第 39 卷 第 5 期
Vol.39 No.5

计 算 机 工 程
Computer Engineering

2013 年 5 月
May 2013

• 安全技术 •

文章编号：1000—3428(2013)05—0156—04 文献标识码：A 中图分类号：TP309.2

一种无证书签名方案的安全性分析及改进

潘 帅，高德智，翟正元

(山东科技大学信息科学与工程学院，山东 青岛 266590)

摘 要：分析洪东招等人提出的无证书签名方案(计算机应用，2010 年第 7 期)，指出该方案不能抵抗公钥替换攻击和恶意的私钥产生器(PKG)攻击，同时采用由 PKG 生成用户公钥并公开的方法对方案进行改进。安全性分析结果表明改进方案可抵抗公钥替换攻击和恶意 PKG 攻击，并基于 q-SDH 问题和扩展逆计算 Diffie-Hellman 问题是困难的假设，在随机预言模型中证明该方案的安全性。

关键词：无证书签名；双线性对；q-SDH 问题；公钥替换攻击；扩展逆计算 Diffie-Hellman 问题；恶意私钥产生器攻击

Security Analysis and Improvement of an Certificateless Signature Scheme

PAN Shuai, GAO De-zhi, ZHAI Zheng-yuan

(College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China)

【Abstract】This paper shows that Hong's efficient certificateless signature scheme is insecure against public key replacement attacks and malicious Private Key Generator(PKG) attacks. Aiming at these problems, the scheme is improved by the means that PKG generates the user's public key and makes it public. The analysis of security shows that the improved scheme is able to resist public key replacement attacks and malicious PKG attacks. Its security relies on the hardness of the q-Strong Diffie-Hellman(q-SDH) problem and Extended-Inverse-Computational Diffie-Hellman(E-Inv-CDH) problem. Under the random oracle model, the improved scheme is proved to be secure against existential forgery on adaptively chosen message attacks.

【Key words】certificateless signature; bilinear pairing; q-SDH problem; public key replacement attack; Extended-Inverse-Computational Diffie-Hellman(E-Inv-CDH) problem; malicious Private Key Generator(PKG) attack

DOI: 10.3969/j.issn.1000-3428.2013.05.034

1 概述

为解决普通公钥签名方案的证书管理问题和基于身份签名方案固有的密钥托管问题，文献[1]提出第一个无证书签名方案。它是介于传统证书签名方案和基于身份的签名方案之间的一种签名方法。这种签名方法不仅保持了基于身份签名方案的所有优点(即不需要利用证书对公钥进行认证)，而且消除了它内在的密钥托管问题。但之后文献[2]指出文献[1]方案存在公钥替换攻击安全缺陷并提出了更安全的方案，随后文献[3]提出了一个无证书签名的通用结构，并通过安全分析证明其方案能抵抗 PKG 攻击和密钥替换攻击。文献[4]发现，当文献[3]方案对“消息和密钥替代攻击”存在脆弱性时，此方案是不安全的。文献[5-6]也提出一些签名方案，虽然提出的方案效率比较高，但随后都被证明存在公钥替换攻击。文献[7]使用哈希函数提出一个效率比较高的可证明安全的数字签名方案，但文献[8]指出此方案对替换公钥攻击是不安全的。文献[8]虽然在公钥替换攻击问题上取得了一定成果，但忽略了 PKG 的诚信问题，存在恶意的 PKG 攻击。在无证书公钥系统中，由于用户的公钥没有被认证，因此考虑替换公钥攻击是必须的。

文献[9]提出一个有效的无证书签名方案(简称洪方案)，并在随机预言模型下证明了它的安全性。但通过分析笔者发现，该方案不能抵抗公钥替换攻击和恶意的 PKG 攻击。本文分析洪方案，对其进行安全性分析，同时给出一个改进方案，并在随机预言模型下证明该方案的安全性。

