对一种基于身份的已知签名人的门限代理签名方案的分析

鲁荣波[①②]　何大可[②]　王常吉[③]
[①](吉首大学数学与计算机科学学院　吉首　416000)
[②](西南交通大学信息安全与国家计算网格实验室　成都　610031)
[③](中山大学计算机科学系　广州　510275)

摘　要：在TAMC'06上，Bao等人以双线性对为工具，首次提出了一种基于身份的已知签名人的门限代理签名方案(以下标记为BCW方案)，并得出了满足强不可伪造性以及原始签名人发送签名了的授权证书时并不需要安全信道等安全性结论。本文对BCW方案进行了安全性分析，成功地给出了一种攻击，攻击者通过公开渠道获得一个合法的原始签名人发送给代理签名人的签名了的授权证书以及代理签名人已经生成的一个有效的代理签名后，能够伪造出一个新的对相同消息的代理签名，而原始签名人变为攻击者自己。由于验证者并不能验证代理签名人到底是代表谁生成了代理签名, 这样，攻击者就获得了与合法原始签名人相同的权益。为了避免这种攻击，本文提出了改进的措施，分析表明，改进措施能有效地弥补了该方案的安全缺陷。

关键词：门限代理签名；代理签名；基于身份的公钥体系；不可伪造性；分布式计算
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2008)01-0100-04

Cryptanalysis of an Identity-Based Threshold Proxy Signature Scheme with Known Signers

Lu Rong-bo[①②]　He Da-ke[②]　Wang Chang-ji[③]
[①](*College of Mathematics and Computer Science*, *Jishou University*, *Jishou* 416000, *China*)
[②](*Laboratory of Information Security and National Computing Gird*, *Southwest Jiaotong University*, *Chengdu* 610031, *China*)
[③](*Department of Computer Science*, *Sun Yat-Sen University, Guangzhou* 510275, *China*)

Abstract: In TAMC' 06, Bao *et al.* proposed a new identity-based threshold proxy signature with known signers from the bilinear pairings (denoted as BCW scheme) for the first time. As for the security, they claimed their scheme satisfies the security requirements of proxy signature such as strong unforgeability and their scheme need not the secure channel for the delivery of the signed warrant and etc.. In this paper, however, an attack against their scheme is presented. That is, based on the proxy signature generated by proxy signers on a message on behalf of an original signer, an attacker can forge a valid threshold proxy signature on the same message which seemed generated by proxy signers on behalf of this attacker himself. After production a forged proxy signature, the attacker has the same authority with the original signer to the proxy signer, and the verifier cannot distinguish that which one is the real original signer. To thwart this attack, an improvement measure is further proposed, which can resolve the security problem existing in this scheme.

Key words: Threshold proxy signature; Proxy signature; Identity-based public key cryptography; Unforgeability; Distributed computing

1　引言

目前，人们已经提出了若干不同类型的代理签名方案[1−4]。在代理签名中引入秘密分存就形成了门限代理签名[4]。(t,n) 门限代理签名就是将一个代理签名密钥分成 n 份子代理签名密钥，n 个代理签名人分别拥有各自的子代理密钥。各代理签名人利用自己的分存子代理密钥生成部分代理签名，当部分代理签名的个数大于或等于 t 时，这些部分代理签名按着某种方式结合，产生了有效的门限代理签名。在分布式计算环境下，门限代理签名在许多领域都有着重要的应用，如电子支票的分发等。

在目前广泛使用的公开密钥体系中，用户的公钥分配是使用证书(Certificate)来实现，证书中包含用户的公钥、ID以及权威机构的签名等。基于证书的公钥体系得到广泛的应用，但也存在如用户必须依赖于CA(Certificate Authority)

