计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(4): 1065−1074, 2025

基于 SM9 的支持策略隐藏的可追踪属性签名

周　权[1]　陈民辉[2]　卫凯俊[2]　郑玉龙[1]
[1]（广州大学数学与信息科学学院　广州　510006）
[2]（广州大学计算机科学与网络工程学院　广州　510006）
（zhouqq@gzhu.edu.cn）

Traceable Attribute-Based Signature for SM9-Based Support Policy Hidden

Zhou Quan[1], Chen Minhui[2], Wei Kaijun[2], and Zheng Yulong[1]
[1]（*School of Mathematics and Information Science*, *Guangzhou University*, *Guangzhou* 510006）
[2]（*School of Computer Science and Cyber Engineering*, *Guangzhou University*, *Guangzhou* 510006）

Abstract　Traceable attribute-based signature (TABS) inherits the merits of attribute-based signature and can trace the real identity of the signer through a trusted third party, avoiding the abuse of anonymity of attribute-based signature. At present, there are very few signature-policy attribute-based signature (SP-ABS) schemes that support traceability in one-to-many authentication scenario, and most of the existing schemes suffer from efficiency and security deficiencies, for example, the computational complexity of the verification phase is linearly related to the number of attributes, which is inefficient. Meanwhile, the fact that the policy is provided directly by the verifier to the signer can easily lead to policy privacy leakage. To solve the above problems, a traceable attribute-based signature scheme supporting policy hiding based on SM9 is proposed in this paper. The scheme uses a linear secret sharing scheme (LSSS) with attribute name and attribute value splitting to construct the access structure, supports partial hiding of the policies, and can protect the policy privacy of the verifier while protecting the signer's identity privacy and attribute privacy. In the verification phase, the scheme only requires constant order bilinear pairing operations and exponential operations, which can achieve efficient fine-grained access control. Finally, the scheme is proved to be unforgeable under the random oracle model by the q-strong Diffie-Hellman (q-SDH) hard problem.

Key words　SM9; attribute-based signature; access control; policy hidden; traceability

摘　要　可追踪的基于属性的签名（traceable attribute-based signature, TABS）继承了属性签名的优点，能通过可信第三方追踪签名者的真实身份，避免了属性签名匿名性的滥用. 目前，针对 1 对多认证场景下支持可追踪的签名策略属性签名（signature-policy attribute-based signature, SP-ABS）方案甚少，现有方案大多存在以下不足：验证阶段的计算复杂度与属性个数呈线性关系，运算效率不高，同时策略由验证者直接提供给签名者容易造成策略隐私泄露. 为此，提出一种基于 SM9 的支持策略隐藏的可追踪属性签名方案，该方案采用属性名和属性值拆分的线性秘密共享方案（linear secret sharing scheme, LSSS）构造访问结构，支持策略的部分隐藏，能在保障签名者身份隐私和属性隐私的情况下，保障验证者的策略隐私，在验证阶段只需要常数量级的配对运算和指数运算，能实现高效的细粒度访问控制. 最后通过 q-SDH（q-strong Diffie-Hellman）难题证明了该方案在随机谕言机模型下具有不可伪造性.

关键词　SM9; 属性签名; 访问控制; 策略隐藏; 可追踪性

中图法分类号　TP309

收稿日期: 2023-09-12; **修回日期**: 2024-10-11

基金项目: 国家重点研发计划项目（2021YFA1000600）

This work was supported by the National Key Research and Development Program of China (2021YFA1000600).

DOI: 10.7544/issn1000-1239.202330744 CSTR: 32373.14.issn1000-1239.202330744

属性签名(attribute-based signature, ABS)[1]是一种灵活的密码学工具,能用属性替代身份来标识用户.在ABS方案中,签名者通过访问策略对消息进行签名,验证者验证该签名可以判断签名者是否满足访问策略但不能确定其身份和具体属性,在访问控制中保障了签名用户的隐私性.在后续的研究中,可追踪的属性签名[2]被提出以平衡ABS匿名性的使用.

属性签名和属性加密[3]类似,也可分为签名策略属性签名(signature-police attribute-based signature, SP-ABS)[4-5]和密钥策略属性签名(key-policy attribute-based signature, KP-ABS)[6].对于SP-ABS,属性嵌入在密钥中,访问策略嵌入在签名中,适用于1对多的认证场景,能对不同的访问策略直接提供不同的签名,而无需更新密钥.现有的SP-ABS方案在验证阶段的配对运算或指数运算大多和属性个数关联,导致计算开销巨大.其次,访问策略是由验证者直接提供给签名者签名,容易泄露访问策略当中隐私敏感的信息.因此,设计一个支持策略隐藏且计算高效的SP-ABS方案是有必要的.

SM9是中国商用密码中的标识密码算法标准[7],包括数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法.SM9签名算法通过身份标识用户,是一种安全性和效率都很高的签名方案.基于属性的签名通过属性标识用户,身份也可以看作是属性的一部分,因此SM9签名算法作为基于身份体系下的密码方案,十分适用于属性签名算法的改造.目前,在面向国家密码算法自主可控的战略需求下,尚未有基于SM9的高效SP-ABS方案.

针对上述问题,本文提出一种基于SM9的支持策略隐藏的可追踪属性签名(policy hidden traceable attribute-based signature, PH-TABS)方案.本文的贡献主要有3点:

1)通过采用将属性拆分为名和值的线性秘密共享方案(linear secret sharing scheme, LSSS)构造基于SM9的SP-ABS方案,该方案同时具有策略可隐藏和身份可追踪的功能.

2)通过安全性分析,证明本文方案在随机谕言机模型下具有不可伪造性.

3)通过计算开销对比分析,表明本文方案在验证阶段只需要常数量级的配对运算和指数运算,相较于现有方案有更高的计算效率.其次,实验仿真对比结果也表明本文方案在性能上优于现有方案.

1 相关工作

基于属性的密码方案为数据的细粒度访问控制提供了支持,其中基于属性的加密在发展[8-10]中扩展出了基于属性的签名,Maji等人[1]提出了基于属性的签名定义,但是他们提出的实例很复杂,其中第3个实例被证明是不安全的[11].Xiong等人[12]通过将计算委托给服务器以降低设备的计算开销,使得属性签名可应用于工业物联网.Su等人[13]结合区块链提出一种可撤销的属性签名方案,用于保护电子病历共享系统中的用户隐私.Li等人[14]提出一种多权威机构的基于属性的混合签名方案,保障了边缘计算环境下用户的身份隐私和数据可靠性.张应辉等人[15]在服务器辅助的基础上提出了可验证的属性签名方案.Yang等人[16]利用属性加密和属性签名提出一个医疗数据共享方案.上述基于属性的签名方案着重于解决计算效率和用户隐私等问题,隐藏签名者身份是属性签名的优点,但一些恶意的签名者可以滥用该优点签署任何消息并否认他们的签名行为.因此,可追踪的基于属性的签名方案被不少人重视并提出.Cui等人[17]在车辆特设网络中通过可追溯性和可撤销性扩展了标准的属性签名方案,防止车辆通信受到匿名性滥用的影响.Gu等人[18]在标准模型中提出一种支持单调谓词的可追踪属性签名方案.Belguith等人[19]提出一个新颖的可追踪的属性签名以实现云中匿名认证.李继国等人[20]为防止属性密钥和敏感信息的泄露提出了可追踪的属性基净化签名方案.

