文章编号:1001 - 9081(2009)09 - 2342 - 02

基于离散对数的数字签名方案

朱紫钊,姚国祥
(暨南大学 信息科学技术学院,广州 510632)
(happiness2080@126.com)

摘 要:分析了离散对数问题(DLP),以素数域上的离散对数为基础,同时结合有限域上的椭圆曲线离散对数问题,提出一种新的数字签名方案,其安全性建立在离散对数算法上。同时,分析了该签名方案的安全性,并将其与其他签名方案的性能进行比较。比较结果显示基于离散对数的数字签名方案比其他的数字签名方案效率要高,而且更安全。

关键词:公钥密码;数字签名;离散对数;椭圆曲线
中图分类号: TP309 **文献标志码**:A

New digital signature scheme based on discrete logarithm

ZHU Zi-zhao, YAO Guo-xiang
(*College of Information Science and Technology, Jinan University, Guangzhou Guangdong* 510632, *China*)

Abstract: The Discrete Logarithm Problem (DLP) was analyzed. Based on the discrete logarithm in the prime field, and combined with the elliptic curve DLP in the limited domain, a new digital signature was brought up. In addition, the security of this digital signature was analyzed and its performance was compared with other signatures. The results of comparison prove that this new digital signature based on discrete logarithm is more effective and secure than the others.

Key words: public key; digital signature; discrete logarithm; elliptic curve

0 引言

自从 1985 年 ElGamal 引入了基于离散对数的公钥密码体制,Victer Miller 和 Koblitz 引入了基于椭圆曲线的公钥密码体制后,目前有很多公钥密码体制的安全性都是基于上述两个问题困难性的[1]。多年来密码学者提出了许多基于离散对数的数字签名方案,但随着计算机技术的不断进步和网络应用的蓬勃发展,普通的数字签名方案已经不能满足要求,或者签名方案步骤繁多,或者安全方面出现了漏洞。

许多签名方案都是基于一个公认的数学难题,随着计算机性能的提高和密码学的发展,这些难题都有可能被攻击,相应的方案就不再安全。因此,许多密码学者提出了基于两个数学难题的签名方案,即同时基于离散对数和因子分解或者同时基于离散对数和大整数分解,使得签名方案更加安全。但经分析发现,这些签名方案都存在着安全性问题或者传输效率和计算效率较低的问题。随着对椭圆曲线研究的不断深入,人们认识到椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)比普通有限域上的离散对数更难解决,在密钥长度相当的情况下,椭圆曲线公钥密码系统比其他的公钥密码系统抵抗攻击的能力更强,且具有较高的安全性。由此本文提出的签名方案是基于椭圆曲线离散对数并且结合素数域上的离散对数问题,对签名方案进行安全性和性能分析,该方案可使用较短的密钥满足较高的安全性需要。短密钥使系统实现所需要的处理单元的计算能力的需求降低,网络上传输公钥需要的带宽等资源的需求相对较小,因此,利用椭圆曲线离散对数问题实现的签名方案具有许多优点。

1 离散对数问题

很多密码技术的安全性都建立在离散对数问题的困难性上,Diffie-Hellman 密码协议和它的各种变体,ElGamal 加密算法和 ElGamal 签名方案以及它的变体等,均建立在离散对数问题之上。

有三种群上的离散对数问题在密码学中比较常用,它们是有限域上的椭圆曲线群、特征为 2 的有限域的乘法群和素数域的乘法群。本文设计的签名方案利用素数域上的乘法群,其中素数域的乘法群上的离散对数问题可以表述如下。

离散对数问题(Discrete Logarithm Problem, DLP)如下[2]:给定一个素数 p,乘法群 Z_p^* 的一个生成元 α 和一个元素 $\beta \in Z_p^*$,求解整数 x,$0 \leqslant x \leqslant p-2$,使得 $\alpha^x = \beta (\mathrm{mod}\ p)$。

P 是一个大素数,那么以上这个离散对数就可被公认为困难问题,即不存在多项式时间算法来求解,为了抵抗已经知道的攻击,一般 P 至少取 256 b,$P-1$ 应该有一大的素因子。

