DOI:10.16749/j.cnki.jecjtu.2015.04.018

文章编号:1005-0523(2015)04-0105-05

一个安全高效的无证书签名方案的分析和改进

刘二根[1],周华静[1,2],王 霞[1,2],郭红丽[1,2]

(华东交通大学1.理学院;2.系统工程与密码学研究所,江西 南昌 330013)

摘要:对刘倩等提出的一个无证书签名方案进行安全性分析。结果表明,方案存在公钥替换攻击,且方案使用了双线性对运算导致效率下降。在此基础上,提出一个新的不使用双线性对的无证书签名方案,并证明了方案可以抵抗两类攻击者的攻击。最后,将提出的改进方案与已有的无证书签名方案进行效率比较,发现新方案具有较高的效率。

关键词:无证书;数字签名;随机预言机模型;双线性对

中图分类号:TP309 **文献标志码**:A

数字签名是现代密码学的一个重要领域,最早的数字签名是基于证书的,而基于证书的密码学体制存在着证书的颁发,存储,撤销等问题。因此,解决此类问题成为密码学领域的重要研究方面。1985年,Shamir[1]第一次提出基于身份的密码学体制,在该体制下,用户密钥生成完全依赖密钥生成中心(KGC),因此,又不可避免地存在密钥托管问题。随着密码学的日益发展,2003年,Al-Riyami等[2]提出的无证书密码体制,既解决了传统的基于证书密码体制下繁琐的证书管理问题,也解决了基于身份密码体制下的密钥托管问题。基于无证书密码体制的种种优点,该体制一经提出便得到学者们的广泛关注。2005年,Huang等[3]首次比较详细地给出无证书签名方案安全模型的定义,并提出一个具体的基于无证书的签名方案。2007年,Liu等[4]也提出一个无证书签名方案。在接下来的几年里,无证书签名不断发展,学者们先后提出各种无证书签名方案。2008年,樊睿等[5]提出一个效率较高的无证书代理签名方案。2010年,李明祥等[6]提出一个高效的无证书部分盲签名方案。2014年,樊爱宛等[7]提出一个强安全的无证书签名方案,同年又提出另一个无证书签名方案[8]。随后,刘倩等[9]对一个无证书签名方案进行安全性分析,发现其对于两类攻击者的攻击并不安全,因此提出改进方案。通过对文献[9]的分析,发现仍然存在公钥替换攻击且效率不高,在此基础上进行改进,提出新的无证书签名方案。并对改进后的方案进行安全性证明和效率分析。

1 预备知识

1.1 困难问题及假设

定义1 离散对数问题(DLP):设G是一个椭圆曲线群,已知$aP\in G$,$a\in Z_q^*$,其中P为G的生成元,求解a的问题称为离散对数问题。

假设1 离散对数困难性假设:如果不存在一个概率多项式时间(PPT)的算法,在时间t内,以一个大于0的概率ε解得群G上的DL问题,则称离散对数困难性假设成立。

1.2 攻击者类型[2]

在无证书密码体制中存在两种类型的攻击者A_{I}和A_{II},分别具有不同的能力。① 类型Ⅰ攻击者A_{I}:A_{I}

收稿日期:2015-01-23

基金项目:国家自然科学基金项目(11061014,61240025);江西省高校科技落地计划项目(KJLD12067);江西省教育厅科研项目(GJJ13339);华东交通大学校立科研基金项目(11JC04)

作者简介:刘二根(1965—),男,教授,研究方向为图论及其应用。

不知道系统主密钥，但是可以任意替换用户公钥；② 类型Ⅱ攻击者$A_{Ⅱ}$：$A_{Ⅱ}$知道系统主密钥，但是不知道用户个人私钥，也不能替换用户公钥。

2 文献[9]方案分析

2.1 方案回顾

文献[9]提出一个改进的无证书签名方案。方案由系统参数生成、秘密值生成、公钥生成、私钥生成、签名及验证这6个算法组成，方案具体描述如下。

1）系统参数生成：设置系统安全参数为k，KGC（Key Generator Center）选取阶为q的加法循环群G_1和乘法循环群G_2，其中$q\leqslant 2^k$且为素数。双线性对映射为$e:G_1\times G_1\rightarrow G_2$，选取群$G_1$的一个生成元为$P\in G_1$，并随机选取$s\in_R \boldsymbol{Z}^*_q$作为系统主密钥，计算$P_{pub}$为系统公钥，$g$为公钥参数。选择两个安全哈希函数$H_1:\{0,1\}^*\times G_1\rightarrow G_1$，$H_2:\{0,1\}^*\times\{0,1\}^*\times G_1\times G_1\times G_1\rightarrow \boldsymbol{Z}^*_q$，则系统公开参数可表示为$params=\{q,e,g,G_1,G_2,P,P_{pub},H_1,H_2\}$，公开$params$，保密主密钥$s$。