2 预备知识

2.1 双线性群

为叙述方便，本文采用与文献[9]中类似的符号。设 G_1,G_2,G_T 是一个阶为素数 q 的群组，其中，G_1,G_2 为加法群，

基金项目：青岛市科技发展计划基金资助项目(11-2-4-6-1-jch)

作者简介：潘 帅(1987－)，女，硕士研究生，主研方向：密码学，信息安全；高德智，教授、博士；翟正元，硕士研究生

收稿日期：2012-05-08 **修回日期：**2012-08-03 **E-mail：**panshuai8676@163.com

G_T 为乘法群。P,Q 分别是 G_1,G_2 的生成元。如果 $e:G_1\times G_2\to G_T$ 满足下列性质的，则称(G_1,G_2,G_T)是一个双线性群，e 是双线性映射。

(1)双线性性：$\forall(S,T)\in G_1\times G_2,\forall a,b\in Z_q^*$，$e(aS,bT)=e(S,T)^{ab}$。

(2)非退化性：存在 $S\in G_1,T\in G_2$，使 $e(S,T)\neq 1$。

(3)可计算性：$\forall(S,T)\in G_1\times G_2$，存在有效的算法可计算 $e(S,T)$。

(4)存在一个高效公开可计算(但不一定可逆)的同构映射：$\phi:G_2\to G_1$，使 $\phi(Q)=P$。

2.2 相关困难问题

考虑双线性群 (G_1,G_2,G_T)，其中，P 是 G_1 的生成元，Q 是 G_2 的生成元。

(1)q 强 Diffie-Hellman 问题(q-SDHP)：在群 G_1,G_2 上，给定元组 $(P,Q,\alpha Q,\cdots,\alpha^q Q)$ 计算一个对 $\left(c,\frac{1}{\alpha+c}P\right)$，其中，$c\in Z_q^*$。

(2)扩展逆计算 Diffie-Hellman 问题(E-Inv-CDHP)：在群 G_1,G_2 上，对于未知的 $\frac{1}{a}\in Z_q^*$，$P\in G_1$，$Q\in G_2$，给定 $(P,\frac{1}{a}Q)$，计算 aP。

3 洪方案的密码学分析

3.1 洪方案介绍

洪方案包括 7 个算法：系统建立，部分私钥生成，设置秘密值，设置私钥，设置公钥，签名算法，验证算法。

(1)系统建立：k 是安全参数，PKG 选择双线性群 (G_1,G_2,G_T) 且阶均为素数 $q>2^k$，Q 为群 G_2 的生成元，$P=\phi(Q)\in G_1$ 为 G_1 的生成元。$e:G_1\times G_2\to G_T$ 是一个安全的双线性对映射，设 $g=e(P,Q)\in G_T$，随机选择 $s\in Z_q^*$ 作为系统主密钥，计算 $Q_{\text{Pub}}=sQ\in G_2$，选择 2 个 Hash 函数：$H_1:\{0,1\}^*\to Z_q^*,H_2:\{0,1\}^*\times G_T\to Z_q^*$ 秘密保存主密钥 s，公开参数 $params=\{G_1,G_2,G_T,P,Q,g,q,Q_{\text{Pub}},e,\phi,H_1,H_2\}$。

(2)部分私钥生成：已知 $ID\in\{0,1\}^*$，PKG 计算 $Q_{ID}=H_1(ID)$，$d_{ID}=\frac{1}{s+Q_{ID}}P$，通过安全信道发送 d_{ID} 给 ID 用户作为部分私钥。ID 用户验证等式 $e(d_{ID},Q_{\text{Pub}}+Q_{ID}Q)=g$。

(3)设置秘密值：ID 用户随机选取 $r\in Z_q^*$，把 r 作为自己的秘密值。

(4)设置私钥：已知系统参数，用户部分私钥 d_{ID}，秘密值 r，输出用户私钥 $SK_{ID}=rd_{ID}$。

(5)设置公钥：输入系统参数，用户的秘密值 r，产生用户公钥 $PK_{ID}=\frac{1}{r}(Q_{\text{Pub}}+Q_{ID}Q)$。

(6)签名算法：随机选择 $x\in Z_q^*$，计算 $R=g^x$，$h=H_2(m,R)$，$S=(x+h)SK_{ID}$，则消息 m 的签名为 $\sigma=(S,R)$。

