计算机研究与发展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202220530
60(2): 362−370, 2023

基于商密 SM9 的属性基在线/离线签名方案

朱留富[1] 李继国[1,2] 赖建昌[3] 黄欣沂[4] 张亦辰[1,2]
[1](福建师范大学计算机与网络空间安全学院 福州 350117)
[2](福建省网络安全与密码技术重点实验室(福建师范大学)福州 350007)
[3](东南大学网络空间安全学院 南京 211189)
[4](香港科技大学(广州)信息枢纽 广州 511458)
(809015896@qq.com)

Attribute-Based Online/Offline Signature Scheme Based on SM9

Zhu Liufu[1], Li Jiguo[1,2], Lai Jianchang[3], Huang Xinyi[4], and Zhang Yichen[1,2]
[1](*College of Computer and Cyber Security*, *Fujian Normal University*, *Fuzhou* 350117)
[2](*Fujian Provincial Key Laboratory of Network Security and Cryptology* (*Fujian Normal University*), *Fuzhou* 350007)
[3](*School of Cyber Science and Engineering*, *Southeast University*, *Nanjing* 211189)
[4](*Information Hub*, *Hong Kong University of Science and Technology* (*Guangzhou*), *Guangzhou* 511458)

Abstract The attribute-based signature (ABS) scheme uses a set of attributes to identify users. The user can generate a valid signature only when the attributes satisfy the access policy. Compared with the traditional digital signature scheme, the ABS scheme not only utilizes a set of attributes to hide the real identity of users to obtain anonymity, but also realizes fine-grained access control by access policy. In ABS schemes based on elliptic curve, a large number of group exponentiation operations or pairing operations are usually required, which are computationally expensive, resulting in high computational overhead in the signature process. The online/offline signature technology can pre-compute expensive operations offline before knowing message, thereby reducing the online computing cost of lightweight devices. As a commercial cipher independently designed by China, the SM9 identity-based cryptographic algorithm has been standardized by ISO/IEC and is widely used. Based on the SM9 identity-based cryptographic algorithm, we propose an attribute-based online/offline signature (ABOOS) scheme based on the SM9 by using the online/offline signature technology in this paper. Not only ine-grained access control can be achieved, but also it is suitable for lightweight devices. In the random oracle model, the security of the proposed scheme is reduced to the *q*-strong Diffie-Hellman (*q*-SDH) hard problem. Theoretical analysis and experimental simulation show that the proposed scheme effectively reduces the computational cost of the signing process, and is suitable for application environments such as the internet of things.

Key words SM9; online/offline signature; attribute-based signature; random oracle model; *q*-SDH problem

摘 要 属性基签名(attribute-based signature, ABS)方案利用属性集标识用户.只有当属性集满足访问策略时用户才能产生有效签名.与传统数字签名方案相比,属性基签名方案不仅利用属性集隐藏用户的真实身份从而获得匿名性,而且通过制定访问策略实现了细粒度访问控制.在基于椭圆曲线的属性基签名方案中通常需要使用大量的群指数运算或配对操作,这些操作计算代价高昂,导致签名过程计算开销较

收稿日期:2022−06−11;**修回日期**:2022−09−09
基金项目:国家自然科学基金项目(62072104, 61972095, U21A20465, 62032005, 61902191);福建省自然科学基金项目(2020J01159)
This work was supported by the National Natural Science Foundation of China (62072104, 61972095, U21A20465, 62032005, 61902191) and the Natural Science Foundation of Fujian Province (2020J01159).
通信作者:李继国(lig1688@163.com)

大. 在线/离线签名技术可以在未知消息之前将高昂的操作通过离线预计算，从而降低了轻量级设备在线计算代价. SM9 标识密码算法作为我国自主设计的商用密码，已由 ISO/IEC 标准化并被广泛使用. 以商密 SM9 标识密码算法为基础，利用在线/离线签名技术，构造了一种基于商密 SM9 的属性基在线/离线签名（attribute-based online/offline signature, ABOOS）方案. 不仅可以实现细粒度访问控制，同时也适用于轻量级设备. 在随机谕言机模型下，方案的安全性可以规约到 q-SDH（q-strong Diffie-Hellman）困难问题. 理论分析和实验仿真表明提出的方案有效降低了签名阶段的计算代价，适用于物联网等应用环境.