2006-08-17 收到，2006-12-25 改回
国家自然科学基金(60503005)和湖南省自然科学基金(03JJY6017)资助课题

的第三方服务；用户可能用自己的公钥替换别人的公钥；接收方在解密密文前不能够鉴别发送方的身份等缺陷。为了避开复杂的证书管理，Shamir最早提出了利用用户的身份直接推导用户公钥的思想[5]，之后又有学者进行了深入的研究[6]。在基于身份的公钥体系中，用户的ID就相当于用户的公钥，这样就不存在CA这样的权威机构，也不需要专门的目录来存放证书，因此，大大降低了管理成本。

最近，在TAMC'06上，Bao等人首次提出了一种已知签名人的基于身份的门限代理签名方案[7](以下标记为BCW方案)，并得出了他们的方案满足代理签名的安全需求如强不可伪造性、强可识别性、强不可否认性、可区分性、防止滥用性，能够抵御各种可能的攻击以及原始签名人发送签名了的代理授权证书并不需要安全信道等安全性结论。本文给出了对BCW方案的一种攻击，在代理签名人代表一个合法原始签名人生成有效的代理签名后，攻击者只要获得该原始签名人通过公开信道发送给代理签名人的签名了的授权证书，就可以伪造一个对相同消息的代理签名，而原始签名人变为攻击者自己。由于验证者并不能验证代理签名人到底是代表谁生成了代理签名, 这样，攻击者就可能获得与合法原始签名人相同的权益。为了避免这种攻击，本文提出改进的措施，分析表明，改进措施能够有效地弥补BCW方案存在的安全缺陷。

2　预备工作

2.1 双线性映射

设 G_1，G_2 分别是同为 q 阶的加群和乘群，P 为 G_1 的生成元。假设在群 G_1，G_2 中，离散对数问题是难解的。可定义双线性映射为 $e: G_1 \times G_1 \to G_2$，满足双映射性、非退化性及可计算性等特性[8]。对于这样定义的 G_1，可以定义以下难解问题：

(1)离散对数问题(DLP)　给定 G_1 中的两个元素 P 和 Q，寻找整数 $n \in Z_q^*$，使得 $Q = nP$ 成立。

(2)计算 Diffie-Hellman(CDH)问题　给定 P, aP, bP, 这里 $a,b \in Z_q^*$，计算 abP。

(3)判定 Diffie-Hellman(DDH)问题　给定 P, aP, bP, cP, 这里 $a,b,c \in Z_q^*$，判定是否存在 $c = ab \bmod q$。

(4) Gap Diffe-Hellman(GDH)问题　CDH 问题难解而 DDH 问题易解，称具有这种特征的群为 GDH 群。

有关双线性映射以及GDH群的构造，可参看文献[8]。

2.2 基于身份和双线性对的密码系统

(1)建立私钥生成中心PKG选取加群 G_1 和乘群 G_2，它们的阶均为大素数 q，P 为 G_1 的生成元，$e: G_1 \times G_1 \to G_2$ 为安全的双线性映射，$H_1: \{0,1\}^* \to Z_q$ 及 $H_2: \{0,1\}^* \to G_1$ 为两个安全的Hash函数。PKG 随机选择 $s \in Z_q^*$，计算 $P_{\text{pub}} = sP$, 秘密保存 s 为系统主密钥(Master-key)。公开 $\{G_1, G_2, e, q, P, P_{\text{pub}}, H_1, H_2\}$。

(2) 加入用户首先发送其身份信息ID及相应的知识证明给PKG。PKG计算用户的私钥 $S_{\text{ID}} = sQ_{\text{ID}} = sH_2(\text{ID})$, 并通过安全信道发送给用户。

3　BCW 方案

3.1 系统设置

系统设置同2.2节(1)。

3.2 私钥获取

原始签名人Alice的身份为 ID_0，PKG为其产生私钥 $S_0 = sQ_0 = sH_2(\text{ID}_0)$，代理签名组为 $L = \{P_1, P_2, \cdots, P_n\}$, P_i 的身份为 ID_{P_i}，PKG为其产生私钥 $\{S_{P_i} = sQ_{P_i} = sH_2(\text{ID}_{P_i})\}$。

