doi:10.11959/j.issn.1000-436x.2016115

强不可伪造的基于身份服务器辅助验证签名方案

杨小东，杨苗苗，高国娟，李亚楠，鲁小勇，王彩芬
（西北师范大学计算机科学与工程学院，甘肃 兰州 730070）

摘 要：标准模型下的基于身份签名方案大多数是存在性不可伪造的，无法阻止攻击者对已经签名过的消息重新伪造一个合法的签名，并且验证签名需要执行耗时的双线性对运算。为了克服已有基于身份签名方案的安全性依赖强和计算代价大等缺陷，提出了一个强不可伪造的基于身份服务器辅助验证签名方案，并在标准模型下证明了新方案在合谋攻击、自适应选择身份和消息攻击下是安全的。分析结果表明，新方案有效减少了双线性对的计算量，大大降低了签名验证算法的计算复杂度，在效率上优于已有的基于身份签名方案。
关键词：基于身份服务器辅助验证签名；强不可伪造性；合谋攻击；标准模型
中图分类号：TP309 **文献标识码**：A

ID-based server-aided verification signature scheme with strong unforgeability

YANG Xiao-dong, YANG Miao-miao, GAO Guo-juan, LI Ya-nan, LU Xiao-yong, WANG Cai-fen
(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

Abstract: Most identity-based signature schemes in the standard model are existentially unforgeable, which cannot prevent adversaries from forging valid signatures on messages that have previously been signed. However, signature verification algorithms of ID-based signature schemes in the standard model require expensive bilinear pairing operations. In order to overcome the shortcomings of the existing ID-based signature schemes such as strong security assumption and high computation cost，a strongly unforgeable ID-based server-aided verification signature scheme was presented. This scheme was proven to be secure under collusion attacks, adaptive chosen identity and message attacks in the standard model. Analysis results show that the proposed scheme effectively reduces computation cost of pairing operation, and it greatly reduces computational complexity of signature verification algorithm. The proposed scheme is more efficient than the existing ID-based signature schemes.
Key words: ID-based server-aided verification signature, strong unforgeability, collusion attack, standard model

1 引言

基于身份密码体制是一种将用户身份标识作为公钥的密码体制，用于解决公钥基础设施 PKI/CA 中数字证书的存储和管理开销等问题[1]。在基于身份的密码体制中，用户的 E-mail 地址等唯一身份标识作为用户的公钥，密钥生成中心 PKG 借助主密钥生成相应的用户私钥。由于不再需要使用传统的公钥证书，因而大大减轻了密钥的管理与分发开销。2001 年，Boneh 和 Franklin[2]利用双线性对工

收稿日期：2015-07-21；**修回日期**：2015-09-10
基金项目：国家自然科学基金资助项目（No.61262057）；甘肃省科技计划基金资助项目（No.145RJDA325）；国家档案局科技基金资助项目（No.2014-X-33）；甘肃省高等学校科研基金资助项目（No.2014-A011）；兰州市科技计划基金资助项目（No.2013-4-22）；西北师范大学青年教师科研能力提升计划基金资助项目（No.NWNU-LKQN-13-23, No.NWNU-LKON-14-7）
Foundation Items: The National Natural Science Foundation of China (No.61262057), The Natural Science Foundation of Gansu Province (No.145RJDA325), The Science and Technology Project of State Archives Administration of China (No.2014-X-33), Research Fund of Higher Education of Gansu Province (No.2014-A011), Science and Technology Project of Lanzhou City of China (No.2013-4-22) The Foundation for Excellent Young Teachers by Northwest Normal University (No.NWNU-LKQN-13-23, No.NWNU-LKON-14-7)

具首次构造出高效的基于身份加密方案；随后国内外学者对基于身份密码体制进行了大量的研究，并取得一系列原创性研究成果[3~6]。

然而，大部分基于身份签名方案的签名验证算法都要进行耗时的双线性对计算，不能有效地应用于各类低端计算设备。手机、无线传感器、智能手表等低端计算设备便于携带，但能源供应有限、计算和存储能力较弱。因此，应用于低端计算设备的签名方案必须优先考虑计算量。然而，双线性对是目前比较耗时的密码操作[7]，迫切需要研究新的基于身份签名方案，减少签名验证算法中的双线性对计算量。