在椭圆曲线密码体制中,一般在椭圆曲线 $E(F_q)$ 上选取一点 $G=(x_G, y_G)$ 作为公共基点,要求这个公共基点的阶 n 为一个素数阶,并使数阶 n 足够大。G 是椭圆曲线的生成元,即 Abel 群 $\langle G\rangle = \{G, 2G, 3G, \cdots, nG\} \subseteq E(F_q)$ 是由点 G 生成的 n 阶循环子群,且以 $\langle G\rangle$ 来构建密码体制。

椭圆曲线离散对数问题如下[3]:给定椭圆曲线 $E(F_q)$,点 $G \in E(F_q)$,G 的阶数为 n,对于给定点 $Q \in \langle G\rangle$,求整数 $x \in [2, n-1]$,使得 $xG = Q$。

适合于乘法群上的离散对数算法,只要稍作修改均可直接应用到基于椭圆曲线的离散对数问题,而且本文设计的数

收稿日期:2009 - 03 - 23;**修回日期**:2009 - 05 - 16。
基金项目:国家自然科学基金资助项目(60773083);广东省科技计划项目(2006B15401002);省部产学研项目(2008B090500201)。
作者简介:朱紫钊(1985 -),男,广东江门人,硕士研究生,主要研究方向:网络技术、信息安全; 姚国祥(1959 -),男,安徽桐城人,教授,博士生导师,主要研究方向:信息系统集成、网络应用、信息安全。

字签名方案主要基于有限循环群上的椭圆曲线离散对数。

2　基于椭圆曲线离散对数问题的数字签名

由于 RSA 密码体制中所要求的素数越来越大,致使工程实现变得越来越困难,最近人们发现椭圆曲线是克服此困难的一个强有力的工具。目前许多数字签名的方案的安全性仅基于一个数学难题,或者是离散对数,或者是素因子分解等,两个数学难题同时变得容易求解是不太可能的,将会增强其安全性。由于椭圆曲线密码体制本身的优点,我们将素数域上的离散对数问题和椭圆曲线上的密码体制结合在一起,使得数字签名方案更加安全。

2.1　新的数字签名方案

1) 系统参数设置。

设 p 是一个素数,$g \in Z_p^*$ 是生成元,那么在素数域 Z_p^* 上求解离散对数问题 $y = g^x (\mathrm{mod}\ p)$ 是数学中的一个难题。

其中:

p 为大素数,$2^{l-1} < p < 2^l$,512 b < l < 1024 b 并且 l 为 64 的倍数,p 满足 Z_p 中的离散对数问题是难解决的;

q 为大素数,$q \mid (p-1)$,$q \geqslant 2^{160}$;

$g \in_R Z_p^*$,且 $g^q \equiv 1 (\mathrm{mod}\ p)$;

E 为安全椭圆曲线;

n 为椭圆曲线公共基点 G 的阶,是一个素数阶并且数阶 n 足够大;

G 为为椭圆曲线的公共基点,也即生成元,Abel 群$\langle G\rangle = \{G,2G,3G,\cdots,nG\} \subseteq E(F_q)$ 是由点 G 生成的 n 阶循环子群。选取一个基域 $GF(P)$ 和定义在该基域上的椭圆曲线 $E_p(a,b)$ 及其上拥有素数阶 n 的生成元点 $G = (x_G, y_G)$,其中有限域 $GF(P)$,椭圆曲线参数 a,b,点 $G = (x_G, y_G)$ 和阶 n 都是公开信息。

2) 产生用户私钥与公钥。

用户 A 随机选取 $x, x \in [1,p]$ 作为私钥,计算:$y \equiv g^x \mathrm{mod}\ p$,$Q = xG$,$y$ 和 Q 作为公钥对外公布。

3) 签名产生过程。

对于任意的消息 m,用户 A 进行如下计算:

① 随机选取一个整数 $d \in [1,q]$,计算椭圆曲线上的一点 $(x_1, y_1) = dG$;

② 转换域元素 x_1 到整数 $\bar{x}_1$,并设置 $k = \bar{x}_1 \mathrm{mod}\ n$;

③ 计算 $r = g^k \mathrm{mod}\ p$,$r \neq 1$,并且计算 $e = H(m)$;

