第35卷 第16期 计 算 机 工 程 2009年8月
Vol.35 No.16 Computer Engineering August 2009
·安全技术· 文章编号：1000—3428(2009)16—0140—03 文献标识码：A 中图分类号：TP309

三类无证书签名方案的缺陷及改进

农 强[1]，郝艳华[1]，吴顺祥[2]
(1. 漳州师范学院计算机科学与工程系，漳州 363000；2. 厦门大学自动化系，厦门 361005)

摘 要：对最近提出的2个在随机预言模型中可证安全的无证书签名方案和1个在标准模型中可证安全的无证书签名方案进行安全性分析，指出这3个方案不能抵抗替换公钥攻击的安全隐患，在这种攻击下攻击者能够生成新的公钥满足合法签名者生成的合法签名。给出改进措施，有效克服原方案中的设计缺陷。

关键词：无证书签名；替换公钥攻击；双线性对

Flaw and Improvement of Three Certificateless Signature Schemes

NONG Qiang[1], HAO Yan-hua[1], WU Shun-xiang[2]
(1. Department of Computer Science and Engineering, Zhangzhou Normal University, Zhangzhou 363000;
2. Department of Automation, Xiamen University, Xiamen 361005)

【Abstract】The security flaws of two provably-secure certificateless signature schemes in the random oracle model and a provably-secure certificateless signature scheme in the standard model are analyzed. It is found that the three schemes are all insecure against public key replacement attack. In this attack, an adversary can generate a new public key satisfying legitimate signatures created by the legitimate signer. In order to avoid these flaws, an improvement measure is proposed, which can resolve the security problems existing in the original schemes.

【Key words】certificateless signature; public key replacement attack; bilinear pairings

1 概述

无证书公钥密码体制[1]避免了传统公钥密码系统中的证书存在问题，同时消除了基于身份密码系统中的密钥托管问题，提高系统的运行效率，降低系统的复杂度，因此，更加适合低带宽和低功率的移动环境中的安全应用。目前，有关无证书密码方案的研究成果还不是很多，技术也还不够成熟，已提出的许多方案被证明是不安全的，它们大多存在替换公钥攻击[2-6]。在无证书公钥系统中，由于用户的公钥无须利用证书来提供认证，因此考虑替换公钥攻击是必须的。

最近，曹雪菲等人、明洋等人和王旭等人分别提出了一些改进的和新的无证书签名方案[7-9]，并都宣称所提的签名方案具有不可伪造性。本文指出他们所提的3个方案都是不安全的，都无法抵抗替换公钥攻击，在这种攻击下，攻击者可以任意替换签名者的公钥，并伪造消息-签名对，使其在被替换的公钥下是有效的。最后，提出了改进的方案来避免这种攻击。

2 预备知识

2.1 双线性对

设 G_1 为由 P 生成的循环加法群，阶为 q，G_2 为具有相同阶 q 的循环乘法群，称具有下列性质的映射 $e: G_1 \times G_1 \to G_2$ 为双线性对：(1)双线性性：$e(aP,bQ)=e(P,Q)^{ab}$，对 $\forall a,b \in Z_q^*$，$\forall Q \in G_1$；(2)非退化性：$\exists P,Q \in G_1$，满足 $e(P,Q) \neq 1$；(3)可计算性：$e(P,Q)$ 可以被有效计算出来。群 G 可取有限域上超奇异椭圆曲线或超椭圆曲线，双线性对可利用该曲线上的 Weil 配对或 Tate 配对改进后进行实现。

2.2 无证书签名体制

一个无证书数字签名体制一般由7个算法组成：即系统设置、部分私钥提取、秘密值生成、私钥生成、公钥生成、签名和验证。其中，密钥生成中心 KGC 将执行前2个算法，且只能产生用户的部分私钥，而用户的公钥私钥对由用户利用其设定的秘密值来生成。可见，该体制中用户的公钥具有自认证性，无需 KGC 签发证书，同时其私钥也只有用户知道。在无证书签名机制的安全模型中，攻击者被定义为2类：