2）秘密值生成：签名者A随机选取$x_A\in \boldsymbol{Z}^*_q$作为自己的秘密值并保存。

3）公钥生成：签名者A计算$PK_A=x_AP$作为自己的公钥，将其公开。

4）私钥生成：① 部分私钥：设签名者A的身份为ID_A，KGC计算$D_A=sQ_A=sH_1(ID_A)\in G_1$，将$D_A$作为签名者$A$的部分私钥，通过秘密信道发送给$A$；② 完整私钥：签名者$A$收到$D_A$后，计算$S_A=D_A=x_A\cdot H_1(ID_A,PK_A)\in G_1$，则用户完整私钥为$S_A$。

5）签名：签名者A的身份为ID_A，签名私钥为S_A，待签名消息为$m\in\{0,1\}^*$，由A执行签名算法。A随机选取一个随机数$r\in_R \boldsymbol{Z}^*_q$，计算$R=g^r\in G_2$，$h=H_2(m\|ID_A\|R\|PK_A)\in \boldsymbol{Z}^*_q$，$V=r\cdot P+h\cdot S_A\in G_1$，则签名为$\sigma=(h,V)$。

6）验证：验证者收到签名后首先计算$h=H_2(m\|ID_A\|R\|PK_A)$，如果等式$e(V,P)e(Q_A,P_{pub}+PK_A)^{-h}=R$成立，则说明签名有效，接受签名，输出1；否则，拒绝，输出0。

2.2 安全性与效率分析

通过对上述方案的分析，发现存在如下缺陷。

缺陷一：该方案存在公钥替换攻击，存在一个类型Ⅰ的攻击者F，可以替换用户公钥，具体攻击为：

攻击者F将签名者A的公钥替换为$PK'_A=P-P_{pub}$，并随机选取随机数为$r'\in_R \boldsymbol{Z}^*_q$，则$R'=g^{r'}$，$h'=H_2(m\|ID_A\|R'\|PK_A)\in \boldsymbol{Z}^*_q$，计算签名为$V'=r'P+h'Q_A$。返回签名$\sigma'=(h',V')$给验证者。下面证明由攻击者伪造的该签名$V'$可以通过验证等式

$$e(V',P)e(Q_A,P_{pub}+PK'_A)^{-h}=e(r'P+hQ_A,P)e(Q_A,P_{pub}+PK'_A)^{-h}=e(P,P)^{r'}e(Q_A,P)^{h}e(Q_A,P)^{-h}=R' \tag{1}$$

因此，签名可以通过验证等式，也就是说攻击者F将签名者A的公钥替换后伪造的签名$\sigma'=(h',V')$是有效的。即方案不能抵抗公钥替换攻击。

缺陷二：通过对方案的效率分析，可以看出上述方案在签名的验证阶段使用了两次双线性对运算，而双线性对运算的时间复杂度和计算复杂度都比哈希运算和指数运算的要高的多。因此，使用双线性对运算会使方案效率下降。

3 方案改进

针对上述方案中安全性及效率上的缺陷，提出一个可抗公钥替换攻击且效率更高的无证书签名方案。方案包括系统初始化（Setup）、用户个人密钥生成（UserKeyGen）、部分私钥生成（PartKeyGen）、签名密钥生成（SignKey）、签名（Sign）及验证（Verify）这6个算法。方案描述如下。

1）系统初始化：设系统安全参数为1^k，KGC选取一个大素数$q\leqslant 2^k$，并生成以q为阶的加法循环群G_1和乘法循环群G_2，选取群G_1的一个生成元$P\in G_1$，并随机选取$s\in_R \boldsymbol{Z}^*_q$作为系统主密钥，计算$P_{pub}=sP$作为

系统主公钥。作双线性对映射 $e:G_1\times G_1\rightarrow G_2$，选取两个安全哈希函数分别为：$H_1:\{0,1\}^*\times G_1\rightarrow Z_q^*$，$H_2:\{0,1\}^*\times\{0,1\}^*\times G_1\rightarrow Z_q^*$。系统公开参数为 $params=\{q,e,G_1,G_2,P,P_{pub},H_1,H_2\}$，KGC公开 $params$，保密 s。

