

基于 DLP 的自认证多接收者签密方案

王之仓¹, 俞惠芳¹, 乔小妮²

(1 青海师范大学 计算机系, 青海 西宁 810008; 2 甘肃省人民医院 网络中心, 甘肃 兰州 730000)

摘 要: 在已有研究的基础之上, 实现了一种基于有限域上的离散对数问题(DLP)的自认证多接收者签密方案. 方案避免了公钥系统中的证书存在问题和密钥托管问题, 为具有多名合法接收者的签密问题提供了有效的解决途径, 算法简单, 安全性高, 适合于在实际中应用.

关键词: 自认证签密; 多接收者签密; 有限域上的离散对数问题; 不可伪造性

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)11-0014-03

Self-certified Multi-recipient Signcryption Scheme Based on Discrete Logarithm Problem

WANG Zhi-cang¹, YU Hui-fang¹, QIAO Xiao-ni²

(1 Department of Computer Science, Qinghai Normal University, Xining 810008, China;

2 Network Center of Gansu Province People Hospital, Lanzhou 730000, China)

Abstract: On the basis of existing literatures, a new self-certified multi-recipient signcryption scheme based on discrete logarithm problem(DLP) in finite field is proposed. The scheme avoids the certificate existence problem and the key escrow problem in public key cryptography and offers a efficient solution to the problem of signcryption with multi-recipient, moreover, it has simple algorithm and high security, so it is propitious to applications in practice.

Key words: self-certified signcryption; multi-recipient signcryption; discrete logarithm problem in finite field; unforgeability

1 引言

在实际生活中, 密文的接收者往往不止一个, 签密者有时需要将同一个消息发送给多名接收者, 并且每名接收者都希望能够独立解密且能验证签名的有效性, 无需相互协作, 任何无关的其他人若没有签密者或接收者的帮助都无法得到相关消息. 多接收者签密^[1-4]可以解决这一问题.

自认证签密^[5]是自认证公钥技术和数字签密技术^[6]相结合的产物, 它不仅可以同时保证开放网络上所传输消息的保密性和认证性, 而且没有密钥

托管问题和证书存在问题.

本文集成多接收者签密和自认证签密的思想, 在有限域上离散对数问题的困难性假设下, 提出了一个基于 DLP 的自认证多接收者签密方案. 此方案不仅可以解决电子政务和电子商务中存在的一些具有多名合法接收者的签密问题, 而且消除了基于证书和基于身份密码环境中的证书的存储、管理、撤销、传输等问题和密钥托管问题, 通信代价低、存储量和计算量少, 是一个算法简单、易于实现的多接收者签密方案.

收稿日期: 2009-09-18; 修回日期: 2009-11-18

基金项目: 青海省科技厅项目(2009-N-719); 青海省科技厅软课题项目(2008-Z-620); 青海省重点课程《现代操作系统》建设项目

2 基于DLP的自认证多接收者签密方案

2.1 初始化

(1) 可信机构 CA(Certificate Authority) 选择两个大素数 p_1 和 q_1 , 并满足 $p_1 = 2p' + 1, q_1 = 2q' + 1$, 其中, p' 和 q' 也是大素数. CA 计算 $p = p_1 q_1$, 并且随机选取 Z_p^* 的一个阶为 $p'q'$ 的生成元 g .

(2) CA 选取密码学上安全的哈希函数

$$h: \{0, 1\}^* \times Z_p^* \rightarrow Z_p^*;$$

$$h_1: \{0, 1\}^n \times Z_p^* \rightarrow Z_p^*;$$

$$h_2: Z_p^* \rightarrow \{0, 1\}^n;$$

$$h_3: Z_p^* \rightarrow Z_p^*.$$

(3) CA 选择一个秘密值 $s \in_R Z_p^*$, 计算 $y = g^s \bmod p$.

(4) CA 公开 $(p, g, h, h_1, h_2, h_3, h_4, y)$, 保密 (p_1, q_1, p', q', s) . 其中, n 是明文消息的比特长度.