在基于属性的访问控制研究中,往往涉及访问策略的使用,然而访问策略在某些情况下可能会包含敏感信息,例如医疗记录中的访问策略“糖尿病AND(医生OR护士)”容易暴露患者可能存在糖尿病相关问题.因此策略隐私也成为了研究人员们关注的重点.Zhang等人[21]将属性表示为属性名和属性值,与密码文本相关的访问策略只包括属性名,从而实现了部分策略隐藏.王悦等人[22]通过合数阶双线性群提出一种基于包含正负及无关值的“与门”的策略隐藏方案.Han等人[23]利用属性拆分的LSSS[21]提出一种可实现撤销和白盒追踪的策略隐藏方案.在属性基的加密机制中,策略由数据拥有者持有并嵌入在加密密文中,需对数据访问者隐藏,在1对多的

认证场景中，策略由验证者持有并提供给签名者签署消息，同样也需要对签名者隐藏.

SM9标识密码算法发展至今已相继成为国际标准和国家标准，但基于SM9构造的属性基签名方案不多. 唐飞等人[24]构造了基于SM9的可追踪属性签名方案. 朱留富等人[25]通过在线/离线技术将高昂的操作预计算，实现轻量级的基于SM9的属性签名方案. 然而文献[24−25]方案均是KP-ABS类型的方案，KP-ABS将策略嵌入到密钥中，属性嵌入到签名中，在面对多种不同签名策略的场景时，需要先变更密钥再生成签名，反观SP-ABS能直接生成不同策略的签名.

综上所述，针对1对多的认证场景，现有的属性签名方案大多存在匿名性滥用、计算开销大、策略隐私容易泄露等问题，本文在SM9签名算法的基础上提出一种支持策略隐藏的可追踪属性签名方案，通过将拆分的LSSS矩阵构造访问结构嵌入到签名中，以及将属性嵌入到密钥中，能实现高效安全的细粒度访问控制.

2 预备知识

本节主要介绍文中用到的相关知识，包括符号约定、双线性映射、q-SDH困难问题、访问结构、线性秘密分享方案和SM9标识签名算法.

2.1 符号约定

本文使用ϑ表示安全参数，N为大素数，$\mathbb{Z}_N$表示整数集合$\mathbb{Z}_N=\{0,1,2,\cdots,N-1\}$，$\{0,1\}^*$表示任意长度的比特串. 加法群上的标量乘运算用$[k]P_i$表示，其中$P_i$是加法群上的生成元，$k\in\mathbb{Z}_N$. $\boldsymbol{M}$是大小为$l\times n$的矩阵，ρ是将$\boldsymbol{M}$的行与属性相关联的函数，$\boldsymbol{M}_i$表示矩阵$\boldsymbol{M}$的第i行. $\mathcal{V}$表示与访问结构$(\boldsymbol{M},\rho)$相关的属性值集合.

2.2 双线性映射

令G_1和G_2是2个N阶加法循环群，G_T是N阶乘法循环群，P_1和P_2分别是G_1, G_2的生成元，ψ表示$G_1\to G_2$的映射，即$\psi(P_2)=P_1$，双线性映射e: $G_1\times G_2\to G_T$满足3个性质.

1）双线性. 对于任意m, $n\in\mathbb{Z}_N$，有以下等式成立：$e([m]P_1,[n]P_2)=e([n]P_1,[m]P_2)=e(P_1,P_2)^{mn}$.

2）非退化性. $e(P_1,P_2)\neq 1$.

3）可计算性. $e(P_1,P_2)$是可以用有效方法计算的.

2.3 q-SDH困难问题

q-SDH困难问题[26]描述如下：令P为G_1的生成元，Q为G_2的生成元，随机选择$c\in\mathbb{Z}_N$并给定一个$q+2$个元素的元组实例$(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)$. 如果没有一个多项式时间算法能以不可忽略的优势$\varepsilon$计算$\left(c,\left[\frac{1}{c+a}\right]P\right)$，则称$q$-SDH问题是困难的.

2.4 访问结构

设置$P=\{P_1,P_2,\cdots,P_n\}$是一组参与实体，如果$\forall B,C$满足$B\in\mathfrak{A}$, $B\subseteq C$则$C\in\mathfrak{A}$，那么集合$\mathfrak{A}\subseteq 2^P$是单调的. 如果一个单调的访问结构$\mathfrak{A}$是由$P$上的非空子集组成的集合，即$\mathfrak{A}\subseteq 2^P\backslash\varnothing$，那么包含在$\mathfrak{A}$中的集合称为授权集，否则称为非授权集.

2.5 线性秘密共享方案

设$A=\{A_1,A_2,\cdots,A_n\}$是属性名集合，n为属性名个数，对于任意$A_i\in A$有属性值$A_i=\{a_{i,1},a_{i,2},\cdots,a_{i,m}\}$，其中$m$为属性名$A_i$的属性值个数. 设$N$是一个大素数，访问结构通过$(\boldsymbol{M},\rho)$表示，其中$\boldsymbol{M}$是大小为$l\times n$的矩阵，$\rho$是一个映射函数，将矩阵$\boldsymbol{M}$的第$i$行$\boldsymbol{M}_i$映射到$A$中的属性名. 定义在$N$上的线性秘密共享方案由以下算法组成：

1）$Share((\boldsymbol{M},\rho),s)\to\{\lambda_i\}_{i\in I}$：设$s$是$A$上需要共享的秘密值，选择随机向量$\boldsymbol{\upsilon}=(s,y_2,\cdots,y_n)$，其中$y_2,\cdots,y_n\in\mathbb{Z}_N$，计算$s$上相应属性名$\rho(i)$的秘密份额$\lambda_i=\boldsymbol{\upsilon}\cdot\boldsymbol{M}_i$.

2）$Reconstruction((\boldsymbol{M},\rho),S)\to\{s\}$：设$S\in\mathfrak{A}$是一个授权集合，对于索引集$I=\{i:\rho(i)\in S\}\subset\{1,2,\cdots,l\}$，存在常数集合$\{\omega_i\in\mathbb{Z}_N\}_{i\in I}$使得$\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\cdots,0)$，因此通过计算$\sum_{i\in I}\omega_i\lambda_i=s$可恢复出秘密.

设$Attr=(I_{\mathcal{H}},\mathcal{H})$为签名者的属性集合，其中$I_{\mathcal{H}}\subseteq A$是签名者的属性名集合，$\mathcal{H}=\{h_i\}_{i\in I_{\mathcal{H}}}$是签名者的属性值集合，定义线性秘密共享方案的访问结构$\gamma=(\boldsymbol{M},\rho,\mathcal{V})$[23]，其中$\rho$将$\boldsymbol{M}_i$映射到$A$中的属性名，每个属性名只出现1次，$\mathcal{V}=\{v_{\rho(i)}\}_{i\in[1,l]}$是与访问结构$(\boldsymbol{M},\rho)$相关的属性值集合. 如果存在$I=\{i:\rho(i)\in S\}\subset\{1,2,\cdots,l\}$满足$(\boldsymbol{M},\rho)$并且对于任意$i\in I$有$h_{\rho(i)}=v_{\rho(i)}$，则认为签名者属性集$Attr$满足访问结构$\gamma$，否则$Attr$不满足$\gamma$. 设$\overline{\gamma}=(\boldsymbol{M},\rho)$为没有属性值集合的不完整访问结构.

