一种新的基于双线性对的代理环签名方案*

罗大文, 何明星, 董丽莉
(西华大学 数学与计算机学院, 四川 成都 610039)

摘　要: 给出一个新的基于双线性对的代理环签名方案, 与 A-S 方案相比, 该方案更有效, 因为在签名生成时不需要双线性对运算。该方案是代理签名和环签名的结合, 由于它具有代理签名和环签名两者的优点, 因此在代理签名者需要代表原始签名者签名, 同时又需要提供匿名性时是非常有用的。

关键词: 环签名; 代理签名; 代理环签名; 离散对数难题
中图法分类号: TP309.2　　**文献标识码**: A　　**文章编号**: 1001-3695(2007)02-0125-02

New Proxy Ring Signature Scheme Based on Bilinear Pairings

LUO Da-wen, HE Ming-xing, DONG Li-li
(School of Mathematics & Computer Engineering, Xihua University, Chengdu Sichuan 610039, China)

Abstract: A new proxy ring signature scheme based on bilinear pairings is proposed. As compared with A-S scheme, this scheme is more efficient because there is no computational cost of bilinear pairings at signature generation. The scheme is the combination of proxy signature and ring signature scheme. It has advantages of proxy signature and ring signature. It is very useful when proxy signers need to sign messages on behalf of the original entity while providing anonymity.

Key words: Ring Signature; Proxy Signature; Proxy Ring Signature; Discrete Logarithm Problem

2001 年, R. Rivest 等人[1]提出了环签名概念, 它是一种新的匿名签名技术, 对于签名者而言是无条件匿名的, 它因签名参数由一定的规则首尾相连形成一个环而得名。代理签名是 1996 年由 M. Mambo 等人[2]提出, 利用代理签名原始签名人可以将他(她)的签名权委托给代理签名者, 对任何消息代理人都可以进行签名, 任何知道原始签名人的公钥者都可以对签名进行验证。代理环签名是由 F. Zhang 等人[3]提出, 它把代理签名和环签名结合起来满足代理签名和环签名的特性。本文结合文献[4, 5], 给出了一个新的代理环签名方案, 该方案比文献[4, 6]中的方案(以下简称 A-S 方案)更有效, 在签名生成时不需要对运算, 而 A-S 方案在签名生成时需要 $2n-1$ 个对运算。在签名验证时, A-S 方案需要两个对运算, 但他们的验证等式是不正确的, 本文给出了正确的验证等式; 修改后的 A-S 方案与本方案同样在签名验证时需要 $n+1$ 个对运算。在电子现金、匿名电子选举等既需要代理签名又需要保护代理签名者的权利时, 该方案是非常有用的。

1　双线性对与代理环签名

1.1　双线性对的性质

设 G_1 是由 P 生成的加法群, 阶为素数 q, G_2 是阶为 q 的乘法群, 双线性对是一个映射 $e: G_1 \times G_1 \to G_2$, 它满足如下性质:

(1) 双线性性。$e(aP, bQ) = e(P, Q)^{ab}$, 其中 $a, b \in Z_q$。

(2) 非退化性。$\exists P, Q \in G_1$, 使 $e(P, Q) \neq 1$。

(3) 可计算性。存在有效的算法计算 $e(P, Q)$, 其中 $P, Q \in G_1$。

1.2　几个计算困难性问题

(1) 离散对数问题(DLP), 寻找 $n \in z_q^*$, 使 $Q = nP$。

(2) 决定性 Diffie-Hellman 问题(DDHP), 已知 P, aP, bP, cP 确定 $c = ab \bmod q$。

(3) 计算性 Diffie-Hellman 问题(CDHP), 已知 P, aP, bP 计算 abP。

(4) 双线性对 Diffie-Hellman 问题(BDHP), 已知 P, aP, bP, cP 计算 $c = e(P, P)^{abc}$。

本文中假定 DLP, CDHP 是计算困难的。

1.3　代理环签名的安全性要求

代理环签名一般具有以下安全特性:

(1) 可区分性。代理环签名区别于代理签名者一般的环签名。

(2) 可验证性。从代理环签名中, 任何人都可以验证签名的正确性。

(3) 不可伪造性。一个授权的代理签名者可以产生一个合法的代理环签名, 但是原始签名者和第三方不能产生一个合法的代理环签名。

(4) 不可否认性。代理签名者一旦生成一个合法的环签名, 就不能再否认。

(5) 无条件匿名性。攻击者(包括原始签名者)也不知道谁是真正的代理环签名者。

收稿日期: 2005-12-12; 修返日期: 2006-02-16
基金项目: 国家自然科学基金资助项目(60473030); 教育部重点资助项目(205136)