2.2 用户注册

(1) 身份为 d_A 的签密者 A 选择一个秘密值 $r_A \in_R Z_p^*$, 计算 $y_A = g^{r_A} \bmod p$. 然后 A 发送 (d_A, y_A) 给 CA.

(2) CA 收到 (d_A, y_A) 以后, 计算 $\phi_A = h(d_A, y_A)$ 和 $\kappa_A = g^{\phi_A} \bmod p$, 并将 (κ_A, ϕ_A) 发给 A.

(3) A 收到 (κ_A, ϕ_A) 以后, 通过等式 $\kappa_A = y^{\phi_A} \bmod p$ 验证 κ_A 的合法性. 若成立, 则 A 就计算 $S_A = r_A h_3(\kappa_A)$ 作为自己的私钥, y_A 作为自己的公钥.

(4) 相应地, 每个接收者 R_j 获得自己的公私钥对: (y_j, S_j) .

2.3 签密生成

给定消息 m , 签密者 A 执行以下步骤:

(1) A 选取 $t \in Z_p^*$, 计算 $r = g^t \bmod p$.

(2) A 计算 $\delta_j = y_j^{t \cdot h_3(y_j^{\phi_j})} \bmod p, c_j = h_2(\delta_j) \oplus m$.

(3) A 计算 $\omega = h_1(m, r) g^{-t} g^{s_A} \bmod p$.

(4) 最后, A 将 $(r, c_1, \dots, c_n, \omega)$ 发送给多个接收者.

2.4 签密验证

给定消息 m 的密文, 每个接收者执行以下步骤:

(1) 计算 $\delta_j = r^{S_j} \bmod p$;

(2) 恢复消息 $m = h_2(\delta_j) \oplus c_j$;

(3) 检验 $r\omega = h_1(m, r) y_A^{h_3(y_A^{\phi_A})} \bmod p$ 是否成立. 如果成立, 就输出“接收”; 否则, 输出“拒绝”.

3 正确性分析

$$\begin{aligned} \delta &= y_j^{t \cdot h_3(y_j^{\phi_j})} \bmod p \\ &= g^{r_j \cdot t \cdot h_3(y_j^{\phi_j})} \bmod p \\ &= g^{t \cdot r_j \cdot h_3(g^{s_j \cdot \phi_j})} \bmod p \\ &= r_j^{r_j \cdot h_3(k_j)} \bmod p \\ &= r^{S_j} \bmod p \\ r\omega &= g^t h_1(m, r) g^{-t} g^{s_A} \bmod p \\ &= h_1(m, r) g^{s_A} \bmod p \\ &= h_1(m, r) g^{r_A h_3(\kappa_A)} \bmod p \\ &= h_1(m, r) g^{r_A h_3(g_j^{\phi_A})} \bmod p \\ &= h_1(m, r) y_A^{h_3(y_A^{\phi_A})} \bmod p \end{aligned}$$

4 安全性分析

4.1 保密性

本文方案建立在有限域上离散对数问题的困难性基础之上, 系统的主密钥具有保密性. 同时, 任何人想要获得消息 m , 必须获得某接收者的私钥 S_j , 而私钥 S_j 由每个接收者自己秘密保存, 攻击者无法获取. 又由 $\delta = r^{S_j} \bmod p$ 和 $m = h_2(\delta) \oplus c$ 可知, 除了每个接收者之外的任何人都无法恢复出相应的明文. 因此, 本文方案具有保密性.

可见, 与本文方案无关的任何第三方从密文中提取出消息明文是不可能的.

4.2 不可伪造性

假设内部攻击者为某个接收者 R_j , R_j 声称 (r, c'_j, ω) 为来自签密者 A 的密文, 那么 R_j 为了使伪造数据能够通过验证, 必须通过 $\delta = y_j^{t \cdot h_3(y_j^{\phi_j})} \bmod p$ 计算出 t , 进而去伪造 (r, ω) . 然而 R_j 不知道 A 选取的随机数 t , 而且 R_j 试图从等式 $r = g^t \bmod p$ 和 $\delta = y_j^{t \cdot h_3(y_j^{\phi_j})} \bmod p$ 计算出 t 都是不可行的, 因为这面临着解决有限域上的离散对数问题和大整数分解问题, 则 R_j 无法伪造出通过解签密阶段验证等式验证的数据, 因而不可能伪造出合法密文.

