一种新的无证书代理签名方案的分析与改进

申军伟[1],杨晓元[1,2],梁中银[1],陈海滨[1]
SHEN Jun-wei[1],YANG Xiao-yuan[1,2],LIANG Zhong-yin[1],CHEN Hai-bin[1]

1.武警工程学院,西安 710086
2.西安电子科技大学 网络信息安全教育部重点实验室,西安 710071
1.Engineering College of Armed Police Force,Xi'an 710086,China
2.Key Laboratory of Network & Information Security of the Ministry of Education,Xidian University,Xi'an 710071,China
E-mail:jhkplwfnsjw@163.com

SHEN Jun-wei,YANG Xiao-yuan,LIANG Zhong-yin,et al.Security analysis and improvement of new certificateless proxy signature.Computer Engineering and Applications,2010,46(8):96-98.

Abstract: This paper analyzes the security of a new certificateless proxy signature proposed by Fan Rui recently.The security of Fan Rui's scheme relies on the CDH problem.It shows that Fan's proxy signature reveals the private key of original signer and is insecure against a key replacement attack and malicious-but-passive KGC attack.It also gives a modified scheme.The improvement is secure against the key replacement attack and the malicious-but-passive KGC attack.This paper elaborately eliminates the defect of the original scheme and improves the efficiency of the protocol.

Key words: certificateless public key cryptography;proxy signature;public key replacement attack;Key Generation Center(KGC);malicious-but-passive KGC attack

摘 要: 樊睿等人提出了一种新的无证书代理签名方案,该方案的安全性是基于 CDH 困难性假设。对该代理签名方案进行了安全性分析,指出该方案不仅泄露了原始签名者的私钥,而且不能抵抗替换公钥攻击和恶意但被动的 KGC 攻击,从而不满足代理签名的安全性要求。同时提出了一个改进方案,改进方案不仅弥补了原方案的安全缺陷,而且改善了协议的性能。

关键词: 无证书公钥密码体制;代理签名;替换公钥攻击;密钥生成中心;恶意但被动的 KGC 攻击
DOI: 10.3778/j.issn.1002-8331.2010.08.027 **文章编号:** 1002-8331(2010)08-0096-03 **文献标识码:** A **中图分类号:** TP309

在传统的公钥密码体制(PKI)中,用户的公钥需要用可信第三方签名的证书来保证其可靠性, 而 Shamir 提出的基于身份的密码体制[1]尽管解决了证书管理问题,但不可避免地存在密钥托管问题。Al-Riyami 和 Paterson[2]在 Asiacrypt2003 上提出了无证书公钥密码体制。在这个密码体制中,有一个拥有主密钥的密钥生成中心(KGC)。KGC 产生与用户身份对应的部分私钥,并将其通过安全信道传输给用户。然后,用户通过部分私钥和一些秘密信息生成实际的用户私钥,这样就有效解决了基于身份密码体制中的密钥托管问题。而且,用户利用 KGC 的公开参数和用户的秘密信息产生公钥。因此,不再需要使用证书来保证公钥的可靠性,解决了基于证书的密码体制中证书的存储和管理问题。

2005 年,Li 等人给出了构造一个无证书代理签名方案[3],但该方案已被证明是不安全的。最近,樊等人[4]也提出了一个新的无证书代理签名方案,说明了方案满足代理签名所要求的所有性质。该文对此方案进行了安全性分析,指出了方案不满足不可伪造性,不能抵抗替换公钥攻击和恶意的 KGC 攻击[5]。针对方案的安全缺陷,提出一个改进方案,改进后的方案能够抵抗伪造攻击,克服了原方案的缺陷,满足代理签名方案的安全性要求。

1 双线性映射

设 G_1 与 G_2 是两个阶为 q 的循环群,q 为大素数, 其中 G_1 是以加法的形式表示的,G_2 是以乘法的形式表示的。P 为 G_1 的生成元。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。若映射 $e:G_1\times G_1\rightarrow G_2$ 满足下列性质则此映射称为双线性映射。

