椭圆曲线密码体制

徐秋亮 李大兴
(山东大学计算机科学系 济南 250100)
(山东大学网络信息安全研究所 济南 250100)

摘 要 椭圆曲线密码体制目前已引起了信息安全及密码学各界的广泛关注,从安全性及有效性来看,这种密码体制有着广阔的应用前景,是一种可能近期在某些领域取代 RSA, DSS等现存体制的密码(签名)体制,现已逐渐形成了研究与开发热点. 文中首先对椭圆曲线及其相关知识作了简单介绍,而后给出了一些典型的椭圆曲线密码体制并较为详细地讨论了这种密码体制的安全性. 文中还以相当的篇幅对适用于密码体制的椭圆曲线的构造方法作了重点介绍,这是实现椭圆曲线密码体制的关键性问题. 作为一篇综述,文中反映了椭圆曲线密码体制的历史进展和现状以及当前所面临的理论问题,体现了该领域目前的最新成就,并对该密码体制的发展提出了看法.

关键词 椭圆曲线,离散对数,密码体制,时间复杂度,安全性

中图法分类号 TP309

ELLIPTIC CURVE CRYPTOSYSTEMS

XU Qiu-Liang and LI Da-Xing
(*Department of Computer Science, Shandong University, Jinan* 250100)
(*Institute of Network Security, Shandong University, Jinan* 250100)

Abstract Recently, elliptic curve cryptosystems have become as a promising new area in public-key cryptography. The main advantage of elliptic curve cryptosystems over other public-key cryptosystems is the fact that they are based on a different intractable problem, and that their keys have smaller sizes for the same level of security. These properties lead to some better performance in application. Because of their security and efficiency, this kind of cryptosystems can be used widely in the future. In fact, they have come into strong consideration not only by theory researchers but also by standards developers. The paper here covers the main various aspects of elliptic curve cryptosystems. The concepts of elliptic curves and their related knowledge are introduced briefly, and a few typical schemes are given. The security of elliptic curve cryptosystems is given a properly detailed description. Building of an elliptic curve suitable for cryptosystems, which is essential to the setup of an elliptic curve cryptosystem, is discussed in detail.

As a summary, the advance and the status quo of the elliptic curve cryptosystems are reflected, and so do the problems the cryptosystems face now. The newest achievements in this area are covered and views on the development of the cryptosystems are proposed.

Key words elliptic curve, discrete logarithm, cryptosystem, time complexity, security

原稿收到日期: 1998-12-29;修改稿收到日期: 1999-08-08. 本课题得到国家"八六三"计划(项目编号 863-306-ZT06-01-4)及山东省自然科学基金(项目编号 Z94G0108)资助. 徐秋亮,男, 1960年 4月生,博士,主要研究方向为数据安全、密码学. 李大兴,男, 1963年 2月生,教授,博士生导师,主要研究方向为网络安全、密码学.

1 引 言

椭圆曲线理论是代数几何、数论等多个数学分支的一个交叉点，一直被认为是纯理论学科．近年来，由于公钥密码学的产生与发展，该学科也找到了它的应用领域．在 RSA密码体制的基础性问题—— 大整数分解和素性检测的研究方面，椭圆曲线是一个强有力的工具[1~6]．特别地，以椭圆曲线上的(有理)点构成的 Abel群为背景结构，实现各种密码体制已是公钥密码学领域的一个重要课题．自 80年代中期被引入[7,8]以来，椭圆曲线密码体制逐步成为一个十分令人感兴趣的密码学分支，1997年以来形成了一个研究热点．这种密码体制的诱人之处在于在安全性相当的前提下，可使用较短的密钥．一般认为，q元域上的椭圆曲线密码体制，当 q的长度为 160bit时，其安全性相当于 RSA使用 1024bit模数[9]，密钥短意味着小的带宽和存储要求，这在某些应用中可能是决定性的因素．椭圆曲线密码体制的诱人之处还在于它建立在一个不同于大整数分解及素域乘法群离散对数问题的数学难题之上．自公钥密码产生以来，人们基于各种数学难题提出了大量的密码方案，但能够经受住时间考验而广泛为人们所接受的只有基于大整数分解及离散对数问题的方案，且不说这两种问题受到亚指数算法的严重威胁，就如此狭窄的数学背景来说也不能不引起人们的担忧，寻找新的数学难题作为密码资源早就是人们努力的一个方向．同时，椭圆曲线资源丰富，同一个有限域上存在着大量不同的椭圆曲线，这为安全性增加了额外的保证，这也为软、硬件实现带来方便．

