改进的无证书代理盲签名方案

刘二根 王 霞 周华静 郭红丽

(华东交通大学理学院 南昌 330013) (华东交通大学系统工程与密码学研究所 南昌 330013)

摘 要 通过对张晓敏提出的高效无证书代理盲签名方案进行安全性分析,发现该方案不能抵抗恶意但被动的KGC攻击,也不能抵抗普通攻击者的签名伪造攻击,而且KGC与原始签名者联合可以获得代理密钥。为了避免这些攻击,提出了一种改进的无证书代理盲签名方案,且该方案具有更高的安全性。

关键词 代理盲签名,恶意但被动的KGC攻击,代理密钥

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.8.019

Improved Certificateless Proxy Blind Signature Scheme

LIU Er-gen WANG Xia ZHOU Hua-jing GUO Hong-li

(School of Science, East China Jiaotong University, Nanchang 330013, China)

(Institute of Engineering and Cryptography, East China Jiaotong University, Nanchang 330013, China)

Abstract Through the security analysis of the certificateless proxy blind signature scheme proposed by Zhang Xiaomin, it was found that the scheme can not resist the malicious-but-passive KGC attack and signature forgery attack, in addition, KGC collusion with the original signer can get proxy key. In order to avoid these attacks, an improved certificateless proxy blind signature scheme was presented, and it has a better security.

Keywords Proxy blind signature, Malicious-but-passive KGC attack, Proxy key

1 引言

2003年,Al-Riyami等人[1]首先提出了无证书公钥密码体制。在无证书密码体制中,用户的私钥一部分由KGC生成,一部分由用户自己生成,从而有效地解决了基于证书密码体制中的密钥存储、管理问题,也克服了基于身份的密码体制的密钥托管问题。许多无证书签名也相继出现[2,3]。

1982年,Chaum[4]首次提出了盲签名的概念。盲签名是指签名者虽然对文件或消息签了名,但并不知道文件或消息的具体内容。1996年,Mambo等人[5]首次提出了代理签名的概念,即若签名者由于某些原因无法亲自签名,他可以将自己的签名权委托给他人,让其代替自己进行签名。将盲签名和代理签名结合,可以产生代理盲签名。2000年,Lin和Jan[6]首次提出了代理盲签名的概念,许多代理盲签名方案也应运而生[7-9]。代理盲签名由于既有盲签名的性质,又具有代理签名的性质,因此能够广泛地应用于电子投票、电子现金等领域。

无证书密码体制和代理盲签名结合可以产生无证书代理盲签名方案。2011年,黄隽等人[10]提出了一个无证书代理盲签名方案,但张建中等人[11]发现该方案不能抵抗公钥替换攻击和恶意的KGC攻击。本文通过对张晓敏[12]的无证书代理盲签名方案进行分析,发现该方案不能抵抗恶意但被动的KGC攻击,也不能抵抗普通攻击者的签名伪造攻击,而且KGC与原始签名者联合可以获得代理密钥。为了克服这些缺陷,提出了一个改进的方案,且新方案具有更好的安全性。

2 预备知识

2.1 双线性映射

设G_1,G_2分别是由P生成的q阶加法群和乘法群,e:$G_1\times G_1\to G_2$是满足下面3个性质的双线性映射。

(1)双线性性:$e(aP,bQ)=e(P,Q)^{ab}$,$\forall P,Q\in G_1$,$a,b\in Z_q^*$;

(2)非退化性:有$P,Q\in G_1$,使得$e(P,Q)\neq 1$;

(3)可计算性:$\forall P,Q\in G_1$,能够计算出$e(P,Q)$。

2.2 离散对数问题(DLP)

对于给定的$P,Q\in G_1$,求满足$Q=nP$的$n\in Z_q^*$是困难的。

3 方案[12]回顾及存在的攻击

3.1 方案回顾

本方案的参与成员有:原始签名者A,代理签名者B,用户C和验证者。

(1)系统初始化。G_1,G_2分别是阶为q的循环加法群和循环乘法群,P是G_1的生成元,e:$G_1\times G_1\to G_2$是一个双线性

到稿日期:2015-07-28 返修日期:2015-11-05 本文受国家自然科学基金项目(11361024,11261019,61472138,61263032),江西省高校科技落地计划项目(KJLD12067),华东交通大学校立科研基金项目(11JC04),江西省科技厅科技项目(20151BDH80071)资助。

