

盲化的基于无证书的可验证加密签名方案

李艳红*, 高德智, 冯文文

(山东科技大学 信息科学与工程学院, 山东 青岛 266590)

(*通信作者电子邮箱 lyh880729@163.com)

摘要: 可验证加密签名方案的公平性完全由仲裁者中立问题决定, 这样就降低了交换签名的安全性。为了应对这种情况, 利用双线性对的性质, 结合无证书公钥密码体制与可验证加密数字签名, 设计了一种盲化的基于无证书的可验证加密签名方案, 方案中的仲裁者不能直接恢复原始签名, 从而加强了交换签名的安全性。在假设离散对数问题(DLP)和计算 Diffie-Hellman 问题(CDHP)难解的前提下, 该方案在随机预言模型中是可证安全的。

关键词: 无证书公钥密码体制; 可验证加密签名; 仲裁者; 双线性对; 随机预言模型

中图分类号: TP309 **文献标志码:** A

Blind and certificateless verifiably encrypted signature scheme

LI Yanhong*, GAO Dezhi, FENG Wenwen

(College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao Shandong 266510, China)

Abstract: The fairness of verifiably encrypted signature scheme is completely determined by the arbitrators neutral problem, which reduces the security of signature exchange. In order to deal with this issue, using the properties of bilinear pairings and combining with certificateless public key cryptography and verifiably encrypted signature, a blind verifiably encrypted signature was designed without certificate. The adjudicator in this scheme cannot restore the original signature directly, thereby the security of exchange signature protocols was enhanced. The proposed scheme was also provably secure in the random oracle module under Discrete Logarithm Problem (DLP) and Computational Differ-Hellman Problem (CDHP) assumption.

Key words: certificateless public key cryptography; verifiably encrypted signature; adjudicator; bilinear pairing; random oracle model

0 引言

无证书公钥密码体制于 2003 年由 Al-Riyami 等在文献[1]中首次提出, 在这种密码体制中, 用户的密钥由两个部分组成: 1) 第一部分私钥是由可信第三方密钥生成中心(Key Generation Center, KGC)生成的, KGC 使用主密钥为用户生成基于身份的部分私钥, 并通过安全信道发送给用户; 2) 用户使用第一部分私钥和自己生成的秘密值独立地生成自己的公钥和私钥。这样不仅能有效地克服传统公钥密码学中证书存在的问题, 而且消除了基于身份密码学中密钥托管的问题。无证书公钥密码体制受到密码学界的广泛关注, 例如文献[2-3]中提出的有关无证书的签名方案。

在生活中, 随着电子商务的广泛应用, 互不信任的双方如何保证公平地交换信息已经成为关键的问题。可验证加密签名(Verifiably Encrypted Signature, VES)为解决公平性提供了可能^[4]。VES 一般涉及到 3 个参与者: 签名者 A、验证者 B 和仲裁者 C。这类协议的基本思想是签名者 A 根据对某一消息的普通签名, 利用仲裁者的公钥进行加密产生可验证的加密签名并发送给验证者; 验证者接收到可验证加密签名后, 就开始验证签名是否有效, 如果有效交换信息成功, 否则就将自己的签名和收到的可验证加密签名一并发送给仲裁者, 请求仲裁, 除此之外, 验证者得不到任何消息。一般一个可验证的加密签名应该满足可验证性和可恢复性。可验证性是指任何验证者能够检验可验证加密签名的确是签名者对该消息的原始

签名进行的加密, 但是验证者不能从中提取出原始签名; 而可恢复性则意味着可验证加密签名能够向验证者保证指定的仲裁者能够从中取出原始的签名。根据可验证加密签名的特点, 一些相关方案被相继提出: Boneh 等^[5]提出第一个非交互的可验证加密签名方案, 该方案在随机预言模型下是可证明安全的, 而且也是第一个无需在用户与仲裁者之间进行特殊注册, 无须零知识证明的方案。利用 Hess^[6]的基于身份的签名方案, Gu 等^[7]提出了另外一种基于身份的可验证加密签名方案, 其突出的优点是: 不仅签名者的公钥是基于身份的, 而且仲裁者的公钥也是基于身份的。文献[8]对基于身份的可验证加密签名方案进行安全性分析, 分析结果显示验证者可以验证恶意签名的有效性, 但是指定的仲裁者不能把恶意签名转化成该签名者的原始签名。此方案容易受到合谋攻击, 也就是说, 恶意验证者在接受到一个签名者的可验证加密之后, 与他人合谋可以得到该签名的原始签名。