(7)验证算法：计算 $h=H_2(m,R)$，接受签名并且返回 1，当且仅当等式 $Ver(m,ID,PK_{ID},\sigma)=1\Leftrightarrow e(S,PK_{ID})g^{-h}=R$ 成立。

3.2 洪方案安全性分析

对洪方案的安全性分析如下：

(1)公钥替换攻击

由于在 CL-PKC 中，没有对用户的公钥进行认证，因此存在公钥替换攻击。经过分析发现，洪方案不能抵抗公钥替换攻击。具体攻击方法如下：

攻击者执行以下步骤：选择 $y\in Z_q^*$，并设 $PK_{ID}'=yQ$，然后随机选择 $x'\in Z_q^*$，计算 $R'=g^{x'}$，$h'=H_2(m,R')$，$S'=(x'+h')\frac{1}{y}P$，则 (S',R') 为身份 ID，公钥 PK_{ID}' 关于消息 m 的有效签名。容易验证：

$$e(S',PK_{ID}')g^{-h'}=e\left(\frac{x'+h'}{y}P,yQ\right)g^{-h'}=$$
$$e(P,Q)^{\frac{1}{y}(x'+h')y}g^{-h'}=e(P,Q)^{(x'+h')}e(P,Q)^{-h'}=$$
$$e(P,Q)^{x'}=R'$$

(2)恶意的 PKG 攻击

恶意的 PKG 利用用户的部分私钥，可以伪造对身份 ID，关于消息 m 的签名。具体步骤如下：

首先，恶意的 PKG 选择 $r'\in Z_q^*$，计算用户的私钥 $SK_{ID}'=r'\frac{1}{s+Q_{ID}}P$ 和公钥 $PK_{ID}'=r'^{-1}(Q_{\text{Pub}}+Q_{ID}Q)$，然后，随机选择 $x'\in Z_q^*$，计算 $R'=g^{x'}$，$h'=H_2(m,R')$，$S'=(x'+h')SK_{ID}'$，则伪造签名 $\sigma'=(R',S')$ 能够得到确认。对伪造签名进行验证的正确性如下：

$$e(S',PK_{ID}')g^{-h'}=e\left((x'+h')r'\frac{1}{s+Q_{ID}}P,r'^{-1}(Q_{\text{Pub}}+Q_{ID}Q)\right)g^{-h'}=$$
$$e\left((x'+h')r'\frac{1}{s+Q_{ID}}P,r'^{-1}(sQ+Q_{ID}Q)\right)g^{-h'}=$$
$$e\left((x'+h')r'\frac{1}{s+Q_{ID}}P,r'^{-1}(s+Q_{ID})Q\right)g^{-h'}==$$
$$e((x'+h')P,Q)g^{-h'}=e(P,Q)^{x'}=R'$$

综上所述，洪方案不能抵抗恶意的 PKG 攻击。

4 改进方案

本文采用与文献[10]中相类似的方法进行改进，即由 PKG 根据用户给定的信息来生成用户公钥并将其公布到系统参数中。将用户公钥公布到系统参数中是为了阻止攻击者进行公钥替换攻击，用给定的用户信息生成用户公钥是为了用户对其进行验证防止恶意的 PKG 攻击，这样就解决了原方案中存在的问题。具体改进方案如下：