2 基于双线性对的短签名方案及 A-S 方案

2.1 基于双线性对的短签名方案

文献[5]中给出了一个基于双线性对的短签名方案,下面加以简单介绍。

(1)系统参数设置。设 G_1 是由 P 生成的阶为素数 q 的加法群,G_2 是阶为 q 的乘法群,$e: G_1 \times G_1 \to G_2$ 是双线性对;$H: \{0,1\}^* \to z_q^*$ 是一个安全的哈希函数。

(2)密钥生成。签名者选择 $x \in_R Z_q^*$,计算 $P_{Pub} = xP$,x 是私钥,P_{Pub} 是公钥。

(3)签名生成。对消息 m,签名者计算 $s = \frac{1}{H(m) + x}P$,签名是 $\sigma = (s, m)$。

(4)签名验证。验证 $e(H(m)P + P_{Pub}, s) = e(P, P)$ 是否成立,若成立,则认为签名有效;否则认为签名无效。

2.2 A-S 方案

文献[4]给出了一个代理环签名方案,文献[6]在文献[4]的基础上给出了一个改进的代理环签名方案。下面对文献[6]加以简述。

(1)签名者随机选择 $A \in G_1$,计算 $c_{k+1} = e(A, P)$,k 表示真实签名者的位置号。

(2)签名者随机选择 $T_i \in G_1$,计算 $c_{i+1} = e(PK_0 + PK_{p_i}, H_3(c_i) H_2(\omega))^{H_1(m // L)} e(T_i, P)$,$i = k+1, k+2, \cdots, k+(n-1) \bmod n$。

(3)签名者计算 $T_i = A - H_1(m // L) H_3(c_i) S_i$,$T = \sum_{i=1}^{n} T_i$。令 $c_n = c_0$,代理环签名为 $\sigma = (c_1, c_2, \cdots, c_n, T)$。

(4)验证者验证 $\prod_{i=1}^{n} c_i = e(PK_0 + PK_{p_i}, \sum_{i=1}^{n} H_3(c_i) H_2(\omega))^{H_1(m // L)} e(T, P)$ 是否成立,若成立,则认为签名有效;否则认为签名无效。

2.3 改进的 A-S 方案

上述验证等式是不正确的,因为右边 $= e(PK_0 + PK_{p_i}, (H_3(c_1) + H_3(c_2) + \cdots + H_3(c_n)) H_2(\omega))^{H_1(m // L)} e(T_1 + T_2 + \cdots + T_n, P) = e(PK_0 + PK_{p_i}, H_3(c_1) H_2(\omega))^{H_1(m // L)} e(T_1, P) e(PK_0 + PK_{p_i}, H_3(c_2) H_2(\omega))^{H_1(m // L)} e(T_2, P) \cdots e(PK_0 + PK_{p_i}, H_3(c_n) H_2(\omega))^{H_1(m // L)} e(T_n, P) \neq \prod_{i=1}^{n} c_i = c_1 c_2 \cdots c_n =$ 左边,应该改为

$$\prod_{i=1}^{n} c_i = \prod_{i=1}^{n} e(PK_0 + PK_{p_i}, H_3(c_i) H_2(\omega))^{H_1(m // L)} e(T, P)$$

修改后右边 $= \prod_{i=1}^{n} e(PK_0 + PK_{p_i}, H_3(c_i) H_2(\omega))^{H_1(m // L)} e(T_1 + T_2 + \cdots + T_n, P) = e(PK_0 + PK_{p_i}, H_3(c_1) H_2(\omega))^{H_1(m // L)} e(T_1, P) e(PK_0 + PK_{p_2}, H_3(c_2) H_2(\omega))^{H_1(m // L)} e(T_2, P) \cdots e(PK_0 + PK_{p_n}, H_3(c_n) H_2(\omega))^{H_1(m // L)} e(T_n, P) = c_1 c_2 \cdots c_n = \prod_{i=1}^{n} c_i =$ 左边。

3 一个新的代理环签名方案

(1)系统参数设置

G_1, G_2, P, e, q 与第 2.1 节中的参数设置相同;H_1, H_2, H_3 是三个安全的哈希函数,其中,$H_1: \{0,1\}^* \to z_q^*$,$H_2: G_1 \to z_q^*$,$H_3: \{0,1\}^* \to G_1$。原始签名者的公钥是 $PK_0 = S_0 P$,私钥是 S_0,$L = \{PS_i\}$ $(i = 1, 2, \cdots, M)$,M 是一个足够大的正整数。L 表示代理签名人的集合,其公钥是 PK_{p_i},私钥是 S_{p_i}。