2）用户个人密钥生成：签名者 A 随机选取 $x_A\in Z_q^*$ 作为用户个人私钥，计算 $X_A=x_AP$ 作为对应的公钥，公开 X_A，保密 x_A。

3）部分私钥生成：此算法由KGC执行，KGC随机选取 $y_A\in Z_q^*$，计算 $D_A=s+y_A+H_1(ID_A,X_A)$ 作为用户的部分私钥，并通过安全信道发送给 A。

4）签名密钥生成：签名者 A 收到 D_A 后，计算 $SK_A=D_A+x_AH_1(ID_A,X_A)$ 作为签名密钥，对应的签名公钥为 $PK_A=SK_AP$。

5）签名：设待签名消息为 $m\in\{0,1\}^*$，签名者 A 随机选取随机数 $k\in Z_q^*$，计算 $K=kP$，$h=H_2(m,ID_A,K)$，$V=SK_A^{-1}(k+h)$，则消息 m 对应的签名对为 $\sigma=(m,K,h,V)$。

6）验证：验证者收到消息 m 的签名对 $\sigma=(m,K,h,V)$ 后，对其进行验证，如果等式 $K=VPK_A-hP$ 成立，则说明签名有效，输出1；否则，签名无效，输出0。

4　新方案的安全性分析

4.1　抗类型Ⅰ攻击者的攻击

定理1　新方案可以抵抗类型I攻击者的公钥替换攻击。

证明　因为类型I攻击者可以任意替换用户公钥，但是在改进的新方案中，由于在KGC生成的部分私钥中利用哈希运算将用户个人公钥进行绑定，因此攻击者无法替换用户公钥。即新方案可以抵抗类型I攻击者的攻击。

4.2　抗类型Ⅱ攻击者的攻击

定理2　新方案对于类型Ⅱ攻击者的适应性选择消息和身份攻击，在随机预言机模型下是存在性不可伪造的。

证明　设一个类型Ⅱ攻击者 $A_{Ⅱ}$。如果在多项式有界的时间 t 内，$A_{Ⅱ}$ 能够以一个不可忽略的概率 ε 伪造一个有效的签名，只需证明，存在一个概率多项式时间的挑战算法 Ω 可以利用 $A_{Ⅱ}$ 成功解决DL问题，问题实例为，已知 (P,aP)，求解 a。在下面的证明中，Ω 模拟密钥生成中心，回答 $A_{Ⅱ}$ 的一系列适应性询问，用 a 模拟签名私钥，设目标用户身份为 ID^*，对应的待签名消息为 m^*。$A_{Ⅱ}$ 向 Ω 进行如下适应性询问：哈希询问、用户个人密钥询问、部分密钥询问、签名密钥询问、签名询问，而 Ω 通过维护一些列表模拟对 $A_{Ⅱ}$ 的回答。

H_1 询问：对应的列表格式为 $L_1(ID_j,X_j,h_{1j})$，$A_{Ⅱ}$ 向 Ω 进行用户身份为 ID_i 的 H_1 询问。Ω 首先检查列表 L_1，如果列表中存在 (ID_i,X_i,h_{1i}) 的项，则直接返回 h_{1i} 给 $A_{Ⅱ}$；否则，列表中不存在 (ID_i,X_i,h_{1i}) 的项，Ω 随机选取 $h_{1i}\in {}_RZ_q^*$，返回给 A_{II}，并将 (ID_i,X_i,h_{1i}) 添加到列表。

H_2 询问：对应的列表格式为 $L_2(m_j,ID_j,K_j,h_{2j})$，$A_{Ⅱ}$ 向 Ω 进行消息为 m_i，用户身份为 ID_i 的 H_2 询问。Ω 检查列表 L_2，如果列表中存在 (m_i,ID_i,K_i,h_{2i}) 的项，直接返回 h_{2i} 给 $A_{Ⅱ}$；否则，Ω 随机选取 $h_{2i}\in {}_RZ_q^*$，并返回给 $A_{Ⅱ}$，将 (m_i,ID_i,K_i,h_{2i}) 添加到列表。

用户个人密钥询问：每一项列表的格式为 $L_s(ID_j,x_j,X_j)$，$A_{Ⅱ}$ 向 Ω 进行用户身份为 ID_i 的签名密钥询问。Ω 先查询列表 L_s，如果列表中已经存在 (ID_i,x_i,X_i) 的项，直接返回 (x_i,X_i) 给 $A_{Ⅱ}$。否则：

