对一种代理签名方案的攻击和改进

孙 颖，许春香，吴 淮，陈艾东

(电子科技大学计算机科学与技术学院 成都 610054)

【摘要】分析了文献[12]提出的一系列代理签名方案的安全性，包括基本的代理签名方案、电子支票的可控授权协议和前向安全的代理签名方案，指出这些方案是不安全的。利用伪造攻击，一个敌手可以成功伪造代理签名密钥，冒充诚实的代理签名人生成有效的代理签名，威胁原始签名人和代理签名人的合法权益，相应地，给出了修正方法抵抗代理签名密钥伪造攻击。

关 键 词 密码学； 数字签名； 代理签名； 伪造攻击

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.03.029

Attack and Improvement of a Proxy Signature Scheme

SUN Ying, XU Chun-xiang, WU Huai, and CHEN Ai-dong

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract The security of some proxy signature schemes including a simple proxy signature scheme, controlled delegation in e-checks using proxy signature and a forward secure proxy signature scheme due to Ref.[12] is analyzed. It is shown that all the schemes are insecure. A forgery attack on these schemes is proposed in this paper. Using the forgery attack, a malicious adversary can forgery a valid proxy signing key on behalf of the original signer without his/her agreement and produce valid proxy signatures, which does harm to the benefits of the original signer and the proxy signer. The corresponding corrected algorithms are proposed to resist this kind of forgery attack.

Key words cryptography; digital signature; forgery attack; proxy signature

作为日常生活中手写签名的电子替代物，数字签名已经成为保证信息完整性、不可抵赖性和实现认证的重要手段，并受到学术界的广泛研究。随着电子商务和电子政务的不断发展，普通的数字签名已经不能满足人们日常生活日益发展的需求，众多有特殊性质的数字签名技术被相继提出，由文献[1]提出的代理签名就是其中的一种，其主要功能是实现签名的授权。在代理签名中，一个原始签名人将其签名权利委托给代理签名人之后，代理签名人就可以代表原始签名人进行签名。这种授权的情况广泛存在于现实生活中，如经理不在时，授权其签名权利给其秘书。文献[1]按照授权类型不同，把代理签名分为完全授权、部分授权和基于委托书的授权3类。在完全授权中，原始签名人把自己的签名密钥直接交给代理签名人，使代理签名人具有与其相同的签名能力。显然，完全授权的方式是不实际和不安全的。在部分授权中，代理签名人可以获得一个与原始签名人密钥不同的代理密钥，使代理人生成的签名与原始签名人的签名不同。该方式的缺点是无法限制代理签名人的签名范围，代理签名人可以对任意消息签名。该缺点可在基于委托书授权的签名方式中得到弥补，委托书中详细描述了代理签名人的签名范围、授权有效期以及代理人和授权人的身份等信息。代理签名提出后，引起了研究学者的极大关注，成为密码学的一个研究热点。

文献[2]首先提出了强代理签名的概念，但强代理签名需满足可区分性、可验证性、强不可伪造性、可识别性、不可否认性和可防止签名权利被滥用。之后，很多代理签名方案及其变形方案被相继提出，如门限代理签名[3-4]、代理盲签名[5]、匿名代理签名[5-6]、代理多重签名[7]、一次代理签名[8-9]、指定验证人代理签名[10-11]等。

文献[12]提出了一种新的代理签名方案，该方案的特色是可以用于授权的控制。该文献首先提出了

收稿日期：2009－10－09； 修回日期：2009－11－02

基金项目：国家863计划(2009AA01Z415)；国家自然科学基金(61003232)；教育部博士点基金(200806140010，2100185120012)；中央高校基本业务费(ZYGX2010J066)；四川省科技创新苗子工程

作者简介：孙 颖(1980－)，女，博士生，主要从事密码学、数字签方面的研究.