(1)Type-Ⅰ类攻击者 A_1。A_1 不知道系统私钥 s，但他可以替换被攻击者的公钥，抽取 KGC 生成的部分私钥或者直接获得签名密钥，然后发出签名请求。如果攻击者 A_1 已经替换了用户的公钥，此时对签名预言发出签名请求，则签名预言机返回的签名将是不正确的，因为将不给定任何额外的假设，此时如同随机预言模型。但是如果 A_1 发出签名请求的同时又将已替换的公钥和相应的秘密信息也发送给签名预言机的话，那么假设预言器的回答是正确的。在实际应用中，A_1 模拟的是除 KGC 之外的攻击者。

(2)Type-Ⅱ类攻击者 A_2。A_2 知道系统私钥 s，但不能替换

基金项目：国家自然科学基金资助项目(60704042)；国家“十一五”科技支撑计划基金资助项目(2007BAK34B04)；福建省教育厅科技基金资助项目(JA08156)；福建省青年科技人才创新基金资助项目(2008F3110)

作者简介：农 强(1978－)，男，讲师、硕士，主研方向：密码学，网络安全；郝艳华，讲师、博士；吴顺祥，教授、博士
收稿日期：2009-03-17 **E-mail：**nong_qiang@163.com

被攻击者的公钥。在实际应用中，A_2 模拟的是恶意的 KGC。

3 对曹雪菲等人方案的攻击

3.1 曹雪菲等人的无证书签名方案[7]

(1)系统设置：输入安全参数 1^k，输出 2 个阶为 q 的循环群 $(G_1,+)$ 和 $(G_2,\times)$，q 为大素数，P 为 G_1 的生成元。定义双线性映射 $e:G_1\times G_1\to G_2$ 和 2 个哈希函数 $H_1:\{0,1\}^*\to G_1$ 和 $H_2:\{0,1\}^*\times G_1\to Z_q^*$。KGC 选择 $s\in_R Z_q^*$，计算 $P_0=sP$，将 s 秘密保存，公开系统参数 $\{G_1,G_2,e,q,P,P_0,H_1,H_2\}$。

(2)部分私钥提取：用户 U_{ID} 向 KGC 提交唯一身份标识符 ID，KGC 检查 ID 的合法性，若 ID 合法，则计算 $Q_{ID}=H_1(ID)$ 并输出 $D_{ID}=sQ_{ID}$。

(3)秘密值提取：U_{ID} 随机选取 $x_{ID}\in_R Z_q^*$ 作为其秘密值。

(4)私钥提取：U_{ID} 计算 $S_{ID}=x_{ID}D_{ID}$ 作为其私钥。

(5)公钥产生：U_{ID} 计算 $PK_{ID}=<X_{ID},Y_{ID}>$ 作为其公钥，其中，$X_{ID}=x_{ID}P$，$Y_{ID}=x_{ID}P_0$。

(6)签名：为了利用私钥 S_{ID} 对消息 m 进行签名，U_{ID} 首先选择 $l\in_R Z_q^*$，计算 $U=lQ_{ID}$ 和 $h=H_2(m\|U)$，然后计算 $V=(l+h)S_{ID}$，则 U_{ID} 对 m 的签名是 $\sigma=<U,V>$。

(7)验证：验证者验证 $e(X_{ID},P_0)=e(Y_{ID},P)$ 和 $e(P,V)=e(Y_{ID},U+hQ_{ID})$ 是否成立，当且仅当 2 次验证的结果成立则接受签名，否则拒绝。

3.2 替换公钥实现对曹雪菲等人方案的攻击

设已知身份 ID 的关于消息 m 和公钥 PK_{ID} 的签名 $\sigma=<U,V>$，攻击者选择 $\alpha\in_R Z_q^*$，计算 $PK_{ID}^{'}=<X_{ID}^{'},Y_{ID}^{'}>=<\alpha X_{ID},\alpha Y_{ID}>$，然后输出签名 $\sigma^{'}=<U,V^{'}>=<U,\alpha V>$。