2.6 SM9标识签名算法

根据SM9相关标准“GM/T 0044—2016 SM9标识密码算法”[7]，SM9签名算法可以概括为4个算法：

1）系统初始化算法$Setup()$. 输入安全参数κ，选择哈希函数H_1, H_2: $\{0,1\}^*\to\mathbb{Z}_N$，密钥生成中心KGC选择hid为公开的签名私钥生成函数识别符，KGC随机选择$a\in\mathbb{Z}_N$作为主私钥MSK，计算主公钥$MPK=[a]P_2$，公开MPK和系统公共参数$PP=\{G_1,G_2,G_T,P_1,P_2,H_1,$

H_2, hid}, PP 作为以下 3 个算法的默认输入.

2)密钥生成算法 $KeyGen()$. 输入给定用户 A 的身份标识 ID_A 和主私钥 MSK, KGC 计算用户 A 的签名私钥 $SK_A=\left[\frac{a}{H_1(ID_A\|hid,N)+a}\right]P_1$.

3)签名算法 $Sign()$. 输入签名消息 m、用户 A 的私钥 SK_A 和主公钥 MPK. 用户 A 随机选择 $r\in\mathbb{Z}_N$, 计算 $h=H_2(m\|e(P_1,MPK)^r,N)$, $S=[(r-h)]SK_A$, 输出签名 $\sigma=(h,S)$.

4)验证算法 $Verify()$. 输入系统主公钥 MPK、消息 m、用户 A 的身份标识 ID_A 和签名 σ'. 验证者计算 $P=[H_1(ID_A\|hid,N)]P_2+MPK$, 验证 $h=H_2(m\|e(S',P)e(P_1,MPK)^h,N)$ 是否成立, 若成立, 则签名 σ 合法, 否则签名 σ 无效.

3 形式化定义和安全模型

本节主要给出 PH-TABS 方案的形式化定义和安全模型. 方案的系统框架如图 1 所示, 主要包括可信中心(KGC)、验证者以及签名者 3 个部分, 其中签名者和验证者均属于用户的一部分. KGC 负责为用户生成属性私钥 SK_{Use}, 并根据用户签名追踪用户的真实身份 ID_{Use}, 签名者根据验证者提供的消息 m 和访问结构 $\bar{\gamma}=(\boldsymbol{M},\rho)$ 执行签名算法生成签名 σ, 验证者通过用户的签名验证该用户是否满足访问策略, 验证通过返回 accept, 否则返回 reject.

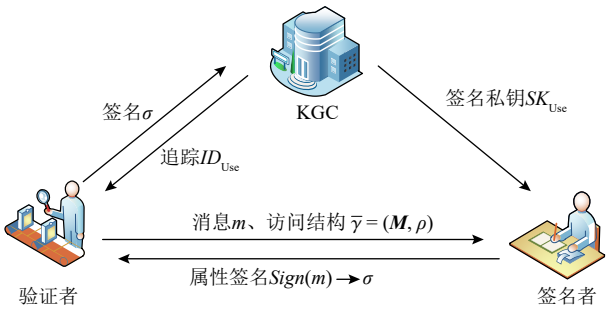


Fig. 1 Framework of PH-TABS scheme

图 1 PH-TABS 方案框架

3.1 方案的形式化定义

PH-TABS 方案由 5 个算法组成:

1)设置算法: $Setup(\vartheta,U)\rightarrow\{PP, MPK, MSK\}$. 输入安全参数 ϑ 和系统属性个数 U, 输出公共参数 PP、主公钥 MPK 和主私钥 MSK, KGC 秘密保存主私钥 MSK.

2)密钥生成算法: $KeyGen(PP, MSK, ID_{Use}, Attr)\rightarrow\{SK_{Use}\}$. 输入公共参数 PP、主私钥 MSK、用户身份 ID_{Use} 和用户属性集 $Attr=(I_{\mathcal{H}},\mathcal{H})$, 输出属性私钥 SK_{Use}.

3)签名算法: $Sign(PP, m, SK_{Use}, \bar{\gamma})\rightarrow\{\sigma\}$. 输入公共参数 PP、消息 m、属性私钥 SK_{Use} 和访问结构 $\bar{\gamma}=(\boldsymbol{M},\rho)$, 输出签名 σ.

4)验证算法: $Verify(PP, MPK, m, \sigma', \gamma)\rightarrow$accept or reject. 输入公共参数 PP、主公钥 MPK、消息 m、签名 σ' 和访问结构 $\gamma=(\boldsymbol{M},\rho,\mathcal{V})$, 若签名验证通过, 输出 accept, 否则输出 reject.

5)追踪算法: $Trace(\sigma)\rightarrow\{ID_{Use}\}$. 输入签名 σ, 输出用户身份 ID_{Use}.

PH-TABS 方案的正确性要求对所有的 $(PP, MPK, MSK)\leftarrow Setup(\vartheta,U)$、所有属性 $Attr\subseteq U$、所有属性私钥 $SK_{Use}\leftarrow KeyGen(PP, MSK, ID_{Use}, Attr)$、所有用户属性满足访问结构 $\bar{\gamma}(Attr)=1$、所有消息 $m\in\{0,1\}^*$、所有签名 $\sigma\leftarrow Sign(PP, m, SK_{Use}, \bar{\gamma})$, 均有 accept$\leftarrow Verify(PP, MPK, m, \sigma, \gamma)$.

3.2 安全模型

在本节中, 定义 PH-TABS 在选择性签名策略和自适应选择消息攻击(selective signing policy and adaptively chosen message attack, SP-CMA)下存在不可伪造的安全模型如下:

1)设置. 伪造者 $\mathcal{F}$ 声明挑战访问策略 δ^* 并将其发送给算法 $\mathcal{B}$. $\mathcal{B}$ 执行系统初始化算法, 公开公共参数 PP 和主公钥 MPK, 秘密保存主私钥 MSK.

2)密钥询问 O_K. 伪造者 $\mathcal{F}$ 自适应查询关于属性集 $Attr$ 的属性私钥, 其中 $\delta^*(Attr)\neq 1$ 并且 $Attr\subseteq U$, 算法 $\mathcal{B}$ 执行密钥生成算法输出属性私钥 SK_{Use} 并发送给 $\mathcal{F}$.

3)签名询问 O_S. 伪造者 $\mathcal{F}$ 询问关于任意访问策略 δ 和消息 m 的签名. $\mathcal{B}$ 执行签名算法, 输出 σ 并发送给 $\mathcal{F}$.

4)伪造. 伪造者 $\mathcal{F}$ 通过挑战访问策略 δ^* 输出关于消息 m^* 的签名 σ^*, 若满足以下条件, 则称 $\mathcal{F}$ 能攻破 PH-ABS 的存在不可伪造安全模型.