关键词 SM9；在线/离线签名；属性基签名；随机谕言机模型；q-SDH 问题

中图法分类号 TP391

物联网技术的发展和普及使得现代生活环境更加友好和便捷，对人们的生活方式产生了重要影响. 物联网将电子设备与互联网连接，能够使互联网连接对象使用嵌入式传感器、射频识别、激光扫描器等信息传感设备进行数据的采集和交换. 通过网络接入，实现物与物、物与人的连接，从而达到智能化感知、识别和管理. 由于采用无线网络通信，使得物联网更容易遭受各种攻击. 身份认证技术能避免非授权用户非法访问数据，为物联网数据提供了可靠的安全保障. 数字签名能提供数据的完整性和真实性，并且可以实现签名者身份认证功能. 在签名时通常涉及椭圆曲线群中的指数运算或配对运算，这些运算往往计算代价高昂，使得轻量级设备无法承受. 在线/离线签名（online/offline signature, OOS）[1] 方案将签名过程分为在线和离线部分，在未知消息之前，通过将高昂的计算分配给离线阶段而仅保留一些轻量级计算给在线阶段的方式，使得原本无法部署在轻量级设备的签名方案也能适用于物联网环境. 传统的公钥密码体制不具有细粒度访问控制功能. 为了解决这一问题，2005 年，Sahai 等人[2] 提出模糊身份加密方案，定义了属性基密码概念. 在属性基加密方案[3-5] 中，用户的身份由一个属性集表示，密文或者密钥与一个访问策略相关联，当用户的属性满足指定的访问策略时，用户可以成功解密密文. 属性基加密体制不仅实现了细粒度访问控制而且具有一对多加密功能，可以很好地解决云计算中的访问控制、数据安全和隐私保护等关键技术问题，得到了国内外学术界和工业界的高度重视. 过去，国内商用密码方案大都是基于国外的密码技术标准，不符合国家网络空间安全自主可控的发展战略. SM9[6] 是中国商用标识密码标准，包含数字签名、加密、密钥交换和密钥封装. 2018 年，SM9 标识签名算法已被采纳为国际标准 ISO/IEC 的一部分，并于 2020 年成为中国国家标准 GM/T 38 635.2—2020. 2020 年，SM9 标识算法成为国际标准. 由于 SM9 标识密码算法是通过椭圆曲线上的配对运算实现的，因此高昂的计算代价成为了其在轻量级设备中应用的瓶颈. 同时，原始的 SM9 标识密码算法无法高效地实现 1 对多的数据共享和访问控制功能. 综上所述，如何将 SM9 标识密码算法应用于轻量级设备和实现 1 对多的数据共享和访问控制是亟待解决并具有挑战的研究方向.

1 相关工作

属性基密码主要包括属性基加密和属性基签名. 在属性基加密方案中，根据访问策略部署的位置不同可分为密文策略[7-9] 和密钥策略[10] 的属性基加密. 密文策略的属性基加密方案中，访问策略与密文关联，属性集与密钥关联. 当属性集满足密文中的访问策略时，用户可以正确解密. 在密钥策略的属性基加密方案中，访问策略与密钥关联，属性集嵌入在密文中，当且仅当密文中的属性集满足密钥中的访问策略时，用户可以正确解密.

