doi:10.11959/j.issn.1000-436x.2015271

对一个基于身份签密方案的分析与改进

张宇[1,2]，杜瑞颖[1]，陈晶[1]，侯健[3]，周庆[2]，王文武[1]
（1. 武汉大学 计算机学院，湖北 武汉 430072；2. 信息保障技术重点实验室，北京 100072；3. 总参陆航研究所，北京 101121）

摘 要：基于身份的签密方案计算开销小，密钥管理简单，适用于保证信息的保密性和认证性。Zhang 等提出了一个高效的基于身份签密方案，并在随机预言模型下证明了该方案的安全性。通过分析发现 Zhang 等的签密方案存在缺陷，针对缺陷提出了相应的改进方案，并且基于随机预言模型证明了新方案的安全性。理论分析和实验仿真证明，所提方案计算复杂度低，适合于实际应用。

关键词：基于身份的签密；可证明安全；双线性对；随机预言模型
中图分类号：TP309 **文献标识码**：A

Analysis and improvement of an identity-based signcryption

ZHANG Yu[1,2], DU Rui-ying[1], CHEN Jing[1], HOU Jian[3], ZHOU Qing[2],WANG Wen-wu[1]
(1. School of Computer, Wuhan University, Wuhan 430072, China;
2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China;
3. Army Aviation Research Institute, Beijing 101121, China)

Abstract: Identity-based signcryption was a cryptography scheme with low computation cost and simple key management, which was suitable to guarantee the confidentiality and authentication of information. Zhang, *et al* proposed an efficient identity-based signcryption scheme, and provided security provement in the random oracle model. Through analysis, it was found out that Zhang's signcryption scheme was imperfect. To avoid the defect, a new identity-based signcryption scheme was proposed, whose security was proved in the random orcale model. Both the theoretical analysis and the experimental results show that proposed scheme is efficient and suitable for practical application.

Key words: identity-based signcryption; provable security; bilinear pairing; random oracle model

1 引言

保密性和认证性是信息安全的 2 个基本要求。密码学的传统方法是采用“先签名后加密”的方式来满足这 2 个基本要求的。但由于需要付出的计算代价为签名和加密之和，这种处理方式的效率比较低。为了解决该问题，文献[1]提出了签密的概念。利用签密，数字签名和公钥加密能够在一个逻辑步骤内实现，并且计算和通信效率要高于传统的“先签名后加密”。因此，签密是同时保证保密性和认证性的理想方法[2,3]。

传统公钥密码体制需要认证机构颁发证书来绑定用户的身份和公钥，这样就带来了证书管理的问题。如果用户规模庞大，系统效率就会非常低。针这一问题，文献[4]提出了基于身份的密码体制。该体制实现了公钥与身份的绑定，无需第三方提供认证服务，使密钥管理变得简单。在基于身份的密码体制中，通过用户的身份信息(如身份证号、E-mail 地址等)，能够获得该用户的公钥，私钥由私钥生成中心(PKG)产生[5,6]。

2002 年，文献[7]提出了基于身份的签密方案。基于身份的签密方案综合了签密体制和基于身份密码体制的优点，计算和通信效率高，密钥管理容易[8]。近年来，基于身份的签密方案的研究取得了一系列成果[7,9~23]。

文献[17]提出了目前计算效率最高的基于身份

收稿日期：2015-05-13；修回日期：2015-07-24
基金项目：信息保障技术重点实验室开放基金资助项目（KJ-13-104）
Foundation Item: The Foundation of Science and Technology on Information Assurance Laboratory (KJ-13-104)

的签密方案 S-IDSC，并基于随机预言模型证明了该方案的安全性。本文通过分析发现，S-IDSC 方案存在缺陷，其签名的验证部分，只有在特定条件下才能成立。针对该方案的缺陷，本文提出了一个改进方案 SS-IDSC，并在随机预言模型中给出了安全性证明。通过理论分析和仿真实验可以发现，相较于已有的方案，SS-IDSC 的计算效率较高。

2　基础知识

2.1　双线性对及困难问题

定义 1　(双线性对)　令 G_1 为由生成元 P 生成的 q 阶循环加法群，G_2 为具有相同阶 q 的循环乘法群，a, b 是 Z_q^* 中的元素。假定 G_1 和 G_2 中的离散对数问题是困难问题。双线性对是满足以下性质的一个映射 $e: G_1 \times G_1 \to G_2$。