(1)设置秘密值：ID 用户随机选取 $x\in Z_q^*$，作为自己的

秘密值，计算 $X=\frac{1}{x}Q$，并将其发送给 PKG。

(2)系统设置：给定安全参数 k，用户的 ID 和用户发送的 X，PKG 执行以下步骤：

1)PKG 选择双线性群 (G_1,G_2,G_T)，其阶为素数 $q>2^k$，并且 Q 为群 G_2 的生成元，$P=\phi(Q)\in G_1$ 为 G_1 生成元，$e:G_1\times G_2\to G_T$ 是一个安全的双线性映射。选择 2 个 Hash 函数：$H_1:\{0,1\}^*\to Z_q^*$，$H_2:\{0,1\}^*\times\{0,1\}^*\times G_T\to Z_q^*$。

2)PKG 随机选择 $s\in Z_q^*$，计算 $Q_{\text{Pub}}=sQ,\ g=e(P,Q),\ Q_{ID}=H_1(ID)$，并秘密保存主密钥 s。

3)PKG 计算 $PK_{ID}=(s+Q_{ID})X=\frac{1}{x}(Q_{\text{Pub}}+Q_{ID}Q)$ 作为用户公钥，并公开系统参数 $params=\{G_1, G_2, G_T, P, Q, g, q, Q_{\text{pub}}, e,\phi,H_1,H_2,PK_{ID}\}$。

(3)部分私钥生成算法：PKG 计算 $D_{ID}=\frac{1}{s+Q_{ID}}P$，并将部分私钥 D_{ID} 通过安全信道发送给用户。

(4)私钥生成算法：用户通过等式 $e(D_{ID},Q_{\text{Pub}}+Q_{ID}Q)=g$，对部分私钥 D_{ID} 进行验证，若验证通过，则生成用户私钥 $SK_{ID}=xD_{ID}$。

(5)公钥验证算法：用户通过等式 $PK_{ID}=\frac{1}{x}(Q_{\text{Pub}}+Q_{ID}Q)$ 验证用户公钥 PK_{ID} 的真实性。

(6)签名算法：选择随机值 $r\in Z_q^*$，计算 $R=g^r$，$h=H_2(m,ID,R)$，$S=(r+h)SK_{ID}$，则用户对消息 m 的签名为 $\sigma=(R,S)$。

(7)验证算法：给定签名 $\sigma=(R,S)$，用户 ID，消息根据公开的系统参数 $params$，执行下列计算：

1)计算 $h=H_2(m,ID,R)$；

2)验证 $e(S,PK_{ID})g^{-h}=R$ 是否成立，成立则接受签名，否则拒绝。

方案正确性验证如下：

$$e(S,PK_{ID})g^{-h}=e((r+h)SK_{ID},PK_{ID})g^{-h}=$$
$$e\left((r+h)x\frac{1}{s+Q_{ID}}P,X(s+Q_{ID})\right)g^{-h}=$$
$$e\left((r+h)x\frac{1}{s+Q_{ID}}P,\frac{1}{x}Q(s+Q_{ID})\right)g^{-h}=$$
$$e(P,Q)^{(r+h)}g^{-h}=e(P,Q)^r=g^r=R$$

5 改进方案的安全性分析

如文献[2]中所述，用户私钥由 PKG 生成的部分私钥和用户自己选择的秘密值共同构成，因此，在 CL-PKC 中有 2 种攻击模型。

类型 1 攻击者可以替换任何用户的公钥，但不具有系统主密钥，它可以做任何询问，但不能询问目标身份 ID^* 的部分私钥。

类型 2 攻击者拥有系统主密钥，但不能替换用户的公钥，他可以做任何询问，但不能询问目标身份 ID^* 的公钥所对应的秘密值。下面参考文献[11]，证明改进方案在 2 种攻击模型下是存在性不可伪造的。

定理 1 在随机预言模型中，类型 1 攻击下，如果存在攻击者 A_1 能够在 t_1 时间内、利用 q_{H_1} 次 H_1 询问和 q_s 次签名询问、以 $\varepsilon_1\geqslant 10\times(q+1)\times(q_s+q_{h_1})/2^k$ 的概率攻破改进后的方案，则能构造一个算法 B 利用 A_1 在多项式时 $t_1'\leqslant(120\,686\times q_{H_1}\times t_1)/(\varepsilon_1\times(1-1/2^k))$ 内解决 q-SDHP 困难问题。