基于身份的服务器辅助验证签名将基于身份签名体制和服务器辅助验证签名体制相结合，验证签名合法性的大部分计算量交给服务器执行，验证者只需进行少量的计算，从而有效减轻了验证者的计算负担，提高签名验证的性能，非常适用于低端计算设备。基于身份服务器辅助验证签名的研究才刚刚起步，公开的相关文献较少。2013 年，Zhang 等[8]设计了一个基于身份的服务器辅助验证签名方案，但其安全依赖于现实世界无法实现的随机预言机假设。一个在随机预言模型下可证明安全的密码系统，在现实中无法确保它的安全性[9]。标准模型下安全的基于身份签名方案能消除理想随机预言机的安全假设，但已有的这类方案[10,11]仅能抵抗攻击者的存在性不可伪造。由于强不可伪造性能同时确保攻击者不能对未签名消息和已签名消息进行伪造签名，被用来设计群签名方案、签密方案及电子现金系统等[12,13]，所以研究强不可伪造的基于身份服务器辅助验证签名方案具有一定的现实意义。

2014 年，Kwon[14]构造了一个满足强不可伪造安全属性的基于身份签名方案，在标准模型中具有系统公开参数少、签名短等特点，但签名验证算法需要 3 个双线性对运算。为了克服已有基于身份签名方案的安全性依赖强和计算代价大等缺陷，本文基于 Kwon 方案[14]设计了一个强不可伪造的服务器辅助验证签名方案，并证明新方案在合谋攻击和强不可伪造攻击下是安全的。新方案的签名验证算法避免了复杂的双线性对运算，与现有的同类方案相比，具有更低的计算复杂度，可应用于签名验证时间受限或计算能力有限的设备。目前还没有关于标准模型下强不可伪造的基于身份服务器辅助验证签名研究的公开文献。

2 预备知识

2.1 双线性映射

假设 G_1 和 G_2 是 2 个阶为素数 p 的循环群，g 是 G_1 的一个生成元，$e:G_1\times G_1\to G_2$ 是满足以下条件的双线性映射[4]。

1) 双线性：对任意的 $a,b\in Z_p^*$，满足 $e(g^a,g^b)=e(g,g)^{ab}$。

2) 非退化性：$e(g,g)\neq 1_{G_2}$。

3) 可计算性：对任意 2 个元素 $g_1,g_2\in G_1$，存在一个有效的算法计算 $e(g_1,g_2)$。

2.2 CDH 假设

定义 1 计算性 Diffie-Hellman（CDH, computational Diffie-Hellman）问题。设 p 是一个大素数，G_1 是阶为 p 的循环群，g 是 G_1 的任意一个生成元，已知 $(g,g^a,g^b)\in G_1^3$，对于未知的 $a,b\in Z_p^*$，计算 $g^{ab}\in G_1$。

定义 2 CDH 假设。若没有一个多项式时间算法能以不可忽略的概率求解 G_1 上的 CDH 问题，那么称群 G_1 上的 CDH 问题是困难的[6]。

3 强不可伪造的基于身份服务器辅助验证签名的形式化安全定义

一个强不可伪造的基于身份服务器辅助验证签名方案包括下面 6 个算法。

1) Setup $(1^\eta)\to cp$ 是系统参数生成算法。对于安全参数 η，该算法生成系统需要的公开参数 cp 和密钥生成中心 PKG 的秘密主密钥 msk。

2) Extract $(msk,ID)\to d_{ID}$ 是密钥提取算法。给定主密钥 msk 和一个用户身份 ID，生成一个与 ID 对应的私钥 d_{ID}。

3) Sign $(m,d_{ID})\to\sigma$ 是签名生成算法。给定消息 m 和私钥 d_{ID}，生成关于消息 m 的签名 σ，其中 d_{ID} 是身份 ID 的私钥。