1) 双线性性：$e(aP,bQ)=e(P,Q)^{ab}$。

2) 非退化性：存在 $P,Q \in G_1$，使 $e(P,Q) \neq 1$ 成立。

3) 可计算性：对所有的 $P,Q \in G_1$，存在有效算法，能够计算 $e(P,Q)$。

可以通过有限域超椭圆曲线上的 Tate 对或 Weil 对来构造[24]双线性映射 e。

定义 2　(BDH 问题和 CDH 问题)　设 G_1、G_2 为素数 q 阶循环群，$e: G_1 \times G_1 \to G_2$ 是双线性映射，P 是 G_1 的生成元。

Bilinear Diffie-Hellman (BDH)问题：对于任意均匀随机选取的未知 $a,b,c \in Z_q^*$，由 $<P,aP,bP,cP>$ 计算 $e(P,P)^{abc}$。

Compute Diffie-Hellman(CDH)问题：对于任意均匀随机选取的未知 $a,b \in Z_q^*$，由 $<P,aP,bP>$ 计算 abP。

2.2　基于身份签密方案的组成

文献[7]中给出了基于身份的签密方案的形式化定义，包含系统建立(setup)、密钥提取(extract)、签密(signcrypt)、解签密(unsigncrypt)等 4 个算法。具体请参阅文献[7]。

2.3　基于身份签密方案的安全性定义

文献[10]通过敌手和挑战者之间的游戏定义了基于身份签密方案的保密性和不可伪造性，具体请参阅文献[10]。

3　对 S-IDSC 方案的分析

3.1　S-IDSC 方案

该方案由以下算法组成。

1) setup：输入安全参数 z，PKG 执行以下步骤。

①选取 2 个阶为素数 q 的循环群 $G_1, G_2, e: G_1 \times G_1 \to G_2$ 是一个双线性对；

②选取 G_1 的一个生成元 P，随机选择 $s \in Z_q^*$ 作为主密钥，通过计算 $P_{\text{pub}}=sP$ 获得系统公钥；

③选取安全的对称密码算法(E,D)，3 个散列函数 $H_1: \{0,1\}^{l_1} \to G_1, H_2: G_2 \to Z_q^*, H_3: G_1 \times \{0,1\}^n \to Z_q^*$。这里，$l_1$ 是身份 ID 的长度，n 是明文的长度。

最后，公布公共参数 $params=(G_1, G_2, e, P, P_{\text{pub}}, n, H_1, H_2, H_3)$，保密主密钥 s。

2) extract：输入 $params$、系统的主密钥 s 和用户身份 u_i，PKG 计算用户的公钥 $Q_i=H_1(u_i)$ 以及私钥 $d_i=sQ_i$，通过安全的方式将私钥发送给用户。

3) signcrypt：假设用户 A 要发送消息 m 给用户 B。A 执行以下步骤。

①计算 $Q_{\text{B}}=H_1(u_{\text{B}})$；

②随机选择 $r \in Z_q^*$，计算 $R=rQ_{\text{B}}$，$\omega=e(d_{\text{A}}, Q_{\text{B}})$，$k=H_2(\omega)$；

③计算 $h_3=H_3(R,m)$，$S=\dfrac{r}{h_3+d_{\text{A}}}$，$c=E_k(S \| m)$；

④发送密文 $\sigma=\{c,h_3\}$ 给用户 B。

4) unsigncrypt：用户 B 接收到密文 σ，执行以下步骤。

①计算 $Q_{\text{A}}=H_1(u_{\text{A}})$，$\omega=e(d_{\text{B}},Q_{\text{A}})$；

②计算 $k=h_2(\omega)$；

③计算 $S \| m=D_k(c)$；

④计算 $R=S(h_3Q_{\text{B}}+d_{\text{B}}Q_{\text{A}})$，验证 $h_3=H_3(R,m)$ 是否成立，若成立，接受 m；否则输出 $\perp$。

在计算 $S=\dfrac{r}{h_3+d_{\text{A}}}$ 和 $R=S(h_3Q_{\text{B}}+d_{\text{B}}Q_{\text{A}})$ 时，要将 G_1 上的点 d_{A} 和 d_{B} 转换为 Z_q^* 中的数。转换时，可以使用点的横坐标来代替点。

