文章编号:1005-0523(2009)05-0075-04

对两种代理盲签名体制的密码学分析

农 强[1],郝艳华[1,2],黄茹芬[1]

(漳州师范学院 1.计算机科学与工程系;2.信息安全与计算机网络福建省高校重点实验室,福建 漳州 363000)

摘要:代理盲签名结合了代理签名与盲签名的优点,而多级代理签名实现了签名权利在许可范围内逐级向下代理的要求。利用椭圆曲线上的双线性对,陈玲玲等人提出了一种基于身份的代理盲签名方案,胡江红等人提出了一种基于身份的多级强代理盲签名方案。给出了这两个方案的密码学分析,指出在陈玲玲等人的方案中,代理签名人可以利用授权证书计算得到原始签名人的私钥,从而可直接伪造原始签名人的签名或授权,同时指出所提的两个方案也无法满足不可追踪性,代理签名人可以将自己在签名协议中的签名和签名的消息联系起来从而跟踪消息的拥有者,从而证明了这两个方案是不安全的。

关 键 词:基于身份;代理盲签名;多级代理;不可追踪性;双线性对

中图分类号:TP309 **文献标识码**:A

随着互联网电子商务等业务的迅速发展,如何在网络中实现签名权转让成为一个重要问题,而代理签名正是解决这一问题的有效途径,它使得用户可以授权其他用户代替他们签发某一消息,同时还具备数字签名的不可伪造、可验证、不可否认、可区分、可识别、防止滥用等性质。自文献[1]首次提出代理签名的概念后,引起了众多学者的关注和研究,并提出了多种不同类型的代理签名方案[2]。在基本的代理签名的应用中,原始签名人和代理签名人只能进行一级代理,但在有些情形下,签名权利需要逐级向下代理,如1个国家的政府机关要进行某专项整治行动,就需要从国家机关到各省、市、县等部门在授权范围内一级一级地向下授权执行。2000年,伊丽江首次提出了多级代理签名[3]的概念,并提出了两个多级代理签名体制,初步解决了签名权的多级授权传递的问题。盲签名[4]的概念由Chaum等人于1983年首先提出,它要求签名人在不知道消息内容的情况下对消息进行签名。盲签名可在电子现金、电子投票等应用中提供用户匿名性。

在电子交易系统中,签名授权人(消费者)通常不希望代理签名者(如银行)能将签署的某则消息(用户可以使用的有效电子货币)和某个具体的支付行为联系起来,这样能保证用户的隐私,因此文献[5]首次提出了代理盲签名的概念。代理盲签名结合了代理签名和盲签名的优点,具有非常重要的应用价值,并已成为研究的热点,国内外重要的代理盲签名方案见文献[6][7][8]。不可追踪性是代理盲签名的一个重要特性,它指签名人的协议信息和消息-签名对是不可链接的,即使给定若干次签名会话的协议信息和若干个消息-签名对,签名人也不能确定协议信息和消息-签名对的对应关系。

基于椭圆曲线上的双线性对,陈玲玲等人提出了一种高效的基于身份的代理盲签名方案[9],胡江红等人提出了一种基于身份的多级强代理盲签名方案[10]。这两个签名方案的作者都指出他们的签名方案是不可伪造的,然而本论文通过安全性分析证明它们是不安全的,因此具有一定的实用意义和学术意义。已有许多类似的研究,如文献[11][12]等等,也是研究代理盲签名方案的密码学分析问题。但是本论文在陈玲玲等人方案的代理密钥生成算法中,代理签名人根据原始签名人的授权可恢复其私钥,进而可直接伪造原始签名人的签名或授权,并指出同样的安全缺陷也存在于另外几篇文献的代理盲签名方案中。同时,在所提的两个方案中,代理签名人在签名时和签名后都能将自己在签名协议中的签名和签名的消息联系起来从而跟踪消息的拥有者,所以这两个方案也无法满足代理盲签名应具备的不可追踪性的安全需求。