4) Verify $(m,pk,\sigma)\to\{0,1\}$ 是签名验证算法。给定用户身份 ID，消息 m 和签名 σ，当 σ 是对应于 ID 的 m 的合法签名，输出 1；否则，输出 0。

5) SAV-Setup $(cp)\to VString$ 是服务器辅助验证参数生成算法。给定系统参数 cp，生成一个字符串 $VString$。

6) SAV-Verify ($VString, m, ID, \sigma$) $\rightarrow$ {0, 1}是服务器辅助验证协议。给定字符串 $VString$ 、用户身份 ID 和消息签名对 (m,σ)，验证者在服务器的协助下验证 σ 的正确性，若当 σ 是对应于 ID 的 m 的合法签名，输出 1；否则，输出 0。

服务器可以是具有强大计算能力的云服务提供商，验证者是计算能力较弱的云计算终端（如智能手机等），利用 SAV-Verify 交互协议在服务器的帮助下完成签名的合法性验证。

定义 3　用 Φ_Verify 表示强不可伪造的基于身份签名方案中验证者的计算开销，Φ_SAV_Verify 表示基于身份服务器辅助验证签名方案中验证者的计算开销。若 $\Phi\_SAV\_Verify < \Phi\_Verify$，则称基于身份服务器辅助验证签名方案是计算节约的[8]。

一个强不可伪造的基于身份服务器辅助验证签名方案至少应满足基于身份签名的强不可伪造性和服务器辅助验证协议 SAV-Verify 的完备性。强不可伪造性能确保攻击者无法生成一个未签名消息或已签名消息的有效签名，完备性保证服务器不能让验证者确信一个非法签名是合法的。为了改进文献[8]给出的基于身份服务器辅助验证签名的安全模型，假设服务器不仅与合法的签名者合谋，也可以与非法的签名者合谋。由于服务器能获得任何消息的签名，因此无法给出一个统一的安全定义来刻画基于身份服务器辅助验证签名的强不可伪造性和服务器辅助验证协议的完备性。文献[12,14]已给出了基于身份签名方案的强不可伪造性安全定义，下面借助攻击者 A 和挑战者 C 之间的安全游戏，给出在合谋攻击和自适应性选择消息攻击下服务器辅助验证协议的完备性安全定义。在这个游戏中，攻击者 A 拥有主密钥和签名密钥。

建立：挑战者 C 首先运行系统参数生成算法 Setup、密钥提取算法 Extract 和服务器辅助验证参数生成算法 SAV-Setup，生成系统参数 cp 、字符串 $VString$ 、主密钥 msk 和身份/私钥对 (ID, d_{ID})，然后将 (cp, msk, ID, d_{ID}) 发送给 A。

查询：由于攻击者 A 已掌握私钥 d_{ID} 和主密钥 msk，所以 A 只需进行有限次服务器辅助验证询问。对于每次询问 (m_i, σ_i)，挑战者 C 和攻击者 A 分别充当验证者和服务器的角色，并将 SAV-Verify 协议运行的结果作为响应返回给 A。

输出：攻击者 A 输出一个消息 m^* 和字符串 σ^*，令 Ω_{m^*} 是 m^* 对应于身份 ID 的所有合法签名集合，$\sigma^* \notin \Omega_{m^*}$。如果 SAV-Verify ($VString, m^*, ID, \sigma^*$)=1 且 Verify ($m^*, ID, \sigma^*$)=0，即攻击者 A 让挑战者 C 确信 σ^* 是 m^* 对应于身份 ID 的合法签名，则称攻击者 A 赢得了游戏。

定义 4　若攻击者 A 在以上游戏中获胜的概率是可忽略的，则称 SAV-Verify 协议满足完备性。

利用签名方案的存在不可伪造性和服务器辅助验证协议的完备性，文献[15]给出了服务器辅助验证签名的安全性定义，文献[8]给出了基于身份服务器辅助验证签名的安全性定义。采用类似的方法，下面给出强不可伪造的基于身份服务器辅助验证签名的安全性定义。

