一种基于无证书的多方合同签署协议的安全性分析与改进

杨小东*① 李梅娟① 任宁宁① 田 甜① 王彩芬②
①(西北师范大学计算机科学与工程学院 兰州 730070)
②(深圳技术大学大数据与互联网学院 深圳 518118)

摘 要：2019年，曹等人(doi: 10.11999/JEIT190166)提出了一个适用于多方合同签署环境中高效的无证书聚合签名方案，并证明了该方案在随机预言模型下存在不可伪造性。然而，通过安全性分析发现，该方案无法抵抗替换公钥攻击和内部签名者的联合攻击。为了解决上述安全缺陷，该文提出一个改进的无证书聚合签名方案。新方案不仅在随机预言模型下基于计算性Diffie-Hellman问题满足不可伪造性，同时也能够抵抗联合攻击。

关键词：无证书聚合签名；联合攻击；不可伪造性；合同签署
中图分类号：TN918; TTP309.7 **文献标识码**：A **文章编号**：1009-5896(2022)10-3627-08
DOI: 10.11999/JEIT210878

Security Analysis and Improvement of a Multi-party Contract Signing Protocol Based on Certificateless

YANG Xiaodong① LI Meijuan① REN Ningning① TIAN Tian① WANG Caifen②
①(*College of Computer Science and Engineering, Northwest Normal University, Lanzhou* 730070, *China*)
②(*College of Big Data and Internet, Shenzhen Technology University, Shenzhen* 518118, *China*)

Abstract: In 2019, CAO et al. (doi: 10.11999/JEIT190166) proposed an efficient certificateless aggregate signature scheme which is suitable for multi-party contract signing environment. They demonstrated that their scheme is unforgeable under the random oracle model. However, by the security analysis, it is found that their scheme can not resist public key substitution attacks and coalition attacks of internal signers. In order to solve the above security defects, an improved certificateless aggregate signature scheme is proposed. The new scheme not only satisfies the unforgeability based on the computational Diffie-Hellman problem under the random oracle model, but also resists coalition attacks.

Key words: Certificateless aggregate signature; Coalition attack; Unforgeability; Contract signing

1 引言

随着信息技术的发展，人们追求更加便捷和高效的管理方式，电子合同在这一趋势下出现并得到广泛应用[1]。电子合同因其高效便捷、成本较低和管理简易方便等特点，在规范电子商务行为、维护市场秩序、促进电子商务领域的持续健康发展等方面十分有利[2]。然而，在电子合同给商业交流带来便捷的同时，也存在联网环境下的合同签署问题。通常，利用数字证书和传统公钥签名等技术进行认证与签署会存在证书管理问题[3]。为解决这类问题，无证书签名方案开始被应用在电子合同签署领域[4]。

无证书密码体制[5–8]能够同时解决基于身份的签名存在的密钥托管问题和传统公钥体制固有的证书管理问题。聚合签名[9]能够将多个签名聚合生成一个签名，有效缩短签名的长度，减少数据的通信带宽和签名验证开销。在无证书签名和聚合签名基础上提出的无证书聚合签名，结合了二者的优势，被广泛应用于多用户场景[10,11]。目前，国内外学者已经提出了一系列无证书聚合签名方案[10–15]，但这些方案大多都面临内部签名者联合攻击[16,17]的风险。另外，一些方案也不能抵抗类型Ⅰ攻击或类型Ⅱ攻击[12,15]。因此，研究同时抵抗类型Ⅰ攻击、类型Ⅱ攻击和联合攻击的无证书聚合签名方案具有重要的意义和价值。

收稿日期：2021-08-26；改回日期：2022-03-07；网络出版：2022-04-08
*通信作者： 杨小东 y200888@163.com
基金项目：国家自然科学基金(61662069，61562077)，中国博士后科学基金(2017M610817)，兰州市科技计划项目(2013-4-22)，西北师范大学青年教师科研能力提升计划(NWNU-LKQN-14-7)
Foundation Items: The National Natural Science Foundation of China (61662069, 61562077), China Postdoctoral Science Foundation (2017M610817), The Science and Technology Project of Lanzhou City (2013-4-22), The Foundation of the Young Teacher's Scientific Research Ability Promotion of Northwest Normal University (NWNU-LKQN-14-7)

近年来，越来越多的学者开始研究无证书聚合签名方案的安全性分析与改进，并给出了一些攻击和改进方法，对同类的无证书聚合签名安全性研究有深远意义[16–18]。2019年，曹素珍等人[19]提出了一种适用于多方合同签署的无证书聚合签名方案(简称曹方案)，并在随机预言模型下证明了该方案存在不可伪造性。然而，本文通过2类攻击对曹方案进行了安全性分析，证明该方案在替换公钥攻击和内部签名者的联合攻击均有安全缺陷。为了克服曹方案中的安全问题，设计了一个改进的无证书聚合签名方案，其安全性规约为计算性Diffie-Hellman (Computational Diffie-Hellman, CDH)[20]假设。分析表明，改进方案不仅能抵抗类型Ⅰ攻击和类型Ⅱ攻击，还能抵抗签名者内部的联合攻击。

2 预备知识

2.1 双线性对

假设G_1为加法循环群，G_2为乘法循环群，群G_1和G_2的阶皆为素数q，P是G_1的一个生成元。$e:G_1\times G_1\to G_2$是满足以下性质的一个双线性映射[20]。

(1) 双线性：对任意$a,b\in Z_q^*$，存在$e(aP,bP)=e(P,P)^{ab}$。

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

(3) 可计算性：对任意$P,Q\in G_1$，可计算$e(P,Q)$。

2.2 困难问题假设

已知$(P,aP,bP)\in G_1$，对于未知的$a,b\in Z_q^*$，CDH问题是计算$abP\in G_1$。

定义1 若没有一个多项式时间算法能以不容忽略的概率解决CDH问题，则称CDH假设成立[20]。

3 曹方案的安全性分析

3.1 曹方案回顾

曹素珍等人[19]构造的无证书聚合签名方案包括11个算法，描述如下：

(1) 系统初始化。给定安全参数k，密钥生成中心(Key Generation Center, KGC)首先选择一个双线性映射$e:G_1\times G_1\to G_2$，其中G_1为由生成元P生成的椭圆曲线加法群，阶为素数$q\geq 2k$，G_2为具有相同阶q的椭圆曲线乘法群。然后定义2个单向的Hash函数$H_1:\{0,1\}^*\times G_1\times G_1\to Z_q^*$和$H_2:G_1\times\{0,1\}^*\to G_1$。KGC将随机数$\lambda\in Z_q^*$设置为系统主密钥，并得到系统公钥$P_{\mathrm{T}}=\lambda P$。最后，KGC秘密保管$\lambda$，并公开发布系统参数$\mathrm{params}=\{G_1,G_2,e,q,P,P_{\mathrm{T}},H_1,H_2\}$。