④ 计算 $s_1 = xe + k \mathrm{mod}\ n$ 和 $s_2 = xe + r \mathrm{mod}\ n$;

那么 (s_1, s_2) 为消息 m 的签名,用户 A 将签名消息组 $(m; (s_1, s_2))$ 发送到签名验证者。

4) 签名验证过程。

当签名验证者收到签名消息组 $(m;(s_1,s_2))$ 后,从数字签名公钥库系统中取出参数 g 和参数 G,并取出用户 A 的公钥 (y,Q),从得到的签名消息中取出 m 和 s_1 计算:$e = H(m)$,$u = g^{s1} y^{-e}$,并验证签名:$Ver(y,Q,G,m,(s_1,s_2)) = True \Leftrightarrow eQ + uG = s_2 G$ 是否成立,若上述方程成立,签名有效,否则签名无效。

5) 证明验证方程的有效性。

$$eQ + uG = eQ + g^{s1} y^{-e} G = exG + g^{xe+k} \cdot g^{-ex} \cdot G = exG + g^k G = (ex + r)G = s_2 G$$

其中:$u = g^{s1} y^{-e}$,$Q = xG$,$g^{s1} = g^{xe+k}$,$y^{-e} = g^{-ex}$,$r = g^k$,$s_2 = ex + r$。

2.2　对签名方案的可能攻击与安全性分析

对于所有椭圆曲线有限群上离散对数问题的算法,都是从一般群 G 上离散对数算法平移而来,一般而言,一般群 G 上离散对数算法可分为两类:Index Calculus 算法和碰撞搜索法。Index Calculus 算法具有亚指数时间复杂度,是目前解决一般群 G 上离散对数问题的最好算法,但对 ECDLP,该算法无论从理论上还是从实际上计算都不可行;碰撞搜索法具有纯指数时间复杂度,不同于上面说的 Index 算法,这一类算法可以用于求解 ECDLP。对一般的 ECDLP,除了上面介绍的方法外无其他的求解方法。

1) 假设攻击证明此方案的安全性是建立在离散对数和椭圆曲线两大难题之上的。攻击有限域上离散对数问题的方法有指数积分法,求解 $y \equiv g^x \mathrm{mod}\ p$ 中的私钥 x,等价于在有限域 F 中求解离散对数,其运算复杂度为:$O(\exp \sqrt[3]{(\mathrm{lb}\ p)(\mathrm{lb}\ (\mathrm{lb}\ p)^2)})$。其中模数 p 是大素数。

目前,攻击椭圆曲线上的离散对数问题的方法只有大步、小步法,求解 $Q = xG$ 中的私钥 x,该方法的运算复杂度为:$O(\exp(\mathrm{lb}\ \sqrt{P_{\max}}))$。其中,$P_{\max}$ 是椭圆曲线所形成的 *Abel* 群的阶的最大素因子[4]。因此,同时引入椭圆曲线密码体制比只基于有限域上的离散对数问题的公钥密码体制更安全,需要花费指数级的时间,计算上不行。

2) 攻击者在得到签名者 A 对文件 m 的签名 (s_1, s_2) 后,试图从式 $s_1 = xe + k \mathrm{mod}\ n$ 和 $s_2 = xe + r \mathrm{mod}\ n$ 中计算得到其私钥,上式中 S_1, S_2, e, n 都是已知的,但要从 $s_1 = xe + k \mathrm{mod}\ n$ 中计算 x,由于式中有两个未知数 x 和 k,x 是私钥,攻击者不知道,求 k 需要解椭圆曲线离散对数问题,而且式 $s_2 = xe + r \mathrm{mod}\ n$ 中的 r 由 k 求出,求 r 需要求解大素数离散对数问题,在不知道 k 的情况下计算 r 是十分困难的,因此,攻击者要从签名 (s_1, s_2) 中求出其私钥 x,计算上不可行。

3) 攻击者试图伪造签名者 A 对消息 m' 的签名 (s_1, s_2) 并通过验证。由于签名中的 s_1 和 s_2 是通过公式 $s_1 = xe + k \mathrm{mod}\ n$ 和 $s_2 = xe + r \mathrm{mod}\ n$ 计算,对于不同的消息 m',其散列函数值 $e' = H(m')$ 不同于 $e = H(m)$,而且攻击者又不知道 x 和 k 值,因此攻击者无法成功伪造签名。