(1)双线性:对于所有的 $P,Q,R\in G_1$ 和 $a,b\in Z_p$,有

$e(P+Q,R)=e(P,R)e(Q,R)$

$e(aP,bQ)=e(P,Q)^{ab}$

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

(3)可计算性:对于所有的 $P,Q\in G_1$,存在一个有效的算法计算 $e(P,Q)$。

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60573032)。

作者简介: 申军伟(1984-),男,助教,主要研究方向:信息安全;杨晓元,男,教授,主要研究方向:信息安全,密码学;梁中银,男,硕士研究生,主要研究方向:信息安全;陈海滨,男,硕士研究生。

收稿日期: 2008-09-18 **修回日期:** 2008-12-22

2 樊等人的无证书代理方案

2.1 系统设置

G_1 和 G_2 是两个阶为 q 的循环群,$P\in G_1$ 作为 G_1 的生成元,定义 3 个密码学上的单向哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\times G_1\rightarrow Z_q^*$,$H_3:G_1\rightarrow Z_q^*$。最后,KGC 选择 $s\in_R Z_q^*$ 作为自己的私钥,计算公钥 $P_{pub}=sP$,将 s 秘密保存,公开系统参数:$params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2,H_3\}$。

2.2 密钥提取

KGC 分别生成用户 A 和 B 的部分私钥 $D_A=sQ_A$,$D_B=sQ_B$,并通过安全信道传送给 A 和 B。原始签名人 A 和代理签名人 B 分别产生公私钥,A 的私钥为 $S_A=x_AD_A$,公钥为 $P_A=<X_A,Y_A>=<x_AP,x_AP_{pub}>$;$B$ 的私钥为 $S_B=x_BD_B$,公钥为 $P_B=<X_B,Y_B>=<x_BP,x_BP_{pub}>$。

2.3 代理授权

A 建立一个授权许可信息 m_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 计算一个短签名 $S_w=S_AH_3(H_1(m_w))$,将(S_w,m_w)发送给 B。B 首先验证等式 $e(X_A,P_{pub})=e(Y_A,P)$是否成立来验证 A 的公钥,若成立说明 A 的公钥正确,然后验证等式 $e(S_w,P)=e(Q_A,Y_A)^{H_3(H_1(m_w))}$是否成立。如果成立,$B$ 计算代理签名密钥:$S_P=S_w+H_3(H_1(m_w))S_B=H_3(H_1(m_w))(S_A+S_B)$。

2.4 签名

当要对消息 m 签名时,代理签名人 B 选择 $a\in_R Z_q^*$,计算 $r=e(P,P)^a$,$v=H_2(m,r)$,$U=vS_P+aP$,则(U,v,m_w)为 B 对 m 的代理签名。

2.5 验证

验证者首先验证等式 $e(X_A,P_{pub})=e(Y_A,P)$和 $e(X_B,P_{pub})=e(Y_B,P)$来验证 A、B 的公钥。然后计算 $Q_A=H_1(ID_A)$,$Q_B=H_1(ID_B)$,$r=e(U,P)[e(Q_A,-Y_A)\ e(Q_B,-Y_B)]^{vH_3(H_1(m_w))}$,验证等式 $v=H_2(m,r)$,若成立则接受签名,否则拒绝。

3 樊方案安全性分析

3.1 代理授权阶段的安全缺陷

代理签名者 B 可以从原始签名者 A 的授权签名中得到原始签名者 A 的私钥 S_A。

由于哈希函数 H_1 将 m_w 映射为群 G_1 中元素,H_3 将 G_1 元素映射为 Z_q^* 中元素,而 $S_w=S_AH_3(H_1(m_w))$,B 可以通过计算 $S_A=S_wH_3(H_1(m_w))^{-1}$ 得到原始签名者的私钥,这样 B 可以随意伪造原始签名人的授权签名,从而代表 A 生成任意权限的代理签名而不会被追究任何责任。