验证者将认为 $\sigma^{'}$ 是 U_{ID} 对 m 的有效签名，因为很容易推断 $e(X_{ID}^{'},P_0)=e(Y_{ID}^{'},P)$ 成立，又因为

$$e(P,V^{'})=e(P,\alpha(l+h)S_{ID})=e(P,\alpha(l+h)x_{ID}sQ_{ID})=e(\alpha x_{ID}sP,(l+h)Q_{ID})=e(Y_{ID}^{'},U+hQ_{ID})$$

其中，$h=H_2(m\|U)$，从而伪造的签名能够通过确认，因而攻击成功。

4 对明洋等人方案的攻击

4.1 明洋等人的无证书签名方案[8]

(1)系统设置：KGC 选取 $<G_1,G_2,e>$，选取任意的生成元 $P\in G_1$ 并计算 $g=e(P,P)$；选取 2 个哈希函数 $H_1:\{0,1\}^*\to Z_q^*$，$H_2:\{0,1\}^*\times G_2\to Z_q^*$，并选取主密钥 $s\in_R Z_q^*$，计算 $P_{pub}=sP$，公开系统参数 $Params=\{G_1,G_2,e,P,P_{pub},g,H_1,H_2\}$。

(2)部分私钥提取：KGC 首先验证签名者 i 的身份 ID_i，计算 $Q_i=H_1(ID_i)$；然后计算部分私钥 $D_i=(Q_i+s)^{-1}P$，并在安全信道下把 D_i 发送给签名者 i；签名者 i 通过检验 $e(D_i,Q_iP+P_{pub})=g$ 是否成立来验证 D_i 的正确性。

(3)秘密值提取：给定参数 $Params$ 和签名者 i 的身份 ID_i，签名者 i 随机选取 $x_i\in_R Z_q^*$ 作为秘密值。

(4)设置私钥：签名者 i 计算 $SK_i=x_iD_i=(Q_i+s)^{-1}x_iP$ 作为其私钥。

(5)设置公钥：签名者 i 计算 $PK_i=(X_i,Y_i)$ 作为其公钥，其中，$X_i=x_iP$，$Y_i=x_iP_{pub}=x_isP$。

(6)签名：签名者 i 随机选取 $r\in_R Z_q^*$，计算 $R=g^r$ 并计算 $h=H_2(m\|R)$，最后计算 $S=(r+h)SK_i$，则消息 m 的签名为 $\sigma=<S,h>$。

(7)验证：验证者验证 $e(X_i,P_{pub})=e(Y_i,P)$ 是否成立，如果不成立，则放弃；然后验证者计算 $R^{'}=e(S,Q_iX_i+Y_i)g^{-h}$，并验证 $h=H_2(m\|R^{'})$ 是否成立，如果成立则接受签名，否则拒绝。

4.2 替换公钥实现对明洋等人方案的攻击

设已知身份 ID_i 的关于消息 m 和公钥 PK_i 的签名 $\sigma=<S,h>$，攻击者选择 $\alpha\in_R Z_q^*$，替换公钥 $PK_i^{'}=(X_i^{'},Y_i^{'})=(\alpha X_i,\alpha Y_i)=(\alpha x_iP,\alpha x_isP)$，然后输出签名 $\sigma^{'}=<S^{'},h>=<\alpha^{-1}S,h>$。该伪造的签名能够得到确认，因为有

$$e(X_i^{'},P_{pub})=e(\alpha x_i^{-1}P,sP)=e(\alpha x_i^{-1}sP,P)=e(Y_i^{'},P)$$

$$R^{'}=e(\alpha^{-1}S,Q_iX_i^{'}+Y_i^{'})g^{-h}=e(\alpha^{-1}(r+h)(Q_i+s)\,x_iP,Q_i\alpha x_iP+\alpha x_isP)g^{-h}=$$

$$e((r+h)(Q_i+s)^{-1}x_iP,(Q_i+s)x_iP)g^{-h}=$$

$$e((r+h)P,P)g^{-h}=e(P,P)^{(r+h)}g^{-h}=$$

$$g^{(r+h)}g^{-h}=g^r=R$$

即 $h=H_2(m\|R^{'})$ 成立，伪造的签名能够通过确认，因而攻击成功。

5 对王旭等人方案的攻击

5.1 王旭等人的无证书签名方案[9]