由于椭圆曲线上的一次群运算最终化为其背景域上不超过 15次乘法运算，因而便于实现，在执行速度方面，目前难以对椭圆曲线密码体制与现存密码体制，比如 RSA，DSA等作出准确的定量比较，粗略地说，椭圆曲线密码体制较对应的离散对数体制要快，且在签名和解密方面较 RSA快，但在签名验证和加密方面较 RSA慢[9]．

安全性显然是任何密码体制的必备条件，椭圆曲线密码体制的安全性分析因而也引起了各国密码学家及有关部门的关注与重视，但成果却并不丰硕．也许这可视为椭圆曲线密码体制具有高强度的一种证据，因此，大多数密码学家对这种密码体制的前景持乐观态度．

2 椭圆曲线的基本概念及相关问题

在本文中，K总表示一个有限域．事实上，在密码学中我们只对两种情形感兴趣：K是大素域 $\mathbf{Z}_p$或特征为 2的有限域 $GF(2^n)$(为了符号上的方便，本文中 q元有限域 $GF(q)$有时也用 F_q表示)．我们还约定 p总表示一个大于 3的素数，$\bar{K}$表示 K的代数闭包，K上的射影平面 $P^2(K)$是 $K^3\setminus\{(0,0,0)\}$上的等价关系“~”的等价类集合，其中，“~”定义为 $(X_1,Y_1,Z_1)\sim(X_2,Y_2,Z_2)$当且仅当存在 $u\in K^*$使得 $(X_1,Y_1,Z_1)=(uX_2,uY_2,uZ_2)$．包含 (X,Y,Z)的等价类记为 $(X:Y:Z)$．形如下式的 3次齐次方程称为 K上的 Weierstrass方程：

$$Y^2Z+a_1XYZ+a_3YZ^3=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \tag{1}$$

其中，$a_1,a_2,\cdots,a_6\in K$．令 $F(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3$，如果对所有满足 $F(X,Y,Z)=0$的射影点 $P=(X:Y:Z)\in P^2(\bar{K})$，$F$在 P点的 3个偏导数 $\frac{\partial F}{\partial X},\frac{\partial F}{\partial Y},\frac{\partial F}{\partial Z}$必不全为 0，则称 Weierstrass方程(1)是平滑的或非奇异的．

设域 K上的 Weierstrass方程(1)是平滑的，该方程在 $P^2(\bar{K})$中的所有解组成的集合 E：

$$E=\{(X:Y:Z)\in P^2(\bar{K})\mid F(X,Y,Z)=0\}$$

称为域 K上的一条椭圆曲线．在任一条椭圆曲线中，存在唯一一点其 Z坐标为 0，该点即是 $O=(0:1:0)$，我们称其为“无穷远点”．椭圆曲线 E的判别式 $\Delta(E)$与 j-不变量 $j(E)$是椭圆曲线理论中两个重要的量，其定义见文献[10]．

为了方便，常将 Weierstrass方程(1)以仿射坐标 $x=X/Z,y=Y/Z$的形式书写为

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{1'}$$

这时, 相应的椭圆曲线 E即是方程 $(1')$ 在仿射平面 $A^2(\bar{K})$中的所有解及一个特殊点—— 无穷远点 O组成的集合. 即

$$E = \{(x,y)\in \bar{K}\times \bar{K} \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}\cup \{O\}.$$

为明确, 以后常用 E/K表示 K 上的椭圆曲线 E. E/K中两个仿射坐标均属于 K的点及无穷远点 O均称为 E/K 的 K有理点, E/K的所有 K有理点组成的集合记为 $E(K)$, 即

$$E(K) = \{(x,y)\in K\times K \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}\cup \{O\}.$$

为了叙述的方便, 我们将不区别椭圆曲线与其定义方程, 并约定 E或 E/K 将总表示有限域 K 上的椭圆曲线, 不再另作说明.