3.3 代理密钥生成

第1步　Alice 随机选择 $k \in Z_q^*$，计算 $r_0 = e(P,P)^k$, $h_1 = H_1(m_w, r_0)$, $V = h_1 S_0 + kP$。其中 m_w 为代理证书。Alice将 (m_w, r_0, V) 发送给每个代理签名人。

第 2 步　每个 $P_i \in L$ 验证 $e(V,P) = e(h_1 S_0 + kP, P) = e(h_1 Q_0, P_{\text{pub}}) r_0$ 是否成立，若成立，则接收 (m_w, r_0, V)。并随机选择 $k_i \in_R Z_q^*$，计算 $r_i = e(P,P)^{k_i}$，广播 r_i。P_i 计算 $r_p = \prod_{i=1}^{n} r_i$, $h_2 = H_1(r_p)$，计算 $s_i = n^{-1}V + h_2 S_{P_i} + k_i P$ 并作为自己的代理秘密。

第3步　$P_i \in L$ 任选 $t-1$ 次多项式 $f_i(z) = s_i + a_{i1}z + a_{i2}z + \cdots a_{it-1}z^{t-1}$，满足 $f_i(0) = s_i = a_{i0}$。其中 $a_{ij} \in G_1$，$j = 1, \cdots, t-1$。P_i 计算并广播 $A_{ij} = e(P, a_{ij})$ $(j = 1, \cdots, t-1)$, 秘密发送 $f_i(j)$ 给其余代理签名人 P_j $(j = 1, \cdots, n; j \neq i)$。

第4步　代理签名人 P_i 从 P_j 那里收到 $f_j(i)$ $(j = 1, \cdots, n; j \neq i)$ 后通过验证式 $e(P, f_j(i)) = \prod_{k=0}^{t-1} A_{jk}{}^{i^k}$ 是否成立来检查 $f_j(i)$ 的有效性。

若检查通过，P_i 计算 $x'_i = \sum_{k=1}^{n} f_k(i)$ 和 $Y_i' = e(P, x'_i)$。其余的代理签名人也可通过计算 $Y_i' = \prod_{j=1}^{n} \prod_{k=0}^{t-1} A_{jk}^{i^k}$ 来得到 Y_i'。若令 $f(z) = \sum_{i=1}^{n} f_i(z)$, 则 $x_i' = f(i)$，对应的 Y_i' 为 $e(P, x_i')$。

3.4 代理签名生成

设 m 为要签名的消息，$p_i (i = 1, 2, \cdots, t)$ 为 t 个代表原始签名人对消息 m 进行代理签名。

第1步　每个 $p_i (i = 1, 2, \cdots, t)$ 计算 $w_i = \prod_{j=1, j \neq i}^{t} j/(j-i)$, 得到部分签名：

$$\sigma_i = (x_i' w_i + S_{P_i}) H_1(m) \tag{1}$$

第2步　t 个代理签名人一起验证：

$$\begin{aligned} e(P, \sigma_i) &= e(P, (x_i' w_i + S_{P_i}) H_1(m)) \\ &= Y_i'^{w_i H_1(m)} e(P_{\text{pub}}, Q_{P_i})^{H_1(m)} \end{aligned} \tag{2}$$

若通过验证，则合作产生 $\sigma' = \sum_{i=1}^{t} \sigma_i$。于是得到代理签名为 $(\sigma', m, m_w, r_0, r_P)$。

3.5 代理签名验证

验证者可以用等式 $e(\sigma',P)=e\left(h_1Q_0+\sum_{i=1}^{n}h_2Q_{P_i}+\sum_{i=1}^{t}Q_{P_i},P_{\text{pub}}\right)^{H_1(m)}(r_0r_P)^{H_1(m)}$ 验证 (σ',m,m_w,r_0,r_P) 的有效性，这里 $h_1=H_1(m_w,r_0)$, $h_2=H_1(r_P)$ 。

