doi:10.3969/j.issn.1000-436x.2014.05.016

强安全无证书签名方案的安全性分析和改进

樊爱宛[1]，杨照峰[1]，谢丽明[2]
（1. 平顶山学院 软件学院，河南 平顶山 467002；2. 平顶山学院 计算机科学与技术学院，河南 平顶山 467002）

摘 要：对王亚飞等人提出的强安全性无证书签名方案进行安全性分析，指出其方案难以抵抗不诚实 KGC 下的公钥替换攻击。针对此类问题，采用改变传统无证书算法顺序，以 KGC 公告板形式公开用户公钥，用户可以通过本地保存的私钥和公钥验证公钥的真实性，从而对 KGC 的行为进行约束。安全性分析表明，改进后的方案能够抵抗基于不诚实 KGC 安全级别下的公钥替换攻击，而且方案避开了无双线性对和逆运算，效率优于已有方案。
关键词：无证书签名；公钥替换攻击；双线性对；离散对数问题
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)05-0118-06

Security analysis and improvement of strongly secure certificate less signature scheme

FAN Ai-wan[1],YANG Zhao-feng[1], XIE Li-ming[2]
（1. Software School, Pingdingshan College, Pingdingshan 467002, China;
2. Computer Science and Technology Department, Pingdingshan College, Pingdingshan 467002, China)

Abstract: By analyzing the security of strongly secure certificateless signature scheme proposed by Wang Yafei *et al*, the problem that the scheme could not resist public key replacement attack under dishonest KGC was pointed out. Aiming at this problem, the behavior of KGC was restrained by the change of traditional certificateless algorithm sequence KGC bulletin board where user public key make public, and verifiability of facticity of public key through the local private keys and public keys. The analysis of security shows that the improved scheme cannot only resist the public key replacement attack based on dishonest KGC, but also be more efficient than the existing schemes for avoiding pairings and inverse operation.
Key words: certificateless signature; public key replacement attack; bilinear pairing; discrete logarithm problem

1 引言

Al-Riyami 和 Paterson 于 2003 年提出了无证书的密码系统[1]。该系统的思想是：首先利用一个第三方 KGC(key generation center)产生用户的部分私钥；其次用户随机选择一个秘密值；然后用户通过部分私钥和秘密值来产生自己的公钥和私钥，系统将部分公钥绑定同一个身份。系统通过 KGC 和用户共同构成的用户公钥和私钥对，解决了公钥的证书管理和密码托管问题。

近几年，由于无证书签名系统的较强实用性，已经有大量的无证书签名方案被提出，如文献[2~5]。但是大部分方案或者不能抵抗公钥替换攻击，或者签名计算效率偏低。其中，影响签名计算效率的主要因素是以双线性对为计算工具。Yum 等[6]于 2004 年第一次提出无双线性对的无证书签名方案。然而，Hu 等[7]指出该方案是无法抵抗公钥替换攻击。2006 年，Yap 等[8]给出了一个签名阶段无需双线性对计算，验证阶段只需 2 个双线性对计算的高效签名方案。然而，Li 等[9]利用具体的攻击策略，证明了该方案无法抵抗公钥替换攻击，并给出了改进方法。

收稿日期：2013-02-24；**修回日期**：2013-05-29
基金项目：河南省中青年骨干教师基金资助项目；河南省科技攻关计划基金资助项目（142102210224）
Foundation Items: The Foundation for University Key Teachers of Henan Province; The Science and Technology Project of Henan Province (142102210224)

