环 Z_n 上椭圆曲线的群法则及其在 Paillier 系统中的应用

张李军,王鲲鹏
(中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: 本文研究了定义在环 Z_n 上椭圆曲线 E 的有理点集 $E(Z_n)$的群的定义法则,以及这类椭圆曲线在密码学上的应用.我们给出了环 Z_n 上椭圆曲线明确的点加公式,使得 $E(Z_n)$形成一个交换群,从理论上清晰地解决了以往在该类曲线上某些点相加不能定义的问题.为了在密码学上方便地应用这类椭圆曲线,还给出了在该加法法则下的 $E(Z_n)$的群结构.利用该群结构选取合适的参数,修复了椭圆曲线 Paillier 密码系统的安全缺陷.

关键词: 环上椭圆曲线; 加法法则; 群结构; 椭圆曲线 Paillier 系统
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 08-1733-06

Group Law of Elliptic Curves over Z_n and Its Application in Paillier Schemes

ZHANG Li-jun, WANG Kun-peng
(*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: Group law of rational points $E(Z_n)$ on elliptic curves E over Z_n and application of this group law are studied in this paper. We present explicit addition formulae to make $E(Z_n)$ an abelian group. This solves the problem that some points addition can not be defined using other addition laws in the literature. For the convenient cryptographic application of such elliptic curves, we give the group structure of $E(Z_n)$ under our addition law. We propose a remedy for the original elliptic curves Paillier schemes which have security defectiveness.

Key words: elliptic curve over ring; addition law; group structure; Paillier schemes

1 引言

椭圆曲线密码体制一般是利用有限域上椭圆曲线,如 ECMQV 密钥交换协议,ECIES 加密方案和 ECDSA 数字签名算法[1]等.这类体制的安全性基于椭圆曲线离散对数问题的难解性.人们对环 Z_n 上椭圆曲线的应用也进行了探索.这些应用包括:Lenstra[2]的因子分解方法,Koyama 等[3]的加密和签名方案,Demytko[4]的模拟 RSA 的椭圆曲线密码体制,Meyer 等[5]的安全性等价于因子分解的椭圆曲线密码体制.近几年来,这方面的研究依然受到关注.张亚娟等[6]给出了一种前向安全的签名体制.朱文余等[7]给出了一种多方密钥交换协议.张宁等[8]给出了一种基于身份的加密体制.这些密码体制的安全性基于大整数因子分解的困难性.

椭圆曲线上的点加运算是构造密码体制的基础,但环 Z_n 上椭圆曲线的理论还比较欠缺,按以往的文献中所用的点加运算,$E(Z_n)$甚至不能形成群.王念平等[9]研究了这类曲线上几种点加的定义,说明了这些公式不能形成群的原因,却没有能给出解决办法.李明等[10]利用一般环上椭圆曲线的点加公式解决了环 $Z_n(n=p^m)$上椭圆曲线的点加问题.我们也用类似的方法,给出了环 $Z_n(n=p^iq^j)$上椭圆曲线的点加定义使得 $E(Z_n)$成为一个群,完善了环 Z_n 上椭圆曲线的理论.

2 环 Z_n 上椭圆曲线点的加法定义

以往对环 Z_n 上椭圆曲线点加的定义方法,可分为仿射和射影两种情况,参见文献[7,9].

(1)仿射情形 Z_n 上椭圆曲线采用仿射方程定义:

$$E_n(a,b): y^2 \equiv x^3 + ax + b \pmod{n}$$

且满足 $gcd(4a^3+27b^2, n)=1$,其上的有理点集定义为:

收稿日期:2010-09-28;修回日期:2010-12-24
基金项目:国家 973 重点基础研究发展计划(No.2007CB311201);国家自然科学基金(No.60970153)

$E(Z_n)=\{(x,y)\in Z_n^2 \mid y^2\equiv x^3+ax+b(\bmod n)\}\cup\{O\}$ 其中 O 为无穷远点.有两种定义:

第一种:套用有限域上点加的公式,设 $P_i=x_i+y_i$, $i=1,2,3$. $P_3=P_1+P_2$,则有

$$x_3=\lambda^2-x_1-x_2(\bmod n),\ y_3=\lambda(x_1-x_3)-y_1(\bmod n)$$

其中 $\lambda=(y_2-y_1)/(x_2-x_1)$,if $x_2\neq x_1$,或 $\lambda=(3x_1^2+a)/(2y_1)$,if $x_2=x_1$.此时只有当 λ 的分母与 n 互素才能计算 P_3,因此曲线上某些点相加无定义.

