基于双难题的环 Z_n 上圆锥曲线的数字签名

林 松 李舟军 王 标

(北京航空航天大学 计算机学院，北京 100191) (国际关系学院 信息科技系，北京 100091)

摘 要：通过对一个剩余类环 Z_n 上圆锥曲线 $C_n(a,b)$ 数字签名方案(Xiao 06 方案)的安全性分析，发现该方案的公开参数选取和算法设计存在问题，导致利用韦达定理可以分解模数 n，说明 Xiao 06 方案的安全性不是基于整数分解难题的. 针对此缺陷，采取保密部分参数和修改验证算法的方法，提出了一个改进的环 Z_n 上圆锥曲线的数字签名方案，并且给出了改进方案的数值模拟. 分析表明，改进的方案是一个同时基于离散对数和整数分解双难题的环 Z_n 上圆锥曲线的数字签名方案，不仅保留了原 Xiao 06 方案的优点(明文嵌入方便，求逆元速度快，元素阶的计算及曲线上点的运算容易)，还具有很强的抗破解能力.

关 键 词：数字签名；整数分解；离散对数；圆锥曲线

中图分类号：TP 309.7

文献标识码：A **文 章 编 号**：1001-5965(2009)09-1067-05

Signature on conic curve over Z_n based on two hard problems

Lin Song Li Zhoujun

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Wang Biao

(Information Science and Technology Department, University of International Relations, Beijing 100091, China)

Abstract: The security of the digital signature scheme (Xiao06 scheme) on conic curve $C_n(a,b)$ over the residue class ring Z_n was analyzed. The analysis result indicates that the published parameters can make the modulus n be factorized using the Weda's theorem, and shows that the Xiao06 scheme is not a scheme whose security based on the integer factorization problem. To address this issue, an improved digital signature scheme on conic curve over Z_n was proposed. Some parameters were kept secretly, and the verification algorithm was modified in the improved scheme. Furthermore, the numerical simulation of the improved scheme was given. The analysis shows that the improved scheme is a digital signature scheme based on two hard problems in computing discrete logarithm and factorizing integer simultaneously, and that the improved scheme has not only the merits (convenience for plaintext embedding, quickness for the inverse operation, and easiness for element order and points computing in curve) of the Xiao06 scheme, but also the advantage of strong anti-cracking ability.

Key words: digital signature; integer factorization; discrete logarithm; conic curve

自从 1976 年文献[1]提出公钥密码思想后，一系列数字签名方案被相继提出，这些方案的安全性大多基于某个数学难题：离散对数问题(DLP, Discrete Logarithm Problem)或整数分解问题(IFP, Integer Factorization Problem). 例如，ElGamal 和数字签名算法(DSA, Digital Signature Algorithm)等的安全性基于 DLP；RSA 的安全性基于 IFP. 基于 DLP 和 IFP 双难题的签名方案的安全性能够得到两个难题的支持，即使其中一个难题解决了，只要另外一个难题仍然难以

收稿日期：2008-08-04

基金项目：国家自然科学基金资助项目(60473057,90604007,90718017)

作者简介：林 松(1970—)，男，福建莆田人，博士后，linsong@buaa.edu.cn.

解决,签名方案的安全性就有保证.因此,设计同时基于双难题的数字签名方案成为了一个热点课题.1988年文献[2]提出了一个同时基于两个数学难题的秘钥分配方案.此后,许多同时基于DLP和IFP双难题的数字签名方案陆续提出[3-5],但是,它们有些已经被证明是不安全的,有些被证明其安全性并不是真正基于双难题的.