①$\mathcal{F}$ 没有询问过任何关于属性集 $Attr^*$ 的密钥, 其中 $\delta^*(Attr^*)=1$.

②$\mathcal{F}$ 没有询问过任何关于访问策略 δ^* 和消息 m^* 的签名.

③σ^* 是一个关于访问策略 δ^* 和消息 m^* 上的有效签名.

定义 1. 如果所有多项式时间伪造者 $\mathcal{F}$ 攻破上述存在不可伪造安全模型的概率是可忽略的, 那么 PH-ABS 在选择性签名策略和自适应选择消息攻击下是存在不可伪造的.

4 方案构造

本节主要给出PH-TABS方案的具体构造.

1) $Setup(\vartheta,U)\rightarrow\{PP, MPK, MSK\}$. KGC执行该算法，初始化系统参数. 给定安全参数ϑ和系统属性个数U，定义系统属性集合$A_i=\{a_{i,1}, a_{i,2}, \cdots, a_{i,m}\}_{i\in[1,|U|]}$，其中$A_i$为属性名，$a_{i,m}$为$A_i$对应的属性值，设置阶均为$N$的加法循环群$G_1$, G_2和乘法循环群G_T; P_1, P_2分别是G_1, G_2的生成元，给定密码杂凑函数H_1, H_2: $\{0, 1\}^*\rightarrow\mathbb{Z}_N^*$，计算群$G_T$中的元素$\mathcal{G}=e(P_1,MPK)$.

KGC选定私钥生成函数识别符hid(hid = 0x01)，随机选择$a\in\mathbb{Z}_N$作为主私钥，计算主公钥$MPK=[a]P_2$.

公开公共参数PP=(N, P_1, P_2, G_1, G_2, hid, $\mathcal{G}$, H_1, H_2, $A_i=\{a_{i,1},a_{i,2},\cdots,a_{i,m}\}_{i\in[1,|U|]}$).

2) $KeyGen(PP, MSK, ID_{\text{Use}}, Attr)\rightarrow\{SK_{\text{Use}}\}$. KGC执行该算法，根据用户属性$Attr$生成私钥$SK_{\text{Use}}$. 算法输入主私钥$MSK$、用户身份$ID_{\text{Use}}\in\{0, 1\}^*$、用户属性集$Attr=(I_{\mathcal{H}},\mathcal{H})$，其中$I_{\mathcal{H}}\subseteq A$是用户的属性名集合，$\mathcal{H}=\{h_i\}_{i\in I_{\mathcal{H}}}$是用户的属性值集合. KGC计算$t_1=H_1(ID_{\text{Use}}\|hid,N)+a$，随机选择$t\in\mathbb{Z}_N$，计算$t_2=(a+t)\cdot t_1^{-1}$，最后计算用户的属性私钥：

$$sk_1=[t_2]P_1,$$
$$sk_2=[ta^{-1}]P_1,$$
$$sk_3=[t]P_1,$$
$$sk_4=H_1(ID_{\text{Use}}\|hid,N),$$

对于任意$i\in I_{\mathcal{H}}$，计算

$$sk_i=[ta^{-1}h_i]P_1.$$

输出$SK_{\text{Use}}=(sk_1, sk_2, sk_3, \text{sk}_4, \{sk_i\}_{i\in I_{\mathcal{H}}})$.

3) $Sign(PP, m, SK_{\text{Use}}, \overline{\gamma})\rightarrow\{\sigma\}$. 验证者给定不完整的访问结构$\overline{\gamma}=(\boldsymbol{M},\rho)$和消息$m\in\{0, 1\}^*$作为输入，签名者执行该算法，继续输入属性私钥$SK_{\text{Use}}$. 首先判断签名者属性是否满足访问结构，即$\overline{\gamma}(I_{\mathcal{H}})=1$，若不满足，算法输出$\perp$，表示签名失败；否则，继续如下计算：

随机选择$r\in\mathbb{Z}_N$，计算群G_T中的元素$w=\mathcal{G}^r$，计算$h=H_2(m\|w, N)$, $L=(r-h) \bmod N$，若$L=0$，重新执行该算法；否则，继续计算

$$\sigma_0=[L]sk_1.$$

令L为访问结构$\overline{\gamma}=(\boldsymbol{M},\rho)$的秘密值，其中$\boldsymbol{M}$是大小为$l\times n$的矩阵，$\rho$是将$\boldsymbol{M}$的行与属性相关联的函数，选择2个随机向量$\boldsymbol{\upsilon}=y_2,\cdots,y_n\in\mathbb{Z}_N$，$\boldsymbol{\eta}=y_{n+2},\cdots,y_{2n}\in\mathbb{Z}_N$. 对于$i\in[1, l]$，计算$\lambda_i=\boldsymbol{\upsilon}\cdot\boldsymbol{M}_i$(表示每个属性所占秘密值的份额)，$\tau_i=\boldsymbol{\eta}\cdot\boldsymbol{M}_i$，其中$\boldsymbol{M}_i$表示$\boldsymbol{M}$的第$i$行向量. 随机选择$d\in\mathbb{Z}_N$，设$I=\{i:\rho(i)\in I_{\mathcal{H}}\}\subset\{1,2,\cdots,l\}$，计算$K=\sum_{i\in I}sk_i$，然后计算：

$$\sigma_1=[sk_4]P_2+MPK,$$
$$\sigma_2=[d]sk_3,$$
$$\sigma_3=[d]sk_2,$$
$$\sigma_i=[\lambda_i]sk_2+[\tau_i d]K.$$

最后，输出签名$\sigma=(h,\sigma_0,\sigma_1,\sigma_2,\sigma_3,\{\sigma_i\}_{i\in I})$.

4) $Verify(PP, MPK, m, \sigma', \gamma)\rightarrow$accept or reject. 验证者执行该算法，验证签名的有效性. 算法输入主公钥MPK，消息m、签名σ'以及访问结构$\gamma=(\boldsymbol{M},\rho,\mathcal{V})$，其中$\mathcal{V}=\{v_{\rho(i)}\}_{i\in[1,l]}$是与访问结构$(\boldsymbol{M},\rho)$相关的属性值. 验证者首先验证

$$e(\sigma'_3,MPK)=e(\sigma'_2,P_2),$$

若等式不成立，算法输出$\perp$，表示验证失败；否则计算群G_T中的元素

$$t=\mathcal{G}^{h'}.$$

设$I=\{i:\rho(i)\in I_{\mathcal{H}}\}\subset\{1,2,\cdots,l\}$，如果$I_{\mathcal{H}}$满足访问结构$\gamma$，则可以找到一组常数$\{\omega_i\in\mathbb{Z}_N\}_{i\in I}$，使得$\sum_{i\in I}\omega_i\lambda_i=L$，$\sum_{i\in I}\omega_i\tau_i=1$，计算

$$W=\sum_{i\in I}[\omega_i]\sigma'_i,$$

$$V=\sum_{i\in I}v_{\rho(i)}.$$

计算群G_T中的元素

$$u=\frac{e(\sigma'_0,\sigma'_1)}{e(W,MPK)e(\sigma'_2,[-V]P_2)},$$

$$w'=u\times t.$$

计算$h_2=H_2(m\|w', N)$，检查等式$h_2=h'$是否成立，成立则表示签名验证通过，算法输出accept，否则输出reject.

