基于环 Z_n 上圆锥曲线的 ElGamal 数字签名方案*)

杨 慧 肖国镇

(西安电子科技大学 ISN 国家重点实验室 信息保密研究所 西安 710071)

摘 要 首先介绍了剩余类环 Z_n 上圆锥曲线 $C_n(a,b)$ 的基本性质,给出了基于环 Z_n 上圆锥曲线的 ElGamal 数字签名方案及其数值模拟。该方案综合利用了大数分解的困难性和有限群上计算离散对数问题的困难性,从而增强了该数字签名方案的安全性。由于在 $C_n(a,b)$ 上明文的嵌入,阶的运算以及点的运算都比较容易,且通过引进标准二进制计算群元素的整数倍的算法,使该方案具有运算速度快,更易于实现等优点。

关键词 环 Z_n 上圆锥曲线,ElGamal 数字签名方案,数值模拟,标准二进制表示

ElGamal Digital Signature Based on the Conic Curves over Z_n

YANG Hui XIAO Guo-Zhen

(Information Security & Privacy Institute in ISN, Xidian University, Xi'an 710071)

Abstract Some basic properties of conic $C_n(a,b)$ over the residue class ring Z_n are presented. The ElGamal digital signature scheme on conic $C_n(a,b)$ over the residue class ring Z_n is designed and its numeric simulation is done. Comprehensively using the difficulties in factorizing large integer and computing discrete logarithm, the security of this digital signature scheme is increased. For the facility of plaintext embedding and the computing of rank and point on conic $C_n(a,b)$, this scheme has the advantages of speedy operation and easy realization, especially by using the NAF.

Keywords Conic curve over Z_n, ElGamal digital signature scheme, Numeric simulation, NAF

自从 Diffie 与 Hellman[1]提出公钥密码体制以来,至今已经形成较为系统的公钥密码学,RSA 与 ElGamal 是两个比较完善的公钥密码算法[2,3]。其中 ElGamal 公钥体制是 ElGamal 于 1985 年提出的,其安全性主要是基于有限域上离散对数问题的困难性。这种基于离散对数问题的双钥密码体制,既可用于加密,又可用于签名,从而得到了广泛的应用。

20 世纪 90 年代,对基于有限域 F_p 上的圆锥曲线 $C_p(a,b)$ 及其在大整数分解和密码算法中应用的研究,引起人们很大的兴趣。对于有限域 F_p 上的圆锥曲线 $C_p(a,b)$,1996 年张明志首先引进了 $C_p(a,b)$ 上的加法运算⊕,并证明了 $(C_p(a,b),\oplus)$ 是一个有限加群[4]。1998 年曹珍富提出了基于 F_p 上圆锥曲线的公钥密码系统[5]及 RSA 的圆锥曲线模拟[6]。由于 $C_p(a,b)$ 中明文嵌入,阶的计算及点的运算都比较容易,这些对设计密码算法具有很强的吸引力。2002 年,孙琦等利用整数的标准二进制表示(NAF)提出一个快速计算群元的整数倍的算法[7,8],将该算法引入圆锥曲线上点的运算可以节约近 1/4 的计算量。2005 年,孙琦[9]、王标[10]等将有限域 F_p 上的圆锥曲线的研究拓展到了环 Z_n 上,并深入讨论了圆锥曲线 $C_n(a,b)$ 和曲线上的公钥密码体制,为环 Z_n 上的圆锥曲线数字签名体制奠定了基础。

本为在文[9,10]的基础上提出了基于环 Z_n 上圆锥曲线的 ElGamal 数字签名方案并给出该方案的数值模拟。

1 环 Z_n 上的圆锥曲线 $C_n(a,b)$

设 Z_n 是一个模 n 的剩余类环,在文[9]中定义环 Z_n 上的圆锥曲线 $C_n(a,b)$ 是同余方程

$$y^2\equiv ax^2-bx(\mathrm{mod}\ n) \tag{1}$$

在 Z_n 上的解 (x,y) 的集,这里 $n=pq,p,q$ 为两个不同的奇素数,$(a,n)=(b,n)=1$。显然 $O=(0,0)\in C_n(a,b)$。记 $C_n(a,b)$(即同余方程(1)的解集)为:

$$C_n(a,b)=\{(x,y)\in Z_n\times Z_n \mid y^2\equiv ax^2-bx(\mathrm{mod}\ n)\}$$

首先以坐标方式给出 $C_n(a,b)$ 中全部有理点的表示[9]:

$$C_n(a,b)=C_1\cup C_2\cup C_3\cup O,$$

其中

$$C_1=\{P_1(t)=(\frac{b}{a-t^2},\frac{tb}{a-t^2}),(a-t^2,n)=1,\forall t\in Z_n\}$$

$$C_2=\{P_2(t)=(pp^{-1}b(a-t^2)^{-1},pp^{-1}bt(a-t^2)^{-1}),(a-t^2,q)=1$$

$$\forall t\in Z_q,pp^{-1}\equiv 1(\mathrm{mod}\ q),(a-t^2)(a-t^2)^{-1}\equiv 1(\mathrm{mod}\ q)\},$$

$$C_3=\{P_3(t)=(qq^{-1}b(a-t^2)^{-1},qq^{-1}bt(a-t^2)^{-1}),(a-t^2,p)=1$$

$$\forall t\in Z_p,qq^{-1}\equiv 1(\mathrm{mod}\ p),(a-t^2)(a-t^2)^{-1}\equiv 1(\mathrm{mod}\ p)\}。$$

显然 $\#C_n(a,b)=|C_1|+|C_2|+|C_3|+1$。

下面以坐标方式定义环 Z_n 上的圆锥曲线 $C_n(a,b)$ 中的加法运算⊕,即对任意

$P=(x_1,y_1)\in C_n(a,b)$,

$Q=(x_2,y_2)\in C_n(a,b)$,$P\oplus Q$ 定义如下[9]:

(一)当 $P\neq Q$ 时,$P\oplus Q$ 定义为

(1)若 $(x_2-x_1,n)=1$,则 $P\oplus Q=P_1(t)\in C_1$,其中 $t\equiv\frac{y_2-y_1}{x_2-x_1}(\mathrm{mod}\ n)$。

(2)若 $(x_2-x_1,n)=p$,则 $P\oplus Q=P_2(t)\in C_2$,其中 $t\equiv\frac{y_2-y_1}{x_2-x_1}(\mathrm{mod}\ q)$。

(3)若 $(x_2-x_1,n)=q$,则 $P\oplus Q=P_3(t)\in C_3$,其中 $t\equiv\frac{y_2-y_1}{x_2-x_1}(\mathrm{mod}\ p)$。

*)本文受国家自然科学基金项目(项目编号:60473028)资助。杨 慧 硕士研究生。

(4)若$(x_2-x_1,n)=n$,则$P\oplus Q=O$。

(二)当$P=Q$时,$P\oplus Q=2P=2(x_1,y_1)$的定义为

(5)若$(y_1,n)=1$,则$2P=P_1(t)\in C_1$,其中$t=\frac{2ax_1-b}{2y_1}\pmod n$。

(6)若$(y_1,n)=p$,则$2P=P_2(t)\in C_2$,其中$t=\frac{2ax_1-b}{2y_1}\pmod q$。

(7)若$(y_1,n)=q$,则$2P=P_3(t)\in C_3$,其中$t=\frac{2ax_1-b}{2y_1}\pmod p$。

(8)若$(y_1,n)=n$,则$2P=O$。

文[9]证明了环Z_n上的圆锥曲线$(C_n(a,b),\oplus)$构成一个有限交换群。

由于同余方程$y^2\equiv ax^2-bx\pmod n$的解集等价于同余方程组:

$$\begin{cases}y^2\equiv ax^2-bx\pmod p\\ y^2\equiv ax^2-bx\pmod q\end{cases}\tag{2}$$

的解集。对于$C_n(a,b)$上每一个点$M=(x,y)\in C_n(a,b)$利用中国剩余定理能被唯一表示成一对$[M_p,M_q]=[(x_p,y_p),(x_q,y_q)]$,其中

$M_p\in C_p(a,b),M_q\in C_q(a,b)$,

$$x\equiv x_p\pmod p,x\equiv x_q\pmod q\tag{3}$$

$$y\equiv y_p\pmod p,y\equiv y_q\pmod q\tag{4}$$

通过这个对应关系,$C_n(a,b)$与$C_p(a,b)\times C_q(a,b)$间存在一一对应关系。因此我们可以十分方便地利用$C_p(a,b)$和$C_q(a,b)$的阶来得到$C_n(a,b)$的阶。显然有

定理 1[9] (1)当$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$时,

$\#C_n(a,b)=(p+1)(q+1)$

(2)当$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$时,$\#C_n(a,b)=(p-1)(q-1)$;