定义 5　若基于身份签名方案满足强不可伪造性，服务器辅助验证协议满足完备性，则称相应的基于身份服务器辅助验证签名方案是安全的。

4　强不可伪造的基于身份服务器辅助验证签名方案设计

本节在 Kwon 方案[14]的基础上，设计一个强不可伪造的基于身份服务器辅助验证签名方案，与 Kwon 方案的主要区别是降低了签名验证者的计算量，将签名验证的大部分计算任务通过服务器辅助验证协议转移给一个不可信的服务器执行。因此，验证者在服务器的协助下完成签名的验证，具有更低的计算复杂度，可应用于签名验证时间受限或计算能力有限的设备。新方案包含的 6 个算法具体如下。

1) Setup 算法

密钥生成中心 PKG 选择 2 个素数阶 p 的循环群 G_1 和 G_2，选取一个 G_1 的生成元 g，选择一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 和一个抗碰撞的散列函数 $H: \{0,1\}^* \times G_1 \times G_1 \rightarrow Z_p$；然后随机选取 $l+5$ 个元素 $(g_2, v_0, v_1, w, u, u_1, \mathrm{L}\ , u_l) \in G_1^{l+5}$，并随机选取 $a \in Z_p^*$，计算 $g_1 = g^{\alpha}$ 和 $P_{\text{pub}} = e(g_2, g_1)$；最后 PKG 将 $msk = a$ 作为自己的秘密主密钥 $msk = a$，公开相应的系统参数 $cp = (G_1, G_2, p, g, g_1, g_2, v_0, v_1, w, u, \{u_i\}_{i=1}^{l}, H, P_{\text{pub}})$。

2) Extract 算法

对于用户身份 $ID=\{ID_1,\mathrm{L}\ ,ID_l\}$，密钥生成中心 PKG 生成对应私钥 d_{ID} 的具体步骤如下。

① 选择一个随机数 $r\in Z_p^*$，利用主密钥 α 计算 $d_{ID}=(d_1,d_2)=(g_2^{\alpha}(u'\prod_{i=1}^{l}u_i^{ID_i})^r,g^r)\in G_1^2$。

② 发送身份 ID 对应的私钥 $d_{ID}=(d_1,d_2)$ 给用户。

③ 收到 $d_{ID}=(d_1,d_2)$ 后，用户通过式(1)检验私钥的有效性。

$$e(d_1,g)=P_{\text{pub}}e(u'\prod_{i=1}^{l}u_i^{ID_i},d_2) \tag{1}$$

若式(1)成立，则表明 d_{ID} 是 PKG 发送给用户的合法私钥。

3) Sign 算法

对于给定的待签名消息 m，签名者利用私钥 $d_{ID}=(d_1,d_2)$ 进行如下操作。

① 随机选取一个元素 $k\in Z_p^*$，计算 $h=H(m\|ID\|d_2\|g^k)$。

② 检查 d_2 的 χ 坐标的最右边比特值 $\gamma\in\{0,1\}$，其中，$d_2=(d_{2x},d_{2y})$ 是 G_1 中的一个点，称第一个坐标 d_{2x} 是 d_2 的 χ 坐标。

③ 计算 $\sigma_1=d_1(v_\gamma w^h)^k$，$\sigma_2=d_2$ 和 $\sigma_3=g^k$，输出消息 m 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$。

4) Verify 算法

对于用户身份 $ID=\{ID_1,\mathrm{L}\ ,ID_l\}$，消息 m 及签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，验证者执行如下操作。

① 检查 σ_2 的 χ 坐标的最右边比特值 $\gamma\in\{0,1\}$。

② 计算 $h=H(m\|ID\|\sigma_2\|\sigma_3)$。

③ 验证式(2)是否成立。

$$e(\sigma_1,g)=P_{\text{pub}}e(u'\prod_{i=1}^{l}u_i^{ID_i},\sigma_2)e(v_\gamma w^h,\sigma_3) \tag{2}$$

