doi:10.11959/j.issn.1000-436x.2016112

无证书强指定验证者多重签名

杜红珍[1]，温巧燕[2]
(1. 宝鸡文理学院数学与信息科学学院，陕西 宝鸡 721013；2. 北京邮电大学网络与交换技术国家重点实验室，北京 100876)

摘 要：为了满足在司法行政、电子政务等领域的应用需求，提出了无证书强指定验证者多重签名的概念和敌手模型，利用双线性对构造了第一个无证书强指定验证者多重签名方案，在计算双线性 Diffie-Hellman 问题和计算 Diffie-Hellman 问题假设下证明了该方案是存在性不可伪造的，而且该方案满足强指定验证者签名和多重签名应具备的性质。方案执行效率高，生成的指定验证者多重签名长度仅为 160 bit，签名验证时需要的双线性对运算个数是固定的，仅需一个双线性对。所以，即使在计算资源与网络带宽受限的无线网络中方案也非常实用。
关键词：无证书公钥密码学；指定验证者多重签名；不可伪造性；双线性对
中图分类号：TP309 **文献标识码**：A

Certificateless strong designated verifier multi-signature

DU Hong-zhen[1], WEN Qiao-yan[2]
(1. School of Mathematics and Information Science, Baoji University of Arts and Sciences, Baoji 721013, China;
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In order to satisfy the application requirements in the fields of judicial administration, e-government, etc., the definition and security model for certificateless strong designated verifier multi-signature were proposed. Then, the first certificateless strong designated verifier multi-signature scheme from bilinear pairings was constructed and it was proved that the scheme is existentially unforgeable under the computational bilinear Diffie-Hellman assumption and the computational Diffie-Hellman assumption. Moreover, the scheme meets the properties of both strong designated verifier signatures and multi-signatures. The scheme achieves high efficiency since the length of designated verifier multi-signature generated by the scheme is only 160 bits and the computational cost of bilinear pairings necessary for verification algorithm is constant, i.e., one bilinear pairing. So, it can be applied in wireless networks of the limited computing resources and network bandwidth.
Key words: certificateless public key cryptography, designated verifier multi-signature, unforgeability, bilinear pairing

1 引言

2003 年，Al-Riyami 等[1]提出了无证书公钥密码学（CL-PKC, certificateless public key cryptography），CL-PKC 性能优良，汲取了传统公钥密码体制和基于 ID 的密码体制的优点，因为它不需要附带证书来认证用户的公钥，从而去掉了维护证书的费用，同时又不存在密钥托管问题，所以对 CL-PKC 的研究很有理论意义和实际应用价值。目前已有很多的无证书加密、签名方案[2~8]被提出。

普通数字签名的验证权是不可控的，即只要有签名人的公钥就可以检验签名的有效性，但在有些环境如电子投招标、电子购物、电子拍卖和知识产权保护等应用中，签名人希望由自己指定签名验证者，从而控制签名的验证权。为了满足这种应用，Jakobsson 等[9]提出了指定验证者签名（DVS, designated verifier

收稿日期：2015-12-27；**修回日期**：2016-05-11
基金项目：国家自然科学基金资助项目（No.61402015, No.61402275）；陕西省教育厅专项科研基金资助项目（No.15JK1022）；陕西省自然科学基础研究基金资助项目（No.2015JM6263）
Foundation Items: The National Natural Science Foundation of China (No.61402015, No.61402275), The Scientific Research Project of Shaanxi Provincial Educations Department (No.15JK1022), The Basic Research Project of Natural Science in Shaanxi Province (No.2015JM6263)

signature）的概念。在文献[9]中，Jakobsson 等还提出了强指定验证者签名（SDVS, strong designated verifier signature）。在一个 SDVS 方案中，签名验证时要用到指定验证者的私钥，所以除了签名人指定的验证者以外，其他人都不能验证签名的有效性。2003 年，Steinfeld 等[10]提出了广义指定验证者签名（UDVS, universal designated verifier signature）的概念，UDVS 与 SDVS 的主要区别是：前者允许任何一个（普通）签名持有者（不一定是签名者本人）根据自己的意愿来指定签名验证者，再将该（普通）签名转化为指定验证者签名。而后者是签名人自己确定签名的验证者，再直接生成指定验证者签名。

目前，在 CL-PKC 下研究指定验证者签名的成果颇丰。2006 年，Huang 等[11]利用双线性对提出了第一个无证书 SDVS 方案。2008 年，Chen 等[12]构造了一个无证书 SDVS 方案，生成的签名长度可压缩到 160 bit。He 等[13]构造了一个无需双线性对的无证书 SDVS 方案。李继国等[14]提出了一个基于证书的 SDVS 方案，签名的长度仅 160 bit。Ming 等[15]给出了无证书 UDVS 的概念。Du 等[16]提出了第一个高效的无证书指定验证者代理签名方案。Hafizul 等[17]在 CL-PKC 下提出了一个广义指定验证者多重签名方案，然而，该方案缺陷较多，比如作者概念不清，误称他们提出了一个无证书强指定验证者多重签名方案，且方案不能抵抗恶意但被动 KGC 的攻击。2015 年，张玉磊等[18]在 CL-PKC 下提出了一个广义指定验证者聚合签名方案，该方案生成的聚合签名长度为 320 bit，签名验证需要的双线性对个数固定，仅需 4 个对，所以方案执行效率较高。

多重签名（MS, multi-signature）的概念由 Itakura 等[19]提出，MS 是一种多方参与的特殊签名，允许多个签名人在同一个消息 m 上进行签署，生成的多重签名 σ 的长度远小于每个人对 m 的普通签名 σ_i 的长度之和，且 σ 的验证代价同样大大低于验证多个 σ_i 所需计算量。多重签名在电子政务、电子病历、蜂窝电话、电子射频技术、传感器等领域应用广泛。

随着新型网络形态和网络服务的出现，研究多方参与的特殊签名已成为密码学界一个新热点。本文在 CL-PKC 下将指定验证者签名与多重签名结合，提出了一种特殊签名——无证书强指定验证者多重签名（CL-SDVMS, certificateless strong designated verifier multi-signature），它允许多个用户对同一个消息生成多重签名，且该多重签名的有效性只有这多个用户指定的验证者才能验证，其他第三方都无法验证签名。与强指定验证者签名类似，一个安全的 CL-SDVMS 方案应该具备强壮性（第三方不可验证性）、不可伪造性、不可传递性和签名源的隐匿性。现实生活中，CL-SDVMS 有很多应用场景，比如多个目击者想要向法官揭发某个犯罪嫌疑人，但为了防止遭到报复，目击者们就指定该法官为签名验证者，采用 CL-SDVMS 方案来检举犯罪嫌疑人，这样，只有该法官可以验证签名的有效性，从而相信签名的真实性。同时 CL-SDVMS 的不可传递性也使目击者得到保护，因为其他人不会相信签名是目击者生成而不是法官生成的。CL-SDVMS 在司法行政如呈报减刑、假释等工作和电子政务等领域有很好的应用前景。