近年来,基于圆锥曲线密码体制的研究引起了学者们的关注:1996年张明志首先引进了有限域 F_p 上圆锥曲线 $C_p(a,b)$ 的加法运算⊕,并证明了 $(C_p(a,b),\oplus)$ 是一个有限加群[6];1998年曹珍富提出了基于有限域 F_p 上圆锥曲线的公钥密码系统[7];2005年孙琦等定义了剩余类环 Z_n 上的圆锥曲线 $C_n(a,b)$,并实现了基于剩余类环上圆锥曲线的RSA和ElGamal公钥密码体制的设计[8-9].其中引人注目的是在群 $(C_n(a,b),\oplus)$ 中的逆元计算、群元整数倍计算十分快捷和容易.2006年肖龙、王标和孙琦提出了一个基于环 Z_n 上圆锥曲线的数字签名方案(本文记为Xiao06方案),其声称是同时基于DLP和IFP双难题的[10].本文对Xiao06方案进行研究分析,发现其在公开参数 N_n 的情况下,模数 n 容易被分解;若参数 N_n 不公开,则Xiao06方案无法完成签名,从而证明了Xiao06方案的安全性不是基于IFP的.但是,Xiao06方案利用环 Z_n 上圆锥曲线来构建密码体制,为实现基于DLP和IFP双难题的数字签名方案提供了新思路.本文改进了Xiao06方案,使其成为了一个真正同时基于双难题的数字签名方案.

1 Xiao06数字签名方案及分析

1.1 Xiao06数字签名方案介绍

环 Z_n 上圆锥曲线的定义和性质详见文献[8-9].设 Z_n 是模 n 的剩余类环,Z_n 上的圆锥曲线 $C_n(a,b)$ 是同余方程 $y^2\equiv ax^2-bx(\mathrm{mod}\ n)$ 在 Z_n 上的解 (x,y) 的集,$n=pq$,其中 p 和 q 为两个不同的大奇素数,$(a,n)=(b,n)=1$.

1.1.1 系统参数

选定圆锥曲线:$C_n(a,b)$,其中 $a,b\in Z_n$,满足 $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$,且 $p+1=2r$,$q+1=2s$,其中 r 和 s 为素数.

则圆锥曲线的阶为

$$N_n=\mathrm{lcm}\{|C_p(a,b)|,|C_q(a,b)|\}=\mathrm{lcm}\{p+1,q+1\}=2rs$$

其中,lcm为计算最小公倍数函数;$|C_p(a,b)|$ 和 $|C_q(a,b)|$ 分别为有限域上圆锥曲线 $C_p(a,b)$ 和 $C_q(a,b)$ 的阶.

1.1.2 公私钥的产生及明文嵌入

1) 选取 $G=(x_G,y_G)$ 为曲线 $C_n(a,b)$ 上的一个基点,其阶为 $N_n=2rs$;

2) 选取 $d\in\mathbf{Z}_{N_n}^*$ 为签名私钥,$Q=dG$ 为签名公钥,$H(m)$ 是对消息 m 的安全Hash映射;

3) 将值 (n,N_n,a,b,G,Q) 公开,值 d 保密;

4) 消息 m 通过明文嵌入算法嵌入到圆锥曲线中,得到一个点 $P(m)=(x_m,y_m)$.

1.1.3 签名过程

1) 随机或伪随机地选择一个整数 $k\in\mathbf{Z}_{N_n}^*$;

2) 签名者计算 $P(m)\oplus kG=(x_1,y_1)$,$\gamma=x_1(\mathrm{mod}\ N_n)$,如果 $\gamma=0$,则返回签名过程的第1)步;

3) 计算 $\delta\equiv k+\gamma d(\mathrm{mod}\ N_n)$,如果 $\delta=0$,则返回到签名过程的第1)步;

则 (γ,δ) 是签名者对消息 m 的签名,这里 γ 和 δ 均取 N_n 的最小非负剩余.

1.1.4 验证过程

1) 验证者计算 $X=\delta G\oplus(-\gamma Q)\oplus P(m)=(x_1,y_1)$,如果 $X=(0,0)$,则拒绝这个签名;

2) 验证者计算 $\nu\equiv x_1(\mathrm{mod}\ N_n)$;

3) 判断,当且仅当 $\nu=\gamma$ 时,接受这个签名.