(1)系统设置：KGC 选取 $<G_1,G_2,e>$，选择任意的生成元 $P_1,P_2\in G_1$，选择 2 个哈希函数 $H_u:\{0,1\}^*\to\{0,1\}^{n_u}$，$H_m:\{0,1\}^*\to\{0,1\}^{n_m}$，其中，$n_u,n_m\in Z$；让 $\alpha\in_R Z_q^*$，计算 $P_b=\alpha P_2$，让 $P_a\in_R G_1^*$，让 $U^{'},M^{'}\in_R G_1^*$，$U_i\in_R G_1^*$，$1\leqslant i\leqslant n_u^{'}$，$M_i\in_R G_1^*$，$1\leqslant i\leqslant n_m^{'}$（$n_u^{'}$ 和 $n_m^{'}$ 的定义将在下面描述），让 $\hat{U}=\{U_i\}$，$\hat{M}=\{M_i\}$；最后公开系统参数 $Params=<G_1,G_2,e,P_1,P_2,P_a,P_b,U^{'},\hat{U},M^{'},\hat{M},H_u,H_m>$，其主密钥为 $mk=\alpha P_a$。

(2)部分私钥提取：以用户的身份 $ID\in\{0,1\}^*$、参数 $Params$ 和主密钥 mk 作为输入，KGC 计算 $u=H_u(ID)$；将 u 从低位到高位看成是由以 s 位二进制为单位组成的串，即 $u=u[1]\|u[2]\|\cdots\|u[n_u^{'}]$，其中，$n_u^{'}=\lceil n_u/s\rceil$，$u[i]\in Z_{2^s}$；计算 $U=U^{'}+\sum_{i=1}^{n_u^{'}}(u[i]U_i)$；让 $r_u\in_R Z_q^*$，最后计算 $psk=(psk_1,psk_2)=(mk+r_uU,r_uP_2)$ 作为对应 ID 的部分私钥并输出。

(3)用户公私钥对提取：选择 $x\in_R Z_q^*$ 作为用户私钥 sk；将 $pk=(pk_1,pk_2)=(xP_1,xP_b)$ 作为其公钥。

(4)签名：设有签名消息 $M\in\{0,1\}^*$，签名者计算 $m=H_m(M)$；同样将 m 看成 $m=m[1]\|m[2]\|\cdots\|m[n_m^{'}]$，其中，$n_m^{'}=\lceil n_m/t\rceil$，$m[i]\in Z_{2^t}$；计算 $M=M^{'}+\sum_{i=1}^{n_m^{'}}(m[i]M_i)$；选择 $r_\pi,r_m\in_R Z_q^*$；用部分私钥提取中的方法计算出 U；将 $\sigma=(V,R_\pi,R_m)=((sk)(psk_1)+r_\pi U+r_mM,\,(sk)(psk_2)+r_\pi P_2,r_mP_2)$ 作为签名输出。

(5)验证：检验等式 $e(pk_1,P_b)=e(P_1,pk_2)$ 和 $e(V,P_2)=e(P_a,pk_2)e(U,R_\pi)e(M,R_m)$ 是否成立，若成立，则签名有效，否则签名无效。

