基于DLP的自认证代理签密方案

俞惠芳 赵海兴 王之仓 王小红
(青海师范大学计算机系 西宁 810008)

摘 要 自认证密码体制可以实现无公钥证书和密钥托管,代理签密是将代理签名和签密相结合的一种方案。在已有研究的基础上,集成自认证密码体制和代理签密,提出了一种新的基于DLP的自认证代理签密方案,并在有限域上离散对数问题的难解性下,给出了其正确性和安全性证明。

关键词 有限域上离散对数问题,代理签密,可公开验证,自认证密码体制

中图法分类号 TP309 **文献标识码** A

Self-certified Proxy Signcryption Based on Discrete Logarithm Problem

YU Hui-fang ZHAO Hai-xing WANG Zhi-cang WANG Xiao-hong
(Department of Computer Science, Qinghai Normal University, Xining 810008, China)

Abstract Self-certified cryptosystem realizes the properties of no public key certificate and key-unescrow, proxy signcryption is a scheme that combines the proxy signature and signcryption. By merging the thoughts of self-certified cryptosystem and proxy signcryption, a new self-certified proxy signcryption scheme based on discrete logarithm problem was proposed on the basis of the existing literatures. Under the hardness of discrete logarithm problem in finite field, the new scheme was proved to be correct and secure.

Keywords Discrete logarithms problem in finite field, Proxy signcryption, Public verifiability, Self-certified cryptosystem

1 引言

针对数字签名仅能提供信息来源认证而不能提供保密性问题,Zheng[1]组合了数字签名和对称密钥加密算法的功能,提出了新型密码学概念"签密",在一个逻辑单步内同时实现了消息的认证性和保密性,而且其计算比传统的"先签名后加密"更有效。1999年,Gamage等[2]提出了第一个代理签密方案,该方案允许一个原始签密人授权他的签密权力给一个代理签密人,代理签密人可以代表原始签密人对授权消息生成有效的代理签密。2002年,Chan等人[3]亦提出了一个代理签密方案,但此方案不具有不可否认性,而且整个通信必须使用安全信道。随着代理签密的发展,学者们提出了许多代理签密方案[4-10]。

本文在已有研究的基础上[2-14],在有限域上离散对数问题[12]的难解性下,提出了一种新的基于DLP的自认证代理签密方案。所提方案具有代理签密的功能,只有指定的接收者才能从密文中恢复消息,克服了传统密码学中的证书存在问题,消除了基于身份密码学中的密钥托管问题。

2 所提方案

2.1 系统初始化

(1)权威机构SA(System 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。SA计算 $p=p_1q_1$,随机选取 Z_p^* 的一个阶为 $p'q'$的生成元 g。

(2)选取密码学上安全的哈希函数:

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

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

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

$h_3:Z_p^*\rightarrow\{0,1\}^n$;

$h_4:Z_p^*\rightarrow Z_p^*$。

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

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

2.2 用户密钥提取

身份为 d_u 的用户 u 选择一个秘密值 $r_u\in_R Z_p^*$,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(d_u,y_u)以后,计算 $Q_u=h(d_u,y_u)$和 $x_u=g^{sQ_u}$,并将(Q_u,x_u)发给用户 u。

用户 u 收到(Q_u,x_u)以后,可通过 $y^{Q_u}=x_u \bmod p$ 验证 x_u 的合法性。如果等式成立,则用户 u 就计算 $S_u=r_uh_4(x_u) \bmod p$ 作为自己的私钥,y_u 作为自己的公钥。

为了叙述方便,原始签密者A、代理签密者B和接收者C相应的公私钥对分别简记为(y_A,S_A),(y_B,S_B)和(y_C,S_C)。

到稿日期:2009-06-12 返修日期:2009-09-03 本文受国家自然科学基金项目(60863006),教育部科学技术研究重点项目(208148),甘肃省科技攻关项目(2GS064-AS2-035-03)和青海省重点课程《现代操作系统》建设项目资助。

俞惠芳(1972—),女,硕士,副教授,CCF会员,主要研究方向为信息安全、现代密码学;赵海兴(1968—),男,博士,教授,博士生导师,主要研究方向为理论计算机、图论;王之仓(1974—),男,硕士,副教授,主要研究方向为信息安全、神经网络;王小红(1982—),女,硕士生,讲师,主要研究方向为理论计算机。

2.3 代理密钥提取

原始签密人 A 建立一个授权许可证 m_w，用以明确原始签密人 A 和代理签密人 B 的身份信息、授权关系和授权关系的使用限制等内容。然后，原始签密人 A 计算 $\theta_A = h_1(m_w) S_A$，并将(m_w, θ_A)发给 B。