(2) 秘密值生成。用户U_i随机选取$x_i\in Z_q^*$作为自己的秘密值usk_i，计算对应的部分公钥$P_i=x_iP$，并给KGC发送自己的身份ID_i和P_i。

(3) 部分私钥生成。KGC收到来自用户U_i的ID_i和P_i。随机选取$v_i\in Z_q^*$，计算$V_i=v_iP$，$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$和$y_i=v_i+\lambda h_i \mathrm{mod} q$，然后将$V_i$公开发布，并给用户$U_i$秘密发送部分私钥$y_i$。

(4) 用户密钥生成。用户U_i接收到y_i后计算$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$，然后判断等式$y_iP=V_i+h_iP_{\mathrm{T}}$是否成立。若成立，则其公钥设置为$\mathrm{pk}_i=(P_i,V_i)$，私钥为$\mathrm{sk}_i=x_i+y_i$；否则，结束执行。

(5) 临时密钥生成。用户U_i的临时私钥为其随机选择的数$x_i'\in Z_q^*$，临时公钥是由临时私钥计算的$P_i'=x_i'P$。

(6) 临时公钥承诺。

(a) 用户U_i选择一个随机数k_i作为其辅助值，对临时公钥进行承诺，得到$C_i=\mathrm{Com}(P_i',k_i)$，并广播$C_i$给其余用户；

(b) 用户接收到C_i后，U_i解开承诺，从而用户获取到临时公钥P_i'。

(7) 共享密钥生成。若对任一用户，公钥承诺均已打开。即可得到共享公钥$P_{\mathrm{pub}}=\sum_{i=1}^{n}P_i'$，与之相对应的共享密钥为$x_{\mathrm{pub}}=\sum_{i=1}^{n}x_i'$。

(8) 签名生成。用户U_i按如下步骤完成关于消息M_i的签名：

(a) 选取一个随机数$r_i\in Z_q^*$，并得到$R_i=r_iP$；

(b) 计算$l_i=H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta)$，得到$S_i=r_iP_{\mathrm{pub}}+\mathrm{sk}_i\cdot l_i$；

(c) 设置消息M_i的签名$\sigma_i=(R_i,S_i)$。

(9) 签名验证。输入身份ID_i、公钥$\mathrm{pk}_i=(P_i,V_i)$、共享公钥P_{pub}、消息M_i和签名$\sigma_i=(R_i,S_i)$。验证者通过$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$和$l_i=H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta)$得到$h_i$和$l_i$，再判断等式$e(S_i,P)=e(R_i,P_{\mathrm{pub}})e(P_i+V_i+h_iP_{\mathrm{T}},l_i)$是否成立。若成立，则$\sigma_i$是合法的单个签名，输出valid；否则，输出invalid。

(10) 聚合签名。聚合器对n个消息/签名对$(M_1,\sigma_1=(R_1,S_1)),(M_2,\sigma_2=(R_2,S_2)),\cdots,(M_n,\sigma_n=(R_n,S_n))$进行聚合签名。计算$S=\sum_{i=1}^{n}S_i$，则聚合签名为$\sigma=(R_1,R_2,\cdots,R_n,S)$。

(11) 聚合签名验证。任一聚合签名生成的参与者都可验证聚合签名。已知消息$M_1,M_2,\cdots,M_n$，签名σ和相关参数，验证者执行：

(a) 首先计算$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$和$l_i=H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta),i=1,2,\cdots,n$。$h_i$和$l_i$可以预运算；

(b) 判断等式$e(S,P)=e\left(\sum_{i=1}^{n}R_i,P_{\mathrm{pub}}\right)\prod_{i=1}^{n}e(P_i+V_i+h_iP_{\mathrm{T}},l_i)$是否成立。若成立，验证者输出valid；否则，输出invalid。

3.2 对曹方案的安全性分析

通过以下2类具体的攻击可以发现曹素珍等人[19]提出的无证书聚合签名方案是存在安全缺陷的。

3.2.1 替换公钥攻击

在不失一般性情况下，假定攻击者$\mathcal{A}_1$是一个恶意用户，选择的目标用户身份为ID_n，公钥为$\mathrm{pk}_n=(P_n,V_n)$。攻击者$\mathcal{A}_1$能执行如下的步骤成功伪造一个身份ID_n关于消息M_n的合法聚合签名。

(1) 随机选取$x_n^*\in Z_q^*$，计算$P_n^*=x_n^*P$和$h_n^*=H_1(\mathrm{ID}_n,P_n^*,P_{\mathrm{T}})$；

(2) 随机选取$z\in Z_q^*$，计算$V_n^*=zP-P_n^*-h_n^*P_{\mathrm{T}}$;

(3) 将公钥$\mathrm{pk}_n=(P_n,V_n)$替换为$\mathrm{pk}_n^*=(P_n^*,V_n^*)$;

(4) 随机选取$x_n'^*\in Z_q^*$，计算$P_n'^*=x_n'^*P$和$P_{\mathrm{pub}}=\sum_{i=1}^{n-1}P_i'+P_n'^*$；

(5) 随机选取$r_n^*\in Z_q^*$，计算$R_n^*=r_n^*P$，$l_n^*=H_2(R_n^*,\mathrm{ID}_n||M_n||R_n^*||\Delta)$和$S_n^*=r_n^*P_{\mathrm{pub}}+z\cdot l_n^*$;