属性基加密方案提供了数据的细粒度访问控制功能并且实现了保密性，但无法提供数据完整性和认证性. 2011 年，Maji 等人[11] 提出了属性基签名方案，实现了细粒度访问控制并能够确保数据的完整性和认证性，在一般群模型中证明了方案的安全性. 2012 年，Okamoto 等人[12] 提出支持非单调访问策略的高效属性基签名（attribute-based signature, ABS）方案，并在标准模型下给出了方案的安全性证明. 在文献 [11−12] 中，签名过程需要使用群中的指数运算和配对运算，这些计算代价高昂，使得方案无法适用于轻量级设备. 为了降低签名算法中高昂的计算代价，1989 年，Even 等人[1] 提出在线/离线签名方案，在线/离线签名通过将签名算法分为在线、离线阶段，在知道签名消息之前，将高昂的计算在离线阶段完成. 而在在线阶段运行一些轻量级计算. 2010 年，Liu 等人[13] 提出基于身份的在线/离线签名方案，并给出了方案

的安全性证明. 为了解决文献 [13] 中密钥托管问题, 2017 年, Liu 等人[14]基于无证书思想提出无密钥托管的身份基在线/离线签名方案. 基于身份的在线/离线签名方案虽然降低了在线签名的计算代价, 但无法实现访问控制和用户身份隐私保护. 为了解决上述问题, Rao[15] 在 2017 年提出了属性基在线/离线签密方案, 利用属性集代替用户身份, 只有当用户属性集满足访问策略时才能产生有效签名. 为了降低签名客户端的计算代价, 张应辉等人[16] 提出可验证的服务器辅助属性基签名方案. 2021 年, Li 等人[17-18] 利用服务器辅助技术, 提出了具有服务器辅助的属性基签名方案, 将大量计算外包给服务器从而降低了计算开销. 为了解决属性基签名方案中的用户身份追踪和敏感消息隐藏问题, 2021 年, 李继国等人[19] 提出可追踪的属性基净化签名方案, 实现了恶意签名者身份追踪和数据脱敏. 目前, 大多数密码方案基于国外密码技术标准设计, 不符合国家网络空间安全自主可控的发展战略. SM9[6] 是中国商用标识密码标准, 包含数字签名、加密和密钥交换. 2018 年, Cheng 等人[20] 分析了 SM9 加密算法和密钥协商协议的安全性, 并给出了安全性证明. 由于 SM9 标识密码算法是通过椭圆曲线上的指数运算和配对运算实现, 因此计算代价高昂, 无法在轻量级设备上使用. 为了提高 SM9 标识签名计算性能, 王松等人[21] 提出了 SM9 标识签名及其验证算法快速实现方案, 但无法降低签名过程中的计算代价. 2021 年, Lai 等人[22] 利用在线/离线签名技术, 提出了基于商密 SM9 的在线/离线签名方案, 在知道签名消息之前, 它将指数运算和配对运算在离线阶段完成, 而在线阶段只运行 Hash 运算或乘法运算, 从而有效降低了在线阶段的计算代价. 为了实现 1 对多的数据通信, 2021 年, 文献 [23] 提出了基于商密 SM9 的高效标识广播加密方案. 文献 [17−23] 仅实现签名或加密功能, 为了同时实现数字签名和数据加密, 文献 [24] 提出了基于商密 SM9 的高效标识签密, 仅执行 1 次操作就能完成签名和加密计算, 有效降低了计算开销.

本文贡献主要有:

本文首次提出基于商密 SM9 的属性基在线/离线签名方案(attribute-based online/offline signature, ABOOS), 提出的方案不仅可以获得细粒度访问控制功能, 并且通过将指数运算和配对运算在离线阶段完成, 降低了在线阶段的计算代价, 能够适用于物联网等应用环境. 本文在随机谕言机模型下证明了 ABOOS 的安全性, 安全性可规约到 q-SDH 困难问题假设. 通过 Charm 平台, 实例化提出的方案并给出性能分析.

2 预备知识

本节介绍文中用到的相关知识, 包括双线性映射、分叉引理、q-SDH 困难问题.

2.1 双线性映射

给定安全参数κ, 生成 1 个双线性元组 $BP=(G_1, G_2, G_T, e, p)$. 其中G_1, G_2, G_T是素数 p阶的循环群. 令P是G_1的 1 个生成元, Q是G_2的 1 个生成元, 1 个双线性映射$e: G_1\times G_2\to G_T$具有 3 个性质.

1)双线性. 对任意$P\in G_1$, $Q\in G_2$和任意$a, b\in\mathbb{Z}_p^*$, 有$e(aP, bQ)=e(P, Q)^{ab}$.

