两类新的基于证书签名方案的安全性分析①

王海民[1], 张金辉[1], 黄 慧[2]

[1](莆田学院 数学学院, 莆田 351100)
[2](闽南师范大学 计算机科学与工程学院, 漳州 363000)

摘 要: 通过对翟正元等人新近提出的基于证书的代理盲签名方案进行了分析, 发现该签名方案并不安全, 至少能够受到两种替换公钥攻击. 攻击者通过替换原始签名的公钥或者替换代理签名者的公钥都能够做到对任意选择的消息成功伪造签名. 另外, 对陈建能等人给出的基于证书聚合签名进行了安全性分析, 指出该签名方案同样能够受到替换公钥攻击. 所给出这些的攻击方法对于基于证书签名的构造具有借鉴意义.

关键词: 基于证书; 代理签名; 盲签名; 聚合签名; 替换公钥攻击; 双线性对

Cryptanalysis of Two New Certificate-Based Signature Schemes

WANG Hai-Ming[1], ZHANG Jin-Hui[1], HUANG Hui[2]

[1](School of Mathematical Sciences, Putian University, Putian 351100, China)
[2](School of Computer Sciences, Minnan Normal University, Zhangzhou 351100, China)

Abstract: A new certificate-based proxy blind signature scheme is analyzed, which is proposed by Di Zhengyuan etc.. However, this scheme is insecure, because it can suffer from at least two types of public key replacement attack. That is, any one can replace the public key of the original singer or the public key of the proxy singer, and then forge a valid proxy signature on any message. In addition, the new certificate-based aggregate signature scheme propose by Chen Jianneng etc., is analyzed. The result showed that their signature scheme also can suffer from the public key replacement attack. Furthermore, the attack method in this paper has valuable reference to the construction of the type of certificate-based proxy signature.

Key words: certificate-based; proxy signature; blind signature; aggregate signature; public key replacement attack; bilinear pairings

1 引言

在信息化社会中, 数字签名作为手写签名的替代品, 其在信息安全, 如身份认证、数据完整性、不可否认性等方面都发挥着重要的应用, 是公开密钥密码的重要研究内容之一.

1976 年, Diffie 和 Hellman 首次提出了公开密钥密码的思想[1], 开辟了现代密码学的新领域——公钥密码学, 从而具有里程碑意义. 公钥密码系统的发展经历了以下几个阶段: 基于目录公钥系统(如 PKI)[2]; 基于身份公钥密码系统[3]; 无证书公钥密码系统[4]; 基于证书公钥密码系统[5], 它不仅克服了上述公钥系统中存在的诸多问题, 如克服了无证书公钥密码系统中的信任级别只能达到 2 级[6]和存在的 DOD 攻击[7]. 在基于证书公钥密码系统中, 可信机构的信任级别达到最高级 3 级, 即完全达到了 PKI 的水平. 因此, 基于证书公钥密码系统被广泛认为是当前几类公钥密码系统中最好的, 是目前的研究热点之一.

从此之后, 众多学者对基于证书签名进行了研究. 2004 年, Kang 等[8]首次给出基于证书数字签名的具体定义及其安全模型, 还同时给出了两个具体的签名方

① 基金项目:国家自然科学基金(61373140);福建省教育厅项目(JA12291);莆田学院教改项目(JG2012020)
收稿时间:2014-06-07;收到修改稿时间:2014-07-07

案. 近几年, 基于证书签名成为一个研究热点, 众多的基于证书签名方案相继被提出, 如文献[9-14]. 最近, 翟正元等人构造了一个新的基于证书的代理盲签名方案[15], 该方案在签名过程中不需要双线性对运算且只需要一次哈希函数运算, 其与已有的一些代理盲签名方案相比更加高效, 同时作者声称该方案在随机预言模型下是安全的, 其安全性是基于计算 CDH 假设. 注意到, 在该签名方案的安全性证明中只考虑的替换代理签名者的公钥, 而并没有考虑原始签名者的替换公钥攻击. 遗憾的是, 本文对其分析后发现, 该签名方案事实上是不安全的, 至少能够受到两类替换公钥攻击, 即攻击者不仅可以通过替换原始签名者的公钥, 也可以通过替换代理签名者的公钥, 从而攻击者能够做到对任意选择的消息成功伪造签名. 这也说明了, 文献[15]中签名的安全性模型是存在问题的, 其证明的安全性是不可信的. 经过分析发现, 文献[16]中给出的无证书聚合签名方案也是不安全的, 能够受到替换公钥攻击, 同样地, 攻击者能够做到对任意选择的消息成功伪造签名. 因此, 本文给出的攻击方法对于基于证书签名的构造, 特别是基于证书代理签名和聚合签名的构造具有借鉴意义.