5) $Trace(\sigma)\rightarrow\{ID_{\text{Use}}\}$. KGC执行该算法，追踪签名用户的真实身份. 由于$\sigma_1=[sk_4]P_2+MPK$，因此KGC可以在为用户生成密钥时提前预计算σ_1的值，而$sk_4=H_1(ID_{\text{Use}}\|hid,N)$包含用户身份$ID_{\text{Use}}$，KGC可维护二元组列表$(ID_{\text{Use}}, \sigma_1)$. 算法输入用户签名$\sigma$，KGC通过查表即可得到签名用户的真实身份$ID_{\text{Use}}$并输出.

5 正确性分析

若一个诚实用户的属性集满足验证者提出的访问结构，那么该用户的签名有效且可以正确地通过验证算法，正确性分析如下：

当用户的属性集 $Attr=(I_{\mathcal{H}},\mathcal{H})$ 满足访问结构 $\gamma=(\boldsymbol{M},\rho,\mathcal{V})$, 那么该用户的属性名集合 $I_{\mathcal{H}}$ 和属性值集合 $\mathcal{H}=\{h_i\}_{i\in I_{\mathcal{H}}}$ 能通过验证算法正确计算 $w'=\mathcal{G}^r$. 设 $I=\{i:\rho(i)\in I_{\mathcal{H}}\}\subset\{1,2,\cdots,l\}$, 根据 LSSS 的性质可以计算 $\sum_{i\in I}\omega_i\lambda_i=L$, $\sum_{i\in I}\omega_i\tau_i=1$, 然后计算 w'.

$$e(\sigma_0,\sigma_1)=e\left(\left[\frac{L(a+t)}{H_1(ID_{\text{Use}}\|hid,N)+a}\right]P_1,[H_1(ID_{\text{Use}}\|hid,N)+a]P_2\right)=e(P_1,P_2)^{L(a+t)},$$

$$e(W,MPK)=e\left(\sum_{i\in I}[\omega_i]\sigma_i,[a]P_2\right)=e\left(\sum_{i\in I}[\omega_i\lambda_i]sk_2+\sum_{i\in I}[\omega_i\tau_i d]K,[a]P_2\right)=e\left(\left[Lta^{-1}+dta^{-1}\sum_{i\in I}h_i\right]P_1,[a]P_2\right)=e(P_1,P_2)^{Lt}e(P_1,P_2)^{dt\sum_{i\in I}h_i},$$

$$e(\sigma_2,[-V]P_2)=e\left([dt]P_1,\left[-\sum_{i\in I}v_{\rho(i)}\right]P_2\right)=e(P_1,P_2)^{\left[-\sum_{i\in I}v_{\rho(i)}\right]dt},$$

$$w'=u\times t=\frac{e(\sigma_0,\sigma_1)}{e(W,MPK)e(\sigma_2,[-V]P_2)}\times\mathcal{G}^h=\frac{e(P_1,P_2)^{L(a+t)}}{e(P_1,P_2)^{Lt}e(P_1,P_2)^{dt\sum_{i\in I}h_i}e(P_1,P_2)^{\left[-\sum_{i\in I}v_{\rho(i)}\right]dt}}\times\mathcal{G}^h=e(P_1,P_2)^{aL}\times\mathcal{G}^h=\mathcal{G}^{(r-h)}\times\mathcal{G}^h=\mathcal{G}^r,$$

因此, 用户的签名有效且能正确通过验证算法, PH-TABS 方案满足正确性要求.

6 安全性分析

6.1 策略隐藏性

PH-TABS 方案的策略隐藏性主要体现在签名算法和验证算法中. 在签名算法中, 验证者给定签名者不完整的访问结构 $\bar{\gamma}=(\boldsymbol{M},\rho)$, 该访问结构只能通过矩阵 $\boldsymbol{M}$ 和函数 ρ 映射到属性名, 不包含属性名对应的属性值集合 $\mathcal{V}=\{v_{\rho(i)}\}_{i\in[1,l]}$, 因此签名者执行签名算法时无法知道访问结构的具体属性值, 也就无法知道完整的访问策略信息. 在验证算法中, 验证者自身持有完整的访问结构 $\gamma=(\boldsymbol{M},\rho,\mathcal{V})$, 其在验证算法中通过完整的访问结构 γ 验证签名者提供的属性签名是否合法, 只有当签名者的属性名对应的属性值集合 $\mathcal{H}=\{h_i\}_{i\in I_{\mathcal{H}}}$ 满足 $h_{\rho(i)}=v_{\rho(i)}$ 时, 签名验证通过, 否则, 签名不合法. 因此, PH-TABS 方案能实现策略的部分隐藏, 保障验证者的策略隐私.

6.2 抗串通攻击性

属性签名中的串通攻击是指多个属性不满足访问结构的用户试图结合他们的密钥来生成一个有效的签名. 在 PH-TABS 方案的密钥生成算法中, 密钥 SK_{Use} 当中嵌入了随机数 $t\in\mathbb{Z}_N$, t 相当于盲化因子, 这起到了区分用户密钥的作用, 使得不同用户的密钥无法结合. 例如一个访问策略需要满足属性 A 和属性 B, 用户 Alice 拥有属性 A 的密钥 $sk_{\text{Alice},i}=[t_{\text{Alice}}a^{-1}h_A]P_1$, 用户 Bob 拥有属性 B 的密钥 $sk_{\text{Bob},i}=[t_{\text{Bob}}a^{-1}h_B]P_1$, 满足属性 A 和属性 B 的密钥 $sk_{AB,i}=[t_{AB}a^{-1}h_i]P_1$, 而 $t_{\text{Alice}}\neq t_{\text{Bob}}\neq t_{AB}$, 他们无法通过密钥结合的方式形成一个新的密钥. 因此 PH-TABS 方案是满足抗串通攻击性的.

6.3 不可伪造性

定理 1. 如果 q-SDH 问题在 (G_1,G_2) 上成立, 那么 PH-TABS 方案是不可伪造的.