2)非退化性. 对任意$P\in G_1$, $Q\in G_2$, 有$e(P, Q)\neq 1$.

3)可计算性. 对任意$P\in G_1$, $Q\in G_2$, $e(P, Q)$可以被有效计算.

此外, 在G_1和G_2之间存在 1 个有效且能公开计算的同构映射$\psi: G_2\to G_1$, 即$\psi(Q)=P$, 其中P, Q分别是G_1, G_2的生成元.

2.2 q-SDH(q-strong Diffie-Hellman) 困难问题和困难问题假设

q-SDH 困难问题. 令P, Q分别为G_1, G_2的生成元, 在(G_1, G_2)群上的 q-SDH 问题可表述为: 给定$q+2$个元素的元组$(P, Q, aQ, a^2Q, \cdots, a^qQ)$, 找到 1 对元素$\left(c, \dfrac{1}{c+a}P\right)$, 其中$c\in\mathbb{Z}_p^*$.

$(t, \varepsilon)-q$-SDH 困难问题假设: 若不存在概率多项式时间t的算法至少以不可忽略的概率ε解决(G_1, G_2)上的 q-SDH 问题, 则称 q-SDH 问题在(G_1, G_2)是(t, ε)困难的.

2.3 分叉引理

本文使用分叉引理[25] 证明方案的安全性. 为了便于描述, 简单回顾如下. 令$\mathcal{T}$为一个输入仅包含公共信息的概率多项式时间的图灵机, 在进行q_s次签名询问和q_h次随机谕言机询问后, 敌手 A 可以在概率多项式时间t内, 以$\varepsilon\geqslant 10(q_s+1)(q_s+q_h)/2^{\kappa}$的概率产生 1 个有效消息签名元组$(M, \sigma_1, h, \sigma_2)$, 其中$M$表示消息, h是关于元组(M, σ_1)的 Hash 值, σ_2表示仅与M, σ_1, h相关的值. 若元组(σ_1, h, σ_2)能够在不知道签名密钥的情况下以不可区分的分布概率进行模拟, 那么就存在另一台概率多项式时间的图灵机$\mathcal{T}'$能够在理想时间$t'\leqslant 120686q_ht/\varepsilon$时, 通过控制敌手 A 模拟替换与签名者的交互并产生 2 个有效消息签名元组$(M, \sigma_1, h, \sigma_2)$和$(M, \sigma_1, h', \sigma_2')$, 使得$h\neq h'$.

3 形式化定义和安全模型

本节给出 ABOOS 方案的形式化定义和安全模型. 图 1 给出了方案的系统框架, 其中包括 3 个实体: 属性授权机构、轻量级签名设备和验证设备. 属性授权机构为签名设备产生密钥sk_{ω_j}, 签名设备在未知消息之前先通过离线阶段进行预计算产生离线签名σ_{off}, 然后再通过在线阶段产生在线签名σ_{on}, 最终将在线签名σ_{on}和消息 M 发送给验证设备. 若签名有效, 验证设备返回 accept; 否则, 返回 reject.

3.1 ABOOS 方案的形式化定义

在线/离线属性基签名方案由 4 个阶段构成.

1)设置. 该算法输入安全参数κ, 输出公开参数 $params$和主密钥msk. 属性授权机构保留主密钥msk.

2)密钥生成. 算法输入公开参数 $params$、主密钥 msk和访问策略$\mathcal{A}$, 输出签名密钥sk_{ω_j}.

3)签名. 该阶段分为离线签名和在线签名 2 个阶段.具体算法为:

①离线签名. 算法输入公开参数 $params$和签名者密钥sk_{ω_j}, 输出离线签名σ_{off};

②在线签名. 算法输入公开参数 $params$、签名者属性集ω_j、离线签名σ_{off}、签名者密钥sk_{ω_j}和消息 M, 输出在线签名σ_{on}.

4)验证. 算法输入公开参数 $params$, 消息M和在线签名σ_{on}. 若签名有效, 则输出 accept; 否则, 输出 reject.