第二种:当 $n=pq$ 时,对点 M 坐标模 p 和模 q,分别记为 M_p 和 M_q.作映射:

$$\phi: E_n(a,b)\rightarrow E_p(a,b)\times E_q(a,b),$$
$$M=(x,y)\mapsto M_p+M_q$$

对 $P,Q\in E_n(a,b)$,定义:$P+Q=\phi^{-1}(P_p+Q_p,P_q+Q_q)$.当两个分量中仅有一个为无穷远点时,在 $E_n(a,b)$上找不到相对应的点.这两种点加定义都不满足封闭性,不能使 $E(Z_n)$形成群.

(2)射影情形 若 Z_n 上椭圆曲线 $E_n(a,b)$采用齐次方程定义,即:

$$E_n(a,b): y^2z\equiv x^3+axz^2+bz^3(\bmod n)$$

且满足 $gcd(4a^3+27b^2,n)=1$.

该曲线上点的等价关系$\backsim$定义为:$(x:y:z)\backsim(x':y':z')$当且仅当存在 $\mu\in Z_n^{\times}$(乘法可逆元),使得$(x:y:z)=\mu(x':y':z')$. $E_n(a,b)$上点的加法定义与仿射情形中第二种定义方法相同,参见文献[9].虽然此时 ϕ 是一个双射,$E(Z_n)$在理论上能形成群,但在 $E(Z_n)$上建立的密码体制的陷门是 n 的分解.对于不知道陷门的用户(如加密者或是验证签名者),则无法计算任意的点相加.因此这样的点加定义并不适合密码学上的应用.我们通过简化一般环上椭圆曲线的加法定义,得出了环 Z_n 上椭圆曲线明确的点加公式,使得 $E(Z_n)$在这种运算下形成群,并且即使不知道的分解也可以计算点加.

3 一般环上椭圆曲线点的加法定义

我们先介绍一些基本的定义.设 R 是一个有单位元 1 的交换环,且 $6\in R^{\times}$(R 中的可逆元).这里假设 6 是可逆元是为了下面使用简化的 Weierstrass 曲线形式.

定义 1 环 R 上的多元组$(x_1,x_2,\cdots,x_m)$称为本原的,如果存在 $r_i\in R$ 满足 $\sum_{i=1}^{m}r_ix_i=1$.特别地,当 $R=Z_n$ 时,本原的意思即为 $gcd(x_1,x_2,\cdots,x_m,n)=1$.

定义 2 环 R 上的矩阵$(a_{ij})_{l\times k}$称为本原的,如果矩阵所有元素组成的多元组$(a_{11},a_{12},\cdots,a_{lk})$是本原的,且矩阵的所有 2×2 阶子矩阵的行列式为 0.

定义 3 环 R 上的射影平面$\mathbb{P}^2(R)$定义为:$\mathbb{P}^2(R)=\{(x,y,z)\in R^3 \mid (x,y,z)$是本原的$\}/\backsim$,其中等价关系$\backsim$定义为:$(x,y,z)\backsim(x',y',z')$当且仅当存在 $\mu\in R^{\times}$,使得$(x,y,z)=\mu(x',y',z')$.记(x,y,z)所在的等价类为$(x:y:z)$.

定义 4 设环 R 上椭圆曲线 E 定义为 $y^2z=x^3+axz^2+bz^3$ 且满足 $4a^3+27b^2\in R^{\times}$,其上的有理点集定义为:$E(R)=\{(x:y:z)\in\mathbb{P}^2(R) \mid y^2z=x^3+axz^2+bz^3\}$.

定义 5 若 R 上的本原矩阵$(a_{ij})_{l\times k}$存在行的线性组合是本原的,则对 $E(R)$的点 $P_i=(x_i:y_i:z_i)$, $i=1,2,3$. $P_3=P_1+P_2$,通过以下三组公式来计算 P_3.