签名验证证明如下:

证明 如果 (γ,δ) 是签名者对消息 m 的签名,则 $\delta\equiv k+\gamma d(\mathrm{mod}\ N_n)$,从而

$$X=\delta G\oplus(-\gamma Q)\oplus P(m)=(\delta-\gamma d)G\oplus P(m)=kG\oplus P(m)=(x_1,y_1)$$

即当且仅当 $\nu=\gamma$ 时,接受这个签名. **证毕**

1.2 Xiao06数字签名方案分析

从Xiao06方案的签名算法过程可以看出,其安全性主要基于求 d 在圆锥曲线群上的DLF,以及 n 的整数分解的困难性问题.

1) 离散对数问题(DLP)

已知 Q 和 G,利用等式 $Q=dG$ 求 d 在圆锥曲线群上的DLP,本部分内容在文献[8-10]中已有证明,在此不再赘述.

2) 整数分解问题(IFP)

对于Xiao06方案中声称的同时基于IFP,假如不能通过已知参数分解模数 n,则也是成立的.但是,由Xiao06方案的系统参数设置以及公私钥的产生可知:

由于 $n=pq$ $N_n=2rs$

而 $p=2r-1$ $q=2s-1$

则　$n=pq=(2r-1)(2s-1)=$

$4rs-2(r+s)+1=2N_n-2(r+s)+1$

于是　$r+s=(2N_n-n+1)/2$　$rs=N_n/2$

因此,根据韦达定理,通过构造一元二次方程,可以求解出 r 和 s 的值,进而得到 p 和 q 的值.

可见,Xiao 06 方案只是基于圆锥曲线群上的 DLP 问题,不是基于 IFP 问题.

2　改进的数字签名方案及数值模拟

2.1　改进的数字签名方案介绍

由分析可知,由于参数 N_n 的公开使得模数 n 可被分解.因此,本文试图只公开模数 n,保密参数 N_n,对 Xiao 06 签名方案进行必要的改进,使其成为一个真正同时基于 DLP 和 IFP 双难题的数字签名方案.

2.1.1　系统参数

与 Xiao 06 方案中的 1.1.1 节相同.

2.1.2　公私钥的产生及明文嵌入

1) 选取 $G=(x_G,y_G)$ 为圆锥曲线 $C_n(a,b)$ 上的一个基点,其阶为 $N_n=2rs$;

2) 选取 $d\in\mathbf{Z}_{N_n}^*$ 为签名私钥,$Q=dG$ 为签名公钥,$H(m)$ 是对消息 m 的安全 Hash 映射;

3) 将值 (n,a,b,G,Q) 公开,值 d 和 N_n 保密;

4) 消息 m 通过明文嵌入算法嵌入到圆锥曲线中,得到圆锥曲线中的一个点 $P(m)=(x_m,y_m)$,其中

$$x_m=\frac{b}{a-m^2}(\bmod n)\qquad y_m=\frac{bm}{a-m^2}(\bmod n)$$

2.1.3　签名过程

1) 随机或伪随机地选择一个整数 $k\in\mathbf{Z}_{N_n}^*$;

2) 签名者计算 $P(m)\oplus kG=(x_1,y_1)$,$\gamma\equiv x_1(\bmod N_n)$,以及 $\gamma G=(x^*,y^*)$,设 (x^*,y^*) 为 G^*,如果 $\gamma=0$,则返回到签名过程的第 1)步;

3) 签名者计算 $\delta\equiv k+\gamma d(\bmod N_n)$,如果 $\delta=0$,则返回到签名过程的第 1)步;

则 (γ,δ,G^*) 是签名者对消息 m 的签名,本文 γ 和 δ 均取 N_n 的最小非负剩余.

2.1.4　验证过程

1) 验证者计算

$X=\delta G\oplus(-\gamma Q)\oplus P(m)=(x'_1,y'_1)$

如果 $X=(0,0)$,则拒绝这个签名;

2) 验证者计算 x'_1G;

3) 验证者判断,当且仅当 $x'_1G=(x^*,y^*)$ 时,接受这个签名.

2.2　改进的数字签名方案数值模拟

参照文献[9]中 2.5 节的系统参数和圆锥曲线基点 G 的选择,对改进的方案进行数值模拟.