B 检查等式$(y_A)^{h_1(m_w)h_4(y^{Q_A})} = g^{\theta_A} \bmod p$ 是否成立。如果成立，则 B 计算代理签密密钥 $\theta_p = \theta_A + h_1(m_w) S_B \bmod p$；否则，要求 A 重发。

2.4 代理签密

代理签密人 B 执行如下步骤：

(1)B 随机选择 $k \in Z_p^*$，计算 $R = g^k \bmod p$；

(2)B 计算 $V = y_C^{kh_4(y^{Q_C})} \bmod p$；

(3)B 计算 $c = h_3(V) \oplus m$；

(4)B 计算 $S = h_2(m, R) g^{-k} g^{\theta_p} \bmod p$；

(5)B 输出密文 $\sigma = (m_w, R, c, S)$。

2.5 解签密

接收者 C 收到密文 σ 以后，执行如下步骤：

(1)C 计算 $V = R^{S_C} \bmod p$；

(2)C 恢复消息 $m = c \oplus h_3(V)$；

(3)C 检查以下验证式是否成立：

$$RS = h_2(m, R) y_A^{h_4(y^{Q_A})h_1(m_w)} y_B^{h_4(y^{Q_B})h_1(m_w)} \bmod p。$$

如果以上验证等式成立，密文 (m_w, R, S) 和用户公钥 (y_A, y_B) 同时被认证，Bob 接受 (m_w, R, S)；否则，验证失败，认为 (m_w, R, S) 是不合法的。

3 正确性分析

$$\begin{aligned} V &= y_C^{kh_4(y^{Q_C})} \bmod p = g^{rc kh_4(g^{sQ_C})} \bmod p \\ &= R^{rc h_4(x_C)} \bmod p = R^{S_C} \bmod p \\ RS &= g^k h_2(m, R) g^{-k} g^{\theta_p} \bmod p \\ &= h_2(m, R) g^{\theta_A + h_1(m_w) S_B} \bmod p \\ &= h_2(m, R) g^{S_A h_1(m_w)} g^{S_B h_1(m_w)} \bmod p \\ &= h_2(m, R) y_A^{h_4(y^{Q_A})h_1(m_w)} y^{h_4(y_B^{Q_B})h_1(m_w)} \bmod p \end{aligned}$$

4 安全性分析

定理 1 在有限域上离散对数问题和大整数分解问题的难解性下，本文方案满足保密性。

证明：假设除了代理签密人和接收者外，还有其他用户能从密文(m_w, R, c, S)中恢复消息明文 m。假如攻击者已经获取密文，则攻击者若想恢复出消息明文，必须知道 V，然而由 $R = g^k \bmod p$ 计算出 k，进而通过 $V = y_C^{kh_4(y^{Q_C})} \bmod p$ 计算出 V 是不可行的，因为有限域上离散对数问题和大整数分解问题是难解问题，攻击者通过 $c = h_3(V) \oplus m$ 提取出消息明文是不可能的。因此，除了代理签密人和接收者外，其他任何人均不能从密文中提取出消息明文。

定理 2 在有限域上离散对数问题和单向散列函数求逆问题的困难性下，本文方案满足不可伪造性。

证明：任何内部和外部攻击者都不可能伪造一个来自代理签密人的关于某个消息 m 的密文。

假定内部攻击者为接收者，接收者试图通过签名 $R = g^k \bmod p$ 求出 k，进而去伪造密文在计算上是不可行的，因为有限域上离散对数问题是个困难问题。若内部攻击者代理签密人试图伪造密文，则他必须知道原始签密人的私钥 S_A，而代理签密人通过 $\theta_A = h_1(m_w) S_A \bmod p$ 计算出 S_A，进而去伪造代理签密是不可行的，因为这意味着要解决有限域上离散对数问题。

由于有限域上离散对数问题、大整数分解问题和单向散列函数求逆问题是困难问题，因此任何外部攻击者试图通过 $RS = h_2(m, R) y_A^{h_4(y^{Q_A})h_1(m_w)} y_B^{h_4(y^{Q_B})h_1(m_w)} \bmod p$ 求出明文 m，进而去伪造密文亦是不可行的。

因此，本文方案能够抵抗伪造攻击，任何攻击者都不可能伪造一个来自代理签密人的关于某个消息 m 的密文。

定理 3 本文方案满足不可否认性。

证明：当代理签密人否认曾向接收者发送过关于消息的密文时，接收者在不泄露其私钥的前提下，能向第三方仲裁者提交必要信息，仲裁者根据这些信息可明确判定代理签密人是否曾经向接收者发送过关于消息的密文。