可验证加密签名在电子合同、电子支付等电子商务领域有着广泛的应用。但是可验证加密签名的交换协议^[9]有个不足之处, 在签名者与验证者交换签名时, 只要仲裁者介入协议, 就知道了签名者与验证者的交换内容, 尤其是不允许他人知道的机密性文件, 这时就需要仲裁者间接恢复出消息的可验证加密签名方案。

鉴于上述原因, 本文在文献[10-13]的基础上, 把无证书公钥密码体制和可验证加密签名方案结合起来, 提出一种新的无证书可验证加密签名方案, 该方案不仅拥有无证书公

收稿日期: 2013-06-25; 修回日期: 2013-08-26。 基金项目: 青岛市科技发展计划项目(11-2-4-6-(1)-jch)。

作者简介: 李艳红(1988-), 女, 山东济宁人, 硕士研究生, 主要研究方向: 密码学、信息安全; 高德智(1963-), 男, 新疆昌吉人, 教授, 博士, 主要研究方向: 应用泛函分析、密码学; 冯文文(1987-), 女, 山东聊城人, 硕士研究生, 主要研究方向: 密码学、信息安全。

钥密码体制和可验证加密签名方案的优点,而且计算效率高,在实际生活中具有重要的应用价值。

1 数学预备知识

1.1 双线性对

双线性对:令 G_1, G_2 是阶为素数 q 的加法群和乘法群, P 是 G_1 的生成元,令 $e: G_1 \times G_1 \rightarrow G_2$ 是满足下列条件的双线性映射:

- 1) 双线性性:对于任意的 $P, Q \in G_1, a, b \in \mathbb{Z}_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$;
- 2) 非退化性:存在 $P, Q \in G_1$, 满足 $e(P, Q) \neq 1$;
- 3) 可计算性:对于任意的 $P, Q \in G_1$, 存在一个有效的算法计算 $e(P, Q)$ 。

在群组 (G_1, G_2) 上,可以定义以下几个密码学问题。

1.2 离散对数问题

离散对数问题 (Discrete Logarithm Problem, DLP): 设 P 和 Q 是群 G_1 中的两个元素,要找到某个正数 $n \in \mathbb{Z}_q^*$, 使之满足 $Q = nP$ 。

1.3 CDH 问题

计算 Diffie-Hellman 问题 (Computing Diffie-Hellman Problem, CDHP): 对于未知的 $a, b \in \mathbb{Z}_q^*$, $P \in G_1$, 已知 (P, aP, bP) , 计算 abP , 如果离散对数可解, CDH 问题可解, 反之不一定成立。

2 新的无证书的可验证加密签名方案

本文结合一个高效的可验证加密签名方案,提出了一种新的无证书的可验证加密签名方案,该方案主要有以下10个步骤:系统参数生成,部分私钥生成,密钥生成,签订协议,普通签名生成,普通签名验证,可验证加密签名生成,可验证加密签名验证,仲裁以及盲解密。

1) 系统参数生成算法。系统生成主密钥和系统公钥,并公开系统参数,保存主密钥。

KGC 选取 G_1 与 G_2 分别是阶为 q 的加法循环群和乘法循环群,令 P 为 G_1 的生成元,设双线性对 $e: G_1 \times G_1 \rightarrow G_2$, 定义哈希函数 $H_1: \{0,1\}^* \rightarrow G_1, H_2: \{0,1\}^* \times G_1^* \times G_1^* \rightarrow \mathbb{Z}_q^*, H_3: G_1 \times G_1 \rightarrow \mathbb{Z}_q^*$ 。KGC 随机选取系统主密钥 $s \in \mathbb{Z}_q^*$, 计算系统公钥 $P_{pub} = sP$, 则公开系统参数: $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$, 保存系统的主密钥 s 。