若式(2)成立，说明 σ 是合法签名，输出 1；否则，σ 是非法签名，输出 0。

5) SAV-Setup 算法

验证者随机选择 $\beta\in Z_p^*$，并设置字符串 $VString=\beta$。这里的字符串 $VString$ 包含了验证者需要预计算的秘密信息 β，如果服务器知道 $VString$，可以让验证者确信一个非法签名是合法的。因此字符串 $VString$ 仅对验证者自己是已知的，对服务器和其他用户是保密的。

6) SAV-Verify 协议

对于字符串 $VString=\beta$ 和用户身份 ID，验证者收到消息签名对 $(m,\sigma=(\sigma_1,\sigma_2,\sigma_3))$ 后，与服务器执行如下的交互协议。

① 验证者首先利用 $VString=\beta$ 计算 $\sigma'=(\sigma_1',\sigma_2',\sigma_3')=((\sigma_1)^{\beta},\sigma_2,\sigma_3)$，然后发送 (ID,m,σ') 给服务器。

② 收到 (ID,m,σ') 后，服务器首先检查 σ_2' 的 χ 坐标的最右边比特值 $\gamma\in\{0,1\}$，然后计算 $h=H(m\|ID\|\sigma_2'\|\sigma_3')$，$K_1=e(\sigma_1',g)$，$K_2=e(u'\prod_{i=1}^{l}u_i^{ID_i},\sigma_2')$ 和 $K_3=e(v_\gamma w^h,\sigma_3')$，最后发送 (K_1,K_2,K_3) 给验证者。

③ 收到 (K_1,K_2,K_3) 后，验证者计算等式 $K_1=(P_{\text{pub}}K_2K_3)^{\beta}$。若等式成立，说明 σ 是合法签名，输出 1；否则，σ 是非法签名，输出 0。

5　安全性证明与有效性分析

5.1　合理性分析

1) 密钥提取算法的合理性

给定身份 ID 对应的私钥 $d_{ID}=(d_1,d_2)=(g_2^{\alpha}(u'\cdot\prod_{i=1}^{l}u_i^{ID_i})^r,g^r)$，其有效性验证如下

$$\begin{aligned}e(d_1,g)&=e(g_2^{\alpha}(u'\prod_{i=1}^{l}u_i^{ID_i})^r,g)\\&=e(g_2^{\alpha},g)e((u'\prod_{i=1}^{l}u_i^{ID_i})^r,g)\\&=e(g_2,g^{\alpha})e(u'\prod_{i=1}^{l}u_i^{ID_i},g^r)\\&=P_{\text{pub}}e(u'\prod_{i=1}^{l}u_i^{ID_i},d_2)\end{aligned}$$

2) 服务器辅助验证协议的正确性验证

对于字符串 $VString=\beta$ 和 m 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)=(g_2^{\alpha}(u'\prod_{i=1}^{l}u_i^{ID_i})^r(v_\gamma w^h)^k,g^r,g^k)$，由于

$$\begin{aligned}\sigma'=(\sigma_1',\sigma_2',\sigma_3')&=((\sigma_1)^{\beta},\sigma_2,\sigma_3)\\&=((g_2^{\alpha}(u'\prod_{i=1}^{l}u_i^{ID_i})^r(v_\gamma w^h)^k)^{\beta},g^r,g^k)\end{aligned}$$