2.2.1　系统参数

圆锥曲线上点的加法可如下定义:

设 $P(t_1)\in C$,$P(t_2)\in C$,则

$$P(t_1)\oplus P(t_2)=P(t_3)$$

其中

$$t_3=\begin{cases}\dfrac{t_1t_2+a}{t_1+t_2} & (t_1+t_2,n)=1\\ \infty & t_1+t_2=0\end{cases}$$

选取圆锥曲线

$C_{5809}(2,1):y^2\equiv 2x^2-x(\bmod 5\,809)$

选取 $a=2$,$b=1$,$n=5\,809$,则

$$a-b\equiv 1(\bmod n)$$

此时　$p=37$　$q=157$

$r=(p+1)/2=19$　$s=(q+1)/2=79$

2.2.2　公私钥的产生及明文嵌入

选取该圆锥曲线的基点 $G=P(15)$,其阶为 $N_n=2rs=2\times19\times79=3\,002$.选取签名私钥 $d=35$,签名公钥 $Q=dG=35P(15)$.用标准二进制计算圆锥曲线中元素 $P(15)$ 的整数倍如下:

$$\begin{aligned}35P(15)&=-P(15)\oplus 2^2(P(15)\oplus 2^3P(15))=\\ &-P(15)\oplus 2^2(P(15)\oplus 2^2P(1\,363))=\\ &P(-15)\oplus 2^2(P(15)\oplus 2P(3\,407))=\\ &P(-15)\oplus 2^2(P(15)\oplus P(1\,007))=\\ &P(-15)\oplus 2^2P(2\,169)=\\ &P(-15)\oplus 2P(2\,982)=\\ &P(-15)\oplus P(4\,002)=P(5\,013)\end{aligned}$$

$Q=P(5\,013)$ 即为公钥.

公开圆锥曲线 C、模数 n 和基点 G 以及签名公钥 Q.

设要签名的消息 $m=17$,根据明文嵌入算法得 $P(17)=(2\,105,931)$.

2.2.3　签名过程

1) 随机选取 $k=4$,$0<k<N_n$;

2) 签名者计算

$$\begin{aligned}P(m)\oplus kG&=P(17)\oplus 4P(15)=\\ &P(17)\oplus 2(2P(15))=\\ &P(17)\oplus 2P(1\,363)=\\ &P(17)\oplus P(3\,407)=\\ &P(911)=(3\,260,1\,461)\end{aligned}$$

取　$\gamma\equiv3\,260(\bmod 3\,002)\equiv258(\bmod 3\,002)$

签名者计算

$$\gamma G=(x^*,y^*)=258P(15)$$

258 的标准二进制表示为(100000010),则

$$258P(15)=2(P(15)\oplus 2^7P(15))=$$
$$2(P(15)\oplus 2^5P(3\,407))=$$
$$2(P(15)\oplus 2^2P(4\,743))=$$
$$2(P(15)\oplus P(7\,605))=$$
$$2P(3\,771)=P(5\,209)$$

设(x^*,y^*)为G^*,若$\gamma=0$,则返回到签名过程的第1)步;

3) 签名者计算 $\delta\equiv k+\gamma d(\mathrm{mod}\,N_n)$

$\delta\equiv 4+258\times 35(\mathrm{mod}\,3\,002)\equiv 28(\mathrm{mod}\,3\,002)$

于是消息$m=17$的签名为(258, 28, $P(3\,570)$),将其发送给验证者.

2.2.4 验证过程

验证者计算

$$X=\delta G\oplus(-\gamma Q)\oplus P(m)=(x'_1,y'_1)=$$
$$28P(15)\oplus(-258)P(5\,013)\oplus P(17)$$

其中根据标准二进制运算得

$$28=(100\quad -100)\qquad 258=(100000010)$$
$$28P(15)=2^2(-P(15)\oplus 2^3P(15)=$$
$$2^2(-P(15)\oplus 2^2P(1\,363))=$$
$$2^2(-P(15)\oplus P(6\,816))=$$
$$2^2(P(5\,794)\oplus P(6\,816))=$$
$$2^2P(6\,069)=2P(8\,419)=P(5\,536)$$
$$258P(5\,013)=2(P(5\,013)\oplus 2^7P(5\,013))=$$
$$2(P(5\,013)\oplus 2^6P(7\,666))=$$
$$2(P(5\,013)\oplus 2^4P(2\,906))=$$
$$2(P(5\,013)\oplus 2^2P(7\,163))=$$
$$2P(3\,292)=P(3\,310)$$