2) 部分私钥生成算法。在部分私钥提取阶段 PKG 生成部分私钥。

当给定签名者 A 的身份信息 $ID_A \in \{0,1\}^*$, PKG 计算局部私钥 $psk_A = sQ_A = sH_1(ID_A)$, 然后通过安全通道发送给签名人 A 。

3) 密钥生成算法。在密钥生成阶段生成签名者 A 、验证者 B 、仲裁者 C 的公钥以及 A 的另一部分私钥。

签名者 A 、验证者 B 、仲裁者 C 分别随机选择 $x_A, x_B, x_C \in \mathbb{Z}_q^*$ 作为各自的秘密值, 计算公钥, $PK_A = x_AP, PK_B = x_BP, PK_C = x_CP$, 则 A 的私钥为 (psk_A, x_A) 。

4) 签订协议。在可验证加密签名方案中,一般假设仲裁者是可信的第三方,但在现实生活中第三方并不可信,这样当交换信息双方发生冲突时,仲裁者可能拒绝恢复消息,就打破了交换的公平性。为了避免此类事情的发生,仲裁者签订一个协议,如果仲裁时,没有恢复签名则追究其责任。这样就对仲裁者强加了约束条件,使得仲裁者有责任恢复原始签名。

将签名者 A 的 Q_A 和消息 m 传送给仲裁者 C , 仲裁者签订

协议 $M \in \{0,1\}^*$, 协议内容包括: 仲裁者 C 在交换双方发生冲突时,一定按照协议完成恢复原始签名的任务。计算如下: $U_C = x_C H_1(M)$, 然后再计算 $W = U_C + H_1(mQ_A)$, 将 (U_C, M) 通过安全通道发送给签名者 A ; 签名者 A 收到 (U_C, M) 后, 计算 $U_C = W - H_1(mQ_A)$ 恢复出协议签名内容。通过计算 $e(U_C, P) = e(H_1(M), PK_C)$ 验证协议的有效性, 如果正确接受协议内容; 否则结束交换信息。

5) 盲签名生成算法。在盲签名阶段, 签名者 A 首先对消息 m 进行签名, 然后将签名盲化。

输入消息 $m \in \{0,1\}^*$, 签名者 A 随机选择 $r_1, r_2 \in \mathbb{Z}_q^*$, 利用私钥 (psk_A, x_A) 进行如下计算: $R_1 = r_1 P, R_2 = r_2 P, h = H_2(m \| ID_A, R_1, R_2), V = (x_A^2 + r_2 h x_A) P + psk_A$, 得到消息 m 的原始签名 $\sigma = (R_1, R_2, V)$ 。为了消息的安全, 采取如下措施: 计算 $V' = V + r_2 PK_B$, 得到盲化的普通签名 $\sigma' = (R_1, R_2, V')$ 。

6) 盲签名的验证算法。在验证阶段, 验证者得到签名者的签名后, 验证该签名是否符合验证等式, 如果符合则接受为有效签名; 否则结束交换信息过程。

输入签名者 A 盲化的普通签名 $\sigma' = (R_1, R_2, V')$ 后, 利用 A, B 的公钥 PK_A, PK_B 进行如下验证: 首先计算 $Q_A = H_1(ID_A), h = H_2(m \| ID_A, R_1, R_2)$, 然后验证等式: $e(V', P) = e(Q_A, P_{pub}) e(PK_A, hR_2 + PK_A) e(PK_B, R_2)$ 是否成立, 如果成立, 则为有效的签名; 否则无效。

7) 可验证加密签名算法。在可验证加密签名阶段, 签名者 A 利用盲化的普通签名和仲裁者签订的协议生成相应的可验证加密签名并提供给验证者 B , 用来交换验证者 B 对消息 m 的签名。

输入消息 m 及 C 的公钥, 则 $\delta = H_3(H_1(M), U_C), h = H_2(m \| ID_A, R_1, R_2), V_1 = V' + r_1 PK_C \delta$; 输出 $\sigma_1 = (R_1, R_2, V_1)$ 作为对 m 无证书的可验证加密签名。