3.2 替换公钥攻击

代理签名方案不能抵抗替换公钥攻击。类型 I 攻击者没有系统主私钥 s,但是攻击者可以用他选择的公钥替换被攻击者的公钥,替换攻击成功后攻击者可以对任意消息进行签名。

签名:对消息 m 和授权信息 m_w 进行签名,类型 I 攻击者按以下步骤执行:

(1)随机选择 $U\in G_1$ 并计算 $h=H_3(H_1(m_w))$;

(2)随机选择 $k\in Z_q^*$ 并计算

$r=e(U,P)[e(-Q_A,P_{pub})e(-Q_B,kP_{pub})]^h$

(3)计算 $v=H_2(m,r)$;

(4)令 $x_A=v^{-1}$ 和 $x_B=k\cdot v^{-1}$;

(5)计算 $X_A'=x_AP$,$Y_A'=x_AP_{pub}$,$X_B'=x_BP$,$Y_B'=x_BP_{pub}$;

(6)用$<X_A',Y_A'>$,$<X_B',Y_B'>$分别替换 A 和 B 的公钥;

(7)返回代理签名(U,v,m_w)。

上述代理签名是有效的,因为代理签名可以通过验证方程,证明如下:

(1)验证者验证 $e(X_A',P_{pub})=e(Y_A',P)$和 $e(X_B',P_{pub})=e(Y_B',P)$成立。因为

$e(X_A',P_{pub})=e(x_AP,P_{pub})=e(x_AsP,P)=e(Y_A',P)$

$e(X_B',P_{pub})=e(x_BP,P_{pub})=e(x_BsP,P)=e(Y_B',P)$

(2)验证者计算

$r'=e(U,P)[e(Q_A,-Y_A)\ e(Q_B,-Y_B)]^{vH_3(H_1(m_w))}$

(3)验证者接受签名当且仅当 $v=H_2(m,r')$。

$$r'=e(U,P)[e(Q_A,-Y_A)\ e(Q_B,-Y_B)]^{vH_3(H_1(m_w))}=$$
$$e(U,P)[e(Q_A,-x_AP_{pub})e(Q_B,-x_BP_{pub})]^{vh}=$$
$$e(U,P)[e(Q_A,-P_{pub})e(Q_B,-kP_{pub})]^{v^{-1}vh}=$$
$$e(U,P)[e(Q_A,-P_{pub})e(Q_B,-kP_{pub})]^{h}=r$$

所以 $v=H_2(m,r')$成立,替换公钥攻击成功,攻击者可以在没有得到原始签名者授权的情况下伪造 B 的任意有效的代理签名。

3.3 Malicious-but-Passive KGC 攻击

恶意的 KGC 针对特定的用户生成特定的系统参数,在用户生成公钥公布后,KGC 就可以利用系统参数的特殊性和用户公钥经过计算得到用户的私钥。

恶意的 KGC 可以按以下步骤对方案进行攻击:

(1)当原始签名人 A 向 KGC 申请部分私钥时,KGC 令 $P=\alpha H(ID_A)$,$\alpha\in_R Z_q$,生成系统参数和部分私钥 $Q_A=H_1(ID_A)$,$D_A=sQ_A$。

(2)A 得到部分私钥后计算私钥 $S_A=x_AD_A=x_AsQ_A$,公钥 $X_A=x_AP$,$Y_A=x_AP_{pub}$,然后公开公钥 $P_A=<X_A,Y_A>$。

(3)KGC 得到 A 的公钥后计算

$\alpha^{-1}Y_A=\alpha^{-1}x_AP_{pub}=\alpha^{-1}x_AsP=\alpha^{-1}x_As\alpha H(ID_A)=x_AsQ_A=S_A$

