文章编号:1001 - 9081(2007)10 - 2459 - 02

基于离散对数和因子分解具有消息恢复的签名方案

袁喜凤,孙艳蕊,孙金青,杨迎辉
(东北大学 理学院,沈阳 110004)
(yanruisun@126.com)

摘 要:基于双难题具有消息恢复的签名方案研究甚少,仅有的一些方案都存在计算效率和传输效率过低的问题。由此提出了一个新的同时基于离散对数和大整数分解两种困难问题的具有消息恢复的签名方案,并对其进行安全性分析及效率分析。其安全性要比基于一个难题的数字签名方案好,并且该方案比已有的基于双难题的具有消息恢复签名方案效率要高。

关键词:数字签名;消息恢复;离散对数;因子分解
中图分类号: TP309 **文献标志码**:A

Signature scheme with message recovery based on discrete logarithms and factoring

YUAN Xi-feng, SUN Yan-rui, SUN Jin-qing, YANG Ying-hui
(*College of Science, Northeastern University, Shenyang Liaoning* 110004, *China*)

Abstract: Recently, there is little research about digital schemes with message recovery based on double hard problems. The computational efficiency and transmission efficiency of the existing schemes is too low. Hence, in the paper, a new digital signature scheme with message recovery was given, in which the security was based on the difficulties of computing discrete logarithms and factoring. And its security analysis and efficiency analysis were also given. The security of the scheme is consequently better than those of the signature schemes which are based on the difficulty of a single problem. And the scheme proposed has higher efficiency than the schemes which exist now.

Key words: digital signature; message recovery; discrete logarithm; factoring

0 引言

具有消息恢复的数字签名是指用户 A 先对消息 m 进行签名,然后将签名数据发送所有的目的用户,任何一个用户接收到签名数据都可以恢复出相应的消息 m。研究如何缩小消息 m 及其签名 s 的总长度是近几年的一个热门课题,其中一个有效的方法就是直接缩短消息 m 及其签名 s 的总长度,该方法的基本思想源于文献[1]中设计的签名方案的消息恢复功能。之后一系列具有消息恢复的签名方案被相继提出[3-5]。但一般来说,这些方案都是基于一个公认的数学难题,如果这个难题被攻破,相应的方案就不安全了。随着科学技术的发展和密码学的不断进步,这些相应的难题随时都有可能被攻破。因此,一些密码学家提出将密码系统建立在多个难题的困难性的基础上。因为,多个数学难题同时被攻破的概率远远小于一个难题被攻破的概率。自 1988 年文献[2]提出第一个同时基于离散对数和因子分解两个数学难题的密钥分配方案之后,一系列基于双难题的签名方案被相继提出[6-9]。但是,近几年对基于双难题具有消息恢复的签名方案研究甚少,2000 年,文献[8]提出了一个基于离散对数和因子分解两种难题的具有消息恢复的签名方案。2004 年,文献[9]将已知的成熟的基于离散对数的密码体制与基于因子分解的密码体制复合起来,设计了一个同时基于这两个难题的签名方案。经分析发现,上述两个签名方案都存在计算效率和传输效率较低的问题。由此本文提出了一个同时基于离散对数和大整数分解两种困难问题的具有消息恢复的签名方案,并对其进行了安全性和效率分析。

1 新的基于双难题的具有消息恢复的签名方案

基于双难题的签名方案是将一个签名体制建立在两个数学难题的困难性基础上(如本文方案是建立在离散对数和因子分解两难题的困难性基础上),只有这两个难题同时被攻破时,该签名方案才能被攻破。

本节根据离散对数问题和大整数分解问题建立了一个具有消息恢复的签名方案,该方案包括 4 个过程:系统初始化、密钥的生成过程、签名过程和验证过程(消息恢复过程)。

系统初始化

1) 设 p 是一个大素数,$p = 2p_1q_1 + 1$,其中 p_1,p_2 都是素数. 这些参数由一个社会信任的公证机构生成。这些参数生成后 p 公开,p_1,p_2 保密;