现在的许多无证书签名方案在提高计算效率的基础上，侧重于防止公钥替换攻击研究，却忽略了签名方案的安全性都以KGC信任诚实为前提的。在无证书的签名系统中，KGC有3种安全级别。1)信任诚实级：KGC不会将部分私钥泄露，更不会与敌手联合攻击用户；2)消极不诚实级：KGC将部分私钥泄露给敌手；3)积极不诚实级：KGC冒充用户生成替换公私钥，并将之泄露给敌手。2012年，Tian等[10]针对He等提出的基于椭圆曲线的无双线性对无证书的高效签名方案[11]，指出该方案不能抵挡恶意KGC的攻击。2013年，王亚飞等[12]针对王圣宝等人的方案[13]中存在弱秘钥攻击问题，给出的改进方案。但是，改进方案并不能抵抗恶意 KGC攻击。

本文分析王亚飞等提出的强安全无对无证书签名方案，发现该方案的安全性是以信任诚实的KGC 为前提的，方案是不能抵抗恶意 KGC 的公钥替换攻击。本文提出了一个改进的方案，通过改变传统的无证书算法顺序、KGC采用公告板形式公开用户公钥和设计公钥真实性的验证算法，对KGC的行为进行约束，从而达到能够抵抗不诚实 KGC下的公钥替换攻击的目的。

2　预备知识

2.1　数学难解问题

假设 G 是一个阶为素数 q 的循环群，P 是它的一个生成元。本文所提出的签名方案以以下数学难解问题为基础。

定义 1　椭圆曲线离散对数问题(ECDLP)：任取 $Q\in G$，求 $n\in Z_q^*$，使其能够满足 $Q=nP$。

定义 2　Diffie-Hellman 问题(CDHP)：已知 $aP\in G$，$bP\in G$，其中，$a\in Z_q^*$，$b\in Z_q^*$，且 a 和 b 未知，求 $abP\in G$。

2.2　无证书签名系统

一个无证书签名系统由以下7个算法组成[1,14]。

系统参数生成。输入安全参数 k ，输出向所有用户公开的系统参数 *params* 和由 KGC 自己保存的系统主密钥。

部分密钥生成。输入用户的身份标识 ID、系统参数 *params* 和主密钥，KGC 输出用户的部分私钥 d_{ID}，并通过秘密信道将 d_{ID} 返回给用户。

设置秘密值。输入系统参数 *params* 和用户的身份标识 ID，用户输出一个秘密值 z_{ID}。

设置私钥。输入系统参数 *params*、用户的身份标识 ID、部分私钥 s_{ID} 和秘密值 z_{ID}，用户输出用户的私钥 SK_{ID}。

设置公钥。输入系统参数 *params*、用户的身份标识 ID 和私钥 SK_{ID}，用户输出用户公钥 PK_{ID}。

签名。输入系统参数 *params*、用户的身份标识 ID、公钥 PK_{ID}、私钥 SK_{ID} 和消息 M，用户输出签名 σ。

验证。输入系统参数 *params*、用户的身份标识 ID、公钥 PK_{ID}、签名 σ 和消息 M，如果验证通过，输出 1，否则输出 0。

通常，系统参数生成和部分密钥生成算法由KGC执行，而其他算法由签名或验证用户执行。

3　王亚飞等的方案安全性分析

王亚飞等的方案具体过程可参见文献[11]，该方案的安全性是以信任诚实的 KGC 为前提的，方案是不能抵抗恶意 KGC 的公钥替换攻击。已知系统公开参数 $Params=\{G, F_q, E/F_q, q, P, P_{\text{pub}}, H_1, H_2\}$，具体攻击方法如下。

1)基于消极不诚实 KGC 安全级别的公钥替换攻击。消极不诚实的KGC将用户部分私钥 $s_{ID}=r_{ID}+H_1(ID,R_{ID})s$ 泄露给了敌手 A，敌手 A 开始对身份 ID，关于消息 M 进行签名伪造。

敌手 A 选择 $z_{ID}'\in Z_q^*$，计算用户公钥对 $PK_{ID}'=(R_{ID}, Z'_{ID})$ ，其中，$Z'_{ID}=z_{ID}'P$；

