新的基于 Shim 签名的可验证加密签名方案

谷利泽[①] 孙艳宾*[①] 卿斯汉[②] 郑世慧[①] 杨义先[①]
[①](北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)
[②](北京大学软件与微电子学院 北京 102600)

摘 要：该文利用 Shim 基于身份的数字签名方案，提出了一个新的基于身份的可验证加密签名方案。作为设计公平交换协议的基本模块，该方案没有使用零知识证明系统提供验证，有效地避免了大量运算。与已有基于身份的可验证加密签名方案相比，该方案效率较高。安全性分析表明，在假设 CDH 问题是难解的情况下，该方案在随机预言模型中是可证安全的。

关键词：基于身份的签名；可验证加密签名；随机预言模型；可证安全性；双线性对
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2011)06-1271-06
DOI: 10.3724/SP.J.1146.2010.01104

New Verifiably Encrypted Signature Scheme Based on Shim's Signature

Gu Li-ze[①] Sun Yan-bin[①] Qing Si-han[②] Zheng Shi-hui[①] Yang Yi-xian[①]
[①](*Information Security Center*, *State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
[②](*School of Software and Microelectronics*, *Peking University*, *Beijing* 102600, *China*)

Abstract: Utilizing the Shim's identity-based signature scheme, a new identity-based verifiably encrypted signature scheme is proposed. As a building block of the fair exchange protocol, this approach does not use any zero-knowledge proofs to provide verifiability, it avoids most of the costly computations. Compared to the previous identity-based verifiably encrypted signature schemes, the proposed scheme is more efficiency. The performance analysis results show that the scheme is provably secure in the random oracle model under the CDH problem assumption.

Key words: Identity-based signature; Verifiably Encrypted Signature (VES); Random oracle model; Provably secure; Bilinear pairings

1 引言

Asokan 等人[1]提出了可验证加密签名(Verifiably Encrypted Signature, VES) 方案的概念，其中包括 3 个参与者：签名者、验证者以及仲裁者。作为设计公平交换协议的基本模块，VES 的核心思想是：签名者向验证者发送利用仲裁者公钥加密过的签名，验证者可以验证加密签名的有效性，但在没有签名者或仲裁者帮助的情况下验证者得不到普通签名；当争议发生时，仲裁者可从 VES 中恢复出签名者的普通签名。此后，这种 VES 思想[1]在文献[2,3]中得到了推广，然而由于在其交换过程中引入了复杂的交互零知识证明系统，效率较低。

为了提高效率，Boneh 等人[4]基于聚合签名的思想提出了第 1 个非交互的可验证加密签名方案。该方案在随机预言模型中是可证安全的，且无需交互零知识证明系统。此后，构造非交互的可验证加密签名受到广泛关注[5−11]。

基于身份的密码体制[12]无需公钥证书的管理与鉴别，相对 PKI/CA 技术，在应用中带来了极大的便利。Zhang 等人[8]建立了基于身份的优化公平协议的安全模型，同时，提出了一个在随机预言模型中可证安全的基于身份的可验证加密签名方案。利用此方案，文献[8]设计了一个高效的基于身份的公平交换协议。

利用 Hess[13]的基于身份的签名方案，Gu 等人[9]提出了另外一个基于身份的可验证加密签名方案，与文献[8]中方案不同的是此方案中仲裁者的公钥也是基于身份的。文献[9]对其方案进行了证明，声称其方案在随机预言模型中是可证安全的。然而，

2010-10-15 收到，2010-12-22 改回
国家自然科学基金(60970135，90718001)和国家 973 计划项目(2007CB310704)资助课题
*通信作者：孙艳宾 ybsun@fomail.com

文献[10]和文献[14]分别指出文献[9]方案是不安全的，同时文献[10]利用 Hess 的基于身份的签名方案给出了一个改进的可验证加密签名方案。2007 年，Kwon 等人[11]利用 Hess 的基于身份的签名方案设计一个新的可证安全的基于身份的可验证加密签名方案，效率优于文献[9,10]中的方案。

