

新的基于双难题的带有消息恢复的签名方案

梁钰敏¹, 曹天杰^{1,2}

(1 中国矿业大学 计算机科学与技术学院, 江苏 徐州 221116;

2 中国科学院研究生院 信息安全国家重点实验室, 北京 100049)

摘 要: 为增强安全性, 基于双难题的签名方案相继被提出, 如基于离散对数和素因子分解问题的签名方案, 其安全目标是只要一个难题未被攻破, 方案就是安全. 分析表明: 如果因子分解问题可解, 杨刚和李艳俊提出的基于双难题的方案(YL)将被攻破; 如果离散对数问题可解, LI 和 CHEN 的方案(LC)不能抵抗伪造攻击. 文中提出一种新的签名方案, 该方案是真正同时基于双难题的, 并能将消息恢复. 通过分析, 与其它方案相比, 更加高效.

关键词: 签名; 因子分解; 离散对数; 二次剩余; 伪造攻击; 消息恢复

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)09-0175-04

A New Signature Scheme with Message Recovery Based on Two Hard Problems

LIANG Yu-min¹, CAO Tian-jie^{1,2}

(1 School of Computer Science and Technology, China University of Mining and Technology,

Xuzhou 221116, China; 2 State Key Laboratory of Information Security, Graduate School

of the Chinese Academy of Sciences, Beijing 100049, China)

Abstract: To enhance the security, many signature schemes were designed based on two hard problems, such as factoring and discrete logarithm. The major goal of these schemes is that they cannot be broken if both problems cannot be solved simultaneously. However, — this paper shows that YL scheme can be broken if the factoring problem is solved, LC scheme is insecure against forgery if the discrete logarithm problem is solved. A new signature scheme is proposed that is really based on two hard problems simultaneously, which can also make the message recovered. Comparing with other schemes, this scheme is more efficient.

Key words: signature; factorization; discrete logarithms; quadratic residue; forgery attack; message recovery

1 引言

数字签名广泛应用于电子商务, 是实现认证、不可否认、数据完整性的有效工具, 其本质的安全属性是不可伪造性. 通常, 签名方案的安全性是建立在一个公认的数学难题的基础上的, 如果这个难题被攻破, 攻击者就可以伪造签名. 因此, 增强数字签名方案安全性的一种途径是构造基于多个难题的数字签名方案, 目标是只要其中一个难题未被攻破, 方案就

是安全的. 由于多个数学难题全部被攻破的概率远小于一个难题被攻破的概率, 因此基于多个难题的签名方案比基于一个难题的方案具有更高的安全性.

文献[1]首先提出了基于离散对数和因子分解难题的密钥分发算法, 文献[2,3]提出了基于双难题的签名方案. 之后, 基于双难题的签名方案不断被提出并被分析改进. 文献[4]设计出一种新的改进方案 YL 签名方案. 欧海文等人(OYYD), Li 等人指出^[3]

存在伪造攻击,并提出了修改方案 OYYD1 方案^[5], LC 方案^[6],此外,欧海文等人还结合 Nyberg-Rupple 方案^[7]和 RSA(Rivest-Shamir-Adleman,公钥加密算法)算法提出了一个基于两个困难问题的带有消息恢复的 OYYD2 方案^[5]. 本文指出 YL 方案^[4]的安全性只是建立在因子分解难题之上. 一旦大数能够因子分解,则存在伪造攻击. LC 方案^[6]在离散对数问题可解的情况下,存在伪造攻击. 目前,基于双难题的 OYYD2 方案^[5]和 WLC1/WLC2 方案^[8]没有发现安全缺陷,但这些方案所需计算量过大. 本文基于离散对数和求二次剩余的平方根问题设计了一个带消息恢复的签名方案,与 OYYD, WLC1 和 WLC2 方案相比,本文的方案具有更小的计算量.