K上的两条椭圆曲线

$$E_1:\quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E_2:\quad y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

称作是同构的, 并记为 $E_1/K\cong E_2K$, 如果存在 $u,r,s,t\in K, u\neq 0$使得变量替换 $(x,y)\to (u^2x + r, u^3y + u^2sx + t)$将 E_1 变为 E_2. 当 K的特征 $\mathrm{Char}(K)\neq 2,3$时, E/K 可在同构意义下化成如下简单形状

$$E':\quad y^2 = x^3 + ax + b \quad a,b\in K$$

这时, $\Delta(E') = -16(4a^3 + 27b^2)\neq 0, j(E') = -1728(4a)^3/\Delta(E')$.当 K 的特征 $\mathrm{Char}(K) = 2$时, 根据 $j(E)$是否为 0, 可分别化为两种基本形状, 参见文献 [11].

在椭圆曲线 E/K中可按"弦切法"定义加法运算"+ "使$\langle E,+\rangle$成为一个 Abel群, $\langle E(K),+\rangle$构成其子群, 称之为 E/K 的有理点子群. 可以证明, 当 $E_1/K\cong E_2/K$ 时 $E_1(K)$与 $E_2(K)$作为 Abel群必是同构的[11]. 所谓椭圆曲线密码体制, 即是建立在 Abel群 $E(K)$上的密码体制, 下面将以$\#E(K)$表示群 $E(K)$的阶. 许多密码学论文中直接称 $E(K)$为"椭圆曲线群", 并将$\#E(K)$称为椭圆曲线的阶, 本文有时也采用这种说法.

3 典型的椭圆曲线密码体制

现有的椭圆曲线密码体制均是从其他群中平移而来, 并未针对 $E(K)$产生新型密码体制, 而这种平移主要是对基于离散对数问题的密码体制, 虽然也有 RSA体制的平移[12,13], 但并无实用及理论价值, 本文仅就基于离散对数的体制进行讨论.

设 G是一个有限群, $a,b\in G$, 若存在正整数 n使得 $a^n = b$, 则 n称为群 G中 b的以 a为底的离散对数, 记为 $n = \log_a b$. 给定 $a,b\in G$, 求 $n = \log_a b$ 称为 G中的离散对数问题, 特别地, 若 $P,Q\in E(K)$, 求 n使得 $nP = Q$, 称为椭圆曲线离散对数问题.

将 ElGamal加密体制直接平移到椭圆曲线群上, 得到的密码体制将需要首先把待加密的明文转化为椭圆曲线上的点, 而后才能进行加密, 这在实用上较为麻烦, 为避免这个麻烦, Menezes和 Vanstone对该体制作了一点轻微的修改[11]. 下面介绍的 EC-ElGamal体制采用了这种改进形式.

EC-ElGamal加密体制:

(1) 选取有限域 K、椭圆曲线 E/K 及基点 $P\in E(K)$ (这些参数可由一组用户公用).

(2) 选取随机数 a, 计算 $Q = aP$.

(3) 公开 K, E, P, Q作为公钥, 密藏 a作为私钥.

假设 Alice已建立了上述体制, 给 Alice发送秘密消息 $M = (M_1, M_2)\in K\times K$, 需完成如下步骤:

① 随机选取正整数 k.

② 计算 $kP, kQ = (\bar{x},\bar{y})$, 若 $\bar{x} = 0$或 $\bar{y} = 0$返回第① 步, 直到 $\bar{x}\neq 0, \bar{y}\neq 0$.

③ 发送 $C = (kP, M_1\bar{x}, M_2\bar{y})$给 Alice.

收到密文 C后, Alice计算 $a(kP) = (\bar{x},\bar{y})$, 进而得到明文 $M = (M_1, M_2)$.

EC-DSS签名体制:

(1) 选取有限域 K、椭圆曲线 E/K 及基点 $P\in E(K)$, 设$\langle P\rangle$是由 P生成的 q阶循环子群, q是一个大

素数.

(2) 选取随机数 x, $0<x<q$, 计算 $Q=xP$.

(3) 选取单向 Hash函数 $H: M\to Z$,其中,M是消息空间,Z是整数集,并选取双射 $g:\langle P\rangle\to\{0,1,\cdots,q-1\}$.

(4) K,E,P,Q,q,g均为公开信息,作为签名验证公开钥,x保持秘密作为签名密钥.

