

基于 DLP 的自认证广义指定验证者密签方案

俞惠芳¹, 赵海兴², 王之仓¹, 杨 林³

(1 青海师范大学 计算机系, 青海 西宁 810008; 2 青海师范大学 数学与信息科学系, 青海 西宁 810008;

3 青海师范大学 化学系, 青海 西宁 810008)

摘 要: 有机集成广义指定验证者签名和自认证签密的思想, 提出了一个基于 DLP 的自认证广义指定验证者签密方案, 方案的困难性基于有限域上的离散对数问题. 所提方案不仅能够保护签密持有者的隐私, 而且消除了证书存在问题 and 密钥托管问题. 由于新方案具有通信代价低、计算量少和安全性强等优点, 在电子商务和电子政务活动中将具有重要应用.

关键词: 自认证签密; 广义指定验证者签名; 有限域上离散对数问题; 强安全性

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)09-0049-03

Self-certified Universal Designated-Verifier Signcryption Scheme Based on Discrete Logarithm Problem

YU Hui-fang¹, ZHAO Hai-xing², WANG Zhi-cang¹, YANG Lin³

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

2 Department of Mathematic and Information Science, Qinghai Normal University, Xining 810008, China;

3 Department of Chemistry, Qinghai Normal University, Xining 810008, China)

Abstract: By integrating the thoughts of universal designated verifier signature and self-certified signcryption, a new self-certified universal designated-verifier signcryption scheme based on discrete logarithm problem in finite field is proposed. The new scheme can protect the privacy of the signcryption holder, moreover it eliminates certificate existence problem and key escrow problem. The proposed has the merits of low communication overheads, little computation cost and good security, so it is propitious to applications in E-commerce and E-government.

Key words: self-certified signcryption; universal designated verifier signature; discrete logarithm problem in finite field; good security

1 引言

广义指定验证者签名^[1-2]是指从“签名者”得到一个有效签名, “签名持有者”能够使“指定验证者”相信他拥有一个从签名者那里得到的有效签名, 但是其他任何人(包括指定验证者)都不能使其他任何人相信这个事实. 自认证签密^[3]不仅能同时实现网上传输消息的认证性和保密性, 而且不存在证书存储、管理、撤销等开销问题和密钥托管问题. 因此, 本

文在有限域上离散对数问题的难解性^[4-7]下, 有机集成广义指定验证者签名和自认证签密^[8]的思想, 提出了一个新的基于 DLP 的自认证广义指定验证者签密方案. 该方案既不需要一个安全的通信信道, 也可以有效保护签密持有者的隐私; 既不需要使用任何公钥证书, 权威机构 SA(System Authority)又无法冒充用户, 是一个通信效率高、安全性强的广义指定验证者签密方案.

收稿日期: 2009-07-07; **修稿日期:** 2009-09-07

基金项目: 国家自然科学基金项目(60863006); 青海省教育厅软课题项目(2008-Z-620); 青海省重点课程《现代操作系统》建设项目

2 所提方案

2.1 系统初始化

(1) SA 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. SA 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) SA 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) SA 选择一个秘密值 $s \in {}_R Z_p^*$, 计算 $y = g^s \bmod p$.

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

2.2 用户注册

身份为 d_u 的用户 u 选择一个秘密值 $r_u \in {}_R F_p^*$, 计算 $y_u = g^{r_u} \bmod p$. 然后用户 u 发送 (d_u, y_u) 给 SA.

SA 收到后, 计算 $Q_u = h(d_u, y_u)$ 和 $x_u = g^{Q_u}$, 并将 (Q_u, x_u) 发给用户 u .

用户 u 收到后, 通过 $y_u^{Q_u} = x_u \bmod p$ 验证 x_u 的合法性. 如果等式成立, 则用户 u 计算 $S_u = r_u h_3(x_u)$ 作为自己的私钥, y_u 作为自己的公钥.

在这里, (d_A, y_A, s_A) 、 (d_{SH}, y_{SH}, s_{SH}) 和 (d_B, y_B, s_B) 分别用来表示签密者 A、签密持有者 SH 和指定验证者 V 相应的身份、公钥以及私钥.