一方面，在解签密阶段，当密文接收者解出了明文 m 后，由于 $RS = h_2(m, R) y_A^{h_4(y^{Q_A})h_1(m_w)} y_B^{h_4(y^{Q_B})h_1(m_w)} \bmod p$ 中的所有参数在此阶段已经公开，因此可公开验证是可行的。另一方面，只有代理签密人才能声称有效的密文(m_w, R, c, S)，任何第三方均可通过解签密阶段的验证式验证(m_w, R, S)是否确实为关于消息 m 的有效密文。可见，接收者在无需泄露其私钥的情况下，只要提交(m_w, R, m, S)给第三方仲裁者，仲裁者就可以同时验证(m_w, R, S)的有效性以及原始签密人和代理签密人的公钥(y_A, y_B)的真实性。所以本文方案在实现可公开验证性的基础上，实现了其不可否认性。

定理 4 在有限域上离散对数问题的难解性下，本文方案满足前向安全性。

证明：如果原始签密人和代理签密人的私钥被意外泄露或偷走，那么第三方也不能恢复出以前所签密消息的明文。

假设第三方在通信信道上已经截获了密文。如果原始签密人和代理签密人的私钥被意外泄露或偷走，由于第三方不知道接收者的私钥 S_C，不可能通过 $V = R^{S_C} \bmod p$ 计算出会话密钥 V，那么第三方只能通过 $V = y_C^{kh_4(y^{Q_C})} \bmod p$ 来计算会话密钥 V。然而这个等式中对于第三方来说，k 是一个未知数，而且第三方由 $R = g^k \bmod p$ 计算出 k 进而计算出会话密钥 V 亦是不可行的，因为求解有限域上离散对数问题和大整数分解是困难的，第三方无法通过此方式计算出会话密钥 V。所以本文方案是前向安全的。

定理 5 本文方案满足强可识别性。

证明：完整有效的代理签密中有原始签密人的授权许可证 m_w，而 m_w 中包含有代理签密人的身份信息，任何与本文方案无关的第三方都能从 m_w 中确定相应代理签密人的身份。

定理 6 本文方案满足抗滥用性。

证明：由于代理签密密钥中包含有原始签密人的授权信息，因而只能用于产生有效的密文，不能用于其它未授权的签密中。

结束语 本文设计了一种新的基于 DLP 的自认证代理签密方案。该方案既保持了自认证密码体制优点，又具有保

(下转第 71 页)

$V_{\pm 3k}$, $V_{\pm 3k+1}$, $V_{\pm 3k+2}$, $U_{\pm 3k-1}$, $U_{\pm 3k}$ 和 $U_{\pm 3k+1}$，其总共需要 80×2 次大整数模乘运算，其次当 $a_i=1$ 约需 12×2 次大整数模乘运算。当 $a_i=-1$ 约需 12×2 次大整数模乘运算。当 $a_i=0$ 约需16×2 次大整数模乘运算，假定 m 三进制展开式中，1，−1 和 0 出现的概率相等，则第二步平均需要 80/3 次大整数模乘运算。因而，计算 V_{l+}, V_{l-}, U_{l+} 和 U_{l-} 总共平均需要 560/3 次大整数模乘运算。该算法需要⌊$\log_3 m$⌋次循环，因而算法总共平均需要 560/3⌊$\log_3 m$⌋次大整数模乘运算。令加密密钥为 e，模数为 n，则 RSA 平方乘模幂算法大约平均需要 1.5⌊$\log_2 e$⌋次模 n 乘法运算，Lucas 序列项计算需要约 3⌊$\log_2 e$⌋次模 n 乘法运算，3F-L 序列项计算需要约 9⌊$\log_2 e$⌋次模 n 乘法运算。与其它密码体制相比，该算法运算速度相对比较慢。为提高 5FLELG 公钥密码算法效率，可将明文编码为 4 段同时进行加解密，该方法将算法的数据吞吐率提高了 3 倍，计算时间和存储空间大幅降低。但是由于其每次迭代计算的模乘运算数量比较多，因而性能还是比 LUCELG 和 3F-LELG 要差。进一步提高序列项计算算法效率，是 5FLELG 公钥密码体制走向实用的关键。

结束语 本文详细研究五阶 Fibonacci-Lucas 序列相关性质，提出 5FLELG 公钥密码体制和数字签名方案，其以五阶 Fibonacci-Lucas 序列来替代 Lucas 序列和三阶 Fibonacci-Lucas 序列，在序列周期、签名认证以及安全性等方面都比较优越。当然，5FLELG 公钥密码体制自身还存在许多缺陷，要想走向实用还需提高其运算速度，验证其安全性等，这也是今后进一步研究的方向。