证明. 假设存在一个多项式时间伪造者 $\mathcal{F}$ 能以不可忽略的优势 ε 攻破存在性不可伪造安全, 那么可以构造一个概率多项式时间算法 $\mathcal{B}$ 以不可忽略的优势解决 q-SDH 问题. $\mathcal{B}$ 和 $\mathcal{F}$ 的安全游戏如图 2 所示, 其中 $\mathcal{C}_{q\text{-SDH}}$ 表示 q-SDH 问题, $\mathcal{C}_{\text{SP-CMA}}$ 表示选择性签名策略和自适应选择消息攻击. 安全游戏具体如下:

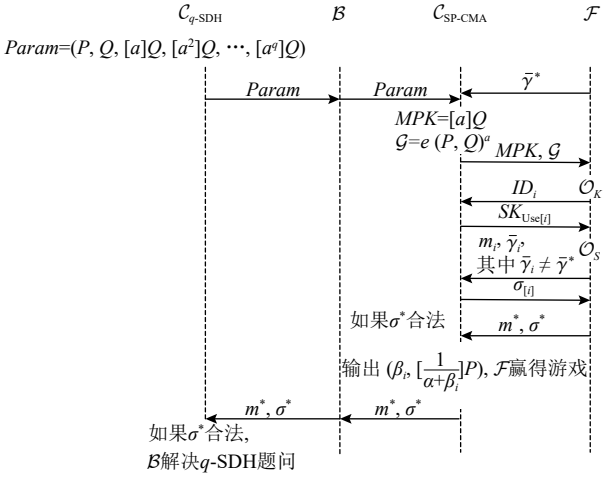


Fig. 2 Security game of PH-TABS scheme

图 2 PH-TABS 方案安全游戏

1)设置. $\mathcal{F}$ 选定挑战访问结构 $\bar{\gamma}^*$ 并发送给 $\mathcal{B}$, $\mathcal{B}$ 获得一个 q-SDH 的随机实例 $(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)$, 其中 $P=\psi(Q)$. 令主私钥 $MSK=a$, 哈希询问: 假设 $\mathcal{F}$ 可以进行 q_{H} 次哈希询问, $\mathcal{B}$ 维护一个空列表 L_1 并记录二元组 (ID_i,β_i), 若 $\mathcal{F}$ 询问关于 ID_i 的哈希值 H_1 已在 L_1 中, $\mathcal{B}$ 直接返回 β_i, 若 ID_i 未曾被询问, 则令

$H_1(ID_i\|hid,N)=\beta_i$并记录(ID_i,β_i)在L_1中. 定义2个多项式：

$$f(X)=\prod_{i=1}^{q-1}(X+\beta_i)=\sum_{i=0}^{q-1}c_iX^i,$$

$$f_i(X)=\frac{f(X)}{X+\beta_i},$$

其中$c_i\in\mathbb{Z}_N$. P_1, P_2分别是G_1和G_2上的生成元, 令$P_1=P$, $P_2=Q$, 然后$\mathcal{B}$计算$MPK=[a]P_2=[a]Q$, $\mathcal{G}=e(P_1,MPK)=e(P,Q)^a$.

2)密钥询问O_{K}. 假设$\mathcal{F}$可以进行q_{K}次密钥询问. $\mathcal{F}$向$\mathcal{B}$询问身份标识为ID_i的签名密钥$SK_{\mathrm{Use}[i]}$, $\mathcal{B}$查询表L_1, 若ID_i不在表中, 则询问失败, $\mathcal{B}$退出游戏. 否则, 设置$t=af(a)$, $\mathcal{B}$计算$SK_{\mathrm{Use}[i]}$为：

$$sk_{[i],1}=\left[\frac{a}{a+\beta_i}+af_i(a)\right]\psi(Q),$$

$$sk_{[i],2}=[f(a)]\psi(Q),$$

$$sk_{[i],3}=[af(a)]\psi(Q),$$

$$sk_{[i],4}=\beta_i,$$

$$sk_{[i],j}=[f(a)h_j]\psi(Q).$$

然后$\mathcal{B}$将ID_i的签名密钥$SK_{\mathrm{Use}[i]}$发送给$\mathcal{F}$.

3)签名询问O_{S}. 假设$\mathcal{F}$可以进行$q-2$次签名询问且属性$Attr_i$一定满足签名策略$\overline{\gamma}(Attr_i)=1$. 设置$r=h+\frac{1}{a}$, $\mathcal{B}$计算$w=\mathcal{G}^r=e(P,Q)^{h+\frac{1}{a}}$, $h=H_2(m_i\|w,N)$, 然后$\mathcal{B}$继续计算$L=r-h=\frac{1}{a}$, 随机选择$d\in\mathbb{Z}_N$, 计算签名$\sigma_{[i]}$如下：

$$\sigma_{[i],0}=[L]sk_{[i],1}=\left[\frac{1}{a+\beta_i}+f_i(a)\right]\psi(Q),$$

$$\sigma_{[i],1}=[sk_{[i],4}]P_2+MPK=[a+\beta_i]Q,$$

$$\sigma_{[i],2}=[d]sk_{[i],3}=[daf(a)]\psi(Q),$$

$$\sigma_{[i],3}=[d]sk_{[i],2}=[df(a)]\psi(Q),$$

$$\sigma_{[i],j}=[\lambda_j]sk_{[i],2}+[\tau_jd]\sum_{j\in I}sk_{[i],j}=\left[\lambda_jf(a)+\tau_jd\sum_{j\in I}h_j\right]\psi(Q).$$

然后$\mathcal{B}$发送消息m_i的签名$\sigma_{[i]}$给$\mathcal{F}$.

4)挑战. $\mathcal{F}$发送(m_i^*,σ^*)给$\mathcal{B}$, $\mathcal{B}$执行验证算法检查签名是否合法, 不合法则挑战失败; 否则, 可得到$\sigma_0^*=\left[\frac{1+f(a)}{a+\beta_i}\right]\psi(Q)$, $f(a)$利用长除法可得$f(a)=\gamma(a)(a+\beta_i)+\gamma_{-1}$, 其中$\gamma(a)=\sum_{i=0}^{q-2}\chi_ia^i$, $\gamma_{-1}\in\mathbb{Z}_N$, 可得

$$\left[\frac{1}{a+\beta_i}\right]P=\frac{1}{1+\gamma_{-1}}(\sigma_{[i],0}^*-[\gamma(a)]P)=$$

$$\frac{1}{1+\gamma_{-1}}\left(\sigma_{[i],0}^*-\sum_{i=0}^{q-2}[\chi_ia^i]P\right).$$

最后, $\mathcal{B}$通过查表L_1获得β_i, 输出$\left(\beta_i,\left[\frac{1}{a+\beta_i}\right]P\right)$作为$q$-SDH问题的解.

综上所述, 若安全游戏完整地进行, 则要成功通过各阶段. 通过q_{K}次密钥询问, 可得密钥全部成功的概率为$\left(\frac{q_{\mathrm{K}}}{q_{\mathrm{H}}}\right)^{q_{\mathrm{K}}}$; 通过$q-2$次签名询问, 可得签名全部询问成功的概率为$\left(\frac{q-2}{q_{\mathrm{H}}}\right)^{q-2}$; 在密钥询问、签名询问均成功通过后, 挑战成功的概率为$\frac{1}{q_{\mathrm{H}}}$. 综合可得, $\mathcal{B}$获胜的概率为$\frac{(q_{\mathrm{K}})^{q_{\mathrm{K}}}(q-2)^{q-2}}{(q_{\mathrm{H}})^{q_{\mathrm{K}}+q-1}}\varepsilon$. 总结, q-SDH问题是难解的, PH-TABS方案是不可伪造的. 证毕.

7 方案分析

在本节中, 通过与现有工作进行比较, 结果如表1所示. 文献[24−25]均给出了KP-ABS类型的基于SM9的属性签名方案, 但KP-ABS在1对多认证场景中需要频繁地更新密钥, 适用性不足. 文献[16, 19]均给出了SP-ABS类型的属性签名方案, 但方案在验证阶段的配对运算均与属性个数相关, 且不具备策略隐藏功能. 本文提出的PH-TABS方案, 访问策略使用表达性丰富的LSSS, 不仅具有策略隐藏和身份可追踪的功能, 在验证阶段只需要常数量级的配对运算和指数运算, 能支持高效的细粒度访问控制.