最近，Shim[15]提出了一个简洁高效的基于身份的签名方案(简记为 Shim 签名方案)，且可用于构造基于身份的聚合签名算法[4]。本文利用 Shim 签名方案构造了一个简洁高效的基于身份的可验证加密签名方案。该方案中，用户与仲裁者之间无需进行特殊注册，也无需引入交互零知识证明系统提供验证，当争议发生时才需仲裁者的介入。作为公平交换协议的基本模块，与类似方案相比，具有较高的效率。根据可验证加密签名的安全模型，我们在随机预言模型中对新方案进行了证明，假设 CDH 问题困难的情况下，新方案是可证安全的。

2 基础知识

2.1 双线性对及相关定义

设 G_1,G_2 分别具有相同素数阶 q 的加法和乘法循环群，P 是 G_1 的生成元。假设离散对数问题在 G_1 和 G_2 上是难解的。称具有下列性质的映射 $e:G_1\times G_1\to G_2$ 为双线性对：

(1)双线性性：对任意的 $P,Q\in G_1$ 和 $a,b\in Z_q$ 有 $e(aP,bQ)=e(P,Q)^{ab}$；

(2)非退化性：存在元素 $P,Q\in G_1$ 使得 $e(P,Q)\neq 1$；

(3)可计算性：存在有效算法可计算 $e(P,Q)$，对任意 $P,Q\in G_1$。

2.2 CDH 问题

定义1 CDH(Computational Diffie-Hellman)问题 设 P 是 G_1 的生成元，给定 $aP,bP\in G_1$ ($\forall a,b\in Z_q^*$)，计算 abP。

2.3 基于身份的可验证加密签名模型

基于身份的可验证加密签名方案的参与者包括：签名者、验证者以及仲裁者。

定义 2 一个基于身份的可验证加密签名方案包括 7 个多项式时间算法：参数设定(Setup)、密钥提取(Extract)、签名(Sign)、验证(Verify)、可验证加密签名(VES-Sign)、可验证加密签名验证(VES-Verify)以及仲裁算法(Adjudication)。算法的具体描述如下：

参数设定(Setup) 系统参数 param，PKG 的会话密钥 s 和公钥 P_{pub}，仲裁者(TTP)的私钥和公钥对 $(x_{\text{Adj}},P_{\text{Adj}})$，公布 P_{pub} 与 P_{Adj}。这里 TTP 与 KGC 不同。

密钥提取(Extract) 给定用户身份 ID，KGC 利用用户身份和会话密钥 s 计算用户私钥 S_{ID}，并发送给用户。

签名算法(Sign) 给定消息 m，用户私钥 S_{ID}，签名者输出普通签名 $V=\text{Sign}(S_{\text{ID}},m)$。

验证算法(Verify) 验证算法 $\text{Verify}(m,V,\text{ID})$ 以消息 m，签名 V 以及用户身份 ID 为输入，输出 1(接收)或 0(拒绝)。

可验证加密签名算法(VES-Sign) 给定消息 m，用户私钥 S_{ID} 以及 TTP 公钥 P_{Adj}，签名者输出可验证加密签名 $W=\text{VES-Sign}(S_{\text{ID}},P_{\text{Adj}},m)$。

可验证加密签名验证算法(VES-Verify) 验证算法 $\text{VES-Verify}(m,W,\text{ID},P_{\text{Adj}})$ 以消息 m，可验证加密签名 W，用户身份 ID 以及 TTP 公钥 P_{Adj} 为输入，输出 1(接受)或 0(拒绝)。

仲裁算法(Adjudication) 当签名者拒绝公开签名给验证者时，TTP 执行此算法，从 W 中恢复出签名者的普通签名 V。此时 $\text{Adj}(m,W,\text{ID},x_{\text{Adj}})$ 输出关于身份 ID 与消息 m 的有效签名。

在此可验证加密签名模型中，仲裁者除了其密钥之外，无需存储其他相关内容，且用户与仲裁者之间无需进行密钥认证。

2.4 基于身份的可验证加密签名安全模型

Dodis 等人[16]提出了关于 VES 方案的一般安全模型，要求 VES 方案是抗签名者、验证者以及仲裁者攻击安全的。文献[8]，文献[9]与文献[11]基于此安全模型分析了各自方案的安全性。我们把模拟 VES 方案密钥提取、可验证加密签名算法以及仲裁算法的随机预言分别记作 O_{Ext}，$O_{\text{VES-Sign}}$ 与 O_{Adj}，k 为安全参数，PPT 为概率多项式时间。具体模型如下：