然后随机选择 $k'\in Z_q^*$，计算 $K'=k'P$，$u'=H_2(M, ID, K', R_{ID}, Z'_{ID})$，$v'=(k'+u')^{-1}(z_{ID}'+u'd_{ID})$，则伪造签名$(u', v', M)$能够得到确认。

对伪造签名有如下证明

$$
\begin{aligned}
K'' &= v'^{-1}\left(Z'_{ID}+u'\left(R_{ID}+H_1(ID,R_{ID})P_{\text{pub}}\right)\right)-u'P\\
&=(k'+u')(z_{ID}'+u'd_{ID})^{-1}\cdot\\
&\quad\left(Z'_{ID}+u'\left(R_{ID}+H_1(ID,R_{ID})P_{\text{pub}}\right)\right)-u'P\\
&=(k'+u')(z_{ID}'+u'd_{ID})^{-1}\cdot\\
&\quad\left(z'_{ID}P+u'\left(r_{ID}P+H_1(ID,R_{ID})sP\right)\right)-u'P\\
&=(k'+u')(z_{ID}'+u'd_{ID})^{-1}(z_{ID}'+u'd_{ID})P-u'P\\
&=(k'+u')P-u'P\\
&=k'P\\
&=K'
\end{aligned}
$$

因为 $h'=H_2(M, ID, K', R_{ID}, Z'_{ID})$ ，所以有 $h'=u'$ 成立，伪造签名通过验证，因此王亚飞等给出的方案不可基于消极不诚实的 KGC 安全级别下的公

钥替换攻击。

2)基于积极不诚实的 KGC 安全级别的公钥替换攻击。其攻击方式与基于消极不诚实的 KGC 安全级别的公钥替换攻击相同，消极不诚实的 KGC 在已知部分秘钥的条件下，充当敌手 A，伪造用户公钥。由此可见，如果签名方案在基于消极不诚实的 KGC 安全级别上是不安全的，则一定在基于积极不诚实的 KGC 安全级别上也是不安全的。故王亚飞等的方案基于积极不诚实的 KGC 安全级下的公钥替换攻击。

4 改进方案及其安全性分析

4.1 改进方案

系统参数生成。输入一个安全参数 k，KGC 选定系统参数 $params=\{q, FR, a, b, P, H_1, H_2, P_{pub}\}$。其中，$F_q$ 为有限域；整数 $q(0<q<2^k)$为大素数，是所选有限域的阶；FR 是有限域 F_q 中元素的表示；椭圆曲线的 2 个系数 a，$b\in F_q$，构建了椭圆曲线 E：$y^2=x^3+ax+b$；G 是一个阶为素数 q 的循环群，该群的元素是由 E 坐标点和无穷远点构成；P 是 G 的一个生成元；H_1 和 H_2 是 2 个单向散列函数，能够保证信息的完整性，其中，H_1：$\{0,1\}^*\times G\rightarrow Z_q^*$，$H_2$：$\{0, 1\}^{*2}\times G^3\rightarrow Z_q^*$。在 Z_q^*中随机选取系统主密钥 s，记 $P_{pub}=sP$。

KGC 身份认证。用户(其身份为 ID)随机选取具有一定时效的 $x\in Z_q^*$，计算 $X = xP$，将 X 发送给 KGC；KGC 计算 $N = sX$，将 N 通过秘密信道发送给用户；用户计算等式 $N = xP_{pub}$ 是否成立，如果成立，则 KGC 身份认证通过，否则失败，中断联系。

设置秘密值。输入系统参数 $params$ 和用户的身份标识 ID。用户随机选取 $z_{ID}\in Z_q^*$，计算 $Z_{ID} = z_{ID}P$；将 Z_{ID} 和 ID 发送给 KGC。