1）如果 $ID_i\neq ID^*$，Ω 随机选取 $x_i\in {}_RZ_q^*$，计算 $X_i=x_iP$，并将 (x_i,X_i) 返回给 $A_{Ⅱ}$，同时将 (ID_i,x_i,X_i) 添加到列表 L_s 中。

2）如果 $ID_i=ID^*$，即 $A_{Ⅱ}$ 询问的是目标用户的个人密钥，Ω 拒绝回答，返回 $(\perp,X_i)$ 给 $A_{Ⅱ}$，并将 $(ID_i,\perp,X_i)$ 添加到列表 L_s 中。

部分密钥询问：对应的列表中每项的格式为 $L_k(ID_j,D_j)$，$A_{\text{Ⅱ}}$向 Ω 进行用户身份为 ID_i 的部分密钥询问。Ω 检查列表 L_k，如果列表中存在 (ID_i,D_i) 的项，直接返回 D_i 给 $A_{\text{Ⅱ}}$。否则：

1）如果 $ID_i \neq ID^*$，Ω 首先查询列表 L_1（假设在此之前已经进行过 H_1 询问，否则可以先进行 H_1 询问），得到 h_{1i}，随机选取 y_i，计算 $D_i = s + y_i + h_{1i}$，并返回给 $A_{\text{Ⅱ}}$，将 (ID_i,D_i) 添加到列表。

2）如果 $ID_i = ID^*$，Ω 拒绝回答，询问终止。

签名密钥询问：相应的列表格式为 $L_{sk}(ID_j,SK_j,PK_j)$，$A_{\text{Ⅱ}}$向 Ω 询问身份为 ID_i 的用户的签名密钥。Ω 检查列表，如果列表中存在 (ID_i,SK_i,PK_i) 的项，直接返回 (SK_i,PK_i) 给 $A_{\text{Ⅱ}}$。否则

1）如果 $ID_i \neq ID^*$，Ω 查询列表 L_1，L_s，L_k 分别得到相应的 h_{1i}，x_i 及 D_i 的值（假设在此之前已经进行过 H_1 询问，用户个人密钥询问及部分密钥询问，不然可以先进行询问），直接计算 $SK_i = D_i + x_i h_{1i}$，$PK_i = SK_i \cdot P$，将 (SK_i,PK_i) 返回给 $A_{\text{Ⅱ}}$，并将 (ID_i,SK_i,PK_i) 添加到列表 L_{sk} 中。

2）如果 $ID_i = ID^*$，Ω 拒绝回答，询问终止。

签名询问：$A_{\text{Ⅱ}}$向 Ω 询问用户身份为 ID_i，待签名消息为 m_i 的签名询问。如果 $ID_i \neq ID^*$，Ω 查询列表 L_2 和 L_{sk}，得到 h_{2i} 及 SK，并随机选取 $k_i \in {}_K\boldsymbol{Z}_q^*$，计算 $V_i = SK_i^{-1}(k_i + h_{2i})$，返回给 $A_{\text{Ⅱ}}$；如果 $ID_i = ID^*$ 且 $m_i = m^*$，Ω 查询列表 L_2，得到 h_{2i} 的值，随机选取 $k_i \in {}_K\boldsymbol{Z}_q^*$，计算 $K_i = k_i P$，再计算 $V_i = (K_i + h_{2i}P)PK_A^{-1}$，将 V_i 返回给 $A_{\text{Ⅱ}}$。

攻击与挑战：最后，经过若干轮的询问，$A_{\text{Ⅱ}}$可以成功伪造出目标用户 ID^* 对于消息 m^* 的签名 $\sigma^* = (m^*,K^*,h^*,V^*)$，根据 Forking 引理[10]知，通过对哈希运算进行分叉，$A_{\text{Ⅱ}}$还可以输出另一个有效签名 $\hat{\sigma}^* = (m^*,K^*,\hat{h}^*,\hat{V}^*)$，下面看算法 Ω 利用 $A_{\text{Ⅱ}}$解决困难问题。

由于 $A_{\text{Ⅱ}}$输出的2个伪造签名都是有效的，因此满足验证等式

$$K^* = V^* PK^* - h^* P \tag{2}$$

$$K^* = \hat{V}^* PK^* - \hat{h}^* P \tag{3}$$

联立式(2)式(3)得 $V^* PK^* - h^* P = \hat{V}^* PK^* - \hat{h}^* P$，因此 $PK^* = (V^* - \hat{V}^*)^{-1}(h^* - \hat{h}^*)P$。

即 $aP = (V^* - \hat{V}^*)^{-1}(h^* - \hat{h}^*)P$，解得 $a = (V^* - \hat{V}^*)^{-1}(h^* - \hat{h}^*)$。