刘二根(1965-),男,硕士,教授,硕士生导师,主要研究方向为图论及其优化、信息安全,E-mail:leg_eg@sina.com;王 霞(1990-),女,硕士生,主要研究方向为信息安全,E-mail:jxwx1990@163.com(通信作者);周华静(1991-),女,硕士生,主要研究方向为信息安全;郭红丽(1988-),女,硕士生,主要研究方向为信息安全。

映射，选择两个安全的哈希函数：$H_1:\{0,1\}^* \rightarrow G_1$，$H_2:\{0,1\}^+ \rightarrow Z_q^+$，随机选择系统主密钥 $s\in Z_q^*$，并计算系统公钥 $P_{pub}=sP$，公开系统公开参数 $params=\{G_1,G_2,P,q,e,H_1,H_2,P_{pub}\}$。

(2)部分密钥生成。原始签名人 A 和代理签名者 B 将其身份信息 ID_A 和 ID_B 发送给 KGC，KGC 计算 $Q_A=H_1(ID_A)$，$Q_B=H_1(ID_B)$，$D_A=sQ_A$，$D_B=sQ_B$，D_A 和 D_B 分别为 A 和 B 的部分私钥，并通过安全信道分别发送给 A 和 B。原始签名人 A 和代理签名者 B 可以通过验证等式 $e(D_i,P)=e(Q_i,P_{pub})$ 是否成立来判断部分私钥的正确性，其中 $i\in\{A,B\}$。

(3)用户密钥生成。A 和 B 分别随机选取秘密值 $x_A,x_B\in Z_q^*$，计算其私钥 $SK_A=x_AD_A$，$SK_B=x_BD_B$，并计算 $X_A=x_AP$，$Y_A=x_AP_{pub}$，$X_B=x_BP$，$Y_B=x_BP_{pub}$。那么，A 的公钥为 $PK_A=(X_A,Y_A)$，私钥为 (SK_A,D_A)；B 的公钥为 $PK_B=(X_B,Y_B)$，私钥为 (SK_B,D_B)。

(4)代理授权。首先生成一个包括双方身份信息、代理权限、代理期限等信息的授权证书 M_ω，A 随机选择 $r\in Z_q^*$，计算 $e(P,P)^r=G$，$S_\omega=SK_AH_2(M_\omega,G,PK_A)+rP$，公开 M_ω,G，并将 (S_ω,M_ω,G) 发给 B。B 收到 (S_ω,M_ω,G) 后，首先通过验证等式 $e(X_A,P_{pub})=e(Y_A,P)$ 是否成立来验证 A 的公钥是否有效，再验证等式 $e(S_\omega,P)=e(Q_A,Y_A)^{H_2(M_\omega,G,PK_A)}G$ 是否成立，若等式成立，则计算 $S_p=S_\omega+SK_BH_2(M_\omega,G,PK_A)$ 作为代理密钥。

(5)代理盲签名的产生。

①代理签名者 B 随机选取 $P'\in_RG_1$，计算 $k=e(P,P')$，将 (k,M_ω,G) 发送给用户 C；

②C 随机选择 $P^*\in_RG_1$，$a,b\in_RZ_q^*$，计算 $Q=a^{-1}P$，$R=T^{bH_2(M_\omega,G,PK_A)}$，$U=ke(P,P^*)^{a^{-1}}$，$c=(H_2(m,RU)+b) \bmod q$，$V=G^{-c}$，其中 $T=e(Q_A,Y_A)e(Q_B,Y_B)$，并将 c 发送给 B；

③B 收到 c 后，计算 $S=cS_p+P'$，并将 S 发送给 C；

④C 收到 S 后，计算 $S'=aS+P^*$，$c'=c-b$，$\sigma=(S',c'Q,V)$ 就是关于消息 m 的代理盲签名。

(6)签名验证。签名验证者收到 $\sigma=(S',c'Q,V)$ 后，先验证消息 m 是否符合 M_ω，B 是否是真实的代理签名人，若是则继续，否则停止；然后通过验证等式 $e(X_i,P_{pub})=e(Y_i,P)$ 是否成立来判断 A 和 B 的公钥是否有效，若等式成立则继续，否则停止；最后验证等式 $H_2(m,e(S',Q)T^{-H_2(M_\omega,G,PK_A)c'}V)=c'$ 是否成立，若成立，$\sigma=(S',c'Q,V)$ 是有效的代理盲签名，否则签名无效。

3.2 方案[12]的攻击方法

(1)恶意但被动的 KGC 攻击

方案[12]不能抵抗恶意的 KGC 攻击，即攻击者在对原始签名人 A 和代理签名者 B 的公钥不做任何替换的情况下，由于攻击者知道系统主密钥 s，他可以冒充原始签名人 A 对 B 进行代理授权。过程如下：