从而得到用户 A 的私钥 S_A,KGC 可以任意伪造用户 A 的授权签名。

4 改进方案

4.1 系统设置

与 3.1 节参数设置类似。

4.2 密钥提取

原始签名人 A 随机选择秘密值 x_A,然后计算并公开公钥 $P_A=X_A=x_AP$,KGC 分别生成用户 A 的部分私钥 $D_A=sQ_A=sH_1(ID_A\parallel X_A)$,并通过安全信道传送给 A,A 秘密保存其私钥为(x_A,D_A)。代理签名者通过相同的步骤生成其私钥(x_B,D_B)和公钥 $P_B=X_B$。

4.3 代理授权

A 生成一个授权许可信息 m_w 来说明包含 A 和 B 的身份信息的授权关系及其 B 的权限。A 计算 $S_w=D_A+x_AH_1(m_w\parallel X_A\parallel X_B)$,将$(S_w,m_w)$发送给 B。B 验证等式 $e(S_w,P)=e(Q_A,P_{pub})\cdot e(H_1(m_w\parallel X_A\parallel X_B),X_A)$是否成立,若成立 B 计算代理签名密钥 $S_P=S_w+D_B+x_BH_1(m_w\parallel X_A\parallel X_B)$。

4.4 代理签名

当要对消息 m 签名时，代理签名人 B 选择 $a\in {}_RZ_q^*$，计算 $r=e(P,P)^a$，$v=H_2(m_w,m,r)$，$U=vS_P+aP$，则 (U,v,m_w) 为 B 对 m 的代理签名。

4.5 验证

验证者首先计算 $Q_A=H_1(ID_A\|X_A)$，$Q_B=H_1(ID_B\|X_B)$，$r=e(U,P)[e(-Q_A-Q_B,P_{pub})e(-H_1(m_w\|X_A),X_A)e(-H_1(m_w\|X_B),X_B)]^v$，然后验证等式 $v=H_2(m_w,m,r)$，若成立则接受签名，否则拒绝。

5 安全性分析

5.1 正确性

$$
\begin{aligned}
r=&e(U,P)[e(-Q_A-Q_B,P_{pub})\ e(-H_1(m_w\|X_A\|X_B),X_A)\ e(-H_1(m\|m_w\|X_A\|X_B),X_B)]^v=\\
&e(vS_P+aP,P)[e(-Q_A-Q_B,P_{pub})e(-H_1(m_w\|X_A\|X_B),X_A)e(-H_1(m\|m_w\|X_A\|X_B),X_B)]^v=\\
&e(S_w+D_B+x_BH_1(m\|m_w\|X_A\|X_B),P)^v[e(-Q_A-Q_B,P_{pub})e(-H_1(m_w\|X_A\|X_B),X_A)e(-H_1(m\|m_w\|X_A\|X_B),X_B)]^v=\\
&e(S_w+D_B,P)^v[e(-Q_A-Q_B,P_{pub})e(-H_1(m_w\|X_A\|X_B),X_A)]^ve(P,P)^a=\\
&e(D_A+x_AH_1(m_w\|X_A\|X_B)+D_B,P)^v[e(-Q_A-Q_B,P_{pub})e(-H_1(m_w\|X_A\|X_B),X_A)]^ve(P,P)^a=e(P,P)^a
\end{aligned}
$$

所以验证等式 $v=H_2(m_w,m,r)$ 成立。

5.2 不可伪造性

因为授权过程在随机预言机模型下可以抵抗适应性选择消息攻击模式的存在性伪造和 ID 攻击，所以任意第三方不可能伪造对证书 m_w 的签名 (m_w,S_w)。同时方案中代理签名密钥是由 A 的授权签名和 B 的私钥共同组成，所以除了 B 以外的任何人都无法生成合法的代理签名密钥。

用户首先产生了秘密值 x_{ID} 和公钥 X_{ID}，随后在 KGC 产生部分私钥时将用户身份和系统公钥（包含在用户公钥中）一起进行 Hash 运算 $Q_{ID}=H_1(ID_{ID}\|X_{ID})$，这样系统参数必须在用户生成部分私钥之前生成，KGC 不能够针对特定用户生成特定的系统参数。这就抵抗了恶意但被动的 KGC 攻击。