4) 假设攻击者通过 $y \equiv g^x \mathrm{mod}\ p$ 成功求出私钥 x。由于在产生签名的过程中选择随机数 d 来计算椭圆曲线的点 $(x_1, y_1) = dG$,而产生签名的式 $s_1 = xe + k \mathrm{mod}\ n$ 和式 $s_2 = xe + r \mathrm{mod}\ n$ 的计算要使用 d 值,因此攻击者无法成功伪造签名 (s_1, s_2)。

5) 由 Hasse 定理:$p + 1 - 2\sqrt{p} \leqslant \#E(F_p) \leqslant p + 1 + 2\sqrt{p}$($\#E(F_p)$ 表示椭圆曲线群上点的总数),可求出椭圆曲线上点的总数的范围[5]。虽然可由 Schoof 算法计算出 $\#E(F_p)$ 的精确值,但其过程非常复杂。椭圆曲线群上点的有限性和点数目的确定性对加密而言是好的属性,因为这些曲线只是包含了一些离散的点,攻击者不知如何把这些点相连成曲线,也就不知如何应用几何关系。

3　效率分析

在各种签名方案中,模指数运算、模乘运算和求逆运算是比较费时的,其中模指数运算最耗时,下面分析这几项运算所用的时间。现在假设 Lpk 为公钥长度,Lsk 为私钥长度,$Lsig$ 为签名长度,T_{mod} 为方案中模乘运算的时间,$T_{\exp}$ 为方案中模指数运算的时间,T_{ath} 为方案中逆运算的时间,sig_{time} 为签名时间

(下转第 2354 页)

2.6 性能分析

在计算复杂度方面,本方案的中间路由节点只是计算两次异或运算、几个Hash函数、两次对称密钥的运算,对称密码体制下的一次解密和一次加密。由于对称密码体制和Hash函数实现的速度要远远快于基于公钥密码体制的匿名通信方案[3],因此,以上这些计算的计算复杂度是非常低的。

在存储复杂度方面,文献[4]的方案为了达到匿名通信目的,每个节点需要的存储量为$6k+7kN$,其中k表示大小为k位的伪名空间,N为当前节点的邻接节点个数。假设一个无线传感器网络有1000个节点,伪名空间大小为64 b,每个节点的邻接节点平均为100个则每个节点需的存储量为$6\times64+7\times64\times100=45184$ b $=5648$ B $=5.6$ KB,如果有10000个节点,则存储量为$6\times64+7\times64\times1000=54.7$ KB,可见随着网络规模增加,方案所需存储量也呈线性增加,并不太适用于资源受限的传感器网络。文献[5]使用哈希函数链提出两个无线传感器网络匿名通信方法,但这两个方案都需要每个节点存贮并维护一张邻接节点信息表,当随着网络节点数增加所需存储空间也急剧增加,不适合大规模分布式无线传感器网络。在本文提出的方案中,每个节点S_i仅需存储$(ID_i, h(ID_i), qh(ID_i), G_1, G_2, e: G_1\times G_1\rightarrow G_2, h(\cdot))$,每个符号表示的意思如2.2节所示,需要的存储量为一个与网络大小无关的常量。

3 结语

本文使用双线性函数的双线性对,哈希函数和异或运算提出了一种可验证安全的无线传感器网络匿名通信方案。方案在路由建立过程中隐藏通信节点的身份信息,只有被选中路径上的节点才能获得完整的路由信息,方案采用对称密钥机制替代公钥签名机制,在保持具有较高的安全性和匿名性同时,大大提高系统的计算复杂度和存储复杂度。本文的下一步工作将进一步在网络仿真平台上对路由建立时间与数据包发送迟延进行仿真,以全面评价该方案的性能。

参考文献:

[1] KONG J, HONG X. ANODR: Anonymous on demand routing with untraceable routes for mobile Ad-Hoc networks [C]// MobiHoc'03: Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Annapolis, MD, USA: ACM Press, 2003: 291-302.