①攻击者预先确定参数 $P=\alpha Q_A$，$\alpha\in Z_q^*$，计算 A 的公钥 $X_A=x_AP$，$Y_A=x_AP_{pub}$，B 的公钥 $X_B=x_BP$，$Y_B=x_BP_{pub}$ 和 $P_{pub}=sP$；

②攻击者选择一个恰当的包括 A 和 B 的身份信息、代理权限、代理期限等信息的授权证书 M_ω，随机选择 $r\in Z_q^*$，计算 $e(P,P)^r=G$，$S_\omega'=\alpha^{-1}Y_AH_2(M_\omega,G,PK_A)+rP$，将 (S_ω',M_ω,G) 发送给 B；

③B 收到 (S_ω',M_ω,G) 后，开始验证等式 $e(X_A,P_{pub})=e(Y_A,P)$ 是否成立，再验证等式：

$$\begin{aligned}e(S_\omega',P)&=e(\alpha^{-1}Y_AH_2(M_\omega,G,PK_A)+rP,P)\\&=e(\alpha^{-1}x_AsQ_A,P)^{H_2(M_\omega,G,PK_A)}e(P,P)^r\\&=e(Q_A,Y_A)^{H_2(M_\omega,G,PK_A)}G\end{aligned}$$

等式成立。至此，恶意的攻击者 KGC 成功地伪造了对 B 的代理授权。B 计算代理密钥 $S_p'=S_\omega'+SK_BH_2(M_\omega,G,PK_A)$，用 S_p' 对消息 m 进行代理盲签名，可以验证最终的签名验证等式是成立的。

(2)普通的攻击者 C 作为消息接受者，可以伪造一系列代理盲签名，具体过程如下：

攻击者 C 随机选择 $P^*\in_RG_1$，$a\in_RZ_q^*$，计算 $Q^*=a^{-1}PU'=e(P,P^*)^{a^{-1}}$，$c^*=H_2(m,U') \bmod q$，$V^*=T^{H_2(M_\omega,G,PK_A)c^*}$，$S^*=P^*$，其中 $T=e(Q_A,Y_A)e(Q_B,Y_B)$，事实上，攻击者成功地伪造了一组关于消息 m 的代理盲签名 $\sigma=(S^*,c^*,Q^*,V^*)$。因为：

$$\begin{aligned}&H_2(m,e(S^*,Q^*)T^{-H_2(M_\omega,G,PK_A)c^*}V^*)\\&=H_2(m,e(P^*,a^{-1}P)T^{-H_2(M_\omega,G,PK_A)c^*}T^{H_2(M_\omega,G,PK_A)c^*})\\&=H_2(m,U')=c^*\end{aligned}$$

(3)恶意的 KGC 与 A 联合可计算出代理密钥

KGC 选取参数 $P=tQ_B$，$t\in Z_q^*$，其它参数不变，因为 $SK_B=x_BD_B=x_BsQ_B=x_Bst^{-1}P=t^{-1}Y_B$，KGC 与 A 联合起来计算出代理密钥 $S_p=S_\omega+t^{-1}Y_BH_2(M_\omega,G,PK_A)$。

4 改进的无证书代理盲签名方案及安全性分析

方案[12]不能抵抗恶意的 KGC 攻击，原因是 KGC 可以通过预先设定系统参数，令 $P=\alpha Q_A$，产生系统公钥和原始签名者 A 的公钥，可以成功伪造出有效的 S_ω'，即成功伪造代理授权。为了抵抗这类攻击，可以将用户身份与其公钥用哈希函数绑定，也就是把 $H_1(ID_A)$ 改为 $H_1(ID_A,PK_A)$，把 $H_1(ID_B)$ 改为 $H_1(ID_B,PK_B)$，这样可以保证先生成系统公钥和用户公钥，然后产生部分私钥，从而可以避免 KGC 对参数 P 的特定选取。

4.1 改进的方案

(1)系统初始化。G_1,G_2 分别是阶为 q 的循环加法群和循环乘法群，P 是 G_1 的生成元，$e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射，选择两个安全的哈希函数：$H_1:\{0,1\}^*\times G_1\rightarrow Z_q^*$，$H_2:\{0,1\}^+\rightarrow Z_q^+$，$H_3:\{0,1\}^*\times G_1\rightarrow Z_q^*$，随机选择系统主密钥 $s\in Z_q^*$，并计算系统公钥 $P_{pub}=sP$，公开参数 $params=\{G_1,G_2,P,q,e,H_1,H_2,P_{pub}\}$。