3.2 安全模型

借鉴文献 [22] 的思想, 本节定义在选择消息和选择策略下的存在不可伪造游戏, 算法 B 和敌手 A 的具体交互为:

初始化. A 首先声明将要挑战的访问策略$\mathcal{A}^*$和$\mathcal{A}^*$中的一个属性集ω_j^*发送给 B.

设置. B 执行设置算法, 输入安全参数κ, 输出公开参数 $params$和主密钥msk, 将公开参数 $params$发送给 A, 自己保留主密钥msk.

密钥询问. A 询问关于访问策略$\mathcal{A}$和属性集ω_j的密钥, 其中$\omega_j \notin \mathcal{A}^*$. B 执行密钥生成算法生成密钥sk_{ω_j}并发送给 A.

签名询问. A 询问关于属性集ω_j和消息M的签名, B 首先执行离线签名算法生成离线签名σ_{off}, 再执行在线签名算法生成在线签名σ_{on}. 最后, 将在线签名σ_{on}发送给 A.

伪造. A 输出一个元组$(\mathcal{A}^*, \omega_j^*, M^*, \sigma^*)$, 若满足 3 个条件, 则称 A 赢得不可伪造性游戏.

1)σ^*是关于$(\mathcal{A}^*, \omega_j^*, M^*)$的 1 个有效签名;

2)A 没有询问过关于$\mathcal{A}^*$和ω_j^*的密钥, 即在密钥生成询问中$\mathcal{A} \neq \mathcal{A}^*$且$\omega_j \notin \mathcal{A}^*$;

3) A 没有询问过关于$(\mathcal{A}^*, \omega_j^*, M^*)$的签名.

定义 1. 如果对于所有概率多项式时间t的敌手

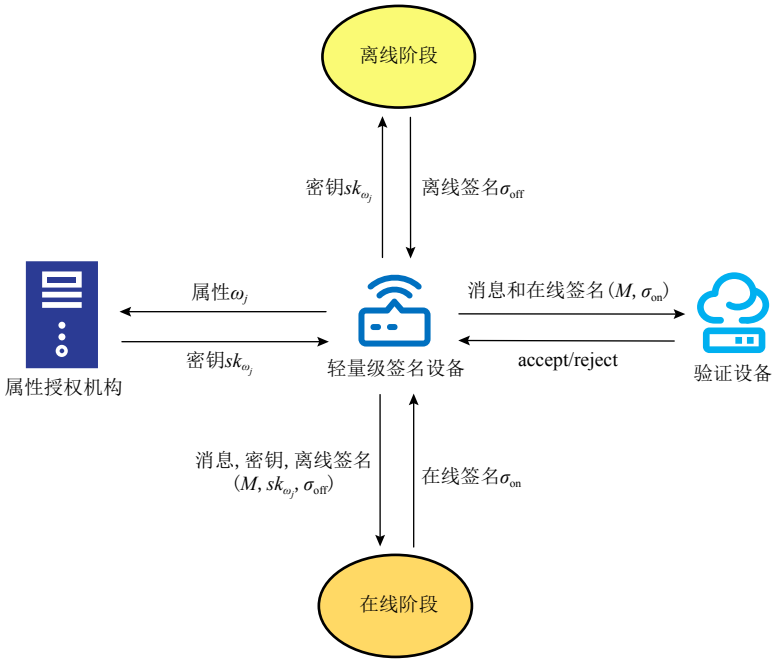

Fig. 1 The framework of ABOOS scheme

图 1 ABOOS 方案框架

进行至多q_k次密钥生成询问和至多q_s次签名询问，它赢得上述不可伪造性游戏的概率是可忽略的，那么提出的方案在选择消息和策略下具有存在性不可伪造.