在签名生成过程中将签名者的公钥作为签名的输入部分 $H_2(m_w\|X_A\|X_B)$，攻击者选择 U、v、r 后，就不能再计算公钥，无法完成公钥的替换，避免了公钥替换攻击。

5.3 不可否认性

完整的代理签名中含有授权证书 m_w 及原始签名者的签名，在整个代理签名过程中都有 m_w，代理签名人不可能更改 m_w。所以代理签名人产生了合法有效的代理签名后，将不能否认自己所产生的代理签名。

5.4 可识别性

代理签名中含有授权证书 m_w，所以任何人都能从代理签名中确定相应代理签名人的身份。

5.5 抗滥用性

在代理签名的整个过程中都使用了 m_w，而 m_w 中说明了代理签名人的权限和有效期限。同时代理签名密钥中含有原始签名人和代理签名人的私钥，所以代理密钥不能用于产生有效代理签名以外的其他目的。改进方案防止代理签名人的滥用，同时也可以防止原始签名人的滥用。

6 结束语

对樊等人方案进行了安全性分析，针对原方案的安全缺陷提出了一个改进方案。樊等人方案的密钥生成方式是用 KGC 生成的部分私钥和用户自己选择的秘密值直接相乘，这样 KGC 就可以针对特定的用户设置特定的系统参数从而可以容易得到用户的私钥。改进方案中采用部分私钥和秘密值分开使用，同时用户在 KGC 生成部分私钥之前生成秘密值和公钥，而且将公钥嵌入到部分私钥中，这样就能有效防止恶意的 KGC 攻击和公钥替换攻击，有效提高了方案的安全性能。

无证书公钥密码体制有效解决了基于证书密码体制的证书管理问题和基于身份密码体制的密钥托管问题。所以无证书代理签名方案在电子现金和电子投票等电子商务中具有广阔的应用前景。

参考文献：

[1] Shamir A.Identity-based cryptosystems and signature schemes[C]//LNCS 196:Advances in Cryptology-Crypto'84.Berlin:Springer-Verlag,1985:7-53.

[2] Al-Riyami S,Paterson K.Certificateless public key cryptography[C]//Lecture Notes in Computer Science 2894:Advances in Cryptology Proceeding of Asiacrypt 2003.Berlin:Springer-Verlag,2003:452-473.

[3] Li X,Chen K,Sun L.Certificateless signature and proxy signature schemes from bilinear pairings[J].Lithuanian Mathematical Journal,2005,45(1):76-83.

[4] Fan Rui,Wang Cai-fen,Lan Cai-hui,et al.A new certificateless proxy signature[J].Computer Application,2008,28(4):915-917.

[5] Au M H,Chen J,Liu J K,et al.Malicious KGC attacks in certificateless cryptography[C/OL]//ASIACCS(2007).http://eprint.iacr.org/2006/255.

（上接 86 页）

新方法也存在一些不足，如未解决单个组件安全强度的调整对网络系统整体安全性的影响这一问题，因此这也是下一步需要完善及发展的方向。

参考文献：

[1] 段云所，刘欣，陈钟.信息系统组合安全强度和脆弱性分析[J].北京大学学报，2005,41(3):484-490.

[2] McAllister R K,Coyle J L.Interdependency analysis[C]//22nd NIST-NCSC National Information Systems Security Conference,1999:403-414.

[3] Almerhag I A,Woodward M E.Security as a quality of service routing problem[C]//International Conference on Emerging Networking Experiments and Technologies,2005.

[4] 闫强.信息系统安全评估研究[D].北京：北京大学，2003.

[5] 闫强，段云所，唐礼勇，等.信息系统中组件组合的安全评估问题研究[J].计算机工程与应用，2003,39(2):1-3.