本文首先提出了 CL-SDVMS 的定义和安全模型，接着利用双线性对构造了第一个 CL-SDVMS 方案，该方案满足强壮性、不可伪造性、不可传递性和签名源的隐匿性。方案执行效率高，因为它是非交互的，且签名的验证仅需一个双线性对，另外，生成的指定验证者多重签名长度固定，不会随签名人数的增加而增长。

2　预备知识

1) 双线性对

k 是一个安全参数，q 是一个 k bit 的素数，G_1 是阶为 q 的循环加法群，P 是 G_1 的生成元，G_2 是 q 阶循环乘法群。双线性映射 $e: G_1 \times G_1 \to G_2$ 满足以下性质。

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

② 非退化性：$\exists P, Q \in G_1$，使 $e(P, Q) \neq 1$；

③ 易计算性：$\forall P, Q \in G_1$，存在有效算法可以计算值 $e(P, Q)$。

2) 计算 Diffie-Hellman (CDH)问题

给定 $P, aP, bP \in G_1$，$a, b \in Z_q^*$ 是未知的随机数，计算 $abP \in G_1$。

3) 计算双线性 Diffie-Hellman (CBDH)问题

给定 $P, aP, bP, cP \in G_1$，$a, b, c \in Z_q^*$ 是未知的随机数，计算 $e(P, P)^{abc}$。

迄今为止，CDH 问题和 CBDH 问题仍是困难的。

3　CL-SDVMS 方案的形式化定义和安全模型

3.1　CL-SDVMS 方案的形式化定义

定义 1　CL-SDVMS 方案的参与实体：一个私

钥生成中心（KGC），n 个签名用户 $ID_i(1\leqslant i\leqslant n)$ 和一个由这 n 个用户指定的验证者 ID_v。CL-SDVMS 方案由以下 6 个算法构成。

1) 系统建立（Setup）算法：输入一个安全参数 k，输出系统主密钥 s 和系统参数 $params$，该算法由 KGC 执行。

2) 部分私钥生成(Partial-Private-Key-Extract)算法：由 KGC 执行，输入 $params$、s 和身份 ID_i，返回用户 ID_i 的部分私钥 D_i。

3) 用户密钥生成(User-Key-Generate)算法：由用户 ID_i 执行，输入 $params$、ID_i，输出该用户的秘密值和公钥（x_i, Pk_i）。

4) 签名(Sign)算法：输入 $params$，待签消息 m，n 个签名人身份集合 $L_{\text{set}}=\{ID_1,ID_2,\cdots,ID_n\}$，签名人的部分私钥/秘密值$(D_i,x_i)(1\leqslant i\leqslant n)$、$ID_i$、公钥 Pk_i，指定验证者的身份/公钥（ID_v,Pk_v），输出指定验证者多重签名 σ。

5) 验证(Verify)算法：输入(m,σ), $params$, $L_{\text{set}}=\{ID_1,ID_2,\cdots,ID_n\}$，$ID_i$，$Pk_i(1\leqslant i\leqslant n)$，指定验证者的部分私钥/秘密值$(D_v, x_v)$，判断 σ 是否有效，输出“1”或“0”，表示 σ 有效或无效。

6) 签名模拟(Simulation)算法：该算法由指定验证者执行，输入 $params$，m，$L_{\text{set}}=\{ID_1,ID_2,\cdots,ID_n\}$，$ID_i$，$Pk_i(1\leqslant i\leqslant n)$，指定验证者的部分私钥/秘密值（$D_v$, x_v），输出一个与 n 个签名人生成的不可区分的签名副本 σ'。

3.2 CL-SDVMS 方案的安全模型

在一个 CL-SDVMS 方案中，存在 2 种具备不同攻击力的敌手 A_1 和 A_2。第一种敌手 A_1 模拟恶意用户，他掌握用户的秘密值，可以替换任意用户的公钥，但不知道系统主密钥和用户的部分私钥。第 2 种敌手 A_2 模拟的是恶意但被动（malicious-but-passive）KGC，他拥有系统主密钥并可以求出用户的部分私钥，但不知道用户的秘密值，且不能替换用户的公钥。

下面通过引入挑战者 X 和敌手 A（A_1 或 A_2）之间的 Game 来模拟 CL-SDVMS 的不可伪造性安全模型。

1) Setup：X 运行 Setup 算法生成系统主密钥 s 和公开参数 $params$，秘密保存 s，将 $params$ 发送给 A。如果 A 是第 2 种敌手 A_2，则发送 $params$ 和 s 给 A_2。

2) Query：A 可以适应性询问以下预言机。

Hash 询问：当 A 询问任意一个散列函数值时，X 输出相应的散列值给 A。

Create-user：当 A 输入 ID_i 时，如果 ID_i 用户已被创立，X 只需将 ID_i 的公钥 Pk_i 返回给 A。否则 X 运行 Partial-Private-Key-Extract 算法和 User-Key-Generate 算法，生成 ID_i 的部分私钥 D_i 和秘密值/公钥(x_i, Pk_i)，这时称 ID_i 用户被创立，最后，X 将 ID_i 的公钥 Pk_i 返回给 A。

本文假定下面的预言机询问中 ID_i 为创立用户。

Public-Key-Replace: 当 A 输入(ID_i,Pk_i')进行公钥替换询问，X 用 Pk_i' 替换 Pk_i（此预言机仅针对 A_1）。

Secret-Value-Extract: 当 A 询问 ID_i 的秘密值时，X 返回相应的秘密值 x_i。如果 ID_i 的公钥已被替换，X 输出 $\perp$（$\perp$ 表示未知值）。

Partial-Private-Key-Extract 询问：输入 ID_i，X 返回部分私钥 D_i 给 A（此预言机仅针对 A_1，A_2 不需要询问该预言机，因为它知道用户的部分私钥）。

