素域上安全椭圆曲线的选取

王红珍[1,2],李竹林[1,2]
(1.延安大学 计算机学院,陕西 延安 716000;
2.延安大学 软件研究与开发中心,陕西 延安 716000)

摘 要:椭圆曲线密码体制基于其长度小、安全性高等特点在公钥密码系统中得到广泛应用,其安全性是基于椭圆曲线上的离散对数的难解性,它还依赖于椭圆曲线的选择。建立椭圆曲线密码体制的首要问题之一就是产生能够抵抗已有算法攻击的安全的椭圆曲线。文中主要研究素域上的椭圆曲线,归纳椭圆曲线选取的安全准则以及用随机法产生安全椭圆曲线,给出一种产生安全椭圆曲线域参数的方法和域参数的验证算法。椭圆曲线的安全是保证密码体系安全的重要因素。

关键词:椭圆曲线密码体制;安全椭圆曲线;选取准则;离散对数
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)07-0140-03

Selection of Security Elliptic Curve over Prime Fields

WANG Hong-zhen[1,2], LI Zhu-lin[1,2]
(1. Department of Computer Science, Yan'an University, Yan'an 716000, China;
2. Software R&D Center, Yan'an University, Yan'an 716000, China)

Abstract: Elliptic curve cryptosystem based on its length, high security in the public key encryption system is applied widely. Its security is based on the elliptic curve discrete logarithm calculation difficulty, but also depend on the elliptic curve selection. Establishment of elliptic curve cryptography is the most important issue is to generate attacks on the security of the existing algorithms elliptic curve. It studies the prime fields of elliptic curves, elliptic curve summarized the safety criteria for selection, randomly generated secure elliptic curves, introduced a method of generating secure elliptic curve domain parameters and the authentication algorithm of domain parameters. Therefore, elliptic curve cryptography security is to ensure the safety of important factors.

Key words: elliptic curve cryptography; security elliptic curve; selection rule; discrete logarithm

0 引 言

椭圆曲线理论是建立在代数几何、数论等多个数学分支方面的一个交叉点,它一直被认为是纯理论学科。1985年,数学家 Victor Miller 和 Neal Koblitz 分别独立地提出了椭圆曲线(ECC)密码算法,ECC 的安全性是基于椭圆曲线上离散对数的 NP 问题[1]。椭圆曲线密码算法是一种安全性高、算法实现性能好的公钥加密算法[2]。目前,已有的对于椭圆曲线密码算法有效的攻击算法有穷搜索法、Pollard ρ 算法、小步大步法、Pohlig-Hellman 算法、分布式 Pollard ρ 算法、Pollard's Lambda 算法、Xedni 算法、多重对数法等,求解难度大多是指数级的。ECC 的安全性离不开椭圆曲线的选择。因而,建立椭圆曲线密码体制的最主要问题就是产生可以抵抗已有算法攻击的安全椭圆曲线。

收稿日期:2011-12-12;**修回日期**:2012-03-15
基金项目:陕西省教育科研项目(2010JK904)
作者简介:王红珍(1973-),女,陕西子长人,实验师,硕士,研究方向为软件体系结构及应用。

1 ECC 的数学基础

1.1 Abel 群

群 G 有时记做 $\{G,\cdot\}$,是定义了一个二元运算的集合,这个二元运算可表示为 $\cdot$,G 中每一个序偶 (a,b) 通过运算生成 G 中的元素 $(a\cdot b)$,并满足以下公理:

(1)封闭性:如果 a 和 b 都属于 G,则 $a\cdot b$ 也属于 G。

(2)结合律:对于 G 中任意元素 a、b、c,$a\cdot(b\cdot c)=(a\cdot b)\cdot c$ 都成立。

(3)单位元:G 中存在一个元素 e,对于 G 中任意元素 a,都有 $a\cdot e=e\cdot a=a$ 成立。

(4)逆元:对于 G 中任意元素 a,G 中都存在一个元素 a',使得式 $a\cdot a'=a'\cdot a=e$ 成立。

(5)交换律:对于 G 中任意的元素 a、b,都有 $a\cdot b=b\cdot a$ 成立。

1.2 域表示

(1)素数域:素数域 F_p 是由整数集合 $\{0,1,2,3,\cdots,p-1\}$ 构成,这里的每一个整数都能用一个长度恰好

为 $t=\lceil \log_2 p \rceil$ 的二进制数来表示,也就是由整数的二进制来表示并且在它的左边添加若干个0来组成。其中 F_p 的元素满足以下的算术运算法则:

加法:如果 $a,b \in F_p$,那么 $a+b=r$,这里的 r 是被 p 除所得剩余,且 $0 \leqslant r \leqslant p-1$。

乘法:如果 $a,b \in F_p$,那么 $a \bullet b=s$,这里的 s 是被 p 除所得剩余,且 $0 \leqslant s \leqslant p-1$。

求逆:如果 a 是 F_p 中的非零元素,那么 a 模 p 的逆元记为 a^{-1},是唯一的整数 $c \in F_p$,c 满足 $a \bullet c=1$。

(2)二进制域:特征值为2的有限域 F_2,被称为二进制域,这样则可以看作有限域 F_2 上的 m 维空间。

1.3 椭圆曲线的定义

定义1　有限域上椭圆曲线的定义:假设 F_q 为一个有限域,并且 F_q 上的椭圆曲线能满足 Weierstrass 方程:

$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6(a_1,a_2,a_3,a_4,a_6 \in F_q)$

的所有解 (x,y) 与无穷远点 O 构成的非空集合。

定义2　素数域上的椭圆曲线的定义则是:设 $q>3$ 是奇素数,在 F_q 上的椭圆曲线 $E:y^2=x^3+ax+b$ 由一个满足同余方程 $y^2 \equiv x^3+ax+b \bmod q$ 的全部解 $(x,y) \in F_q \times F_q$ 和一个无穷远点 O 组成,这里的 $a,b \in F_q$ 是二个满足 $4a^3+27b^2 \neq 0 \bmod q$ 的常数。

2 安全椭圆曲线选取的相关问题

2.1 椭圆曲线的参数

在设计椭圆曲线加解密的实现方案时,首先要考虑的是根据给出的椭圆曲线域的参数来确定所选椭圆曲线。然而在 IEEE P1363 标准中,它所定义的椭圆曲线域的参数是一个七元组:$T=(q,FR,a,b,G,n,h)$,在这里 q 表示有限域 $GF(q)$ 的域类型,q 只能是素数或 2^m;FR 是域表示法,例如 $f(x)$ 是 F_2^m 上域元素的表示法;当 q 是素数时,方程为 $y^2=x^3+ax+b$,当 q 是 2^m 时,方程是 $y^2+xy=x^3+ax^2+b$,a,b 为曲线方程中的系数;G 是基点;n 为大素数并且等于点 G 的阶,h 为小整数称做余因子并且 $h=\#E(F_q)/n$(其中 $\#E(F_q)$ 为椭圆曲线的阶)。主要的安全性的参数是 n,因而 ECC 算法密钥的长度则被定义为 n 的长度[3]。

2.2 椭圆曲线的选取

椭圆曲线密码体制的安全性是基于离散对数问题(ECDLP)的 NP 难解问题。假如离散对数是容易计算的,那么从一个用户的公钥就能够很容易地算出他的私钥,这样 ECC 就不安全了。而只有当选择到合适的有限域 $GF(q)$ 及椭圆曲线(EC),能够抗击 ECDLP 算法的攻击,才能保证所选 EC 的安全性。因此选取曲线时应当遵循下面的原则[4,5]:

(1)选取 EC 的阶应该包含有一个大素数因子 $n(n>2^{160})$,并且对于固定的有限域 F_q,n 应当尽可能的大,也就是越大越好。

(2)所选的曲线应当尽最大可能地排除反常椭圆曲线、奇异椭圆曲线或超奇异椭圆曲线,超奇异椭圆曲线或反常椭圆曲线现已被证实是不安全的椭圆曲线,并且超奇异椭圆曲线无法抵挡 MOV 攻击,奇异椭圆曲线无法抵挡 Smart 攻击。

