具有指定接收组(t, n)门限共享验证签名加密方案

李继国[1], 曹珍富[2], 李建中[1]
(1. 哈尔滨工业大学计算机学院, 黑龙江哈尔滨 150001; 2. 上海交通大学计算机系, 上海 200030)

摘 要: 本文提出了一个具有指定接收者验证的签名加密方案. 该方案是数字签名与公钥密码体制的有机集成. 与普通数字签名方案相比, 除了具有认证性、数据完整性外还具有保密性和接收方的隐私性. 然后又利用门限方案构造了一个(t, n)门限共享验证签名加密方案. 与现有的门限共享验证签名加密方案相比具有数据传输安全、通信代价更小、执行效率更高、能够确切地检查出哪个验证者篡改子密钥等特点.

关键词: 数字签名; 共享验证; 签名加密
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2003) 07-1086-03

(t, n) Threshold Shared Verification Signature Encryption Scheme with Specified Receiving Groups

LI Ji-guo[1], CAO Zhen-fu[2]
(1. School of Computer Science & Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China;
2. Department of Computer Science & Technology, Shanghai Jiao Tong University, Shanghai 200030, China)

Abstract: In this paper, first, a signature encryption scheme with specified receiver verification is proposed. The scheme perfectly integrates digital signature scheme with public key cryptography system. Compared with common digital signature scheme, it has authentication, secrecy, data integrity and privacy of the receiver. Then, we use threshold scheme to construct a (t, n) threshold shared verification signature encryption scheme. Compared with proposed threshold shared verification signature encryption scheme, it has more secrecy of data transmission, requires smaller communication cost, performs efficiently and decides exactly which verifier tampers secret shadow etc.

Key words: digital signature; shared verification; signature encryption

1 引言

数字签名是一种实用的认证技术, 随着计算机和网络通信技术的发展, 数字签名技术得到了广泛的应用. 国内外众多的专家学者对数字签名的理论、技术和应用进行了深入的探讨与研究. 人们根据不同的应用提出了诸多的数字签名方案[1~4]. 1996 年, Nyberg 和 Rueppel[1] 提出了具有消息恢复的新型数字签名方案. 他们的方案被认为是数据加密与数字签名密码技术的结合. 在 Nyberg 和 Rueppel 的认证加密方案中, 签名者可以发送签名的密文或密文的签名给指定的接收者, 只有指定的接收者才能恢复和验证签名的密文或密文的签名. 他们也暗示最好使用先签名后加密的密码学原则. 最近, Lin 和 Laih[5], Miyaji[6], 李子臣, 李中献和杨义先[7] 等指出 Nyberg 和 Rueppel[1] 提出的方案是不安全的. 1993 年 L. Harn[4] 提出一个门限共享验证签名方案. Lee 和 Chang[8] 指出 Harn 的方案易受伪造攻击. 1998 年 Hsu 和 Wu[3] 提出的(t, n)门限共享验证签名加密方案只是数据加密与数字签名方案的简单叠加.

本文基于 Nyberg 和 Rueppel 的思想, 提出了一个具有指定接收者的签名加密方案. 它是数据加密和数字签名的有机结合并且能抵抗已有的攻击. 该方案比直接使用加密和数字签名方案[2, 3] 达到同样的目的需要更小的带宽且执行效率更高. 在此基础上, 本文还利用 Shamir[9] 的门限方案构造了具有指定接收者的门限共享验证签名加密方案. 该方案除具有保密性、认证性与完整性外, 还具有门限方案[9, 10] 的优点. 这样做主要是为了分散验证者的权力, 以防签名滥用.

2 一个新型具有指定接收者的签名加密方案

我们的方案分三个阶段, 系统初始化阶段、签名加密阶段和签名加密消息的恢复阶段.