于是有

$$K_1 = e(\sigma_1', g) = e((g_2^{\alpha}(u'\prod_{i=1}^{l} u_i^{ID_i})^r (v_\gamma w^h)^k)^\beta, g)$$

$$= e(g_2^{\alpha\beta}, g)e((u'\prod_{i=1}^{l} u_i^{ID_i})^{r\beta}, g)e((v_\gamma w^h)^{k\beta}, g)$$

$$= e(g_2, g^{\alpha})^\beta e(u'\prod_{i=1}^{l} u_i^{ID_i}, g^r)^\beta e(v_\gamma w^h, g^k)^\beta$$

$$= e(g_2, g_1)^\beta e(u'\prod_{i=1}^{l} u_i^{ID_i}, \sigma_2')^\beta e(v_\gamma w^h, \sigma_3')^\beta$$

$$= (P_{\text{pub}} K_2 K_3)^\beta$$

5.2　安全性分析

本文提出的新方案基于 Kwon 方案[14]，而文献[14]基于 CDH 困难问题假设，已在标准模型下证明了 Kwon 方案满足强不可伪造性。由定义 5 可知，仅需证明服务器辅助验证协议满足完备性，就可以证明本文方案是安全的。

定理 1　本文方案的服务器辅助验证协议能抵抗合谋攻击，并在自适应性选择消息击下满足完备性。

证明　在执行服务器辅助验证协议 SAV-Verify 中，攻击者 A 代表服务器，挑战者 C 代表验证者。A 发送给 C 一个非法的消息签名对 (m^*, σ^*)，A 的目标是让 C 确信 σ^* 是消息 m^* 的合法签名。

1) 系统建立。C 随机选择 $\beta^* \in Z_p^*$，通过运行 Setup 算法和 SAV-Setup 算法产生系统参数 cp、主密钥 msk 和字符串 $VString = \beta^*$。对于用户身份 ID^*，挑战者 C 随机选择 $r^* \in Z_p^*$，运行 Extract 算法生成 ID^* 的私钥 $d_{ID}^* = (d_1^*, d_2^*) = (g_2^{msk}(u'\prod_{i=1}^{l} u_i^{ID_i^*})^{r^*}, g^{r^*})$，发送 $\{cp, msk, ID^*, d_{ID}^*\}$ 给 A。

2) 查询。由于 A 拥有主密钥 msk，可以生成任意用户的私钥和任意消息的签名，所以攻击者 A 只需进行服务器辅助验证询问。对于攻击者 A 发起的每次询问 (m_i, σ_i)，C 通过与 A 执行 SAV-Verify 协议进行响应，并将运行结果发送给 A。

3) 输出。经过有限次的询问后，攻击者 A 将伪造的消息签名对 $(m^*, \sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*))$ 发送给挑战者 C，这里 Ω_{m^*} 是 m^* 对应于用户身份 ID^* 的所有合法签名的集合，$\sigma^* \notin \Omega_{m^*}$。挑战者利用 $VString$ 计算 $(\sigma^*)' = ((\sigma_1^*)', (\sigma_2^*)', (\sigma_3^*)') = ((\sigma_1^*)^{\beta^*}, \sigma_2^*, \sigma_3^*)$，将 $((\sigma_1^*)', (\sigma_2^*)', (\sigma_3^*)')$ 发送给攻击者 A。A 首先检查 $(\sigma_2^*)'$ 的 χ 坐标的最右边比特值 $\gamma^* \in \{0,1\}$，然后计算 $h^* = H(m^* \| ID^* \| (\sigma_2^*)' \| (\sigma_3^*)')$，$K_1^* = e((\sigma_1^*)', g)$，$K_2^* = e(u'\prod_{i=1}^{l} u_i^{ID_i^*}, (\sigma_2^*)')$ 和 $K_3^* = e(v_{\gamma^*} w^{h^*}, (\sigma_3^*)')$，并将 (K_1^*, K_2^*, K_3^*) 返回给挑战者 C。

下面分析等式 $K_1^* = (P_{\text{pub}} K_2^* K_3^*)^{\beta^*}$ 成立的概率是 $\frac{1}{p-1}$。

① 因为 $(\sigma_1^*)' = (\sigma_1^*)^{\beta^*}$ 且 β^* 是 Z_p^* 是随机选取的，所以攻击者 A 利用 σ^* 正确伪造出 $(\sigma^*)'$ 的概率是 $\frac{1}{p-1}$。