设有消息 $m\in M$, 对 m的签名过程为

① 随机选取整数 k, $0<k<q$;

② 计算 $R=kP$;

③ 解关于 s的同余方程 $H(m)\equiv -xg(R)+ks \bmod q$

对 m的签名为 (R,s). 签名验证方程为

$$(H(m)s^{-1}\bmod q)P+(g(R)s^{-1}\bmod q)Q=R$$

EC-Diffie-Hellman密钥交换协议:

选取有限域 K、椭圆曲线 E/K及基点 $P\in E(K)$. K,E,P为公开信息.若 Alice与 Bob想进行密钥交换,执行如下步骤:

① Alice随机选取正整数 m,计算 $K_A=mP$,并将 K_A传送给 Bob;

② Bob随机选取正整数 n,计算 $K_B=nP$,并将 K_B传送给 Alice;

③ Alice计算: $K_C=mK_B$; Bob计算: $K_C=nK_A$. K_C即为 Alice和 Bob所商定的密钥.

4 椭圆曲线密码体制的安全性

椭圆曲线密码体制的安全性取决于椭圆曲线离散对数问题的难解性.一般而言,群 G上的离散对数算法可分成两类: 指数计算法与碰撞搜索法. 指数计算法具有亚指数时间复杂度,但要求在 G中"平滑性"概念有意义,且 G中包含足够多的平滑元素. 类群、GF(2^n)的乘法群及 Z_p^* 均满足该性质. 目前最好的指数计算法是线性筛法[14]与数域筛法[15]. 碰撞搜索法可用于一般群,该类算法具有纯指数时间复杂度. 目前最有效的碰撞法是 Pllard ρ方法[16]和 Pohlig-Hellman方法[17],这也是目前对椭圆曲线密码体制最有影响的方法. 下面就一般群形式简述这两个方法. 以下假设 G是一个 n阶 Abel群, $H=\langle h\rangle$ 是由 $h\in G$生成的 m阶循环子群.

4.1 Pollard ρ-方法

Pollard ρ方法是一个随机算法,无法给出运算时间上界,而只能给出其期望运算次数.

设 m是已知的,随机将 G分成大约等势的 3份 G_1,G_2,G_3,使得 $x\in G_i$ ($i=1,2,3$)的判断是容易的(大约相当于一次或几次 G的运算),对 $y\in H=\langle h\rangle$,随机选取 a_0,b_0使 $1<a_0,b_0<m$,令 $y_0=h^{a_0}y^{b_0}$,定义如下序列:

$$(y_{i+1},a_{i+1},b_{i+1})=\begin{cases}(hy_i,a_i+1,b_i) & y_i\in G_1\\ (y_i^2,2a_i,2b_i) & y_i\in G_2\\ (yy_i,a_i,b_i+1) & y_i\in G_3\end{cases}\qquad i=0,1,2\cdots \tag{2}$$

其中,a_i,b_i可用模 m约化,故不会过大而不可控制. 该序列的构造保证了下列等式成立:

$$y_i=h^{a_i}y^{b_i},\quad i=0,1,2\cdots$$

若将序列 $\{y_i\}$视为从 H到 H的一个(部分)随机映射,其期望循环长度为 $O(\sqrt{m})$,因此,通过比较 y_i与 y_{2i}我们可期望在 $O(\sqrt{m})$时间内求到正整数 k使得 $y_k=y_{2k}$, $k=O(\sqrt{m})$,即 $h^{a_k}y^{b_k}=h^{a_{2k}}y^{b_{2k}}$或 $y^{b_k-b_{2k}}=h^{a_{2k}-a_k}$,当 $\gcd(b_k-b_{2k},m)=1$时便求得

$$\log_h y=\frac{a_{2k}-a_k}{b_k-b_{2k}}\bmod m.$$

在密码体制中,$\gcd(b_k-b_{2k},m)=1$以很高的概率成立(比如,在 DSS中,m是一个素数). 该算法的期望运算

次数为 $O(\overline{n_h})$.