(3)$\#E$ 不能整除 $q^k-1,1 \leqslant k \leqslant 20$(为了防止 MOV 攻击)。

(4)选择 $GF(q)$ 的子域 H,满足它的阶 $|H|$ 是 $\#E$ 的最大素因子 n,并在 H 上实现 ECC。

随机选取曲线。随机选取曲线的参数 $a,b \in F_q$(q 是素数,那么满足 $4a^3+27b^2 \neq 0$),计算 $N=\#E(F_q)$ 和大素数因子 n,直到所选曲线被认为能够满足安全需求为止。这是一种理想化的方法,所选曲线安全性足够高,而且它能完全依赖于椭圆曲线阶的计算。

2.3 椭圆曲线的阶

假设 E 是 $y^2=x^3+ax+b$ 定义的椭圆曲线,满足该式的点 (x,y) 及一特殊点 O 构成的集合,记为 E,即满足 $E(F_q)=\{(x,y \in F_q \times F_q | y^2=x^3+ax+b)\} \cup \{O\}$,$E$ 中的元素称为 E 的有理点,E 相应称为 E 的有理点集合[6,7]。

Hasse 定理:令 $\#E(F_q)=q+1-t$,则 $|t| \leqslant 2\sqrt{q}$。

Weil 定理:设 E 是有限域 F_q 上的椭圆曲线,令 $t=q+1-\#E(F_q)$,则有 $\#E(F_{q^k})=q^k+1-\alpha^k-\beta^k$,式中 α,β 满足:

$$1-tT+qT^2=(1-\alpha T)(1-\beta T)$$

应用 Hasse 定理和 Weil 定理可计算许多椭圆曲线群的阶。

2.4 椭圆曲线域的参数的生成

文中只给出一种产生安全椭圆曲线域的参数的算法:

(1)首先根据给定的曲线的域,任意选取方程系数 a,b,使椭圆曲线 E 存在并满足:$y^2=x^3+ax+b$(q 为素数),其中 $a,b \in F_q$,满足 $4a^3+27b^2 \neq 0$

(2)计算 $N=\#E(F_q)$;

(3)需要验证 N 是否能够被一个大素数 $n(n>2^{160}$ 且 $n>4\sqrt{q})$ 整除,如果不能被整除,则转到步骤(1);

(4)需要验证大素数 n 是否能被 $q^k-1(1 \leqslant k \leqslant 20)$ 整除,如果不能被整除,则转到步骤(1);

(5)要验证大素数 n 是不是等于 q,如果它们相等,

则转到步骤(1);

(6)任意选择一点 $G' \in E(F_q)$,设置 $G=(N/n)G'$,重复这一步骤,至 $G \neq O$(为无穷远点)。

对于 $\#E(F_q)$ 的计算是一个纯数学问题。Rschool、Atkin、Elkies、Morain,Lercie 等人为此做了不少工作,Rschool 提出的著名 School 算法,经过 Atkin 和 Elkies 的改进提出了 SEA(School Elkies Atkin)算法。后来,Morain,Lercier 等专家又对 SEA 做了进一步的改进,目前,SEA 已被公认为是计算圆锥曲线的阶的比较有效的计算方法。除了 SEA,Satoh 还提出了 Satoh 算法以及目前对二进制域效率较高的 AGM 算法、MSS 算法、Satoh-FGH 算法、SSTT 算法等[8,9]。

2.5 验证域参数

在实际应用中,完全有可能会出现这样的问题:即无效的域参数的插入或者传输的错误,因此在使用域参数前必须对域参数来进行验证,以此保证域参数所须具备的数学特性,进而确保密码体制的安全。

在此给出对验证域参数的算法[9,10]:

输入的数据:$T=(q,a,b,G,n,h)$

输出的结果:T 有效或无效

(1)验证 q 为奇素数;

(2)验证 $G \neq O$;

(3)验证 $a,b,x_G,y_G \in F_q$;

