基于圆锥曲线的数字签名和Schnorr盲签名

刘 辉,李子臣
(河南理工大学 计算机科学与技术学院,河南 焦作 454000)

摘 要:圆锥曲线公钥密码系统中参数的选取会影响其安全性,为了构造有限域 F_p 上的安全的圆锥曲线公钥密码系统,需要合理地选取参数。文中对有限域 F_p 上的圆锥曲线公钥密码算法进行了分析,指出其安全性基于计算圆锥曲线上离散对数困难性,而构造圆锥曲线公钥密码的参数影响到它的安全性,对其参数的选取给出建议。提出一种基于圆锥曲线的数字签名方案,并对Schnorr盲签名方案在圆锥曲线上进行模拟,对提出的方案进行了安全和效率方面的分析,证明提出的方案是安全和高效的。

关键词:圆锥曲线;数字签名;盲签名
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2008)07-0133-02

Digital Signature and Schnorr Blind Signature Based on Conic Curves

LIU Hui, LI Zi-chen
(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: The parameters selection in public-key cryptosystem based on conic curve can affect its secutity. In order to construct a secure public-key cryptosystem based on conic curve in finite filed F_p, the reasonable parameters must be chosed. In this paper, a public-key cryptosystem based on conic curve in finite filed F_p was analyzed, pointing out the security based on the difficulty of discrete logarithm on conic curve and the parameters selection affect its security, the parameters selection else was suggested. Purpose a digital signature scheme based on conic curve and Schnorr blind signature scheme's conic analog was given in this paper. Finally, else analyzed the security and efficiency of the scheme, proving that the scheme is secure and efficient.

Key words: conic curve; digital signature; blind signature

0 引 言

20世纪90年代提出的圆锥曲线在公钥体制密码系统中的应用,引起了人们的极大兴趣,很多学者针对圆锥曲线密码学做了大量的研究工作。1996年张明志[1]首先对有限域的圆锥曲线引进了加法运算 s 并证明了是一个有限加群,1998年,曹珍富教授[2,3]提出了基于有限域 F_p 上的圆锥曲线的公钥密码系统,并给出了RSA在其上的模拟。2001年,戴宗铎等[4]对基于圆锥曲线的密码进行了分析。最近孙琦等人[5]把其扩展到环上,并在其上模拟了KMOV数字签名方案。利用有限域上明文嵌入方便、逆元计算简单及曲线上点的运算都比较容易的特点,提出一种基于圆锥曲线的数字签名方案,并实现盲签名在圆锥曲线上的模拟。

收稿日期:2007-10-18
基金项目:河南省自然科学基金(0411010700)
作者简介:刘 辉(1983-),男,河南范县人,硕士研究生,主要研究方向为网络与信息安全;李子臣,教授,主要从事网络与信息安全、密码学方面的研究。

1 圆锥曲线密码系统

1.1 有限域 F_p 上的圆锥曲线

有限域 F_p(p 为奇素数)上的圆锥曲线是指同余方程:

$$y^2 = ax^2 - bx \bmod p, a, b \in F_p^*(F_p^* \text{ 为 } F_p \text{ 的乘群}) \quad (1)$$

将 $y \equiv xt(\bmod p)$ 代入式(1)中,则圆锥曲线 $C(F_p)$ 的全部点可表示为:

$$C(F_p)p = \{p(t) = (x,y) = b(a-t^2)^{-1}, bt(a-t^2)^{-1} \mid t \in F_p, t^2 \neq a\} \cup \{p(\infty) = (0,0)\} \quad (2)$$

其中 $(a-t^2)^{-1}$ 为 $(a-t^2)$ 在有限域 F_p 上的乘法逆元。

在 $C(F_p)$ 上定义加法运算 $\oplus$:

1) 对于 $P = p(t) \in C(F_p)$,满足 $p(t) \oplus p(\infty) = p(\infty) \oplus p(t) = p(t)$。

2) 设 $P_1 = p(t_1), P_2 = p(t_2) \in C(F_p)$ 且 $t_1, t_2 \neq \infty$,定义 $P_1 \oplus P_2 = P_3$,即 $p(t_1) \oplus p(t_2) = p(t_3)$,其中

$t_3 =$

$$\begin{cases}(t_1+t_2+a)(t_1+t_2)^{-1}\bmod p, t_1+t_2\neq 0 \bmod p\\ \infty, t_1+t_2=0 \bmod p\end{cases} \tag{3}$$

$C(F_p)$ 上点 $P=p(t)$ 的逆元记作 $-P$，$-P$ 也是 $C(F_p)$ 上一点，且 $-P=p(-t)$，$-p(\infty)=p(\infty)$。

在 $C(F_p)$ 上定义点乘运算：令 k 是一个整数且 $P=p(t)\in C(F_p)$：

$$kP=kpm'=(t)=\begin{cases}p(t)\oplus\cdots\oplus p(t), k>0\\ p(\infty), k=0\\ (-k)p(-t), k<0\end{cases} \tag{4}$$