2 基于双难题签名方案的密码分析

2.1 YL 签名方案的密码分析

YL 的签名方案描述如下: p 为一个大素数,且 $p-1$ 有两个大的素因子 p_1 和 q_1 , $n=p_1q_1$, 显然 $n \mid (p-1)$. 设 g 为有限域 $GF(p)$ 中阶为 n 的元素, 设 $H(x)$ 是一个安全的单向哈希函数: $H(x) = e_1, e_2, \dots, e_t, e_i \in \{0, 1\}, i=1, 2, \dots, t$. 参数 p, n, g 和 $H(x)$ 公开, p_1, q_1 秘密保存. 用户 A 选取 $x \in [1, n]$, 计算 $y = g^{x^2} \bmod p$. 选取 $u \in [1, n]$, 计算 l , 使得 $lu^2 = 1 \bmod n$, 计算 $z = g^l \bmod p$. 然后随机选取 $u_1, u_2, \dots, u_t$, 这里 $u_i \in [1, n], (i=1, 2, \dots, n)$, 计算 l_i , 使得:

$$l_i u_i^2 = 1 \bmod n$$

用户 A 的私钥是 $(x, u, u_1, u_2, \dots, u_t)$, 公钥是 $(y, z, l_1, l_2, \dots, l_t)$. 对于任一消息 m , 用户 A 进行如下计算: 随机选取 $k \in [1, n]$, 满足 $\gcd(k, n) = 1$, 则 $r = g^{k^2} \bmod p$ ($r \neq 1$). 用户 A 用私钥中的 x, u , 随机数 k 和明文 m 计算:

$$s_1 = u(km + xr) \bmod n$$

$$H(s_1) = (e_1, e_2, \dots, e_t)$$

$$s_2 = (kr - mx) \prod_{i=1}^t u_i^{e_i} \bmod n$$

其中 $e_i \in \{0, 1\}$, (r, s_1, s_2) 即为明文 m 的签名. 当接收者收到 (r, s_1, s_2) 后, 计算:

$$H(s_1) = (e_1, e_2, \dots, e_t)$$

$$v_1 = s_1^2 \bmod n$$

$$v_2 = s_2^2 \prod_{i=1}^t l_i^{e_i} \bmod n$$

将 v_1, v_2 代入:

$$z^{v_1} g^{v_2} \equiv (yr)^{m^2+r^2} \bmod p$$

检验是否成立, 若成立, 则 (r, s_1, s_2) 为消息 m 的签名.

下面证明 YL 签名方案的安全性只是建立在因子分解难题之上. 设 (r, s_1, s_2) 为明文 m 的签名, 在因子分解问题可解的情况下, 能够构造出对明文 m' ($m' \neq m$) 的签名 (r, s'_1, s'_2) . 由于 $n = p_1 q_1$, 模 n 有 $(p_1-1)(q_1-1)/4$ 个二次剩余, 每一个二次剩余有 4 个平方根. 因此, 不妨设 $(m'^2 + r^2)(m^2 + r^2)^{-1}$ 是模 n 的二次剩余 (如果不是二次剩余, 则选择另外的 $m' \neq m$). 在可以分解 n 的因子的情况下, 二次剩余问题容易求解. 因此能够计算出 w 使得 w 满足:

$$w^2 = (m'^2 + r^2)(m^2 + r^2)^{-1} \bmod n$$

计算:

$$s'_1 = ws_1$$

$$H(s'_1) = (e'_1, e'_2, \dots, e'_t)$$

$$v_2 = s_2^2 \prod_{i=1}^t l_i^{e_i} \bmod n$$

$$H(s'_1) = (e'_1, e'_2, \dots, e'_t)$$

计算 s'_2 使得 s'_2 满足:

$$s'^2_2 \prod_{i=1}^t l_i^{e'_i} = w^2 v_2 \bmod n,$$

这里 s'_2 是有解的, 如:

$$s'_2 = ws_2 \prod_{i=1}^t u_i^{e'_i - e_i} \bmod n$$

是 4 个解中的一个. 验证 (r, s'_1, s'_2) 为明文 m' 的签名, 由于 (r, s_1, s_2) 为明文 m 的签名, 计算:

$$H(s'_1) = (e'_1, e'_2, \dots, e'_t)$$

$$v_1 = s_1^2 \bmod n$$

$$v_2 = s_2^2 \prod_{i=1}^t l_i^{e_i} \bmod n$$

(r, v_1, v_2, m) 满足签名验证公式:

$$z^{v_1} g^{v_2} \equiv (yr)^{m^2+r^2} \bmod p$$

计算:

$$H(s'_1) = (e'_1, e'_2, \dots, e'_t)$$

$$v'_1 = s'^2_1 = (ws_1)^2 = w^2 v_1 \bmod n$$

$$v'_2 = s'^2_2 \prod_{i=1}^t l_i^{e'_i} = w^2 v_2 \bmod n$$

则可证:

$$\begin{aligned} z^{v'_1} g^{v'_2} &\equiv z^{w^2 v_1} g^{w^2 v_2} \equiv (z^{v_1} g^{v_2})^{w^2} \equiv ((yr)^{m^2+r^2})^{w^2} \\ &\equiv (yr)^{(m^2+r^2)w^2} \equiv (yr)^{m'^2+r^2} \bmod p \end{aligned}$$

于是签名验证公式成立, (r, s'_1, s'_2) 为明文 m' 的签名. 由以上分析可见, YL 签名方案的安全性只是建立在因子分解难题之上. 一旦 n 能够因子分解,

此方案则存在伪造攻击.

2.2 LC 签名方案的密码分析

LC 签名方案描述如下: p 为一个素数, 且 $p-1$ 有两个大的素因子 p_1 和 q_1 , $n=p_1q_1$. 设 g 为有限域 $GF(p)$ 中阶为 n 的元素, 公开 p, n, g . 用户 A 选取 $x \in [1, n]$ 使得 $\gcd(x, p-1)=1$, 对应的公钥: $y=g^x \bmod p$, $z=g^{x^2} \bmod p$. 对 m 签名, A 执行: 选择 $t \in Z_n$ 使得 $\gcd(t, p-1)=1$, 计算 $k=g^{t^2} \bmod p$, $r=g^k \bmod p$ 且保证 $r \neq 1$. f 是哈希函数(hash). 计算 s 满足 $f(m, r)=(xr+ts) \bmod (p-1)$. 元组 (r, s) 是消息 m 的签名, 签名验证公式为:

$$r^{s^2} y^{2f(m,r)r} = g^{f^2(m,r)} z^{r^2} \bmod p$$

在离散对数问题可解的情况下, LC 方案存在伪造攻击. 设离散对数问题可解, 由公钥 y 可计算出 x , 对任意的 m, t , 且 $\gcd(t, p-1)=1$, 计算:

$$r=g^{t^2} \bmod p$$

$$s=t^{-1}(f(m, r)-xr) \bmod n$$

则有:

$$\begin{aligned} r^{s^2} y^{2f(m,r)r} &= (g^{t^2})^{s^2} (g^x)^{2f(m,r)r} = g^{f^2(m,r)+x^2r^2} \\ &= g^{f^2(m,r)} z^{r^2} \bmod p \end{aligned}$$

显然这样构造的元组 (r, s) 是消息 m 的签名.

3 新的基于双难题的带消息恢复的签名方案

Nyberg 和 Ruppel 基于离散对数问题提出一个带有消息恢复的签名方案, 称为 Nyberg-Ruppel 方案, 本文将该方案求二次平方剩余的问题结合, 提出一个基于离散对数和求二次剩余的平方根问题的带消息恢复的签名方案, 该方案对 Nyberg 和 Ruppel 提出的带消息恢复的签名方案进行了一些改进. 具有两个优点: 较小的计算量, 能够消息恢复.