(6) 输出消息M_n的签名$\sigma_n^*=(R_n^*,S_n^*)$。$\sigma_n^*=(R_n^*,S_n^*)$很容易被确定是一个合法的签名，因为σ_n^*能通过单个签名验证等式。由于σ_n^*并非来源于签名询问，且系统主密钥λ对$\mathcal{A}_1$是未知的，所以$\mathcal{A}_1$成功伪造了关于身份ID_n和消息M_n的合法签名σ_n^*。

(7) 通过对(ID_i,M_i)进行签名询问，取得相应的签名$\sigma_i=(R_i,S_i)$，$i=1,2,\cdots,n-1$。

(8) 计算$S^*=\sum_{i=1}^{n-1}S_i+S_n^*$，输出关于$\{M_1,M_2,\cdots,M_n\}$的聚合签名$\sigma^*=(R_1,R_2,\cdots,R_n^*,S^*)$。

由于$\sigma_n^*=(R_n^*,S_n^*)$是$\mathcal{A}_1$伪造的合法签名，$\sigma_i=(R_i,S_i),i=1,2,\cdots,n-1$来源于签名询问，伪造的聚合签名$\sigma^*=(R_1,R_2,\cdots,R_n^*,S^*)$能通过验证等式，故$\mathcal{A}_1$成功伪造了一个合法的聚合签名。这证明曹方案无法抵抗替换公钥攻击，即曹方案在第Ⅰ类攻击$\mathcal{A}_1$下是不安全的。以上攻击能够成功的原因在于签名方案构造过程中存在形如$P_i+V_i+h_iP_{\mathrm{T}}=0$的验证等式，能够被线性化分析[8]，通过自己可控的部分公钥得到主密钥对应的部分公钥，进而通过替换公钥伪造出有效签名。

3.2.2 联合攻击

在不失一般性的前提下，假设用户$\mathcal{B}_1$和$\mathcal{B}_2$是两个任意的内部签名者，$\mathcal{B}_1$的身份和公钥为$(\mathrm{ID}_1,\mathrm{pk}_1)$，$\mathcal{B}_2$的身份和公钥为$(\mathrm{ID}_2,\mathrm{pk}_2)$。通过以下步骤，$\mathcal{B}_1$生成了关于$M_1$的非法签名$\sigma_1$，$\mathcal{B}_2$生成了关于$M_2$的非法签名$\sigma_2$，但$\mathcal{B}_1$和$\mathcal{B}_2$合作生成的聚合签名$\sigma$却是合法的。

(1) $\mathcal{B}_1$随机选取$r_1\in Z_q^*$，计算$R_1=r_1P$，并将r_1P_{pub}发送给$\mathcal{B}_2$。

(2) $\mathcal{B}_2$随机选取$r_2\in Z_q^*$，计算$R_2=r_2P$，并将r_2P_{pub}发送给$\mathcal{B}_1$。

(3) $\mathcal{B}_1$收到r_2P_{pub}后，计算$l_1=H_2(R_1,\mathrm{ID}_1||M_1||R_1||\Delta)$和$S_1=r_2P_{\mathrm{pub}}+\mathrm{sk}_1\cdot l_1$，输出$M_1$的签名$\sigma_1=(R_1,S_1)$。

(4) $\mathcal{B}_2$收到r_1P_{pub}后，计算$l_2=H_2(R_2,\mathrm{ID}_2||M_2||R_2||\Delta)$和$S_2=r_1P_{\mathrm{pub}}+\mathrm{sk}_2\cdot l_2$，输出$M_2$的签名$\sigma_2=(R_2,S_2)$。

(5) 聚合器得到关于M_1和M_2的聚合签名$\sigma=(R_1,R_2,S)$，这里$S=S_1+S_2$。

用户$\mathcal{B}_1$生成的单个签名$\sigma_1=(R_1,S_1)$不是一个关于M_1的合法签名。因为$\mathcal{B}_1$的签名σ_1不满足单个签名验证等式，具体为

$$\begin{aligned}e(S_1,P)=&e(r_2P_{\mathrm{pub}}+\mathrm{sk}_1\cdot l_1,P)\\=&e(r_2P_{\mathrm{pub}}+(x_1+y_1)l_1,P)\\=&e(R_2,P_{\mathrm{pub}})e(P_1+V_1+h_1P_{\mathrm{T}},l_1)\\\neq&e(R_1,P_{\mathrm{pub}})e(P_1+V_1+h_1P_{\mathrm{T}},l_1)\end{aligned}$$

类似地，$\mathcal{B}_2$生成的$\sigma_2=(R_2,S_2)$也不是一个关于M_2的合法签名。但二者生成的聚合签名$\sigma=(R_1,R_2,S)$却是关于M_1和M_2的合法签名，因为σ满足聚合签名验证等式，具体为

$$\begin{aligned}e(S,P)=&e(r_2P_{\mathrm{pub}}+\mathrm{sk}_1\cdot l_1+r_1P_{\mathrm{pub}}+\mathrm{sk}_2\cdot l_2,P)\\=&e\left(\sum_{i=1}^{2}r_iP_{\mathrm{pub}},P\right)e\left(\sum_{i=1}^{2}(\mathrm{sk}_i\cdot l_i),P\right)\\=&e\left(\sum_{i=1}^{2}R_i,P\right)\prod_{i=1}^{2}e\left(\mathrm{sk}_i\cdot P,l_i\right)\\=&e\left(\sum_{i=1}^{2}R_i,P\right)\prod_{i=1}^{2}e(P_i+V_i+h_iP_{\mathrm{T}},l_i)\end{aligned}$$

由上述分析可知，$\mathcal{B}_1$和$\mathcal{B}_2$能通过非法的单个签名合作得到一个合法的聚合签名，即曹方案对于签名者内部的联合攻击也是不安全的。

4 改进的无证书聚合签名方案

4.1 方案描述

(1) 系统初始化、秘密值生成与曹方案中所描述的算法相同，但在系统初始化算法中增加了2个单向的Hash函数$H_0:\{0,1\}^*\times G_1\times G_1\to Z_q^*$，$H_3:\{0,1\}^*\to\{0,1\}^l$，需要注意$l\in Z_q^*$是$H_3$输出长度的固定值，其值设置为$G_1$中一个元素的长度。