4 安全性分析

攻击者可以按照下面步骤伪造一个签名 $(\sigma'',m,m_w',r_0',r_P)$ 来冒充代理签名人对消息 m 的签名。

第 1 步 攻击者 Charlie 从 PKG 那里获得私钥 $S_C=sQ_C=sH_2(\text{ID}_C)$，然后生成代理授权证书 m_w'，授权参数与 m_w 相同，其中原始签名人为 Charlie，代理签名人为 $L=\{P_1,P_2,\cdots,P_n\}$, ID_C 为 Charlie 的身份。这里 Charlie 可能是另外一个合法的原始签名人，因此，代理授权证书 m_w' 可能是通过合法途径生成的。

第 2 步 攻击者 Charlie 从公开渠道获得代理签名人生成的代表原始签名人 Alice 生成的合法有效的代理签名 (σ',m,m_w,r_0,r_P) 以及 (m_w,r_0,V) 。

第 3 步 Charlie 随机选择 $k'\in Z_q^*$，计算 $r_0'=e(P,P)^{k'}$, $h_1'=H_1(m_w',r_0')$, $V'=h_1'S_C+k'P$, $\sigma''=\sigma'+(V'-V)H_1(m)$。则 $(\sigma'',m,m_w',r_0',r_P)$ 是一个有效的代理签名。这是因为

$$\begin{aligned}
e(\sigma'',P)&=e(\sigma'+(V'-V)H_1(m),P)\\
&=e\left(\sum_{i=1}^{t}\sigma_i+(V'-V)H_1(m),P\right)\\
&=e\left(\sum_{i=1}^{t}(x_i'w_i+S_{P_i})H_1(m)+(V'-V)H_1(m),P\right)\\
&=e\left(\sum_{i=1}^{t}(x_i'w_i+\sum_{i=1}^{t}S_{P_i})H_1(m)+(V'-V)H_1(m),P\right)\\
&=e\left(\left(f(0)+\sum_{i=1}^{t}S_{P_i}\right)H_1(m)+(V'-V)H_1(m),P\right)\\
&=e\left(\left(\sum_{i=1}^{n}f_i(0)+\sum_{i=1}^{t}S_{P_i}\right)H_1(m)+(V'-V)H_1(m),P\right)\\
&=e\left(\left(nn^{-1}V+\sum_{i=1}^{n}(h_2S_{P_i}+k_iP)+\sum_{i=1}^{t}S_{P_i}\right)\right.\\
&\qquad\left.\cdot H_1(m)+(V'-V)H_1(m),P\right)\\
&=e\left(\left(V'+\sum_{i=1}^{n}(h_2S_{P_i}+k_iP)+\sum_{i=1}^{t}S_{P_i}\right)H_1(m),P\right)\\
&=e\left(\left(h_1'S_C+k'P+\sum_{i=1}^{n}(h_2S_{P_i}+k_iP)\right.\right.\\
&\qquad\left.\left.+\sum_{i=1}^{t}S_{P_i}\right)H_1(m),P\right)\\
&=e\left(\left(h_1'S_C+\sum_{i=1}^{n}h_2S_{P_i}+\sum_{i=1}^{t}S_{P_i}\right)H_1(m),P\right)\\
&\quad e((k'P+k_iP)H_1(m),P)\\
&=e\left(h_1'Q_C+\sum_{i=1}^{n}h_2Q_{P_i}+\sum_{i=1}^{t}Q_{P_i},P_{\text{pub}}\right)^{H_1(m)}(r_0'r_P)^{H_1(m)}
\end{aligned}$$

这里 $h_1'=H_1(m_w',r_0')$, $h_2=H_1(r_P)$ 。

则攻击者 Charlie 就成功地伪造了一个原始签名人为自己，代理签名人为 $L=\{P_1,P_2,\cdots,P_n\}$ 的对消息 m 的门限代理签名 $(\sigma'',m,m_w',r_0',r_P)$，由于验证者并不能验证代理签名人到底是代表谁生成了代理签名。这样，攻击者就获得了与合法原始签名人 Alice 相同的权益。

