一种安全椭圆曲线的有效构造方法*)

吴开贵　吴中福
（重庆大学计算机学院　重庆 400044）

摘　要　椭圆曲线密码系统是公钥基础设施中的一种非常有效的技术，但是产生相应的椭圆曲线是很困难的。本文提出了一种在已知有限数域上产生一类安全椭圆曲线的算法。当素数 $p=6k+1(k\in Z,Z$ 为自然数）时，该素数可表示成 $W^2+4V^2(W,V\in Z)$ 的形式。基于该结论，证明了有限域 F_p 上的 j 不变为 1728 的椭圆曲线 $y^2=x^3+1$ 的阶 $\#E(F_p)$ 为 $p+1\pm 2W$（当 $W=4L+1$，$L\in Z$，$\#E(F_p)=p+1-2W$；当 $W=4L-1$，$L\in Z$，$\#E(F_p)=p+1+2W$），并提出了一种构造安全椭圆曲线的算法，分析了算法的有效性。

关键词　复数乘法，椭圆曲线，有限域

A Method of Generating Secure Elliptic Curves

WU Kai-Gui　WU Zhong-Fu
(College of Computer Science, Chongqing University, Chongqing 400044)

Abstract　Elliptic curve cryptography is a very efficient basic technology for public key infrastructures, but there is a paucity of efficient means for generating suitable elliptic curves. This paper presents a method for generating elliptic curves of known order over finite fields. It is well known that if the prime $p=6k+1$, $k\in Z$, this prime can be factored into W^2+4V^2, $W,V\in Z$. Based on this, the paper proved that the order of the elliptic curve $E: y^2=x^3+1$ over finite fields F_p with j-invarant being 1728 is $p+1\pm 2W$(when $W=4L+1, L\in Z, \#E(F_p)=p+1+2W$; when $W=4L-1, L\in Z, \#E(F_p)=p+1-2W$). Furthermore, the constructing method of elliptic curves is propsed.

Keywords　Complex multiplication, Elliptic curve, Finite field

1　引言

有限域上的椭圆曲线已经在公共密钥体系的身份认证和签名方案中使用，而椭圆曲线上的离散对数问题能抵抗所有的已知亚指数算法的攻击。跟传统的加密函数相比，在保持同一安全水平下，在执行加密方案时椭圆曲线系统具有更快的速度和更短的密钥长度。

在椭圆曲线密码系统中一个很重要的计算问题就是构造一个有限域上安全的椭圆曲线。一种途径就是随机地产生曲线，通过计算点数来确定它的安全性[1]。不幸的是，在一个大素数有限域上计算点的个数在速度上是相当慢的[2]。另外一种方法就是使用复数乘法(Complex Multiplication)[3]。首先寻找一个满足密码系统健壮性曲线的基数，然后再构造一个具该基数的曲线。如果这个曲线的自同态环有小的类数，那么这种方法就要比通过计算点数寻找健壮曲线要快。但是我们很难估计用复数乘法方法产生椭圆曲线所需的时间。

根据文[4]，如果在椭圆曲线密码系统中重复地使用同一个在有限域上的曲线，即使每次使用一个随机的基点，我们容易将新的离散对数问题变换到旧的离散对数问题上去，因而可以利用旧的基本数据来更快地攻击这一类密码系统。此外如果攻击者建立了一个庞大基本数据库，那么他通过一个用大步小步(Baby step and Giant step)算法，在 $O(q^{1/d})$，$d>2$ 的时间内，攻击这个椭圆曲线密码系统。

本文介绍椭圆曲线的基本原理。当选择一个判别式 $D=4$，本文提出快速构造满足安全条件的椭圆曲线系统算法。

2　有限域上的椭圆曲线

令 $p>3$ 是一个奇素数，有限域 F_p 上的椭圆曲线 E[5]方程定义如下：

$$y^2=x^3+ax+b \tag{1}$$

满足 $a,b\in F_p$，并且 $4a^3+27b^2\neq 0(\mathrm{mod}\ p)$。满足定义方程式(1)的所有点$(x,y)$，$x\in F_p$，$y\in F_p$，以及一个叫无穷点的特殊点$\infty$构成集合 $E(F_p)$。

chord-and-tangent 规则给出了在椭圆曲线 $E(F_p)$ 上两点相加所得到的第三点。点集 $E(F_p)$ 在加法操作下构成了加法群，∞点构成群单位元。这个群在构建椭圆曲线密码系统中起着非常重要的作用。