3.2　对 S-IDSC 方案的分析

假设 P' 为 G_1 上的任意点，定义操作 $X(P')$，其功能为将 P' 转换为 Z_q^* 中的数。

S-IDSC 方案的签密过程中，发送方计算 $S=\dfrac{r}{h_3+X(d_{\text{A}})}$，因此有 $r=S(h_3+X(d_{\text{A}}))$。又因为 $R=rQ_B$，所以可以得出 $R=S(h_3Q_{\text{B}}+X(d_{\text{A}})Q_{\text{B}})$。解签密过程中，接收方计算 $R'=S(h_3Q_{\text{B}}+X(d_{\text{B}})Q_{\text{A}})$。为保证 $R=R'$ 成立，必须保证在 X 操作下等式 $X(d_{\text{A}})Q_{\text{B}}=X(d_{\text{B}})Q_{\text{A}}$ 成立，而取点的横坐标操作并

不满足该性质。

3.3 改进方案 SS-IDSC

针对 S-IDSC 方案的缺陷，本文提出了相应的改进方案，称为 SS-IDSC，具体如下。

1) setup：与 S-IDSC 方案相同。

2) extract：与 S-IDSC 方案相同。

3) signcrypt：步骤①、步骤②与 S-IDSC 中相同。

③计算 $h_3=H_3(R,m)$，$S=\dfrac{d_{\mathrm{A}}}{h_3+r}$，$c=E_k(S\|m)$；

④发送密文 $\sigma=\{c,R\}$ 给用户 B。

4) unsigncrypt：步骤①~步骤③与 S-IDSC 中相同。

④计算 $h_3=H_3(R,m)$，验证 $e(S,R+h_3Q_B)=\omega$ 是否成立，若成立，接受 m；否则输出 $\perp$。

容易得知，根据双线性对的性质等，方案的正确性可以得到保证。

$$\begin{aligned}\omega&=e(d_{\mathrm{A}},Q_{\mathrm{B}})=e(sQ_{\mathrm{A}},Q_{\mathrm{B}})\\&=e(Q_{\mathrm{A}},d_{\mathrm{B}})\end{aligned}$$

$$\begin{aligned}e(S,R+h_3Q_{\mathrm{B}})&=e\left(\frac{d_{\mathrm{A}}}{r+h_3},rQ_{\mathrm{B}}+h_3Q_{\mathrm{B}}\right)\\&=e(d_{\mathrm{A}},Q_{\mathrm{B}})\\&=\omega\end{aligned}$$

4 对 SS-IDSC 的安全性分析

SS-IDSC 方案的安全性可以由以下定理保证。

定理 1 如果存在一个敌手 D 能够以不可忽略的概率 ξ 赢得 IND-IBSC-CCA2 游戏[10](至多进行 q_i 次 H_i 询问(i=1,2,3)、q_e 次 extract 询问、q_s 次 signcrypt 询问和 q_u 次 unsigncrypt 询问)，则存在区分者 C，能够在 $t'<t+(q_s+2q_u)t_e$ 时间内，以概率 ξ' 解决 BDH 问题。这里，$\xi'>\dfrac{8\xi}{q_1^{\ 2}(q_1-1)^2q_2}$。

证明 假设 C 接收到随机的 BDH 问题实例 $(P,P_1,P_2,P_3)=(P,aP,bP,cP)$，他的目标是计算出 $e(P,P)^{abc}$。敌手 D 作为 C 的子程序，在 IND-IBSC-CCA2 游戏中扮演敌手，C 在该游戏中扮演挑战者。

初始化：C 发送系统参数给 D，其中 $P_{\mathrm{pub}}=cP$。C 维护列表 L_1，L_2，L_3 用以跟踪 D 对预言机 H_1、H_2、H_3 的询问。不妨假设 D 不会进行重复的询问。