(2)代理钥的生成

①原始签名者选择 ω,把 $S_0 H_3(\omega)$ 传给代理签名者。

②代理签名者计算 $S_i = S_0 H_3(\omega) + S_{p_i} H_3(\omega)$,计算并公开 $PK_i = H_2(S_i) P$。

(3)签名生成

代理签名者选择 $L' \subseteq L$ 作为代理签名集合,对于消息 m,选择 $a_i \in_R z_q^*$,计算 $c_k = -\frac{1}{H_1(m) + H_2(S_k)} \sum_{i \neq k} a_i [H_1(m) + PK_i] + \frac{1}{H_1(m) + H_2(S_k)} P$($c_k$ 表示真实签名者所对应的签名),$c_i = a_i P$ $(i = 1, 2, \cdots, n, i \neq k)$,签名为 $\sigma = (m, c_1, c_2, \cdots, c_n)$。

(4)签名验证

验证 $\prod_{i=1}^{n} e(H_1(m) P + PK_i, c_i) = e(P, P)$。如果等式成立,则签名是正确的;否则签名无效。

(5)签名验证证明

如果 $\sigma = (m, c_1, c_2, \cdots, c_n)$ 是代理签名者对消息 m 的数字签名,则有

$$\prod_{i=1}^{n} e(H_1(m) P + PK_i, c_i) = \prod_{i \neq k} e(H_1(m) P + PK_i, c_i) e(H_1(m) P + PK_k, c_k) = \prod_{i \neq k} e(a_i [H_1(m) P + PK_i], P) e([H_1(m) + H_2(S_k)] P, \frac{1}{H_1(m) + H_2(S_k)} (P - \sum_{i \neq k} a_i [H_1(m) P + PK_i])) = e(\sum_{i \neq k} a_i [H_1(m) P + PK_i], P) e(P, P - \sum_{i \neq k} a_i [H_1(m) P + PK_i]) = e(\sum_{i \neq k} a_i [H_1(m) P + PK_i], P) e(P, -\sum_{i \neq k} a_i [H_1(m) P + PK_i]) e(P, P) = e(P, P)$$

4 安全性分析

(1)原始签名者的密钥是安全的,代理签名者和攻击者由 $S_0 H_3(\omega)$ 不能得出 S_0,它面临的是一个离散对数难题。

(2)不能伪造代理钥 S_i,因为 $S_i = S_0 H_3(\omega) + S_{p_i} H_3(\omega)$,它是两个签名之和,要解出 S_i 就要已知 S_0 和 S_{p_i},而由 $S_0 H_3(\omega)$ 和 $S_{p_i} H_3(\omega)$ 去求 S_0 和 S_{p_i},这是一个离散对数难题。

(3)签名不能伪造:①即使攻击者随机选择 a_i 计算出 c_i $(i \neq k)$,c_k 也不能伪造,因为计算 c_k 还需要代理钥 S_k,由(2)可知 S_k 是安全的。②不能伪造签名 $\sigma = (m, c_1, c_2, \cdots, c_n)$,使它满足签名验证等式,这是一个 CDHP 难题。

(4)代理签名者是无条件匿名的,因为随机选择的 a_i 是均匀分布的,由签名 $\sigma = (m, c_1, c_2, \cdots, c_n)$ 猜出代理签名者的概率不会超过 $\frac{1}{n}$。

5 结论

本文给出了一个新的基于双线性对的代理环签名方案,它把代理签名和环签名结合起来。由于具有代理签名和环签名两者的优点,该方案比 A-S 方案更有效,在签名生成时不需要对运算。在电子现金、匿名电子选举等既需要 (下转第 154 页)

(2) 检查本地计算机中的数字证书,验证数字证书;

(3) 处理证书链;

(4) 处理被封装的数据,完成数字证书数据的处理。

身份认证子系统采用瘦客户模型的 *N* 层体系结构设计。客户端不需要安装用户软件,只需要有一个 Web 浏览器,数据存储层是通过数据库管理子系统创建的数据库。数据库中存放有用户建立的数据或称为多维数据集。服务器端主要由 Web 服务器(Web 服务器证书宿主)和邮件数据库服务器组成。设置数据源;构建 Web 服务;为 Web 服务组件建立虚拟目录,然后设置 Web 服务扩展和 Web 服务的初始化以及验证证书。

2.4 监控模块的实现

监控模块主要负责各个子系统运行状态的监控,及时向系统管理员报告异常情况。该模块有以下组件:

(1) 系统登录状态监控组件,对每个用户登录状态的记录;

(2) 文件传输状态组件,对那些需要通过连接发送的任何类型的数据传输状态的记录;