更进一步，由于在 BCW 方案中签名的授权证书 (m_w,r_0,V) 是通过公开信道发送的，如果 $L=\{P_1,P_2,\cdots,P_n\}$ 有两个分别由 Alice 和 Charlie 签名的授权证书 (m_w,r_0,V) 和 (m_w',r_0',V')，那么任何人都可以把代理签名组 $L=\{P_1,P_2,\cdots,P_n\}$ 代表原始签名人 Alice 对消息 m 生成的代理签名 (σ',m,m_w,r_0,r_P) 转化成一个新的代理签名 $(\sigma',m,m_w',r_0',r_P)$，这里，$\sigma'=\sigma'+(V'-V)H_1(m)$。而原始签名人变为 Charlie。

5 改进措施及分析

BCW 方案不满足强不可伪造性的原因是由于：在代理签名产生过程中，代理签名人并没有使用签名了的授权证书 (m_w,r_0,V)，因此，攻击者可以按照以上攻击步骤通过修改代理签名。因此，为了抵抗以上攻击，只需要对 BCW 方案部分代理签名生成过程进行修改，这里只描述修改部分，其余的同原方案。

在代理签名生成阶段，式 (1) 变为新的等式：$\sigma_i=(x_i'w_i+H_1(m)S_{P_i})H_1(m,m_w)$ 。

相应地，为了验证 σ_i 的有效性，验证等式(2)也变为

$$\begin{aligned}
e(P,\sigma_i)&=e(P,(x_i'w_i+H_1(m)S_{P_i})H_1(m,m_w))\\
&=Y_i'^{w_iH_1(m,m_w)}e(P_{\text{pub}},H_1(m)Q_{P_i})^{H_1(m,m_w)}
\end{aligned}$$

指定秘书计算 $\sigma'=\sum_{i=1}^{t}\sigma_i$ 。最后得到对消息 m 的代签名仍是 (σ',m,m_w,r_0,r_P) 。

在代理签名验证阶段，验证者通过检验以下等式是否成立来验证代理签名 (σ',m,m_w,r_0,r_P) 的有效性：

$$\begin{aligned}
e(\sigma',P)=e\Bigg(&h_1Q_0+\sum_{i=1}^{n}h_2Q_{P_i}\\
&+H_1(m)\sum_{i=1}^{t}Q_{P_i},P_{\text{pub}}\Bigg)^{H_1(m,m_w)}(r_0r_P)^{H_1(m,m_w)}
\end{aligned}$$

等式成立的原因为

$$\begin{aligned}
e(\sigma',P)&=e\left(\sum_{i=1}^{t}\sigma_i,P\right)\\
&=e\left(\sum_{i=1}^{t}(x_i'w_i+H_1(m)S_{P_i})H_1(m,m_w),P\right)\\
&=e\left(\left(\sum_{i=1}^{n}f_i(0)+H_1(m)\sum_{i=1}^{t}S_{P_i}\right)H_1(m,m_w),P\right)\\
&=e\left(\left(nn^{-1}V+\sum_{i=1}^{n}(h_2S_{P_i}+k_iP)+H_1(m)\right.\right.\\
&\qquad\left.\left.\cdot\sum_{i=1}^{t}S_{P_i}\right)H_1(m,m_w),P\right)
\end{aligned}$$

$$= e\left(\left(h_1 S_0 + kP + \sum_{i=1}^{n}(h_2 S_{P_i} + k_i P) + H_1(m) \cdot \sum_{i=1}^{t} S_{P_i}\right) H_1(m, m_w), P\right)$$

$$= e\left(h_1 Q_0 + \sum_{i=1}^{n} h_2 Q_{P_i} + H_1(m) \cdot \sum_{i=1}^{t} Q_{P_i}, P_{\text{pub}}\right)^{H_1(m,m_w)} (r_0 r_P)^{H_1(m,m_w)}$$