证明：假设存在类型 1 的敌手 A_1，则可以构造一个算法 B，它可以通过和 A_1 交互来解决 q-SDH 问题。假设 A_1 攻击的目标身份是 ID^*，最终他能伪造身份 ID^* 关于消息 m^* 的有效签名。在证明过程中，H_1, H_2 可以看作是随机预言机。

给定 B 一个多元组 $(P,Q,\alpha Q,\alpha^2Q,\cdots,\alpha^qQ)$，其目标是计算一个对 $\left(c,\frac{1}{c+\alpha}P\right)$，其中，$\alpha,c,q\in Z_q^*$。下面证明算法 B 能利用 A_1 来解决 q-SDHP 问题。

(1)建立系统参数

1)选择生成元 $G\in G_1$，则可计算 q–1 个对 $\left(y_i,\frac{1}{y_i+\alpha}G\right)$，其中，$y_1,y_2,\cdots,y_{q-1}\in {}_RZ_q^*$，展开 $f(Z)=\prod_{i=1}^{q-1}(Z+y_i)$ 可获得 $c_0,c_1,\cdots,c_{q-1}\in Z_q^*$，满足 $f(Z)=\sum_{i=0}^{q-1}c_iZ^i$。设 $H=\sum_{i=0}^{q-1}c_i(\alpha^iQ)=f(\alpha)Q\in G_2$，$G=\phi(H)=f(\alpha)P\in G_1$，那么公钥 $H_{\text{Pub}}=\sum_{i=1}^{q}c_{i-1}(\alpha^iQ)=\alpha H$。

2)对 $1\leqslant i\leqslant q-1$，B 计算 $f_i(Z)=\frac{f(Z)}{Z+y_i}=\sum_{i=0}^{q-2}d_iZ^i$，则 $\sum_{i=0}^{q-2}d_i\phi(\alpha^iQ)=f_i(\alpha)P=\frac{f(\alpha)}{\alpha+y_i}P=\frac{1}{\alpha+y_i}G$，从而计算出对 $\left(y_i,\frac{1}{y_i+\alpha}Q\right)$。B 计算 $g=e(G,H)$，$H_{\text{Pub}}=\alpha H$，并将系统参数 $params=\{G_1,G_2,G_T,G,H,q,H_{\text{Pub}},e,\phi,H_1,H_2,PK_{ID}\}$ 发送给 A_1，并且为了简单起见假设以下 A_1 的每次询问都是不同的。A_1 随机选择一个挑战身份 $ID^*\in\{0,1\}^*$，挑战消息 m^*。

(2) H_1 询问：当 A_1 对 H_1 进行关于身份 ID_i 的 Hash 询问时，如果 $ID_i=ID^*$，B 返回一个随机 $Q^*\in Z_q^*$ 且 $Q^*\notin\{y_1,y_2,\cdots,y_{q_h}\}$，其中，$q_h$ 表示 H_1 询问的最大次数；否则 B 随机选择 $Q_i\in\{y_1,y_2,\cdots,y_{q_h}\}$ 给 A 作为 $H_1(ID_i)$ 的值。

(3) H_2 询问：当 A_1 关于消息 m^*、ID_i、R_i 对 H_2 进行 Hash 询问时，B 随机选择 $h_i\in Z_q^*$ 给 A_1 作为 $H_2(m_i,ID_i,R_i)$ 的值。