$$\begin{aligned}
(1)\ x_3' &= (x_1y_2-x_2y_1)(y_1z_2+y_2z_1)+(x_1z_2-x_2z_1)y_1y_2\\
&\quad -a(x_1z_2+x_2z_1)(x_1z_2-x_2z_1)\\
&\quad -3b(x_1z_2-x_2z_1)z_1z_2\\
y_3' &= -3x_1x_2(x_1y_2)-y_1y_2(y_1z_2-y_2z_1)\\
&\quad -a(x_1y_2-x_2y_1)z_1z_2+a(x_1z_2+x_2z_1)\\
&\quad \cdot(y_1z_2-y_2z_1)+3b(y_1z_2-y_2z_1)z_1z_2\\
z_3' &= 3x_1x_2(x_1z_2-x_2z_1)-(y_1z_2+y_2z_1)\\
&\quad \cdot(y_1z_2-y_2z_1)+a(x_1z_2-x_2z_1)z_1z_2\\
(2)\ x_3'' &= y_1y_2(x_1y_2+x_2y_1)-ax_1x_2(y_1z_2+y_2z_1)\\
&\quad -a(x_1y_2+x_2y_1)(x_1z_2+x_2z_1)\\
&\quad -3b(x_1y_2+x_2y_1)z_1z_2-3b(x_1z_2+x_2z_1)\\
&\quad \cdot(y_1z_2+y_2z_1)+a^2(y_1z_2+y_2z_1)z_1z_2\\
y_3'' &= y_1^2y_2^2+3ax_1^2x_2^2+9bx_1x_2(x_1z_2+x_2z_1)\\
&\quad -a^2x_1z_2(x_1z_2+2x_2z_1)-a^2x_2z_1(2x_1z_2+x_2z_1)\\
&\quad -3abz_1z_2(x_1z_2+x_2z_1)-(a^3+9b^2)(z_1^2z_2^2)\\
z_3'' &= 3x_1x_2(x_1y_2+x_2y_1)+y_1y_2(y_1z_2+y_2z_1)\\
&\quad +a(x_1y_2+x_2y_1)z_1z_2+a(x_1z_2+x_2z_1)\\
&\quad \cdot(y_1z_2+y_2z_1)+3b(y_1z_2+y_2z_1)z_1z_2\\
(3)\ x_3''' &= (x_1y_2+x_2y_1)(x_1y_2-x_2y_1)\\
&\quad +ax_1x_2(x_1z_2-x_2z_1)+3b(x_1z_2+x_2z_1)\\
&\quad \cdot(x_1z_2-x_2z_1)-a^2(x_1z_2-x_2z_1)z_1z_2\\
y_3''' &= y_1y_2(x_1y_2-x_2y_1)-3ax_1x_2(y_1z_2-y_2z_1)\\
&\quad +a(x_1y_2+x_2y_1)(x_1z_2-x_2z_1)\\
&\quad +3b(x_1y_2-x_2y_1)z_1z_2-3b(x_1z_2+x_2z_1)\\
&\quad \cdot(y_1z_2-y_2z_1)+a^2(y_1z_2-y_2z_1)z_1z_2\\
z_3''' &= -(x_1y_2+x_2y_1)(y_1z_2-y_2z_1)\\
&\quad -(x_1z_2-x_2z_1)y_1y_2-a(x_1z_2+x_2z_1)\\
&\quad \cdot(x_1z_2-x_2z_1)-3b(x_1z_2-x_2z_1)z_1z_2
\end{aligned}$$

可证明由这三组公式得到的矩阵 $\begin{pmatrix}x_3' & y_3' & z_3'\\ x_3'' & y_3'' & z_3''\\ x_3''' & y_3''' & z_3'''\end{pmatrix}$ 是本原的,再由 R 所满足的条件知,该矩阵存在行的线性组合是本原的,记为$(x_3:y_3:z_3)$.定义该椭圆曲线上有

理点集 $E(R)$的群运算法则如下: 零元: $O=(0:1:0)$, 逆元: $-(x_1:y_1:z_1)=(x_1:-y_1:z_1)$,加法:$(x_1:y_1:z_1)+(x_2:y_2:z_2)=(x_3:y_3:z_3)$.此时 $E(R)$形成一个交换群,证明参见文献[11].该定义解决了点加的定义问题,还没有计算一般的环 R 的本原线性组合的有效算法.对于环 Z_n 的情形,我们却找到了简洁的算法.

4　环 Z_n 上椭圆曲线的点加公式

密码学上已用到的环 Z_n 的模的形式有 $n=pq$,参见文献[3~8], $n=p^2q$, $n=p^2q^2$, $n=p^m$,参见文献[10,12].我们将详细讨论各种情形的环 Z_n 上椭圆曲线的加法公式.

(1)当 $n=p^m$, $m\geqslant 1$ 时,李明,王鲲鹏[10]证明了如下的结果:

定理 1　设是定义在环 $R=Z_n(n=p^m)$上的椭圆曲线, $P_1,P_2\in E(R)$, $P_3=P_1+P_2$, $P_i=(x_i:y_i:z_i)$.若 $P_1 \pmod p\neq P_2 \pmod p$,则令$(x_3:y_3:z_3)=(x_3':y_3':z_3')$;否则令$(x_3:y_3:z_3)=(x_3'':y_3'':z_3'')$.