4.2 Pohlig-Hellman方法

在 Silver之后, Pohlig和 Hellman发现, Abel群 G的阶的平滑性对于在 G中求解离散对数问题是有帮助的.现设 $n_h=\prod_{p^e \| n_h} p^{e_p}$,对于 $y\in H$,由中国剩余定理,要计算 $m=\log_h y$,只须求出所有 $m \bmod p^{e_p}$即可. 为计算 $m \bmod p^e$,其中, $p^e \| n_h$, $e\geqslant 1$,令 $m\equiv\sum_{i=0}^{e-1} m_i p^i \bmod p^e$,这里, $m_i\in\{0,1,\cdots,p-1\}$.由 $h^m=y$可知

$$(yh^{-(m \bmod p^i)})^{n_h/p^{i+1}}=(h^{n_h/p})^{m_i},$$

于是,问题转化为求 $\bar{y}_i=(yh^{-(m \bmod p^i)})^{n_h/p^{i+1}}$对于 $\bar{h}=h^{n_h/p}$的对数,因为 $\bar{h}$的阶为 p,当 p较小时 $\log_{\bar{h}}\bar{y}_i$是易求的. 该算法的时间复杂度为 $\sum_{p|n_h} O(\overline{e_p \max(e_p,p)}\log(p\min(e_p,p)))$.

由于上两算法关于 n_h或其最大素因子的长度是纯指数复杂度的,当 n_h含较大素因子 (比如,含长度≥160bit的素因子)时失效,这对椭圆曲线密码体制构不成真正的威胁,针对椭圆曲线离散对数问题进行的密码分析才是该体制面临的真正考验. 为了能方便计算椭圆曲线的阶,一类被称为"超奇异椭圆曲线"的特殊椭圆曲线 E/F_q(其中, $q=p^m$是素数幂)曾被建议用于建立密码体制,但是, Menezes等于 1993年证明[18],对于超奇异椭圆曲线 E/F_q, $E(F_q)$上的离散对数问题可在概率多项式时间内归约为 F_q的扩域 F_{q^k}上的离散对数问题,其中 $k\leqslant 6$,当 $p\neq 3$时, $k\leqslant 4$,这从根本上否定了超奇异椭圆曲线用于密码系统的可能性.所幸的是,这类椭圆曲线极易识别和避免. Semaev于最近也找到一类不宜用于密码体制的椭圆曲线,他在文献[19]中指出,对特征为 p的域 K上的椭圆曲线 E/K, $E(K)$的 p阶子群中的离散对数问题可在线性时间内归约为 K的加法群上的离散对数问题,这就是说,对大素域 $\boldsymbol{Z}_p$上的椭圆曲线 $E/\boldsymbol{Z}_p$,若# $E(\boldsymbol{Z}_p)=p$则 $E(\boldsymbol{Z}_p)$中的离散对数问题可在线性时间内归约为 $\boldsymbol{Z}_p$的加法群上的离散对数问题,从而可在线性时间内求解(这类椭圆曲线称为异常(anomalous)曲线). 这个结果多少有些令人惊异,更令人惊异的也许是这个结果早就被几个数论学家(比如 Ed Schaefer)假定是众所周知的事实而未发表,密码学界则对此一无所知, 1997年前制定的各种密码标准从未考虑到这种情况. 对椭圆曲线密码体制的攻击,还应提到文献[20],该文献利用椭圆曲线的结构特性改进 Pllard d方法,从而产生一个加速因子. 现令 $K=GF(2^n)$为 2^n元域,并设 K上的椭圆曲线 E/K的系数均在子域 $GF(2)$之中(这类曲线称为子域曲线).文献[20]中给出的求解 $E(K)$上离散对数问题的改进 Pllard d方法较原始 Pllard d方法期望运行时间降低 $\overline{n/e}$倍,尽管这一结果并未改进算法时间复杂度的阶,但当 e较小时,其对安全性的影响也不可忽视.

综上所述,椭圆曲线密码体制的安全性依赖于椭圆曲线离散对数问题的难解性,为保证体制的安全性,所使用的基点的阶应含长度不小于 160bit的素因子,超奇异椭圆曲线及异常椭圆曲线是目前仅知的不宜用于密码体制的椭圆曲线[21]. 使用子域曲线则应谨慎.