(4)部分私钥询问：当 A_1 询问身份 ID_i 的部分私钥时，B 判断是否有 $ID_i=ID^*$ 成立，若 $ID\neq ID^*$，则 B 计算

$D_{ID_i}=\left(\frac{1}{\alpha+Q_i}\right)G$ 返回给 A_1，否则 B 停止。

(5)公钥询问：当收到 A_1 关于身份 ID_i 的公钥询问，B 判断是否有 $ID_i=ID^*$ 成立，若 $ID\neq ID^*$，B 随机选择 $r_i\in Z_q^*$，计算 $PK_{ID_i}=\frac{1}{r_i}\left(H_{Pub}+Q_iH\right)$ 并返回给 A_1，否则 B 随机选择 $r^*\in Z_q^*$，计算 $PK_{ID^*}=\frac{1}{r^*}\left(H_{\text{Pub}}+Q^*H\right)$。

(6)私钥询问：当 A_1 询问身份 ID_i 的私钥时，B 判断是否有 $ID_i=ID^*$ 成立，若 $ID\neq ID^*$，B 返回私钥 $SK_{ID_i}=r_iD_{ID_i}$ 给 A_1，否则 B 停止。

(7)公钥替换询问：当收到 A_1 关于身份 ID_i 的公钥替换询问，B 设 ID_i 的公钥为 $PK_{ID_i}{}'$，秘密值为 r'。

(8)签名询问：当 A_1 询问 (m^*,ID_i) 签名时 B 判断是否有 $ID_i=ID^*$ 成立，若 $ID\neq ID^*$，B 根据签名算法计算出 $\sigma=(R,S)$ 并返回给 A_1。否则 B 停止。

(9)伪造：A_1 输出身份为 ID_i 及公钥为 $PK^*_{ID^*}$ 关于消息 m^* 的有效签名 $\sigma=(R,S)$，由 Rafael-Ricardo 分叉引理[12]可知：若 $\varepsilon_1\geqslant 10\times(q_s+1)\times(q_s+q_{h_1})/2^k$，则 A_1 能够生成消息 m^* 的另一个有效的签名 $\sigma'=(R,S')$，则有 $e(S,PK^*_{ID^*})g^{-h}=e(S',PK^*_{ID^*})g^{-h'}$，其中，$h\neq h'$，则有：

$$e(S-S',PK^*_{ID^*})=g^{h-h'}\Leftrightarrow e\left(S-S',\frac{1}{r^*}(H_{\text{Pub}}+Q^*H)\right)=$$
$$g^{h-h'}\Leftrightarrow e\left((S-S')\frac{1}{r^*}(\alpha+Q^*),H\right)=$$
$$e((h-h')G,H)$$

从而得到 $(\frac{1}{\alpha+Q^*})G=\frac{1}{r^*}(S-S')(h-h')^{-1}$，从而 B 可在时间 $t_1'\leqslant(120\,686\times q_{H_1}\times t_1)/(\varepsilon_1\times(1-1/2^k))$ 内成功解决 q-SDH 问题。

定理 2 在随机预言模型中，类型 2 攻击下，如果存在攻击者 A_2 能够在 t_2 时间内，利用 q_{H_2} 次 H_2 询问和 q_s 次签名询问，以 $\varepsilon_2\geqslant 10\times(q_s+1)\times(q_s+q_{H_2})/2^k$ 的概率攻破改进后的方案，则能构造一个算法 B 利用 A_2 在多项式时间 $t_2'\leqslant(120686\times q_{H_2}\times t_2)/(\varepsilon_2\times(1-1/2^k))$ 内解决 E-Inv-CDH 困难问题。

证明：假设 A_2 能伪造签名成功，那么 B 可以利用 A_2 的能力解决给定的 E-Inv-CDH 问题。给定一个随机实例 $\left(P,Y=\frac{1}{a}Q\right)$，B 的目标是计算出 aP。假设 A_2 攻击的目标身份为 ID^*，最终它能在时间 t' 内，以不可忽略的概率 ε'，伪造出用户身份 ID^*，关于消息 m^* 的合法签名 $\sigma=(R,S)$。

(1)系统参数设置：B 随机选择主密钥 $s\in Z_q^*$，计算 $H_{\text{pub}}=sQ$，$g=e(P,Q)$，$PK_{ID}=(s+Q_{ID})Y$，并将系统参数 $params=\{G_1,G_2,G_T,e,q,H_{\text{Pub}},g,H_1,H_2,PK_{ID}\}$ 提交给 A_2。