部分私钥生成。输入用户的身份标识 ID、系统参数 $params$ 和主密钥 s，KGC 为用户生成部分私钥。KGC 收到 Z_{ID} 和 ID 后，随机选取 $r_{ID}\in Z_q^*$；KGC 计算 $R_{ID} = r_{ID}P$；计算 $d_{ID}=r_{ID} + H_1(ID,R_{ID})s$；KGC 将（$R_{ID}$, d_{ID}）通过秘密信道发送给用户。

部分私钥验证。输入用户的身份标识 ID、系统参数 $params$、R_{ID} 和部分私钥 d_{ID}，验证部分私钥是否是 KGC 生成。用户计算等式 $d_{ID}P = R_{ID} + H_1(ID, R_{ID})P_{pub}$ 是否成立。若成立，则计算 $N' = xR_{ID}$，将 N' 通过秘密信道发送给 KGC；否则失败，中断联系。

公钥发布。输入用户的身份标识 ID、系统参数 $params$、r_{ID} 、主密钥 s、N'和 N，KGC 验证用户真实性并发布公钥。KGC 计算等式 $sN'=sxr_{ID}P = r_{ID}N$ 是否成立。若成立，则公布用户公钥 (Z_{ID} , R_{ID})，并以列表形式(ID, Z_{ID}, R_{ID})在 KGC 中用公告板公示。

设置公钥。用户设置其公钥为 PK_{ID} = (Z_{ID} , R_{ID})，将其保存本地文件中。

设置私钥。用户设置其私钥为 SK_{ID} (z_{ID} , d_{ID})，将其保存在本地文件中。

公钥真实性验证。用户可用自己保存的公钥与 KGC 公告板上的公钥进行对照，可发现公钥的真实性。还可以通过 $d_{ID}P + z_{ID}H_1(ID,Z_{ID})P=R_{ID} + H_1(ID, R_{ID})P_{pub} + H_1(ID,Z_{ID})Z_{ID}$ 是否成立，判断公钥的真实性。

签名。当输入一个消息 $M\in Z_q^*$，用户按以下方式对消息 M 进行签名。

1)选取 k，计算 $K = kP$。

2)计算 $h = H_2(ID,M, Z_{ID} ,R_{ID},K)$。

3)计算 $v= (k + d_{ID} + hz_{ID}) \bmod q$。

4)发送消息和签名结果(M, K, v)。

验证。验证者按如下方式验证身份为 ID 的用户对消息 M 的签名有效性。

1)从 KGC 的公告板处获取身份为 ID 签名者的基本信息(Z_{ID} , R_{ID})及系统参数。

2)计算 $h = H_2(ID,M, Z_{ID} ,R_{ID},K)$；$h_1 = H_1(ID, R_{ID})$。

3)计算 $U=vP$；$U' = R_{ID} + h_1P_{pub} + hZ_{ID}$。

4)判断 $K=U-U'$等式是否成立。若成立则输出 1，否则输出 0，并将自己的私钥和公钥公开，以便其他用户验证。

本文改进方案由系统参数生成、KGC 身份认证、设置秘密值、部分私钥生成、部分私钥验证、公钥发布、设置公钥、设置私钥、公钥真实性验证、签名及签名验证等 10 部分构成，其中，KGC 身份认证、部分私钥验证、公钥真实性验证可在用户对 KGC 身份及公钥产生怀疑时使用。本文改进方案将设置秘密值放在部分私钥生成之前产生，使用户设置的秘密值成为 KGC 产生部分私钥的前置条件，KGC 公钥最后由 KGC 汇总发布在公告板上，有效地约束了 KGC 的行为。

4.2 改进方案的安全性分析

1)正确性

改进方案的签名及验证算法是正确的。根据改进方案中的签名验证等式进行算法正确性验证，证明如下

$$\begin{aligned} U-U' &= vP-(R_{ID}+h_1P_{\text{pub}}+hZ_{ID}) \\ &= ((k+d_{ID}+hz_{ID}) \bmod q)P-(R_{ID}+h_1P_{\text{pub}}+hZ_{ID}) \\ &= K+R_{ID}+h_1P_{pub}+hZ_{ID}-(R_{ID}+h_1P_{\text{pub}}+hZ_{ID}) \\ &= K \end{aligned} \tag{1}$$