从上面的讨论可以看到,椭圆曲线密码体制的分析结果并不丰硕,上面所述的结果便是到目前为止仅有的有影响的结果,这可从正反两方面来理解: 这种密码体制确实是强的,或者,这种密码体制尚未被很好地认识,不管从哪个方面看,椭圆曲线密码体制还需进一步地深入研究. 事实上, 1997年以来,椭圆曲线密码体制及其安全性分析引起了密码学家及各界的极大关注与重视,现已形成了研究热点,有关各界,包括学校(如 Royal Holloway College)、商业组织(如 Certicom)及政府(如美国国家安全局)已在从各个方面探索椭圆曲线密码技术,这种密码体制也引起了"密码体制标准"研制者的极大兴趣. IEEE标准 P1363/D8(1998年 10月版)及 P1363/D9(1999年 2月版)对椭圆曲线密码体制作了较以前更为详尽的讨论,成为重点内容之一. ANSI(美国国家标准局)授权的金融业标准委员会 X9正在制定椭圆曲线数字签名标准 X9.62和密钥协商及传递标准 X9.63, RSA实验室也不甘落后,也已开始着手制定编号为 PKCS# 13的椭圆曲线密码标准,该标准将融合、平衡其他标准,并与其他 PKCS标准有机结合,对椭圆曲线密码体制实现的细节作出更具体的规定. 在学术界, 1997年 11月 Waterloo大学组织了一个专门的学术会议,研究椭圆曲线离散对数问题,众多著名密码学家及数学家应邀参加. 但直到目前,在密码分析方面仍未取得实质性进展,这种情况持续时间

越长,越使人们相信椭圆曲线密码体制的强度. 大多数密码学家对这种密码体制的强度及应用前景越来越抱乐观态度. 像 RSA一样,只有经过了长时间的分析,椭圆曲线密码体制才会真正为人们所接受.

5 椭圆曲线的选取

要建立椭圆曲线密码体制,首要的问题是选取一个合适的背景有限域 K 及在 K 上选取一条合适的椭圆曲线 E/K. 从实用观点看,K 有两种选择: 大素域 $\boldsymbol{Z}_p$ 或特征为 2的有限域 $GF(2^n)$.从近年来的实践结果看,大素域更为有效一些 (这与人们的预想不同). 椭圆曲线的选取则要考虑安全性、实用性等诸多因素,有些密码体制 (如, ElGamal签名体制、DSS签名体制) 需要知道 E 的阶# $E(K)$或# $E(K)$的一个大素因子,另一些体制 (如, Diffie–Hellman密钥交换协议、ElGamal加密体制) 虽不需要知道 $E(K)$的阶,但为避免 Pohlig–Hellman攻击,需保证# $E(K)$中有大素因子. 椭圆曲线的选取现有两种可以考虑的方法.

(1) 随机选取

随机选取一条椭圆曲线 E/K,计算其阶# $E(K)$直到获得满意的曲线为止. 由于这种方法的随机性,从安全性角度来看这是一种理想的方法.

Hasse定理告诉我们一个关于# $E(F_q)$的估计: 令# $E(F_q)=q+1-t$,则$|t|\leqslant 2\sqrt{q}$,但要具体求出# $E(F_q)$却并非易事, Schoof在这方面做出了开创性的成果[22]. 令 φ是 $E(\bar{F}_q)$上的 Frobenius自同态:

$$\varphi:(x,y)\mapsto(x^q,y^q)\quad\forall\,(x,y)\in E(\bar{F}_q)$$

其特征方程为 $\varphi^2-t\varphi+q=0$,其中,$t\in\boldsymbol{Z}$,$|t|\leqslant 2\sqrt{q}$,# $E(F_q)=q+1-t$.设 l 是一个小素数,$E[l]$为 $E(\bar{F}_q)$的 l-扭点构成的子群,通过将 φ限制在 $E[l]$中,利用搜索可求出 t'满足 $t'\equiv t \bmod l$,即对于小素数 l 可求出 $t \bmod l$. Schoof算法的基本想法就是对一系列小素数 $l=3,5,7,\cdots,L$,其中,L 满足$\prod_{\substack{\text{素数}\\ p\leqslant L\\ p\neq 2}}p\geqslant 4\sqrt{q}$,求出$t \bmod l$,从而由中国剩余定理得到 t,进而得到# $E(F_q)$.

Schoof的这个算法具有时间复杂度 $O(\log^9 q)$,理论上是个有效算法,在实际中却不实用,但这个方法指出了求# $E(F_q)$的一个努力方向,引起了极大关注.自此以后,围绕计算 $t \bmod l$ 已有大量成果发表出来[23,24],并且在方法的实现上有了较大进展. Lercier和 Morain曾在 DEC Alpha3000/500上计算出 $GF(2^{300}+157)$上椭圆曲线的阶,也曾在 DEC Alpha Workstation 250(266MHz)上计算出 $F_{2^{300}}$上椭圆曲线的阶,用时都是大约 40分钟.目前记录则是 DEC Alpha Workstation 250上用 103天 5小时计算出了 $F_{2^{1301}}$上一条椭圆曲线的阶. 由于阶中含大素因子的椭圆曲线相对较少 (在 $F_{2^{196}}$上约 2‰),利用该方法建立椭圆曲线密码体制仍存在困难,特别地,对求阶中含 2个大素因子以上的椭圆曲线,上述方法完全不可行.