(2)当 n 含有两个素因子时,我们将 n 的形式推广到 $n=p^iq^j$,并证明了如下的结果:

定理 2　设是定义在环 $R=Z_n$ 上的椭圆曲线,其中 $n=p^iq^j$, i,j 为正整数,则 E 上的加法公式也只需要公式组(1)和公式组(2).设 $P_1,P_2\in E(R)$, $P_3=P_1+P_2$,其中 $P_t=(x_t:y_t:z_t)$, $t=1,2,3$,按如下的计算 P_3:

若 $P_1=P_2$,则选用公式组(2)计算出$(x_3'':y_3'':z_3'')$.令$(x_3:y_3:z_3)=(x_3'':y_3'':z_3'')$;

若 $P_1\neq P_2$,则先选用公式组(1)计算出$(x_3':y_3':z_3')$.若 $gcd(x_3',y_3',z_3',n)=1$,则令$(x_3:y_3:z_3)=(x_3':y_3':z_3')$;若 $gcd(x_3'',y_3'',z_3'',n)>1$,则再用公式组(2)计算出$(x_3'':y_3'':z_3'')$.

若 $gcd(x_3'',y_3'',z_3'',n)=1$,则令$(x_3:y_3:z_3)=(x_3'':y_3'':z_3'')$;否则令$(x_3:y_3:z_3)=(x_3'+x_3'':y_3'+y_3'':z_3'+z_3'')$.

要证明定理 2,需要几个引理.我们需要验证环 Z_n 满足定义 5 中的条件.

引理 1(存在性)　环 Z_n 上的本原矩阵存在行的线性组合是本原的.

证明　设$(a_{ij})_{l\times k}$是环 Z_n 上的本原矩阵,则该矩阵所有元素的最大公因子(设为 gcd_1)与 n 互素,且矩阵的行是成比例的.即存在向量 $\boldsymbol{v}$ 以及整数 $a_1,a_2,\cdots,a_l$ 使得矩阵的第行可以写成 $a_i\boldsymbol{v}$ 的形式.由条件 $gcd_1=gcd(a_1,a_2,\cdots,a_l)\,gcd(\boldsymbol{v})$, $gcd(gcd_1,n)=1$ 得到 $gcd(\boldsymbol{v},n)=1$, $gcd(a_1,a_2,\cdots,a_l,n)=1$.因此存在数 $r_1,r_2,\cdots,r_l$ 满足 $\sum_{i=1}^{l} r_ia_i=1$,从而进一步得到本原线性组合 $\boldsymbol{v}=\boldsymbol{v}\sum_{i=1}^{l} r_ia_i=\sum_{i=1}^{l} r_ia_i\boldsymbol{v}$.

引理 2(唯一性)　环 Z_n 上本原矩阵行的本原线性组合在等价关系$\backsim$下是唯一的.

证明　我们设矩阵$(a_{ij})_{l\times k}$行的任意两个本原线性组合分别是 $\boldsymbol{v}_1=\sum_{i=1}^{l} r_ia_i\boldsymbol{v}$ 和 $\boldsymbol{v}_2=\sum_{i=1}^{l} s_ia_i\boldsymbol{v}$.令 $r=\sum_{i=1}^{l} r_ia_i\boldsymbol{v}$, $s=\sum_{i=1}^{l} s_ia_i$,则有 $\boldsymbol{v}_1=r\boldsymbol{v}$, $\boldsymbol{v}_2=s\boldsymbol{v}$.由 $\boldsymbol{v}_1$ 和 $\boldsymbol{v}_2$ 是本原的可知 $gcd(r,n)=gcd(s,n)=1$.显然有 $\boldsymbol{v}_1=rs^{-1}\boldsymbol{v}_2$,其中 s^{-1}为 s 在 Z_n 中的乘法逆元.

证明　我们首先证明只需公式组(1)和(2)即可构成的一组加法公式.

为了叙述方便,我们用 $E_n(a,b)$代替 E,采用反证法.设 P_1 和 P_2 是 $E_n(a,b)$上的两个点,假设用公式组(1)和(2)计算 P_1+P_2 同时失效,不能得到一个本原的线性组合,那么情况只可能 $p\mid gcd(x_3':y_3':z_3')$且 $p\mid gcd(x_3'':y_3'':z_3'')$(*),或者 $q\mid gcd(x_3':y_3':z_3')$且 $q\mid gcd(x_3'':y_3'':z_3'')$.这两种情况类似,我们只证明第一种情况.对曲线方程作系数模 p 的约化, $E_n(a,b)\rightarrow E_p(a \bmod p, b \bmod p)$,则有 $P_1(\bmod p)$和 $P_2(\bmod p)$是 $E_p(a \bmod p, b \bmod p)$上的点.考虑约化后的椭圆曲线,由定理 1 知,公式组(1)和(2)构成一组加法公式,而用这两组公式计算点 $P_1(\bmod p)+P_2(\bmod p)$的结果与用同样的公式计算 P_1+P_2 后再模 p 得到的结果是相同的.但由条件(*)知,此时在约化后的曲线上计算 $P_1(\bmod p)+P_2(\bmod p)$将失效,与定理 1 矛盾.即我们总能从公式组(1)和(2)的结果得到本原的线性组合,现在推导具体的计算公式.