2) 可验证性

改进方案中有 4 处验证。

① 用户根据 $N=xP_{\text{pub}}$ 是否成立，对 KGC 身份进行验证。算法有效性的验证如下

$$N=sxP=xsP=xP_{\text{pub}} \tag{2}$$

② 用户根据 $d_{ID}P=R_{ID}+H_1(ID,R_{ID})\,P_{\text{pub}}$ 是否成立，对 d 是否来源于 KGC 的验证。算法有效性的验证如下

$$\begin{aligned} d_{ID}P &= (r_{ID}+H_1(ID,R_{ID})s)P \\ &= r_{ID}P+H_1(ID,R_{ID})sP \\ &= R_{ID}+H_1(ID,R_{ID})P_{\text{pub}} \end{aligned} \tag{3}$$

③ KGC 根据 $sN'=sxr_{ID}P=r_{ID}N$ 是否成立，对公钥是否来源于用户的验证。算法有效性的验证如下

$$sN'=sxr_{ID}P=r_{ID}N \tag{4}$$

④ 用户根据 KGC 公告板的变化，对公钥真实性进行验证，还可以通过 $d_{ID}P+z_{ID}H_1(ID,Z_{ID})P=R_{ID}+H_1(ID,R_{ID})\,P_{\text{pub}}+H_1(ID,Z_{ID})\,Z_{ID}$ 是否成立，判断公钥真实性。

3) 可抵抗基于消极不诚实 KGC 安全级别的公钥替换攻击

与原方案相比，改进后方案中的签名验证公钥 (Z_{ID}, R_{ID})是由 KGC 根据用户所提供的信息公布到公告板中，即使 KGC 将用户部分私钥 d_{ID} 泄露给敌手，敌手也不能将伪造的新公钥替换原公钥(Z_{ID}, R_{ID})，因为替换的结果最终要在公告板上显现。所以改进方案在基于消极不诚实 KGC 安全级别上是安全的。

4) 可抵抗基于积极不诚实的 KGC 安全级别的公钥替换攻击

假如 KGC 利用自己选择的随机值 $r_{ID}'\in Zq^*$，生成新的用户公钥 $R_{ID}'=r_{ID}'P$，并公布到公告板中，那么用户可根据等式 $d_{ID}P+z_{ID}H_1(ID,Z_{ID})P=R_{ID}'+H_1(ID,R_{ID})\,P_{\text{pub}}+H_1(ID,Z_{ID})\,Z_{ID}'$，判断 KGC 积极不诚实的行为。所以改进方案在基于积极不诚实 KGC 安全级别上是安全的。

5) 抗伪造性

改进方案在自适应选择消息攻击下是存在性不可伪造的。下面在随机预言机模型下进行抗伪造性的证明。

定理 1　在随机预言机模型下，如果 A 为恶意的 KGC，在多项式时间内，至多做了 q_{H_1} 次 H_1 询问，q_{H_2} 次 H_2 询问，q_z 次秘密值询问和 q_v 次签名询问后，以不可忽略的概率 ε 攻破本文改进方案，那么存在一个算法 X，在多项式时间内以 $\varepsilon/(q_{H_1}\ q_{H_2})$ 的优势成功解决 ECDLP 问题。

证明　令 X 是加法循环群 G 上的 ECDLP 问题解决算法，给定一个 ECDLP 问题的随机实例$(P, Y=aP)$，X 的目标是利用 A 的攻击程序计算出 a。

系统参数生成：X 选定系统参数 $D=\{q, FR, a, b, P, H_1, H_2, P_{\text{pub}}\}$及公告板中的 (Z_{ID}, R_{ID})发送给 A。