这个加法规则可用几何的办法来解释。令 $P=(x_1,y_1)$ 和 $Q=(x_2,y_2)$是椭圆曲线 E 上两个不同的点。那么 P 与 Q 的和用 $R=(x_3,y_3)$来表示，可以如下定义：首先作一条通过 P 和 Q 的直线；这条直线交椭圆曲线于第三个点。那么 R 就是第三个点关于 x 轴的映象。如果 $P=(x_1,y_1)$那么 $2P$ 用 $R=(x_3,y_3)$来表示，可以如下定义：首先作椭圆曲线上 P 点的切线，这条直线交椭圆曲线于第二个点，那么 R 就是这第二点关于 x 轴的映象。

通过几何法推导出关于两点的和的代数公式如下：

1. $P+\infty=\infty+P=P$ 对于所有的 $P\in E(F_p)$.

2. 如果 $P=(x,y)\in E(F_p)$，那么 $(x,y)+(x,-y)=\infty$。(点 $(x,-y)$ 记为 $-P$，并且称之为负 P；可以检测 $-P$ 也是椭圆曲线上的一点)

*)本文受国家自然科学基金(No. 30400446)资助。

3.(点加) 令 $P=(x_1,y_1)\in E(F_p)$ 和 $Q=(x_2,y_2)\in E(F_p)$，满足 $P\neq\pm Q$。那么 $P+Q=(x_3,y_3)$，方程式为：

$$\begin{cases}x_3=\lambda^2-x_1-x_2\\ y_3=\lambda(x_1-x_3)-y_1\end{cases}\tag{2}$$

满足

$$\lambda=\begin{cases}(y_2-y_1)(x_2-x_1)^{-1} & \text{if } x_2\neq x_1\\ (3x_1^2+a)(2y_1)^{-1} & \text{otherwise}\end{cases}\tag{3}$$

两个关于 E 的重要量：

判别式 $\Delta=-16(4a^3+27b^2)$ (4)

j 不变量 $j=1728(4a)^3/\Delta$ (5)

这里 $\Delta\neq 0$。

引理 1 给定 $j_0\in F_p$，存在一个定义在 F_p 上的椭圆曲线 E 满足 $j(E)=j_0$。

我们容易构造给定的具有 j 不变量 j_0 的椭圆曲线，考虑到 $j_0\neq 0$ 也不等于 1728；令 $k=j_0/(1728-j_0)$，$j_0\in F_p$ 那么方程式

$$y^2=x^3+3kx+2k\tag{6}$$

给出了一个 j 不变量 $j(E)=j_0$ 的椭圆曲线。

定理 1 同构的椭圆曲线有相同的 j 不变量。

定理 2(Hasse) 用 $\#E(F_p)$ 表示椭圆曲线 $E(F_p)$ 的点的个数。如果 $\#E(F_p)=p+1-t$，那么 $|t|\leqslant 2p$。

定义 1(对偶曲线) 给定的 E：$y^2=x^3+ax+b$ 有 $a,b\in F_p$，关于 c 对偶椭圆曲线为：

$$E_c:y^2=x^3+ac^2x+bc^3\tag{7}$$

满足 $c\in F_p$。

定理 3 假设在 F_p 的 E 其阶为 $\#E(F_p)=p+1-t$，那么它的对偶椭圆曲线的阶为：

$$\#E(F_p)=\begin{cases}p+1-t \text{ 如果 } C \text{ 是 } F_p \text{ 中的平方数}\\ p+1+t \text{ 如果 } C \text{ 不是 } F_p \text{ 中的平方数}\end{cases}\tag{8}$$