[2] ZHU BO, WAN ZHI-GUO, KANKANHALLI M S, *et al*. Anonymous secure routing in mobile Ad-Hoc networks [C]// Proceedings of the 29th Annual IEEE Inter national Conference on Local Computer Networks. Tampa, USA: IEEE Computer Society, 2004: 102-108.

[3] 章洋,范植华,何晓新,等.移动自组网络中多径路由的匿名安全[J].电子学报, 2005,33(11): 2022-2029.

[4] MISRA S, XUE G. Efficient anonymity schemes for clustered wireless sensor networks[J]. International Journal of Sensor Networks, 2006, 1(1/2): 50-63.

[5] YI OU-YANG, LE ZHENG-YI, XU YU-RONG, *et al*. Providing anonymity in wireless sensor networks [C]// Proceedings of the 2007 IEEE International Conference on Pervasive Services. Washington, DC: IEEE Computer Society, 2007: 145-148.

[6] BARRETO P S L M, KIM H Y, LYNN B, *et al*. Efficient algorithms for pairing-based cryptosystems [C]// Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, LNCS 2442. Berlin: Springer-Verlag, 2002: 354-368.

(上接第2343页)

复杂度,val_{time}为验证时间复杂度。将本文的签名方案与其他方案进行比较,见表1所示。

表1 四种方案的密钥长度、签名长度及时间复杂度比较

运算	本文方案	文献[6]方案	文献[7]方案	文献[8]方案
Lpk	$[\log n]+2[\log p]$	$n[\log n]+[\log p]$	$[\log p]+T$	$[\log n]+[\log p]$
Lsk	$[\log n]$	$[\log n]$	$[\log n]+T$	$[\log n]$
$Lsig$	$2[\log n]$	$[\log n]+[\log p]$	$3[\log n]$	$[\log n]+[\log p]$
sig_{time}	$T_{exp}+3T_{mod}$	$T_{exp}+2T_{mod}$	$T_{exp}+4T_{mod}+T_{ath}$	$2T_{exp}+3T_{mod}$
val_{time}	$T_{exp}+2T_{mod}$	$[\log n](T_{exp}+T_{mod})$	$2T_{exp}+[\log t]T_{mod}$	$2T_{exp}+3T_{mod}$

表1中,计算公钥$Lpk=(n,p)$,其长度为$[\log n]+[\log p]$,模指数运算T_{exp}为计算如$y\equiv g^x \bmod p$的时间,模乘运算T_{mod}为计算如$s_1=xe+k \bmod n$的时间,逆运算T_{ath}为计算如$k^{-1} \bmod n$的时间。从表1可以看出,本文中的方案与文献[6-8]中方案相比具有签名密钥短、计算时间复杂度小等优点。

4 结语

本文提出了一个新的签名方案,从新的角度将素数域上的离散对数和椭圆曲线结合起来,基于椭圆曲线离散对数的签名方案,可以大大提高数字签名的安全性和性能,它的安全性同时基于这两个困难问题的求解,达到了设计要求。并且,将本文方案与其他签名方案进行了比较,具有较快的运行速度和较好的安全性。随着计算机技术的发展,减少基于双难题签名方案的复杂度,以及如何提高签名方案的效率将是今后深入研究的内容。

参考文献:

[1] KOBLITZ N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209.

[2] MENEZES A J, VAN OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography[M]. 胡磊,王鹏,译. 北京:电子工业出版社, 2005.

[3] WILLIAM S. Cryptography and network security principles and practices [M]. 孟庆树,王丽娜,傅建明,等译. 4版. 北京:电子工业出版社, 2007.

[4] 胡向东,魏琴芳.应用密码学教程[M].北京:电子工业出版社,2005.

[5] 王衍波,薛通.应用密码学[M].北京:机械工业出版社.2003.

[6] 贾晓芸,罗守山,袁超伟.一种新的基于离散对数的签名方案[J].西安电子科技大学学报:自然科学版, 2008,35(2): 352-354.

[7] 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): 61-64.

[8] 任俊伟,林东岱.一种基于因数分解和离散对数的签名算法的分析与改进[J].计算机工程与应用, 2005,41(7): 132-135.