对于任意素域  $GF(p)$  的椭圆曲线的阶  $N = p+1-t$ ，粗略地均匀分布于 Hasse 区间。该算法先对小素数  $l_i$  计算  $t_i \equiv t \pmod{l_i}, i=1,2,\dots,s$ ，且  $\prod_{i=1}^s l_i > 4\sqrt{p}$ ，然后用中国剩余定理计算  $t$ 。

### 2.3 椭圆曲线上点的阶

设  $E(GF(p))$  是素域  $GF(p)$  上的椭圆曲线群， $G$  是该群上的一点，则定义满足  $nP = \infty$  ( $\infty$  为无穷远点) 的最小正整数  $n$  为点  $G$  的阶。

一般地，群中任意点的阶与该群的阶比例相关<sup>[1]</sup>，即点的阶  $n$  为群的阶  $N$  的一个因子。

### 2.4 椭圆曲线的基点

基点  $G(x, y)$  是满足椭圆曲线方程  $y^2 \equiv x^3 + ax + b \pmod{p}$ ，并且阶为素数的椭圆曲线上的点。

ECC 参数选择中，在确定了安全的椭圆曲线  $y^2 \equiv x^3 + ax + b \pmod{p}$  之后，基点  $G$  的选择也是非常重要的。基点的选择必须在满足安全性要求的情况下，选择点乘效率最高的基点。

选择基点的坐标，常有 2 种方法：

(1)平方根算法，选取基点横坐标整数  $x$  使  $y^2 \equiv x^3 + ax + b \pmod{p}$  是模  $p$  的平方剩余，令  $A = x^3 + ax + b$ ，则基点纵坐标  $y \equiv \sqrt{A} \pmod{p}$ 。再计算点  $(x, y)$  的阶，若其为素数且为椭圆曲线群的阶  $N$  的因子，则该点可作为基点。

(2)随机算法，设在椭圆曲线上一点  $G(m, l)$ ，一定满足椭圆曲线方程即： $l^2 \equiv m^3 + am + b \pmod{p}$ ，变形得  $b \equiv l^2 - m^3 - a \cdot m \pmod{p}$ 。这样，将椭圆曲线参数  $p, a, b$  的随机选取，转变为随机选取参数  $p, a, m, l$ 。然后可计算点  $G(m, l)$  的阶  $n$ ，若  $n$  为素数则该点可作基点。

## 3 随机产生椭圆曲线

椭圆曲线的参数  $p, a, b$  决定了椭圆曲线群  $E(GF(p))$  的阶  $N$ 。根据群论中拉格朗日定理的推论可知椭圆曲线群的阶为素数或若干素数之积，即  $N = hn$ ，其中， $h$  为余因子可取 1, 2, 3 等小素数， $n$  为基点  $G$  的阶，所以， $n$  只能取椭圆曲线群的阶  $N$  的某个素因子或者当  $N$  本身为素数时取  $N$ 。

下文就  $h$  的不同取值，分别讨论随机椭圆曲线及基点如何产生。

### 3.1 $h=1$ 时随机椭圆曲线及其全体点的产生算法

当余因子  $h=1$  时， $N = hn = n$ ，椭圆曲线群的阶  $N$  等于基点  $G$  的阶  $n$  且都为素数。因为阶为素数的有限群不存在真子群且为循环群，所以椭圆曲线群里每一个点都可作为基点。这种情况下，基点选定的同时也选定了椭圆曲线<sup>[3-4]</sup>。

$h=1$  时得出素域  $GF(p)$  上的随机椭圆曲线  $y^2 \equiv x^3 + ax + b \pmod{p}$  及其基点  $G(m, l)$  的产生算法如下：

- (1)随机选择素数  $p$ ；
- (2)随机选择正整数  $a, m, l$ ，其中，基点  $G(m, l)$ ；
- (3)计算  $b \equiv l^2 - m^3 - a \cdot m \pmod{p}$ ；
- (4)判断若  $4a^3 + 27b^2 \equiv 0 \pmod{p}$  或  $a > p$ ，则返回(1)；
- (5)利用 SEA 算法或子域曲线法计算该椭圆曲线的阶  $N$ ；
- (6)如果阶  $N$  不为素数或不满足安全要求或等于  $p$ ，则返回(1)；
- (7)椭圆曲线的阶  $N$  为素数，则基点的阶  $n = N$ ，余因子