询问阶段：D 在这个阶段进行多项式有界次适应性询问。

H_1 询问：输入参数为 u_i。Γ 从 $\{1,2,\cdots,q_1\}$ 中随机选择 α、β。对于 D 的第 α 次询问，返回 $H_1(u_\alpha)=aP$，将 $(u_\alpha,aP,-)$ 添加入 L_1；第 β 次询问，返回 $H_1(u_\beta)=bP$，将 $(u_\beta,bP,-)$ 添加入 L_1。其他情况下，C 随机选择 $l_i\in Z_q^*$。此处，l_i 需满足 $l_i\notin L_1$。将 (u_i,l_iP,l_i) 添加到列表 L_1，返回 $H_1(u_i)=l_iP$。

H_2 询问：输入参数是 ω。C 检查 L_2 中是否已存在元组 (ω,k)。若存在，则返回对称密钥 k。否则，随机从 Z_q^* 中选择 L_2 中未出现过的 k，添加 (ω,k) 到 L_2 并返回 k。

H_3 询问：输入参数是 (R,m)。C 首先检查 L_3 中是否存在元组 (R,m,h_3)。若存在，则返回 h_3。否则，随机从 Z_q^* 中选择 L_3 中未出现过的 h_3，添加 (R,m,h_3) 到 L_3 并返回 h_3。

extract 询问：输入参数是 u_i。不妨假设 D 在对 u_i 执行该询问前已经执行过 H_1 询问。若 $i=\alpha$ 或 $i=\beta$，C 退出游戏。否则，C 查找 L_1 获取 (u_i,l_iP,l_i)，返回 $d_i=l_icP$。

signcrypt 询问：输入参数为 $(m,u_{\mathrm{A}},u_{\mathrm{B}})$。$u_{\mathrm{A}}$ 为发送方身份，u_{B} 为接收方身份，分以下 3 种情况考虑。

1) 如果 $u_{\mathrm{A}}\neq u_\alpha$ 且 $u_{\mathrm{A}}\neq u_\beta$，C 可以通过 extract($u_{\mathrm{A}}$) 询问得出 d_{A}，然后简单运行签密运算 signcrypt($m,d_{\mathrm{A}},u_{\mathrm{B}}$) 即可。

2) 如果 $u_{\mathrm{A}}=u_\alpha$ 或 $u_{\mathrm{A}}=u_\beta$，但 $u_{\mathrm{B}}\neq u_\alpha$ 且 $u_{\mathrm{B}}\neq u_\beta$，C 执行如下步骤。

①首先查找 L_1 获取 $(u_{\mathrm{B}},l_{\mathrm{B}}P,l_{\mathrm{B}})$，可以得出 $d_{\mathrm{B}}=l_{\mathrm{B}}cP$。随机选取 $a_1\in Z_q^*$，计算 $S=\dfrac{aP}{a_1}$。

②随机选取 $h_3\in Z_q^*$，计算 $R=a_1l_{\mathrm{B}}cP-h_3l_{\mathrm{B}}P$。检索 L_3 中是否已存在 (R,m,h_3') 并且 $h_3'\neq h_3$。如果存在，则重复本步骤，直到三元组的前两元在 L_3 中没有出现过，将此条目加入 L_3 中。

③计算 $\omega=e(Q_{\mathrm{A}},d_{\mathrm{B}})$，通过 H_2 询问获取 $k=H_2(\omega)$，$c=E_k(S\|m)$。

④发送密文 $\sigma=\{c,R\}$ 给攻击者 D。

3) 若 u_{A} 和 u_{B} 就是 u_α 和 u_β，则随机选择 $R^*\in G_1$，$S^*\in G_1$，$\omega^*\in G_2$，通过 H_2 询问获取 $k^*=H_2(\omega^*)$，$c=E_{k^*}(S^*\|m)$，发送密文 $\sigma^*=\{c^*,R^*\}$ 给攻击者 D。这里，也需要像步骤 2)中一样，保证 L_3 中不存在冲突项。由于 D 无法获取 u_{A} 或 u_{B} 的私钥，不能验证 σ^* 的合法性。

unsigncrypt 询问：输入参数为 $(\sigma,u_{\mathrm{A}},u_{\mathrm{B}})$。

1) 如果 $u_{\mathrm{B}} \neq u_{\alpha}$ 且 $u_{\mathrm{B}} \neq u_{\beta}$，C 可以通过 extract($u_{\mathrm{B}}$) 询问得出 d_{B}，然后简单运行解签密运算 unsigncrypt($\sigma, u_{\mathrm{A}}, d_{\mathrm{B}}$) 即可。