(2) 部分密钥生成。KGC随机选择$v_i\in Z_q^*$，首先计算$V_i=v_iP$，$h_i'=H_0(\mathrm{ID}_i,V_i,P_{\mathrm{T}})$和$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$，然后计算$y_i=h_i'(v_i+\lambda h_i)\mathrm{mod}q$，最后将$V_i$公开发布，并给$U_i$秘密发送部分私钥$y_i$。

(3) 用户密钥生成。用户U_i接收到y_i后计算$h_i'=H_0(\mathrm{ID}_i,V_i,P_{\mathrm{T}})$和$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$，然后判断等式$y_iP=h_i'(V_i+h_iP_{\mathrm{T}})$是否成立。若成立，则

将公钥设置为$\mathrm{pk}_i=(P_i,V_i)$，私钥为$\mathrm{sk}_i=x_i+y_i$；否则，结束执行。

(4) 临时密钥生成、临时公钥承诺、共享密钥生成、签名与曹方案中所描述的算法相同。

(5) 验证。输入身份ID_i、公钥$\mathrm{pk}_i=(P_i,V_i)$、共享公钥P_{pub}、消息M_i和签名$\sigma_i=(R_i,S_i)$。验证者通过$h_i'=H_0(\mathrm{ID}_i,V_i,P_{\mathrm{T}})$，$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$和$l_i=H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta)$得到$h_i'$，$h_i$和$l_i$。再判断等式$e(S_i,P)=e(R_i,P_{\mathrm{pub}})e(P_i+h_i'(V_i+h_iP_{\mathrm{T}}),l_i)$是否成立。若成立，则$\sigma_i$是合法的单个签名，输出valid；否则，输出invalid。

(6) 聚合签名。聚合器对n个消息签名对$(M_1,\sigma_1=(R_1,S_1)),(M_2,\sigma_2=(R_2,S_2)),\cdots,(M_n,\sigma_n=(R_n,S_n))$进行聚合签名。计算$S=H_3(e(S_1,P),e(S_2,P),\cdots,e(S_n,P))$，输出聚合签名为$\sigma=(R_1,R_2,\cdots,R_n,S)$。

(7) 聚合签名验证。每一个聚合签名的参与者均可以验证聚合签名，输入消息$M_1,M_2,\cdots,M_n$，签名σ和相关参数。验证者计算$h_i'=H_0(\mathrm{ID}_i,V_i,P_{\mathrm{T}})$，$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$和$l_i=H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta)$，$i=1,2,\cdots,n$，判断等式$S=H_3(e(R_1,P_{\mathrm{pub}})e(P_1+h_1'(V_1+h_1P_{\mathrm{T}}),l_1),\cdots,e(R_n,P_{\mathrm{pub}})e(P_n+h_n'(V_n+h_nP_{\mathrm{T}}),l_n))$成立与否。若成立，输出valid；否则，输出invalid。

4.2 正确性分析

计算$h_i'=H_0(\mathrm{ID}_i,V_i,P_{\mathrm{T}})$，$h_i=H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$和$l_i=H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta)$，其中$i=1,2,\cdots,n$。

首先验证单个消息的签名是否满足验证等式$e(S_i,P)=e(R_i,P_{\mathrm{pub}})e(P_i+h_i'(V_i+h_iP_{\mathrm{T}}),l_i)$。因为存在

$$\begin{aligned}e(S_i,P)=&e(r_iP_{\mathrm{pub}}+\mathrm{sk}_i\cdot l_i,P)\\=&e(r_iP_{\mathrm{pub}},P)e((x_i+y_i)l_i,P)\\=&e(r_iP,P_{\mathrm{pub}})e((x_i+y_i)P,l_i)\\=&e(R_i,P_{\mathrm{pub}})e(P_i+h_i'(V_i+h_iP_{\mathrm{T}}),l_i)\end{aligned}$$

故可验证单个签名的正确性；

然后验证$S=H_3(e(R_1,P_{\mathrm{pub}})e(P_1+h_1'(V_1+h_1P_{\mathrm{T}}),l_1),\cdots,e(R_n,P_{\mathrm{pub}})e(P_n+h_n'(V_n+h_nP_{\mathrm{T}}),l_n))$是否成立。因为存在

$$\begin{aligned}S=&H_3(e(S_1,P),e(S_2,P),\cdots,e(S_n,P))\\=&H_3(e(R_1,P_{\mathrm{pub}})e(P_1+h_1'(V_1+h_1P_{\mathrm{T}}),l_1),\\&\cdots,e(R_n,P_{\mathrm{pub}})e(P_n+h_n'(V_n+h_nP_{\mathrm{T}}),l_n))\end{aligned}$$

故可验证聚合签名的正确性。

4.3 安全性分析

定理1 在随机预言模型中，若一个类型Ⅰ攻击者$\mathcal{A}_1$在多项式时间内能够通过执行$q_i(i=1,2,3)$次哈希询问、q_{psk}次部分私钥询问、q_{pk}次公钥询问、q_{usk}次秘密值询问、q_{rep}次公钥替换询问和q_{s}次签名询问，以一个不可忽略的优势ε_1成功伪造出签名，那么存在挑战者C能够以不可忽略的优势ε_1'求解出CDH问题。

证明 假定C收到CDH问题的实例$(P,aP,bP)\in G_1$，其目的是得到abP。为此，C扮演$\mathcal{A}_1$的挑战者并将它作为子程序与之进行交互。假定目标用户为ID^*。

(1) 初始化阶段。C执行系统初始化，得到系统参数$\mathrm{params}=\{G_1,G_2,e,q,P,P_{\mathrm{T}},H_0,H_1,H_2,H_3\}$和主密钥$\lambda$，其中$P_{\mathrm{T}}=aP(a\in Z_q^*)$。另外，令$P_{\mathrm{pub}}=P_{\mathrm{T}}$为用户的共享公钥，秘密保存$\lambda$，并将params和$P_{\mathrm{pub}}$发送给$\mathcal{A}_1$。为避免对各个预言机询问的非连续应答，$C$维护初始状态下为空的列表$L_0,L_1,L_2,L_3,L_{\mathrm{X}},L_{\mathrm{D}},L_{\mathrm{PK}}$。