文献[3]给出了计算圆锥曲线 $C(F_p)$ 的点数 $\#C(F_p)$ 的计算公式，其中 $[\frac{a}{p}]$ 是勒让得符号。

$$\#C(F_p)=\begin{cases}p-1, [\frac{a}{p}]=1\\ p+1, [\frac{a}{p}]=-1\end{cases} \tag{5}$$

文献[1]证明了圆锥曲线 $C(F_p)$ 上的点和加法运算构成群，文献[3]证明了在圆锥曲线上已知一点 P 和 $Q=kP$，计算出 k 的值是困难的。称为圆锥曲线上的离散对数难题，可以像椭圆曲线那样构造公钥密码系统。

1.2 参数选择与安全性

文献[6]经过分析指出，参数 a 的选取会影响其安全性。并证明了当 a 为有限域 F_p 上的二次剩余时，有限域 F_p 上的离散对数安全性被降低到有限域 F_p 上的乘法群的离散对问题的安全性，特别的当 a 为有限域 F_p 上的二次剩余且有二重根时，安全性被降低到有限域 F_p 上的普通加法群的离散对数问题的安全性。当 a 不是有限域上的二次剩余时，有限域 F_p 上圆锥曲线的离散对数安全性没有降低，所以在选取有限域 F_p 上的圆锥曲线时，必须保证选取的参数 a 不是有限域 F_p 的二次剩余。

2 圆锥曲线数字签名方案

随机选取有限域 F_p 上的一条圆锥曲线 $C(F_p): y^2=ax^2-bx \bmod p$，其中 $[\frac{a}{p}]=-1$。选择阶数足够大的一基点 $P\in C(F_p)$，其阶为 $\mathrm{ord}(P)$，签名者选择 $d\in[0,\mathrm{ord}(P)-1]$ 作为私钥，$Q=dP$ 作为公钥。

下面利用圆锥曲线上的离散对数难题，实现一种对消息 m 的数字签名方案。

签名生成：

1) 随机选择一个整数 $k\in[0,\mathrm{ord}(P)-1]$；

2) 计算 $kP=(x_1,y_1)$，$r_1=x_1 \bmod \mathrm{ord}(P)$，如果 $r_1=0$，则返回到 1)；

3) 计算 $e=\mathrm{SHA}-1(m)$；

4) 计算 $r=r_1e \bmod \mathrm{ord}(P)$，$s=k+rd \bmod \mathrm{ord}(P)$，如果 $r=0$ 或 $s=0$，则返回到 1；

(r,s) 是对消息 m 的签名。

签名验证：验证者如下验证 (r,s) 是对消息的签名：

(1) 验证 r,s 是 $[1,\mathrm{ord}(P)-1]$ 中的整数；

(2) 计算 $e=\mathrm{SHA}-1(m)$；

(3) 计算 $X=sG-rQ=(x_1,y)$，如果 $X=0$，则拒绝这个签名，否则，计算 $v=x_1e \bmod \mathrm{ord}(P)$，当且仅当 $v=r$ 时接受这个签名。

方案分析：如果 (r,s) 是对消息 m 的正确签名，则 $s=k+rd \bmod \mathrm{ord}(P)$，从而 $sP-rQ=(s-rd)P=kP=(x_1,y_1)$，由此证明方案是正确的。$d$ 是私有的，任何人都无法伪造有效的签名，方案的安全性建立在圆锥曲线上离散对数的安全性基础上。

3 Schnorr 盲签名在圆锥曲线上的模拟

Schnorr 盲签名方案是由 Schnorr[6] 提出的一种安全性和效率较高的一种签名方案，郭涛等人[7]实现了 Schnorr 盲签名在椭圆曲线上的模拟，由于圆锥曲线在实现效率上比椭圆曲线要高，文中实现 Schnorr 盲签名在圆锥曲线上的模拟，参数仍然使用前面方案中的系统参数。下面给出简单的签名步骤。

签名过程：

1)签名者随机选择 $k\in[0,\mathrm{ord}(P)-1]$，并计算 $R=kP$，然后把 P 发送给用户 U。

2)U 随机选择 $\beta,\lambda\in[0,\mathrm{ord}(P)-1]$，并计算 $A=R+\beta Q+\lambda P=(x,y)$。

3)U 计算 $t=x \bmod \mathrm{ord}(P)$，$c=\mathrm{SHA}-(m\|t)$，$c'=c-\beta$。发送 c' 给签名者 S。

4) S 计算 $s'=k-c'd \bmod \mathrm{ord}(P)$，然后把 s' 发给 U。

5) U 计算 $s=s'+\lambda \bmod \mathrm{ord}(P)$。则 (c,s) 即为对消息 m 的签名。

签名验证：

(1) 验证者计算 $cQ+sP=(x',y')$，令 $v=x' \bmod \mathrm{ord}(P)$；

(2) 验证 v 和 t 是否相等，若相等则接受签名，否则拒绝。

方案分析：经过方程推导可以验证 $cQ+sP=R+\beta Q+\lambda P$，由此可以证明本方案是成立的。在整个签名的过程中，签名者始终没有见到消息 m，以后他也不能将自己的签名和特定消息联系起来。这样保证了签