定理 4(Atkin-Morain) 令 p 是一个奇素数

$$4p=W^2+DV^2\tag{9}$$

满足 $W,V\in Z$，那么存在一个定义在 F_p 的椭圆曲线 E 有 $\#E(F_p)=p+1-t$。

对于一个给定的 p，满足式(9)的整数 D 被称之为 p 的 CM 判别式。通过整数 $Q(\sqrt{-D})$ 由复数乘法确定曲线 E。我们可以通过类域论计算出椭圆曲线的 j 不变量。一旦知道了 j 不变量，利用引理 1 就可以构建出具有 $p+1-t$ 个点的椭圆曲线。实际上，这种方法给出了一个具有 $p+1-t$ 或者 $p+1+t$ 个点的椭圆曲线。如果构造的椭圆曲线有 $p+1+t$ 个点，那么我们必须得到这个椭圆曲线的对偶曲线，利用它得到具有 $p+1-t$ 个点的椭圆曲线。在知道阶的情况下构造椭圆曲线的技术，称之为复数乘法 CM 方法[3]。

定义 2 称椭圆曲线 E 是具有密码系统安全的，是指 $|E(F_q)|=k\cdot r$ 满足素数 $r>2^{160}$，并且正整数 $k\leqslant 4$。

第一个必要条件避免了一般的如 Pollard ρ 算法的攻击，而第二个则是有效性方面的原因。另外，为了避免异常曲线，素数 r 和 p 应该不同。

3 安全椭圆曲线构造算法

这个算法可以这样简单描述：构造具有特殊形式的素数 $p=4k+1$，然后构成安全椭圆曲线。

定理 5 令 p 是素数，$p>3$，方程式

$$W^2+4V^2=p\tag{10}$$

可以解当仅当 $\left(\frac{-3}{p}\right)=1$，就是说 $p=6k+1,k\in Z$。

证明从略。

定理 5 说明如果素数 $p=6k+1$，那么 3 是一个 p 的 CM 判别式。怎样去解方程式 $p=W^2+4V^2$ 呢？可以使用 Cornacchia 的算法。算法运行如下：

1)令 x_0 是 $x^2\equiv -D \pmod p$ 的解满足 $p>x_0>p/2$；

2)作为一个连分数逐步展开 p/x_0：

$p=q_0x_0+x_1$，

$x_0=q_1x_1+x_2$，

…

$x_r=q_{r+1}x_{r+1}+x_{r+2}$

当 $x_r^2<p\leqslant x_{r-1}^2$ 时终止

3)赋值

$u=x_r$ 和 $v=\sqrt{\frac{p-x_r^2}{d}}$

4)如果 v 不是整数，p 不能被分解为 u^2+Dv^2。

在 $D\equiv 3 \pmod 8$ 的情况下，我们能够用这个相同的算法，来求解 $x^2+x+(D+1)/4 \pmod p$ 的解 x_0。

定理 6 令素数 $P\equiv 1 \bmod 6$，那么 $p=W^2+4V^2$，$W=4L\pm 1$，当 $W=4L-1$ 时椭圆曲线 $E:y^2=x^3+1$ 的阶为 $p+1-2W$；当 $W=4L+1$ 时，椭圆曲线 $E:y^2=x^3+1$ 阶为 $p+1+2W$。

证明：一个不可约的 $\pi\in Z[i]$，如果是 π 等于 $1 \pmod{2+2i}$，那么称 π 为本原元。对于元素 $\pi=2V+Wi$ 我们有 $\pi\pi'=p=W^2+4V^2$ 是素数，因此 π 是不可约的。根据文[6]

$$\#E(F_p)=p+1-\overline{\left(\frac{2}{\pi}\right)_4\pi}-\left(\frac{2}{\pi}\right)_4\bar{\pi}\tag{11}$$

有如下关于四次方程特征 $1+i$ 模一个素数 π[3] 的结论：

$$\left(\frac{1+i}{\pi}\right)_4=i^{(2v-w-W^2-1)/4}\tag{12}$$

$$\left(\frac{1+i}{\pi}\right)_4=i^{(-2v-w+W^2+1)/4}\tag{13}$$

因此

$$\left(\frac{2}{\pi}\right)_4=\left(\frac{1-i}{\pi}\right)_4=\left(\frac{1-i}{\pi}\right)_4=i^{-w/2}\tag{14}$$