(2) 询问阶段。$\mathcal{A}_1$进行多项式有界次适应性询问。

(a) H_0询问。为响应$\mathcal{A}_1$的H_0询问，C维持记录项为$(\mathrm{ID}_i,V_i,P_{\mathrm{T}},h_i')$的列表$L_0$。当$C$收到$\mathcal{A}_1$对$H_0(\mathrm{ID}_i,V_i,P_{\mathrm{T}})$的询问时，若$(\mathrm{ID}_i,V_i,P_{\mathrm{T}},h_i')$在列表$L_0$中存在，则返回$h_i'$给$\mathcal{A}_1$；否则，$C$随机选择$h_i'\in Z_q^*$，将$(\mathrm{ID}_i,V_i,P_{\mathrm{T}},h_i')$加入列表$L_0$，并返回$h_i'$给$\mathcal{A}_1$。

(b) H_1询问。为响应$\mathcal{A}_1$的H_1询问，C维持记录项为$(\mathrm{ID}_i,P_i,P_{\mathrm{T}},h_i)$的列表$L_1$。当$C$收到$\mathcal{A}_1$对$H_1(\mathrm{ID}_i,P_i,P_{\mathrm{T}})$的询问时，若$(\mathrm{ID}_i,P_i,P_{\mathrm{T}},h_i)$在列表$L_1$中存在，则返回$h_i$给$\mathcal{A}_1$；否则，$C$随机选择$h_i\in Z_q^*$，将$(\mathrm{ID}_i,P_i,P_{\mathrm{T}},h_i)$加入到列表$L_1$，并返回$h_i$给$\mathcal{A}_1$。

(c) H_2询问。为响应$\mathcal{A}_1$的H_2询问，C维持记录项为$(\mathrm{ID}_i,M_i,R_i,\Delta,l_i)$的列表$L_2$。当$C$收到$\mathcal{A}_1$对$H_2(R_i,\mathrm{ID}_i||M_i||R_i||\Delta)$的询问时，查询列表$L_2$，若$(\mathrm{ID}_i,M_i,R_i,\Delta,l_i)$在列表$L_2$中存在，则返回$l_i$给$\mathcal{A}_1$；否则，$C$随机选择$t\in Z_q^*$，设置$l_i=tP$，返回$l_i$给$\mathcal{A}_1$，并将$(\mathrm{ID}_i,M_i,R_i,\Delta,l_i)$加入到列表$L_2$。

(d) 秘密值询问。为响应$\mathcal{A}_1$的秘密值询问，C维持记录项为(ID_i,P_i,x_i)的列表L_{X}。当收到$\mathcal{A}_1$对ID_i的秘密值询问时，C检查列表L_{X}是否包含x_i。若有，将x_i返回给$\mathcal{A}_1$。否则，若$\mathrm{ID}_i\neq\mathrm{ID}^*$，$C$随机选择$x_i\in Z_q^*$，计算$P_i=x_iP$，将$x_i$返回给$\mathcal{A}_1$，并将$(\mathrm{ID}_i,P_i,x_i)$加入到列表$L_{\mathrm{X}}$；若$\mathrm{ID}_i=\mathrm{ID}^*$，结束游戏。

(e) 部分私钥询问。为响应$\mathcal{A}_1$的部分私钥询问，C维持记录项为$(\mathrm{ID}_i,h_i,h_i',V_i,y_i)$的列表$L_{\mathrm{D}}$。当收到$\mathcal{A}_1$对$\mathrm{ID}_i$的部分私钥询问时，$C$检查列表$L_{\mathrm{D}}$是否包含$y_i$。若有，将$y_i$返回给$\mathcal{A}_1$；否则，若$\mathrm{ID}_i\neq\mathrm{ID}^*$，$C$随机选择$y_i\in Z_q^*$，计算$V_i=\dfrac{y_i}{h_i'}P-h_iP_{\mathrm{T}}$，将$y_i$返回给$\mathcal{A}_1$，并将$(\mathrm{ID}_i,h_i,h_i',V_i,y_i)$加入到列表$L_{\mathrm{D}}$；否则，结束游戏。

(f) 公钥询问。为响应$\mathcal{A}_1$的公钥询问，C维持记录项为(ID_i,P_i,V_i)的列表L_{PK}。当收到$\mathcal{A}_1$对ID_i的

公钥询问时，C检查列表L_{PK}，若发现L_{PK}中存在ID_i的公钥记录，将(P_i, V_i)返回给$\mathcal{A}_1$；否则，在执行了秘密值询问和部分私钥询问后，用询问返回值刷新L_{PK}，同时返回(P_i, V_i)给$\mathcal{A}_1$。

(g) 公钥替换询问。$\mathcal{A}_1$能够使用(P_i^*, V_i^*)替换ID_i的公钥(P_i, V_i)。

(h) 签名询问。对于收到的$\mathcal{A}_1$对ID_i的签名询问，C首先检查是否有$\mathrm{ID}_i = \mathrm{ID}^*$。若有，结束游戏；否则，$C$正常签名，选取随机数$b \in Z_q^*$，得到$R_i = bP$和$S_i = bP_{\mathrm{pub}} + \mathrm{sk}_i \cdot l_i$。$C$生成签名$\sigma_i = (R_i, S_i)$，并用$\sigma_i$响应$\mathcal{A}_1$。

(3) 伪造阶段。询问结束时，$\mathcal{A}_1$输出了一个伪造签名$(\mathrm{ID}^*, \sigma^* = (R_i^*, S_i^*))$。在以上询问中，不得询问$\mathrm{ID}^*$的完整私钥，$\mathrm{ID}^*$不能是已被替换公钥的那个身份，同时输出的$\sigma^*$不能是伪造者对$\mathrm{ID}^*$签名询问的应答。$C$通过$L_{\mathrm{PK}}$得到$(P_i^*, V_i^*)$，调用$H_2$预言机得到$t$，输出$abP = S_i^* - tP_i^* - th_i' V_i^* - h_i' h_i taP$作为CDH问题实例的解答。原因如下：

$$\begin{aligned} e(S_i^*, P) =& e(R_i^*, P_{\mathrm{pub}}) e(P_i^* + h_i'(V_i^* + h_i P_{\mathrm{T}}), l_i) \\ =& e(R_i^*, P_{\mathrm{pub}}) e(P_i^*, l_i) e(h'_i V_i^*, l_i) e(h_i' h_i P_{\mathrm{T}}, l_i) \\ =& e(bP, aP) e(P_i^*, tP) e(h_i' V_i^*, tP) \\ & \cdot e(h_i' h_i aP, tP) \\ =& e(abP, P) e(tP_i^*, P) e(th_i' V_i^*, P) \\ & \cdot e(h_i' h_i taP, P) \end{aligned}$$

