文章编号:1005－0523(2006)02－0144－03

基于椭圆曲线的具有消息恢复的数字签名方案

刘 欣[1],龙 昆[2],亢保元[1]

(1.中南大学 数学科学与计算技术学院,湖南 长沙 410075;2.南昌大学 学工处,江西 南昌 330000)

摘要:基于椭圆曲线离散对数问题(ECDLP)和平方剩余问题,本文提出了一种新的具备消息自动恢复特性的数字签名方案,同时对该方案进行了各种安全性分析,得出结论:该方案具有前向安全性,而且在第三方仲裁时无需泄露密钥(即具有零知识特性).

关 键 词:数字签名;椭圆曲线;消息恢复;零知识证明

中图分类号:TP391.41 **文献标识码**:A

1 引言

数字签名在现代电子数据处理过程中扮演着非常重要的角色,而具有消息恢复特性的数字签名不需发送原始数据,因而比其他数字签名具有更为重要的作用.具有消息恢复特性的数字签名只有指定的验证者才能够在验证过程中恢复消息.基于一般离散对数问题的消息恢复签名方案是由 K. Nyberg 和 R. A. Ruppel[1]在 1994 年首先提出的,之后人们提出了各种具有消息恢复特性的数字签名方案,如文献[2－4]是基于离散对数问题或因子分解的,文献[5]是基于 ECDLP 问题的.事实上,基于 ECDLP 问题的签名方案与一般的离散对数问题相比具有如下优点:安全性能更高;计算量小,处理速度快;存储空间占用小;带宽要求低.虽然文献[5]提出了基于椭圆曲线的具有消息恢复特性的签名方案,但它仍然存在安全性问题,对该文的分析请参阅文献[6].因而本文在文献[2]的思想基础上提出了一种基于 ECDLP 问题的具有消息恢复的数字签名.

2 具有消息恢复的数字签名方案

假定系统中有两个用户 A 和 B,A 对消息 m 进行签名并将签名后的消息发送到 B,B 收到签名消息后恢复消息并对签名进行验证.该方案包含三个阶段:系统初始化阶段,签名过程和签名验证(消息恢复)过程.

2.1 系统初始化

设 E 是定义在有限域 F_q 上的一条安全的椭圆曲线,使得 E 上的 F_q－有理点群的阶被一个大素数 n 整除,保证椭圆曲线上有理点群上的离散对数问题是难解的.选取一个基点 $P\in E$, P 的阶为 n,即有 $nP=O$, O 表示无穷远点, h 是一个安全的 hash 函数.基点 P、椭圆曲线 E、hash 函数 h 以及素数 n 公开.系统内的每个用户 U_i 选择整数 u_i 满足 $1<u_i<n$,并将 u_i 作为签名私钥,计算 k_i 满足 $k_iu_i^2=1 \bmod n$, k_i 作为 U_i 的验证私钥,然后计算 U_i 的公钥 $P_i=k_iP$,公开 P_i.同理 U_i 再选择整数 v_i 满足 $1<v_i<n$,并将 v_i 作为私钥,计算公钥 t_i 满足 $t_iv_i^2=1 \bmod n$,公开 t_i.

2.2 签名过程

收稿日期:2006－01－22

作者简介:刘 欣(1982－),女,湖南怀化,中南大学在读硕士研究生,研究方向为密码学.

若用户 A 要发送消息 m 给用户 B,用户 A 首先从系统公开文件中获取基点 P、素数 n、$hash$ 函数以及用户 B 的公钥 P_B.

1) 用户 A 计算 $e=h(m)$, $V=(m+e)P_B$.

2) 用户 A 计算 $z=m+(V)_x \bmod n$(其中 $(\cdot)_x$ 表示 E 上的点 $(\cdot)$ 的 x 坐标).

3) 用户 A 随机选择两个整数 r 和 R,且 $\gcd(r,n)=1$,然后用户 A 计算 $T=RP_B$,并将 T 公开.

4) 用户 A 计算 $x=\frac{u_A}{2}\left(r+\frac{h(z)+m+e+R}{r}\right) \bmod n$, $y=\frac{u_A v_A}{2}\left(r-\frac{h(z)+m+e+R}{r}\right) \bmod n$,则数组 (x,y,z) 就是用户 A 对消息 m 的签名,用户 A 将 (x,y,z) 发送给用户 B.