A 的攻击：X 将散列函数 H_1、H_2 作为随机预言机，A 可以作 H_1 查询、H_2 查询、秘密值查询、公钥查询和签名查询。由于用户公钥是 KGC 发布的，且 A 是恶意 KGC，可以计算用户部分私钥，故用户公钥和用户部分私钥都不需再查询。设 ID_i 是 A 对身份 ID 第 i 次查询，ID^*为 A 攻击的对象，所有查询的列表初始为空。

H_1 查询：格式为$(ID_i,\ R_{ID_i}, h_{1ID_i})$的列表 L_1 保存在 X 中。当 X 收到攻击者 A 发送的针对$(ID^*,\ R_{ID^*})$的查询时，若 ID_i 在 L_1 列表中，则 X 返回对应的 h_{1ID_i} 值，否则 X 选择 $h_{1ID^*}\in Z_q^*$，且 h_{1ID^*}不在$(h_{1ID_1}, h_{1ID_2}, \cdots, h_{1ID}q_{H_1})$，将 h_{1ID^*}返回给 A，并将(ID^*, h_{1ID^*})添加到表 L_1 中。

H_2 查询：格式为$(ID_i,\ M_i,\ Z_{ID_i}, R_{ID_i},\ K,\ h_{2ID_i})$的列表 L_2 保存在 X 中。当 X 收到攻击者 A 发送的针对$(ID^*, M_i, Z_{ID^*}, R_{ID^*}, K)$的查询时，若询问项存在于表 L_2 中，则 X 返回对应的 h_{2ID_i} 值给 A，否则 X 随机选择 $h_{2ID^*}\in Z_q^*$返回给 A，并将$(ID^*, M_i,\ Z_{ID^*}, R_{Ii^*}, K, h_{2ID^*})$添加到表 L_2 中。

秘密值查询：格式为(ID_i, z_{IDi})的列表 L_3 保存在 X 中。当 X 收到攻击者 A 发送的针对$(ID_i,\ z_{IDi})$的查询时，若询问项存在于表 L_3 中，则 X 返回对应的 Z_{ID_i} 值给 A，否则判断 $ID_i=ID^*$是否成立，若成立，则 X 终止，若不成立，则 X 随机选择 $Z_{ID_i}\in Z_q^*$给 A，并将$\{ID_i,\ Z_{ID_i}\}$添加到表 L_3 中。

签名查询：A 作签名询问，判断 $ID_i=ID^*$是否成立，若成立，则 X 终止，若不成立，则 X 终止，

表 1 **本文方案与其他方案在运算量和基于 KGC 安全级别的安全性比较**

方案	运算量			基于 KGC 安全级别的安全性		
	签名阶段	验证阶段	总运算量	可信	消极不诚实	积极不诚实
文献[2]	2P	E+M+P	E+M +3P	安全	安全	安全
文献[12]	1P+I	3P+I	4P+2I	安全	不安全	不安全
文献[13]	1P+2I	3P	4P+2I	不安全	不安全	不安全
改进方案	1P	3P	4P	安全	安全	安全

否则 X 根据签名算法计算出签名(K, v)，并将(K, v)发送给 A。

A 输出身份为 ID^*，关于消息 M 的有效伪造签名(K, v)，由分叉引理可知，A 能够生成消息 M 的另一个有效伪造签名(K, v') ，设 $z_{ID^*}=a$，则有

$$\begin{aligned} vP &= (k + d_{ID} + hz_{ID})P \\ &= K + R_{ID} + h_1 P_{\text{pub}} + haP \end{aligned} \tag{5}$$

$$\begin{aligned} v'P &= (k + d_{ID} + h'z_{ID})P \\ &= K + R_{ID} + h_1 P_{\text{pub}} + h'aP \end{aligned} \tag{6}$$

$$\begin{aligned} (v - v')P &= (h - h')aP \\ a &= (v - v')/(h - h') \end{aligned} \tag{7}$$