收稿日期:2009-06-16

基金项目:福建省自然科学基金项目(2009J01307);福建省教育厅科技项目(JA09161)

作者简介:农 强(1978-),男(壮族),广西南宁人,硕士,讲师,研究方向为密码学与网络安全。

1 双线性对及困难假设

设$(G_1,+)$和$(G_2,\times)$为q阶循环群,q为一大素数。P为G_1的生成元,设在群G_1,G_2中离散对数问题是困难的,可定义双线性映射为$e:G_1\times G_1\to G_2$,其满足双线性性、非退化性和可计算性三种特性。对于这样定义的G_1,我们可以定义离散对数问题(DLP)、可计算 Diffie-Hellman 问题(CDHP)、可判定 Diffie-Hellman 问题(DDHP)、Gap Diffe-Hellman(GDH)问题等难解问题,并称具有 CDH 问题难解而 DDH 问题易解特征的群为 GDH 群。有关详细内容可参看文献[13]。

2 对文献[9]代理盲签名方案的安全性分析

2.1 陈玲玲等人的代理盲签名方案回顾

(1) 系统参数设置:KGC 选取$<G_1,G_2,e,q>$,选取任意的生成元$P\in G_1$和3个强无碰撞的密码哈希函数$H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\times G_2\to Z_q^*$,$H_3:G_1\to Z_q^*$。KGC 选择$t\in_R Z_q^*$,计算$P_{pub}=tP$,将$t$秘密保存,公开系统参数$Params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2,H_3\}$。

(2) 密钥提取:原始签名人A和代理签名人B提交他们的身份ID_A,ID_B给 KGC,KGC 计算他们相应的公钥/密钥对为$PK_A=H_1(ID_A)$,$SK_A=tPK_A$;$PK_B=H_1(ID_B)$,$SK_B=tPK_B$,然后分别安全地发送给A和B。

(3) 代理密钥生成:A建立一个授权许可W来明确说明包含A和B的身份信息的授权关系,同时也说明该授权关系的使用限制等内容。A首先计算一个短签名$S_W=H_3(H_1(W))SK_A$,然后将(S_W,W)发送给B。B计算并验证等式$e(S_W,P)=(PK_A,P_{pub})^{H_3(H_1(W))}$是否成立。若成立,$B$计算代理签名密钥:$S_P=S_W+H_3(H_1(W))SK_B$。

(4) 代理盲签名生成:代理签名人B给C的消息m进行盲数字签名,过程如图1

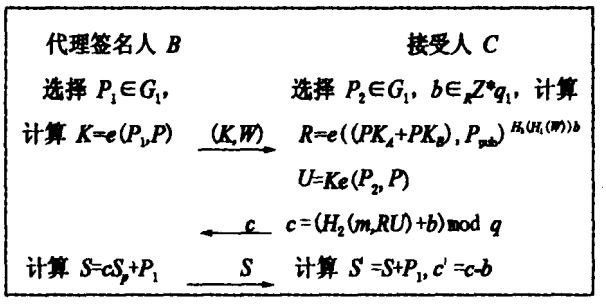

图1 文献[9]代理盲签名生成过程

则$\sigma(m)=(S',c',m,W)$为消息m的基于身份的代理盲签名。

(5) 签名验证:已知$\sigma(m)$,验证人验证$c'=H_2(m,e(S',P)e(PK_A+PK_B,P_{pub}))^{-c't}$是否成立,其中$t=H_3(H_1(W))$。

2.2 对代理密钥生成算法的分析

在上述方案的代理密钥生成算法中存在安全漏洞,因为当代理签名人B收到原始签名人A发送给他的授权证书(S_W,W)后,他可以通过计算$H_3(H_1(W))^{-1}\in_R Z_q^*$,然后计算$H_3(H_1(W))^{-1}S_W=H_3(H_1(W))^{-1}H_3(H_1(W))SK_A=SK_A$。这样,$B$就可以恢复出$A$的私钥,进而可以假冒$A$伪造签名或代理授权,这就损害了原始签名人的合法权益。这里特别要指出的是,该攻击方法也适用对文献[14][15]中的代理密钥生成算法的攻击。