5.2 替换公钥实现对王旭等人方案的攻击

设已知身份 ID 的关于消息 M 和公钥 pk 的签名

$\sigma=(V,R_\pi,R_m)$，攻击者选择 $\mu\in_R Z_q^*$，替换公钥 $pk'=(pk_1',pk_2')=(\mu xP_1,\mu xP_b)$，然后输出签名 $\sigma'=(V',R_\pi',R_m')=(\mu V,\mu R_\pi,\mu R_m)$。该伪造的签名能够得到确认，因为

$$e(pk_1',P_b)=e(\mu xP_1,\alpha P_2)=e(P_1,\mu x\alpha P_2)=e(P_1,pk_2')$$

$$e(V',P_2)=e(V,P_2)^\mu=e(P_a,pk_2)^\mu e(U,R_\pi)^\mu e(M,R_m)^\mu=$$

$$e(P_a,\mu pk_2)e(U,\mu R_\pi)e(M,\mu R_m)=e(P_a,pk_2')e(U,R_\pi')e(M,R_m')$$

伪造的签名能够通过确认，所以攻击成功。

6 上述 3 个方案的改进及安全性分析

除签名和验证步骤外，与原方案相同的部分不再赘述，以下只列出签名和验证过程。

6.1 曹雪菲等人方案的改进

(1)签名：U_{ID} 选择 $l\in_R Z_q^*$，计算 $U=lQ_{ID}$ 和 $h=H_2(m\|U\|PK_{ID})$，然后计算 $V=(l+h)S_{ID}$，则 U_{ID} 对 m 的签名是 $\sigma=<U,V>$。

(2)验证：计算 $h=H_2(m\|U\|PK_{ID})$ 并验证 $e(X_{ID},P_0)=e(Y_{ID},P)$ 和 $e(P,V)=e(Y_{ID},U+hQ_{ID})$ 是否成立。

6.2 明洋等人方案的改进

(1)签名：签名者 i 随机选取 $r\in_R Z_q^*$，计算 $R=g^r$ 并计算 $h=H_2(m\|R\|PK_i)$，最后计算 $S=(r+h)SK_i$，则消息 m 的签名为 $\sigma=<S,h>$。

(2)验证：首先计算 $h=H_2(m\|R\|PK_i)$，然后计算 $R'=e(S,Q_iX_i+Y_i)g^{-h}$，验证 $e(X_i,P_{pub})=e(Y_i,P)$ 和 $h=H_2(m\|R'\|PK_i)$ 是否成立。

6.3 王旭等人方案的改进

(1)签名：设有签名消息 $M\in\{0,1\}^*$，签名者选择 $r_\pi,r_m\in_R Z_q^*$，计算 $R_\pi=(sk)(psk_2)+r_\pi P_2$，$R_m=r_mP_2$，并计算 $m=H_m(M\|R_\pi\|R_m\|pk)$，同样将 m 看成 $m=m[1]\|m[1]\|\cdots\|m[n_m']$，其中，$n_m'=\lceil n_m/t\rceil$，$m[i]\in Z_{2^t}$；计算 $M=M'+\sum_{i=1}^{n_m'}(m[i]M_i)$，用同样的方法计算出 U；

最后计算 $V=((sk)(psk_1)+r_\pi U+r_mM)$ 并将 $\sigma=(V,R_\pi,R_m)$ 作为签名输出。

(2)验证：接收签名 $\sigma=(V,R_\pi,R_m)$ 后，验证者首先计算 $m=H_m(M\|R_\pi\|R_m\|pk)$，然后检验等式 $e(pk_1,P_b)=e(P_1,pk_2)$ 和 $e(V,P_2)=e(P_a,pk_2)e(U,R_\pi)e(M,R_m)$ 是否成立。

6.4 改进方案的安全性分析

改进方案将用户的公钥作为强抗碰撞密码哈希函数的输入，使攻击者无法替换用户的公钥。由于哈希函数 $H_2(\cdot)$ 的单向性，即使公钥 PK_{ID} 是给定的，文献[7]的攻击者要找到一个新的公钥 PK_{ID}' 使得满足 $e(Y_{ID},U+H_2(m\|U\|PK_{ID})Q_{ID})=e(Y_{ID}',U+H_2(m\|U\|PK_{ID}')Q_{ID})$ 是计算不可行的。同理，对于给定的公钥 PK_i，文献[8]的攻击者要找到一个新的公钥 PK_i' 使得 $e(S,Q_iX_i+Y_i)g^{-H_2(m\|R\|PK_i)}=e(S',Q_iX_i'+Y_i')\ g^{-H_2(m\|R\|PK_i')}$ 也是计算不可行的。上述改进后的签名方案对 Type-Ⅰ和 Type-Ⅱ类型攻击者具有安全性的证明思路与原来的证明思路类似，区别仅在于取哈希函数时，输入的值不一样。