$h = N/n = 1$ ；

(8)输出椭圆曲线参数为  $T = (p, a, b, G, n, h)$ ；

(9)由基点  $G(m, l)$  点乘则生成椭圆曲线群中所有点。

### 3.2 $h>1$ 时随机椭圆曲线及其全体点的产生算法

当余因子为  $h>1$  的小素数时，椭圆曲线群的阶  $N = hn$  为合数，这时，存在一个阶为  $n$  的子循环群和一个阶为  $h$  的子循环群<sup>[1]</sup>。

**引理** 设  $n_1$  与  $n_2$  是不同的素数， $G$  是  $n_1 n_2$  阶的群，且  $G_1$  和  $G_2$  分别是  $G$  的  $n_1$  和  $n_2$  阶元素，则  $G_1 + G_2$  必为  $n_1 n_2$  阶元素，从而  $G$  必为一循环群。

证明：

(1)假设  $G_1 + G_2$  为  $n_1$  阶元，则  $n_2(G_1 + G_2) = \infty$ ，即  $n_2 G_1 + n_2 G_2 = \infty$ 。因为  $n_2 G_2 = \infty$ ，所以  $n_2 G_1 = \infty$ ，即  $n_1 | n_2$ ，这与  $n_2$  是素数矛盾，可知  $G_1 + G_2$  不是  $n_1$  阶元。

(2)同理可证  $G_1 + G_2$  不是  $n_2$  阶元。

综上可证， $G_1 + G_2$  必为  $n_1 n_2$  阶元素。

不妨设点  $G_1(x_1, y_1)$  为椭圆曲线群的  $n$  阶子循环群中一个元素，点  $G_2(x_2, y_2)$  为椭圆曲线群的  $h$  阶子循环群中一个元素，则该 2 点坐标一定满足椭圆曲线方程，则有：

$$y_1^2 \equiv x_1^3 + ax_1 + b \pmod{p}$$

$$y_2^2 \equiv x_2^3 + ax_2 + b \pmod{p}$$

由方程组可计算出  $a, b$  这 2 个参数。令

$$G(x_0, y_0) = G_1(x_1, y_1) + G_2(x_2, y_2)$$

根据引理， $G(x_0, y_0)$  必为  $N = hn$  阶的点，则  $G(x_0, y_0)$  可作椭圆曲线的生成元，椭圆曲线的全体有理点就产生了。

下面给出  $h>1$  时素域随机椭圆曲线  $y^2 \equiv x^3 + ax + b \pmod{p}$  及其基点  $G$  的产生算法：

- (1)随机选择素数  $p$ ；
- (2)随机选择正整数  $x_1, y_1, x_2, y_2$ ，分别为椭圆曲线上 2 点  $G_1(x_1, y_1)$ ， $G_2(x_2, y_2)$  的坐标；
- (3)解方程组
 
$$\begin{cases} y_1^2 \equiv x_1^3 + ax_1 + b \pmod{p} \\ y_2^2 \equiv x_2^3 + ax_2 + b \pmod{p} \end{cases}$$

并求出  $a, b$  参数；

(4)判断若  $4a^3 + 27b^2 \equiv 0 \pmod{p}$  或  $a > p$ ，则返回(1)；

(5)判断  $G_1(x_1, y_1)$  的阶是否为素数  $n$  及  $G_2(x_2, y_2)$  的阶是否为素数  $h$ ，不为素数或不满足安全要求或为  $p$ ，则返回(1)；

(6)计算阶为  $N = hn$  的生成元  $G(x_0, y_0) = G_1(x_1, y_1) + G_2(x_2, y_2)$ ；

(7)椭圆曲线的阶为  $N = hn$ ，基点  $G_1(x_1, y_1)$  的阶为  $n$ ，余因子  $h$ ，输出椭圆曲线参数为  $T = (p, a, b, G, n, h)$ ；