(1)若 $P_1=P_2$,则$(x_3':y_3':z_3')=(0:0:0)$.此时若 $gcd(x_3'',y_3'',z_3'',n)>1$,则与前面证明的结论矛盾,所以有 $gcd(x_3'',y_3'',z_3'',n)=1$,即$(x_3'',y_3'',z_3'')$是本原的.令$(x_3:y_3:z_3)=(x_3'':y_3'':z_3'')$.

(2)若 $P_1\neq P_2$,且 $gcd('x_3,y_3',z_3',n)=1$,即(x_3',y_3',z_3')是本原的,令$(x_3:y_3:z_3)=(x_3':y_3':z_3')$.

(3)若 $P_1\neq P_2$,且 $gcd(x_3':y_3':z_3',n)>1$,不妨设为 p(为 q 时证明相同).此时若 $gcd(x_3'',y_3'',z_3'',n)=1$,则令$(x_3:y_3:z_3)=(x_3'',y_3'',z_3'',n)$.若 $gcd(x_3'',y_3'',z_3'',n)>1$,则一定有 $gcd(x_3'',y_3'',z_3'',n)=q$.令$(x_3:y_3:z_3)=(x_3'+x_3'':y_3'+y_3'':z_3'+z_3'')$.易知该线性组合是本原的.

我们称定理 2 中得到的公式为本原加法公式.该本原加法公式还是完备的(适用于任何点).

例　设 $E:y^2z=x^3-xz^2+z^3$ 是定义在环 Z_{35}上的椭圆曲线,根据本原加法公式有:

(1)无穷远点 O 相加,即$(0:1:0)+(0:1:0)$.由公式(2)知$(0:1:0)+(0:1:0)=(0:1:0)$.

(2)一个非无穷远点 P 和 O 相加,选取任何一个公式都会得到结果 P.

如用公式组(1),有(0:6:1) + (0:1:0) = (0:29:34) = (0:6:1).

如用公式组(2),有(0:6:1) + (0:1:0) = (0:1:6) = (0:6:1).

(3)倍点计算,直接选用公式组(2). 如 2(1:6:1) = (22:8:13).

(4)两个不同的点相加且都不是点 O,这时有几种情况:

(a)互为负点,则两个公式都得到和为. 如计算(1:1:1) + (1:34:1)都会得到(0:8:0),即点 O.

(b)只需用一个公式组即可. 例如由公式组(1)计算得(1:6:1) + (3:5:1) = (5:3:8).

由公式组(2)则有(1:6:1) + (3:5:1) = (30:18:13),它们是同一个点.

(c)需要用到本原线性组合. 如公式组(1)给出(1:6:1) + (15:6:1) = (21:21:14). 公式组(2)给出(1:6:1) + (15:6:1) = (15:15:20),则有(1:6:1) + (15:6:1) = (21 + 15:21 + 15:14 + 20) = (1:1:34).

5 $E(Z_n)$的群结构

下面我们将推导在本原加法公式下 $E(Z_n)$的群结构,首先我们易得如下的定理:

定理 3 设是定义在环 $Z_{n_1n_2}$上的椭圆曲线,其中,n_1n_2是互素的奇数,则在本原加法公式下有群同构:$E(Z_{n_1n_2}) \simeq E(Z_{n_1}) \times E(Z_{n_2})$.

证明 由定理2的证明知,环 $Z_{n_1n_2}$满足定义5的条件,而 Washington[11]给出了在定义5中的加法下有该群结构成立. 而本原加法公式只是定理5中公式的简化,因此有相同的群结构成立.

推论 1 设是定义在有限域上的椭圆曲线,则在本原加法公式下有群同构:

$$E(F_p) \simeq Z_{l_1} \times Z_{l_2},\ \text{其中}\ l_1 \mid l_2, l_1 \mid (p-1)$$

证明 当环 R 是一个域时,定义5的加法公式与通常按弦切律定义出的公式得到的结果一致[14],只是增加了公式的完备性. 因此这两种点加的定义方式给出相同的群运算,故群结构相同.

现在我们给出 $E(Z_{p^m})$的群结构:

定理 4 设 $E: y^2z = x^3 + axz^2 + bz^3$ 是定义在环 Z_{p^m}上的椭圆曲线,$2 \leqslant m \leqslant 4$,则在本原加法公式下有群同构:$E(Z_{p^m}) \simeq Z_{p^{m-1}} \times Z_{l_1} \times Z_{l_2}$,其中 $l_1 \mid l_2, l_1 \mid (p-1)$.