3.1 签名过程

用户 A 选择自己的一个大素数 $p=4p_1q_1+1$ 和剩余类环 $Z_p=Z/(P)$ 中一个阶为 $n=p_1q_1$ 的元素 g , 其中 $p_1=2p_2+l$, $q_1=2q_2+l$, 并且 p_1, q_1, p_2, q_2 都是素数. 选取 $x \in Z_n$, 使得 $\gcd(x, n)=1$, 计算 $y=g^x \bmod p$. x 和 y 分别为私钥和公钥. 对 m 签名时, A 执行: 首先选择 $t \in Z_n$ 使得 $\gcd(t, p-1)=1$, 计算

$$m_1=h(g^t \bmod n, m) \bmod n$$

将 m 和 m_1 连接起来记为 m' , 即 $m'=m \parallel m_1$, 若 $m' > n$, 则将其分成一系列的数据单元 m_i' ($1 \leq i \leq k$), 且 $0 < m_i' \leq n$, 然后对每一个单元进行签名. 这里假设 $0 < m' \leq n$, 然后计算:

$$r=m'g^{-t} \bmod p.$$

计算 s 使得:

$$s^2=(t-xr) \bmod n,$$

如果 $t-xr$ 不是模 n 的二次剩余则重新选择 t . (r, s) 即为消息的签名发送给验证者. 验证者收到消息后, 对签名进行验证并恢复出消息, 验证者验证等式:

$$m'=g^{s^2}ry^r \bmod p$$

由于 $m'=m \parallel m_1$, 这样接受者能够得到 m 和 m_1 , 然后验证者检验以下等式是否成立, 以验证恢复出的是否是真是的:

$$m_1=h\left(\frac{m'}{r} \bmod n, m\right) \bmod n$$

若成立则接受签名, 签名对 (r, s) 是有效的, 否则, 可知签名对已被破坏, 恢复出的消息不正确. 消息恢复过程如下:

$$\begin{aligned} g^{s^2}ry^r \bmod p &= g^{t-xr}(g^x)^r \bmod p = rg^{t-xr+x} \bmod p \\ &= rg^t \bmod p = m'g^{-t}g^t \bmod p = m' \bmod p \end{aligned}$$

验证过程为:

$$\begin{aligned} \frac{m'}{r} \bmod n &= \frac{g^{s^2}ry^r}{r} \bmod n = g^{s^2}y^r \bmod n \\ &= g^{s^2}g^x \bmod n = g^{t-xr+x} \bmod n \\ &= g^t \bmod n \end{aligned}$$

3.2 安全性及效率分析

分析该方案的安全性. 假设离散对数问题可解, 则由公钥 y 可以计算出私钥 x . 攻击者可以选取 $t \in Z_n$, 计算 $r=m'g^{-t} \bmod p$. 但攻击者因为不可分解 n , 因此无法计算 s 使得 $s^2=(t-xr) \bmod n$. 假设攻击者具有因子分解的能力, 则攻击者可以计算出素数 p_1, q_1, p_2, q_2 . 攻击者可以选取 $t \in Z_n$, 计算 $r=m'g^{-t} \bmod p$, 但攻击者因为不可求解出 x , 因此无法计算 s 使得 $s^2=t-xr \bmod n$. 由此可知, 除非攻击者可以同时解决因式分解和离散对数问题, 这个方案是安全的. 表 1 对比了以上几个方案.

表 1 各个方案所基于的难题

签名方案	基于的难题
YL 签名方案	因子分解
LC 签名方案	离散对数
本文方案	因子分解和离散对数

考虑算法的计算量. 由于 Nyberg 和 Ruppel 方案在签名与验证过程中避免了逆运算, 注意 $r=m'g^{-t}=m'g^{n-t} \bmod p$, 计算 r 需要一次模 p 幂乘运

算. 在计算 s 使得 $s^2 = t - xr \pmod n$ 时, 如果 $t - xr$ 不是二次剩余, 重新选择 $t_1 = t - 2$, 计算 $r_1 = m' g^{-(t-2)} = rg^2 \pmod p$, 判断 $t_1 - xr_1$ 是否为二次剩余, 若还不是则选择 $t_2 = t_1 - 2$ 等, 这里不需再进行模 p 幂乘运算. 由于 Z_n 中模 n 有 $(p_1 - 1)(q_1 - 1)/4$ 个二次剩余, 因此, 平均来说计算签名只需要 1 次模 p 的幂乘运算. 验证时, 计算:

$$m' = g^s r y^r \pmod p$$

这里需要 2 次幂乘运算.