Sign 询问：A 输入签名者/指定验证者身份（ID_i, ID_v），公钥(Pk_i, Pk_v)，消息 $m\in\{0,1\}^*$，身份集 L_{set}，X 运行 Sign 算法生成相应的部分签名 σ_i，再返回 σ_i 给 A。

注：任何一个用户都可以由部分签名 σ_i 得到（完整）多重签名 σ，所以不需要多重签名预言机。

Verify 询问：A 输入签名者/指定验证者身份（ID_i, ID_v），公钥(Pk_i, Pk_v)，消息/签名（m，σ_i），身份集 L_{set}，X 运行 Verify 算法判断 σ_i 的有效性，再输出“1”或“0”给 A。

3) Forgery: 最后，敌手 A 伪造了一个在消息 m^* 上关于 $L_{\text{set}}^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$ 的有效指定验证者多重签名 σ^*，其中，n 个签名者的身份/公钥为（ID_i^*,Pk_i^*），指定验证者身份/公钥为（ID_v^*,Pk_v^*），且满足：

① 如果 A 是第一种敌手 A_1，L_{set}^* 中至少有一个 ID_I^* $(1\leqslant I\leqslant n)$ 和指定验证者 ID_v^* 没有提交给 Partial-Private-Key-Extract 预言机，且（m^*，ID_I^*，L_{set}^*）没有提交给 Sign 预言机，则 A 获胜；

② 如果 A 是第 2 种敌手 A_2，L_{set}^* 中至少有一个 ID_I^* $(1\leqslant I\leqslant n)$ 和指定验证者 ID_v^* 没有提交给 Secret-Value-Extract 预言机，且（m^*，ID_I^*，L_{set}^*）没有提交给 Sign 预言机，则 A 获胜。

A 的优势 $Adv_A^{CL-SDVMS}$ 为 A 在 Game 中获胜的

概率。

定义 2　如果不存在概率多项式时间敌手 A(A_1 或 A_2)在以上 Game 中能以不可忽略的优势获胜，则一个 CL-SDVMS 方案在适应性选择消息攻击下是存在性不可伪造的（EUF-CL-SDVMS-CMA2 安全）。

4　一个高效的无证书强指定验证者多重签名方案

4.1　基本方案

本节构造了一个无证书强指定验证者多重签名方案，由下面 6 个算法组成。

1) 系统建立算法：k 是一个安全参数，$(G_1,+),(G_2,\times)$ 是 2 个阶为素数 $q>2^k$ 的循环群，P 是 G_1 的一个生成元，双线性映射 $e:G_1\times G_1\to G_2$，4 个安全散列函数 $H_1,H_1':\{0,1\}^*\to G_1$，$H_2,H_2':\{0,1\}^*\to Z_q^*$。KGC 选取随机数 $s\in Z_q^*$ 作为系统主密钥，计算公钥 $P_0=sP$，公开系统参数 $params$: $\{k,G_1,G_2,q,P,e,P_0,H_1,H_1',H_2,H_2'\}$。

2) 部分私钥生成算法：给定用户身份 ID_i，KGC 计算该用户的部分私钥 $D_i=sQ_i$ 和 $D_i'=sQ_i'$，其中，$Q_i=H_1(ID_i)$，$Q_i'=H_1'(ID_i)$。

3) 用户密钥生成算法：用户 ID_i 选随机数 $x_i\in Z_q^*$ 作为秘密值，计算公钥 $Pk_i=x_iP$。

4) 签名算法：待签消息 m，n 个签名人身份集合 $L_{\text{set}}=\{ID_1,ID_2,\cdots,ID_n\}$，指定验证者的身份/公钥（$ID_v,Pk_v$），签名人 ID_i $(1\leqslant i\leqslant n)$ 操作如下。

① 计算 $l_i=H_2(m,ID_i,Pk_i,ID_v,Pk_v,x_iPk_v)$。

② 计算 $l_i'=H_2'(m,L_{\text{set}},x_iPk_v)$，$Q_v=H_1(ID_v)$。

③ 计算 $\sigma_i=e(l_iD_i+l_i'D_i',Q_v)$。

则 σ_i 是签名人 ID_i 对 m 的部分指定验证者签名。

得到 n 个部分指定验证者签名 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 后，任何人都可以计算出最终关于 $L_{\text{set}}=\{ID_1,ID_2,\cdots,ID_n\}$ 的指定验证者多重签名 $\sigma=\prod_{i=1}^n\sigma_i$。

5) 验证算法：输入 (m,σ)，$L_{\text{set}}=\{ID_1,ID_2,\cdots,ID_n\}$，$Pk_i(1\leqslant i\leqslant n)$，指定验证者 ID_v (其部分私钥 $D_v=sQ_v$，秘密值 x_v)计算如下。

① 计算 $l_i=H_2(m,ID_i,Pk_i,ID_v,Pk_v,x_vPk_i)$，$l_i'=H_2'(m,L_{\text{set}},x_vPk_i)$。

② 检验 $\sigma\overset{?}{=}e\left(\sum_{i=1}^n(l_iQ_i+l_i'Q_i'),D_v\right)$ 是否成立，如果成立，则该指定验证者多重签名 σ 有效，否则无效。

6) 签名模拟算法：对消息 m，指定验证者 ID_v 可以生成有效的指定验证者多重签名副本。

① 计算 $l_i^*=H_2(m,ID_i,Pk_i,ID_v,Pk_v,x_vPk_i)$ $l_i'^*=H_2'(m,L_{\text{set}},x_vPk_i)$，$1\leqslant i\leqslant n$。

② 计算 $\sigma'=e\left(\sum_{i=1}^n(l_i^*Q_i+l_i'^*Q_i'),D_v\right)$，则 σ' 为指定验证者 ID_v 生成的签名副本。

下面给出方案正确性的证明。

证明　因为 $x_iPk_v=x_ix_vP=x_vx_iP=x_vPk_i$，所以 $l_i=H_2(m,ID_i,Pk_i,ID_v,Pk_v,x_iPk_v)=H_2(m,ID_i,Pk_i,ID_v,Pk_v,x_vPk_i)$ 和 $l_i'=H_2'(m,L_{\text{set}},x_iPk_v)=H_2'(m,L_{\text{set}},x_vPk_i)$。

则
$$\begin{aligned}\sigma&=\prod_{i=1}^n\sigma_i\\&=\prod_{i=1}^n e\left((l_iD_i+l_i'D_i'),Q_v\right)\\&=\prod_{i=1}^n\left(e(l_iD_i,Q_v)e(l_i'D_i',Q_v)\right)\\&=\prod_{i=1}^n e(l_iQ_i,D_v)e(l_i'Q_i',D_v)\\&=e\left(\sum_{i=1}^n(l_iQ_i+l_i'Q_i'),D_v\right)\end{aligned}$$