2.1 系统初始化阶段

可信中心 CA 选取两个大素数 p, q 满足 q| p - 1, 随机选取 q 阶生成元 g ∈ Z_p. 用户 U_A 和 U_B 分别随机选取秘密钥 x_A ∈ Z_q^* 和 x_B ∈ Z_q^*, 计算并发送他们的公钥 $y_A = g^{x_A} \bmod p$, y_B =

收稿日期: 2001-12-30; 修回日期: 2002-04-23
基金项目: 国家自然科学基金(No. 60072018); 国家杰出青年科学基金(No. 60225007); 高校博士点专项基金(No. 20020248024)

$g^{x_B} \bmod p$ 给可信中心 CA, CA 公开 p, q, g, y_A 和 y_B.

2.1.2　签名加密阶段

假设用户 U_A 对消息 $M \in Z_p$ 签名并发送给指定的接收者 U_B. 首先用户 U_A 随机选取 $k \in Z_q^*$ 并计算 $v_1 = g^{-k} \bmod p$ 和 $v_2 = y_B^k \bmod p$. 然后计算签名(r, s) 如下:

$$r = Mv_1 g^{-v_2} \bmod p \quad (1)$$

$$s = k - x_A r \bmod q \quad (2)$$

则签名(r, s) 也是签名消息 M 的密文, 因为消息被隐藏在 r 中.

2.1.3　签名加密消息的恢复阶段

接收者 U_B 收到签名(r, s) 后, 首先计算 $vc_1 = g^s y_A^r = g^{x_A + s} = g^k \bmod p$ 和 $v_2 = y_B^k = v^{kx_B} \bmod p$, 然后接收者 U_B 恢复消息 $M = rvc_1 g^{-v_2} \bmod p$ 并由冗余信息验证消息 M 的有效性.

定理 1　如果签名者 U_A 遵循签名加密阶段的步骤, 则指定的接收者 U_B 能够正确地恢复签名消息 M.

2.1.4　安全性分析

(a) 攻击者从用户 U_A 的公钥 y_A 获得秘密钥 x_A 等价于求解离散对数问题. 接收者 U_B 由已知签名对(r, s) 利用式(2) 求秘密钥 x_A, 必须先求出 k, 而由 v_1, v_2 求 k 等价于求解离散对数问题.

(b) 假定攻击者随机选取 $k \in Z_q^*$ 从而由式(1) 可计算出 r, 但由于户 U_A 的秘密钥 x_A 对于攻击者来说是未知的, 故攻击者由式(2) 求 s 是不可能的.

(c) 只有指定接收者 U_B 才能恢复消息. 尽管攻击者能由签名对(r, s) 获得 vc_1, 但攻击者得不到 v_2. 因为他没有接收者 U_B 的秘密钥 x_B, 而由接收者 U_B 的公钥求其秘密钥 x_B 等价于求解离散对数问题, 从而攻击者不能恢复消息 M.

3　具有指定接收组的(t, n) 门限共享验证签名加密方案

该方案分四个阶段, 系统初始化阶段、注册阶段、签名加密阶段和签名加密消息的恢复阶段.

3.1.1　系统初始化阶段(与 2.1 节相同)

3.1.2　注册阶段

令 U_A 是签名者, 组 $G = \{U_1, U_2, \cdots, U_n\}$ 是 n 个验证者的集合. $ID_i \neq 0$ 是 U_i($i = 1, \cdots, n$) 的身份. U_A 随机选取秘密钥 $x_A \in Z_q^*$, 计算并发送他的公钥 $y_A = g^{x_A} \bmod p$ 给 CA, 为了组 G 和 G 的所有验证者注册, CA 随机选取 $x_G \in Z_q^*$ 为组 G 的秘密钥, 其相应的公钥为 $y_G = g^{x_G} \bmod p$. 然后, CA 随机产生 t - 1 次多项式

$$f(x) = x_G + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \bmod q$$

其中 $a_i \in Z_q$($i = 1, 2, \cdots, t-1$), $a_{t-1} \bmod q \neq 0$. 分别计算组 G 中验证者 $U_i \in G$ 的秘密钥与公钥为

$$x_i = f(ID_i) \bmod q, \quad y_i = g^{x_i} \bmod p$$

最后, CA 通过安全信道发送 x_i($i = 1, 2, \cdots, n$) 给 $U_i \in G$ 并且公开所有的公钥 y_G, y_i($i = 1, \cdots, n$).