如果 A 伪造签名成功，那么 X 就能利用 A 求出 ECDLP 的一个解。避免这种情况的发生为敌手 A 在秘密值查询和 H_2 查询时以失败而告终，其概率至少为 $\varepsilon/(q_{H_1} q_{H_2})$。所以在多项式时间内，$X$ 只能以至少 $\varepsilon/(q_{H_1} q_{H_2})$的优势成功解决 ECDLP 问题。由此可见，改进方案能抵抗敌手 A 在随机预言机模型下的选择适应性消息攻击。

5 改进方案效率分析

各种运算的时间符号定义和时间复杂度换算关系可按文献[15,16]估算。其中，相对乘法运算，加法运算、模运算、点加运算和散列运算都可以忽略不计。标记 E、M、A、P、I 分别代表方案中的双线性运算、指数运算、乘法运算、点乘运算和逆运算。1E≈1 480 A；1M≈240A；1P≈29A；1I≈11A。

从表 1 可以看出，1)在签名及其验证签名阶段，只有文献[2]中的方案与所提出的改进方案一样在基于 3 种 KGC 安全级别下是安全的，但是，这个方案使用了复杂的双线性运算和指数运算，本文改进方案使用了无双线性和无指数运算，在计算代价上要比文献[2]中的方案降低不少；2)文献[12]和文献[13]虽然在计算过程中也采用了无双线性和无指数运算，但是文献[13]已经被证明在基于可信 KGC 环境下是不安全的，文献[12]被证明在基于消极不诚实 KGC 环境下是不安全的，而且这 2 种方案还使用了逆运算，增加了计算量；3)本文改进方案在保证能抵抗公钥替换攻击的同时提高了签名效率。

6 结束语

本文分析了王亚飞等提出的强安全无对无证书签名方案，指出此方案的安全性是建立在信任诚实 KGC 的基础上。本文提出了一个改进的方案，该方案首先改变传统无证书秘钥和公钥产生顺序；其次在公钥生成中，KGC 采用公告板形式公开用户公钥；最后用户可以通过本地保存的私钥和公钥，验证公钥的真实性，从而对 KGC 的不诚实行为进行约束，最终达到了可抵抗消极不诚实 KGC 下的公钥替换攻击和可判别 KGC 的积极不诚实性的效果。该方案的签名阶段只需要 1 个点乘运算，验证阶段只需要 3 个点乘运算，并且避开了逆运算。所提方案在保证能抵抗公钥替换攻击的同时提高了签名效率。

参考文献：

[1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[A]. Proc of Asiacrypt 2003[C]. Springer-Verlag, Berlin，2003. 452-473.

[2] CHOI K Y, PARK J H, HWANG J Y, *et al*. Efficient certificateless signature schemes[A]. Proc of the ACNS 2007 LNCS 4521[C]. Heidelberg: Springer-Verlag, 2007. 443-458.

[3] HARN L, REN J, LIN C L. Design of DL-basedcertificateless digital signatures[J]. Journal of Systems and Software, 2009,82(5):789-793.

[4] LIPPOLD G, BOYD C, NIETO J M G. Efficient certificateless KEM in the standard model[A]. Proc of the ICISC 2009 LNCS 5984[C]. Heidelberg: Springer-Verlag, 2010. 34-46.

[5] TSO R, KIM C, YI X. Certificateless message recovery signatures providing girault's level-3 security[J]. Journal of Shanghai Jiaotong University (Science), 2011, 16(5): 577-583.

[6] HUANG X, MU Y, SUSILO W, *et al*. Certificateless signatures: new schemes and security models[J]. The Computer Journal, 2012, 55(4): 457-474.

[7] HU B, WONG D, ZHANG Z, *et al*. Key replacement attack against a generic construction of certificateless signature[A]. Proc of the 11th Australasian Conference on Information Security and Privacy[C]. Mel-bourne, Australia, 2006. 235-246.