抗签名者攻击 要求签名者产生的有效可验证加密签名，诚实的仲裁者能从中提取出签名者的签名。也就是说，在随机预言模型中任意 PPT 敌手 $\mathcal{A}$ 在进行以下模拟试验时，成功概率是可以忽略的，即

$$\text{Setup}(1^k)\to(\text{param},x_{\text{Adj}},P_{\text{Adj}})$$

$$(m,W,\text{ID})\leftarrow\mathcal{A}^{O_{\text{Adj}},O_{\text{Ext}}}(\text{param},P_{\text{Adj}})$$

$$V\leftarrow\text{Res}(m,W,\text{ID},x_{\text{Adj}})$$

$$\text{Success of }\mathcal{A}=[\text{VES-Verify}(m,W,\text{ID},P_{\text{Adj}})=1,\text{Verify}(m,V,\text{ID})=0]$$

抗验证者攻击 验证者得到签名者的有效 VES 后，在没有签名者和仲裁者的帮助下，无法从 VES 中恢复出普通签名。也就是说，在随机预言模型中任意 PPT 敌手 $\mathcal{A}$ 在进行以下模拟实验时，成功概率是可以忽略的，即

$$\text{Setup}(1^k)\rightarrow(\text{param},x_{\text{Adj}},P_{\text{Adj}})$$

$$(m,V,\text{ID})\leftarrow\mathcal{A}^{O_{\text{Ext}},O_{\text{VES-Sign}},O_{\text{Adj}}}(\text{param},P_{\text{Adj}})$$

$$\text{Success of }\mathcal{A}=[\text{Verify}(m,V,\text{ID})=1,$$

$$m\notin\text{Query}(\mathcal{A},O_{\text{Adj}}),\text{ID}\notin\text{Query}(\mathcal{A},O_{\text{Ext}})]$$

其中 $\text{Query}(\mathcal{A},O_{\text{Adj}})$ 与 $\text{Query}(\mathcal{A},O_{\text{Ext}})$ 分别表示询问 O_{Adj} 与 O_{Ext} 预言组成的集合。

抗仲裁者攻击　仲裁者在没有得到签名者关于消息 m 的可验证加密签名时，无法生成关于消息 m 的一般签名。也就是说，在随机预言模型中任意 PPT 敌手 $\mathcal{A}$ 在进行以下模拟实验时，成功概率是可以忽略的，即

$$\text{Setup}(1^k)\rightarrow(\text{param},x^*_{\text{Adj}},P_{\text{Adj}})$$

$$(m,V,\text{ID})\leftarrow\mathcal{A}^{O_{\text{VES-Sign}}}(x^*_{\text{Adj}},\text{param},P_{\text{Adj}})$$

$$\text{Success of }\mathcal{A}=[\text{Verify}(m,V,\text{ID})=1,$$

$$m\notin\text{Query}(\mathcal{A},O_{\text{VES-Sign}})]$$

其中 $\text{Query}(\mathcal{A},O_{\text{VES-Sign}})$ 表示 $\mathcal{A}$ 询问 $O_{\text{VES-Sign}}$ 预言组成的集合。

定义 3　如果基于身份的可验证加密签名是抗签名者、验证者以及仲裁者攻击安全的，则可验证加密签名方案是安全的。

3　基于身份的可验证加密签名方案

本文中基于 Shim 签名的可验证加密签名方案包括 7 个算法：参数设定(Setup)、密钥提取(Extract)、签名(Sign)、验证(Verify)、可验证加密签名(VES-Sign)、可验证加密签名验证(VES-Verify)以及仲裁算法(Adjudication)，详细过程如下：

参数设定　给定 (G_1,G_2,e,q,P)，KGC 随机选择密钥 $s\in Z_q^*$，令 $P_{\text{pub}}=sP$，选择哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\rightarrow Z_q^*$。仲裁者随机选择私钥 $x_{\text{Adj}}\in Z_q^*$，计算公钥 $P_{\text{Adj}}=x_{\text{Adj}}P$。系统参数为 $\text{param}=\{G_1,G_2,e,q,P,P_{\text{pub}},H_1,H_2\}$，其中 s 为会话密钥，x_{Adj} 为仲裁者的密钥。