2 预备知识

假设 G_1 和 G_2 分别为 q 阶的加法循环群和乘法循环群, 其中 q 为大素数, 不妨设 P 为群 G_1 的生成元, 则把满足下述性质的映射 $e:G_1\times G_1\to G_2$ 称为双线性对.

(1) 双线性: $\forall a,b\in Z_q^*$ 和 $P,Q\in G_1$, 有

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

(2) 非退化性: $e(P,P)\neq 1_{G_2}$.

(3) 可计算性: 对任意的 $P,Q\in G_1$, 存在计算 $e(P,Q)$ 的有效算法.

群 G_1 上的两个密码学困难问题:

(1) 离散对数问题(DLP): 设 P 和 Q 为群 G_1 中的任意两个元素, 求整数 n 满足 $Q=nP$.

(2) 计算 Diffie－Hellman 问题(CDHP): 对于 P,aP,bP, 其中 $a,b\in Z_q^*$, 计算 abP.

由于篇幅关系, 基于证书代理签名、代理盲签名、聚合签名的定义及其它们的安全性模型请参见文献[14-16].

3 文献[15]基于证书的代理盲签名方案回顾

文献[15]结合基于证书密码体制和代理盲签名的特点, 构造了一个新的基于证书代理盲签名方案, 具体构造如下:

(1) 系统参数生成

输入参数 k, 产生两个 q 阶循环群 G_1,G_2, 其中 G_1 为加法循环群, G_2 为乘法循环群, q 为大素数. 设 P 为群 G_1 的生成元. $e:G_1\times G_1\to G_2$ 为双线性映射. 两个安全的 Hash 函数 $H_1:\{0,1\}^*\times G_1\times G_1\to G_1, H_2:\{0,1\}^*\times G_1\to Z_q^*$. 原始签名者 A 随机选择 $x_A\in Z_q^*$, 并计算 $PK_A=x_AP$, 将 x_A 作为主密钥秘密保存, 公开系统参数:

$$params=\{G_1,G_2,e,P,q,H_1,H_2,PK_A\}.$$

(2) 用户密钥生成

代理签名者 B 随机选择 $x_B\in Z_q^*$, 计算 $PK_B=x_BPK_A=x_Bx_AP$, 则代理签名者 B 的公私钥对为 (PK_B,x_B).

(3) 代理证书生成

原始签名者 A 根据实际情况首先构造一个授权证书 m_ω, 其中包括原始签名者和代理签名者的身份信息 ID_A、ID_B 以及授权的代理期限等信息. A 计算 $P_B=H_1(m_\omega,PK_A,PK_B)$, 并为代理签名者 B 的公钥 PK_B 生成代理证书 $Cert_B=x_A^{-1}P_B$, 再将 $Cert_B$ 通过安全信道发送给 B.

(4) 代理密钥生成

代理签名者 B 收到 $Cert_B$ 后, 先验证

$$e(Cert_B,PK_A)=e(P_B,P)$$

是否成立, 如果成立, 那么接受代理证书 $Cert_B$, 然后计算代理签名密钥 $S_p=x_BP_B+Cert_B$.

(5) 代理盲签名生成

对于消息 $m\in\{0,1\}^*$ 的基于证书代理盲签名是通过下面协议生成:

① B 随机选择 $r\in Z_q^*$, 计算 $R_1=rPK_B, R_2=rP$, 并将 (R_1,R_2) 发送给用户 C.

② C 收到 (R_1,R_2) 后, 随机选择 $\alpha,\beta\in Z_q^*(\alpha\neq\beta)$ 作为盲化因子计算

$$R=\alpha R_1+\beta R_2, t=H(m,R),$$

并令 $t_1=\alpha^{-1}t, t_2=\beta-\alpha$, 接着把 t_1,t_2 发送给 B.