当 $W=4L-1$ 时，那么 $i^{-W/2}=-i$

$$\begin{aligned}\#E(F_p)&=p+1-i(2V+Wi)-(-i)(2V-Wi)\\&=p+1+2W\end{aligned}\tag{15}$$

当 $W=4L+1$ 时，那么 $i^{-W/2}=i$

$$\begin{aligned}\#E(F_p)&=p+1+i(2V+Wi)-i(2V-Wi)\\&=p+1-2W\end{aligned}\tag{16}$$

安全性考虑：因为 p 是素数，$\#E(F_p)=p+1-2W$ 是偶数。如果 $\#E(F_p)/2$ 或者 $\#E(F_p)/4$ 是一个素数，那么满足强的安全条件，也即是椭圆曲线 $E(Fp)$ 是密码系统安全的。

因此，构造安全椭圆曲线的算法如下：

1)给定一个素数的长度，产生一个形如 $6k+1$ 的素数 p。

2)分解这个素数 p 到 W^2+4V^2 形式。

3)选择 j 不变量为 1728，那么椭圆曲线方程式为 $y^2=x^3+1$。

4)计算有限域上的椭圆曲线的阶 $\#E(F_p)$。

5)测试无论那个数 $\#E(F_p)/2$ 或者 $\#E(F_p)/4$ 是否是一个素数。如果都不是，则返回到第一步。

6)选择基点并计算这个点的阶。

4 实例

为了证实这个思想，作者用 C++ 编程语言开发了产生这类椭圆曲线的程序。选择素数长度，比方说，192 位，这个程序生成一个素数 p = 1928952416777687917470659164182613737573049894109870667458 9。这个素数能被表示为 W^2+4V^2，W=55002053592931705449171458117，V=637657789655571204607292216 65。这个椭圆曲线的阶 $\#E(F_p)$ 是 192895241677687917470659164171613326854463553020036375 8356。并且 $\#E(F_p)=h*r$，h=4，r = 4822381041944219793676647910429033317136158882550090939589。数字 r 是素数。执行程序耗时 15 秒。椭圆曲线 $E(F_p)$是密码系统安全的。

结论 本文提出了一个产生一类椭圆曲线的方法。当 $p=6k+1$，并且 p 是素数时，那么 p 能够被分解为 W^2+4V^2。本文也证明了在有限域 F_p 具有 j 不变量为 1728 的椭圆曲线 E 的阶是 $p+1\pm 2W$（当 $W=4L+1$ 时，$\#E(F_p)=p+1+2W$；当 $W=4L-1$ 时，$\#E(F_p)=p+1-2W$），同时给出了构建这类椭圆曲线的快速算法。

参 考 文 献

1 Muller V, Paulus S. On the Generation of Cryptographically Strong Elliptic Curves:[Technical Report]. Technical University of Darmstadt, 1997

2 Schoof R. Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp. ,1985,44:483～494

3 Atkin A O L, Morain F. Elliptic curves and primality proving. Mathematics of Computation,1993,61(203):29～68

4 Kurotani K, Matsuo K, Chao J, et al. Consideration of security of hyperelliptic cryptosystems. IEICE, Symposium on Cryptography and information Security, SCIS'98, 4.1-D, Jan. ,1983

5 Johnson D, Menezes A. The Elliptic Curve Digital Signature Algorithm (ECDSA):[Technical report CORR 99-34]. Dept. of C&O, University of Waterloo, Canada. Available at: http://www.cacr.math.uwaterloo.ca

6 Ireland K, Rosen M. A Classical Introduction to Modern Number Theory. Spring-Verlag, 1982

7 Morain F. Building cyclic elliptic curves modulo large primes. In: D. Davies, editor, Advances in Cryptology - EUROCRYPT'91, volume 547 of Lecture Notes in Comput. Sci. , Springer-Verg, 1991. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, United Kingdom, 1991. 328～336

(上接第 105 页)

3 实验环境、结果与性能分析

为验证 MADIDS 的性能，针对其规则更新进行了实验。由于条件限制，实验环境仅在电子科技大学校园网内选取了三处位置进行，如图 5 所示。其中，主服务器 MS 放置于子网 202.115.14.1/24 内；第一个域的各个节点包括 DS1、Host1、Host 2、Host 3，放置于子网 202.112.10.1/24 内；第二个域的各个节点包括 DS2、Host4、Host 5、Host 6，放置于子网 202.115.1.1/24 内。其中主服务器为一台 Intel 服务器，配置为 1.2G CPU，512M 内存、100Mbps 以太网卡，其它 8 个节点均采用 PC 赛扬 666。