密钥提取　给定用户身份 $\text{ID}\in(0,1)^*$，计算 $Q_{\text{ID}}=H_1(\text{ID}_{\text{ID}})\in G_1$，$S_{\text{ID}}=sQ_{\text{ID}}$。KGC 根据此算法生成用户的私钥 S_{ID}，并通过安全信道发送给用户。

签名算法　给定签名者密钥 S_{ID}，消息 $m\in\{0,1\}^*$，随机选择 $r_1,r_2\in Z_q^*$，并计算

$$C_1=r_1P,\ \ C_2=r_2P$$

$$h=H_2(\text{ID},m,C_1,C_2)$$

$$V=S_{\text{ID}}+hr_1P_{\text{pub}}$$

其中 (V,C_1,C_2) 为消息 m 的普通签名。

验证算法　给定消息 m 的普通签名 (V,C_1,C_2)，验证者首先计算 $Q_{\text{ID}}=H_1(\text{ID})$，$h=H_2(\text{ID},m,C_1,C_2,)$，然后验证等式：

$$e(P,V)=e(P_{\text{pub}},Q_{\text{ID}}+hC_1)$$

是否成立。如果成立，(V,C_1,C_2) 为有效的普通签名；否则，无效。

可验证加密签名算法　给定签名者密钥 S_{ID}，签名消息 m，仲裁者的公钥 P_{Adj}，随机选择 $r_1,r_2\in Z_q^*$，并计算

$$C_1=r_1P,\ \ C_2=r_2P$$

$$h=H_2(\text{ID},m,C_1,C_2)$$

$$V=S_{\text{ID}}+hr_1P_{\text{pub}}$$

$$W=V+r_2P_{\text{Adj}}$$

其中 (W,C_1,C_2) 为消息 m 的可验证加密签名。很容易看出，可验证加密签名算法是由签名算法增加 $W=V+r_2P_{\text{Adj}}$ 得到。

可验证加密签名验证算法　给定消息 m 的可验证加密签名 (W,C_1,C_2)，验证者首先计算 $Q_{\text{ID}}=H_1(\text{ID})$，$h=H_2(\text{ID},m,C_1,C_2)$，然后验证等式

$$e(P,W)=e(P_{\text{pub}},Q_{\text{ID}}+hC_1)e(P_{\text{Adj}},C_2)$$

是否成立。如果成立，(W,C_1,C_2) 为消息 m 的有效可验证加密签名；否则，无效。

仲裁算法　给定仲裁者私钥 x_{Adj}，消息 m 的有效可验证加密签名 (W,C_1,C_2)，仲裁者首先利用可验证加密签名验证算法验证其有效性。如果有效，仲裁者计算

$$V=W-x_{\text{Adj}}C_2$$

返回关于消息 m 的签名 (V,C_1,C_2) 给验证者。

其中，签名算法与验证算法是在 Shim 的基于身份的签名方案基础上增加参数 C_2 变形得到的，目的是用来进行 VES 的验证及仲裁。

4　安全性与效率分析

下面，我们将根据可验证加密签名方案的安全模型分析本文中新方案的安全性，同时我们对新方案的效率与已有的基于身份的可验证加密签名方案进行了对比。具体情况如下：

4.1 安全性分析

引理 1[15]　假设 CDH 问题是难解的，则 Shim 签名方案在随机预言模型中是可证安全的。

证明　略(详情请见文献[15]中定理 3.1)。

定理 1　假设 CDH 问题是难解的，普通签名方案在随机预言模型中是可证安全的。

证明　由于基于身份的可验证加密签名中的普通签名方案签名算法与验证算法是在 Shim 的基于身份的签名方案基础上增加参数 C_2 变形而来。因此，由引理 1 可知，普通签名方案在随机预言模型中是可证安全的。