[8] YAP W S，HENG S H，GOI B M． An efficient certificateless signa-ture scheme[A]. Emerging Directions in Embedded and Ubiqui-ous Computing: EUC 2006，LNCS 4097[C]. Berlin: Springer-Verlag，2006.322-331.

[9] LI J G, HUANG X Y, MU Y, *et al*.Cryptanalysis and improvement of an efficient certificateless signature scheme[J]. Journal of Communi-cations and Networks, 2008,10(1):10-17.

[10] TIAN M, HUAN L. Cryptanalysis of a certificateless signature sche-mewithout pairings[EB/OL].http://onlinelibrary.wiley.com/doi/ 10.1002/dac.2310/full,2012.

[11] HE D, CHEN J, ZHANG R. An efficient and provably-secure certifi-cateless signature scheme without bilinear pairings[J]. International Journal of Communication Systems, 2012, 25(11):1432-1442.

[12] 王亚飞，张睿哲.强安全无对的无证书签名方案[J].通信学报，2013, 34(2):94-100.
WANG Y F, ZHANG R Z.Strongly secure certificateless signature scheme without pairings[J]. Journal on Communications, 2013, 34(2):94-100.

[13] 王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J].通信学报, 2012, 33(4):93-98.
WANG S B, LIU W H, XIE Q. Certificateless signature scheme with-out bilinear pairings[J]. Journal on Communications, 2012, 33(4):93- 98.

[14] HUANG X Y, SUSILO W, MU Y, *et al*. On the security of certificate-less signature schemes from asiacrypt 2003[A]. Proc of the CANS 2005 LNCS 3810[C]. Heidelberg: Springer-Verlag, 2005. 13-25.

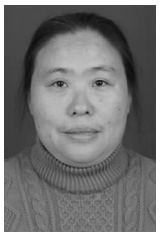
[15] CHEN L, CHENG Z, SMART N P. Identity-based key agreementpro-tocols from pairings[J]. Int J Inf Secur, 2007, 6(4):213-241.

[16] COURTOI N, KLIMOV A, PATARIN J. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[A]. EUROCRYPT 2000[C]. Berlin, Germany, 2000. 392-407.

作者简介：

樊爱宛（1978-），男，河南内乡人，平顶山学院副教授，主要研究方向为信息安全。

杨照峰（1978-），男，河南襄城人，平顶山学院讲师，主要研究方向为信息安全。



谢丽明（1965-），女，河南襄城人，平顶山学院教授，主要研究方向为信息安全、数据挖掘。

（上接第 117 页）

[21] 蔡绍滨, 方伟. 基于区间的云相似度比较算法[J]. 小型微型计算机, 2011, 32(12): 2456- 2460.
CAI S B, FANG W. Research of interval-based cloud similarity com-parison algorithm[J]. Journal of Chinese Computer Systems, 2011, 32(12):2456-2460.

[22] CHENG S, LI J, REN Q, *et al*. Bernoulli sampling based (*ε*, *δ*)-approximate aggregation in large-scale sensor networks[A]. Proc of the 29th IEEE INFOCOM[C]. San Diego, CA, USA, 2010.1181-1189.

作者简介：

徐晓斌（1986-），男，河南鹤壁人，北京邮电大学博士生，主要研究方向为物联网安全、无线传感器网络等。

张光卫（1970-），男，山东德州人，博士，北京邮电大学讲师，主要研究方向为物联网安全、人工智能、数据挖掘。

王尚广（1982-），男，河南周口人，博士，北京邮电大学讲师，主要研究方向为车联网技术、物联网。

孙其博（1975-），男，河南郑州人，博士，北京邮电大学副教授，主要研究方向为服务计算、物联网和网络安全。

杨放春（1957-），男，北京人，博士，北京邮电大学教授、博士生导师，主要研究方向为新一代通信网络、服务计算、云计算、车联网。