综上所述，若$\mathcal{A}_1$成功伪造一个签名，则C便可以通过$\mathcal{A}_1$求得abP，即C成功地解决了CDH问题，而CDH问题是一个困难问题，故本方案具有不可伪造性。　　证毕

定理2　在随机预言模型中，若存在一个类型Ⅱ攻击者$\mathcal{A}_2$在多项式时间内能够通过执行$q_i (i = 1, 2, 3)$次哈希询问、q_{pk}次公钥询问、q_{usk}次秘密值询问和q_{s}次签名询问，以ε_2的概率成功伪造合法的签名，则存在挑战者C能以$\varepsilon_2' \geq \left(1 - \frac{1}{q_3}\right)^{q_{\mathrm{usk}}} \left(1 - (1 - \frac{1}{q_3})^n\right) \left(1 - \frac{q_1}{p}\right) \left(1 - \frac{q_2}{p}\right) \varepsilon_2$的概率解决CDH问题。

证明　假定C收到CDH问题的实例$(P, aP, bP) \in G_1$，其目的是得到abP。为此，C扮演$\mathcal{A}_2$的挑战者并将它作为子程序与之进行交互。假定目标用户为ID^*。

(1) 初始化阶段。C运行系统初始化算法，生成系统参数$\mathrm{params} = \{G_1, G_2, e, q, P, P_{\mathrm{T}}, H_0, H_1, H_2, H_3\}$和系统主密钥$\lambda$，系统公钥$P_{\mathrm{T}} = \lambda P$，用户的共享公钥为$P_{\mathrm{pub}} = \kappa P$(其中$\kappa \in Z_q^*$)，公开params，并将$\lambda$和$P_{\mathrm{pub}}$发送给$\mathcal{A}_2$。为保证对各个预言机询问的连续应答，$C$维护初始状态下为空的列表$L_0, L_1, L_2, L_3, L_{\mathrm{X}}, L_{\mathrm{D}}, L_{\mathrm{PK}}$。

(2) 询问阶段。$\mathcal{A}_2$进行多项式有界次适应性询问。相较于$\mathcal{A}_1$询问阶段，在此阶段中，少了公钥替换询问，在H_2询问和公钥询问中有所不同，其他部分不变。

(a) H_2询问。当C收到$\mathcal{A}_2$对$H_2(R_i, \mathrm{ID}_i || M_i || R_i || \Delta)$的询问时，查询列表$L_2$，若$(\mathrm{ID}_i, M_i, R_i, \Delta, l_i)$在列表$L_2$中存在，则返回$l_i$给$\mathcal{A}_2$；否则，$C$随机选择$b \in Z_q^*$，设置$l_i = bP$，返回$l_i$给$\mathcal{A}_2$，并将$(\mathrm{ID}_i, M_i, R_i, \Delta, l_i)$加入到列表$L_2$。

(b) 公钥询问。当C收到$\mathcal{A}_2$对ID_i的公钥询问时，C检查列表L_{PK}，若发现L_{PK}中存在ID_i的公钥记录，将(P_i, V_i)返回给$\mathcal{A}_2$；否则，随机选择$a \in Z_q^*$，计算$P_i = aP$，再执行部分私钥询问，刷新L_{PK}，同时返回(P_i, V_i)给$\mathcal{A}_2$。

(3) 伪造阶段。询问结束时，$\mathcal{A}_2$输出了一个伪造签名$(\mathrm{ID}^*, \sigma^* = (R_i^*, S_i^*))$。在以上询问中，$\mathrm{ID}^*$的秘密值不能被询问，且输出的$\sigma^*$不能是伪造者对$\mathrm{ID}^*$身份下签名询问的应答。$C$调用$H_2$预言机得到$l_i = bP$，通过$L_{\mathrm{D}}$得到$y_i^*$，输出$abP = S_i^* - \kappa R_i^* - y_i^* P$作为CDH问题实例的解答。原因如下：

$$\begin{aligned} e(S_i^*, P) =& e(R_i^*, P_{\mathrm{pub}}) e(P_i^* + h_i'(V_i^* + h_i P_{\mathrm{T}}), l_i) \\ =& e(R_i^*, P_{\mathrm{pub}}) e(P_i^*, l_i) e(h_i'(V_i^* + h_i P_{\mathrm{T}}), l_i) \\ =& e(R_i^*, \kappa P) e(aP, bP) e(y_i^* P, bP) \\ =& e(\kappa R_i^*, P) e(abP, P) e(y_i^* bP, P) \end{aligned}$$

综上所述，若$\mathcal{A}_2$成功伪造一个签名，则C可以通过$\mathcal{A}_2$求得abP，即C成功地解决了CDH问题，而CDH问题是一个困难问题，故本方案具有不可伪造性。　　证毕

定理3　若H_3是一个抗碰撞的Hash函数，则本文设计的无证书聚合签名方案在联合攻击下是安全的。

证明　如果参与聚合签名生成的所有单个签名都是合法的，则有

$$e(S_i, P) = e(R_i, P_{\mathrm{pub}}) e(P_i + h_i'(V_i + h_i P_{\mathrm{T}}), l_i), \quad i = 1, 2, \cdots, n$$

对于聚合签名$S = H_3(e(S_1, P), e(S_2, P), \cdots, e(S_n, P))$，存在

$$\begin{aligned} S =& H_3(e(R_1, P_{\mathrm{pub}}) e(P_1 + h_1'(V_1 + h_1 P_{\mathrm{T}}), l_1), \cdots, \\ & e(R_n, P_{\mathrm{pub}}) e(P_n + h_n'(V_n + h_n P_{\mathrm{T}}), l_n)) \end{aligned}$$