4.2　方案的安全性分析

4.2.1　不可伪造性

定理 1　在 Random Oracle 模型和 CBDH 及 CDH 难题假设下，本文的 CL-SDVMS 方案在 2 类敌手 A_1 和 A_2 的攻击下是 EUF-CL-SDVMS-CMA2 安全的。

定理 1 由引理 1 和引理 2 推出。

引理 1　在 Random Oracle 模型下，假定有敌手 A_1 在概率多项式时间 t 内以优势 ε 攻破了本文 CL-SDVMS 方案，记 A_1 最多询问 Create-User，Partial-Private-Key-Extract，Sign 和 Verify 的次数分别为 $q_c(q_c>n)$、q_p、q_s 和 q_v，则存在一个算法 X，使用 A_1 为黑盒子，在时间 $t'<t+(4q_c+2q_s+2q_v+n)t_{\text{Sm}}+(q_s+q_v)t_{\text{Pr}}+t_{\text{inv}}$ 内，以 $\varepsilon'\geqslant\varepsilon\left(\frac{n}{q_c^2}\right)\cdot\left(1-\frac{2}{q_c}\right)^{q_p}\left(1-\frac{1}{q_c(q_c-1)}\right)^{q_s+q_v}$ 的优势解决 CBDH 难题，t_{Sm} 是 G_1 群上一个标量乘时间，t_{Pr} 是一个双线性对运算时间，t_{inv} 是计算 Z_q^* 上一个求逆时间。

证明　本 CL-SDVMS 方案涉及 n 个签名用户

$ID_1, ID_2, \cdots, ID_n$ 和一个由这 n 个用户指定的验证者 ID_v，不妨假设除用户 $ID_I \in \{ID_1, ID_2, \cdots, ID_n\}$ 以外，其余 n–1 个用户都被敌手 A_1 贿赂（本文赋予了敌手更强的攻击能力，此处模拟的是一种极端情形，实际场景中一般不少于一个诚实者）。设 X 为挑战者，给定群 G_1 上 CBDH 问题的任意实例 $aP, bP, cP \in G_1$，其中，a, b, c 未知，X 最终目的是输出值 $e(P,P)^{abc}$。

X 运行系统建立算法，令 $P_0 = aP$，生成系统参数 $params: \{k, G_1, G_2, q, P, e, P_0, H_1, H_1', H_2, H_2'\}$，将 $params$ 发给 A_1，A_1 查询预言机如下（本文假定敌手不重复询问）。

Create-user：A_1 输入 $ID_i (1 \leqslant i \leqslant q_c)$，X 调出列表 K^{list} 查看，如果 ID_i 用户已被创立，X 只需将 ID_i 的公钥 Pk_i 返回给 A_1；否则，X 执行如下。

1) 如果 $ID_i \neq ID_I, ID_v$，X 选 3 个随机数 $r_i, r_i', x_i \in Z_q^*$，计算 $Q_i = r_i P$，$Q_i' = r_i' P$，用户的部分私钥 $D_i = r_i(aP)$，$D_i' = r_i'(aP)$，用户的公钥 $Pk_i = x_i P$，将数据（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）插入列表 K^{list}，返回 Pk_i 给 A_1。

2) 如果 $ID_i = ID_I$，X 选 3 个随机数 $r_i, r_i', x_i \in Z_q^*$，计算 $Q_i = r_i(bP)$，$Q_i' = r_i'(bP)$，$D_i = \perp$，$D_i' = \perp$（符号 $\perp$ 表示未知值），$Pk_i = x_i P$，将数据（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）插入列表 K^{list}，返回 Pk_i 给 A_1。

3) 如果 $ID_i = ID_v$，X 选 3 个随机数 $r_i, r_i', x_i \in Z_q^*$，计算 $Q_i = r_i(cP)$，$Q_i' = r_i'(cP)$，$D_i = \perp, D_i' = \perp$，$Pk_i = x_i P$，将数据（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）插入列表 K^{list}，返回 Pk_i 给 A_1。

H_1, H_1' 询问：当 A_1 输入身份 ID_i，X 调出列表 K^{list}，如果 K^{list} 中有对应记录，则返回 Q_i、Q_i'；否则，询问 Create-user 预言机后得到 Q_i、Q_i' 并返回给 A_1。

Partial-Private-Key-Extract：当 A_1 输入 ID_i（以下默认 ID_i 用户已被创立），X 调出列表 K^{list}，如果 $ID_i \neq ID_I, ID_v$，则返回 D_i、D_i'；否则，停止模拟，输出 failure。

Public-Key-Replace：当 A_1 输入 (ID_i, Pk_i') 进行公钥替换询问，X 调出列表 K^{list}，用 Pk_i' 替换 Pk_i，即 $Pk_i = Pk_i'$ 再替换对应的秘密值 $x_i = \perp$。

Secret-Value-Extract：A_1 输入 ID_i，X 调出列表 K^{list}，返回 x_i 给 A_1。

H_2-询问：A_1 输入 $(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j)$，X 调出列表 H^{list}，返回以前赋予的散列值；否则，选随机数 $l_i \in Z_q^*$，令 $l_i = H_2(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j)$，添加 $(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 到 H^{list} 中，输出 l_i。

H_2'-询问：当 A_1 输入 $(m, L_{\text{set}}, x_i Pk_j)$ 时，X 输出以前赋予的散列值；否则，选随机数 $l_i' \in Z_q^*$，定义 $l_i' = H_2'(m, L_{\text{set}}, x_i Pk_j)$，添加 $(m, L_{\text{set}}, x_i Pk_j, l_i')$ 到列表 L^{list} 中，返回 l_i'。

Sign：A_1 输入签名者/指定验证者的身份（ID_i, ID_j）和公钥(Pk_i, Pk_j), 消息 m，身份集 L_{set}，X 执行如下。

1) 如果 $ID_i \neq ID_I$, ID_v 时，X 调出列表 $K^{\text{list}}(ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i)$、列表 $H^{\text{list}}(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 和列表 $L^{\text{list}}(m, L_{\text{set}}, x_i Pk_j, l_i')$，计算 $\sigma_i = e(l_i D_i + l_i' D_i', Q_j)$，返回指定验证者签名 σ_i 给 A_1。