于是

$$X=P(5\,536)\oplus P(-3\,310)\oplus P(17)=$$
$$P(5\,536)\oplus P(2\,499)\oplus P(17)=$$
$$P(3\,407)\oplus P(17)=$$
$$P(911)=(3\,260,1\,461)$$

验证者计算

$$x'_1G=3\,260G=3\,260P(15)$$

3 260的标准二进制表示为

$$3\,260=(10\quad -1010\quad -1000\quad -100)$$

则

$$3\,260P(15)=2^2(P(-15)\oplus 2^4(P(-15)\oplus$$
$$2^2(P(15)\oplus 2^2(P(-15)\oplus$$
$$2^2P(15)))))=$$
$$2^2(P(-15)\oplus 2^4(P(-15)\oplus$$
$$2^2P(2\,116)))=$$
$$2^2(P(5\,794)\oplus 2^4P(7\,333)=$$
$$2^2(P(5\,794)\oplus P(8\,347))=$$
$$2^2P(6\,259)=P(5\,209)=(x^*,y^*)$$

即签名为真.

3 改进方案的安全性分析

从下面两种可能的攻击来分析改进方案的安全性:

攻击1:假设攻击者能够求解IFP问题,试图伪造出给定消息的有效签名.若IFP问题已经解决,攻击者为伪造签名,仍然无法绕过由$Q=dG$求解私钥d的DLP问题.

攻击2:假设攻击者能够求解DLP问题,试图伪造出给定消息的有效签名.即攻击者能够从$Q=dG$求解私钥d,为了伪造签名,通过验证式子,需要计算$\delta=k+\gamma d(\mathrm{mod}\,N_n)$(要获取秘密随机数$k$的值).然而,由于$N_n$未公开,要从公开的模数$n$计算出$N_n$,则需要分解模数$n$,即求解IFP问题.

由以上分析可见,攻击者想攻破本文改进的数字签名方案,不得不同时解决DLP和IFP双难题.因此,在DLP和IFP不能同时求解的情况下,本改进方案是安全的.

4 结 论

本文对一个基于环Z_n上圆锥曲线的Xiao 06数字签名方案进行了密码分析,主要结论是:当采用Xiao 06方案中的参数设置时,由于公开参数N_n,使得模数n易于被分解,从而导致Xiao 06方案不是一个真正基于DLP和IFP双难题的数字签名方案.针对该缺陷,提出了Xiao 06方案的改进方案,新改进的签名方案保密参数N_n,从而使得模数n难于被分解,同时相应修改了Xiao 06方案中的签名过程和验证过程.改进的方案除了保留Xiao 06方案的明文嵌入方便、求逆元速度快、元素阶计算及曲线上点运算容易等优点外,还是一个真正同时基于DLP和IFP双难题的环Z_n上圆锥曲线的数字签名方案,具有很强的安全性和抗破解能力.

参考文献(References)

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

[2] McCurley K C. A key distribution system equivalent to factoring[J]. Cryptology, 1988, 1(2):95-106

[3] 吴秋新,杨义先,胡正名.同时基于离散对数和素因子分解的新的数字签名方案[J].北京邮电大学学报, 2001, 24(1): 61-65
Wu Qiuxin, Yang Yixian, Hu Zhengming. New signature schemes based on discrete logarithms and factoring[J].