参 考 文 献

[1] Smith P. LUC public key encryption-a secure alternative to RSA [J]. Dr. Dobb's Journal, 1993, 18(1): 44-49

[2] Smith P, Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms[C]// Advances in Cryptology-Asiacrypt'94. Berlin: Springer -Verlag, 1995: 355-364

[3] Bleichenbacher D, Bosma W, Lenstra A K. Some remarks on lucas-based Cryptosystem[C]// Advances in Cryptology-CRYPTO'95. Berlin: Springer-Verlag, 1995: 386-396

[4] 王丽萍，周锦君. F-L 公钥密码体制[J]. 通信学报，1999，20(4)：1-6

[5] 王丽萍，韩付成. 基于三阶 Fibonacci-Lucas 序列的一种新的公钥密码体制和数字签名[C]// 密码学进展-ChinaCrypt'2000. 北京：科学出版社，2000：140-144

[6] Gong G, Harn L. Public-key cryptosystems based on cubic finite field extensions[J]. IEEE Transaction on Information Theory, 1999, 45(7): 2601-2605

[7] Lenstra A K, Verheul E R. The XTR public key system[C]// Advances in Cryptology-CRYPTO' 2000. LNCS 1880. Berlin: Springer-Verlag, 2000: 1-19

[8] Giuliani K, Gong G. Analogues to the Gong - Harn and XTR Cryptosystems[EB/OL]. http://www. cacr. math. uwaterloo. ca/techreports/2003/corr2003-34. ps, 2003

[9] 陈小松，唐勇民. 基于 n 阶 Dickson 多项式的公钥密码系统[J]. 系统工程，2005，22(3)：124-126

[10] 姜正涛，柳毅，王育民. 基于 LFSR 高次剩余问题构造公钥密码体制的研究[J]. 电子与信息学报，2006，28(3)：542-545

(上接第 67 页)

密性、不可伪造性、不可否认性、强可识别性和抗滥用性等安全特性，而且设计简单、易于实现，无需交互式验证，在通信时不必要使用安全信道，不存在证书管理、存储、撤消等开销问题和密钥托管问题。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]// Advances in Cryptology- CRYPTO' 97. Lecture Notes in Computer Science 1294. Berlin: Springer-Verlag, 1997: 165-179

[2] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy signcryption[C] // Proceedings of 22nd Australasian Computer Science Conference. Berlin: Springer-Verlag, 1999: 420-431

[3] Chan W K, Wei V K. A threshold proxy signcryption[C]//Proceedings of International Conference on Security and Management. Monte Carlo Resort, Las Vegas, Nevada, USA, 2002: 24-27

[4] Li X, Chen K. Identity based proxy signcryption scheme from pairings[C]// Proc. of the 2004 IEEE International Conference on Services Computing. Shanghai, 2004: 494-497

[5] Wang Q, Cao Z F. Two proxy signcryption schemes from bilinear pairings[C]//Proceedings of CANS 2005. Berlin: Springer- Verlag, LNCS 3810. 2005: 161-171

[6] Wang M, Li H, Liu Z J. Efficient identity based proxy-signcryption schemes with forward security and public verifiability[C]// ICCNMC 2005. LNCS3619. Berlin: Springer-Verlag, 2005: 982-991

[7] Li X X, Ch K F. Identity based proxy-signcryption scheme from pairings[C]// IEEE International Conference on Services Computing. Los Alamitos, California: IEEE Computer Society Press, 2004: 494-497

[8] 张学军，王育民. 高效的基于身份的代理签密[J]. 计算机工程与应用，2007，43(3)：109-111

[9] 胡振鹏，钱海峰，李志斌. 基于身份的多接收者的代理签密方案[J]. 华东师范大学学报：自然科学版，2008(1)：83-87

[10] 于刚，黄根勋. 一个前向安全的基于身份的代理签密方案[J]. 计算机工程与应用，2008(2)：157-159

[11] 冯登国，赵险峰. 信息安全技术概论[M]. 北京：电子工业出版社，2009：97-99

[12] WENBO MAO[英]. 现代密码学理论与实践[M]. 北京：电子工业出版社，2004：169-171

[13] 俞惠芳，王彩芬，刘丹青. 基于椭圆曲线的自认证多代理签密方案[J]. 西北师范大学学报：自然科学版，2010，45(6)：43-45

[14] 俞惠芳，王彩芬. 一种新的基于自认证的门限代理签密方案[J]. 计算机工程与设计，2010，30(24)：5588-5590