(2)公钥生成。A 分别随机选取秘密值 $x_A\in Z_q^*$，并计算 $X_A=x_AP$，$Y_A=x_AP_{pub}$，A 的公钥为 $PK_A=(X_A,Y_A)$。

(3)用户密钥提取。原始签名人 A 将其身份信息 ID_A 发送给 KGC，KGC 计算 $Q_A=H_1(ID_A,PK_A)$，$D_A=sQ_A$，D_A 为 A 的部分私钥，并通过安全信道分别发送给 A。A 可以通过验证等式 $e(D_A,P)=e(Q_A,P_{pub})$ 是否成立来判断部分私钥的正确性。A 计算 $SK_A=x_AD_A$ 后将其作为自己的私钥。同理，代理签名者 B 的公钥、私钥生成方法与 A 的相同，即公钥 $PK_B=(X_B,Y_B)$，私钥为 (SK_B,D_B)。

(4)代理授权。首先生成一个包括双方身份、代理权限、代理期限等信息的授权证书 M_ω，A 随机选择 $r\in Z_q^*$，计算 $e(P,P)^r=G$，$S_\omega=SK_A+H_2(M_\omega,G,PK_A)rP$，将 (S_ω,M_ω,G) 通过安全信道发给 B。B 收到 (S_ω,M_ω,G) 后，首先通过验证

等式$e(X_A,P_{pub})=e(Y_A,P)$是否成立来验证A的公钥是否有效。再验证等式$e(S_\omega,P)=e(Q_A,Y_A)G^{H_2(M_\omega,G,PK_A)}$是否成立，若等式成立，则计算代理密钥$S_p=S_\omega+SK_B$。

(5)代理盲签名阶段。

①代理签名者B随机选取$P'\in_R G_1$，计算$k=e(P,P')$，将k发送给用户C；

②C随机选择$a,b\in_R Z_q^*$，$P^*\in G_1$，计算$U=k^a e(P,P^*)^b$，$h=H_3(m,U) \bmod q$，$h'=a^{-1}h$，并将h'发送给B；

③B收到h'后，计算$S'=h'S_p+P'$，并将S发送给C；

④C收到S后，计算$S=aS'+bP^*$，$\sigma=(M_\omega,U,G,S)$就是关于消息m的代理盲签名。

(6)代理盲签名的验证。签名验证者首先计算$h=H_3(m,U)$，然后验证等式$H_3(m,e(S,P)T^{-h}G^{-hH_2(M_\omega,G,PK_A)})=h$是否成立，其中$T=e(Q_A,Y_A)e(Q_B,Y_B)$，若等式成立则接受该签名，否则拒绝。

4.2 安全性分析

(1)可验证性

证明：

$$\begin{aligned}
&H_3(m,e(S,P)T^{-h}G^{-hH_2(M_\omega,G,PK_A)})\\
&=H_3(m,e(aS'+bP^*,P)T^{-h}G^{-hH_2(M_\omega,G,PK_A)})\\
&=H_3(m,e(h'S_p+P',P)^a e(P^*,P)^b T^{-h}\\
&\quad G^{-hH_2(M_\omega,G,PK_A)})\\
&=H_3(m,e(S_\omega+SK_B,P)^{ah'}e(P',P)^a e(P^*,P)^b T^{-h}\\
&\quad G^{-hH_2(M_\omega,G,PK_A)})\\
&=H_3(m,e(S_\omega,P)^h e(SK_B,P)^h e(P',P)^a e(P^*,P)^b\\
&\quad T^{-h}G^{-hH_2(M_\omega,G,PK_A)})\\
&=H_3(m,T^h G^{hH_2(M_\omega,G,PK_A)}k^a e(P^*,P)^b T^{-h}\\
&\quad G^{-hH_2(M_\omega,G,PK_A)})\\
&=H_3(m,U)=h
\end{aligned}$$

(2)不可伪造性

在文献[12]对原方案安全性分析的基础上，本文只从无证书代理盲签名方案的两类攻击即公钥替换攻击和恶意但被动的KGC攻击两个方面来分析新方案的安全性。

攻击者要想通过公钥替换攻击成功地伪造代理授权，那么公钥需满足等式$e(X_A,P_{pub})=e(Y_A,P)$，$e(S_\omega,P)=e(Q_A,Y_A)G^{H_2(M_\omega,G,PK_A)}$，无法求得这样的公钥，所以无法通过替换公钥来伪造代理授权。同样，也无法通过替换公钥来伪造代理盲签名。