2) 公证机构选取 $g \in GF(P)$,令 $n = p_1q_1$,g 的阶为 n,G 是由 g 生成的循环群。将 n,g 公开;

3) 公证机构选取两个抵抗碰撞的单向杂凑函数:$h: z_n \to z_n$,$h_1: \{0,1\}^* \to \{0,1\}^{k_2}$,其中 $k_2 = \frac{1}{2}\lfloor \log n \rfloor$,为一正整数。将 h,h_1 公开。

收稿日期:2007 - 04 - 19;**修回日期**:2007 - 06 - 21。 **基金项目**:国家自然科学基金资助项目(60475036)。

作者简介:袁喜凤(1982 -),女,河南周口人,硕士研究生,主要研究方向:密码学与信息安全; 孙艳蕊(1965 -),女,河北丰南人,教授,博士,主要研究方向:网络可靠性计算、信息安全; 孙金青(1982 -),女,河北邢台人,硕士研究生,主要研究方向:信息安全; 杨迎辉(1982 -),男,河南洛阳人,硕士研究生,主要研究方向:信息安全。

密钥的生成

1）对与每个签名用户，随机选取一个秘密密钥 $x \in z_n$；$1 < x < \frac{n}{2}$；

2）计算 $y = g^{x^2} (\mathrm{mod}\ p)$，其中 $x^2 \in z_n$；

3）用户将 (n,y) 作为其公钥公开，(x,p_1,q_1) 作为其私钥秘密保存。

签名生成过程

假设用户 A 先对消息 $m \in \{0,1\}^{k_1}$ 进行签名（其中 $k_1 + k_2 = \lfloor \log n \rfloor$，当消息 m 较大时，可以采用递推的方式构造消息分块签名，把前一个参数作为后一个参数的输入，这样恢复消息时只需进行递推运算就可以一个一个地恢复出全部消息了）。然后将签名数据发送所有的目的用户，任一用户接收到签名数据都可以恢复出相应的消息 m。

用户 A 对消息 $m \in \{0,1\}^{k_1}$ 的签名过程如下：

1）随机选取一个整数 R，计算：$m_1 = h_1(g^{R^2} \mathrm{mod}\ n, m) (\mathrm{mod}\ n)$；

2）把 m_1 串接到消息 m，所得的信息记为 $m' = m \| m_1$，计算 $r = (m' - g^{R^2}) (\mathrm{mod}\ p)$；

3）计算 $R = (s + h(r))x (\mathrm{mod}\ n)$，此为数字签名方程；

4）将 (s,r) 作为消息 m 的签名传送给 B；

验证过程（消息恢复过程）

1）接收者利用签名者的公钥 y 恢复出消息 $m' = r + y^{(s+h(r))^2} \mathrm{mod}\ n$，$m'$ 中含有 m_1 和 m；

2）接收者计算 $\lfloor m' \rfloor_{k_2} = h_1((m' - r) \mathrm{mod}\ n, \lceil m' \rceil^{k_1}) (\mathrm{mod}\ n)$，若等式成立，则消息恢复正确，否则不正确，其中 $\lfloor m' \rfloor_{k_2}$ 为 m' 的低 k_2 位，$\lceil m' \rceil^{k_1}$ 为 m' 的高 k_1 位。

根据签名 $r = (m' - g^{R^2}) (\mathrm{mod}\ p)$，$R = (s + h(r))x (\mathrm{mod}\ n)$ 及签名者公钥 y，任意签名接收者都可根据验证过程第 1 步的计算式 $m' = r + y^{(s+h(r))^2} (\mathrm{mod}\ n)$ 恢复 m'。从 m' 中恢复 m 和 m_1，满足 $\lfloor m' \rfloor_{k_2} = h_1((m' - r) \mathrm{mod}\ n, \lceil m' \rceil^{k_1}) (\mathrm{mod}\ n)$。下面给出证明：