② 如果攻击者 A 发送的 (K_1^*, K_2^*, K_3^*) 满足 $K_1^* = (P_{\text{pub}} K_2^* K_3^*)^{\beta^*}$，则有

$$\beta^* = \log_{P_{\text{pub}} K_2^* K_3^*} K_1^*$$

由于 $\beta^* \in Z_p^*$，因此攻击者 A 找到满足以上等式的元素 β^* 的概率是 $\frac{1}{p-1}$。由此可见，对于一个非法的消息签名对 (m^*, σ^*)，A 能让 C 确信 σ^* 是消息 m^* 的有效签名的概率是 $\frac{1}{p-1}$，即本文方案的 SAV-Verify 协议在自适应性选择消息和合谋攻击下满足完备性。

在本文方案的服务器辅助验证协议 SAV-Verify 中，验证者将 σ_1 的幂运算值 σ_1^{β} 发送给攻击者，由于参数 β 对服务器是保密的，因而可有效抵抗针对服务器辅助验证签名方案的各类合谋攻击[16,17]。

定理 2　在标准模型下，Kwon 方案在自适应性选择身份和消息攻击下满足强不可伪造性[14]。

定理 3　在标准模型下，本文提出的基于身份服务器辅助验证签名方案在合谋攻击、自适应选择身份和消息攻击下是安全的。

通过定义 5、定理 1 和定理 2，很容易得到定理 3。

5.3　性能比较

为了表述方便，用 PS 方案表示 Paterson 和 Schuldt[10]提出的基于身份签名方案，TTS 方案表示 Tsai 等[12]提出的基于身份签名方案，ZS-SAVIDS-1 方案和 ZS- SAVIDS-2 方案分别表示 Zhang 等[8]提出的第 1 个和第 2 个基于身份服务器辅助验证签名方案。假定所有方案选择相同长度的素数 p，以及相同阶的群 G_1 和 G_2。由于计算量比较大的密码学操

表 1　　**计算开销与安全性能比较**

方案	签名验证者的计算开销				签名长度	标准模型	安全属性	安全假设
	G_1 中的幂运算	G_2 中的幂运算	双线性对运算	计算复杂度				
PS 方案	0	0	3	$3P$	$3\|G_1\|$	是	存在不可伪造性	CDH 假设
TTS 方案	0	1	4	M_2+4P	$3\|G_1\|$	是	强不可伪造性	CDH 和 CRH 假设
Kwon 方案	1	0	3	M_1+3P	$3\|G_1\|$	是	强不可伪造性	CDH 假设
ZS-SAVIDS-1 方案	1	4	1	M_1+4M_2+P	$2\|G_1\|$	否	存在不可伪造性	BDH 假设
ZS-SAVIDS-2 方案	1	4	0	M_1+4M_2	$2\|G_1\|$	否	存在不可伪造性	BDH 假设
本文方案	1	1	0	M_1+M_2	$3\|G_1\|$	是	强不可伪造性	CDH 假设

作是双线性对与幂运算，因此不再详细讨论其余运算操作。用 M_1 表示 G_1 上的幂运算，用 M_2 表示 G_2 上的幂运算，用 P 表示双线对运算的数量，所有方案的比较结果如表 1 所示。

由表 1 可知，在本文方案中验证者只需进行 2 次幂运算；但在 Kwon 方案中，验证者的计算开销是 3 次双线性对和 1 次幂运算，因此根据定义 3 可得知本文方案是计算节约的。

与其他 5 个方案相比，本文方案的签名验证者的计算开销最小，大大提高了签名的验证速度，具有较高的计算效率，在低端计算设备中具有更好的适应性。虽然 Zhang 等[8]提出的 2 个方案具有较短的签名长度，但这 2 个方案的安全性依赖于理想随机预言机，而本文方案的安全性仅依赖于 CDH 困难问题，并满足强不可伪造性，具有更高的安全性。本文方案与 Kwon 方案[14]的系统公开参数长度相同，但小于 PS 方案[10]和 TTS 方案[12]的系统参数长度，具有较高的通信代价。

6　结束语

基于 Kwon 方案和 CDH 假设，提出了一个强不可伪造的基于身份服务器辅助验证签名方案，其安全性不依赖于理想的随机预言机。验证者在本文方案中不需要执行耗时的双线性对运算，大大降低了验证者的计算开销。本文方案的系统参数小，通信代价低，非常适用于各类低端计算设备。下一步的工作是设计具有更短公开参数的基于身份服务器辅助验证签名方案。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// CRYPTO 1984, LNCS 0196. Springer Berlin Heidelberg, c1984: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//CRYPTO 2001, LNCS 2139. Springer Berlin Heidelberg, c2001: 213-229.