恶意的KGC要想成功地伪造代理授权，先设定特殊的参数P，令$P=\alpha Q_A=\alpha H_1(ID_A,PK_A)$或者$P=\alpha Q_B=\alpha H_1(ID_B,PK_B)$，但在公钥未产生前是不可能的。因此，方案能够抵抗恶意但被动的KGC攻击。

(3)盲性

对于一个给定的消息签名对(m,M_ω,U,G,S)，代理签名者即使在签名过程中保存了(h',S')，也无法从$h'=a^{-1}h$和$S=aS'+bP^*$这两个等式中计算出盲化因子a,b，从而无法知道消息m的真实内容。因此，新方案具有盲性。

(4)不可否认性

因为授权证书M_ω包括A和B的身份信息、代理权限、代理期限等内容，所以一旦代理盲签名有效，那么原始签名者和代理签名者都不可以否认自己的签名。

(5)可区分性

由于验证等式中既包含原始签名者的公钥，又有代理签名者的公钥，授权证书M_ω也出现在验证等式中，因此可以将原始签名者和代理签名者区分开。

结束语 本文通过对文献[12]提出的无证书代理盲签名方案进行安全性分析，发现原方案不能抵抗恶意的KGC攻击，也不能抵抗普通攻击者的签名伪造攻击，而且KGC和原始签名者联合可以求得代理密钥证书。针对这些问题，提出了一种改进的代理盲签名，且新方案具有更高的安全性。

参 考 文 献

[1] Al-Riyami S, Paterson K. Certificateless public key cryptography [M] // Laih C S, ed. Advances in Cryptology-ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452-473

[2] Zhou Cai-xue. Cryptanalysis and improvement of three ceritificateless signature schemes[J]. Computer Engineering, 2012, 38(19): 114-118(in Chinese)
周才学. 三个无证书签名方案的密码学分析与改进[J]. 计算机工程, 2012, 38(19): 114-118

[3] Wang Sheng-bao, Liu Wen-hao, Xie Qi. Certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2012, 33(4): 93-98(in Chinese)
王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J]. 通信学报, 2012, 33(4): 93-98

[4] Chaum D. Blind Signatures for Untraceable Payments[C]// Advance in Cryptology: Proceedings of Crypto'82. 1983: 199-203

[5] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]// Proceedings of 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996: 48-57

[6] Lin W D, Jan J K. A security personal learning tools using a proxy blind signature scheme[C]// Proc of International Conference on Chinese Language Computing. 2000: 273-277

[7] Song Min, Zhang Yue-gong. An improved certificateless proxy blind signature scheme[C]// Proceedings of the 14th IEEE Conference on Communication Technology (ICCT). 2012: 645-649

[8] Zhang Bi-jun, He Ming-xing. An e-voting scheme based on proxy blind signature [J]. Journal of Xihua University (Natural Science), 2013, 32(4): 10-13(in Chinese)
张碧军, 何明星. 一个基于代理盲签名的电子选举方案[J]. 西华大学学报(自然科学版), 2013, 32(4): 10-13

[9] Zhang Ying-ying, Chen Wei, Zeng Ji-wen. Analysis and improvement of a certificateless proxy blind signature[J]. Application Research of Computers, 2014, 31(2): 540-542(in Chinese)
张瑛瑛, 陈玮, 曾吉文. 对一个无证书代理盲签名方案的分析与改进[J]. 计算机应用研究, 2014, 31(2): 540-542

[10] Huang Juan, Du Wei-zhang. Certificateless proxy blind signature scheme[J]. Computer Engineering and Applications, 2011, 47(31): 73-75(in Chinese)
黄隽, 杜伟章. 无证书代理盲签名方案[J]. 计算机工程与应用, 2011, 47(31): 73-75

[11] Zhang J Z, Yang L. Cryptography analysis and improvement on certificateless proxy blind signature scheme[J]. Computer Engineering and Applications, 2014, 50(4): 90-93(in Chinese)
张建中, 杨丽. 无证书代理盲签名方案的密码学分析与改进[J]. 计算机工程与应用, 2014, 50(4): 90-93, 156

[12] Zhang Xiao-min. An efficient certificateless proxy blind signature scheme[J]. Computer Security, 2011(3): 54-59(in Chinese)
张晓敏. 一类高效的无证书代理盲签名方案[J]. 计算机安全, 2011(3): 54-59