定理 2 假设 CDH 问题是难解的，则基于身份的可验证加密签名在随机预言模型中是可证安全的。

证明 下面我们将分别说明本文的 VES 方案是抗签名者、验证者与仲裁者攻击。

抗签名者攻击 利用随机预言 O_{Adj} 与 O_{Ext}，一个恶意的签名者的目的是生成关于消息 m 的一个有效的可验证加密签名 (W,C_1,C_2)，而其他人无法从中提取出有效的一般签名 (V,C_1,C_2)。然而，对于任意满足：$e(P,W)=e(P_{\text{pub}},Q_{\text{ID}}+hC_1)e(C_2,P_{\text{Adj}})$ 的可验证加密签名 (W,C_1,C_2)，我们有 $V=W-x_{\text{Adj}}C_2$，且

$$\begin{aligned}e(P,V)&=e(P,W-x_{\text{Adj}}C_2)\\&=e(P_{\text{pub}},Q_{\text{ID}}+hC_1)e(C_2,P_{\text{Adj}})e(P,-x_{\text{Adj}}C_2)\\&=e(P_{\text{pub}},Q_{\text{ID}}+hC_1)e(C_2,P_{\text{Adj}})e(P_{\text{Adj}},-C_2)\\&=e(P_{\text{pub}},Q_{\text{ID}}+hC_1)\end{aligned}$$

其中 (V,C_1,C_2) 是由仲裁者从 (W,C_1,C_2) 中提取的关于消息 m 的有效普通签名，由定理 1 可知普通签名方案是可证安全的，因此签名者无法否认其签名。即 (V,C_1,C_2) 是签名者关于消息 m 的有效签名。事实上，O_{Adj} 对恶意签名者并无帮助，因为 O_{Adj} 询问得到的是 $x_{\text{Adj}}C_2$，而恶意签名者其实已经知道 $x_{\text{Adj}}C_2$，因为 $r_2P_{\text{Adj}}=r_2x_{\text{Adj}}P=x_{\text{Adj}}C_2$。

抗验证者攻击 如果一个恶意验证者 $\mathcal{A}$ 利用 $O_{\text{VES-Sign}}$，O_{Ext} 与 O_{Adj} 能够伪造关于身份 ID 的一个有效签名 (V,C_1,C_2)，其中与之对应的可验证加密签名 (W,C_1,C_2) 未进行 O_{Adj} 询问，ID 未进行 O_{Ext} 询问。则我们可以构造一个算法 $\mathcal{C}$ 能够利用 $\mathcal{A}$ 来求解 CDH 问题。给定算法 $\mathcal{C}$ 一个 CDH 问题的实例 (P,aP,bP)，目的是利用 $\mathcal{A}$ 输出 abP。

Setup：$\mathcal{C}$ 随机选择 $k_a\in Z_q^*$，令 $P_{\text{pub}}=k_aaP$ 为 KGC 的公钥，令 $P_{\text{Adj}}=aP$。发送相关系统参数 $(G_1,G_2,q,e,P,P_{\text{pub}},H_1,H_2)$ 给 $\mathcal{A}$。

O_{H_1} 询问：为了回答关于预言 O_{H_1} 的询问，$\mathcal{C}$ 建立一个列表，记作 H_1-List，其中元素形式为 $(\text{ID},Q_{\text{ID}},s_i)$。当 $\mathcal{A}$ 进行关于身份 ID 的预言 O_{H_1} 询问时，$\mathcal{C}$ 检查 H_1-List 是否定义。如果已定义，直接返回 Q_{ID}。如果没有，随机选择 $s_i\in Z_q^*$，返回 $Q_{\text{ID}}=H_1(\text{ID}_i)=s_iP$，并把 $(\text{ID},Q_{\text{ID}},s_i)$ 加入到 H_1-List。

O_{H_2} 询问：为了回答关于预言 O_{H_2} 的询问，$\mathcal{C}$ 建立一个列表，记作 H_2-List，其中元素形式为 (ID,m,C_1,C_2,h)。当 $\mathcal{A}$ 进行 (ID,m,C_1,C_2) 的预言 O_{H_2} 询问时，如果 H_2-List 存在 (ID,m,C_1,C_2,h)，则返回 h；如果 H_2-List 不存在，随机选择 $h\in Z_q^*$，返回 $H_2(\text{ID},m,C_1,C_2)=h$。然后把 (ID,m,C_1,C_2,h) 加入到 H_2-List 中。