证明 对 E 的方程及该曲线上的点作模 p 的约化:$\phi, E(Z_{p^m}) \to \bar{E}(F_p), (x, y, z) \mapsto (\bar{x}, \bar{y}, \bar{z})$,在本原加法公式下,易知该映射是群同态. 首先证明 ϕ 是满射. 设 $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$,$\bar{F}(x, y, z)$为模 p 约化. 由 $gcd(4a^3 + 27b^2, p) = 1$ 知 $\bar{F}(x, y, z)$是椭圆曲线. 故对任意的 $\tilde{P}(x_0, y_0, z_0) \in E(F_p)$,有$\frac{\partial \bar{F}}{\partial x}(\tilde{P})$,$\frac{\partial \bar{F}}{\partial x}(\tilde{P})$,$\frac{\partial \bar{F}}{\partial x}(\tilde{P})$不全为零. 不妨设$\frac{\partial \bar{F}}{\partial x}(\tilde{P}) \neq 0$,任取$(y', z') \in Z_{p^m} \times Z_{p^m}$满足$(\bar{y}', \bar{z}') = (y_0, z_0)$,则方程 $F(x, y', z') = 0$ 模 p 约化后只有单根(否则 $\bar{F}(x, y, z) = 0$ 有奇异点),因此可由 Hensel 引理产生提升得到方程$(x, y', z') = 0$ 在 Z_{p^m}中的解 $P = (x', y', z')$使得 $\bar{P} = \tilde{P}$. 从而映射 ϕ 是满射.

下面考虑映射 ϕ 的核 $ker(\phi)$. 考察短正合列 $0 \to ker(\phi) \to E(Z_{p^m}) \to \bar{E}(F_p) \to 0$,对映射 ϕ,显然存在提升映射 $\psi: \bar{E}(F_p) \to E(Z_{p^m})$满足 $\phi\psi = I$,I 表示恒等映射. 因此该短正合列是分裂的. 我们得到 $E(Z_{p^m}) \simeq ker(\phi) \times \bar{E}(F_p)$. 因为 $ker(\phi)$中的点形如$(t_2p : 1 : t'p^3)$,由 Hensel 定理知,t 可取从 0 到 p^{m-1}的任意值. 而对任意的两个点$(t_1p : 1 : t'p^3)$和$(t_2p : 1 : t''p^3)$,若 $t_1 = t_2$,则$(t_1p : 1 : t'p^3) = (t_2p : 1 : t''p^3)$. 因此 $ker(\phi)$中点的个数为 $\# ker(\phi) = p^{m-1}$.

现在证明群 $ker(\phi)$是一个循环群. 当 $2 \leqslant m \leqslant 4$ 时,根据 $ker(\phi)$中点的形式知公式(2)可以简化为:$x_3 = x_1 + x_2$; $y_3 = 1$; $z_3 = 0$. 此时 $ker(\phi)$是由点$(p, 1, z)$生成的 p^{m-1}阶循环群.

由定理 3,4 和推论 1 立即得到如下结果:

定理 5 设 $E: y^2z = x^3 + axz^2 + bz^3$ 是定义在环 Z_n上的椭圆曲线,其中 $n = p^iq^j$,$2 \leqslant i, j \leqslant 4$,则在本原加法公式下有群同构:

$$E(Z_n) \simeq Z_{p^{i-1}} \times Z_{p^{j-1}} \times Z_{l_1} \times Z_{l_2} \times Z_{k_1} \times Z_{k_2}$$

其中 $l_1 \mid l_2, k_1 \mid k_2, l_1 \mid (p-1), k_1 \mid (q-1)$.

实际中环 Z_n 上椭圆曲线密码体制 i, j 的取值都小于 3,故定理 5 已满足需要. 但理论上,我们提出:

猜想 对任意取值为正整数的 i, j,定理 5 的结论仍然成立.

6 椭圆曲线 Paillier 系统

Paillier 把整数剩余类环上的 Paillier 系统移植到环上椭圆曲线有理点集上,构造了椭圆曲线 Paillier 系统,这是一类重要的利用环 Z_n 上椭圆曲线建立的密码系统,根据 n 的形式的不同,有三种不同的方案. 下面我们列出这些方案的系统参数,如表 1 所示. 完整的方案参见文献[12].