因为：

$$r + y^{(s+h(r))^2} (\mathrm{mod}\ n) = r + g^{x2(s+h(r))^2} (\mathrm{mod}\ n) = r + g^{((s+h(r))x)^2} (\mathrm{mod}\ n) = r + g^{R^2} (\mathrm{mod}\ n) = m' (mod\ n)$$

由此任何接收者可恢复 m'。又由 m' 的组成可恢复出 m 和 m_1，且由签名过程（1）、（2），满足 $\lfloor m' \rfloor_{k_2} = h_1((m' - r) \mathrm{mod}\ n, \lceil m' \rceil^{k_1}) (\mathrm{mod}\ n)$。

2 安全性分析及效率分析

2.1 安全性分析

1）攻击者欲利用签名者 A 的公钥 y 和 $y = g^{x^2} (\mathrm{mod}\ p)$，求出私钥 x，须先求解离散对数问题求得 x^2 的值，然后根据模 n 的因子解二次同余式解得 x，即同时面临大整数因子分解和离散对数两个数学难题。

2）对消息恢复方程 $m' = r + y^{(s+h(r))^2} (\mathrm{mod}\ n)$ 的代换攻击无效，对任意的消息 m'，攻击者任取 r，要从消息恢复方程 $m' = r + y^{(s+h(r))^2} (\mathrm{mod}\ n)$ 中解出 s，必须先解离散对数，再用模 n 的因子解二次同余，即同时面临大整数分解问题。若攻击者任取 s，从消息恢复方程中解出 r，比同时求解离散对数和大整数分解两种困难问题还要难。

3）即使攻击者拥有 t 组有效签名，仍不能求出另外的签名，因为这些消息恢复方程 $m_i' = r_i + y^{(s_i+h(r_i))^2} (\mathrm{mod}\ n) (i = 1,\cdots,t)$ 是独立无关的。

4）假定离散对数问题已经被破解，攻击者从公钥 $y = g^{x^2} (\mathrm{mod}\ p)$ 中可以求出 x^2 的值，利用 (m',r) 以及签名过程2）中的 $r = (m' - g^{R^2}) (\mathrm{mod}\ p)$，可以解出 R^2 的值，但是欲从签名方程 $R = (s + h(r))x (\mathrm{mod}\ n)$ 中求出 s，须用模 n 的因子解二次同余，即面临大整数分即面临大整数分解问题。假定容易计算因子分解，在离散对数问题没有被破解的情况下，该方案是一个基于离散对数难题的签名方案。

2.2 效率分析

众所周知，在循环群中，指数运算、求逆运算以及模乘运算是比较费时的，下面分析比较这几项运算所用的时间。假设 $T_{\exp}$ 是计算指数函数所需要的时间，T_{inv} 为计算逆元素所需时间，T_{mod} 为计算模乘所需的时间，$pk.l$ 为公钥长度，$sk.l$ 为私钥长度，$sig.l$ 为签名长度，sig_{tim} 为签名时间复杂度，val_{tim} 为验证时间复杂度。将本文方案的密钥长度、签名长度及时间复杂度与文献[8]、[9] 进行比较，见表 1。

表 1 三种方案的密钥长度、签名长度及时间复杂度比较

运算	本文方案	文献[8]方案	文献[9]的方案
pk,l	$[\log n] + [\log p]$	$\lceil \log n \rceil [\log n] + [\log p]$	$2[\log n] + [\log p]$
$sk.l$	$2[\log n]$	$(\lceil \log n \rceil + 1)[\log n]$	$3[\log n]$
$sig.l$	$[\log n] + [\log p]$	$2[\log n] + [\log p]$	$[\log n] + [\log p]$
sig_{tim}	$T_{\exp} + 2T_{\mathrm{mod}} + T_{\mathrm{inv}}$	$[\log n](T_{\exp} + T_{\mathrm{mod}}) + 3T_{\mathrm{mod}} + 2T_{\mathrm{inv}}$	$2T_{\exp} + 2T_{\mathrm{mod}} + T_{\mathrm{inv}}$
val_{tim}	$T_{\exp} + T_{\mathrm{mod}}$	$[\log n](T_{\exp} + T_{\mathrm{mod}}) + 4T_{\mathrm{mod}} + 2T_{\mathrm{inv}}$	$2T_{\exp} + (e + 2)T_{\mathrm{mod}}$