O_{Ext} 询问：当 $\mathcal{A}$ 提交关于身份 ID 的 O_{Ext} 预言询问时，$\mathcal{C}$ 令 $S_{\text{ID}}=s_iP_{\text{pub}}=k_aa(s_iP)=k_aaQ_{\text{ID}}$，并返回 S_{ID} 作为 $\mathcal{A}$ 询问的结果。

$O_{\text{VES-Sign}}$ 询问：当 $\mathcal{A}$ 提交消息 m，签名者身份 ID 以及仲裁者的公钥 P_{Adj} 进行可验证加密签名预言 $O_{\text{VES-Sign}}$ 询问，$\mathcal{C}$ 首先进行如下计算：

(1)令 $C_2=bP$；

(2)随机选择 $h,\alpha\in Z_q$，计算 $C_1=\alpha P-h^{-1}Q_{\text{ID}}-k_a^{-1}h^{-1}C_2$；

(3)令 $H_2(\text{ID},m,C_1,C_2)=h$；

(4)计算 $W=\alpha hP_{\text{pub}}$；

返回 (W,C_1,C_2,m) (正确性验证略)作为可验证加密签名预言 $O_{\text{VES-Sign}}$ 询问的结果。

O_{Adj} 询问：当 $\mathcal{A}$ 提交关于消息 m，签名者身份 ID 以及仲裁者的公钥 P_{Adj} 的可验证加密签名 (W,C_1,C_2,m) 进行仲裁预言 O_{Adj} 询问时，$\mathcal{C}$ 进行如下计算：

(1)首先询问关于身份 ID_i 的预言 O_{Ext}，获得 Q_{ID}；

(2)随机选择 $\alpha\in Z_q$，并计算 $C_1=k_a^{-1}\alpha P$；

(3)令 $V=S_{\text{ID}}+h\alpha P_{\text{Adj}}$；

返回 (V,C_1,C_2) (正确性验证略)作为仲裁预言询问的输出结果。

输出：最后，$\mathcal{A}$ 在已知签名者身份 ID^* 以及仲裁者公钥 P_{Adj} 的情况下从可验证加密签名 (W^*,C_1^*,C_2,m^*) 中提取出签名 (V^*,C_1^*,C_2,m^*)，要求

(1)未提交 (W^*,C_1^*,C_2,m^*) 进行仲裁预言 O_{Adj} 询问；

(2)未提交 ID^* 进行过密钥提取预言 O_{Ext} 询问；

因此 $\mathcal{C}$ 可利用 (W^*,C_1^*,C_2,m^*) 与 (V^*,C_1^*,C_2,m^*) 计算出 abP 的值，其中有

$$e(W^*,P)=e(P_{\text{pub}},Q_{\text{ID}^*}+hC_1^*)e(C_2,P_{\text{Adj}})$$

$$e(V^*,P)=e(P_{\text{pub}},Q_{\text{ID}^*}+hC_1^*)$$

由以上两式可知

$e(W^*-V^*,P)=e(C_2,P_{\text{Adj}})=e(bP,aP)=e(abP,P)$，(这里 $C_2=bP$ 是由 $O_{\text{VES-Sign}}$ 询问中得到)从而可得 $abP=W^*-V^*$，得到了 CDH 问题实例 (P,aP,bP) 的一个解。

抗仲裁者攻击 如果恶意仲裁者 $\mathcal{A}$ 能利用随机预言 O_{Sign}，O_{H_2} 以及提取普通签名所用的私钥伪造一个消息 m 的普通签名 (V,C_1,C_2,m)，其中未进行预言 O_{Sign} 询问。那么我们可以构造一个伪造算法 $\mathcal{C}$ 利用 $\mathcal{A}$ 来伪造普通签名。

对于 $\mathcal{A}$ 的关于消息 m 的签名预言 O_{Sign} 询问，$\mathcal{C}$ 选择 $r_1,r_2,h\in Z_q^*$，计算 $C_1=r_1P-h^{-1}W$，$V=$