③ B 收到 t_1,t_2 后, 计算

$V_1=(t_1+r)S_p, V_2=rt_2Cert_B$，
并将(V_1,V_2)发送给C.

④ C收到(V_1,V_2)后，计算$V=\alpha V_1+V_2$，则消息m的代理盲签名$\sigma=(m_\omega,m,R,V)$.

(6) 代理盲签名验证

验证者V收到消息m及其代理盲签名$\sigma=(m_\omega,m,R,V)$后，先从m_ω中得到原始签名者和代理签名者的身份等信息，计算$P_B=H_1(m_\omega,PK_A,PK_B)$，验证

$$e(V,PK_A)=e(P_B,H_2(m,R)(PK_B+P)+R)$$

是否成立，如果上式成立，则V接受代理盲签名，否则拒绝.

4 对文献[15]签名方案的两种替换公钥攻击

对上述签名方案进行分析后，下面指出该方案至少存在两种替换公钥攻击，具体攻击方法如下，其中系统相关参数与原签名方案一致:

(1) 针对原始签名者A的替换公钥攻击

攻击者通过以下步骤伪造签名:

① 随机选择$R'\in G_1$，并选择任意待签名的消息m'，令

$$T'=H_2(m',R')(PK_B+P)+R';$$

② 随机选择$l'\in Z_q^*$，替换代理签名者A的公钥为$PK_A'=l'^{-1}T';$

③ 计算$P_B'=H_1(m_\omega,PK_A',PK_B);$

④ 令$V'=l'P_B'$.

注意到，

$$\begin{aligned}&e(V',PK'_A)\\&=e(l'P_B',l'^{-1}T')\\&=e(P_B',H_2(m',R')(PK_B+P)+R')\end{aligned}$$

即攻击者所构造的签名$\sigma'=(m_\omega,m',R',V')$满足验证算法，因此$\sigma'=(m_\omega,m',R',V')$为消息$m'$的有效签名，伪造成功.

(2) 针对代理签名者B的替换公钥攻击

攻击者通过以下步骤伪造签名:

① 随机选择$r'\in Z_q^*$，令$R'=r'PK_A;$

② 随机选择$l'\in Z_q^*$，替换代理签名者B的公钥为$PK_B'=l'PK_A-P;$

③ 选择任意待签名的消息m'，计算

$$H_2(m',R'),\ P_B'=H_1(m_\omega,PK_A,PK_B');$$

④ 令$V'=(l'H_2(m',R')+r')P_B'$.

注意到，

$$\begin{aligned}&e(P_B',H_2(m',R')(PK_B'+P)+R')\\&=e(P_B',H_2(m',R')(l'PK_A-P+P)+r'PK_A)\\&=e(P_B',(H_2(m',R')l'+r')PK_A)\\&=e((H_2(m',R')l'+r')P_B',PK_A)\\&=e((H_2(m',R')l'+r')P_B',PK_A)\\&=e(V',PK_A)\end{aligned}$$

即攻击者所构造的签名$\sigma'=(m_\omega,m',R',V')$满足验证算法，因此$\sigma'=(m_\omega,m',R',V')$为消息$m'$的有效签名，伪造成功.

综上所述，攻击者通过替换原始签名者A的公钥PK_A或者替换代理签名者B的公钥PK_B，都能做到对任意选择的消息成功伪造签名，因此，原签名方案是不安全的.

5 文献[16]中基于证书聚合签名方案回顾

(1) 系统建立 证书生成中心(CA)选择 2.1 节中定义的双线性对e，G_1和G_2，P是G_1的一个生成元. 随机选取$s\in Z_q^*$作为系统的私钥，计算系统的公钥$PK_c=sP$. CA选择一个公开无碰撞的 Hash 函数，$H_1:\{0,1\}^*\to G_1$. CA公开系统参数(G_1,G_2,e,q,P,PK_c,H_1)，并且保密系统私钥s，不让CA以外的任何人知道.

(2) 签名者公私钥生成 签名者是拥有某一特殊身份的个体，并且这个身份是唯一的. 任意一个签名者身份信息用ID_i表示，每个签名者都随机选取一个秘密值$\alpha_i\in Z_q^*$作为自己的私钥SK_i，计算$PK_i=\alpha_iP$作为自己的公钥，其中$(1\le i\le N)$,N为聚合签名者总人数.