8) 可验证加密签名验证算法。给定消息 m , 无证书的可验证加密签名 $\sigma_1 = (R_1, R_2, V_1)$, 以及 A, B, C 的公钥 PK_A, PK_B, PK_C 后, 验证者利用上述信息进行如下计算: $\delta = H_3(H_1(M), U_C), h = H_2(m \| ID_A, R_1, R_2)$, 当且仅当 $e(V_1, P) = z_A e(Q_A, P_{pub}) e(R_1, PK_C \delta) e(R_2, hPK_A + PK_B)$ 成立, 其中 $z_A = e(PK_A, PK_A)$, 如果成立, 则 $\sigma_1 = (R_1, R_2, V_1)$ 为消息 m 的有效无证书的可验证加密签名, 验证者 B 与签名者 A 交换签名; 否则, 无效。

9) 仲裁者算法。在仲裁阶段, 验证者 B 首先对可验证加密签名进行验证, 如果可验证加密签名可以通过验证, 则将自己对消息的签名发送给签名者; 否则验证者将自己的签名和收到的可验证加密签名一并发送到仲裁处, 请求仲裁。

给定仲裁者 C 消息 m 以及 $\sigma_1 = (R_1, R_2, V_1)$ 后, 首先仲裁者利用自己的私钥 x_C , 以及协议内容 M , 计算 $U_C = x_C H_1(M), \delta = H_3(H_1(M), U_C)$, C 恢复消息如下: $V_2 = V_1 - x_C R_1 \delta$; 然后返回关于消息 m 的签名 $\sigma_2 = (R_1, R_2, V_2)$ 给验证者 B 。

10) 盲解密算法。在盲解密阶段, 验证者 B 收到仲裁处的结果, 利用自己的私钥恢复出原始签名。

B 收到 $\sigma_2 = (R_1, R_2, V_2)$ 后, 接着盲解密 $V = V_2 - x_B R_2$, 得到消息 m 的原始签名 $\sigma = (R_1, R_2, V)$ 。

3 安全性分析

以下从无证书的可验证加密签名方案的安全性需求的几个方面证明其安全性。

1) 正确性。

首先验证等式 $e(V', P) = e(Q_A, P_{\text{pub}})e(PK_A, hR_2 + PK_A)e(PK_B, R_2)$ 。

$$\begin{aligned} e(V', P) &= e((x_A^2 + r_2 hx_A)P + psk_A + r_2 PK_B, P) = \\ &= e(x_A^2 P + r_2 hx_A P + psk_A + r_2 PK_B, P) = \\ &= e(x_A P + hR_2, x_A P)e(psk_A, P)e(PK_B, r_2 P) = \\ &= e(PK_A + hR_2, PK_A)e(Q_A, P_{\text{pub}})e(PK_B, R_2) \end{aligned}$$

所以 $e(V', P) = e(Q_A, P_{\text{pub}})e(PK_A, PK_A + hR_2)e(PK_B, R_2)$ 成立; 然后再验证等式 $e(V_1, P) = z_A e(Q_A, P_{\text{pub}})e(R_1, PK_C \delta) e(R_2, hPK_A + PK_B)$ 。

由于

$$\begin{aligned} e(V_1, P) &= \\ &= e((x_A^2 + r_2 hx_A)P + psk_A + r_2 PK_B + r_1 PK_C \delta, P) = \\ &= e(x_A^2 P, P)e(sQ_A, P)e(r_2 hx_A P, P) \\ &= e(r_2 PK_B, P)e(r_1 PK_C \delta, P) = \\ &= e(PK_A, PK_A)e(Q_A, P_{\text{pub}})e(hPK_A, R_2) \\ &= e(PK_B, R_2)e(PK_C \delta, R_1) = \\ &= z_A e(Q_A, P_{\text{pub}})e(R_2, hPK_A + PK_B)e(R_1, PK_C \delta) \end{aligned}$$

所以 $e(V_1, P) = z_A e(Q_A, P_{\text{pub}})e(R_2, hPK_A + PK_B)e(R_1, PK_C \delta)$ 成立, 其中 $z_A = (PK_A, PK_A)$ 。