$r_1 \cdot h \cdot P_{\text{pub}}$，其中 $h = H_2(\text{ID}, m, C_1, C_2)$。$\mathcal{A}$ 接受 (V, C_1, C_2) 为一个有效签名。当 $\mathcal{A}$ 输出一个伪造的签名 (V^*, C_1^*, C_2^*, m^*)，m^* 并未进行 O_{Sign} 询问，则 $\mathcal{C}$ 可以输出相同的签名 (V^*, C_1^*, C_2^*) 给 $\mathcal{A}$。因此，如果 $\mathcal{A}$ 能够成功伪造签名，则 $\mathcal{C}$ 也能成功伪造签名。

由定理 1 可知，普通签名方案在随机预言模型中是可证安全的，因此假设 CDH 问题是难解的情况下，$\mathcal{A}$ 成功伪造普通签名的成功概率是可忽略的。

综上所述，根据定义 3，假设 CDH 问题是困难的，则利用 Shim 的基于身份的签名构造的基于身份的可验证加密签名在随机预言模型中是可证安全的。

4.2 效率分析

表 1 将本文中新方案的效率与文献[9–11]中的方案进行了对比。不失一般性，在对比中，我们仅考虑最耗时的双线性对运算(记作 $\hat{e}$)与次耗时的标量乘法运算(记作 M)，详细情况见表 1。

表 1 效率对比

	签名	验证	VES 签名	VES 验证	仲裁
文献[9]	$1\hat{e}+2\text{M}$	$2\hat{e}+1\text{M}$	$2\hat{e}+5\text{M}$	$3\hat{e}+1\text{M}$	$1\hat{e}+1\text{M}$
文献[10]	$1\hat{e}+2\text{M}$	$2\hat{e}+1\text{M}$	$2\hat{e}+4\text{M}$	$4\hat{e}+2\text{M}$	$1\hat{e}+1\text{M}$
文献[11]	$1\hat{e}+2\text{M}$	$2\hat{e}+1\text{M}$	$1\hat{e}+4\text{M}$	$3\hat{e}+1\text{M}$	$1\hat{e}+1\text{M}$
本文方案	3M	$2\hat{e}+1\text{M}$	4M	$3\hat{e}+1\text{M}$	1M

在表 1 的文献[9–11]中，$r = e(P,P)^{k_1} = e(P, k_1 P)$，计算量为 $1\hat{e}+1\text{M}$。从表 1 可以看出，本文提出的基于身份的可验证加密签名的效率优于文献[9–11]中的方案。

5 结论

构造优化的公平交换协议[8,16–20]一直是电子商务研究的方向，而可验证加密签名方案作为公平交换协议的基本模块已成为研究的重点。本文中利用 Shim 的基于身份的签名方案提出了一个基于身份的可验证加密签名方案。根据文献[8,9,11,16]中关于可验证加密签名方案的安全模型我们对本文的方案进行了安全性分析，在随机预言模型中，该方案可抗签名者、验证者以及仲裁者攻击。与文献[9–11]中的基于身份的可验证加密签名方案相比，本文提出的新方案效率优于前面的方案。

参 考 文 献

[1] Asokan N, Schunter M, and Waidner M. Optimistic protocols for fair exchange[C]. The 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, 1997: 7–17.

[2] Camenisch J and Damgard I B. Verifiable encryption, group encryption, and their applications to group signature and signature sharing schemes[C]. Advances in Cryptology: Proceedings of ASIACRYPT 2000, Kyoto, Japan, December 3–7, 2000, Vol. 1976: 331–345.

[3] Ateniese G. Verifiable encryption of digital signatures and applications [J]. *ACM Transactions on Information and System Security*, 2004, 7(1): 1–20.

[4] Boneh D, Gentry C, and Lynn B. Aggregate and verifiably encrypted signatures from bilinear maps [C]. Advances in Cryptology: Proceedings of EUROCRYPT 2003, Warsaw, Poland, May 4–8, 2003, Vol. 2656: 416–432.

[5] 辛向军, 李刚, 董庆宽, 肖国镇. 一个高效的随机化的可验证签名方案[J]. 电子学报, 2008, 36(7): 1378–1382.
Xin Xiang-jun, Li Gang, Dong Qing-kuan, and Xiao Guo-zhen. An efficient randomized verifiably encrypted signature scheme [J]. *Acta Electronica Sinica*, 2008, 36(7): 1378–1382.