(2) 构造给定阶的椭圆曲线

Atkin和 Morain的论文“Elliptic Curves and Primality Proving”[4]使人们看到了获得密码体制所需要的椭圆曲线的另一条途径,该文提出的利用复乘构造素域 $\boldsymbol{Z}_p$ 上具有特定阶椭圆曲线的思想及方法已引起了广泛关注,并被多篇论文讨论、改进[25-28].密码标准 IEEE P1363(草稿, 1999.2)也采用了该策略作为生成椭圆曲线的方法之一. 利用这种思想,本文作者在文献[28]中提出并实现了素数阶及阶中含多个大素因子的椭圆曲线的构造方法.

设 $-D$ 是一个负奇基本判别式, $H_D(X)$表示 $-D$ 的 Hilbert类多项式,又设 p 是一个素数,若整数 x,y 满足 $4p=x^2+Dy^2$,则对 $H_D(X)$的任意关于模 p 的根 j_0,必存在 j-不变量为 j_0 的椭圆曲线 $E/\boldsymbol{Z}_p$满足

$$\#E(\boldsymbol{Z}_p)=(x-2)^2+Dy^2 \tag{3}$$

虽然椭圆曲线不能由 j-不变量唯一确定,通过 j-不变量 j_0 找出满足式 (3)的椭圆曲线是容易的. 事实上, j-不变量为 j_0 的椭圆曲线恰构成 2个等势的同构类.

下面是文献[28]中提出的构造素域 $\boldsymbol{Z}_p$ ($p>3$)上的素数阶椭圆曲线的方法的简化描述.

(1) 取定负奇基本判别式 $-D$,使其具有小的类数 (比如, $D=19$);

(2) 在适当范围内,随机选取整数 x,y,令 $4q=(x^2+Dy^2)$,检测 q 的素性,直到 q 是素数为止;

(3) 令 $4p=(x+2)^2+Dy^2$, 检测 p 的素性,若 p 不是素数,返回第 2步,直到 p 为素数;

(4) 计算 $H_D(X)\equiv 0 \bmod p$ 的根 j_0(由于 $-D$ 具有小的类数,该方程易解);

(5) 构造 j-不变量为 j_0 的椭圆曲线 $E: y^2=x^3+ax+b$,取随机数 $c\in Z_p^*$,在 $E': y^2=x^3+c^2ax+c^3b$ 上任取一点 $P\neq 0$,判断 $qP=0$? 直到成立.

可以证明,算法结束时 E' 即为 Z_p 上 q 阶椭圆曲线[28].

该算法具有较高的效率,可轻易在大素域 Z_p 上构造出素数阶椭圆曲线.

受到 MOV 归约的启示,人们对利用复乘构造椭圆曲线的方法存在着某些疑虑,对 p 的形状的限制、对 $-D$ 的限制是否会影响体制的安全性? 国内外密码学家对此有着广泛关注,但到目前为止,没有任何线索说明这种曲线存在弱点.

6 结 论

从上述讨论可以看出,椭圆曲线密码体制正受到学术界、开发商、政府部门、密码标准研制组织等有关各界的重视,已形成研究、开发热点并开始从理论走向实用.虽然对这种密码体制人们的认识尚嫌不足,但最近几年内,它极有可能在某些领域成为现存密码体制的替代者,椭圆曲线密码产品会逐渐为人们所了解,与安全性相关的椭圆曲线离散对数问题相应会受到更多的关注.可以预计,在最近几年内,椭圆曲线阶的计算方法及实现技术会有较大进展,对具有小的复乘的椭圆曲线的密码分析也许会得到更为确定性的结论.