数据库平台为 mysql4.0，实验中管理的 IDS 为 snort。移动 Agent 平台采用 Windows NT4+Aglet1.3+JDK1.0 来搭建，通过 Aglet Workbench 及相应软件包实现。实验中首先配准所有主机的时钟，在每个节点上都由一个读系统时间的程序进行计时，并与 MADIDS 的运行配合进行。对规则更新进行了 500 次实验，从 Main Server 上的 EDMS 更新开始计时，直到最后一个 Host 上的 EDH 得到更新为止，作为一次完整的实验过程。由于已对所有节点的时钟进行了配准，系统一次规则更新的周期时间，可由最后一个完成移动 Agent 返回动作的 Host 上的时间标记，减去 MS 上的初始时间标记得到。从实验情况来看，每次实验都能完成 MADIDS 的设计目标，一个新规则在两个域的 8 个节点得到全面配置，最短耗时 0.8 秒，最长耗时为 3.3 秒。周期长短取决于当前网络拥塞状况、移动 Agent 执行效率、数据库执行效率等因素。

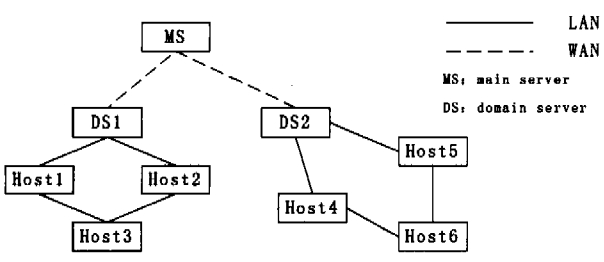

图 5 MADIDS 实验环境示意图

由实验与分析可知，这种"分层核对"机制具有如下优点：(1)有效地减少 MADIDS 中对新的入侵行为特征标记的管理和复制入侵行为特征标记内容的通信量，特别是在 WAN 上的通信量；(2)Main Server 不需维护每一个主机的新入侵特征，而仅仅需要维护 Domain Server 即可，这样就大大降低了维护的整体开销。限于篇幅，规则生成机制外，其它内容不再赘述。

结论 本文提出了一种基于移动 Agent 的新型入侵检测系统 — MADIDS。MADIDS 使用分层体系结构，整个系统由若干域组成，域内通过 LAN 连接，域间通过 WAN 连接。每个域由域服务器管理，所有域服务器由主服务器管理。这种体系结构保证了很好的伸缩性和扩展性，MADIDS 在系统管理中使用了"分层生成"机制，这种机制降低了维护系统整体性和一致性的负荷，网络通信较小，非常适合在 WAN 中使用。

参 考 文 献

1 Mell P, McLarnon M. Mobile agent attack resistant distributed hierarchical intrusion detection system. In: Proceedings of RAID' 99, CERIAS, Purdue University, 1999

2 Gregory M, White B, Fisch E A, Pooch U W. Cooperating security managers: A peer based intrusion detection system. IEEE Network, 1996.14

3 Slagell M. The Design and Implementation of MAIDS (Mobile Agents for Intrusion Detection System). Masters Creative Component paper, Mark Slagell, Iowa State University, May 2001

4 张云勇. 移动 Agent 及其应用. 北京：清华大学出版社，2002

5 Baumann J, Hohl F, Rothermel K, Straβer M. Mole - Concepts of a Mobile Agent System. WWW Journal, Special issue on Applications and Techniques of Web Agents, 1998

6 Karnik N M, Tripathi A R. Design Issues in Mobile-Agent Programming Systems, IEEE Concurrency, 1998, 6(3):52～61

7 Johansen D. Mobile Agent Applicability. In: Rothermel K, et al. eds, Mobile Agents: MA'98: proceedings, Berlin[etc.]: Springer, 1998, Lecture notes in computer science; ISBN 3-540-64959-X, 1998, 1477