(3)当$\left(\frac{a}{p}\right)=1,\left(\frac{a}{q}\right)=-1$时,$\#C_n(a,b)=(p-1)(q+1)$;

(4)当$\left(\frac{a}{p}\right)=-1,\left(\frac{a}{q}\right)=1$时,$\#C_n(a,b)=(p+1)(q-1)$。

定理 2[9] 设$A\in C_n(a,b)$,称使$kA=O$成立的最小正整数k为A的阶,记为$O(A)$。$\forall A=(x,y)\in C_n(a,b)$,$A$在$C_p(a,b)\times C_q(a,b)$中有唯一的点$(A_p,A_q)$与之对应,且点$A$的阶$O(A)=lcm\{O(A_p),O(A_q)\}$。

推论[9] 设$n=pq,p,q$为两个不同的大素数,满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$,且$p+1=2r,q+1=2s$,其中$r,s$也为素数,则曲线$C_n(a,b)$中存在一个点$G$,其阶$N_n=2rs$。称该点$G$为$C_n(a,b)$的一个基点,集合$S=\{O,G,2G,\cdots,(N_n-1)G\}$构成$C_n(a,b)$的一个子群。

定理 3[10] $n=pq,p,q$为两个不同的大素数,满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$,且$p+1=2r,q+1=2s$,其中$r,s$是素数,我们有:

(1)当$a-b\equiv 1\pmod n$时,则:

$$G=\begin{cases}P_1(1),&(1,1)\text{是}C_p(a,b)\text{的生成元}\\ &\text{或}(1,1)\text{是}C_q(a,b)\text{的生成元};\\ P_1(a),&(1,1)\text{是}C_p(a,b)\text{的}r\text{阶元}\\ &\text{或}(1,1)\text{是}C_q(a,b)\text{的}s\text{阶元}。\end{cases}$$

(2)当$a-b\equiv 4\pmod n$时,则

$$G=\begin{cases}P_1(2),&(1,2)\text{是}C_p(a,b)\text{的生成元}\\ &\text{或}(1,2)\text{是}C_q(a,b)\text{的生成元};\\ P_1(a/2),&(1,2)\text{是}C_p(a,b)\text{的}r\text{阶元}\\ &\text{或}(1,2)\text{是}C_q(a,b)\text{的}s\text{阶元}\end{cases}$$

在密码算法的实现过程中,$C_n(a,b)$的明文嵌入算法为:设$n=pq,p,q$,为两个不同的大素数,当$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$时,对于$0\leqslant m<n$,有$(m^2-a,n)=1$,令$x_m=\frac{b}{a-m^2}\pmod n$,$y_m=\frac{bm}{a-m^2}\pmod n$则取$P_1(m)=(x_m,y_m)$表示明文$m$的嵌入。实际上,此时$|C_1|=n$,环$Z_n$和集$C_1$之间可以建立一一对应。对任一明文$m,m\in Z_n$,均可嵌入到$C_1$中去。

2 环Z_n上圆锥曲线的ElGamal数字签名方案

签名者A选定一条圆锥曲线:$y^2=ax^2-bx\pmod n$,其中,$a,b\in Z_n$,$(a,n)=(b,n)=1$,$n=pq,p,q$为两个不同的大素数,满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$,且$p+1=2r,q+1=2s$,其中$r,s$是素数,则曲线的阶$N_n=lcm\{|C_p(a,b)|,|C_q(a,b)|\}$

$=\{p+1,q+1\}=2rs$。

2.1 参数选择

(1)设$G=(x_G,y_G)$为曲线$C_n(a,b)$上一点,其阶为$N_n=2rs$,称G为$C_n(a,b)$的一个基点;

(2)设$d\in Z_{N_n}^*$为签名私钥,$Q=dG$为签名验证公钥;

(3)$H(m)$是对消息m的一种安全hash映射;

(4)随机选取一个整数$k\in Z_{N_n}^*$,且$(k,N_n)=1$;

(5)公开n,N_n,a,b,G,Q,k作为公钥,私钥为d。

2.2 签名过程

(1)计算l,使$kl=1\pmod{N_n}$;

(2)计算$kG=(x_1,y_1),\gamma=x_1\pmod{N_n}$;

(3)计算$\delta=(H(m)-d\gamma)l\pmod{N_n}$,如果$\delta=0$,则重新选择$k$并返回步骤(1);将$(\gamma,\delta)$作为对消息$m$的签名发送给收方B。