6.1 椭圆曲线 Paillier 系统的安全缺陷及修复

由于之前没有环 Z_{p^2}上椭圆曲线的点加公式,因此在构造方案二和三时,Paillier 采用将基域 F_p 上椭圆曲线提升到域F_{p^2}上的办法,再利用中国剩余定理得到基

表 1　椭圆曲线 Paillier 系统的三种方案

	n 的形式	曲线形式	模 p 后的曲线	模 q 后的曲线	基点的阶
一	pq	$E_n(0,b)$	超奇异曲线	超奇异曲线	$gcd(p+1,q+1)$
二	p^2q	$E_n(a,b)$	异常曲线的扭曲线	任意的曲线	$lcm(p(p+2),\#E_q)$
三	p^2q^2	$E_n(a,b)$	异常曲线的扭曲线	异常曲线的扭曲线	$pq\cdot lcm(p+2,q+2)$

注:表 1 中的曲线形式 $E_n(a,b)$即为定义 3.4 所定义的环 Z_n 上的椭圆曲线,$E_n(0,b)$表示曲线方程中 $a=0$. $\#E_q$ 表示曲线模 q 后的 F_q-有理点个数. *gcd* 和 *lcm* 分别表示最大公因子和最小公倍数.

点. Galbraith[13]注意到在这两种方案中上椭圆曲线都是异常曲线(anomalous)的二次扭曲线,从而构造出了分解的算法.由于方案二和三的安全性正是基于分解的困难性,因此导致它们都被攻破.

针对 Galbraith 提出的攻击算法,一种修复方法是用基域 F_p 上的一条随机曲线 E' 来代替异常曲线的扭曲线,但这种方法首先需要多次使用数点算法 SEA 来计算 $\#E'(F_p)$以寻找适合的曲线,再将曲线进行提升,计算量较大,建立密码方案系统参数的过程比较繁琐.

6.2　一种简便的修复方法

现在我们利用第 5 节得到的本原加法公式下的 $E(Z_n)$群结构的结论来给出一种简便的修复方法.为了更容易地建立系统参数,我们利用下面的引理[11]:

引理 3　设 $p\equiv 2\pmod 3$,则椭圆曲线 $E_p(0,b)$上的 F_p-有理点群 $E(F_p)$是阶为 $p+1$ 的循环群.

修复方案的基本参数:选取素数 $p,q\equiv 2\pmod 3$,和任意的非零的 $b\in Z_n$,选取曲线形式为 $E_n(0,b)$.此时曲线分别模 p 和模 q 后都是超奇异曲线,所以有 $\#E_p(F_q)=p+1$, $\#E_q(F_q)=q+1$.

方案二的修复:$n=p^2q$,利用修复方案的基本参数,选取阶为 $p\cdot lcm(p+1,q+1)$基点 G.

方案三的修复:$n=p^2q^2$,同样利用修复方案的基本参数,因为 $\#E_{p^2}(Z_{p^2})=p(p+1)$, $\#E_{q^2}(Z_{q^2})=q(q+1)$.我们可选取阶为 $pq\cdot lcm(p+1,q+1)$的基点 G.

基点的构造:首先选定 p,q 和 b 确定曲线 $E_n(0,b)$.

方案二中,令 $E_{p^2}(0,\bar{b})$是模 p^2 后的曲线,$G_1=(p:1:z)+(x_1:y_1:z_1)$,其中 z 是根据坐标 $x=p$ 和 $y=1$ 唯一确定的 z,点$(x_1:y_1:z_1)$是模 p 后的曲线 $E_{p^2}(0,\bar{b})$的有理点群 $E_p(F_p)$的任一个生成元.由定理 4 知点 G_1 是 $E_{p^2}(0,\bar{b})$上阶为 $p(p+1)$的点.再选取 G_2 是模 q 后的曲线 $E_q(0,\bar{b})$的有理点群 $E_p(F_p)$的任一个生成元.令 G 是曲线 $E_n(0,b)$上的一个点,满足 $G \bmod p^2=G_1$, $G \bmod q=G_2$.由中国剩余定理构造出点 G,易知 G 的阶为 $p\cdot lcm(p+1,q+1)$.

方案三中的基点 G 构造类似于方案二,只需要把方案二中的 G_2 换成在模 q^2 后的曲线 $E_{q^2}(0,\bar{b})$上的阶为 $q(q+1)$的点,此时 $G \bmod p^2=G_1$, $G \bmod q^2=G_2$.

6.3　修复的方案的特点

安全性:由于现在的曲线 $E_n(0,b)$模 p 和模 q 都不是异常曲线的扭曲线,从而 Galbraith 提出的基于异常曲线的攻击算法失效.环 Z_n 上椭圆曲线密码体制的安全性是基于 n 的分解[3,5,12],采用超奇异曲线并不会使得 MOV[14]和 FR[15]攻击有效,因此可以认为是安全的.

效率:我们选取曲线 $E_n(0,b)$且模 p 和 q 模都是超奇异的,一方面是为了省去复杂的数点算法,减少计算量.另一方面是参数 $a=0$ 会极大的提高计算加法的效率.利用环上椭圆曲线点加的公式在构造系统参数时不再需要 Paillier 的曲线提升算法[12],使得建立密码系统时更加简便.但相比有限域上的椭圆曲线密码协议,椭圆曲线 Paillier 系统效率不高,所以这方面的研究只具有理论上的价值.