2) 如果 $u_{\mathrm{B}} = u_{\alpha}$ 或 $u_{\mathrm{B}} = u_{\beta}$，但 $u_{\mathrm{A}} \neq u_{\alpha}$ 且 $u_{\mathrm{A}} \neq u_{\beta}$，C 执行如下步骤。

①首先查找 L_1 获取 $(u_{\mathrm{A}}, l_{\mathrm{A}}P, l_{\mathrm{A}})$，可以得出 $d_{\mathrm{A}} = l_{\mathrm{A}}cP$；

②计算 $\omega = e(d_{\mathrm{A}}, Q_{\mathrm{B}})$，若 $\omega \notin L_2$，则返回 $\perp$；否则查询 L_2 获取 $k = H_2(\omega)$；

③计算 $S \| m = D_k(c)$。若 $(R, m) \notin L_3$，则返回 $\perp$；否则查询 L_3 获取 $h_3 = H_3(R, m)$；

④验证 $e(S, R + h_3 Q_{\mathrm{B}}) = \omega$ 是否成立。若成立，则返回 m；否则返回 $\perp$。

3) 如果 u_{A} 和 u_{B} 就是 u_{α} 和 u_{β}，由于攻击者 D 不可能拥有相关私钥，密文 σ 只可能来自于 signcrypt 询问。挑战者 C 通过查询 signcrypt 相关记录予以应答。

挑战：D 选择长度均为 L 的明文 $\{m_0, m_1\}$ 和挑战身份 $\{u_{\mathrm{A}}, u_{\mathrm{B}}\}$。如果 u_{A}，u_{B} 不是 u_{α} 和 u_{β}，C 退出游戏。否则，C 随机选择 $R \in G_1$，$c \in \{0,1\}^n$，其中，n 是明文长度为 L 时对称加密算法 E 输出密文的长度，发送 $\sigma = \{c, R\}$ 给 D。

猜测：询问阶段中的操作此处都可以执行。但不能对 u_{A} 或 u_{B} 执行 extract 询问，也不能对 σ 执行 unsigncrypt 询问。本阶段结束时，D 输出 γ' 作为其对 m_{γ} 中 γ 的猜测。此时，C 从 L_2 中随机选择条目 (ω, k)，输出 ω 作为对 BDH 问题的解答。

下面分析 C 成功的概率。

如果 D 在询问阶段中对 u_{α} 或 u_{β} 执行了 extract 询问，C 将退出游戏。C 不在询问阶段中退出游戏的概率 $\Pr[\neg(\text{C abort in I})] = \dfrac{\mathrm{C}_{q_1-2}^{q_1-q_e}}{\mathrm{C}_{q_1}^{q_1}} = \dfrac{(q_1-q_e)(q_1-q_e-1)}{q_1(q_1-1)}$。由于 $(q_1 - q_e) \geqslant 2$，所以 $\Pr[\neg(\text{C abort in I})] \geqslant \dfrac{2}{q_1(q_1-1)}$。D 在猜测过程中选中 u_{α} 和 u_{β} 作为挑战身份的概率大于 $\dfrac{1}{\mathrm{C}_{q_1}^2} = \dfrac{2}{q_1(q_1-1)}$。

令 ω' 代表 BDH 问题的正确解答，Ω 代表事件攻击者 D 在模拟过程中对 ω' 执行了 H_2 询问。文献[24]中已经证明，如果 D 以概率 ξ 赢得游戏，那么 $\Pr[\Omega] \geqslant 2\xi$。

D 随机从 L_2 中选择一个条目，恰好选中 ω' 所在条目的概率为 $\dfrac{1}{q_2}$。

综上，

$$\Pr[\text{C succeed}] > \frac{2}{q_1(q_1-1)} \frac{2}{q_1(q_1-1)} \frac{2\xi}{q_2} = \frac{8\xi}{q_1^2(q_1-1)^2 q_2}$$

每次签密询问中，至多需要 1 次双线性对运算；每次解签密询问中，至多需要 2 次双线性对运算。所以 C 的计算时间 $t' < t + (q_s + 2q_u)t_e$。