2.3 验证过程

B收到签名(γ,δ)后作如下的验证

(1)取$u_1=\gamma,u_2=\delta k\pmod{N_n}$

(2)计算$U=u_1Q\oplus u_2G\pmod n$。如果$U=(0,0)$,则拒绝这个签名,否则,计算$V=H(m)G\pmod n$。当且仅当$U=V$时,接受这个签名。

签名验证证明:

$U=u_1Q\oplus u_2G\pmod n=\gamma Q\oplus\delta kG\pmod n$

$=\gamma dG\oplus(H(m)-d\gamma)lkG\pmod n=H(m)G\pmod n$

$V=H(m)G\pmod n$

当且仅当$U=V$时,接受这个签名。

3 ElGamal数字签名体制的数值模拟

A方选取圆锥曲线C:$y^2\equiv 2x^2-x\pmod{5809}$,即$a=2,b=1,n=5809$,此时$p=37,q=157,r=(p+1)/2=19,s(q+1)/2=79,N_n=2rs=3002$。任取$d=11$,设$m$的hash函数$H(m)=23$。

由于$a-b\equiv 1\pmod n$,且$(1,1)$在$C_{37}(2,1)$中的阶为$r=19$,由定理3可取基点$G=P_1(2)$。

于是

$Q=dG=11P_1(2)=(1\ 0-1\ 0-1)P_1(2)$

$=-P_1(2)\oplus 2^2(P_1(-2)\oplus 2^2P_1(2))$

$=-P_1(2)\oplus 2^2(P_1(-2)\oplus P_1(3390))$

$=-P_1(2)\oplus 2^2P_1(2491)$

$=P_1(-2)\oplus P_1(970)=P_1(10)$

任取 $k=1887$

公钥为，$n=5809$，$N_n=3002$，$a=2$，$b=1$，$G=P_1(2)$，$Q=P_1(10)$，$k=1887$，私钥为 $d=11$。

签名过程：

(1)由 $kl\equiv 1(\mathrm{mod}\ N_n)\Rightarrow l=35$

(2)计算 $kG=1887P_1(2)$

$=(1\ 0\ 0\ 0-1\ 0-1\ 0\ 0\ 0-1)P_1(2)$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2(P_1(-2)\oplus 2^4P_1(2)))$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2(P_1(-2)\oplus P_1(4594)))$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2P_1(5344))$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus P_1(2695))$

$=-P_1(2)\oplus 2^5P_1(2209)=P_1(-2)\oplus P_1(1472)$

$=P_1(4416)=(3254,4007)$

$r=3254\mathrm{mod}\ 3002=252$

(3)$\delta=(H(m)-d\gamma)l(\mathrm{mod}\ N_n)$

$=(23-11\times 252)\times 35(\mathrm{mod}\ 3002)=2851$

将$(\gamma,\delta)=(252,2851)$作为对消息 m 的签名。

签名验证：

(1)计算 $u_1=\gamma=252$，$u_2=\delta k(\mathrm{mod}\ N_n)$

$=2851\times 1887(\mathrm{mod}\ 3002)=253$

(2)$u_1Q=252P_1(10)$

$=(1\ 0\ 0\ 0\ 0\ 0-1\ 0\ 0)P_1(10)$

$=P_1(4272)$

$u_2G=253P_1(2)$

$=(1\ 0\ 0\ 0\ 0\ 0-1\ 0\ 1)P_1(2)=P_1(3343)$

$U=u_1Q\oplus u_2G=P_1(4272)\oplus P_1(3343)$

$=P_1(5238)$

$V=H(m)G=23P_1(2)$

$=(1\ 0-1\ 0\ 0-1)P_1(2)=P_1(5238)$

$U=V$，接受这个签名。

结论 本文提出了一种基于环 Z_n 上圆锥曲线的 ElGamal 数字签名方案，其安全性是基于大数分解和有限 Abel 群 $C_n(a,b)$ 上计算离散对数问题的困难性。由于在 $C_n(a,b)$ 上，明文嵌入，阶的运算以及点的运算都比较容易，特别是求逆元很容易，因此 ElGamal 在 $C_n(a,b)$ 上的模拟比它在椭圆曲线 $E_n(a,b)$ 上模拟要简单得多。而且通过引进标准二进制计算群元素的整数倍的算法，能节约近 1/4 的计算量，使该方案更具有应用价值。