7 结束语

本文对曹雪菲等人、明洋等人和王旭等人的一些改进的和新的无证书签名方案提出了替换公钥攻击，进而对其进行安全性分析与改进，有效克服了原方案中的安全隐患。

参考文献

[1] Al-Riyami S, Paterson K. Certificateless Public Key Cryptography[C]//Proc. of ASIACRYPT'03. Berlin, Germany: Springer-Verlag, 2003: 452-473.

[2] Huang Xinyi, Susilo W, Mu Yi, et al. On the Security of Certificateless Signature Schemes from Asiacrypt 2003[C]//Proc. of CANS'05. Berlin, Germany: Springer-Verlag, 2005: 13-25.

[3] Cao X F, Kenneth G P, Kou W D. An Attack on a Certificateless Signature Scheme[EB/OL]. (2006-03-21). http://eprint.iacr.org/2006/367.

[4] Hu B, Wong D, Zhang Zhengfeng, et al. Key Replacement Attack Against a Generic Construction of Certificateless Signature[C]//Proc. of ACISP'06. Berlin, Germany: Springer-Verlag, 2006: 235-246.

[5] Yap W S, Heng S H, Goi B M. Cryptanalysis of Some Proxy Signatures Schemes Without Certificates[C]//Proc. of WISTP'07. Berlin, Germany: Springer-Verlag, 2007: 115-126.

[6] Rafael C, Ricardo D. Two Notes on the Security of Certificateless Signatures[C]//Proc. of ProvSec'07. Heidelberg, Germany: Springer-Verlag, 2007: 85-102.

[7] 曹雪菲, Kenneth G P, 寇卫东. 对一类无证书签名方案的攻击及改进[J]. 北京邮电大学学报, 2008, 31(2): 64-67.

[8] 明　洋, 王育民. 有效的无证书签名方案[J]. 电子科技大学学报, 2008, 37(2): 175-177.

[9] 王　旭, 钱雪忠. 一个标准模型下可证明安全的无证书签名方案[J]. 计算机工程与应用, 2008, 44(11): 129-132.

编辑　索书志

(上接第 139 页)

参考文献

[1] Zheng Yuliang. Digital Signcryption or How to Achieve Cost (Signature & Encryption) Cost(Signature)+Cost(Encryption)[C]//Proc. of Cryptology-CRYPYO'97. Berlin, Germany: Springer-Verlag, 1997.

[2] 耿　莉, 王尚平, 周　峰, 等. 一种新的基于身份的签密方案[J]. 计算机工程, 2004, 30(19): 52-54.

[3] He Weihua, Wu Tongchen. Cryptanalysis and Improvement of Petersen-michels Signcryption Scheme[J]. IEE Proceedings: Computers and Digital Technique, 1999, 146(2): 123-124.

[4] Bao Feng, Deng R H. A Signcryption Scheme with Signature Directly Verifiable by Public Key[C]//Proc. of Cryptography-PKC'98. Berlin, Germany: Springer-Verlag, 1998.

[5] Yum D H, Lee P J. New Signcryption Schemes Based on KCDSA[C]//Proc. of ICISC'01. Berlin, Germany: Springer-Verlag, 2001.

[6] Jung H Y, Lee D H, Lim J I, et al. Signcryption Schemes with Forward Secrecy[C]//Proc. of WISA'01. Seoul, Korea: [s. n.], 2001.

[7] 李发根. 基于双线性对的签密体制的研究[D]. 西安: 西安电子科技大学, 2007.

[8] Girault M. Self-certified Public Keys[C]//Proc. of Cryptology-EUROCRYPT'91. Berlin, Germany: Springer-Verlag, 1991.

编辑　顾姣健