2.3 可追踪性分析

在上述方案中,作者指出在签名过程中,B和C之间实行的是交互协议,在交互时,C对消息进行了盲化,所以签名人不知道所签消息是什么,且签名(S',c',m,W)也是由C计算得到,当签名被公开后,他也无法将其与某个签名联系起来。但实际上,只要盲签名人B记录所有他能够收集到的每次签名时的协

议信息(K,c,S),即使最终签名(S',c',m,W)是用随机值P_2和b处理后的结果,当签名(S',c',m,W)被公开后,B可以通过以下步骤来确定协议信息和消息-签名对的对应关系:

(1) 代理签名人B分别计算$\alpha = Ke(S' - S,P)$和$\beta = c - c'$;

(2) 代理签名人B接着计算$\gamma = e((PK_A + PK_B),H_3(H_1(W))P_{pub})^{\beta}$;

代理签名人B最后验证等式$c' = H_2(m,\alpha\gamma)$是否成立,若成立,则说明签名人B可以将消息与签名联系起来。因为

$$\begin{aligned}\alpha\gamma &= Ke(S' - S,P)e((PK_A + PK_B),H_3(H_1(W))P_{pub})^{\beta}\\ &= Ke(P_2,P)e((PK_A + PK_B),H_3(H_1(W))P_{pub})^{c-c'}\\ &= e((PK_A + PK_B),P_{pub})^{H_3(H_1(W))b}Ke(P_2,P) = RU\end{aligned}$$

所以有$\alpha\gamma = RU$,即$H_2(m,RU) = H_2(m,\alpha\gamma) = c'$成立,代理签名人此时能够判断出对应于消息$m$的代理盲签名$(S',c',m,W)$是否是由他签署的,从而最终说明上述代理盲签名不具有不可追踪性。

3　对文献[10]多级代理盲签名方案的安全性分析

3.1　胡江红等人的多级代理盲签名方案回顾

(1) 系统初始化:可信中心TA选取$<G_1,G_2,e,q>$,选取任意的生成元$P\in G_1$和2个密码哈希函数$H:\{0,1\}^* \to G_1,h:\{0,1\}^* \to Z_q^*$,并选择$x\in_R Z_q^*$,计算$pk = xP$,公开$(P,xP)$,将$x$作为主密钥。设原始签名者为$P_0$,各级代理签名者为$P_1,P_2,\cdots,P_n$,原始签名者和各级代理签名者分别提交其身份$ID_0,ID_1,ID_2,\cdots,ID_n$,TA计算他们相应的私钥$S_i = xH(ID_i)$,其中$0\leqslant i\leqslant n$。

(2) 代理密钥生成:设W是授权信息,第$i-1$级代理签名者对第i级代理签名的授权是否合法要根据W_{i-1}来判断。首先P_{i-1}选择$t_{i-1}\in_R Z_q^*$,计算签名$K_{i-1} = t_{i-1}H(W_i) + S_{i-1} + K_{i-2}$,并通过安全信道将$K_{i-1}$发送给$P_i$,公开参数$t_{i-1}P$和$W_i$。

P_i收到K_{i-1}后,计算并验证等式$e(K_{i-1},P) = \prod_{j=1}^{i} e(H(W_j),t_{j-1}P)e(H(ID_{j-1}),xP)$是否成立,若成立,$P_i$计算其代理私钥$S_i' = K_{i-1} + S_i$和代理公钥$Q_i' = H(ID_0) + \sum_{j=1}^{i} H(ID_j)$。