2.3 签密生成

给定消息 m , 签密者 A 选取 $t \in Z_p^*$, 计算 $r_1 = g^t \bmod p, \delta = y_{SH}^{h_4(y^{Q_{SH}})} \bmod p, \tau = h_2(\delta) \oplus m, \sigma_1 = h_1(m, r_1) g^{-t} g^{s_A} \bmod p$.

最后, 签密者 A 将 (r_1, τ, σ_1) 发送给签密持有者 SH.

2.4 签密验证

给定消息 m 指定签密组 (r_1, τ, σ_1) , 签密持有者 SH 执行以下步骤:

(1) 计算 $\delta = r_1^{s_{SH}} \bmod p$;

(2) 恢复消息 $m = h_2(\delta) \oplus \tau$;

(3) 随后, 签密持有者 SH 检验以下验证等式是否成立:

$$r_1 \sigma_1 = h_1(m, r_1) y_A^{h_3(y^{Q_A})} \bmod p$$

如果成立, 就输出“接收”, 否则, 输出“拒绝”.

2.5 指定签密

签密持有者 SH 选取 $k \in Z_p^*$, 计算 $r_2 = g^k \bmod p, \omega = y_V^{h_3(y^{Q_V})} \bmod p, c = h_2(\omega) \oplus m, \sigma_2 = h_1(m, r_2) \sigma_1$. 然后, 将 $(r_2, c, \sigma_1, \sigma_2)$ 发送给指定验证者 V.

2.6 指定签密验证

给定消息指定签密 $(r_2, c, \sigma_1, \sigma_2)$, 指定验证者 V 执行以下步骤:

(1) 计算 $\omega = r_2^{s_V} \bmod p$;

(2) 恢复消息 $m = h_2(\omega) \oplus c$;

(3) 检验以下等式是否成立:

$$r_1 \sigma_2 = h_1(m, r_1) h_1(m, r_2) y_A^{h_3(y^{Q_A})} \bmod p.$$

如果上述验证等式成立, 输出“接受”, 否则, 输出“拒绝”.

3 正确性分析

3.1 签密验证阶段的正确性

$$\begin{aligned} \delta &= y_{SH}^{h_3(y^{Q_{SH}})} \bmod p \\ &= g^{r_{SH} h_3(y^{Q_{SH}})} \bmod p \\ &= g^{r_{SH} h_3(g^{s_{SH}})} \bmod p \\ &= r_{SH}^{s_{SH}} \bmod p \\ r_1 \sigma_1 &= g^t h_1(m, r_1) g^{-t} g^{s_A} \bmod p \\ &= h_1(m, r_1) g^{r_A h_3(x_A)} \bmod p \\ &= h_1(m, r_1) g^{r_A h_3(g^{s_A})} \bmod p \\ &= h_1(m, r_1) y_A^{h_3(y^{Q_A})} \bmod p \end{aligned}$$

3.2 指定签密验证阶段的正确性

$$\begin{aligned} \omega &= y_V^{h_3(y^{Q_V})} \bmod p \\ &= g^{k_V h_3(y^{Q_V})} \bmod p \\ &= r_2^{r_V h_3(g^{s_V})} \bmod p \\ &= r_2^{s_V} \bmod p \\ r_2 \sigma_2 &= g^t h_1(m, r_1) h_1(m, r_2) g^{-t} g^{s_A} \bmod p \\ &= h_1(m, r_1) h_1(m, r_2) g^{r_A h_3(x_A)} \bmod p \\ &= h_1(m, r_1) h_1(m, r_2) g^{r_A h_3(g^{s_A})} \bmod p \\ &= h_1(m, r_1) h_1(m, r_2) y_A^{h_3(y^{Q_A})} \bmod p \end{aligned}$$

4 安全性分析

4.1 不可转移性

在指定签密验证算法中需要使用指定验证者的私钥 s_V , 因此, 指定验证者自己能够生成有效的指定签密 $\sigma_2 = h_1(m, r_1) \sigma_1$. 任何第三方得到指定签

名 σ_2 时,不能区分该签密是签密持有者生成的还是指定验证者生成的.

4.2 保密性

除签密者、签密持有者和指定验证者能够知道消息明文外,任何第三方都无法提取出消息明文.