2) 可验证性和可恢复性。

可验证性: 如果 C 是不可信的仲裁者, 仲裁时如果出现错误或者伪造一个假冒的, 而验证者只需要验证解密的签名 $\sigma' = (R_1, R_2, V')$ 是否满足等式 $e(V_2, P) = z_A e(Q_A, P_{\text{pub}})e(hPK_A + PK_B, R_2)$, 所以仲裁者 C 是可验证的。

可恢复性: 上面讨论可以断定 C 能够进行解密, 且如果 B 得到 $\sigma_2 = (R_1, R_2, V_2)$ 后, 就可以恢复 A 的原始签名, 因此恢复性显然成立。

3) 不可伪造性。

定理 1 在 CDH 问题难解的前提下, 盲化的基于无证书的可验证加密签名方案在随机预言模型中是可证安全的。

证明 下面从两方面证明本文方案是抵抗验证者和仲裁者攻击的。

1) 抗验证者攻击。如果恶意的验证者 B' 通过仲裁询问、密钥询问和可验证加密签名询问 (O_{Adj} , O_{Ext} , $O_{\text{VES-Sign}}$), 伪造一个普通的签名 (R_1, R_2, V) , 对应的可验证加密签名为 (R_1, R_2, V_1) 。现在构造一个算法 D 且通过恶意的验证者 B' 来求解 CDH 问题。给定一个 CDH 问题的实例 (P, aP, bP) , 目的是利用 B' 计算出 abP 。

参数设置: 令 $X = aP, Y = bP, D$ 随机选择 $\alpha \in \mathbb{Z}_q^*$, 设定 $P_{\text{pub}} = X$ 以及 $PK_C = \alpha X$ 发送相关参数 $(G_1, G_2, q, e, P, P_{\text{pub}}, PK_C, H_1, H_2, H_3)$ 给 B' 。 B' 进行对随机预言询问, B' 维护 L_1, L_2, L_3 这三张列表, 在以下询问中, 假设每次以同样的 ID_A^* 询问, D 回答询问如下:

H_1 询问 (O_{H_1}): 为了回答关于预言 O_{H_1} 的询问, D 建立列表 $H_1\text{-list}$, 其中元素形式为 $(ID_A^*, H_1(ID_A^*), \beta, c)$, 当 B' 进行关于身份 ID_A^* 的预言 O_{H_1} 询问时, D 作如下响应: D 随机选择 $c \in \{0, 1\}^*$, $\beta \in \mathbb{Z}_q^*$, 若 $c = 0$, D 计算 $Q_A = \beta Y$; 若 $c = 1$, D 计算 $Q_A = H_1(ID_A^*) = \beta P$ 。将 $(ID_A^*, H_1(ID_A^*), \beta, c)$ 保存到 $H_1\text{-list}$ 中, 并将 Q_A 返回给 B' 。

H_2 询问 O_{H_2} : 为了回答关于预言 O_{H_2} 的询问, D 建立列表 $H_2\text{-list}$, 其中元素形式为 $(m \| ID_A^*, R_1, R_2, h)$, 当 B' 进行 $(m \| ID_A^*, R_1, R_2)$ 的预言 O_{H_2} 询问时, 如果 $H_2\text{-list}$ 中存在 $(m \| ID_A^*, R_1, R_2, h)$, 则返回 h ; 如果不存在, 随机选择 $h \in$

\mathbb{Z}_q^* , 返回 $H_2(m \| ID_A^*, R_1, R_2) = h$, 然后将 $(ID_A^* \| m, R_1, R_2, h)$ 加入 $H_2\text{-list}$ 中。

O_{H_3} 询问: 为了回答关于预言 O_{H_3} 的询问, D 建立列表 $H_3\text{-list}$, 输入 $(H_1(M), U_C)$ 询问 O_{H_3} 时, 如果 $(H_1(M), U_C, \lambda)$ 在 $H_3\text{-list}$ 中, 返回 λ ; 否则随机选择 $\lambda \in \mathbb{Z}_q^*$; 将 $(H_1(M), U_C, \lambda)$ 添加到 $H_3\text{-list}$ 中, 返回 $H_3(H_1(M), U_C) = \lambda$ 。