从表 1 中可以看出，本文中的方案与文献[8]、[9]中方案相比具有签名密钥短，计算时间复杂度小等优点。因此本文中方案是一个安全性和效率都较高的方案。

3 结语

本文提出了一个新的同时基于离散对数和大整数分解两种困难问题的具有消息恢复的签名方案，通过对其进行安全性分析，其安全性比基于一个困难问题的签名方案要好。并且，将本文方案与文献[8]、[9]中的签名方案进行比较，本文中的方案具有签名密钥短，计算时间复杂度小等优点。减小基于双难题签名方案的复杂度，以及如何构造可证明安全的签名方案将是今后讨论的内容。

参考文献：

[1] NYBERG K, RUEPPEL R A. Message recovery for signature schemes based on the Discrete logarithm [J]. Designs, Codes and Cryptogrphy, 1996, 7(1-2):61-81.

[2] MOCURLEYK C. A key distribution system equivalent to factoring [J]. Cryptology, 1988, 1(2): 95-106. （下转第 2463 页）

品迅速地作出判断以实现流水化作业。为此,可以通过下述方案优化性能。

把 N 维空间内的向量 $\boldsymbol{c}_o$ 视为 N 个数字,把它分为每组 k 个数字的 m 组数字。在嵌入水印信息时,选取的参考模板 w_r 维数为 k,对 m 组数字都进行嵌入水印的操作。同样,根据概率的知识,在检测时,利用由 N 维向量 $\boldsymbol{c}$ 拆分成的 m 组数字取平均值而得到的 k 维向量 $\boldsymbol{c}'$,同样与参考模板 w_r 满足检测要求。这样,N 次乘法计算便减为 k 次乘法计算,从而达到了优化了性能的目的。

4　典型应用

由于本模型具有的优秀性质,使得它可以被应用在多种场合,下面描述两种应用方案。

4.1　水印商标

在超市中,为了能够迅速有效地检测顾客手中的产品的信息,例如这种产品是什么,现行的方案是依赖条形码技术。条形码技术作为一种成熟的方便识别的技术,有着许多优良的特性,但也有它自身的不足之处。例如在漂亮的产品包装袋上印着黑白相间的条形码,本身就非常影响产品的外观。应用本模型,很容易做到只要检测包装的商标,就可以识别出产品的多种特性。

每种产品的商标,可以视为一幅 $L \times W$ 的一幅真彩色位图,每个像素的颜色在 RGB 面上对应 3 个 0 ~ 255 中的某个数值。这样这件商品的商标可以被抽象为一个 $L \times W \times 3$ 维的向量。在商标的印制过程中,可以将各种特征信息,例如自身的特征代码、型号、生产地等信息。作为水印信息,采用本文介绍的算法,嵌入到商标中去。由于对商标图像做的是微调操作,商品的商标从外观上并无变化。在超市收银台,可以通过采集商标的视觉信息,利用本文介绍的水印检测算法检测出包含在商标背后的各种信息。而且由于算法具有良好的鲁棒性,因此诸如商标的污损并不会影响检测结果。

4.2　实验结果

实验中,采用的原始商标是一幅分辨率为 128 × 80 的 256 色灰度图像,即一个维数为 128 × 80 的向量。需要嵌入的水印信息是长度为 8 字节的 4 个汉字:“中科信息”。

