

基于椭圆曲线的盲数字签名及其身份识别

王龙葛,王天芹,田珂,徐飞

(河南大学 数据与知识工程研究所,河南 开封 475004)

摘要:椭圆曲线密码体制以其特有的优越性被广泛用于进行数据加密和构建数字签名方案。同样,它也可以用来构建盲数字签名方案。介绍了椭圆曲线密码体制的相关知识,基于求解椭圆曲线离散对数问题的困难性,设计了一种基于椭圆曲线离散对数问题的盲数字签名方案,并在此基础上设计了一种身份识别协议,该方案可以同时满足盲数字签名的正确性、匿名性、不可伪造性和不可追踪性等特性要求。从理论上分析该方案是安全的,并具有一定的实用价值。

关键词:椭圆曲线;离散对数问题;盲数字签名;身份识别

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2008)06-0142-02

A Blind Digital Signature Scheme and User Authentication Based on Elliptic Curves Cryptosystem

WANG Long-ge, WANG Tian-qin, TIAN Ke, XU Fei

(Institute of Data and Knowledge Engineering, Henan University, Kaifeng 475004, China)

Abstract: The elliptic curve cryptosystem is far and wide used to encrypt information and construct digital signature scheme by its speciality. Also it can be used to construct blind digital signature scheme. Introduces the knowledge about elliptic curves cryptosystem. On the difficulty of calculating ECDLP, a new blind digital signature scheme based on elliptic curves cryptosystem is designed, and a user authentication scheme based on the blind digital signature is presented. This scheme can meet correctness, unfalsification and untracing of the blind digital signature scheme. The scheme is secure in theory and is suitable for some practice.

Key words: elliptic curves; discrete logarithmic problem; blind digital signature; user authentication

0 引言

盲数字签名是一种特殊的数字签名方案^[1,2], 1983年 Chaum 首先提出了盲数字签名的概念^[3], 在电子投票和数字货币协议得到了广泛的应用。一个盲签名方案是一个包含2个参与者的密码协议: 一个用户U和一个签名者s。它通常具有以下两个特征: 消息的内容对签名者保密; 签名者后来看到签名时不能与盲消息对应起来。用户A可以用签名来检验签名者的身份, 任何第三者也可以验证。如签名者为一权威机构, 用户可以用该机构的盲签名来向第三方证明他得到了权威机构的许可。

一般情况下, 一个安全的盲数字签名应具有如下特性:

- (1) 可验证性, 任何人可以使用签名者的公钥来验证签名是否正确;
- (2) 盲性, 需要签名的消息的内容对签名者是不可见的;
- (3) 不可伪造性, 除签名者以外的其它人, 不可能伪造签名并通过验证;
- (4) 不可追踪性, 在签名被接收者泄露后, 签名者不能追踪签名。

文中提出了一种基于椭圆曲线密码体制的盲数字签名方案, 并在该签名方案基础上设计了一种身份识别方案, 其安全性基于椭圆曲线离散对数问题, 较一般的离散对数问题, 椭圆曲线离散对数问题的求解更为困难。

1 基于椭圆曲线的盲数字签名方案

1.1 椭圆曲线上的离散对数问题

椭圆曲线上密码系统的安全核心是椭圆曲线上的离散对数问题(ECDLP)^[4]。

设乘法群G是一个阶为n的有限循环群, α 是它

收稿日期: 2007-09-23

基金项目: 国家自然科学基金资助项目(10671056); 河南大学重点基金项目(05ZDZR001)

作者简介: 王龙葛(1983-), 女, 河南南阳人, 硕士研究生, 研究方向为密码学、信息安全; 王天芹, 博士, 副教授, 硕士生导师, 研究方向为数论与密码学。

的生成元, $\beta \in G$ 。则以 α 为基的 β 的离散对数问题为: 求解 $x, 0 \leq x \leq n$, 使得 $\beta = \alpha^x$ 。那么 $x = \log_{\alpha} \beta$, 称其为以 α 为基的 β 的离散对数。

若 E 为 F_p 上的椭圆曲线, G 为 E 上的一点, 那么 E 上关于 G 椭圆曲线离散对数问题即为: 给定一点 $N \in G$, 求解整数 x , 使 $xG = N$ 。这里的 xG 表示数乘, 也就是 x 个 G 相加。容易看出, 对该系统的攻击依赖于在有限域 F_p 上求解方程: $G^x \equiv N \pmod{p}$ 或者计算 $x = \log_G N \pmod{p}$ 。