密钥询问 (O_{Ext}): 当 B' 提交关于身份 ID_A^* 的 O_{Ext} 预言询问时, D 首先在 $H_1\text{-list}$ 列表中查找相应的 $(ID_A^*, H_1(ID_A^*), \beta, c)$, 若 $c = 0$, D 失败终止; 否则 D 利用 $H_1\text{-list}$ 中的 $(ID_A^*, H_1(ID_A^*), \beta, c)$, 计算 $psk_A = \beta P_{\text{pub}} = \beta(aP) = a(\beta P) = aQ_A$, 并将 psk_A 返回给 B' 。

当 B' 提交关于 ID_i 的秘密值预言询问时, D 判断是否有 $ID_i = ID_A^*$ 成立, 如果 $ID_i \neq ID_A^*$, D 随机选择 $x_A \in \mathbb{Z}_q^*$, 将其发送给 B' 。

可验证加密签名询问 ($O_{\text{VES-Sign}}$): 当 B' 提交消息 m , 签名者身份 ID_A^* 以及仲裁者的公钥 PK_C , 验证者自己的公钥 PK_B 时, 进行可验证加密签名预言 $O_{\text{VES-Sign}}$ 询问时, D 首先在 $H_1\text{-list}$ 查询得到 $(ID_A^*, H_1(ID_A^*), \beta, c)$, 然后 D 进行如下计算: 令 $R_2 = bP$, 随机选择 $r_1, r_2 \in \mathbb{Z}_q^*$, 计算 $R_1 = r_2 P - h^{-1} \alpha R_2 \lambda - h^{-1} Q_A$, 令 $H_3(H_1(M), U_C) = \lambda, H_2(m \| ID_A^*, R_1, R_2) = h$, 最后计算 $V_1 = V' + r_2 PK_B + r_1 PK_C \lambda$, 并将 (V_1, R_1, R_2) 作为回应返回给 B' 。

仲裁者询问 (O_{Adj}): 当 B' 提交关于消息 m , 签名者的身份 ID_A^* 以及仲裁者公钥 PK_C 的可验证加密签名 (V_1, R_1, R_2) 进行仲裁者预言 O_{Adj} 询问时, D 进行如下计算: 首先询问 O_{Ext} 得到 psk_A, x_A , 然后随机选择 $\omega \in \mathbb{Z}_q^*$, 并计算 $R_1 = \alpha \omega P$, 令 $V = psk_A + (x_A^2 + r_2 hx_A)P$ 。

输出: 最后 B' 在已知签名者身份 ID_A^* 以及仲裁者公钥 PK_C 的情况下, 从可验证加密签名 (V_1, R_1, R_2) 中提取出签名 $(ID_A^*, V, R_1, R_2, h, m)$, 同时满足首先 B' 进行 O_{Ext} 询问时, D 不终止; 其次未提交 (V_1, R_1, R_2) 进行仲裁预言 O_{Adj} 询问, 最后未提交 ID_A^* 进行密钥提取预言 O_{Ext} 询问。

利用分叉引理在多项式时间内, D 利用 B' 可以得到另一个普通签名 $(ID_A^*, V^*, R_1, R_2, h', m)$, 则

$$\begin{aligned} V &= psk_A + (x_A^2 + r_2 hx_A)P, V^* = \\ &= psk_A + (x_A^2 + r_2 h' x_A)P \end{aligned}$$

D 在 $H_1\text{-list}$ 中查询相应的 $(ID_A^*, H_1(ID_A^*), \beta, c)$, 如果 $c = 1$, D 失败终止; 否则 D 计算

$$\begin{aligned} h^{-1}V - h'^{-1}V^* &= (h^{-1} - h'^{-1})(psk_A + x_A^2 P) = \\ &= (h^{-1} - h'^{-1})(a(\beta bP) + x_A PK_A) \end{aligned}$$

由此 D 可得到 CDH 问题实例 (P, aP, bP) 的解: $abP = (h^{-1}V - h'^{-1}V^*)(\beta(h^{-1} - h'^{-1}))^{-1} - x_A PK_A$ 。