Table 1 Comparison of Schemes

表1 方案比较

方案	类型	访问结构	可追踪	策略隐藏
文献[24]	KP-ABS	Tree	√	×
文献[25]	KP-ABS	And-Gates	×	×
文献[16]	SP-ABS	LSSS	×	×
文献[19]	SP-ABS	LSSS	√	×
本文方案	SP-ABS	LSSS	√	√

注: “√”表示方案支持该功能; “×”表示方案不支持该功能.

8 性能分析

本节主要介绍本文方案与文献[16, 19]在计算开销、通信开销以及性能上的比较.

本文方案与文献[16, 19]的计算开销对比如表2所示. 其中T_{e}为群G_T上的指数运算, T_{p}为双线性配对运算, T_{mul}为群G_1或G_2上的标量乘运算, T_{add}为群G_1或G_2上的加法运算, i为签名者属性个数. 从表2中可以看出, 本文方案在各阶段的计算中与属性相关的计算量均少于文献[16, 19], 尤其在签名阶段和

Table 2 Comparison of Computation Cost of Schemes

表 2 方案计算开销对比

方案	设置	密钥生成	签名	验证
文献 [16]	$iT_p+iT_e+iT_{add}$	$2iT_{add}$	$3iT_{mul}+(1+4i)T_p+(1+i)T_e$	iT_p+2iT_e
文献 [19]	$(1+i)T_{mul}+T_e$	$(4+i)T_{add}+(6+2i)T_{mul}$	$(7+i)T_{add}+(8+3i)T_{mul}+3T_p+T_e$	$(1+i)T_{add}+(1+2i)T_{mul}+(1+i)T_p+T_e$
本文方案	$T_{mul}+T_p$	$(3+i)T_{mul}$	$(1+2i)T_{add}+(4+2i)T_{mul}+T_e$	$iT_{add}+(1+i)T_{mul}+5T_p+T_e$

验证阶段中, 本文方案只需常数量级的配对操作. 因此, 随着属性个数的增长, 相比文献 [16, 19], 本文方案的计算优势将越来越明显. 本文方案与文献 [16, 19] 的通信开销对比如表 3 所示. 其中$|G|,|G_T|,|\mathbb{Z}_N|$分别表示各个群元素的大小. 从表 3 中可以看出, 本文方案在签名阶段和密钥生成阶段的通信开销和文献 [19] 相当, 随着属性个数的增加, 本文方案通信开销将远低于文献 [16].

Table 3 Comparison of Communication Cost of Schemes

表 3 方案通信开销对比

方案	密钥生成	签名
文献 [16]	$2i\|G\|$	$(1+i)\|G_T\|+i\|G\|$
文献 [19]	$(2+i)\|G\|$	$(3+i)\|G\|+2\|G_T\|$
本文方案	$(3+i)\|G\|+\|\mathbb{Z}_N\|$	$(4+i)\|G\|+\|\mathbb{Z}_N\|$

本文方案与文献 [16, 19] 的各阶段性能以及总体性能对比如图 3~7 所示. 在操作系统 64 b Windows11、Intel® Core™ i5-11400H CPU、内存 16 GB 的实验环境下, 通过 Java 编程语言及其 JPBC(Java pairing based cryptography)[27] 和 BouncyCastle 库仿真实现了本文方案与文献 [16, 19] 的方案, 椭圆曲线选取 256 b 的 BN 曲线, 曲线方程为 $y^2=x^3+5$, 分别在属性个数为 8, 16, 32, 64 的情况下测试了各个阶段以及总体方案的运行时间, 其中实验数据均取给定属性个数下 30 次实验结果的平均值, 其中文献 [16, 19] 是对称群下的方案, 为保证实验对比条件的一致性, 在仿真前均已将文献 [16, 19] 在通用方式下转换为非对称群下的方案[28].

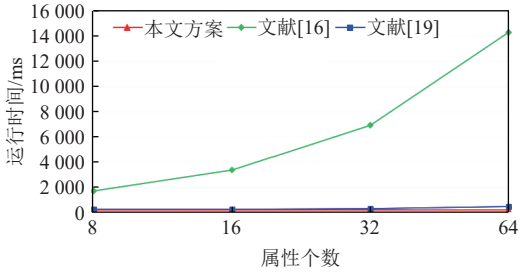


Fig. 3 Performance comparison of setup algorithm

图 3 设置算法性能对比

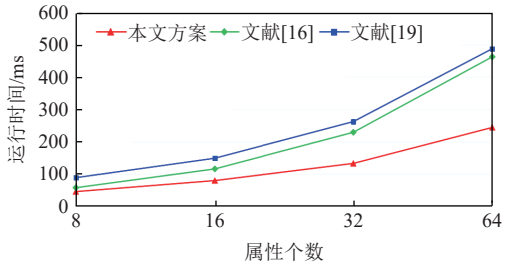


Fig. 4 Performance comparison of key generation algorithm

图 4 密钥生成算法性能对比

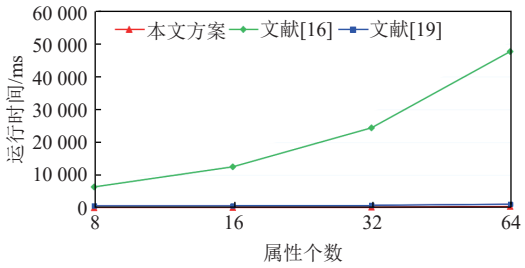


Fig. 5 Performance comparison of signing algorithm

图 5 签名算法性能对比

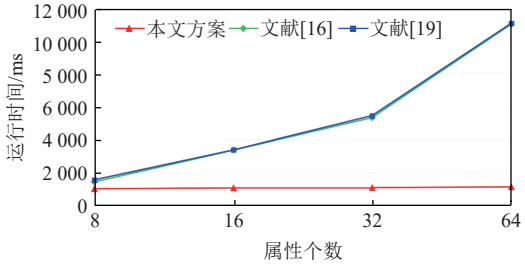


Fig. 6 Performance comparison of verifying algorithm

图 6 验证算法性能对比

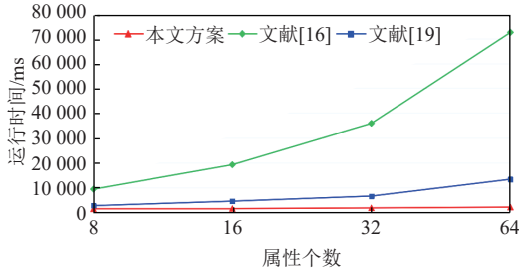


Fig. 7 Performance comparison of overall scheme

图 7 方案总体性能对比

性能对比实验结果表明，本文方案各阶段性能以及总体性能均优于文献[16, 19]. 尤其在验证阶段，本文方案只需常数量级的配对运算，随着属性个数的增加，性能优势明显.