(3) 签名者证书生成 签名者把包含ID_i和PK_i的信息提交给证书生成中心(CA)，CA验证其信息的真实性以及ID_i没有重复之后，计算$Q_i=H_1(PK_c,PK_i,ID_i)$，$cert_i=sQ_i$，把$cert_i$发送给签名者i作为其私有的证书，签名者i在签名时只要把$cert_i$的值直接带入算法中计算即可.

(4) 单个签名 签名聚合者把n个不同的消息，分别记为$m_1,m_2,\cdots,m_n$，并且使之与签名者的身份$ID_1,ID_2,\cdots,ID_n$一一对应，即拥有身份ID_i的签名者负责对消息m_i签名. 签名者ID_i对消息m_i的签名过程如下:

随机选择一个数 $r_i \in Z_q^*$，计算 $R_i = r_i P, h_i = H_2(m_i, R_i, PK_i)$, 其中 $H_2(x)$ 是一个 Hash 函数，$H_2 : \{0,1\}^* \times G_1 \times G_1 \to G_1, T_i = \alpha_i h_i + cert_i + r_i Q_i$, $\sigma_i = (T_i, R_i)$ 就是签名者 ID_i 对消息 m_i 的签名.

(5) 单个签名验证 签名聚合者收到签名 (T_i, R_i) 后验证等式

$$e(T_i, P) = e(h_i, PK_i) e(Q_i, PK_c + R_i)$$

是否成立, 若不成立则拒绝接受该签名. 若成立则接受该签名为有效签名.

(6) 签名的聚合 签名聚合者收齐 n 个有效的签名后, 通过以下两个等式进行聚合:

$$U = \sum_{i=1}^{n} T_i, V_i = e(Q_i, R_i),$$

$\sigma = (U, V_1, V_2, \cdots, V_n)$ 即为该整体消息 m 的聚合签名.

(7) 聚合签名的验证 签名验证者如果希望对某个聚合签名 $\sigma = (U, V_1, V_2, \cdots, V_n)$ 进行验证的话, 只要验证下面的等式是否成立即可

$$e(U, P) = = \prod_{i=1}^{n} e(h_i, PK_i) e\left(\sum_{i=1}^{n} Q_i, PK_c\right) \prod_{i=1}^{n} V_i$$

若等式成立, 则签名 $\sigma = (U, V_1, V_2, \cdots, V_n)$ 是有效的聚合签名, 反之, 为无效的聚合签名.

6 对文献[16]中签名方案的替换公钥攻击

对上述签名方案进行分析后, 下面指出该签名方案中的单个签名算法容易受到替换公钥攻击, 此外, 聚合签名也容易受到替换公钥攻击, 使得攻击者可以对任意选择的消息成功伪造签名. 具体攻击方法如下, 其中系统相关参数与原签名方案一致:

(1) 对单个签名算法的攻击

下面的攻击方法显示, 攻击者通过替换签名人的公钥, 可以做到对任意选择的消息 m_i' 成功伪造签名:

① 随机选择 $\alpha_i' \in Z_q^*$，并替换签名的公钥为 $PK_i' = \alpha_i' P$;

② 随机选择 $r_i' \in Z_q^*$，令 $R_i' = r_i' P - PK_c$;

③ 计算 $h_i' = H_2(m_i', R_i', PK_i')$，$Q_i' = H_1(PK_c, PK_i', ID_i)$;

④ 令 $T_i' = \alpha_i' h_i' + r_i' Q_i'$.

则得到消息 m_i' 的有效签名 $\sigma_i' = (T_i', R_i')$.