7　结论

本文研究了环上椭圆曲线的有理点集群法则的定义,给出了 $E(Z_n)$中明确的点加算法,从理论上解决了以往不能使用一个简便和有效计算点加的公式使得该类椭圆曲线上有理点集形成群的问题.我们还推导了在本文给出的本原加法公式下 $E(Z_n)$的群结构.在密码学的应用上,利用该群结构和本原加法公式,我们提供了有安全缺陷的椭圆曲线 Paillier 系统的一种简便的修复方法.

参考文献

[1] Blake Ian F, Seroussi G, Smart N P. Advances in Elliptic Curve Cryptography[M]. London: Cambridge University Press, 2005.

[2] Lentra H WJr. Factoring integers with elliptic curves[J]. The Annals of Mathematics, 1987, 126(3): 649 – 673.

[3] Koyama K, Maurer U, Okamato T, et al. New public-key schemes based on elliptic curves over the ring[A]. Advances in Cryptology-CRYPTO 91, Lecture Notes in Computer Science 576[C]. Berlin: Springer, 1993. 252 – 266.

[4] Demytko N. A new elliptic curve based on analogue of RSA [A]. Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science 765[C]. Berlin: Springer, 1994. 40 – 49.

[5] Meyer B, Mller V. A public key cryptosystem based on elliptic curves over equivalent to factoring[A]. Advances in Cryptology-EUROCRYPT'96, Lecture Notes in Computer Science 1070 [C]. Berlin: Springer, 1996. 49 – 59.

[6] 张亚娟,祝跃飞,黄秋生.环上的椭圆曲线签名体制[A].第九届全国青年通信学术会议论文集[C].北京:电子工业出版社,2004. 1. 989 – 994.

[7] 朱文余,孙琦.环 Z_n 上椭圆曲线的密钥交换协议[J].电子学报,2005,33(1):83 – 87.
Zhu Wen-yu, Sun Qi. The elliptic curve over Z_n and key exchange protocol[J]. Acta Electronica Sinica, 2005, 33(1): 83 – 87. (in Chinese)

[8] 张宁,辛向军,肖国镇.利用环上的椭圆曲线实现基于身份的加密体制[J].西安电子科技大学学报,2007,34(2):290 – 293.
Zhang Ning, Xin Xiang-jun, Xiao Guo-zhen. ID-based encryption from elliptic curves over ring[J]. Journal of Xidian University. 2007, 34(2): 290 – 293. (in Chinese)

[9] 王念平,金晨辉.关于环 Z_n 上的椭圆曲线[J].计算机工程与应用,2007,43(11):78 – 80.
Wang Nian-ping, Jin Chen-hui. On elliptic curves over Z_n[J]. Computer Engtneering and Applications, 2007, 43(11): 78 – 80. (in Chinese)

[10] 李明,王鲲鹏.局部环 Z/p^nZ 上椭圆曲线密码系统[J].中国科学院研究生院学报,2009,26(5):695 – 702.
Li Ming, Wang Kunpeng. Cryptosystem based on elliptic curve over local field Z/p^nZ[J]. Journal of the Graduate School of the Chinese Academy of Science, 2009, 26(5): 695 – 702. (in Chinese)

[11] Washington L C. Elliptic Curves: Number Theory and Cryptography[M]. Washington DC, USA: CRC Press, 2003.

[12] Paillier P. Trapdooring discrete logarithms on elliptic curves over rings[A]. Advances in Cryptology-Asiacrypt'2000, Lecture Notes in Computer Science 1976[C]. Berlin: Springer, 2000. 573 – 584.

[13] Galbraith Steven D. Elliptic curve paillier schemes[J]. Journal of Cryptology, 2002, 15: 129 – 138.

[14] Menezes A J, Okamoto T, Vanstone S A. Reducing elliptic curve logarithms to logarithms in a finite field[J]. IEEE Transaction on Information Theory, 1993, 39(5): 1639 – 1646.

[15] Frey G, Rck H G. A remark concerning m-divisibility and the discrete logrithm in the divisor class group of curves[J]. Mathematics of Computation, 1994, 62(206): 865 – 874.

作者简介



张李军 男,1983 年出生于四川彭山,中国科学院研究生院信息安全国家重点实验室博士研究生,主要研究方向为椭圆曲线密码学.
E-mail: ljzhang@is.ac.cn



王鲲鹏 男,1971 年出生于河北尚义,中国科学院研究生院信息安全国家重点实验室副教授,主要研究方向为密码学、代数数论.