参 考 文 献

1 Diffe W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644～654

2 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems[J]. Comm ACM, 1978, 21: 120～126

3 El-Gamal T. A public key cryptosystem and a signature scheme based on the discrete logarithm[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469～472

4 张明志. 用圆锥曲线分解整数[J]. 四川大学学报(自然科学版), 1996, 33(4): 356～359

5 曹珍富. 基于有限域 F_P 上圆锥曲线的公钥密码系统[A]. 密码学新进展-Chinacrypt'98[C]. 北京：科学出版社, 1998. 45～49

6 曹珍富. RSA 与改进的 RSA 的圆锥曲线模拟[J]. 黑龙江大学自然科学学报, 1999(4): 15～18

7 孙琦，张起帆，彭国华. Dickson 多项式 $g_e(x,1)$ 公钥密码体制的新算法[J]. 四川大学学报(自然科学版), 2002, 1: 18～23

8 孙琦，张起帆，彭国华. 计算群元的整数倍的一种算法及其在公钥密码体制中的应用[A]. 密码学进展-ChinaCrypt'2002. 见：第七届中国密码学学术会议论文集[C]. 北京：电子工业出版社, 2002. 117～124

9 孙琦，朱文余，王标. 环 Z_n 上圆锥曲线和公钥密码协议[J]. 四川大学学报(自然科学版), 2005, 42(3): 471～478

10 王标，朱文余，孙琦. 基于剩余类环 Z_n 上圆锥曲线的公钥密码体制[J]. 四川大学学报(工程科学版), 2005, 37(5): 112～117

(上接第 87 页)

(2)本文中信誉度的最初始状态属于主观信任，假定为均匀分布，介于可信与不可信中间，初步反映了人类社会网络的信誉基本状况，有一定的科学意义。为了进一步提高本方案的精确度，需要对主观信任的科学性问题进行研究，这正是我们下一步要研究的目标。

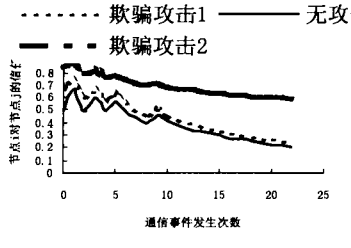

图 4 信誉欺骗攻击对信誉的影响

(3)图 4 显示了来自可信节点的欺骗攻击影响还是比较大的，应考虑在这里再引入遗忘因子减少其欺骗影响。

(4)关于信誉阈值 θ_0 也是一个非常值得研究的问题，因为它与具体的应用网络密切相关，对于异常行为的检测至关重要。可以考虑采用仿真手段去研究一些敏感网络或敏感节点的信誉阈值，为建立行业可信网络提供理论依据。

参 考 文 献

1 Perrig A, Szewczyk R, Wen V, Culler D, Tygar D. SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal, September 2002

2 Karlof C, Sastry N, Wagner D. TinySec: Link Layer Encryption for Tiny Devices. To appear in ACM SenSys, 2004

3 Deng J, Han H, Mishra S. The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks. In: the Proceedings of IPSN, April 2003

4 Watro R, Kong D, Cuti S F, Gardiner C, Lynn C, Kruus P. TinyPK: Securing Sensor Networks with Public Key Technology. In: second workshop on Security in Sensor and Ad-hoc Networks, 2004

5 Eschenauer L, Gligor V D. A key Management Scheme for Distributed Sensor networks. In: Proceedings of ACM CCS, November 2002

6 Chan H, Perrig A, Song D. Random Key Predistribution Schemes for Sensor Networks. In: Proceedings of IEEE Symposium on Security and Privacy, 2003

7 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management [C]. In: Proceedings of IEEE Conf. Security and Privacy, Oakland, California, USA, 1996

8 Blaze M, Feigenbaum J, Ioannidis J, Keromytis A[S]. RFC2704 - The KeyNote Trust Management System Version 2. 1999

9 Li N, Mitchell J, Winsborough W. Design of a rolebased trust management framework[C]. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland

10 肖德琴，周权，张焕国，等. 基于时序逻辑的加密协议分析，计算机学报，2002. 10

11 刘卫江主编. 概率论与数理统计. 北京：清华大学出版社；北京交通大学出版社, 2005

12 Jsang A, Ismail R. The Beta Reputation System[C]. In: Proc. of the 15th Bled Electronic Commerce Conference, June 2002