3.1.3　签名加密阶段

假设签名者 U_A 对消息 $M \in Z_p$ 签名并发送给指定的接收组 G 中的验证者. 其中 M 中包含有能够被认证所需的足够冗余信息. 首先签名者 U_A 随机选取 $k \in Z_q^*$ 并计算 $v_1 = g^{-k} \bmod p$ 和 $v_2 = y_G^k \bmod p$. 然后计算签名(r, s) 如下:

$$r = Mv_1 g^{-v_2} \bmod p, \quad s = k - x_A r \bmod q$$

最后发送消息 M 的密文(r, s) 给组 G.

3.1.4　签名加密消息的恢复阶段

不妨设组 G 中的 t 个验证者(记为 $w = \{U_1, U_2, \cdots, U_t\}$) 想合作由接收到的签名密文(r, s) 恢复消息 M.

首先, 每个 $U_i \in w$ 计算 $vc_1 = g^s y_A^r = g^{rx_A + s} = g^k \bmod p$. 然后使用其秘密钥 x_i 计算

$$u_i = vc_1^{x_i l_i \bmod q} \bmod p$$

其中 $l_i = \prod_{j=1, j \neq i}^{t} - ID_j (ID_i - ID_j)^{-1} \bmod q$, U_i 把 u_i 交给组 G 中的验证合成者计算

$$v_2 = \prod_{i=1}^{t} u_i \bmod p = vc_1^{\sum_{i=1}^{t} x_i l_i \bmod q} \bmod p = vc_1^{x_G} \bmod p = y_G^k \bmod p$$

于是验证合成者恢复消息 $M = rvc_1 g^{-v_2} \bmod p$.

定理 2　如果签名者 U_A 遵循门限签名加密阶段的步骤, 则指定的接收组 G 能够正确地恢复签名消息 M.

4　方案的安全性和复杂性分析

4.1.1　安全性分析

该方案的安全性是基于计算离散对数的困难性和门限方案的安全性. 并且能抵抗文献[3] 所提出的各种攻击. 具体分析见本文 2. 4 节以及文献[3 ~ 9] . Tompa 和 Woll[11] 指出: Shamir[9] 的(t, n) 门限方案存在欺骗问题. 本文提出的方案在消息恢复阶段也面临欺骗问题. 我们可以通过如下方法解决这个问题.

假定有一个或几个验证者提供假子消息进行欺骗, 则验证合成者恢复消息后, 通过冗余信息验证所恢复的消息 M 是无效的. 此时, 他把 u_i($i = 1, \cdots, t$) 通过安全信道发送给签名者 U_A. U_A 检查等式 $y_i^{k l_i \bmod q} \bmod p = u_i$ 是否成立. 如果成立, 说明验证者 U_i 是诚实的. 否则, 说明他篡改子密钥进行欺骗应给予重罚. 然后再选择相应个数的验证者重新恢复消息 M.

4.1.2　复杂性分析

令 TE, TM 和 TI 分别表示计算模指数、模乘和模逆的时间. 用 $|x|$ 表示整数 x 的比特长度. 由于本方案的注册阶段只执行一次, 所以主要考虑签名加密阶段和消息恢复阶段的时间复杂性和通信代价. 我们的分析如表 1, 表 2.

表 1

时间复杂性	HZW 方案	Ham 方案	本文方案
签名加密阶段	3(TE + TM)	无	3(TE + TM)
消息恢复阶段	3TE + (2t + 2) TM + (t - 1) TI	(2t + 3) TE + tTM + (t - 1) TI	4TE + (2t + 2) TM + (t - 1) TI

表 2

通信量	H2W 方案	Harn 方案	本文方案
签名加密阶段	2| p| + | q|	3| p| + | q|	| p| + | q|
消息恢复阶段	(t+ 2)| p| + | q|	2t| p| + | M|	| p|

表 1、2 中消息恢复阶段的时间复杂性和通信代价是指每个验证者的时间复杂性和通信代价.