4 方案构造

借鉴文献[26]的思想，可以从基于身份(identity based signature, IBS)方案构造ABS方案，再利用原始的SM9标识签名方案构造基于商密SM9的属性基在线/离线签名方案.在方案中，令系统属性域为$U=\{att_1, att_2, \cdots, att_u\}$，访问策略$\mathcal{A}=\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_n\}$表示1组授权属性集，其中$\mathcal{A}_i=\{att_{i1}, att_{i2}, \cdots, att_{is_i}\}$，$\omega_j=\{att_{j1}, att_{j2}, \cdots, att_{jd}\}$表示签名者属性集，其中$u=|U|$，$n=|\mathcal{A}|$，$1\leqslant s_i\leqslant u$且$1\leqslant d\leqslant u$. 若$\omega_j\in\mathcal{A}$，称属性集$\omega_j$满足访问策略$\mathcal{A}$. 设置算法$\phi(\omega, U)$将属性集$\omega$转换为1个二进制标识$ID_\omega$，$\phi(\omega, U)$定义为：首先输入属性集$\omega$，系统属性域$U$，令$ID_\omega[i]$表示$ID_\omega$的第$i$位，若$att_i\in\omega$，令$ID_\omega[i]=1$；否则，令$ID_\omega[i]=0$. 其中$1\leqslant i\leqslant u$，$u=|U|$. 然后算法输出$ID_\omega$. 最后调用算法$\phi(\omega, U)$将访问策略$\mathcal{A}=\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_n\}$转换成一个二进制标识集合$I=\{ID_{\mathcal{A}_1}, ID_{\mathcal{A}_2}, \cdots, ID_{\mathcal{A}_n}\}$.

ABOOS方案包含5个算法：设置、密钥生成、在线签名、离线签名和验证.

1)设置. 给定安全参数κ，属性授权机构生成1个双线性配对元组$BP=(G_1, G_2, G_T, e, p)$. 随机选取G_1的生成元P_1，G_2的生成元P_2. 然后，随机选取$\alpha\in\mathbb{Z}_p^*$作为主密钥，计算$P_{\text{pub}}=\alpha P_2$，$g=e(P_1, P_{\text{pub}})$. 系统属性域$U=\{att_1, att_2, \cdots, att_u\}$，$u=|U|$. 选取2个Hash函数$H_1: \{0,1\}^*\to\mathbb{Z}_p^*$，$H_2: \{0,1\}^*\to\mathbb{Z}_p^*$. 属性授权机构随机选取1比特密钥生成函数标识$hid$，则公开参数为$params=(BP, P_1, P_2, P_{\text{pub}}, g, U, hid, H_1, H_2)$.

2)密钥生成. 属性授权机构为属性集ω_j产生密钥sk_{ω_j}. 利用算法$\phi(\omega, U)$将访问策略$\mathcal{A}=\{\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_n\}$转换成二进制标识集合$I=\{ID_{\mathcal{A}_1}, ID_{\mathcal{A}_2}, \cdots, ID_{\mathcal{A}_n}\}$. 算法输入访问策略$\mathcal{A}$、集合$I$、属性集$\omega_j$、主密钥$msk$和公开参数$params$. 属性授权机构随机选取$r_s\in\mathbb{Z}_p^*$，计算密钥$sk_{\omega_j}=(sk_1, sk_2)$，其中

$$sk_1=\frac{\alpha r_s^{-1}}{\left[\dfrac{\prod\limits_{i=1}^{n}H_1(ID_{\mathcal{A}_i}\|hid, r_s)}{\prod\limits_{\mathcal{A}_i\neq\omega_j, i\in[1,n]}H_1(ID_{\mathcal{A}_i}\|hid, r_s)}+\alpha\right]}P_1,\ sk_2=r_s.$$

此时将sk_1，sk_2相乘可知，密钥sk_{ω_j}满足商密SM9标识签名算法密钥结构. 若$\dfrac{\prod\limits_{i=1}^{n}H_1(ID_{\mathcal{A}_i}\|hid, r_s)}{\prod\limits_{\mathcal{A}_i\neq\omega_j, i\in[1,n]}H_1(ID_{\mathcal{A}_i}\|hid, r_s)}+\alpha=0$，属性授权机构重新选取随机数$r_s\in\mathbb{Z}_p^*$，并重新为签名者生成密钥.