即$\sigma = (R_1, R_2, \cdots, R_n, S)$是一个合法的聚合签名。

另外，如果聚合签名$\sigma = (R_1, R_2, \cdots, R_n, S)$是合法的，则存在

$$\begin{aligned} S =& H_3(e(R_1, P_{\mathrm{pub}}) e(P_1 + h_1'(V_1 + h_1 P_{\mathrm{T}}), l_1), \cdots, \\ & e(R_n, P_{\mathrm{pub}}) e(P_n + h_n'(V_n + h_n P_{\mathrm{T}}), l_n)) \\ =& H_3(e(S_1, P), e(S_2, P), \cdots, e(S_n, P)) \end{aligned}$$

由Hash函数H_3的抗碰撞性可知

$$e(S_i,P)=e(R_i,P_{\text{pub}})e(P_i+h_i'(V_i+h_iP_{\text{T}}),l_i),\ i=1,2,\cdots,n$$

即单个签名$\sigma_i=(R_i,S_i)$也是合法的。

由上述分析可知，一个聚合签名是合法的当且仅当所有参与该聚合签名生成的单个签名都是合法的。因此，本文所设计的改进方案能够抵抗联合攻击。 证毕

4.4 性能分析

本小节将通过聚合签名长度、计算开销和安全性进行本文方案的性能分析，并与已有的无证书聚合签名文献[10,14,15,17,19]方案进行比较，其中文献[17]方案是文献[15]方案的改进方案。在聚合签名长度方面，主要是为了检查长度是否固定。计算开销方面考虑了单个签名生成阶段和聚合签名验证阶段的开销，且开销主要考虑了耗时大的2种运算：点乘运算和双线性对运算，这两种运算在Intel Core i5-3470 @ 3.20 GHz的处理器、4 GB内存和Windows 7 操作系统的实验环境下运行时间分别为3.740 ms和11.515 ms[11]。在安全性方面，检查方案是否能够抵抗类型 I 攻击、类型 II 攻击和联合攻击。

为了便于说明，用符号s和e分别代表1次点乘运算和1次双线性对运算，$|G_1|$代表G_1中一个元素的长度，n代表生成聚合签名的参与者个数。表1列出了本文方案与其他几个无证书聚合签名方案的性能比较。图1比较了参与者个数n以20为增量从20增加到100时，本文方案与其他几个方案在聚合签名验证阶段的时间开销。

表 1 几个无证书聚合签名方案的性能比较

	聚合签名长度	计算开销		安全性		
		单个签名生成	聚合签名验证	抗类型 I 攻击	抗类型 II 攻击	抗联合攻击
文献[10]方案	$(n+1)\|G_1\|$	$3s$	$3e+2ns$	是	是	否
文献[14]方案	$(n+1)\|G_1\|$	$3s$	$3e+2ns$	是	是	否
文献[15]方案	$(n+1)\|G_1\|$	$4s$	$3e+3ns$	是	否	否
文献[17]方案	$(n+1)\|G_1\|$	$3s$	$2ne+3ns$	是	是	是
文献[19]方案	$(n+1)\|G_1\|$	$2s$	$(n+2)e+ns$	否	是	否
本文方案	$(n+1)\|G_1\|$	$2s$	$2ne+2ns$	是	是	是

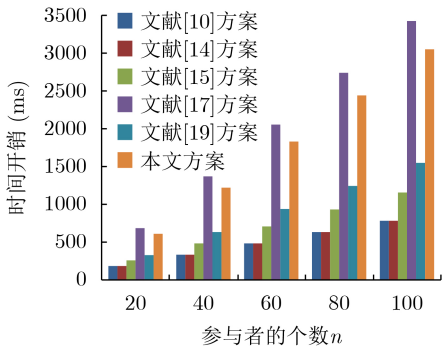

图 1 几个方案的聚合签名验证时间开销比较

由表1可知，上述几个方案的聚合签名长度都是不固定的且具有相同值。从计算开销来看，上述这6个方案在单个签名生成阶段所需要的计算开销差异较小，且其开销都不受参与者个数n的影响。然而，结合图1可知它们在聚合签名验证阶段的计算开销与单个签名生成阶段不同，计算开销都会随着参与者个数n的增加而增加。本文方案虽然在聚合签名验证这一阶段所需的计算开销明显高于文献[10,14,15,19]方案，但它能够抵抗联合攻击，这是文献[10,14,15,19]方案所不具备的安全性能。与同样能够抵抗联合攻击的文献[17]方案相比，本文方案聚合签名验证的计算开销更小。文献[17]方案作为文献[15]方案的改进方案，其在聚合签名验证方面的计算开销也是明显高于文献[15]方案的。通过对比，可以发现抗联合攻击这一安全性能的实现是以增加聚合签名验证的开销为代价的。另外签署方具备一定的计算能力，能够接受较大的计算开销。综合考虑，本文所提出的改进方案在多方合同签署环境完全适用。最重要的是，本文的改进方案能够同时解决文献[19]方案中存在的2个安全缺陷。

5 结束语

本文首先对文献[19]的方案进行了安全性分析，通过2类具体的伪造攻击，证明了该方案并不满足不可伪造性。其次针对文献[19]方案所存在的安全问题，设计了一个改进的无证书聚合签名方案。最后在随机预言模型和CDH问题的困难假设下，证明了新方案在类型 I 攻击和类型 II 攻击下存在不可伪造性并且还能够抵抗联合攻击。然而，改进方案存在较多的双线性对运算，计算效率低，使得签名验证开销较大，后期将进一步研究如何设计出更加高效的无证书聚合签名方案。

参 考 文 献

[1] 冯勃. 电子合同在当代合同管理中的应用优势及挑战[J]. 辽宁经济, 2020(3): 44–45. doi: 10.14041/j.cnki.1003-4617.2020.03.017.
FENG Bo. The application advantages and challenges of electronic contracts in contemporary contract management[J]. *Liaoning Economy*, 2020(3): 44–45. doi: 10.14041/j.cnki.1003-4617.2020.03.017.

[2] 蒲天豪, 陈浩天, 李林峻, 等. 基于区块链技术的电子合同应用研究[J]. 网络安全技术与应用, 2021(2): 27–29.
PU Tianhao, CHEN Haotian, LI Linjun, *et al*. Research on the application of electronic contracts based on blockchain technology[J]. *Network Security Technology & Application*, 2021(2): 27–29.