2.3　签名验证(消息恢复)过程

用户 B 接收到用户 A 的签名 (x,y,z) 之后,用户 B 首先从系统公开文件中获取基点 P、素数 n、$hash$ 函数以及用户 A 的公钥 P_A 和 t_A,并获取用户公开的参数 T.

1) 用户 B 计算 $P_R=u_B^2T$, $V_1=(x^2-t_Ay^2)P_A$, $V_2=V_1-h(z)P-P_R$, $V_3=k_BV_2$,

2) 用户 B 计算 $m=z-(V_3)_x$,并验证等式 $(m+e)P=V_2$ 是否成立,若等式成立,则用户 B 接受 m 为原消息.

下面我们证明上述方案中的消息恢复过程是正确的.

$$P_R=u_B^2T=u_B^2RP_B=u_B^2Rk_BP=RP$$

$$V_1=(x^2-t_Ay^2)P_A=u_A^2(h(z)+m+e+R)P_A=u_A^2k_A(h(z)+m+e+R)P=(h(z)+m+e+R)P$$

$$V_2=V_1-h(z)P-P_R=(h(z)+m+e+R)P-h(z)P-P_R=(m+e)P$$

$$V_3=k_BV_2=k_B(m+e)P=(m+e)P_B=V$$

$$m=z-(V_3)_x=z-(V)_x$$

因此,我们可以看出消息 m 就是用户 A 传给用户 B 的消息.

3　安全性分析

下面对这个签名方案进行各种安全性分析.

1) 显然,从用户的公钥求解相应的私钥等价于求解 $ECDLP$ 问题或平方剩余问题.

2) 由 $P_R=u_B^2T=RP$ 知,因为攻击者没有用户 B 的私钥 u_B,则攻击者无法获得相应的 P_R,就算攻击者知道了 P_R,由方程 $(m+e)P=(x^2-t_Ay^2)P_A-h(z)P-P_R$ 知,要恢复相应的消息 m,攻击者将面对 $ECDLP$ 问题.

3) 若用户 B 想获取 A 的私钥,根据方程 $x^2-t_Ay^2=u_A^2(h(z)+m+e+R)$ 知,因为 B 不知道 R,所以用户 B 想得到 u_A^2 要面对因式分解问题.如果 B 收集了 l 份消息 m_i 的 l 组签名 (x_i,y_i,z_i), $i=1,\ldots,l$,根据上面的方程列方程组得

$$\begin{cases} x_1^2-t_Ay_1^2=u_A^2(h(z_1)+m_1+e_1+R_1) \\ x_1^2-t_Ay_1^2=u_A^2(h(z_l)+m_l+e_l+R_l) \end{cases}$$

从方程组看出,一共有 l 个方程,却有 $l+1$ 个未知数,因而无法从该方程组中解出 u_A^2 以及 R_i,故利用多组有效签名也无法获得用户密钥.

4) 即使攻击者知道了消息 m 的一组有效签名 (x,y,z),由方程 $x^2-t_Ay^2=u_A^2(h(z)+m+e+R)$ 知,若攻击者想知道其他消息,必须面对因式分解问题,正是因为攻击者无法解出 u_A^2,则不会泄露以前的消息,故本方案具有前向安全性.

5) 当用户 A 与 B 发生争执时,可以在不泄露双方密钥的情况下向可信的第三方 TC 验证签名的有效性.TC 首先获取用户 A 所公开的 T 值,以及 x、y 和 z 值.首先 TC 任意选取 r_1,并计算 $T_1=T+r_1P_B$,并将 T_1 传送给 B, B 计算 $T_2=u_A^2T_1$,并将 T_2 传给 TC,那么 TC 计算 $P_R=T_2-r_1P$.为防止 B 未使用其私钥,TC 任意选取 r_2,并计算 $T_3=P_R+r_2P$,并将 T_3 传送给 B, B 计算 $T_4=k_BT_3$,并将 T_4 传给 TC,那么 TC 验证 $P_R=T_4-r_2P_B$.若等式成立,则 P_R 是正确值.下面按照类似步骤验证 A 的签名是否正确.首先 TC 计算 $P_1=(x^2-t_Ay^2)P_A-h(z)P-P_R$,任意选取 s_1,将 P_1+s_1P 发送给 B,然后 B 计算 $P_2=k_B(P_1+s_1P)$,并将 P_2 发给 TC,TC 计算 $P_3=P_2-s_1P_B$,则 $P_3=P_2-s_1P_B=k_BP_1=(m+e)P_B=V_3$.同理,为防止 B 未使用私钥,TC 选取 s_2,计算 $P_4=P_3+s_2P_B$,并将 P_4 传送给 B, B 计算 $P_5=u_B^2P_4=P_1+s_2P$,并将 P_5 传给 TC,那么 TC 验证 $P_1=T_5-s_2P$.若等式成立,则 P_3 是正确值.由此 TC 可以计算 $m=z-(P_3)_x=z-(V_3)_x$ 并进行验证.