参 考 文 献

1 Lenstra H W. Factoring integers with elliptic curves. Annals of Mathematics, 1987, 126: 649~673

2 Montgomery P. Speeding the pollard and elliptic curve methods of factorization. Mathematics of Computation, 1987, 48: 243~264

3 Montgomery P. A FFT extension of the elliptic curve method of factorization. [Ph D dissertation], UCLA, Los Angeles, 1992

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

5 Goldwasser S, Kilian J. Almost all primes can be quickly certified. In: Proc of the 18th Annual ACM Symposium on Theory of Computing, 1986. 316~329

6 Pomerance C. Very short primality proofs. Mathematics of Computation, 1987, 48: 315~322

7 Miller V. Uses of elliptic curves in cryptography. In: Williams H C eds. Advances in Cryptology—— CRYPTO '85 Proceedings, LNCS 218. Berlin: Springer-Verlag, 1986. 417~426

8 Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48: 203~209

9 Robshaw M, Yin Y. Elliptic Curve Cryptosystems. An RSA Laboratories Technical Note. Revised June 27, 1997

10 Silverman J. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986

11 Menezes A. Elliptic Curve Public Key Cryptosystems. Boston: Kluwer Academic Publishers, 1993

12 Demytko N. A new elliptic curve based analogue of RSA. In: Helleseth ed. Advances in Cryptology—— Eurocrypt '93 Proceedings, LNCS 765. Berlin: Springer-Verlag, 1994. 40~49

13 Koyama K, Maurer U M, Okamoto T, Vanstone S A. New public-key schemes based on elliptic curves over the ring Zn. In: Feigenbaum J eds. Advances in Cryptology—— CRYPTO '91 Proceedings, LNCS 576. Berlin: Springer-Verlag, 1992. 40~49

14 Coppersmith D, Odlyzko A M, Schroeppel R. Discrete logarithms in GF(p). Algorithmica, 1986, 1: 1~15

15 Lenstra A K, Lenstra H W. The Development of the Number Field Sieve. Berlin: Springer-Verlag, 1993

16 Pollard J M. Monte Carlo methods for index computation(mod p). Mathematics of Computation, 1978, 32: 918~924

17 Pohlig S C, Hllman M E. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans Inform Theory, 1978, 24: 106~110

18 Menezes A, Okamoto T, Vanstone S A. Reducing elliptic curves logarithms to logarithms in a finite field. IEEETIT, 1993, 39(5): 1639~1646

19 Semaev I A. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Mathematics of Computation, 1998, 67(221): 353~356

20 Wiener M J, Zuccherato R J. Faster attacks on elliptic curve cryptosystems. In: Tavares S, Meijer H eds. Selected Areas in Cryptography—— SAC'98. Berlin: Springer-Verlag, 1998

21 IEEE P1363/D9 (Draft Version 9). Standard specification for public key cryptography. 1999. http://grouper.ieee.org/groups/1363

22 Schoof R. Elliptic curves over finite field and the computation of square roots mod p. Mathematics of Computation, 1985, 44: 483~494

23 Lercier R, Morain F. Counting the number of points on elliptic curves over finite fields: strategies and performances. In: Guillou L C, Quisquater J J eds. Advances in Cryptology—— EUROCRYPT'95 Proceedings, LNCS 921, 1995. 79~94

24 Lercier R. Finding good random elliptic curves for cryptosystems defined over. In: Fumy W ed. Advances in Cryptology—— EUROCRYPT'97 Proceedings, LNCS 1233. Berlin: Springer-Verlag, 1997. 379~392

25 Morain F. Building cyclic elliptic curves modulo large primes. In: Davies D W ed. Advances in Cryptology—— EUROCRYPT'91 Proceedings, LNCS 547. Berlin: Springer-Verlag, 1991. 328~336

26 Miyaji A. Elliptic curves over Fp suitable for cryptosystems. In: Seberry J, Zheng Y eds. Advances in Cryptology—— AUSCRYPT'92 Proceedings, LNCS 718. Berlin: Springer-Verlag, 1993. 479~491

27 Lay G J, Zimmer H G. Constructing elliptic curves with given group order over large finite fields. In: Adleman L M, Huang M D eds. Algorithmic Number Theory Proceedings, LNCS 877. Berlin: Springer-Verlag, 1994. 250~263

28 徐秋亮,李大兴.适用于建立密码机制的椭圆曲线的建造方法及实现.计算机学报,1998,21(12):1059~1065
(Xu Qiuliang, Li Daxing. Constructing elliptic curves suitable for cryptosystems—— Methods and implementation. Chinese Journal of Computers(in Chinese), 1998, 21(12): 1059~1065)