注：如果列表 K^{list}、H^{list}、L^{list} 中没有对应记录，则 X 再逐一询问 Create-user，H_2 和 H_2' 预言机来获得想要的值。

2) 如果 $ID_i = ID_I$，$ID_j \neq ID_v$，X 调出列表 K^{list}（$ID_j, r_j, r_j', Q_j, Q_j', D_j, D_j', x_j, Pk_j$）、列表 $H^{\text{list}}(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 和列表 $L^{\text{list}}(m, L_{\text{set}}, x_i Pk_j, l_i')$，计算 $\sigma_i = e(l_i Q_i + l_i' Q_i', D_j)$，返回 σ_i 给 A_1。

3) 如果 $ID_i = ID_I$，$ID_j = ID_v$，X 停止模拟，输出failure。

Verify：A_1 输入签名者/指定验证者的身份（ID_i, ID_j）和公钥(Pk_i, Pk_j)、消息/指定验证者签名（m, σ_i）、身份集 L_{set}，验证如下。

1) 如果 $ID_i \neq ID_I, ID_v$，X 调出列表 K^{list}（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）、列表 $H^{\text{list}}(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 和列表 $L^{\text{list}}(m, L_{\text{set}}, x_i Pk_j, l_i')$，检验 $\sigma_i \stackrel{?}{=} e(l_i D_i + l_i' D_i', Q_j)$，如果等式成立则返回“1”，表示签名有效；否则返回“0”，说明签名无效。

2) 如果 $ID_i = ID_I$，$ID_j \neq ID_v$，X 调出列表 K^{list}（$ID_j, r_j, r_j', Q_j, Q_j', D_j, D_j', x_j, Pk_j$）、列表 $H^{\text{list}}(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 和列表 $L^{\text{list}}(m, L_{\text{set}},$

$x_i Pk_j, l_i'$)，检验 $\sigma_i \stackrel{?}{=} e(l_i Q_i + l_i' Q_i', D_j)$，返回“1”或“0”给 A1。

3) 如果 $ID_i = ID_I$，$ID_j = ID_v$，X 停止模拟，输出 failure。

Forgery：最后，敌手 A_1 伪造了一个在消息 m^* 上关于 $L_{\text{set}}^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$ 的有效指定验证者多重签名 σ^*，其中，n 个签名者的身份/公钥为（ID_i^*, Pk_i^*）($1 \leqslant i \leqslant n$)，指定验证者身份/公钥为（$ID_j^*, Pk_j^*$）。若 $ID_j^* \neq ID_v$ 和 $ID_I \notin \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$，则 X 停止模拟，输出 failure；否则，$ID_j^* = ID_v$，且 $ID_I \in \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$，下面不妨假设 $ID_1 = ID_1^*$。

X 调出列表 K^{list}（$ID_i^*, r_i^*, r_i'^*, Q_i^*, Q_i'^*, D_i^*, D_i'^*, x_i^*, Pk_i^*$）、列表 H^{list}（$m^*, ID_i^*, Pk_i^*, ID_v, Pk_v, x_i^* Pk_v, l_i^*$）和列表 $L^{list}(m^*, L_{\text{set}}^*, x_i^* Pk_v, l_i'^*)$，因为 σ 有效，所以以下等式成立

$$\begin{aligned}\sigma^* &= e(l_1^* Q_1^* + l_1'^* Q_1'^*, D_v) e(\sum_{i=2}^n l_i^* Q_i^* + l_i'^* Q_i'^*, D_v) \\ &= e(l_1^* r_1^* (bP) + l_1'^* r_1'^* (bP), r_v acP) \cdot \\ &\quad e(\sum_{i=2}^n l_i^* r_i^* P + l_i'^* r_i'^* P, r_v acP)\end{aligned}$$

从而，X 可以计算

$$e(P,P)^{abc} = \left(\frac{\sigma^*}{e(\sum_{i=2}^n l_i^* r_i^* (aP) + l_i'^* r_i'^* (aP), r_v (cP))} \right)^{\left(r_v (l_1^* r_1^* + l_1'^* r_1'^*)\right)^{-1}}$$

即 X 可以解决 CBDH 难题，但目前 CBDH 问题是困难的，所以规约出本文方案是 EUF-CL-SDVMS-CMA2 安全的。

下面计算 X 成功的概率。用 E_1、E_2、E_3、E_4、E_5 表示 5 个事件如下。

1) E_1：X 回答 A_1 的 Partial-Private-Key-Extract 询问时没有失败。

2) E_2：X 回答 A_1 的 Sign 询问时没有失败。

3) E_3：X 回答 A_1 的 Verify 询问时没有失败。

4) E_4：A_1 成功地伪造了 1 个在消息 m^* 上的指定验证者多重签名 σ^*，其中，n 个签名者的身份为 $ID_1^*, ID_2^*, \cdots, ID_n^*$，指定验证者身份为 ID_j^*。

5) E_5：在 E_4 发生情况下，有 $ID_j^* = ID_v$ 和 $ID_I \in \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$。

显然，

$$\Pr[E_1] \geqslant \left(1 - \frac{2}{q_c}\right)^{q_p}$$

$$\Pr[E_2 | E_1] \geqslant \left(1 - \frac{1}{q_c(q_c - 1)}\right)^{q_s}$$

$$\Pr[E_3 | E_1 \wedge E_2] \geqslant \left(1 - \frac{1}{q_c(q_c - 1)}\right)^{q_v}$$

$$\Pr[E_4 | E_1 \wedge E_2 \wedge E_3] \geqslant \varepsilon$$

$$\Pr[E_5 | E_1 \wedge E_2 \wedge E_3 \wedge E_4] \geqslant \frac{n}{q_c^2}$$

则

$$\begin{aligned}&\Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4 \wedge E_5] \\ &= \Pr[E_1] \Pr[E_2 | E_1] \Pr[E_3 | E_1 \wedge E_2] \Pr[E_4 | E_1 \wedge E_2 \wedge E_3] \\ &\quad \Pr[E_5 | E_1 \wedge E_2 \wedge E_3 \wedge E_4] \\ &\geqslant \varepsilon \left(\frac{n}{q_c^2}\right) \left(1 - \frac{2}{q_c}\right)^{q_p} \left(1 - \frac{1}{q_c(q_c - 1)}\right)^{q_s + q_v}\end{aligned}$$

当事件 E_1、E_2、E_3、E_4、E_5 都发生时，X 获胜，其概率为 $\varepsilon' \geqslant \varepsilon \left(\frac{n}{q_c^2}\right) \left(1 - \frac{2}{q_c}\right)^{q_p} \left(1 - \frac{1}{q_c(q_c - 1)}\right)^{q_s + q_v}$。