也就是说，挑战者 Ω 成功解决了离散对数困难问题，这与困难性假设矛盾。因此，对于类型Ⅱ攻击者，在适应性选择消息和身份攻击下满足存在性不可伪造。

5 效率比较

将改进后的新方案与其他签名方案进行效率比较，其中P表示双线性对运算，H表示哈希运算，E表示指数运算，M表示标量乘运算，结果如表1所示。

表1 各方案效率比较

Tab.1 The efficiency comparison of each scheme

方案	密钥生成阶段	签名阶段	验证阶段
文献[9]方案	1H+2M	1H+1E+2M	2P+1E
文献[11]方案	1H+1M	1H+3M	3P+1E
文献[12]方案	2H+2M	1P+1H+1E+2M	3P+1H+1E
本文的方案	1H+1M	1H+2M	2M

由于双线性对运算的时间复杂度和计算复杂度都较高，一次双线性对运算的计算复杂度分别是指数运算和哈希运算的7倍和21倍；时间复杂度是指数运算的10倍[5]。从表1可以看出，本文方案全文没有使用双线性对运算，效率较高。

6　结束语

通过对文献[9]的分析和研究,发现文献[9]中的方案在安全性和效率方面都存在漏洞,因此对其进行改进,并在随机语言机模型下证明了改进方案满足存在不可伪造性。将本文方案与已有无证书签名方案进行效率比较,发现本文方案在效率上具有优势。

参考文献:

[1] SHAMIR A. Identity-Based Cryptosystem and Signature Scheme[C]//Advances in Cryptology-Crypto′84. Berlin: Springer-Verlag, 1984:47-53.
[2] AL-RIYAMI S, PATERSON K G. Certificateless Public Key Cryptography[C]//Advances in Cryptology-ASIACRYPT′03. Berlin: Springer-Verlag, 2003:452-473.
[3] HUANG X, SUSILO W, MU Y, et al. On the security of a certificateless signature Schemes from Asia Crypt′03[C]//Proceedings of CANS′05. Berlin: Springer-Verlag, 2005:13-25.
[4] LIU J K, AU M H, SUSILO W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model [C]// Proc ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2007:302-311.
[5] 樊睿,王彩芬,蓝才会,等. 新的无证书代理签名方案[J]. 计算机应用, 2008,28(4):915-917.
[6] 李明祥,杜光辉,罗新方. 高效的无证书部分盲签名方案[J]. 计算机工程与设计, 2010,31(22):4817-4819.
[7] 樊爱宛,杨照峰,谢丽明. 强安全无证书签名方案的安全性分析和改进[J]. 通信学报, 2014,35(5):118-123.
[8] 樊爱宛,申远,赵伟艇. 无证书签名方案的安全性分析与改进[J]. 计算机应用, 2014,34(8):2342-2344,2349.
[9] 刘倩,范安东,张丽娜,等. 一个高效的无证书签名方案分析与改进[J]. 河南科技大学学报:自然科学版, 2014,35(4):49-53.
[10] POINTCHEVAL D, STERN J. Security Proofs for Signature Schemes[C]//Proceedings of the EUROCRYPT′96. Spain: Saragossa, 1996:387-398.
[11] 王丽莎,张建中. 一种高效安全的无证书数字签名方案[J]. 计算机工程与应用, 2012,48(15):70-73.
[12] 张磊,张福泰. 一类无证书签名方案的构造方法[J]. 计算机学报, 2009,32(5):940-945.
[13] 陈玲玲,亢保元,张磊. 一种高效的基于身份的代理盲签名方案[J]. 华东交通大学学报, 2008,25(1):113-116.

Analysis and Improvement of Secure and Efficient Certificateless Signature Scheme

Liu Ergen[1], Zhou Huajing[1,2], Wang Xia[1,2], Guo Hongli[1,2]

(1.School of Science, East China Jiaotong University, Nanchang 330013, China; 2. Institute of Engineering and Cryptography, East China Jiaotong University, Nanchang 330013, China)

Abstract: The security analysis of the certificateless signature scheme proposed by Liu Qian et al. shows that the scheme is not secure for public key replacement attack and the efficiency of the scheme is low due to the usage of bilinear pairings. This paper proposes a new certificateless signature scheme without bilinear pairings on the basis of original scheme, and it is proved that the new scheme is secure for two types of attackers. After comparing the new scheme with existing signature schemes, it maintains that the new scheme is efficient.

Key words: certificateless; digital signature; random oracle model; bilinear pairings

(责任编辑　姜红贵)