(3) 签名生成:设签名请求者Alice要求P_i对消息M_i进行签名,过程如图2。

代理签名人 P_i		接受人 Alice
选择 $\alpha_i\in_R Z_q^*$,		选择 $\beta_i\in_R Z_q^*$, 计算
计算 $r_i' = e(P,t_{i-1}P)^{\alpha_i}$	$\xrightarrow{r_i'}$	$r_i = r_i'e(P,t_{i-1}P)^{\beta_i}$
	$\xleftarrow{V_i}$	$V_i = h(M_i \| r_i)$
计算 $U_i' = V_iS_i' + \alpha_i t_{i-1}P$	$\xrightarrow{U_i'}$	计算 $U_i = U_i' + \beta_i t_{i-1}P$

图2　文献[10]代理盲签名生成过程

则代理签名者P_i对消息M_i的盲签名为(U_i,r_i)。

(4) 签名验证:签名接收者Alice验证$r_i = e(P,U_i)\prod_{j=1}^{i} e(t_{j-1}P,H(W_j))^{-V_i}e(xP,Q_j')^{-V_i}$是否成立,如果成立,则接受签名,否则拒绝或要求代理签名者重新签名。

3.2　可追踪性分析

同理,在胡江红等人的方案中,作者指出对代理签名者P_i而言,盲签名值(U_i,r_i)虽是已知的,但从他与Alice交互过程中无法确定参数β_i,从而也就无法确定盲参数因子t_{i-1},因为他们中都出现了GDH困难问题,所以P_i并不知道哪次签名与这个签名相关联,因此他就不可能追踪签名。然而经分析发现,只要代理签名人P_i记录所有他能够收集到的每次签名时的协议信息(U',V_i,r_i'),即使最终签名(U_i,r_i)是用随

机值 β_i 和 t_{i-1} 处理后的结果，当签名 (U_i, r_i) 被公开后，P_i 可以通过以下步骤来确定协议信息和消息－签名对的对应关系：

(1) 代理签名人 P_i 计算 $R = e(U_i - U_i', P)$。

(2) 代理签名人 P_i 接着计算 $T = r_i'^{V_i}$。

代理签名人 P_i 最后验证等式 $R^{V_i}T = r_i^{V_i}$ 是否成立，若成立，则说明签名人 P_i 可以将消息与签名联系起来。因为

$$R^{V_i}T = e(U_i - U_i', P)^{V_i} r_i'^{V_i} = e(\beta_i \cdot t_{i-1}P, P)^{V_i} e(P, t_{i-1}P)^{\alpha_i V_i}$$

$$= e(t_{i-1}P, P)^{\beta_i V_i} e(t_{i-1}P, P)^{\alpha_i V_i} = (r_i' e(P, t_{i-1}P)^{\beta_i})^{V_i} = r_i^{V_i}$$

所以代理签名人 P_i 此时能够判断出对应于消息 M_i 的代理盲签名 (U_i, r_i) 是否是由他签署的，从而最终说明上述多级代理盲签名也不具有不可追踪性。

4 结论

代理盲签名是近年来出现的一种新的签名技术，在电子商务和电子投票系统中具有广泛的应用前景。本文对他人提出的两种代理盲签名方案进行了密码分析，分别指出它们存在的安全隐患。考虑进一步的研究工作，希望设计出可证明安全的代理盲签名方案。

参考文献：

[1] Mambo M, Usdua K, Okamoto E. Proxy signature: delegation of the power to sign messages[J]. IEICE Transactions on Fundations, 1996, E79－A(9): 1 338－1 353.

[2] Zhang F, Safavi-Naini R, Lin C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairing [EB/OL]. http://eprint.iacr.org, 2003－10－04.

[3] 伊丽江. 代理签名及应用研究[D]. 西安：西安电子科技大学，2000. 56－58.

[4] Chaum D. Bind signature for untraceable payments[A]. Chaun D, Rivest R L Swpman A T. Advances in Cryptology: Proceedings of Crypto'82[C]. New York: Plenum, 1983. 199－203.