Journal of Beijing University of Posts and Telecommunications,2001,24(1):61－65(in Chinese)

[4] 董晓蕾,曹珍富,李晓红. 基于双难题的两个数字签名方案的密码分析[J]. 上海交通大学学报, 2006, 40(7):1174－1177
Dong Xiaolei, Cao Zhenfu, Li Xiaohong. Cryptanalysis of two signature schemes based on two hard problems[J]. Journal of Shanghai Jiaotong University, 2006, 40(7):1174－1177(in Chinese)

[5] 李子臣,徐国爱,杨义先. He-Wu 数字签名方案的攻击方法[J]. 北京邮电大学学报, 1999, 22(4):6－8
Li Zichen, Xu Guoai, Yang Yixian. Cryptanalysis of improved Rabin's crypto-system[J]. Journal of Beijing University of Posts and Telecommunications, 1999, 22(4): 6－8 (in Chinese)

[6] 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
Zhang Mingzhi. Factoring integer with conics[J]. Journal of Sichuan University: Natural Science Edition, 1996, 33(4): 356－359(in Chinese)

[7] 曹珍富. 基于有限域 F_P 上圆锥曲线的公钥密码系统[C]//刘木兰,龚奇敏. 密码学进展—ChinaCrypt'98. 北京:科学出版社,1998:45－49
Cao Zhenfu. A public key cryptosystem based on the conic curve over finite fields F_P[C]//Liu Mulan, Gong Qimin. Advances in Cryptology-ChinaCrypt'98. Beijing: Science Press, 1998:45－49 (in Chinese)

[8] 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
Sun Qi, Zhu Wenyu, Wang Biao. The conic curves over Z_n and public-key cryptosystem protocol[J]. Journal of Sichuan University: Natural Science Edition, 2005, 42(3): 471－478 (in Chinese)

[9] 王标,朱文余,孙琦. 基于剩余类环 Z_n 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
Wang Biao, Zhu Wenyu, Sun Qi. Public-key cryptosystem based on the conic curves over Z_n[J]. Journal of Sichuan University: Engineering Science Edition, 2005, 37(5): 112－117(in Chinese)

[10] 肖龙,王标,孙琦. 基于环 Z_n 上的圆锥曲线数字签名和多重数字签名[J]. 西安交通大学学报,2006,40(6):648－651
Xiao Long, Wang Biao, Sun Qi. Digital signature and multiple digital signatures based on the conic curve over Z_n[J]. Journal of Xi'an Jiaotong University, 2006, 40(6):648－651(in Chinese)

(责任编辑:文丽芳)

(上接第 1051 页)

参考文献(References)

[1] 张益强,张其善,杨东凯,等. 基于 GPS 遥感的延迟映射接收机关键技术[J]. 北京航空航天大学学报,2006, 32(3): 333－336
Zhang Yiqiang, Zhang Qishan, Yang Dongkai, et al. Design of delay mapping receiver for GPS remote sensing [J]. Journal of Beijing University of Aeronautics and Astronautics, 2006, 32(3): 333－336(in Chinese)

[2] 刘经南,邵连军,张训械. GNSS_R 研究进展及其关键技术[J]. 武汉大学学报(信息科学版), 2007, 32(11):955－960
Liu Jingnan, Shao Lianjun, Zhang Xunxie. Advances in GNSS-R studies and key technologies [J]. Journal of Wuhan University (Geomatics and Information Science), 2007, 32(11):955－960(in Chinese)

[3] Gleason S, Hodgart S, Mackin S, et al. Detection and processing of bistatically reflected GPS signals from low earth orbit for the purpose of ocean remote sensing [J]. IEEE Transactions On Geoscience And Remote Sensing, 2005, 43(6): 1229－1241

[4] Masters D, Akos D, Esterhuizen S. Integration of GNSS bistatic radar ranging into an aircraft terrain awareness and warning system [C]//Proc ION GNSS. Long Beach, CA: Institude of Navigation, 2005: 1739－1748

[5] James Bao-yen Tsui. GPS 软件接收机基础[M]. 陈军译. 北京: 电子工业出版社, 2007
James Bao-yen Tsui. Fundamentals of global positioning system receivers a software approach[M]. Translated by Chen Jun. Beijing: Publishing House of Electponic Industry, 2007

[6] Mansndhar D, Shibasaki R. Pototype software-based GPS receiver for reflected signal analysis [C]// Proc IGARSS. Seoul, Korea: NSC, 2005, 7: 4689－4692

(责任编辑:娄　嘉)