[6] 杨浩淼, 孙世新, 徐继友. 一种无随机预言机的高效可验证加密签名方案[J]. 软件学报, 2009, 20(4): 1069–1076.
Yang Hao-miao, Sun Shi-xin, and Xu Ji-you. Efficient verifiably encrypted signature scheme without random oracles [J]. *Journal of Software*, 2009, 20(4): 1069–1076.

[7] Ruckert M and Schroder D. Security of verifiably encrypted signatures and a construction without random oracles [C]. The 3rd International Conference on Pairing-based Cryptography, Palo Alto, CA, USA, 2009, Vol. 5671: 17–34.

[8] Zhang Z F, Feng D G, and Xu J Y, *et al*.. Efficient ID-based optimistic fair exchange with provable security [C]. The 7th International Conference on Information and Communications Security, Beijing, China, December 10–13, 2005, Vol. 3783: 14–26.

[9] Gu C X and Zhu Y F. An ID-based verifiable encrypted signature scheme based on Hess's scheme [C]. The 1st SKLOIS Conference on Information Security and Cryptology, Beijing, China, December 15–17, 2005, Vol. 3822: 42–52.

[10] Zhang J H and Zou W. A robust verifiably encrypted signature scheme [C]. Proceedings of the EUC Workshops 2006, Seoul, Korea, August 1–4, 2006, Vol. 4097: 731–740.

[11] Kwon S and Lee S H. An efficient ID-based verifiably encrypted signature scheme based on Hess's scheme [C]. The

3rd International Conference: ISPEC 2007, Hong Kong, China, May 7–9, 2007, Vol. 4464: 93–104.

[12] Shamir A. Identity based cryptosystems and signature schemes[C]. Advances in Cryptology: Proceedings of CRYPTO 84, California, USA, August 19–22, 1984, Vol. 196: 47–53.

[13] Hess F. Efficient identity based signature schemes based on pairings [C]. The 9th Annual International Workshop on Selected Areas in Cryptography, Newfoundland, Canada, August 15–16, 2002, Vol. 2595: 310–324.

[14] 张振峰. 基于身份的可验证加密签名协议的安全性分析[J]. 计算机学报, 2006, 29(9): 1688–1693.
Zhang Zhen-feng. Cryptanalysis of an identity-based verifiably encrypted signature scheme[J]. *Chinese Journal of Computers*, 2006, 29(9): 1688–1693.

[15] Shim K A. An ID-based aggregate signature scheme with constant pairing computations [J]. *The Journal of Systems and Software*, 2010, 83(10): 1873–1880.

[16] Dodis Y and Reyzin L. Breaking and repairing optimistic fair exchange from PODC 2003 [C]. Proceedings of the 2003 ACM Workshop on Digital Rights Management 2003, Washington, DC, USA,October 27, 2003: 47–54.

[17] Shao Z H. Fair exchange protocol of signatures based on aggregate signatures [J]. *Computer Communications*, 2008, 31(10): 1961–1969.

[18] Shao Z H. Fair exchange protocol of Schnorr signatures with semi-trusted adjudicator [J]. *Computers and Electrical Engineering*, 2010, 36(6): 1035–1045.

[19] Sun Y B, Gu L Z, and Qing S H, *et al*.. Timeliness optimistic fair exchange protocol based on key-exposure-free chameleon hashing scheme [C]. The 12th International Conference on Advanced Communication Technology (ICACT2010), Gangwon-Do, Korea, February 7–10, 2010: 1560–1564.

[20] Sun Y B, Gu L Z, and Qing S H, *et al*.. New optimistic fair exchange protocol based on short signature [C]. The 2nd International Conference on Communication Software and Networks (ICCSN 2010), Singapore, February 26–28, 2010: 99–104.

谷利泽： 男，1965年生，副教授，研究方向为数字签名技术与应用.

孙艳宾： 男，1980 年生，博士生，研究方向为安全协议的设计与分析.

卿斯汉： 男，1939年生，研究员，博士生导师，研究领域为信息系统安全理论和技术.