这样 B' 利用 D 就求出了 CDH 的一个解, 出现矛盾。所以改进的方案能够抵抗对手 B' 在随机预言模型下的攻击, 因此不能成功伪造签名。

2) 抗仲裁者攻击。若恶意的仲裁者 C' 能利用随机预言 $O_{H_2}, O_{\text{VES-Sign}}$ 以及提取普通签名的私钥伪造一个消息 m 的普通签名 (V, R_1, R_2) , 其中消息 m 未进行 $O_{\text{VES-Sign}}$ 询问, 那么可以构造一个算法 D' 利用 C' 来伪造普通签名。

对于 C' 关于消息 m 的签名预言 $O_{\text{VES-Sign}}$ 询问, D' 随机选择 $r_1, r_2, h \in \mathbb{Z}_q^*$, 计算 $R_1 = r_2 P - h^{-1} \lambda R_2 \beta - h^{-1} Q_A$, 若 $(ID_A^*, V, R_1, R_2, h, m)$ 已在 $H_2\text{-list}$ 中, 则重新选择 $r_1, r_2, h \in \mathbb{Z}_q^*$; 否则 D' 计算 $V_1 = (x_A^2 + x_A h r_2)P + psk_A, C'$ 接受 (V_1, R_1, R_2) 为一个

(下转第 3535 页)

力和光纤快速的传输能力。

参考文献:

- [1] LEE M-J, LEE H-Y, LEE H-K, *et al.* Improved watermark synchronization based on local auto-correlation function [J]. *Journal of Electronic Imaging*, 2009, 18(2): 1–11.
- [2] CHOI D, DO H, CHOI H, *et al.* A blind MPEG-2 video watermarking robust to camcorder recording [J]. *Signal Processing*, 2010, 90(4): 1327–1332.
- [3] WOHLGEMUTH S, ECHIZEN I, SONEHARA N, *et al.* On privacy-compliant disclosure of personal data to third parties using digital watermarking [J]. *Journal of Information Hiding and Multimedia Signal Processing*, 2011, 2(3): 270–281.
- [4] DEGUILLAUME F, CSURCA G, O'RUANAIDH J J, *et al.* Robust 3D DFT video watermarking [C]// *Proceedings of the 1999 Conference on Security and Watermarking of Multimedia Contents*, SPIE 3657. Bellingham: SPIE, 1999: 113–124.
- [5] HARTUNG F, GIROD B. Digital watermarking of MPEG-2 coded video in the bitstream domain [C]// *ICASSP 1997: Proceedings of the 1997 International Conference on Acoustic, Speech, & Signal Processing*. Piscataway: IEEE, 1997, 4: 2621–2624.
- [6] BARTOLINI F, CAPELLINI V, CALDELLI R, *et al.* MPEG-4 video data protection for multimedia fruition [C]// *VSM 2000: Proceedings of the 6th International Conference on Virtual Systems and Multimedia*. Amsterdam: IOS Press, 2000: 35–40.
- [7] BARNI M, BARTOLINI F, CAPELLINI V, *et al.* A DWT-based technique for spatio-frequency masking of digital signatures [C]// *Proceedings of the 1999 Conference on Security and Watermarking of Multimedia Contents*, SPIE 3657. Bellingham: SPIE, 1999: 31–39.
- [8] GOPAL K, LATHA M MADHAVI. Watermarking of digital video stream for source authentication [J]. *International Journal of Computer Science Issues*, 2010, 7(4): 18–26.
- [9] LEE J-W, OH T-W, LEE M-J, *et al.* Video watermarking on overlay Layer [C]// *IHH-MSP 2011: Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Piscataway: IEEE, 2011: 85–88.
- [10] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. *International Journal of Computer Vision*, 2004, 60(2): 91–110.
- [11] MATAS J, CHUM O, MARTIN U, *et al.* Robust wide baseline stereo from maximally stable extremal regions [C]// *Proceeding of the 2002 British Machine Vision Conference*. Edinburgh: BMVA Press, 2002: 761–767.
- [12] ZHANG X J, CAO X C, LI J J. Geometric attack resistant image watermarking based on MSER [J]. *Frontiers of Computer Science*, 2013, 7(1): 145–156.
- [13] MIKOLAJCZYK K, TUYTELAARS T, SCHMID C, *et al.* A comparison of affine region detectors [J]. *International Journal of Computer Vision*, 2005, 65(1): 43–72.
- [14] LIU T M, ZHANG H J, QI F H. A novel video key-frame-extraction algorithm based on perceived motion energy model [J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2003, 13(10): 1006–1013.
- [15] LIU C. Beyond pixels: exploring new representations and applications for motion analysis [D]. Cambridge: Massachusetts Institute of Technology, 2009.
- [16] LI L, QIAN J, PAN J. High capacity watermark embedding based on local invariant features [C]// *ICME 2010: Proceedings of the 2010 Internal Conference on Multimedia and Expo*. Piscataway: IEEE, 2010: 1311–1314.