[5] Lin W, Jan J K. A security personal learning tools using a proxy bind signature scheme[A]. Proceedings of International Conference on Chinese Language Computing[C]. USA: Chinese Language Computer Society Knowledge Systems Institute, 2000. 273－277.

[6] 李方伟，谭利平，邱成刚. 基于离散对数的代理盲签名[J]. 电子科技大学学报，2008，37(2)：172－174.

[7] ZHANG Jian-hong, MAO Jian. Linkability analysis of some blind signature schemes[A]. International Conference on Computational Intelligence and Security 2006[C]. Berlin: Springer, 2007. 556－566.

[8] Sherman S M Chow. Blind signature and ring signature schemes: Rehabilitation and attack[J]. Computer Standards and Interfaces, 2008, 31(4): 707－712.

[9] 陈玲玲，亢保元，张　磊. 一种高效的基于身份的代理盲签名方案[J]. 华东交通大学学报，2008，25(1)：113－116.

[10] 胡江红，张建中. 新的基于双线性对的多级强代理盲签名方案[J]. 计算机工程与应用，2007，43(18)：123－125，149.

[11] 黄　辉，秦　静，李　丽. 一个改进的代理盲签名方案[J]. 计算机应用，2007，27(6)：1 539－1 541.

[12] 雷治军，刘文化，禹　勇. 对一种代理盲签名方案的密码学分析[J]. 计算机应用，2008，28(5)：1 144－1 145.

[13] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297－319.

[14] 张学军，王育民. 高效的基于身份的代理盲签名[J]. 计算机应用，2006，26(11)：2 586－2 588.

[15] LANG Wei-min, YANG Zong-kai, CHENG Wen-qing, *et al*. A new ID-based proxy blind signature scheme[J]. Wuhan University Journal of Natural Sciences, 2005, 10(3): 555－558.

(下转第 130 页)

[10] Slicer, Deborah. Reading the Earth: New Direction in the Study of Literature and Environment[M]. Idaho: University of Idaho Press, 1999. 109 - 110.
[11] 朱 虹. 英国小说的黄金时代[M]. 北京: 中国社会科学出版社, 1997.

North and South: Conflict and Deconstruction

ZHOU Xiang-hua

(School of Science and Technology, Nanchang University, Nanchang 330047, China)

Abstract: From the perspective of eco-feminism, this thesis aims to interpret Mrs. Gaskell's eco-feminist thoughts presented in her North and South. Based on the analysis of Mrs. Gaskell's ingenious design about the conflicts between North and South in the novel, it tries to explore the exposure and deconstruction of binary oppositions between women and men, nature and industrial culture.

Key words: North and South; eco-feminism; binary oppositions; conflict; deconstruction

(责任编辑: 刘棉玲 吴泽九)

(上接第 78 页)

Cryptanalysis of Two Proxy Blind Signature Schemes

NONG Qiang[1], HAO Yan-hua[1,2], HUANG Ru-fen[1]

(1. Department of Computer Science and Engineering; 2. Key Laboratory of Information Security and Computer Network, Zhangzhou Normal University, Zhangzhou 363000, China)

Abstract: The proxy blind signature scheme combines the good properties of both proxy signature and blind signature scheme, while the multi-level proxy signature scheme can realize step by step under agreement. Recently, based on bilinear pairings of elliptic curve, Chen Lingling proposed an ID-based proxy blind signature scheme, and Hu Jianghong proposed an ID-based multi-level proxy blind signature scheme. Through the cryptanalysis of the two schemes, it shows that in Chen's scheme, the proxy signer can calculate the original signer's private key by receiving his authorization, and then he can forge any signature or authorization directly. At the same time, the two proposed schemes can not satisfy the untraceability, the proxy signer can link a signature to the corresponding message of signing protocol so that he can trace the message holder, therefore the two schemes are not secure.

Key words: ID-based; proxy bind signature; multi-level proxy; untraceability; bilinear pairings

(责任编辑: 刘棉玲)