(3) 日志组件,包含对身份验证情况的记录、文件传输的记录和检索文件信息的记录等,提供每日记录。

从前面介绍的安全体系结构中我们可以看出,一个好的信息安全系统监控是必不可少的,同时也是对该系统运行情况的一个监视。

典型的蛮力攻击的工作量很大,例如,黑客在查找到用户名和口令组合之前,会向 Web 服务器发送数以百万计的请求。有了监控子系统,就可以在黑客的攻击造成损害之前发现攻击的迹象。最好的做法之一就是记录安全异常,该信息可以存储在中心数据库中。管理员迅速审查该信息就可以轻易发现潜在的问题,这样更方便,如果出现安全漏洞,就必须正确修复以便控制它造成的损害。

3 结束语

对商业数据进行身份认证和加密保护是保障商业机密的绝好机会。将数字证书与数据库身份验证提供的历史观点相结合,可以对商业建立更好的模型,更好地保护现在的商业活动,发现商业机会。安全最终将在电子邮件系统中占据重要的地位。

系统已经在 Windows 平台中得到了实现,它是一个自主开发的计划集成多种商业电子邮件系统的安全电子邮件平台,该系统已在实际项目上获得了应用,产生了较好的实际效果。虽然我们做了很多工作,但是与其他成熟的软件比较起来,系统还显得很稚嫩,有待进一步的完善,将来可以考虑在以下方面进行改进:

(1) 数据库方面,可以考虑用二进制或用户自定义类型(在 SQL Server 2005 以及 Oracle 9i 均有支持)等敏感的数据类型代替 Text 类型以减少数据转换的开销;

(2) 在数据加密存储功能方面可以加入更合理的数据调度策略,使得系统反应更加敏捷;

(3) 在数据存储类型方面可以考虑如何把其他类型的数据纳入安全保护范围之内,如视频和音频数据[7];

(4) 在数据加密传输方面,可以加入更多实用或有研究前途的数据加密算法。

参考文献:

[1] 周学广. 信息安全导论[D]. 南京:海军电子工程大学电子工程学院,2001. 83-87.

[2] 卢正鼎,廖振松. Rijndael 算法的研究[J]. 计算机工程与科学,2005,27(6):72-74.

[3] D. R. Stinson. 密码学原理与实践[M]. 冯登国. 北京:电子工业出版社,2002. 34-36.

[4] 杨义先,林须端. 编码密码学[M]. 北京:人民邮电出版社,1992. 53-56.

[5] 崔国华,洪帆,付小青,等. 数据库系统中一种更安全的加密机制[J]. 华中理工大学学报,2000,28(7):29-31.

[6] 陈铁英,陈华,刘瑜. 基于三层次的数据库加密应用系统[J]. 华中科技大学学报,2005,33(7):41-46.

[7] 徐正全,杨志云,李伟,等. 数字视频加密技术发展现状及展望[J]. 武汉大学学报(信息科学版),2005,30(7):570-573.

作者简介:

郭文强(1975-),男,吉林安图人,讲师,博士研究生,主要研究方向为信息管理、数字信号处理;赵玉章(1956-),男,新疆奇台人,副教授,学士,主要研究方向为数据库、信息管理;韩莉英(1972-),女,四川人,讲师,主要研究方向为信息管理、数据库应用。

(上接第 126 页)代理签名又要保护代理签名者的权利时,该方案是非常有用的。

参考文献:

[1] ivest R, Shair A, Tauman M. How to Leak a Secret[C]. Advances in Cryptology-Asiacrypt, LNCS 2248, 2001. 552-565.

[2] Mambo M, Usuda K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages[J]. IEICE Trans. Fundamentals, 1996, E79-A(9):1338-1353.

[3] Zhang F, Naini R S, Lin C Y. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Scheme from Bilinear Pairings [R]. Cryptology ePint Archive, 2003.

[4] Amit K Awasthi, Sunder Lal. A New Proxy Ring Signature Scheme [C]. Proceedings of RMS, 2004. 29-33.

[5] Zhang Fangguo, Reihaneh Safavi-Naini, Willy Susilo. An Efficent Signature Scheme from Bilinear Pairings and Its Applications[A]. Feng Bao, Robert H Deng, Jianying Zhou. The 7th International Workshop on Theory and Practice in Public Key Cryptography, volume 2947 of Lecture Notes in Computer Science[C]. Singapore: Springer, 2004. 277-290.

[6] Amit K Awasthi, Sunder Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings[R]. Cryptology ePrint Archive, 2004.

作者简介:

罗大文(1972-),男,四川中江人,讲师,硕士研究生,主要研究方向为信息安全;何明星(1964-),男,四川南江人,教授,博士,主要研究方向为信息安全;董丽莉(1980-),女,山东文登人,硕士研究生,主要研究方向为信息安全。