(上接第 3521 页)

有效签名。最后 C' 输出一个伪造签名 (V^*, R_1^*, R_2^*, m^*) , 其中 m^* 未进行 $O_{\text{Ver-Sign}}$ 询问, 则 D' 可以从 C' 得到 (V^*, R_1^*, R_2^*) , 并输出同一个签名。因此如果 C' 能成功构造一个普通签名, 那么 D' 也能成功伪造一个普通签名。又因为文献[13]中定理 3.1 已经给出详细证明, 说明普通签名方案在随机预言模型下是可证安全的, 因此在 CDH 问题难解的前提下, D' 不可能成功伪造普通签名。所以本方案是抗恶意仲裁者攻击。

综上所述, 本文提出的方案在随机预言模型下是可证安全的。

4 结语

本文结合双线性对、无证书公钥密码体制和可验证加密签名方案, 提出一种高效的盲化的无证书可验证加密签名方案, 该方案不仅能够间接恢复出消息, 抵抗存在性伪造, 而且具有更高的安全性, 在实际生活中具有重要的应用价值, 比如公平交换协议、电子合同等。

参考文献:

- [1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// *ASIACRYPT 2003: Proceedings of Cryptology*, LNCS 2894. Berlin: Springer-Verlag, 2003: 452–473.
- [2] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme [C]// *Proceedings of the 2005 Computational Intelligence and Security*, LNCS 3802. Berlin: Springer-Verlag, 2005: 110–116.
- [3] 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.
- [4] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems [J]. *Communications of the ACM*, 1978, 21(2): 120–126.
- [5] BONEH D, GENTRY C, LYNN B, *et al.* Aggregate and verifiably encrypted signatures from bilinear maps [C]// *EUROCRYPT 2003: Proceedings of the Advances in Cryptology*, LNCS 2656. Berlin: Springer-Verlag, 2003: 416–432.
- [6] HESS F. Efficient identity based signature schemes based on pairing [C]// *Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography*, LNCS 2595. Berlin: Springer-Verlag, 2003: 310–324.
- [7] GU C X, ZHU Y F. An ID-based verifiable encrypted signature scheme based on Hess's scheme [C]// *Proceedings of the 1st SK-LOIS Conference on Information Security and Cryptology*, LNCS 3822. Berlin: Springer-Verlag, 2005: 42–52.
- [8] ASOKAN N, SHOUP V, WADNER M. Optimistic fair exchange of digital signature (extended abstract) [C]// *EUROCRYPT98: Proceedings of the 1988 International Conference on the Theory and Application of Cryptographic Techniques*, LNCS 1403. Berlin: Springer-Verlag, 1988: 591–606.
- [9] CASTRO R, DAHAB R. Two notes on the security of certificateless signature [C]// *Proceedings of Provable Security*, LNCS 4784. Berlin: Springer-Verlag, 2007: 85–102.
- [10] 周敏, 杨波, 傅贵, 等. 基于无证书的可验证加密签名方案 [J]. *计算机科学*, 2009, 36(8): 105–108.
- [11] 李兵方, 茹秀娟, 张姗姗. 一个高效的可验证加密签名方案 [J]. *咸阳师范学院学报*, 2010, 25(2): 45–48.
- [12] 谷利泽, 孙艳宾, 卿斯汉, 等. 新的基于 Shim 签名的可验证加密签名方案 [J]. *电子与信息学报*, 2011, 33(6): 1271–1276.
- [13] SHIM K-A. An ID-based aggregate signature scheme with constant pairing computations [J]. *Journal of Systems and Software*, 2010, 83(10): 1873–1880.