定理 2　如果存在一个敌手 D 能够以不可忽略的概率 ξ 赢得 EUF-IBSC-CMA 游戏(至多进行 q_i 次 H_i 询问(i=1,2,3)、q_e 次 extract 询问、q_s 次 signcrypt 询问和 q_u 次 unsigncrypt 询问)，则存在区分者 C，能够在 $t' < t + (q_s + 2q_u)t_e$ 时间内，以概率 ξ' 解决 BDH 问题。这里，$\xi' > \dfrac{4\xi}{q_1^2(q_1-1)^2 q_2}$

证明　假设 C 接收到随机的 BDH 问题实例 $(P, P_1, P_2, P_3) = (P, aP, bP, cP)$，其目标为计算出 $e(P,P)^{abc}$。C 将敌手 D 作为子程序使用。D 扮演 EUF-IBSC-CMA 游戏的敌手，C 扮演该游戏的挑战者。

初始化：与定理 1 证明过程类似。

询问阶段：与定理 1 证明过程类似。

伪造：D 输出一个新的三元组 (σ, u_A, u_B)。如果 u_{A}，u_{B} 不是 u_{α} 和 u_{β}，C 退出游戏。否则，C 从 L_2 中随机选择条目 (ω, k)，输出 ω 作为对 BDH 问题的解答。

下面分析 C 成功的概率。

类似于定理 1 中的分析，C 不在询问阶段中退出游戏的概率 $\Pr[\neg(\text{C abort in I})] \geqslant \dfrac{2}{q_1(q_1-1)}$。D 在伪造过程中选中 u_{α} 和 u_{β} 作为挑战身份的概率大于 $\dfrac{1}{\mathrm{C}_{q_1}^2} = \dfrac{2}{q_1(q_1-1)}$。

令 ω' 代表 BDH 问题的正确解答。如果 u_{A} 和 u_{B} 就是 u_{α} 和 u_{β}，并且 unsigncrypt($\sigma, u_{\mathrm{A}}, u_{\mathrm{B}}$) $\neq \perp$，那么可以确定生成密文 σ 时使用的对称密钥是 $k = H_2(\omega')$，即 ω' 存在于 L_2 中。D 随机从 L_2 中选择一个条目，恰好选中 ω' 所在条目的概率为 $\dfrac{1}{q_2}$。

综上，

$$\Pr[\text{C succeed}] > \frac{2}{q_1(q_1-1)} \frac{2}{q_1(q_1-1)} \frac{\xi}{q_2}$$

$$= \frac{4\xi}{q_1^2(q_1-1)^2 q_2}$$

类似于定理 1 证明中的分析，C 的计算时间 $t' < t + (q_s + 2q_u)t_e$。

5 效率分析

5.1 理论分析

从计算代价和通信代价 2 个方面来衡量本文提出的签密方案。

为了方便，用符号 E、M、P 分别代表 G_2 中的指数运算次数，G_1 中的标量乘运算次数，双线性对运算次数。$x(+y)$代表 x 次双线性对运算，y 次双线性对预运算。$|G_1|$表示 G_1 中元素的长度，$|q|$表示有限域 Z_q 中元素的长度，$|m|$表示明文长度，$|ID|$表示身份 ID 的长度。

本方案的签密过程中，需要 2 次标量乘运算，1 次双线性对预运算；解签密过程中，只需要 1 次标量乘运算，1 次双线性对运算，1 次双线性对预运算。本方案需要传输的信息是密文 $\sigma = \{c, R\}$，传输量为 $|c| + |R| = 2|G_1| + |m|$。表 1 给出了本文方案与已有的几个重要签密方案的对比。可以看出，本文方案效率有明显的优势。

表 1 本文的方案与已有的签密方案的性能对比

方案	签密			解签密			密文长度
	P	M	E	P	M	E	
文献[7]	0(+1)	3	0	3(+1)	0	1	$2\|G_1\|+\|m\|$
文献[13]	0(+1)	3	0	3	1	0	$2\|G_1\|+\|ID\|+\|m\|$
文献[14]	0(+1)	4	1	2(+2)	0	2	$2\|G_1\|+\|m\|$
文献[20]	0(+1)	3	1	2(+2)	0	2	$2\|G_1\|+\|ID\|+\|m\|$
文献[21]	0	2	2	2	1	1	$2\|G_1\|+\|G_2\|+\|ID\|+\|m\|$
文献[22]	0	4	1	2	3	1	$3\|G_1\|+\|m\|$
本文方案	0(+1)	2	0	1(+1)	1	0	$2\|G_1\|+\|m\|$