将 X 在 Game 中每次应答时进行的运算时间加起来可得

$$t' < t + (4q_c + 2q_s + 2q_v + n) t_{\text{Sm}} + (q_s + q_v) t_{\text{Pr}} + t_{\text{inv}}$$

引理 2　在 Random Oracle 模型下，假定有敌手 A_2 在概率多项式时间 t 内以优势 ε 攻破了本文 CL-SDVMS 方案，记 A_2 最多询问 Create-User、Secret-Value-Extract、Sign 和 Verify 的次数分别为 $q_c (q_c > n)$、q_p、q_s 和 q_v，则存在一个算法 X，使用 A_2 为黑盒子，在时间 $t' < t + (5q_c + 2q_s + 2q_v) t_{\text{Sm}} + (q_s + q_v) t_{\text{Pr}}$ 内，以 $\varepsilon' \geqslant \varepsilon \left(\frac{n}{q_c^2}\right) \left(1 - \frac{n}{q_c}\right)^{q_p} \left(1 - \frac{1}{(q-1)^2}\right)$ 的优势解决 CDH 难题，t_{Sm} 是 G_1 群上一个标量乘时间，t_{Pr} 是一个双线性对运算时间。

证明　给定群 G_1 上 CDH 问题的任意实例 $aP, bP \in G_1$，其中 a, b 未知，X 的目标是输出值 abP。

运行系统建立算法，令 $P_0 = sP$，生成系统参数 $params: \{k, G_1, G_2, q, P, e, P_0, H_1, H_1', H_2, H_2'\}$，将系统主密钥 s 和 $params$ 发给 A_2，A_2 查询预言机如下（假定敌手不重复询问）。

Create-user：A_2 输入 $ID_i (1 \leqslant i \leqslant q_c)$，X 调出列表 K^{list} 查看，如果 ID_i 用户已被创立，A 只需将

ID_i 的公钥 Pk_i 返回给 A_2；否则，X 选 2 个随机数 $r_i, r_i' \in Z_q^*$，计算 $Q_i = r_i P$，$Q_i' = r_i' P$，用户的部分私钥 $D_i = r_i sP$，$D_i' = r_i' sP$。接着计算用户 ID_i 的公钥如下。

1) 如果 $ID_i \neq ID_I, ID_v$，X 选随机数 $x_i \in Z_q^*$，计算 $Pk_i = x_i P$，将数据（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）插入列表 K^{list}，返回 Pk_i 给 A_2。

2) 如果 $ID_i = ID_I$，X 令 $Pk_i = aP, x_i = \perp$，将数据（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）插入列表 K^{list}，返回 Pk_i 给 A_2。

3) 如果 $ID_i = ID_v$，X 令 $Pk_i = bP$，$x_i = \perp$，将数据（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）插入列表 K^{list}，返回 Pk_v 给 A_2。

H_1、H_1' 询问：当 A_2 输入身份 ID_i，X 调出列表 K^{list}，如果 K^{list} 中有对应记录，则返回 Q_i、Q_i'；否则，询问 Create-user 预言机后得到 Q_i、Q_i' 并返回给 A_2。

Secret-Value-Extract：A_2 输入 ID_i，如果 $ID_i \neq ID_I, ID_v$，X 调出列表 K^{list}，返回 x_i 给 A_2；否则，输出 failure。

H_2-询问：A_2 输入 $(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j)$，X 调出列表 H^{list}，返回以前赋予的散列值；否则，选随机数 $l_i \in Z_q^*$，令 $l_i = H_2(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j)$，添加 $(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 到 H^{list} 中，输出 l_i。

H_2'-询问：当 A_2 输入 $(m, L_{\text{set}}, x_i Pk_j)$ 时，X 输出以前赋予的散列值；否则，选随机数 $l_i' \in Z_q^*$，定义 $l_i' = H_2'(m, L_{\text{set}}, x_i Pk_j)$，添加 $(m, L_{\text{set}}, x_i Pk_j, l_i')$ 到列表 L^{list} 中，返回 l_i'。

Sign：A_2 输入签名者/指定验证者的身份（ID_i, ID_j）和公钥(Pk_i, Pk_j), 消息 m，身份集 L_{set}，X 调出列表 K^{list}（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）、列表 H^{list} $(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 和列表 $L^{\text{list}}(m, L_{set}, x_i Pk_j, l_i')$，计算 $\sigma_i = e(l_i D_i + l_i' D_i', Q_j)$，返回指定验证者签名 σ_i 给 A_2。

Verify：A_2 输入签名者/指定验证者的身份（ID_i, ID_j）和公钥(Pk_i, Pk_j), 消息/指定验证者签名（m, σ_i）、身份集 L_{set}，X 调出列表 K^{list}（$ID_i, r_i, r_i', Q_i, Q_i', D_i, D_i', x_i, Pk_i$）、列表 H^{list} $(m, ID_i, Pk_i, ID_j, Pk_j, x_i Pk_j, l_i)$ 和列表 $L^{\text{list}}(m, L_{\text{set}}, x_i Pk_j, l_i')$，检验 $\sigma_i \stackrel{?}{=} e(l_i D_i + l_i' D_i', Q_j)$，如果等式成立则返回“1”，表示签名有效；否则，返回“0”，说明签名无效。

Forgery：最后，敌手 A_2 伪造了一个在消息 m^* 上关于 $L_{\text{set}}^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$ 的有效指定验证者多重签名 σ^*，其中，n 个签名者的身份/公钥为（ID_i^*, Pk_i^*）($1 \leqslant i \leqslant n$)，指定验证者身份/公钥为（$ID_j^*, Pk_j^*$），若 $ID_j^* \neq ID_v$ 和 $ID_I \notin \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$，则 X 停止模拟，输出 failure；否则，$ID_j^* = ID_v$，且 $ID_I \in \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$，下面不妨假设 $ID_I = ID_1^*$。X 调出列表 H^{list} 或 L^{list}，查看记录 $(m^*, ID_1^*, Pk_1^*, ID_v, Pk_v, x_1^* Pk_v, l_1^*)$ 或 $(m^*, L_{\text{set}}^*, x_1^* Pk_v, l_1'^*)$，如果 H^{list} 或 L^{list} 中没有这样的记录，则失败退出；否则，就有 $x_1^* Pk_v = abP$，从而 X 得到 abP 值，即 X 可以解决 CDH 难题，但目前 CDH 问题仍是困难的，所以，可规约为本文方案在 A_2 攻击下是 EUF-CL-SDVMS-CMA2 安全的。另外，X 成功的概率计算方法与引理 1 的相同，此处不再赘述。