(2)攻击：B 把哈希函数 H_1,H_2 作为预言机，A_2 可以作 H_1 询问，H_2 询问，秘密值询问，公钥询问和签名询问(因为用户公钥由 PKG 生成，而 A_2 又是一个恶意的 PKG，可以计算用户部分私钥，因此，用户的公钥和部分私钥均不需要再询问)，假设 A_2 的询问是不同的，模拟询问如下：

(3) H_1 询问：当 A_2 对 H_1 进行关于身份 ID_i 的 Hash 询问时，如果 $ID_i=ID^*$，B 返回一个随机 $Q^*\in Z_q^*$ 且 $Q^*\notin\{y_1,y_2,\cdots,y_{q_h}\}$，其中，$q_h$ 表示 H_1 询问的最大次数；否则 B 随机选择 $Q_i\in\{y_1,y_2,\cdots,y_{q_h}\}$ 给 A_1 作为 $H_1(ID_i)$ 的值。

(4)H_2 询问：当 A_1 关于消息 m^*，ID_i，R_i，对 H_2 进行 Hash 询问时，B 随机选择 $h_i\in Z_q^*$ 给 A_1 作为 $H_2(m_i,ID_i,R_i)$ 的值。

(5)秘密值询问：当 A_2 询问关于身份 ID_i 的秘密值时，B 判断是否有 $ID_i=ID^*$ 成立，若 $ID\neq ID^*$，B 随机选择 $x\in Z_q^*$，将其发送给 A_2。

(6)签名询问：A_2 作签名询问，若 $ID_i=ID^*$，则 B 终止，否则 B 根据签名算法计算出签名 $\sigma=(R,S)$，并将 σ 发送给 A_2。A_2 输出身份为 ID_i，关于消息 m^* 的有效伪造签名 $\sigma=(R,S)$，由 Rafael-Ricardo 分叉引理[12]可知：若 $\varepsilon_2\geqslant 10\times(q_s+1)\times(q_s+q_{H_2})/2^k$，则 A_2 能够生成消息 m^* 的另一个有效的伪造签名 $\sigma'=(S',R)$，则有 $e(S,PK_{ID})g^{-h}=e(S',PK_{ID})g^{-h'}$，其中 $h\neq h'$，从而可推出：

$$e(S-S',PK_{ID})=g^{h-h'}\Leftrightarrow e\left(S-S',(s+Q_{ID})\frac{1}{a}Q\right)=$$
$$e((h-h')P,Q)\Leftrightarrow e\left((s+Q_{ID})\frac{1}{a}(S-S'),Q\right)=$$
$$e((h-h')P,Q)\Leftrightarrow(s+Q_{ID})\frac{1}{a}(S-S')=$$
$$(h-h')P\Leftrightarrow aP=(s+Q_{ID})(S-S')(h-h')^{-1}$$

从而 B 可在时间 $t_2'\leqslant(120\,686\times q_{H_2}\times t_2)/(\varepsilon_2\times(1-1/2^k))$ 内就求出了 E-inv-CDHP 的一个解，出现矛盾。因此，改进的方案能抵抗敌手 A_2 在随机预言模型下的选择适应性消息攻击。

6 结束语

本文分析了洪方案[9]的安全性，指出洪方案存在安全性隐患。一方面，由于没有对公钥进行认证，存在公钥替换攻击；另一方面，恶意的 PKG 利用用户的部分私钥伪造用户的身份对消息进行签名攻击。为克服该方案的不足，对该方案进行部分改进，并在随机预言模型下证明改进的方案是安全的。由此可见，设计无证书签名方案时，必须注意无证书环境的安全要求，防止一般用户的公钥替换攻击和恶意的 PKG 攻击。在今后的研究中，应在保证签名方案安全性的同时，提高方案的运行效率。

(下转第 164 页)