容易验证, 上述构造的消息 m_i' 的签名 $\sigma_i' = (T_i', R_i')$ 能够通过验证算法.

$$\begin{aligned} & e(T_i', P) \\ &= e(\alpha_i' h_i' + r_i' Q_i', P) \\ &= e(\alpha_i' h_i', P) e(r_i' Q_i', P) \\ &= e(h_i', \alpha_i' P) e(Q_i', r_i' P) \\ &= e(h_i', PK_i') e(Q_i', PK_c + R_i') \end{aligned}$$

(2) 对聚合签名算法的攻击注意到,

$$e(U, P) = e\left(\sum_{i=1}^{n} T_i, P\right) = \prod_{i=1}^{n} e(T_i, P),$$

另外

$$\begin{aligned} & \prod_{i=1}^{n} e(h_i, PK_i) e\left(\sum_{i=1}^{n} Q_i, PK_c\right) \prod_{i=1}^{n} V_i \\ &= \prod_{i=1}^{n} e(h_i, PK_i) e\left(\sum_{i=1}^{n} Q_i, PK_c\right) \prod_{i=1}^{n} e(Q_i, R_i) \\ &= \prod_{i=1}^{n} e(h_i, PK_i) \prod_{i=1}^{n} e(Q_i, PK_c + R_i) \\ &= \prod_{i=1}^{n} e(h_i, PK_i) e(Q_i, PK_c + R_i) \end{aligned}$$

即聚合签名的验证式等价于

$$\prod_{i=1}^{n} e(T_i, P) = \prod_{i=1}^{n} e(h_i, PK_i) e(Q_i, PK_c + R_i)$$

显然, 聚合签名验证算法中验证式只是单个签名验证等式左右两边分别相乘而得到的等式, 因此对单个签名算法的攻击方法同时适用于对聚合签名验证算法的攻击, 只是需要同时替换所有签名人的公钥, 那么攻击者就可以对任意选择的消息成功伪造聚合签名.

7 结语

对新近提出的两类基于证书签名方案进行了安全性分析, 发现这两个基于证书签名方案都是不安全的, 给出了具体的攻击方法, 攻击者通过这些攻击方式可以对任意选择的消息成功伪造签名, 所给出的攻击方法对同类签名的设计具有借鉴意义.

参考文献

1 Diffie W, Hellman M. New direction in cryptography. IEEE Trans. on Information Theory, 1976, IT-22(6): 644–654

2 Gutmann P. PKI: It's not dead, just resting. IEEE Computer, 2002, 35(8): 41–49.

3 Shamir A. Identity-based cryptosystems and signature schemes. In: Blakely GR, Chaum D, eds. CRYPTO'84. Berlin. Springer-Verlag. LNCS. 1984, (196). 47–53.

4 Al-Riyami S, Paterson K. Certificateless public key

cryptography. In: Lee PJ, ed. ASIACRYPT'03. Berlin. Springer-Verlag. LNCS. 2003, (2894). 452–473.

5 Gentry C. Certificate-based encryption and the certificate revocation problem. In: Biham E, ed. Eurocrypt 2003. Berlin. Springer-Verlag. LNCS. 2003, (2656). 272–293.

6 Girault M. Self-certified public keys. In: Donald W.D, ed. Advances in Cryptology proceeding of Eurocrypt 1991. Berlin. Springer-Verlag. LNCS. 1991, (547), 490–497.

7 Liu J, Au M, Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In: Weirich S, ed. Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security. 2007. 273–283.

8 Kang B, Park J, Hahn S. A certificate-based signature scheme. In: Marc J, ed. Proc. of Topics in Cryptology-CT-RSA 2003. Berlin. Springer-Verlag. LNCS. 2004, (2964). 99–111.

9 李继国,钱娜,黄欣沂,张亦辰.基于证书强指定验证者签名方案.计算机学报,2012,35(8):1579–1587.

10 黄振杰,郭亚峰.一个双线性对下高效的基于证书签名方案.江苏大学学报(自然科学版),2013,34(3):320–325.

11 吴晨煌,郭瑞景,陈智雄.高效的基于证书短签名方案.计算机系统应用,2013,22(2):129–132,145.

12 陈江山,黄振杰.一个高效的基于证书签名方案.计算机工程与应用,2012,48(30):98–102.

13 Li J, Huang X, Zhang Y, et al. An efficient short certificate-based signature scheme. The Journal of Systems and Software, 2012, 85: 314–322.

14 Li J, Xu L, Zhang Y. Provably secure certificate-based proxy signature schemes.Journal of Computers, 2009, 4(6): 444–452.

15 翟正元,高德智,梁向前,潘帅.新的基于证书的代理盲签名方案.计算机工程与应用,2014,50(4):57–62.

16 陈建能,岳昊,黄振杰.一个可证安全的基于证书聚合签名方案.计算机工程与应用,2013,49(21):60–64.