(4)验证曲线是随机生成的;

(5)验证 a,b 是否满足曲线方程($4a^3+27b^2 \neq 0$);

(6)验证 G 是曲线上的一点;

(7)验证 n 是素数;

(8)验证 $n > 2^{160}$ 且 $n > 4\sqrt{q}$;

(9)验证 $nG=O$;

(10)验证 $h=\lfloor (\sqrt{q}+1)^2/n \rfloor, h=n$;

(11)验证对于每个 $k(1 \leqslant k \leqslant 20)$;

(12)验证 $n \neq q$;

(13)若上述有任一验证失败,那么 T 是无效的;如果验证通过则认为 T 是有效的。

综上论述,可以看到,域参数的生成是复杂的,所以在实际应用中大家可以选择 NIST 所推荐的安全曲线及参数,并将产生的参数放置于可信任的机构如 CA 中,需要时,从 CA 获得有效的参数,可由 CA 确保参数的有效性及安全性(CA:认证权威机构)[11]。

3 结束语

椭圆曲线密码体制的安全性是基于椭圆曲线离散对数的 NP 难解问题,而安全椭圆曲线的选取则是建立椭圆曲线密码体制的基石,所以曲线的安全是保证密码体系安全的重要因素。在过去的十多年里,椭圆曲线离散对数问题受到了数学界的极大关注[12]。目前,还没有发现椭圆曲线离散对数(ECDLP)有哪些特别大的弱点。

参考文献:

[1] 杨 剑,杨铭熙,李腊元. 增强安全的 IEEE802.15.4 协议研究[J]. 计算机技术与发展,2007,17(12):136-139.

[2] 张晓丰,樊启华,程红斌. 密码算法研究[J]. 计算机技术与发展,2006,16(2):179-180.

[3] 于雪燕,胡金初,柴春铁. 椭圆曲线密码体制及其参数生成的研究[J]. 计算机技术与发展,2006,16(11):160-161.

[4] 张 雁,林 英,郝 林. 椭圆曲线密码体制的研究热点综述[J]. 计算机工程,2004(2):127-129.

[5] 刘志猛,彭代渊. 基于椭圆曲线加密体制的实现[J]. 信息安全与通信保密,2006(4):94-96.

[6] 张龙军,沈钧毅,赵 霖. 椭圆曲线密码体制体制性研究[J]. 西安交通大学学报,2001(10):1038-1041.

[7] 王衍波,薛通编. 应用密码学[M]. 北京:机械工业出版社,2003.

[8] IEEE P1363/D6(Drafe Version 6). Standard Specification for Public Key Cryptography [EB/OL]. 2004. http://grouper.ieee.org/groups/1361/P1363/draft.html.

[9] 张 雁,林 英,郝 林. 构建安全椭圆曲线密码体制的关键问题[J]. 计算机应用,2004(12):82-84.

[10] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) [S]. 1998.

[11] Johnson D, Menezes A. The Elliptic Curve Digital Signature Algorithm (ECDSA) [R]. Canada: University of Waterloo, 2000.

[12] 王平水,杨桂元. 基于有限域上圆锥曲线的公钥密码系统[J]. 微机发展(现更名:计算机技术与发展),2005,15(6):99-101.

(上接第 139 页)

ACM SIGCOMM Conference. [s.l.]:[s.n.],2003.

[9] Yasami Y, Mozaffari S P. A novel unsupervised classification approach for network anomaly detection by k-means clustering and ID3 decision tree learning method[J]. ACM Journal of Supercomputing,2010,53(1):231-245.

[10] Park N H, Oh S H, Lee W S. Anomaly intrusion detection by clustering transactional audit streams in a host computer[J]. Information Sciences,2010,180(12):2375-2389.

[11] 李 娜,钟 诚. 基于划分和凝聚层次聚类的无监督异常检测[J]. 计算机工程,2008,34(2):120-123.

[12] 周亚建,徐 晨,李继国. 基于改进 CURE 聚类算法的无监督异常检测方法[J]. 通信学报,2010,31(7):19-23.