与本文方案无关的外部攻击者即使在公开信道上截获了 $(y_A, y_j, \kappa_A, \kappa_j, r, \omega, c_1, \dots, c_n)$, 但是他却无法获得 $(s, \delta_1, \dots, \delta_n, r_A, r_j, S_A, S_j, t)$, 因而任何外部攻击者根本无法伪造出合法密文.

综上所述, 任何内部攻击者和外部攻击者伪造出合法密文是不可行的.

4.3 不可否认性

当签密者否认其曾经向多个接收者发送过关于

消息 m 的密文时,多个接收者在不泄露其私钥的前提下,能向仲裁者提交必要信息,仲裁者根据这些信息可明确判定签密者是否曾向多个接收者发送过关于消息 m 的密文.

接收者恢复出消息 m 后,只需要提交 (r, m, ω) 给任何仲裁者,那么第三方仲裁者检查等式 $r\omega = h_1(m, r)y_A^{h_2(y_A)} \bmod p$ 是否成立即可.如果成立,则多接收者签密有效的,否则认为是无效的.此过程不需要签密者和多个接收者的私钥,因而公开验证是可行的.再者,由于只有签密者才能声称有效的密文 $(r, c_1, \dots, c_n, \omega)$,任何仲裁者均可通过 $r\omega = h_1(m, r)y_A^{h_2(y_A)} \bmod p$ 验证签密的有效性,所以多名接收者只需要公开 (r, m, ω) ,无需泄露其私钥,便可以实现其不可否认性.

5 结束语

本文提出的基于 DLP 的自认证多接收者签密方案,不存在用户公钥存储、管理、传输问题和 CA 不能冒充用户等优点,而且有利于保护多个密文接收者的隐私,适合于在实际中应用.

参考文献:

- [1] Duan S S, Cao Z F. Efficient and provably secure multi-receiver identity-based signcryption[C]// ACISP 2006, LNCS 4058. Berlin: Springer-Verlag, 2006:195-206.
- [2] 李梅,李大兴. 基于 Tate 对的指定多接收者签密方案[J]. 山东大学学报:工学版, 2006, 36(3):43-45.
- [3] 朱珍超,张玉清,王凤娇. 一个具有强安全性的多接收者签密方案[J]. 中国科学院研究生院学报, 2008, 25(3):395-402.
- [4] 娄建军,王尚平. 可认证安全的多接收者签密方案[J]. 微计算机信息, 2008, 24(2/3):76-78.
- [5] 俞惠芳,王彩芬. 一个高效的自认证签密方案[J]. 计算机工程, 2009, 35(16):138-139.
- [6] 宋文敏,杨广林. 一个扩展的基于身份的签密方案[J]. 微电子学与计算机, 2006, 23(10):138-140.

作者简介:

王之仓 男,(1974-),硕士,副教授.研究方向为信息安全、神经网络.

俞惠芳 女,(1972-),硕士,副教授.研究方向为信息安全、现代密码学.

乔小妮 女,(1980-),硕士.研究方向为数据挖掘.

(上接第 13 页)

- [2] Horn B K P, Rhunck B G. Determining optical flow [J]. Artificial Intelligence, 1981, 17(1/3):185-203.
- [3] Gonzalez R C. Digital image processing[M]. 2nd ed. 北京:电子工业出版社, 2006.
- [4] 高康林. 红外序列图像的双滤波侧抑制边缘检测算法[J]. 微电子学与计算机, 2007, 24(4):156-158.
- [5] 杨敬安. 基于光流计算的三维并行运动检测的研究[J]. 微电子学与计算机, 1994, 11(2):21-24.
- [6] Hu W M, Tan T N, Wang L, et al. A survey on visual

surveillance of object motion and behaviors [J]. IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, 2004, 34(3):334-352.

- [7] 张睿萍. 基于运动检测的视频监控系统[J]. 计算机与现代化, 2008(10):27-29.

作者简介:

刘振宇 男,(1982-),博士研究生.