4.2.2 强壮性（第三方不可验证性）

本文 CL-SDVMS 方案在验证签名 σ 的有效性时，必须计算式子 $\sigma \stackrel{?}{=} e(\sum_{i=1}^{n} l_i Q_i + l_i' Q_i', D_v)$，其中，$l_i = H_2(m, ID_i, Pk_i, ID_v, Pk_v, x_v Pk_i)$，$l_i' = H_2'(m, L_{\text{set}}, x_v Pk_i)$。显然，计算该式子时要用到指定验证者 ID_v 的部分私钥 D_v 和秘密值 x_v，所以，只有指定验证者 ID_v 才能验证 σ 的有效性，任何第三方（包括敌手 A_1 和 A_2）因为没有指定验证者的部分私钥和秘密值，所以无法计算 $e(\sum_{i=1}^{n} l_i Q_i + l_i' Q_i', D_v)$，从而不能验证 σ 是否等于 $e(\sum_{i=1}^{n} l_i Q_i + l_i' Q_i', D_v)$，即不能验证多重签名的有效性。所以，本文方案是一个强指定验证者多重签名方案。

4.2.3 签名源隐匿性

签名源隐匿性是指给定一个消息/指定验证者多重签名对（m, σ），即使第三方 Coral 知道 n 个签名人 ID_i($1 \leqslant i \leqslant n$) 和指定验证者 ID_v 的私钥，也不能判断出 σ 是 ID_i 还是 ID_v 生成的。

本文 CL-SDVMS 方案满足签名源隐匿性，下面对 Coral 赋予不同的攻击能力，分以下 2 种情况证明该性质。

1) Coral 模拟敌手 A：A 拥有系统参数 *params*，签名人 ID_i($1 \leqslant i \leqslant n$) 和指定验证者 ID_v 的公钥，且掌握 $n-1$ 个签名人 ID_i 的私钥（即部分私钥和

秘密值。

给定一个消息/指定验证者多重签名对(m,σ)，如果 A 要推断σ的真正签名人，首先需要知道谁的私钥用于签名生成中，即需要从式子$\sigma = e(\sum_{i=1}^{n} l_i D_i + l_i' D_i', Q_v)$或$e(\sum_{i=1}^{n} l_i Q_i + l_i' Q_i', D_v)$中得出。然而已知$\sigma$，如果可以求出$\sum_{i=1}^{n} l_i D_i + l_i' D_i'$或$D_v$，则可以使用 A 为黑盒子，在概率多项式时间内解决双线性对求逆问题（给定$T \in G_1, e(T,Q) \in G_2$，求解$Q \in G_1$），然而迄今为止，该问题仍是困难的，所以 A 从$\sigma$中推不出谁是真正的签名人。

2) Coral 模拟敌手 T：T 除了具备 A 的攻击能力外，他还掌握所有签名人$ID_i (1 \leqslant i \leqslant n)$和指定验证者$ID_v$的私钥。

给定消息/指定验证者多重签名对（m,σ），T 要判断σ的真正签名人，如果他用n个$ID_i (1 \leqslant i \leqslant n)$的私钥$((D_i, D_i'), x_i)$，可以计算得到$\sigma = e(\sum_{i=1}^{n} l_i D_i + l_i' D_i', Q_v)$，其中，$l_i = H_2(m, ID_i, Pk_i, ID_v, Pk_v, x_i Pk_v)$，$l_i' = H_2'(m, L_{set}, x_i Pk_v)$，$1 \leqslant i \leqslant n$，$Q_v = H_1(ID_v)$。

但是，如果用ID_v的私钥(D_v, x_v)可以计算$\sigma' = e\left(\sum_{i=1}^{n} (l_i^* Q_i + l_i'^* Q_i'), D_v\right)$，其中，$l_i^* = H_2(m, ID_i, Pk_i, ID_v, Pk_v, x_v Pk_i)$，$l_i'^* = H_2'(m, L_{\text{set}}, x_v Pk_i)$ $(1 \leqslant i \leqslant n)$。

显然，$\sigma = \sigma'$。即无论是用$ID_i (1 \leqslant i \leqslant n)$的私钥还是$ID_v$的私钥都可以求出同一$\sigma$，所以 T 根本无法判断出$\sigma$的真正签名人。

综上，本文的 CL-SDVMS 方案满足签名源隐匿性。

4.2.4　不可传递性

不可传递性是指指定验证者ID_v虽然可以验证多重签名σ的有效性，但他不能使任何第三方相信σ就是n个签名人$ID_i (1 \leqslant i \leqslant n)$所签，因为$ID_v$可以通过签名模拟算法生成与$\sigma$不可区分的签名副本$\sigma'$。

显然，由签名源隐匿性可推出 CL-SDVMS 方案满足不可传递性。因为给定签名σ，即使第三方知道n个签名人$ID_i (1 \leqslant i \leqslant n)$和指定验证者$ID_v$的私钥，也不能判断出$\sigma$是$ID_i$还是$ID_v$生成的，所以，如果指定验证者$ID_v$给他出示$\sigma$时，他不能相信$\sigma$就是$ID_i (1 \leqslant i \leqslant n)$所签。

4.3　方案的性能分析

Hafizul Islam SK 方案[17]是一个无证书广义指定验证者多重签名方案，与本文方案最为接近，所以将本文 CL-SDVMS 方案与文献[17]方案进行了比较，如表 1 所示。其中，Sm、Pr 分别表示群G_1上 1 次标量乘计算、1 次双线性对计算，其他运算耗时较短，此处忽略不计。

表 1　方案性能比较（共 n 个签名用户）

方案	签名计算量	验证计算量	签名长度	安全性
文献[17]方案	(2n+1)Pr+5nSm	1Pr +2Sm	320 bit	不安全
本文方案	nPr+3nSm	1Pr +3nSm	160 bit	安全