9 结束语

为实现1对多认证场景下安全高效的细粒度访问控制，本文提出一种基于SM9的支持策略隐藏的可追踪属性签名方案，该方案在验证阶段只需常数量级的配对操作和指数操作，同时支持身份追踪和策略隐藏功能. 安全性分析中通过q-SDH难题证明了本文方案在随机谕言机模型下是不可伪造的，从功能、计算开销、通信开销以及性能4个方面的对比实验表明，本文方案有较高的效率.

作者贡献声明：周权负责理论指导、方案分析、论文修改；陈民辉提出初步方案、实验仿真、论文初稿撰写；卫凯俊和郑玉龙负责实验分析、论文修改.

参 考 文 献

[1] Maji K, Prabhakaran M, Rosulek M. Attribute-based signatures[C]// Proc of the 11th Int Conf on Topics in Cryptology. Berlin: Springer, 2011: 376−392

[2] Escala A, Herranz J, Morillo P. Revocable attribute-based signatures with adaptive security in the standard model[C]//Proc of the 4th Int Conf on the Theory and Application of Cryptographic Techniques in Africa. Berlin: Springer, 2011: 224−241

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Proc of the 28th IEEE Symp on Security and Privacy (SP'07). Los Alamitos, CA: IEEE Computer Society, 2007: 321−334

[4] Su Jinshu, Cao Dan, Zhao Baokang, et al. ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of things[J]. Future Generation Computer Systems, 2014, 33: 11−18

[5] Wang Changji, Li Wentao. An efficient attribute-based signature scheme with claim-predicate mechanism[J]. International Journal of Grid and Utility Computing, 2013, 4(2/3): 151−159

[6] Rao Y S, Dutta R. Bandwidth-efficient attribute-based key-insulated signatures with message recovery[J]. Information Sciences, 2016, 369: 648−673

[7] State Cryptography Administration. GM/T 0044—2016 Identity-based cryptographic algorithms SM9[S]. Beijing: Standard Press of China, 2016 (in Chinese)
(国家密码管理局. GM/T 0044—2016 SM9标识密码算法[S]. 北京：中国标准出版社，2016)

[8] Cheung L, Newport C. Provably secure ciphertext policy ABE[C]// Proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM, 2007: 456−465

[9] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89−98

[10] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute based encryption[C]//Proc of the 35th Int Colloquium on Automata, Languages, and Programming. Berlin: Springer, 2008: 579−591

[11] Zhang Yan, Feng Dengguo, Zhang Zhengfeng, et al. On the security of an efficient attribute-based signature[C]//Proc of Int Conf on Network and System Security. Berlin: Springer, 2013: 381−392

[12] Xiong Hu, Bao Yangyang, Nie Xuyun, et al. Server-aided attribute-based signature supporting expressive access structures for industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2019, 16(2): 1013−1023

[13] Su Qianqian, Zhang Rui, Xue Rui, et al. Revocable attribute-based signature for blockchain-based healthcare system[J]. IEEE Access, 2020, 8: 127884−127896

[14] Li Youhuizi, Chen Xu, Yin Yuyu, et al. SDABS: A flexible and efficient multi-authority hybrid attribute-based signature scheme in edge environment[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(3): 1892−1906

[15] Zhang Yinghui, He Jiangyong, Guo Rui, et al. Server-aided and verifiable attribute-based signature for industrial Internet of things[J]. Journal of Computer Research and Development, 2020, 57(10): 2177−2187 (in Chinese)
(张应辉，贺江勇，郭瑞，等. 工业物联网中服务器辅助且可验证的属性基签名方案[J]. 计算机研究与发展，2020，57(10)：2177−2187)

[16] Yang Xiaodong, Li Ting, Pei Xizhen, et al. Medical data sharing scheme based on attribute cryptosystem and blockchain technology [J]. IEEE Access, 2020, 8: 45468−45476

[17] Cui H, Deng R H, Wang Guilin. An attribute-based framework for secure communications in vehicular ad hoc networks[J]. IEEE/ACM Transactions on Networking, 2019, 27(2): 721−733

[18] Gu Ke, Wang Keming, Yang Lulu. Traceable attribute-based signature[J]. Journal of Information Security and Applications, 2019, 49: 102400

[19] Belguith S, Kaaniche N, Laurent M, et al. Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds[J]. Journal of Parallel and Distributed Computing, 2020, 135: 1−20

[20] Li Jiguo, Zhu Liufu, Liu Chengdong, et al. Provably secure traceable attribute-based sanitizable signature scheme in the standard model[J]. Journal of Computer Research and Development, 2021, 58(10): 2253−2264 (in Chinese)
(李继国，朱留富，刘成东，等. 标准模型下证明安全的可追踪属性基净化签名方案[J]. 计算机研究与发展，2021，58(10)：2253−2264)

[21] Zhang Yinghui, Zheng Dong, Deng R H. Security and privacy in smart health: Efficient policy-hiding attribute-based access control[J]. IEEE Internet of Things Journal, 2018, 5(3): 2130−2145

[22] Wang Yue, Fan Kai. Effective CP-ABE with hidden access policy[J]. Journal of Computer Research and Development, 2019, 56(10): 2151−2159 (in Chinese)
(王悦, 樊凯. 隐藏访问策略的高效 CP-ABE 方案[J]. 计算机研究与发展, 2019, 56(10): 2151−2159)

[23] Han Dezhi, Pan Nannan, Li K C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 19(1): 316−327

[24] Tang Fei, Ling Guowei, Shan Jinyong. Traceable attribute signature scheme based on domestic cryptographic SM9 algorithm[J]. Journal of Electronics & Information Technology, 2022, 44(10): 3610−3617 (in Chinese)
(唐飞, 凌国玮, 单进勇. 基于国产密码算法 SM9 的可追踪属性签名方案[J]. 电子与信息学报, 2022, 44(10): 3610−3617)

[25] Zhu Liufu, Li Jiguo, Lai Jianchang, et al. Attribute-based online/offline signature scheme based on SM9[J]. Journal of Computer Research and Development, 2023, 60(2): 362−370 (in Chinese)
(朱留富, 李继国, 赖建昌, 等. 基于商密 SM9 的属性基在线/离线签名方案[J]. 计算机研究与发展, 2023, 60(2): 362−370)

[26] Boneh D, Boyen X. Short signatures without random oracles[C]// Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 56−73

[27] De Caro A, Iovino V. jPBC: Java pairing based cryptography[C]// Proc of IEEE Symp on Computers and Communications. Piscataway, NJ: IEEE, 2011: 850−855

[28] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption[C]//Proc of the 2013 ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 463−474



Zhou Quan, born in 1971. PhD, associate professor. His main research interests include information security and cloud computing.
周　权, 1971 年生. 博士, 副教授. 主要研究方向为信息安全、云计算.



Chen Minhui, born in 1998. Master candidate. His main research interests include attribute encryption and access control.
陈民辉, 1998 年生. 硕士研究生. 主要研究方向为属性加密、访问控制.



Wei Kaijun, born in 1999. Master candidate. His main research interests include access control and information security.
卫凯俊, 1999 年生. 硕士研究生. 主要研究方向为访问控制、信息安全.



Zheng Yulong, born in 2000. Master candidate. His main research interests include cryptography and information security.
郑玉龙, 2000 年生. 硕士研究生. 主要研究方向为密码学、信息安全.