5.2 实验仿真

实验用 PC 平台配置如下。AMD Athlon 7850 处理器，4 GB DDR2 内存，操作系统为 Windows XP Professional SP3。安装 VMWare 9，虚拟机使用单处理器，1 GB 内存，操作系统为 Red Hat Enterprise Linux Server release 6.3。

在仿真中，本文使用了 Pairing-Based Cryptography(PBC)库[25]，选择了运算速度快，效率高的 A 类曲线[25]($y^2=x^3+x$，素数群的阶 r 取 160 bit，q 取 512 bit，循环加法群 G_1 中的点元素 p 取 512 bit)。所有的实验结果均是通过随机执行 100 次后取平均值获得的。

为了便于比较，本文也仿真了文献[13]中的方案 IIBS。实验结果如图 1、图 2 所示。图 1 所示为签密运算的开销，本文方案进行一次签密运算需要 9.73 ms，IIBS 进行一次签密方案需要 18.96 ms。图 2 示所为解签密运算的开销，本文方案进行一次解签密运算需要 7.38 ms，而 IIBS 需要 17.81 ms。相较于 IIBS，本文方案的效率具有明显的优势。

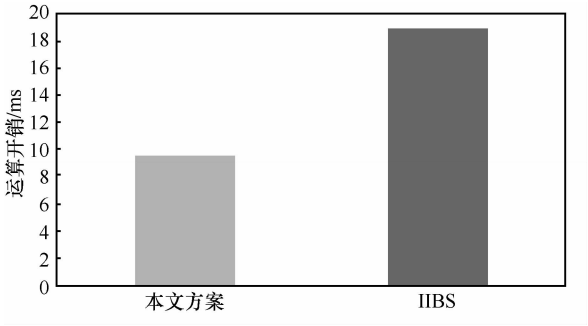


图 1 签密开销

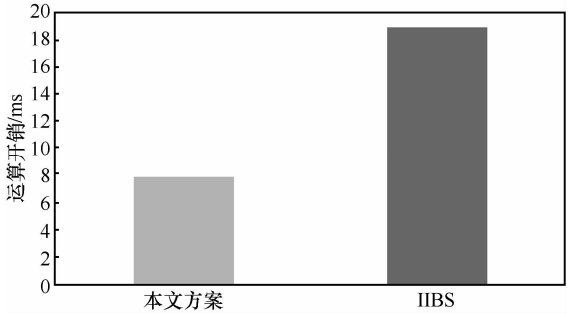


图 2 解签密开销

6 结束语

针对文献[17]存在的缺陷，本文提出了一个改进的基于身份的签密方案，并在随机预言模型下对新方案的安全性进行了证明。理论分析和实验仿真显示，本文提出的签密方案计算效率高，适合用来保证数据的保密性和认证性。

参考文献：

[1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)[A]. Advances in Cryptology—CRYPTO'97[C]. Springer, 1997.165-179.

[2] LI J, ZHAO J, ZHANG Y. Certificateless online/offline signcryption scheme[J]. Security and Communication Networks, 2014,8(11):1979-1990.

[3] LI Z H, FAN K, LI H. Efficient multiple signcryption scheme based on

two hard problems[J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(6):23-26.

[4] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proceedings of CRYPTO 84[C]. 1985.47-53.

[5] ANAND D, KHEMCHANDANI V, SHARMA R K. Identity-based cryptography techniques and applications (a review)[A]. International Conference on Computational Intelligence & Communication Networks[C]. IEEE, 2013.343-348.

[6] PHANEENDRA H D. Identity-based cryptography and comparison with traditional public key encryption: a survey[J]. International Journal of Computer Science & Information Technology, 2014,5(4):5521.

[7] MALONE-LEE J. Identity-based signcryption[A]. Proceedings of Public Key Cryptography-PKC 2005[C]. 2005.362-379.

[8] KHAN F L M K. A survey of identity-based signcryption[J]. IETE Technical Review, 2014, 28(3): 265-272.