4.3.1　效率分析

由于双线性对计算最昂贵，1 次双线性对计算耗时至少是标量乘计算时间的 20 倍以上[20],即$1 t_{\text{Pr}} \approx 20 t_{\text{Sm}}$（$t_{\text{Pr}}$、$t_{\text{Sm}}$分别表示一个双线性对运算与一个标量乘运算时间），则本文方案签名和验证的计算总时间量为$(n+1)\mathrm{t}_{\text{Pr}} + 6nt_{\text{Sm}} \approx 20(n+1)t_{\text{Sm}} + 6nt_{\text{Sm}} = (26n+20)t_{\text{Sm}}$，文献[17]方案的计算总时间量为$(2n+2)t_{\text{Pr}} + (5n+2)t_{\text{Sm}} \approx 20(2n+2)t_{\text{Sm}} + (5n+2)t_{\text{Sm}} = (45n+42)t_{\text{Sm}}$。显然，$(26n+20)t_{\text{Sm}} < (45n+42)t_{\text{Sm}}$，如取签名人数$n$=5，则本文方案的签名和验证总耗时是文献[17]方案的 56.1%。

另外，本文生成的签名长度为 160 bit，文献[17]方案为 320 bit，即本文方案传输签名的带宽比文献[17]方案节省了 50%。

综上，本文方案的计算与通信代价大大低于文献[17]方案。

4.3.2　安全性分析

1) 本文方案满足不可伪造性，但文献[17]方案不能抵抗恶意但被动的 KGC 的伪造攻击。

2) 本文方案是非交互的，即签名前或签名过程中都不需要参与方交互信息来生成签名。文献[17]方案是交互的，在签名生成过程中需要每个签名人给其他签名人广播信息，且只有收到其他签名人的广播信息后才可以继续实施签名，这种交互的方案实用性不好。

3) 本文方案是可以抵抗恶意组合的，因为签名σ中有全体签名人身份集合$L_{\text{set}} = \{ID_1, ID_2, \cdots, ID_n\}$，所以，敌手不可能通过串联 2 组不同用户的多重签名来得到一个新的多重签名，但文献[17]方案则不能抵抗敌手的恶意组合。

由 1)和 2)可见，本文方案是一个性能良好的安全高效的 CL-SDVMS 方案。

5　结束语

CL-SDVMS 在司法行政如呈报减刑、假释等工

作和电子政务等领域有很好的应用前景。本文提出了第一个非交互、紧凑的 CL-SDVMS 方案，经证明方案满足强壮性、不可伪造性、不可传递性和签名源隐匿性。另外，该方案的实施所需计算量与通信量都很小，非常适合计算资源、网络带宽受限的新型无线网络环境。接下来的工作是构造无需双线性对的高效 CL-SDVMS 方案。

参考文献：

[1] AL-RIYAMI S, PATERSON K G. Certificateless public key cryptography[C]//ASIACRYPT 2003, LNCS 2894, Springer-Verlag.c2003: 452-473.

[2] YUM D H, LEE P J. Generic construction of certificateless encryption[C]//ICCSA 2004. LNCS 3043, Springer-Verlag, c2004:802-811.

[3] HE D B, HUANG B, CHEN J H. New certificateless short signature scheme[J]. Information Security IET, 2013, 7(2):113-117.

[4] YUAN Y, WANG C. Certificateless signature scheme with security enhanced in the standard model [J]. Information Processing Letters, 2014, 114, 492-499.

[5] DU H Z, WEN Q Y. Security analysis of two certificateless short signature schemes [J]. IET Information Security, 2014, 8(4): 230-233.

[6] CHEN Y C, TSO R, HORNG G, et al. Strongly secure certificateless signature: cryptanalysis and improvement of two schemes [J]. Journal of Information Science and Engineering, 2015, 31: 297-314.

[7] YEH K H, TSAI K Y, FAN C Y. An efficient certificateless signature scheme without bilinear pairings[J]. Multimed Tools Appl. Doi: 10.1007/s11042-014-2154-4.

[8] SEO S H, NABEEL M, DING X Y, et al. An efficient certificateless encryption for secure data sharing in public clouds[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(9):2107-2119.

[9] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifier proofs and their applications[C]//Advances in Cryptology-Eurocrypt 1996. LNCS 1070, Berlin, Springer-Verlag, c1996: 142-154.

[10] STEINFELD R, BULL L, WANG H, PIEPRZYK J .Universal designated verifier signatures[C]//Advanced in Asiacrypt'03, Berlin: Springer-Verlag, c2003: 523-542.

[11] HUANG X Y, SUSILO W, MU Y and ZHANG F T. Certificateless designated verifier signature schemes[C]//SNDS 2006, IEEE Computer, c2006: 15-19.

[12] CHEN H, SONG R S, ZHANG F T, et al. An efficient certificateless short designated verifier signature scheme[C]//WiCOM, IEEE, c2008: 1-6.

[13] HE D B, CHEN J H. An efficient certificateless designated verifier signature scheme[J]. International Arab Journal of Information Technology, 2013, 10(4): 389-396.

[14] 李继国, 钱娜, 黄欣沂, 等. 基于证书强指定验证者签名方案[J]. 计算机学报, 2012, 35(8): 1579-1587.
LI J G, QIAN N, HUANG X Y，et al. Certificate-based strong designated verifier signature scheme[J]. Chinese Journal of Comupters, 2012, 35(8): 1579-1587.

[15] MING Y, SHEN X Q, WANG Y M. Certificateless universal designated verifier signature schemes[J]. The Journal of China Universities of Posts and Telecommunications, 2007,14(3): 85-90.

[16] DU H Z, WEN Q Y. Efficient certificateless designated verifier signatures and proxy signatures[J]. Chinese Journal of Electronics, 2009, 18(1): 95-100.

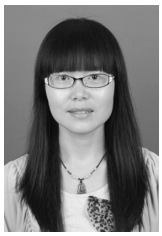
[17] HAFIZUL I S, BISWAS G P. Certificateless strong designated verifier multisignature scheme using bilinear pairings[C]//International Conference on Advances in Computing, Communications and Informatics. c2012: 540-546.

[18] 张玉磊, 周冬瑞, 李臣意, 等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2015, 36(2): 1-8.
ZHANG Y L, ZHOU D R, LI C Y, et al. Efficient certificateless aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2015, 36(2): 1-8.

[19] ITAKURA K and NAKAMURA K. A public-key cryptosystem suitable for digital multisignatures[J]. NEC Research and Development, 1983, (71):1-8.

[20] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(4): 213-241.

作者简介：



杜红珍（1978-），女，陕西扶风人，博士，宝鸡文理学院副教授，主要研究方向为密码学、物联网安全和数字签名技术。

温巧燕（1959-），女，陕西西安人，北京邮电大学教授、博士生导师，主要研究方向为密码学与信息安全。