签密持有者在指定签密算法中给出 $\omega = y_V^{k_3(y_V^{Q_V})} \bmod p$,攻击者由 $r_2 = g^k \bmod p$ 求出 k ,进而伪造会话密钥 τ 以便恢复消息明文是不可行的,因为这相当于破解有限域上的离散对数问题.再者攻击者不知道 s_V ,则无法通过 $\tau = r_2^{\tau} \bmod p$ 求出 τ ,所以攻击者无法恢复出消息明文.因此,任何其他用户从密文中恢复出消息明文是不可能的.

4.3 指定签密验证的指定性

从恢复消息等式 $m = h_2(\omega) \oplus c$ (其中 $\omega = r_2^{s_V} \bmod p$)中可以看出,要确保能够正确恢复出消息明文 m ,需要用到指定验证者的私钥 s_V .只有拥有合法私钥 s_V 的指定验证者才能正确恢复出 m .在正确恢复出 m 的基础上,指定验证者才能通过判断等式 $r_1\sigma_2 = h_1(m, r_1)h_1(m, r_2)y_A^{h_A(y_A^{Q_A})} \bmod p$ 是否成立来验证签密 (σ_1, σ_2) .而任何与本文方案无关的第三方试图利用已有信息 (σ_1, σ_2) 求出 m 是不可能的,因为求解有限域上的离散对数问题和单向散列函数的逆是困难的.

4.4 不可伪造性

任何攻击者都不可能伪造一个来自签密者和签密持有者的签密组.

一个外部攻击者试图假冒签密者伪造消息 m 的签密组 (r_1, τ, σ_1) 和 $(r_2, c, \sigma_1, \sigma_2)$.由于外部攻击者不知道 (t, s_A, k) ,因而无法构造合法的能够通过签密持有者和指定验证者验证的签密.所以任何外部攻击者在不知道 (t, s_A, k) 情况下,要伪造出合法的密文是不可行的.

假设内部攻击者为指定验证者,指定验证者向第三方称 $(r'_2, c, \sigma_1, \sigma'_2)$ 为合法的签密组,其中 (r'_2, σ'_2) 为指定验证者伪造的数据.为了使得伪造数据通过验证,他必须确定 k ,但 k 是一个随机数且只有签密持有者知道,即使指定验证者知道 r_2 ,想通过 $r_2 = g^k \bmod p$ 计算出 k 也是不可行,因为求解

有限域上的离散对数问题是困难的.因此,指定验证者是不可能伪造出合法密文.

5 结束语

本文设计了一个基于有限域上离散对数问题的自认证广义指定验证者签密方案,此方案既可以保护签密持有者的隐私,又具有自认证签密的优点,是一个高效安全的广义指定验证者签密方案.

参考文献:

- [1] Steinfeld R, Bull L, Wang H, et al. Universal designated - verifier signatures [C]//Proceedings of Advances in Cryptology - Asiacrypt'03. Berlin: Springer - Verlag, 2003: 522 - 542.
- [2] Zhang Fanguo, Susilo Willy, Mu Yi, et al. Identity - based universal designated verifier signature[C]//Proceedings of EDC Workshops'05. Berlin: Springer - Verlag, 2005:825 - 834.
- [3] Shi R. A (t, n) threshold shared verification signature scheme based on discrete logarithms [J]. Computer Research&Development, 2000, 37(3): 319 - 323.
- [4] 韩小西,王贵林,鲍丰,等. 针对基于离散对数多重签名方案的一种攻击[J]. 计算机学报,2004,27(8):1147 - 1152.
- [5] 徐光宝,张建中. 一个基于离散对数的群签名方案[J]. 计算机工程, 2005, 31(9):143 - 144.
- [6] 张串绒,肖国镇. 一个可公开验证签密方案的密码分析和改进[J]. 电子学报, 2006,34(1):177 - 179.
- [7] 黄文婷,殷新春. 一种基于 ACJT 群签名方案的前向安全电子现金方案[J]. 微电子学与计算机,2008,25(9): 168 - 170.
- [8] 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):1 - 2.

作者简介:

俞惠芳 女,(1972-),副教授.研究方向为信息安全、现代密码学.

赵海兴 男,(1968-),教授.研究方向为理论计算机、图论.

王之仓 男,(1974-),副教授.研究方向为信息安全、神经网络.

杨林 男,(1962-),教授.研究方向为计算机网络、神经网络.