有限域上离散对数问题的求解非常困难, 椭圆曲线离散对数问题比有限域上的离散对数问题更难求解。

在有限域 F_p 上选择一条椭圆曲线及一个具有较高阶的基点 $G \in E(F_p)$, 计算该点的数乘 kG (所谓数乘就是一连串点的加法运算, 即: $k * G = G + G + \dots + G$, 共有 k 个 G 相加) 相对来说是容易的, 但是在已知 G 和 kG 的情况下要求解 k 是一个极其困难的问题, 在目前的运算条件下, 对椭圆曲线离散对数问题还没有一般的子指数时间算法^[5]。

本方案的安全性就建立在椭圆曲线离散对数问题的难解性之上。

1.2 方案设计过程

m 为待签名的消息, 用户 A 把消息盲化后发送给签名者 B , B 签名后发还。

1) 系统初始化。

F_p 为特征值 char 不为 2, 3 的有限域, p 为 $\geq 120\text{bit}$ 的大素数。

椭圆曲线 $E: y^2 = x^3 + ax + b, a, b \in F_p$ 且 $4a^3 + 27b^2 \neq 0$ 。

$P \in E(F_p)$ 是一个公共基点, 且 $l = \text{ord}(P)$ 是公共基点的阶 ($l \geq 120\text{bit}$)

$\#E(F_p)$ 至少有 40 位以上的大素数因子。

签名者 B 的私钥为 $x \in \{1, \dots, l-1\}$, 公钥为 $P_B = xP$

2) 消息的盲化过程。

选择随机数 $r \in \{1, \dots, l-1\}$

对待签名消息 m 编码得点 $p(m) = (m_x, m_y) \in E(F_p)$, 输出盲消息 $b(r, m) = rm_x m_y \pmod{l}$

3) 签名生成过程。

Step1: 用户 A 选择随机数 $r \in \{1, \dots, l-1\}$,

计算 $r^{-1}, rr^{-1} = 1 \pmod{l}, m' = b(r, m) = rm_x m_y, R' = r^{-1}P$

将 m', R' 发送给签名者 B 。

Step2: 签名者 B 选择随机数 $k \in \{1, \dots, l-1\}$,

计算 $R = kR' = (r_x, r_y)$ 其中 r_x 为 R 的 x 坐标, r_y 为 R 的 y 坐标。

计算 $e' = r_x m', y' = k + x e' \pmod{l}$

将 (e', y') 发送给 A 。

Step3: 用户 A 计算 $y = r^{-1} y' \pmod{l}, e = r^{-1} e' \pmod{l}$

输出签名 (y, e) 。

4) 签名验证过程。

验证者收到签名 (y, e) 后, 验证 $R = yP - eP_B, e = r_x m_x m_y \pmod{l}$ 是否成立。若等式成立, 则验证通过, 否则签名不正确。

1.3 基于上述签名的身份识别

假定上述签名方案中的签名者是一个网络认证机构——CA, 用户 A 的签名消息 m 包含了用户 A 的身份信息, 其中可能含有 A 不愿公开的信息, 所以将之盲化, 按照上述签名方案生成签名 (y, e) , 于是 A 就得到了 CA 分配的身份证书 (y, e, m', R') , 如果 A 想向 B 证明身份, 其过程如下:

Step1: 用户 A 选择随机数 $a \in \{1, \dots, l-1\}$, 计算 $D = aP$ 。

Step2: 用户 A 发送证书 (y, e, m', R') 和 D 给用户 B 。

Step3: 用户 B 验证 CA 的签名, 即计算 $R' = yP - eP_A = (r'_x, r'_y)$ 并检验 $e = r'_x m_x m_y \pmod{l}$ 是否成立。

Step4: 用户 B 选择随机数 $b \in \{1, \dots, l-1\}$, 送给用户 A 。

Step5: 用户 A 计算 $u = a - br^{-1} \pmod{l}$, 并把 u 的值发送给用户 B 。

Step6: 用户 B 验证 $D = uP + bR'$ 是否成立。若成立则承认用户 A 的身份, 否则拒绝。

在身份识别的过程中, 如果攻击者伪造用户 A 的身份证书 (y, e, m', R') , 则 step3 不成立。如果攻击者在 step5 中计算 u' 发送给用户 B , 由于攻击者无法知道用户 A 的随机数 a 和 r , 因此 step6 不成立。

2 方案的安全性分析

(1) 可验证性。

$$\begin{aligned} R &= yP - eP_B \\ &= r^{-1}y'P - r^{-1}e'P_B \\ &= r^{-1}(k + xe')P - r^{-1}r_x m' xP \\ &= r^{-1}P(k + xe' - r_x m' x) \\ &= r^{-1}P(k + xr_x m' - r_x m' x) \\ &= r^{-1}Pk = R'k = R \end{aligned}$$

(下转第 147 页)