6) 若用户 B 想由方程 $(m+e)P=(x^2-t_Ay^2)P_A-h(z)P-P_R$ 直接伪造用户 A 的签名,固定 m,可计算得 z,再固定 x 或 y,用户 B 将面临 $ECDLP$ 问题及平方剩余问题.若固定 x、y 和 m,再求出 z 使得 z 同时满足 $z=m+((m+e)P_B)_x$ 和 $h(z)P=C$ (C 为常数)这两个方程,但是这更加困难.因此本

方案可以抵抗伪造攻击.

7) 若攻击者令 $\tilde{x}=tx,\tilde{y}=ty,\tilde{z}=z$,则 $\tilde{x}^2-t_A\tilde{y}^2=t^2(x^2-t_Ay^2)=t^2u_A^2(m+e+h(z)+R)$,要从这个等式中求出 m,攻击者将面对因式分解问题,同时还将面对求解单向函数的逆问题.

若令 $\tilde{x}=x,\tilde{y}=y-1,\tilde{z}=z$,则 $\tilde{x}^2-t_A\tilde{y}^2=x^2-t_Ay^2+2t_Ay-t_A,(\tilde{x}^2-t_A\tilde{y}^2)P_A-h(\tilde{z})P-P_R=(m+e)P-2t_AyP_A-t_AP_A=(\tilde{m}+\tilde{e})P$,同样攻击者将面对 ECDLP 问题和求解单向函数的逆问题.

4 结论

通过上一节的安全性分析,我们可以看出,本文所提出的这种新的具备消息自动恢复特性的数字签名方案是建立在 ECDLP 和平方剩余问题之上的,并且该方案可以抵抗多种攻击,具有前向安全性,在第三方仲裁时也无需泄露用户密钥.

参考文献:

[1] K. Nyberg, A. R. Rueppel, Message recovery for signature schemes based on the discrete logarithm problem [A]. Advances in Cryptoolgy-Eurocrypt '94, LNCS 950, Springer, Berlin, 1994, 175-190.

[2] 李子臣,杨义先.具有消息恢复的数字签名方案[J].电子学报,(1):2000,125-126.

[3] 卢建朱,陈火炎.具有消息恢复的数字签名方案及其安全性[J].小型微型计算机系统,2003,(4)695-697.

[4] 武 丹,李善庆.具有消息恢复的数字签名方案的一个注记[J].浙江大学学报(理学版),2004(3),156-158.

[5] S.F. Tseng, M.S. Hwang, Digital signature with message recovery and its variant based on elliptic curve discrete logarithm problem[J]. Computer Standards & Computation, 136(2003), 203-214.

[6] Z. Shao, Improvement of digital signature with message recovery and its variant based on elliptic curve discrete logarithm problem[J]. Computer Standards & Interfaces, 27(2004), 61-69.

New Message Recovery Signature Scheme Based on Elliptic Curve

LIU Xin[1], LONG Kun[2], KAN Bao-yuan[1]

(1. School of Math Science and Computer Technology, Central South University, Changsha 410075; 2. Nanchang Univ., Nanchang 330000, China)

Abstract: Based on both ECDLP and quadratic residue problem, in this paper, we present a new signature scheme with message recovery. We also analyze the security of the new scheme and conclude that the scheme satisfies forward security. In a case of dispute, both the sender and the receiver can convince arbiters whether the signature is valid or not without revealing their secret keys.

Key words: digital signature; elliptic curve; message recover; zero-knowledge proof