与其他基于双难题的签名方案比较. OYYD2 方案签名/验证各需要 2 次/3 次幂乘运算[14]. 文献[10]提出了两个基于双难题的签名方案 WLC1 和 WLC2 方案, 这两个签名方案在签名时都涉及到乘法逆运算, 乘法逆运算的计算代价与幂乘运算相当, 此外, 第一个方案签名/验证各需要 2 次/5 次幂乘运算, 第二个方案签名/验证各需要 1 次/4 次幂乘运算. 表 2 对比了几个方案中的主要计算量, 由此可知与目前已知的没有发现安全缺陷的方案相比, 本方案是高效的.

表 2 各个方案所需的主要运算

签名方案	签名所需幂乘 运算次数	验证所需幂乘 运算次数	是否有乘法 逆运算
OYYD2 签名方案	2	3	是
WLC1	2	5	是
WLC2	1	4	是
本文方案	1	2	否

4 结束语

本文分析了基于离散对数和素因子分解困难问题的两个数字签名方案, 指出了这些方案不能够依赖于两个难题, 存在安全上的缺陷. 同时提出了一个高效的基于双难题且具有消息恢复性质的签名方

案, 与其它方案相比具有更小的计算量.

参考文献:

- [1] McCurley Kevin S. A key distribution system equivalent to factoring[J]. Cryptology, 1988, 1(2): 95-105.
- [2] Harn L. Public-key cryptosystem design based on factoring and discrete logarithms[J]. IEE Proceedings-Computers and Digital Techniques, 1994, 141(3): 193-195.
- [3] He J, Kiesler T. Enhancing the security of ElGamal's signature scheme[J]. IEE Proceedings-Computers and Digital Techniques, 1994, 141(4): 249-252.
- [4] 杨刚, 李艳俊. 基于离散对数和因子分解的签名方案[J]. 北京理工大学学报, 2004, 24(4): 324-326.
- [5] 欧海文, 叶顶锋, 杨君辉, 等. 关于同时基于因子分解与离散对数问题的签名体制[J]. 通信学报, 2004, 25(10): 143-147.
- [6] LI Chun-hui, Chen Yi-hong. Enhancing the Security of He-Kiesler Signature Schemes[J]. Journal of Beijing Institute of Technology, 2003, 12(3): 326-328.
- [7] Nyberg K, Rueppel R A. Message recovery for signature schemes based on the discrete logarithm[C]// Advances in Cryptology, EUROCRYPT'94 springer Verlag, 1994: 175-190.
- [8] WANG Ching-te, LIN Chu-hsing, CHANG Chin-chen. Signature schemes based on two hard problems simultaneously[C]// Proceedings of the 17th International Conference on Advanced Information Networking and Applications. [S. L.]: IEEE, 2003: 557-560.

作者简介:

梁钰敏 女, (1991—), 硕士研究生. 研究方向为密码学与网络安全.

曹天杰 男, (1967—), 博士生导师, 教授. 研究方向为密码协议、匿名与隐私、网络安全.

(上接第 174 页)

- [5] 孙妍, 陶正苏, 陈德福. 基于无线传感器网络的室内精确定位算法[J]. 传感器与微系统, 2009, 28(5): 99-102.
- [6] 温立, 胡波. 无线传感器网络中一种改进的分布式加权多维尺度定位算法[J]. 电路与系统学报, 2009, 14(4): 1-7.
- [7] 崔逊学, 刘建军, 樊秀梅. 传感器网络中一种分布式无锚节点定位算法[J]. 计算机研究与发展, 2009, 46(3): 425-433.
- [8] 叶小岭, 王伟, 张颖超, 等. 无线传感器网络中一种改

进的 DV-Hop 定位算法[J]. 计算机测量与控制, 2010, 18(2): 488-490.

- [9] 余义斌, 曹长修, 李昌兵. 基于权重重心法的传感器网络节点定位[J]. 计算机仿真, 2007, 24(6): 296-300.
- [10] 解慧英. 无线传感器网络中一种改进的 DV-Hop 定位算法[D]. 武汉: 武汉科技大学, 2008.

作者简介:

张丽虹 女, (1976—), 硕士, 讲师. 研究方向为计算机网络、信息安全、无线传感网络.