实验采用上节介绍的算法,每次嵌入 2 比特信息,分 32 次嵌入。算法在 32 次水印信息嵌入的过程中,采用 seed 为 100 ~ 131 的伪随机数发生器产生 32 个参考模板,并对这 32 个 128 × 80 进行归一化操作,使其满足均值为 0,标准差为 1 的均匀分布。当 2 比特信息分别为 00, 01, 10, 11 时,通过调整嵌入强度 α, 使其在相应的参考模板下的检测值分别为 -1.25, -0.75, $+0.75$, $+1.25$。

通过添加水印信息,可以得到如图1、2的测试结果。在外观上,两个商标很难看出差别。

图1　原始商标

图2　水印商标

在检测过程中,当检测值分别在区间 $(-1.5, -1)$, $(-1, -0.5)$, $(0.5, 1)$, $(1, 1.5)$ 时,认为检测到了 00, 01, 10, 11 四种结果。当检测值在区间 $(-0.5, 0.5)$ 时,认为没有检测到水印。

利用上节介绍算法制作的水印检测器,依次用 100, 101, 102,…,131 生成参考模板检测水印信息。可以分 32 次得到 64 比特水印信息,即中科信息四个汉字。

4.3　广告监视

在许多国家和地区,在广播电视中插播广告是敏感的话题。遇到的问题主要包括广告播放时间是否超出了规定的时间,即观众的权益是否受到侵害;各个商家的广告是否被如数播放出来,即商家的权益是否受到侵害。出现这类问题的原因在于,被播放的信息很难被识别出来,没有一个有效的方法来监视广告播放的情况。本文提到的模型能够很好地解决这类问题。为了能监督广播电视播放内容的信息,可以在播放的信息,例如在音频中以水印的形式嵌入播放内容特征信息。这样,通过提取水印的方式,广告的播放情况便可以很容易的被检测出来,从而达到广告监视的目的。

5　结语

经大量的实验,本文介绍的模型和算法,利用数字水印技术,可以较好地解决识别面临的很多难题。作为一种计算机视觉技术,它也非常适合对各种媒体对象快速自动识别和自动监控。同时,该模型凭借它的各种优良特性,使它在媒体信息数字化流行的今天,有着广泛的应用空间。

参考文献:

[1]　申丽珍. 多媒体信息版权保护新技术[J]. 计算机仿真, 2005, 22(8): 73 – 76.

[2]　尹浩, 林闯, 邱锋, 等. 数字水印技术综述[J]. 计算机研究与发展, 2005, 42(7): 1093 – 1099.

[3]　牛夏牧, 赵亮, 黄文军, 等. 利用数字水印技术实现数据库的版权保护[J]. 电子学报, 2003, 31(z1): 2050 ~ 2053 .

[4]　袁占亭, 张秋余, 陈宁. 数字水印及多媒体信息安全[J]. 计算机工程与科学, 2005, 27(7): 49 – 51.

[5]　王艳辉, 王相海. 用于图像认证的数字水印技术综述[J]. 计算机工程与应用, 2007, 43(2): 33 – 37.

[6]　钟磊, 单承赣, 王艳. 基于数字水印的经典图像认证算法分析[J]. 重庆邮电学院学报: 自然科学版, 2006, 18(6): 770 – 773.

(上接第 2460 页)

[3]　MIYAJI A. A message recovery signature scheme equivalent to DSA over elliptic curves [C]// Proceedings of the Asiacrypt's 96, LNCS 1163. Berlin: Springer-Verlag, 1996: 1 – 14.

[4]　ZHANG F, SUSILO W, MU Y. Identity-Based Partial Message Recovery Signatures [C]// LNCS 3570. Berlin: Springer-Verlag, 2005: 45 – 56.

[5]　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, 24(4): 695 – 697.

[6]　SHAO Z. Signature schemes based on factoring and discrete logarithms[J]. IEEE Proceeding Computers and Digital Techniques, 1998, 145(1): 33 – 36.

[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 – 65.

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

[9]　欧海文, 叶顶锋, 杨君辉, 等. 关于同时基于因子分解和离散对数问题的签名体制[J]. 通信学报, 2004, 25(10): 143 – 147.