由于经济全球化的影响,应该以前瞻的目光来发展我国的 PKI。由于电子商务多为全球跨国界行为,因此 CA 与 CA 间特别是国与国之间 CA 的交互认证问题亦有待解决,而这其中所涉及的问题除技术层面外,政治与经济利益等因素也是用户或国家考虑的重点。目前国内相关专家学者已考虑三种可行解决方案,即 Root CA、Bridge CA 及 OCSP(Online Certificate Status Protocol) Responder(即证书状态在线查询)。无论未来我国会以何种方案来实施,必须既要考虑建立统一的国家证书管理中心来解决 CA 交互认证问题,还要尊重并依循市场发展机制,提供统一数据查询平台,供一般使用者在线查询数字证书合法性及有效性,使数字证书的相关业务朝更多元化发展。

4 结束语

据 IDC 调查,全球 PKI 市场正在急剧扩大,预计到今年有望达到 30 亿美元的规模^[6]。若针对以上在

建制 PKI 系统中提出的问题采取较好的应对措施,这将会极大促进 PKI 在我国各行业的应用和普及,推进我国信息化建设。

参考文献:

- [1] 李明柱. PKI 技术及应用开发指南[EB/OL]. 2002-06-12. www.developerworks.com.
- [2] 谷和启. 公钥基础设施 PKI 技术与应用发展[EB/OL]. 2003-11-10. http://network.ccidnet.com.
- [3] 从国际电子商务立法到中国的电子商务政策法律环境[EB/OL]. 2004-07-13. http://www.chinaeclaw.com.
- [4] 吴世忠. 规范 CA 认证中心的建设已成当务之急[N]. 光明日报, 2000-07-19(B1).
- [5] 卢旭成. 《电子签名法》实施两年成绩显著, 电子认证服务: 在规范中开拓发展[N]. 中国计算机报, 2007-05-09(A2).
- [6] 余勇. 标准化推动 PKI 发展[EB/OL]. 2003-06-27. http://www.ccidnet.com.

(上接第 141 页)

- [3] Susilo W, Safavi-Naini R, Pieprzyk J. RSA based fail-stop signatures schemes[C]//International Workshop on security. Washington, D C, USA: IEEE Computer Society Press, 1999: 161-166.
- [4] 马春波, 何大可. 门限失败-停止签名[J]. 计算机工程与

应用, 2004(19): 145-146.

- [5] 杨波. 现代密码学[M]. 北京: 清华大学出版社, 2003: 143-181.
- [6] 卿斯汉. 安全协议[M]. 北京: 清华大学出版社, 2005: 66-75.

(上接第 143 页)

$$\text{又 } e = r^{-1}e' = r^{-1}r_xm' = r^{-1}r_xrm_xm_y = r_xm_xm_y$$

由上可知, 该签名能通过验证。

(2) 盲性。盲性是盲数字签名的重要特性, 匿名意味着签名者不知道需要签名的真实内容。在此方案的签名过程中, 签名者 B 在不知道用户 A 的盲因子的情况下, 只能获得用户 A 盲化后的信息 m' , 而由 m' 得到 m 等价于求解椭圆曲线离散对数问题, 所以签名者不可能看到明文消息。

(3) 不可伪造性。任何人要伪造签名 (y, e) , 并通过验证方程 $e = r_xm_xm_y \bmod l$ 的检验, 其困难性等价于求解椭圆曲线离散对数问题。

(4) 不可追踪性。假设签名者保留 (y, e, m', R') , 若签名者想追踪签名, 他需要通过盲化消息 m' 求得有关 A 的秘密信息, 但是由于 m' 求解 m 的难度等价于求解椭圆曲线的离散对数问题, 所以在签名被接收者泄露后, 签名者不能追踪签名。

3 结束语

设计了一种基于椭圆曲线密码体制的盲数字签名及其身份识别方案, 具有较高的安全性, 并在电子商务、电子投票中具有一定的理论和实用价值。众所周知, 目前还没有有效求解椭圆曲线离散对数问题的算法, 所以该方案目前是安全的。

参考文献:

- [1] Fan C I, Chen W K, Yeh Y S. Randomization enhanced Chaum's blind signature schemes[J]. Comput. Commun., 2000, 23: 199-203.
- [2] Shao Z. Improved user efficient blind signatures[J]. Electronic Letter, 2000, 36(16): 209-219.
- [3] Chaum D. Blind Signature System[C]//Advances in Cryptology, CRYPTO'83. NEW YORK: Springer Verlag, 1983.
- [4] 杨义先, 钮心忻. 应用密码学[M]. 北京: 北京邮电大学出版社, 2005: 133-147.
- [5] 冯登国. 密码分析学[M]. 北京: 清华大学出版社, 2000.