一个基本代理签名方案，并声称该方案满足代理签名的所有安全性质之后，该文发现该基本方案适用于在电子支票系统中限制代理签名人的金融授权，因此基于该基本方案，设计了一个新方案，并提出了一个具体的协议，用于解决代理环境中电子支票的授权控制问题；最后结合前向安全思想，提出了一个具有代理撤销功能的多个代理签名人的代理签名方案，用于更新代理密钥，以便解决代理签名密钥的泄露问题。虽然该文献声称其所有的方案都是安全的，并且给出了一些安全性分析，但本文的研究发现，该文献的方案并不安全，一个敌手可以成功伪造代理签名密钥，冒充诚实的代理签名人生成有效的代理签名，说明该文献的方案不满足数字签名应该具备的最重要、最基本的不可伪造性，有重大的安全缺陷。

为了修正该文献方案的缺陷，本文将分析该代理签名方案，找出其安全性漏洞，并提出一个改进的新算法，以抵抗代理签名密钥伪造攻击。

1　文献[12]的基本方案

1.1　基本代理签名方案

基本代理签名方案由代理密钥生成、代理签名生成和代理签名验证3个算法组成。系统参数包括 p 和 q 两个大素数，其中，$q \mid p-1$，g 为 Z_p^* 的 q 阶乘法子群的生成元，$h:\{0,1\}^* \to Z_q^*$ 为一个安全的Hash函数。

1) 代理密钥生成。原始签名人Alice的私钥为 $x_A \in Z_q^*$，相应的公钥为 $y_A = g^{x_A} \bmod p$。代理签名人Bob的私钥为 $x_B \in Z_q^*$，相应的公钥为 $y_B = g^{x_B} \bmod p$。为了生成对委托书 w 的签名，Alice随机选择 $k_A \in Z_q^*$，并计算 $K = g^{k_A} \bmod p$，$S_A = k_A y_B + x_A h(w) \bmod q$，并发送 (w, K, S_A) 给代理签名人Bob。Bob收到授权 (w, K, S_A) 后，检验 $g^{S_A} = y_A^{h(w)} K^{y_B} \bmod p$ 是否成立，如果成立，认为授权有效；否则，授权无效。如果授权有效，Bob计算其代理签名密钥 (x_p, y_p)，其中 $x_p = S_A + x_B y_A \bmod p$，$y_p = g^{x_p} \bmod p$。

2) 代理签名生成。拥有代理签名密钥对 (x_p, y_p) 的代理签名人可以利用任意基于离散对数困难问题的签名方案生成消息 m 的代理签名 $(\mathrm{sign}(m, x_p), K, m, y_A, y_B)$。

3) 代理签名验证。验证人首先计算 $y_p = y_A^{h(w)} K^{y_B} y_B^{y_A} \bmod p$，然后用基于离散对数问题的签名算法的验证算法检验 $\mathrm{sign}(m, x_p)$ 是否是公钥 y_p 下的有效的签名。如果检验通过，代理签名有效；否则无效。

1.2　对基本方案的分析

本文对文献[12]基本方案的安全性分析表明，该方案并不满足其所声称的强不可伪造性。事实上，该方案容易遭受普遍性伪造攻击(universal attack)，任意一个敌手都有能力伪造一个有效的代理签名密钥，冒充代理签名人Bob代替原始签名人Alice对任意消息签名。这是因为在代理签名密钥验证式 $y_p = y_A^{h(w)} K^{y_B} y_B^{y_A} \bmod p$ 时出现了孤悬因子 K，为敌手伪造代理签名密钥提供了可能。具体伪造过程为：

1) 首先，敌手制作一个委托书 w，其中详细说明了原始签名人和代理签名人的身份、授权期限、授权签名的范围等授权信息。

2) 然后，敌手利用扩展的欧几里德算法计算出 y_B^{-1}，并随机选择 $r \in Z_q^*$，计算 $K = (y_A^{-h(w)} g^r y_B^{-y_A})^{y_B^{-1}} \bmod p$。代理签名密钥对为 $(x_p = r, y_p = g^r \bmod p)$

3) 拥有代理签名密钥对 (x_p, y_p) 的敌手可以利用任意基于离散对数困难问题的签名方案生成消息 m 的代理签名 $(\mathrm{sign}(m, x_p), K, m, y_A, y_B)$。

敌手伪造的代理签名一定可以通过代理签名验证，因为此时：

$$y_p = y_A^{h(w)} K^{y_B} y_B^{y_A} \bmod p =$$
$$y_A^{h(w)} ((y_A^{-h(w)} g^r y_B^{-y_A})^{y_B^{-1}})^{y_B} y_B^{y_A} \bmod p =$$
$$g^r \bmod p = g^{x_p} \bmod p$$

并且，以 $(x_p = r, y_p = g^r \bmod p)$ 为签名密钥，利用基于离散对数困难问题的签名方案生成的签名也可以通过相应的签名验证。

1.3　对基本方案的改进

改进的方法是为了避免在代理签名验证式中出现孤悬因子。本文给出一个简单的改进方法，在参数选择时，选择一个安全的Hash函数 $h:\{0,1\}^* \times Z_p \to Z_q^*$。