[9] 张秋璞, 叶顶锋. 对一个基于身份的多重签密方案的分析和改进[J]. 电子学报, 2011, 39(12): 2713-2720.
ZHANG Q P, YE D F. Cryptanalysis and improvement of an identity-based multi-signcryption scheme[J]. Acta Electronica Sinica, 2011, 39(12): 2713-2720.

[10] LIBERT B, QUISQUATER J. A new identity based signcryption scheme from pairings[A]. IEEE Information Theory Workshop[C]. 2003.155-158.

[11] REDDY D N K C. Signcryption scheme for identity-based cryptosystems[J]. Mathematics of Computation, 2003, 48.

[12] CHOW S S, YIU S M, HUI LC *et al.* Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity[A]. Information Security and Cryptology-ICISC 2003[C]. 2004.352-369.

[13] CHEN L, MALONE-LEE J. Improved identity-based signcryption[A]. Public Key Cryptography-PKC 2005[C]. 2005.362-379.

[14] YU P, LF GH, GANG L. An efficient identity-based signcryption scheme[J]. Chinese Journal of Computers, 2006, 9: 018.

[15] ZHANG M W, YANG B, ZHOU M, *et al.* Analysis and improvement of two signcryption schemes[J]. Journal of Electronics and Information Technology, 2010, 32(7): 1731-1736.

[16] JIANHONG Z. Security analysis of two signcryption schemes[J]. Journal of Southeast University (Natural Science Edition). 2007: S1.

[17] 张串绒, 张玉清, 李发根, 等, 适于 ad hoc 网络安全通信的新签密算法[J]. 通信学报, 2010, 31(3): 19-24.
ZHANG C R, ZHANG Y Q, LI F G. New signcryption algorithm for secure communication of ad hoc networks[J]. Journal on communications. 2010, 31(3): 19-24.

[18] 黄欣沂, 张福泰, 伍玮. 一种基于身份的环签密方案[J]. 电子学报. 2006, 34(2): 263-266.
HUANG X Y, ZHANG F T, WU W. An identity-based ring signcryption scheme[J]. Acta Electronica Sinica, 2006, 34(2): 263-266.

[19] 张串绒, 肖国镇. 一个可公开验证签密方案的密码分析和改进 [J]. 电子学报, 2006, 34(1): 177-179.
ZHANG C R, XIAO G Z. Cryptanalysis and improvement of a signcryption scheme with public verifiability[J]. Acta Electronica Sinica, 2006, 34(1): 177-179.

[20] YU G, MA X, SHEN Y, *et al*. Provable secure identity based generalized signcryption scheme[J]. Theoretical Computer Science, 2010, 411(40): 3614-3624.

[21] KUSHWAH P, LAL S. An efficient identity based generalized signcryption scheme[J]. Theoretical Computer Science, 2011, 412(45): 6382-6389.

[22] LI F, KHAN M K, ALGHATHBAR K, *et al*. Identity-based online/offline signcryption for low power devices[J]. Journal of Network and Computer Applications, 2012, 35(1): 340-347.

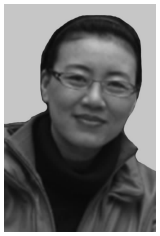
[23] ZHAO X, WANG X. An efficient identity-based signcryption from lattice[J]. International Journal of Security and Its Applications, 2014, 8(2):363-371.

[24] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[25] LYNN B. The pairing-based cryptography (PBC) library[EB/OL]. http://crypto.stanford.edu/pbc. 2012.

作者简介：

张宇（1984-），男，山东泰安人，武汉大学博士生，主要研究方向为网络安全。



杜瑞颖（1964-），女，河南新乡人，武汉大学教授、博士生导师，主要研究方向为网络安全、无线网络。

陈晶[通信作者]（1981-），男，湖北武汉人，武汉大学副教授、博士生导师，主要研究方向为网络安全、无线网络。E-mail: chenjing@whu.edu.cn。

侯健（1983-），男，山东泰安人，总参陆航研究所工程师，主要研究方向为计算机仿真。

周庆（1964-），男，江苏泰兴人，信息保障技术重点实验室高级工程师，主要研究方向为信息安全技术。

王文武（1991-），男，湖北石首人，武汉大学硕士生，主要研究方向为网络安全。