这里 $h_1 = H_1(m_w, r_0)$, $h_2 = H_1(r_P)$ 。

如果攻击者试图按照第 4 节相同的步骤来伪造一个有效的代理签名，他必须保证式 $e\left(\left(h_1 Q_0 + \sum_{i=1}^{n} h_2 Q_{P_i} + H_1(m) \cdot \sum_{i=1}^{t} Q_{P_i}\right), P_{\text{pub}}\right)^{H_1(m,m_w)} (r_0 r_p)^{H_1(m,m_w)}$ 与 式 $e\left(\left(h_1' Q_C + \sum_{i=1}^{n} h_2 Q_{P_i} + H_1(m) \sum_{i=1}^{t} Q_{P_i}\right)^{H_1(m,m_w')}, P_{\text{pub}}\right)(r_0' r_p)^{H_1(m,m_w')}$ 相等。

然而，由于哈希函数 $H_1(\cdot)$ 的单向性，即使 Q_0 , Q_C , r_0 , Q_{P_i} , m , m_w 和 r_p 是给定的。要找到一个新的授权证书 m_w' , 以及 h_1' 和 r_0' 来 满足等式： $e\left(\left(h_1 Q_0 + \sum_{i=1}^{n} h_2 Q_{P_i} + H_1(m) \cdot \sum_{i=1}^{t} Q_{P_i}\right), P_{\text{pub}}\right)^{H_1(m,m_w)} (r_0 r_p)^{H_1(m,m_w)}$ 和 $e\left(\left(h_1' Q_C + \sum_{i=1}^{n} h_2 Q_{P_i} + H_1(m) \sum_{i=1}^{t} Q_{P_i}\right)^{H_1(m,m_w')}, P_{\text{pub}}\right)(r_0' r_p)^{H_1(m,m_w')}$ 也是不可能的。

其强可识别性、强不可否认性、可区分性、防止滥用性等分析同原方案[7]。

6　结束语

本文分析了 BCW 方案的安全性，指出该方案并不满足强不可伪造性以及不需要安全信道发送签名了的授权证书等安全结论，成功给出了一种伪造攻击，并指出了 BCW 方案存在这样安全漏洞的原因并提出了改进的措施，分析表明，改进措施有效地克服了 BCW 方案存在的安全缺陷。

参 考 文 献

[1] Mambo M,Usuda K and Okamoto E. Proxy signature: Delegation to sign messages. *IEICE Trans. on Fundatamentals*, 1996, E79-A(9): 1338–1354.

[2] Lal S and Awasthi A K. Proxy blind signature scheme. Available at http:/eprint.iacr. org /2003.

[3] Yi Lijiang, Bai Guoqiang, and Xiao Guozhen. Proxy multi-signature scheme. *Electron.Lett.*, 2000, 36(6): 527–528.

[4] Zhang K. Threshold proxy signature schemes. In: Proc of the 1st Int'l Information Security Workshop (ISW'97), Springer-Verlag, 1997, LNCS 1396: 191–197.

[5] Shamir A. How to share a secret. *Communication of the ACM*, 1979, 22(11): 612–613.

[6] Boneh D and Franklin M. Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto'01, Springer-Verlag, 2001, LNCS 2139: 213–229.

[7] Bao Haiyong, Cao Zhenfu, and Wang Shengbao. Indentity-based threshold proxy signature scheme with knows signers. The 3nd Annual Conference in Theory and Applications of Models of Computation-TAM'06, Springer-Verlag, 2006, LNCS 3959: 538–546.

[8] Boneh D, Lynn B, and Shacham H. Short signatures from the Weil pairing. In: Boyd C. ed.. Advances in Cryptology-Asiacrypt'2001. Springer-Verlag, 2001, LNCS 2248: 514–532.

鲁荣波：　男，1970年生，副教授，博士生，研究方向为信息安全、电子支付等.

何大可：　男，1944年生，教授，博士生导师，主要研究方向为网络安全、信息安全、电子支付、并行计算等.

王常吉：　男，1972 年生，博士，副教授，主要研究方向为电子支付和密码学理论与应用等.