1) 代理密钥生成。为了生成对委托书 w 的签名，Alice随机选择 $k_A \in Z_q^*$，计算 $K = g^{k_A} \bmod p$，$S_A = k_A y_B + x_A h(w, K) \bmod q$，并发送 (w, K, S_A) 给代理签名人Bob。Bob收到授权 (w, K, S_A) 后，检验 $g^{S_A} = y_A^{h(w,K)} K^{y_B} \bmod p$ 是否成立，如果成立，授权有效；否则，授权无效。如果授权有效，Bob计算其代理签名密钥 (x_p, y_p) 为：

$$x_p = S_A + x_B y_A \bmod p$$
$$y_p = g^{x_p} \bmod p$$

2) 代理签名生成。拥有代理签名密钥对

(x_p, y_p) 的代理签名人可以利用任意基于离散对数困难问题的签名方案生成消息 m 的代理签名 $(\mathrm{sign}(m, x_p), K, m, y_A, y_B)$。

3) 代理签名验证。验证人首先计算 $y_p = y_A^{h(w,K)} K^{y_B} y_B^{y_A} \bmod p$，然后用基于离散对数问题的签名算法的验证算法检验 $\mathrm{sign}(m, x_p)$ 是否是公钥 y_p 下的有效签名。如果检验通过，代理签名有效；否则无效。

在Hash函数是抗碰撞的假设下，本文提出的攻击方法对改进方案不再奏效，因为要计算 K，使得 $K = (y_A^{-h(w,K)} g^r y_B^{-y_A})^{y_B^{-1}} \bmod p$ 成立面临着攻破Hash函数的抗碰撞性。其他安全性分析与文献[12]对基本方案的安全性分析相同。

2 电子支票的可控授权协议与分析

文献[12]利用其基本代理签名方案设计了一个电子支票的可控授权协议，应用场景如下。

当组织一个国际会议时，会议主席给不同的委员会以不同的金融权利，委员会成员可以利用代理签名对电子支票签名。会议主席首先以会议的名义在银行开户，并把所有的资金存入到该账户，然后把对第 i 个委员会成员的授权信息(如可以提取的资金上限)写到委托书 m_i 中，并随机选择 $k_i \in Z_q^*$

计算 (K_i, S_{A_i}) 并发送给第 i 个成员，其中 $K_i = g^{k_i} \bmod p$，$S_{A_i} = k_i y_i + x_A h(m_i) \bmod q$。接收到 (K_i, S_{A_i}) 后，每个成员通过检验 $g^{S_{A_i}} = y_A^{h(m_i)} K_i^{y_i} \bmod p$ 是否成立验证授权的有效性。如果授权有效，每个成员计算其代理签名密钥：

$$x_{pi} = S_{A_i} + x_i y_A \bmod q$$

$$y_{pi} = g^{x_{pi}} \bmod p$$

成员 i 拥有代理签名密钥 x_{pi} 后，可以利用基于离散对数的数字签名体制如DSA签名对符合 m_i 规定的支票签名，得到代理签名 σ。银行在对支票的签名进行验证时，首先计算代理签名验证公钥 $y_{pi} = y_A^{h(m_i)} K_i^{y_i} y_i^{y_A} \bmod p$，然后利用基于离散对数的数字签名体制的验证算法和公钥 y_{pi} 对支票的签名进行验证。如果恶意的委员会成员修改 m_i 欲提取更多的资金，其只有伪造出相应的 (x_{pi}, y_{pi}) 才能通过银行的验证，文献[12]声称这种伪造是不可能的。

事实上，文献[12]所声称的结论是错误，正如本文对基本代理签名方案的分析，敌手很容易伪造一个有效的代理签名密钥对 (x_{pi}, y_{pi})：

1) 首先，敌手制作一个委托书 m_i^*，其中的授权信息可以由敌手任意设置。

2) 然后，敌手随机选择 $r^* \in Z_q^*$，计算 $K_i^* = (y_A^{-h(m_i^*)} y_i^{-y_A} g^{r^*})^{y_i^{-1}} \bmod p$。