通过以上分析, 表明本方案的计算时间复杂性与 H2W 方案[3] 相当, 优于 Harn 方案[4]. 通信量低于 H2W 方案[3] 和 Harn 方案[4]. 具体分析参考文献[3, 4].

5 结论

本文提出了一个具有指定接收者的签名加密方案. 该方案是数字签名与公钥密码体制的有机集成. 而不是象文献[3, 4] 那样直接使用加密与数字签名方案进行简单的叠加, 因此, 我们的方案的计算量与通信量要比文献[3, 4] 的小. 与普通数字签名方案相比, 除了具有认证性、数据完整性外还具有保密性和接收方的隐私性. 然后又利用门限方案构造了一个(t, n) 门限共享验证签名加密方案. 与现有的门限共享验证签名加密方案相比具有数据传输安全、通信代价更小、执行效率更高、能够确切地检查出哪个验证者篡改子密钥等特点.

参考文献:

[1] K Nyberg, R A Rueppel. Message recovery for signature scheme based on discrete logarithm problem [J]. Designs Codes and Cryptography, 1996, 7: 61- 81.

[2] R J Anderson, R Needham. Robustness principles for public key protocols [A]. Advances in Cryptology2CRYPTOc95 [C]. Springer2Verlag, 1995. 236- 247.

[3] C L Hsu, T C Wu. Authenticated encryption scheme with (t, n) shared verification [J]. IEE. 2Computer Digital Technology, 1998, 145(2): 117 - 120.

[4] L Harn. Digital signature with (t, n) shared verification based on discrete logarithms [J]. Electron. Lett, 1993, 29(24): 2094- 2095.

[5] C C Lin, C S Laih. Cryptanalysis of nyberg2rueppels message recovery scheme [J]. IEEE Communications Letters, 2000, 4(7): 231- 232.

[6] A Miyaji. Another countermeasure to forgeries over message recovery signature [J]. IEICE Trans. Fundamentals, November, 1997, E80A (11): 2191- 2200.

[7] 李子臣, 李中献, 杨义先. 具有消息恢复签名方案的伪造攻击[J]. 通信学报, 2000, 21(5): 84- 87.

[8] W B Lee, C C Chang. Comment: Digital signature with (t, n) shared verification based on discrete logarithms [J]. Electron. Lett, 1995, 31 (3): 176- 177.

[9] A Shamir. How to share a secret [J]. Commun. ACM, 1979, 24(11): 612- 613.

[10] 曹珍富. 基于公钥密码系统的门限密钥托管方案 [J]. 中国科学 E 辑, 2000, 30(4): 360- 366.

[11] M Tompa, H Woll. How to share a secret with cheaters [J]. J. Cryptology, 1988, 1(2): 133- 138.

作者简介:

李继国 男, 1970 年 12 月生于黑龙江富裕县, 1996 年获黑龙江大学数学系应用数学专业学士学位, 2000 年获哈尔滨工业大学数学系基础数学专业硕士学位, 现为哈尔滨工业大学计算机学院博士生, 主要研究方向为密码学和网络安全的理论与应用等. Email: ljg1688@163. com

曹珍富 男, 1962 年 8 月出生于江苏, 计算机学士, 数学博士, 1987 年和 1991 年分别被破格由助教越级晋升为副教授和教授, 现任上海交通大学计算机系教授和博士生导师、信息产业部信息安全技术专家组成员、国家信息化专家咨询组成员等, 主要研究领域: 数论和现代密码学, 信息安全和网络安全的理论与应用等, 已发表学术论文 200 余篇, 独立出版专著 4 部, 主持完成二十余项国家级和省部级的研究课题, 作为第一完成人已获得包括中国高校科学技术一等奖在内的六项省部级奖励. Email: zfcao@cs. sjtu. edu. cn

李建中 男, 1950 年生于黑龙江哈尔滨, 教授, 博导, 主要研究领域为: 数据库系统技术, 并行计算技术.