(8)由生成元即  $G(x_0, y_0)$  进行点乘运算则生成椭圆曲线群中所有点。

## 4 随机椭圆曲线及其全体点的产生实例

### 4.1 $h=1$ 时随机椭圆曲线及其全体点的产生实例

为便于说明问题，随机选择小素数  $p = 37$  及  $a = 1, m = 0, l = 4$  的椭圆曲线  $E(GF(p))$ ： $y^2 \equiv x^3 + x + b$ ，计算  $b \equiv l^2 - m^3 - a \cdot m \pmod{p} = 16$ ，利用子域曲线法计算该椭圆曲线的阶  $N = 41$ 。因为 41 是素数，基点  $G$  的阶  $n$  等于椭圆曲线群的阶  $N$ ，所以  $E(GF(p))$  是循环群，群中除了点  $0(\infty, \infty)$  外任何

一点都可作基点(即生成元)<sup>[1,5]</sup>。

以基点  $G(0,4)$  为生成元, 用点乘法生成椭圆曲线群的全元素如下:

- $1P = (0, 4), 2P = (11, 27), 3P = (16, 13),$
- $4P = (31, 4), 5P = (6, 33), 6P = (4, 26),$
- $7P = (17, 32), 8P = (19, 30), 9P = (21, 14),$
- $10P = (32, 16), 11P = (30, 31), 12P = (3, 34),$
- $13P = (23, 25), 14P = (7, 25), 15P = (2, 27),$
- $16P = (10, 29), 17P = (24, 10), 18P = (20, 28),$
- $19P = (14, 31), 20P = (22, 17), 21P = (22, 20),$
- $22P = (14, 6), 23P = (20, 9), 24P = (24, 27),$
- $25P = (10, 8), 26P = (2, 10), 27P = (7, 12),$
- $28P = (23, 12), 29P = (3, 3), 30P = (30, 6),$
- $31P = (32, 21), 32P = (21, 23), 33P = (19, 7),$
- $34P = (17, 5), 35P = (4, 11), 36P = (6, 4),$
- $37P = (31, 33), 38P = (16, 24), 39P = (11, 10),$
- $40P = (0, 33), 41P = (\infty, \infty)$

该椭圆曲线参数组为  $T = (p, a, b, G, n, h) = (37, 1, 16, [0, 4], 41, 1)$ 。

#### 4.2 $h > 1$ 时随机椭圆曲线及其全体点的产生实例

对素域椭圆曲线  $y^2 = x^3 + ax + b$ , 取  $p = 89$ , 设 2 点  $G_1(0,3)$ ,  $G_2(10,0)$  在椭圆曲线上, 即 2 点坐标一定满足椭圆曲线方程, 则有下列方程组:

$$\begin{cases} 3^2 = 0^3 + a \cdot 0 + b \pmod{89} \\ 0^2 = 10^3 + a \cdot 10 + b \pmod{89} \end{cases}$$

解之得椭圆曲线参数  $a = -3, b = 9$ , 且  $4a^3 + 27b^2 \equiv 32 \neq 0 \pmod{p}$  满足非奇异性要求, 因而构造的椭圆曲线方程为  $y^2 = x^3 - 3x + 9 \pmod{89}$ ; 然后, 计算  $G_1(0,3)$  的阶为  $n = 19$ , 计算  $G_2(10,0)$  的阶为  $h = 2$ , 2 点的阶均为素数, 所以, 它们可分别生成阶为  $n = 19$  的椭圆曲线的子循环群以及阶为  $h = 2$  的子循环群; 因为  $G_1(0,3)$  的阶为  $n = 19$ ,  $G_2(10,0)$  的阶为  $h = 2$ , 则相加点  $G(x_0, y_0) = G_1(0,3) + G_2(10,0) = (7,8)$  的阶为  $N = hn = 38$ , 该点可以作阶为  $N = hn = 38$  的椭圆曲线群的生成元。

下面由该生成元  $G(7,8)$  产生椭圆曲线群的所有元素:

- $1P = (7, 8), 2P = (67, 75), 3P = (36, 59),$
- $4P = (2, 10), 5P = (41, 59), 6P = (21, 60),$

- $7P = (53, 50), 8P = (12, 30), 9P = (68, 44),$
- $10P = (32, 75), 11P = (25, 47), 12P = (79, 14),$
- $13P = (37, 34), 14P = (77, 50), 15P = (73, 77),$
- $16P = (18, 25), 17P = (48, 50), 18P = (0, 86),$
- $19P = (10, 0), 20P = (0, 3), 21P = (48, 39),$
- $22P = (18, 64), 23P = (73, 12), 24P = (77, 39),$
- $25P = (37, 55), 26P = (79, 75), 27P = (25, 42),$
- $28P = (32, 14), 29P = (68, 45), 30P = (12, 59),$
- $31P = (53, 39), 32P = (21, 29), 33P = (41, 30),$
- $34P = (2, 79), 35P = (36, 30), 36P = (67, 14),$
- $37P = (7, 81), 38P = (\infty, \infty)$

### 5 结束语

本文讨论在椭圆曲线阶为素数情况下, 椭圆曲线上每个点都可作为生成元, 椭圆曲线群中所有的元素皆由此生成元生成, 研究椭圆曲线阶为 2 个素数乘积时安全的椭圆曲线及其群中所有元素的产生方法。此时, 椭圆曲线群的阶为  $N = hn$ , 必然存在一个阶为  $n$  的子循环群和一个阶为  $h$  的子循环群, 可证椭圆曲线也是一个阶为  $N = hn$  的循环群。先找出阶为  $n$  的子循环群中的一个元素  $G_1(x_1, y_1)$  和阶为  $h$  的子循环群中的一个元素  $G_2(x_2, y_2)$ , 这 2 个元素做点加运算得到的一点  $G(x_0, y_0)$  必为椭圆曲线群中的元素。已证椭圆曲线是个循环群, 所以,  $G(x_0, y_0)$  可作生成元, 进而产生椭圆曲线上所有的有理点。

#### 参考文献

- [1] Darrel H, Alfred M, Scott V. 椭圆曲线密码学导论[M]. 张焕国, 译. 北京: 电子工业出版社, 2005.
- [2] Trappe W, Washington L C. 密码学概论[M]. 邹红霞, 许朋文, 李勇奇, 译. 北京: 人民邮电出版社, 2004.
- [3] 王春生, 姚云飞. 椭圆曲线上基的选择与实现[J]. 大学数学, 2006, 22(2): 89-93.
- [4] 侯爱琴, 高宝建, 辛小龙. 信息明文嵌入椭圆曲线的改进算法及实现[J]. 计算机软件与应用, 2008, 25(7): 58-69.
- [5] 库俊华, 游林, 王升国. Maple 在椭圆曲线密码体制中的应用[J]. 计算机工程, 2007, 33(6): 98-100.

编辑 陈文

(上接第 137 页)

### 3 结束语

本文提出的隐写算法通过在光滑区域和边界区域嵌入较多的隐藏信息而在中间地带嵌入较少的信息, 大大提高了数据隐藏的容量。实验证明了该算法的有效性。

#### 参考文献

- [1] Wu Dachun, Tsai W H. A Steganographic Method for Images by Pixel Value Differencing[J]. Pattern Recognition Letters, 2003, 24(9/10): 1613-1626.
- [2] Wu Hsien-Chu, Wu Nan, Tsai C S, et al. Image Steganographic Scheme Based on Pixel Value Differencing and LSB Replacement Methods[J]. IEE Proceedings: Vision Image and Signal Processing,

2005, 152(5): 611-615.

- [3] Lee Chih-Chiang, Wu Hsien-Chu, Tsai C S, et al. Adaptive Lossless Steganographic Scheme with Centralized Difference Expansion[J]. Pattern Recognition, 2008, 41(6): 2097-2106.
- [4] Tian Jun. Reversible Data Embedding Using a Difference Expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890-896.
- [5] 王威娜, 张新鹏, 王朔中. 针对边缘匹配嵌入法的密写分析及嵌入率估计[C]//第十二届全国图像图像学学术会议论文集. 北京: [出版者不详], 2005.

编辑 张帆