[3] 沈笑天. 电子签章技术下合同证据的真实性分析[J]. 老字号品牌营销, 2020(7): 62–63.
SHEN Xiaotian. The authenticity analysis of contract evidence under electronic signature technology[J]. *Time-honored brand marketing*, 2020(7): 62–63.

[4] 高莹, 吴进喜. 基于区块链的高效公平多方合同签署协议[J]. 密码学报, 2018, 5(5): 556–567. doi: 10.13868/j.cnki.jcr.000265.
GAO Ying and WU Jinxi. Efficient multi-party fair contract signing protocol based on blockchains[J]. *Journal of Cryptologic Research*, 2018, 5(5): 556–567. doi: 10.13868/j.cnki.jcr.000265.

[5] AL-RIYAMI S S and PATERSON K G. Certificateless public key cryptography[C]. The 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, China, 2003: 452–473. doi: 10.1007/978-3-540-40061-5_29.

[6] MEI Qian, ZHAO Yanan, and XIONG Hu. A new provably secure certificateless signature with revocation in the standard model[J]. *Informatica*, 2019, 30(4): 711–728. doi: 10.15388/Informatica.2019.226.

[7] YU Huifang and LI Wen. A certificateless signature for multi-source network coding[J]. *Journal of Information Security and Applications*, 2020, 55: 102655. doi: 10.1016/J.JISA.2020.102655.

[8] 张振超, 刘亚丽, 殷新春, 等. 无证书签名方案的分析及改进[J]. 密码学报, 2020, 7(3): 389–403. doi: 10.13868/j.cnki.jcr.000375.
ZHANG Zhenchao, LIU Yali, YIN Xinchun, *et al*. Analysis and improvement of certificateless signature schemes[J]. *Journal of Cryptologic Research*, 2020, 7(3): 389–403. doi: 10.13868/j.cnki.jcr.000375.

[9] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003: 416–432.

[10] WU Libing, XU Zhiyan, HE Debiao, *et al*. New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment[J]. *Security and Communication Networks*, 2018, 2018: 2595273. doi: 10.1155/2018/2595273.

[11] XU Zhiyan, HE Debiao, KUMAR N, *et al*. Efficient certificateless aggregate signature scheme for performing secure routing in VANETs[J]. *Security and Communication Networks*, 2020, 2020: 5276813. doi: 10.1155/2020/5276813.

[12] 张玉磊, 李臣意, 王彩芬, 等. 无证书聚合签名方案的安全性分析和改进[J]. 电子与信息学报, 2015, 37(8): 1994–1999. doi: 10.11999/JEIT141635.
ZHANG Yulei, LI Chenyi, WANG Caifen, *et al*. Security analysis and improvements of certificateless aggregate signature schemes[J]. *Journal of Electronics & Information Technology*, 2015, 37(8): 1994–1999. doi: 10.11999/JEIT141635.

[13] 罗敏, 孙腾, 张静茵, 等. 两个无证书聚合签名方案的安全性分析[J]. 电子与信息学报, 2016, 38(10): 2695–2700. doi: 10.11999/JEIT151350.
LUO Min, SUN Teng, ZHANG Jingyin, *et al*. Security analysis on two certificateless aggregate signature schemes[J]. *Journal of Electronics & Information Technology*, 2016, 38(10): 2695–2700. doi: 10.11999/JEIT151350.

[14] LI Jiguo, YUAN Hong, and ZHANG Yichen. Cryptanalysis and improvement for certificateless aggregate signature[J]. *Fundamenta Informaticae*, 2018, 157(1/2): 111–123. doi: 10.3233/FI-2018-1620.

[15] 王大星, 滕济凯. 车载网中可证安全的无证书聚合签名算法[J]. 电子与信息学报, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.
WANG Daxing and TENG Jikai. Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc network[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

[16] ZHANG Futai, SHEN Limin, and GE Wu. Notes on the security of certificateless aggregate signature schemes[J]. *Information Sciences*, 2014, 287: 32–37. doi: 10.1016/j.ins.2014.07.019.

[17] 杨小东, 麻婷春, 陈春霖, 等. 面向车载自组网的无证书聚合签名方案的安全性分析与改进[J]. 电子与信息学报, 2019, 41(5): 1265–1270. doi: 10.11999/JEIT180571.
YANG Xiaodong, MA Tingchun, CHEN Chunlin, *et al*. Security analysis and improvement of certificateless aggregate signature scheme for vehicular Ad hoc networks[J]. *Journal of Electronics & Information*

Technology, 2019, 41(5): 1265–1270. doi: 10.11999/JEIT180571.

[18] 谢永, 李香, 张松松, 等. 一种可证安全的车联网无证书聚合签名改进方案[J]. 电子与信息学报, 2020, 42(5): 1125–1131. doi: 10.11999/JEIT190184.
XIE Yong, LI Xiang, ZHANG Songsong, *et al*. An improved provable secure certificateless aggregation signature scheme for vehicular Ad hoc NETworks[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1125–1131. doi: 10.11999/JEIT190184.

[19] 曹素珍, 王斐, 郎晓丽, 等. 基于无证书的多方合同签署协议[J]. 电子与信息学报, 2019, 41(11): 2691–2698. doi: 10.11999/JEIT190166.
CAO Suzhen, WANG Fei, LANG Xiaoli, *et al*. Multi-party contract signing protocol based on certificateless[J]. *Journal of Electronics & Information Technology*, 2019, 41(11): 2691–2698. doi: 10.11999/JEIT190166.

[20] 俞惠芳, 杨波. 可证安全的无证书混合签密[J]. 计算机学报, 2015, 38(4): 804–813. doi: 10.3724/SP.J.1016.2015.00804.
YU Huifang and YANG Bo. Provably secure certificateless hybrid signcryption[J]. *Chinese Journal of Computers*, 2015, 38(4): 804–813. doi: 10.3724/SP.J.1016.2015.00804.

杨小东：男，博士后，教授，研究方向为应用密码学与信息安全.
李梅娟：女，硕士生，研究方向为密码学与信息安全.
任宁宁：女，硕士生，研究方向为车联网安全.
田　甜：女，硕士生，研究方向为可搜索加密.
王彩芬：女，博士，教授，研究方向为信息安全协议与网络安全.

责任编辑：马秀强