[3] KAR J. Provably secure on-line/off-line identity-based signature scheme for wireless sensor network[J]. IJ Network Security, 2014, 16(1): 29-39.

[4] TIAN M, HUANG L. Efficient identity-based signature from lattices[M]. ICT Systems Security and Privacy Protection, Springer Berlin Heidelberg, 2014: 321-329.

[5] TSENG Y M, TSAI T T, HUANG S S. Leakage-free ID-based signature[J]. The Computer Journal, 2015, 58(4): 750-757.

[6] ATTRAPADUNG N, EMURA K, HANAOKA G, et al. A revocable group signature scheme from identity-based revocation techniques: achieving constant-size revocation list[C]//Applied Cryptography and Network Security.c2014: 419-437.

[7] HAO S G, LI Z, GHULAM M. A union authentication protocol of cross-domain based on bilinear pairing[J]. Journal of Software, 2013, 8(5): 1094-1100.

[8] ZHANG J, SUN Z. An ID-based server-aided verification short signature scheme avoid key escrow[J]. Journal of Information Science and Engineering, 2013, 29(3): 459-473.

[9] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557-594.

[10] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model[C]//ACISP, LNCS 4058. Springer Berlin Heidelberg, c2006: 207-222.

[11] WU Q, ZHANG L Y. New strongly unforgeable identity-based signature scheme in the standard model[J]. Journal of Beijing University of Posts and Telecommunications, 2011, 34(3): 71-74.

[12] TSAI T T, TSENG Y M, HUANG S S. Efficient strongly unforgeable ID-based signature without random oracles[J]. Informatica, 2014, 25(3): 505-521.

[13] HUNG Y H, TSAI T T, TSENG Y M, et al. Strongly secure revocable

ID-based signature without random oracles[J]. Information Technology and Control, 2014, 43(3): 264-276.

[14] KWON S. An identity-based strongly unforgeable signature without random oracles from bilinear pairings [J]. Information Sciences, 2014, 276(1): 1-9.

[15] WU W, MU Y, SUSILO W, et al. Provably secure server-aided verification signatures[J]. Computers & Mathematics with Applications, 2011, 61(7): 1705-1723.

[16] WANG Z, WANG L, YANG Y, et al. Comment on Wu, et al.'s server-aided verification signature schemes[J]. IJ Network Security, 2010, 10(2): 158-160.

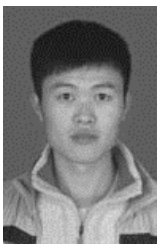
[17] WU H, XU C X, DENG J, et al. On the security of server-aided verification signature schemes[J]. Journal of Computational Information System, 2013, 9(4): 1449-1454.

作者简介：

杨小东（1981-），男，甘肃甘谷人，西北师范大学副教授，主要研究方向为密码学及云计算安全。

杨苗苗（1991-），女，甘肃金昌人，西北师范大学硕士生，主要研究方向为大数据安全。

高国娟（1991-），女，甘肃永登人，西北师范大学硕士生，主要研究方向为信息安全。



李亚楠（1990-），男，山东沂州人，西北师范大学硕士生，主要主要研究方向为网络安全。

鲁小勇（1982-），男，甘肃张掖人，西北师范大学博士生、工程师，主要研究方向为信息系统安全。

王彩芬（1963-），女，河北安国人，西北师范大学教授、博士生导师，主要研究方向为密码学、网络安全和信息安全。