3) 设置代理签名密钥对为 $(x_p = r^*, y_p = g^{r^*} \bmod p)$。

4) 拥有代理签名密钥对 (x_p, y_p) 的敌手可以利用任意基于离散对数困难问题的签名方案生成符合 m_i^* 规定的支票的代理签名。

对文献[12]的协议中的代理签名方案的修正方法与本文对基本代理签名方案的修正类似，在参数选择时，选择一个安全的Hash函数 $h: \{0,1\}^* \times Z_p \to Z_q^*$。在签名生成和验证过程中，把相应的 $h(m_i)$ 改为 $h(m_i, K_i)$。

文献[12]结合代理签名和前向安全的思想，提出了一个前向安全的代理签名方案，用于方便代理撤销。与本文之前的分析方法类似，文献[12]的前向安全代理签名方案仍然容易遭受代理签名密钥伪造攻击，在此不再重复。

3 结束语

本文分析了文献[12]最近提出的一系列代理签名方案的安全性，包括基本的代理签名方案、电子支票的可控授权协议和前向安全的代理签名方案，指出这些方案的不安全之处，即一个恶意的敌手可以成功伪造代理签名密钥，假冒诚实的代理签名人生成验证有效的代理签名。本文给出了相应的修正方法，使修正后的方案可以抵抗代理签名密钥伪造攻击。

参 考 文 献

[1] 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.

[2] LEE B, KIM H, KIM K. Strong proxy signature and its applications[C]//SCIS 2001. Oiso, Japan: The Institute of Electronics, Information and Communication Engineers, 2001: 603-608.

[3] SHAO Z H. Improvement of threshold proxy signature scheme[J]. Computer Standsrds & Interface, 2004, 27: 53-59.

[4] ZHANG K. Threshold proxy signature scheme[C]//Proc of the 1997 Information Security Workshop. Tatsunokuchi, Ishikawa, Japan: Springer-Verlag, 1997: 191-197.

[5] ZHANG Fang-guo, NAINI R S, LIN C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings[R]. Cryptology ePrint Archive Report, 2003.

[6] YU Yong, XU Chun-xiang, HUANG Xin-yi, et al. An efficient anonymous proxy signature scheme with provable security[J]. Computer Standards & Interfaces, 2009, 31(2): 348-353.

[7] YI L, BAI G, XIAO G. Proxy multi-signature scheme: a new type of proxy signature scheme[J]. Electron Lett, 2000, 36(6): 527-528.
[8] KIM H, BAEK J, LEE B, et al. Secrets for mobile agent using one-time proxy signature[C]//The Institute of Electronics, Information and Communication Engineers. Oiso, Japan: [s.n.], 2001: 845-850.
[9] MEHTA M, HARN L. Efficient one-time proxy signatures[J]. IEE Proceedings of Communications. 2005, 152(2): 129-133.
[10] ZHANG Jian-hong. An improved designated-verifier proxy signature scheme[C]//International Conference on Networking, Architecture and Storage 2007. Guilin, China: IEEE Press, 2007: 77-82
[11] YU Yong, XU Chun-xiang, ZHANG Xiao-song, et al. Designated verifier proxy signature scheme without random oracles[J]. Computers and Mathematics with Applications, 2009, 57(8): 352-1364.
[12] SUNITHA N R, AMBERKER B B. Proxy signature scheme for controlled delegation[J]. Journal of Information Assurance and Security, 2008, 2: 159-174.

编 辑 税 红

(上接第615页)

[6] LEI Y, TAI K C. In-parameter-order: a test generating strategy for pairwise testing[J]. IEEE Transaction on Software Engineering, 2002, 28(1): 1-3.
[7] COHEN M B, COLBOURN C J, GIBBONS P B, et al. Constructing test suites for interaction testing[C]//Proc of the Intl Conf on Software Engineering. [S.l.]: [s.n.], 2003: 38-48.
[8] NURMELA K H. Upper bounds for covering arrays by tabu search[J]. Discrete Applied Mathematics, 2004, 138(9): 143-152.
[9] SHIBA T, TSUCHIYA T, KIKUNO T. Using artificial life techniques to generate test cases for combinatorial testing[C]//Proc of the IEEE Annual Int'l Computer Software and Applications Conf. [S.l.]: IEEE, 2004: 72-77.
[10] LEI Y, KACKER R, KUHN D R, et al. IPOG: a general strategy for t-way software testing[C]//Proc of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems. [S.l.]: IEEE, 2007: 549-556.

编 辑 税 红