(下转第 138 页)

5 结束语

基于数据挖掘的 MANET 网络入侵检测技术已经成为近年来研究的一个热点。文中采用数据挖掘的算法思想,尽可能快速高效地从网络海量数据信息中挖掘出有效的规则数据,并进行规则匹配,在模拟的移动自组织网络中,初步实现了该模型思想。以后的研究方向主要有:

(1)进一步改进挖掘算法,提高挖掘效率;

(2)根据移动自组织网络特性,采用分布式方法改进入侵检测模型,把入侵检测尽可能部署到 MANET 网络的移动代理中。

参考文献:

[1] Ichlamtac, Mconti. Mobile Ad hoc Networking: Imperatives and Challenges[J]. Ad hoc Networks ,2003,1(1):13-64.

[2] 卿斯汉,蒋建春,马恒太,等.入侵检测技术研究综述[J].软件学报,2004,25(7):19-29.

[3] Agrawal R, Imielinski T, Swanmi A. Mining Association Rules Between Sets of Items in Large Database[C]//Proc. of ACM-SIGMOD on Management of Data. Washington D. C: [s. n.],1993:206-207.

[4] Agrawal R, Srikant R. Fast Algorithms for Mining Association Rules[C]//Proc. of VLDB. Santiago, Chile: [s. n.], 1994: 487-499.

[5] Han J, Cai Y, Cercone N. Data-driven Discovery of Quantitative Rules in Relational Databases[J]. IEEE Transaction on Knowledge and Data Engineering,1993,5(1):29-40.

[6] Agrawal R, Omiecinski E, Navathe S. An Efficient Algorithm for Mining Association Rules in Large Databases[C]// the 21st VLDB Conference. Zurich, Switzerland: [s. n.],1995.

[7] Inmon W H. The Operational Data Store[M]. New York: John Wiley & SonsInc,1996.

[8] Au Wai-Ho, Chan K C C. FARM: a data mining system for discovering fuzzy association rules[C]//The 1999 IEEE International Fuzzy Systems Conference. FUZZ-IEEE'99. Seoul, South Korea: [s. n.],1999:1217-1222.

[9] Orchard R. Fuzzy reasoning in jess: the fuzzy J toolkit and fuzzy jess[C]//Proceedings of ICEIS 2001,3rd International Conference on Enterprise Information Systems. Setubal, Portugal: [s. n.],2001:533-542.

[10] 朱天清,熊 平.模糊关联规则挖掘及其算法研究[J].武汉工业学院学报,2005,24(1):24-28.

[11] Kuok C, Fu A, Wong M. Mining fuzzy association rules in database[J]. The ACM SIGMOD Record,1998,27(1):41-46.

[12] 毛国君,刘椿年.基于项目序列操作的数据挖掘算法[J].计算机学报,2002,25(4):417-422.

[13] Pasquier N, Bastide Y, Taouil R, et al. Efficient Mining for Association Rules Using Closed Item set Lattices[J]. Information Systems,1999,24(1):25-46.

[14] Massachusetts Institute of Technology. Lincoln Laboratory Data Sets[EB/OL]. 1999. http://www.11.mit.edu/IST/ideval/data/.

[15] Scalable Network Technologies[EB/OL]. 2005-03-10. http://www.qualnet.com.

[16] Huang Y A, Lee W. A Cooperative Intrusion Detection System for Ad Hoc Networks[C]//Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks. Fairfax, Virginia: [s. n.],2003.

(上接第 134 页)

名的盲性。私钥只有签名者自己知道,别人伪造他的签名也是不可能的,方案的安全性依然基于圆锥曲线上离散对数的困难性。

4 结束语

对有限域上的圆锥曲线进行了分析,指出参数选择对其安全性的影响,针对圆锥曲线上的离散对数难题,提出一种数字签名方案,并实现了 Schnorr 盲签名在圆锥曲线上的模拟。为其他数字签名和盲签名方案在圆锥曲线上的模拟提供了可能性。另外,在本方案中,如何取得阶数比较大的基点 P 值得进一步研究。

参考文献:

[1] 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.

[2] 曹珍富.基于有限域 F_p 上圆锥曲线的公钥密码系统[C]//刘木兰等编.第五届中国密码学学术会议论文集.北京:科学出版社,1998:45-49.

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

[4] Dai Zong-duo, Pei Ding-yi, Yang Jun-hui, et al. Cryptanalysis of a public key cryptosystem based on conic curves [C]//Proceeding of Cryp TEC'99: International Workshop on Cryptographic Techniques and E-Commerce. Hong Kong: City University of Hong Kong, 1999:259-261.

[5] 孙 琦,朱文余,王 标.环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.

[6] 许旭东,靳岩岩,赵 磊.圆锥曲线公钥密码算法参数选择[J].计算机工程,2007,33(15):159-160.

[7] 王化群,张力军,赵君喜.基于椭圆曲线的 Schnorr 盲签名[J].计算机工程与设计,2005,26(7):1819-1822.