3)离线签名. 算法输入公开参数$params$，签名者密钥$sk_{\omega_j}=(sk_1, sk_2)$. 签名者随机选取$r, k\in\mathbb{Z}_p^*$，计算$w=g^r$，$l=sk_2\times(r-k)\bmod p$，$S=l\times sk_1$. 输出离线签名$\sigma_{\text{off}}=(r, k, w, S)$.

4)在线签名. 算法输入公开参数$params$，$\sigma_{\text{off}}=(r, k, w, S)$和消息$M$.签名者利用算法$\varphi(\omega, U)$将属性集$\omega_j$转换成一个二进制标识$ID_{\omega_j}$. 计算$h=H_2(M\|w, p)$，$\tau=(r-h)(r-k)^{-1}\bmod p$，$y=H_1\left(ID_{\omega_j}\|hid, sk_2\right)$. 输出在线签名$\sigma_{\text{on}}=(h, \tau, y, S)$.

5)验证. 当验证者获得消息签名对$(M, \sigma_{\text{on}})=(M, (h, \tau, y, S))$，可以通过执行算法验证签名. 1)计算$t=g^h$；2)计算$P=yP_2+P_{\text{pub}}$；3)计算$\beta=e(\tau\cdot S, P)$；4)计算$w'=\beta\cdot t$；5)计算$h_2=H_2(M\|w', p)$. 检查等式$h_2=h$是否成立. 若成立，则签名有效，输出accept；否则，输出reject.

5 正确性和安全性分析

5.1 正确性分析

若签名者产生1个有效签名，那么该签名可以通过验证算法. 正确性分析为：

当用户属性集ω_j满足给定的访问策略$\mathcal{A}$，即$\omega_j\in\mathcal{A}$时，可以得到$ID_{\omega_j}\in\{ID_{\mathcal{A}_1}, ID_{\mathcal{A}_2}, \cdots, ID_{\mathcal{A}_n}\}$，则有等式成立.

$$w'=\beta\times t=e(\tau\times S, P)\times g^h=e\Bigg((r-h)\times\frac{\alpha r_s^{-1}(r-k)\times(r-k)^{-1}r_s}{\left[\dfrac{\prod\limits_{i=1}^{n}H_1(ID_{\mathcal{A}_i}\|hid, r_s)}{\prod\limits_{\mathcal{A}_i\neq\omega_j, i\in[1,n]}H_1(ID_{\mathcal{A}_i}\|hid, r_s)}+\alpha\right]}P_1,$$

$$H_1\left(ID_{\omega_j}\|hid, r_s\right)P_2+\alpha P_2\Bigg)\times e\left(P_1, P_{\text{pub}}\right)^h=$$

$$e\Bigg(\frac{\alpha(r-h)}{H_1\left(ID_{\omega_j}\|hid, r_s\right)+\alpha}P_1,$$

$$\left(H_1\left(ID_{\omega_j}\|hid, r_s\right)+\alpha\right)P_2\Bigg)\times e(P_1, \alpha P_2)^h=$$

$$e(\alpha(r-h)P_1, P_2)\times e(P_1, \alpha P_2)^h=$$

$$e(\alpha rP_1, P_2)=w.$$

因此$h_2=H_2(M\|w', p)=H_2(M\|w, p)=h$.所以提出的方案满足正确性要求.

5.2 安全性分析

本节给出 ABOOS 方案的安全性证明，基于 q-SDH 困难问题假设提出的方案在选择消息和选择策略下具有存在性不可伪造.

定理 1. 令 H_1, H_2是随机谕言机.若存在概率多项式时间的敌手 A 能够以β的优势赢得不可伪造性游戏，则存在一个概率多项式时间的算法 B 能够以ε的概率解决 q-SDH 困难问题，其中$\varepsilon \leqslant \dfrac{\beta}{q_{H_1}}$, q_{H_1}是H_1询问次数.

证明. 通过 A 和 B 的交互游戏证明定理 1.给定 1 个 q-SDH 困难问题实例 $(P, Q, aQ, a^2Q, \cdots, a^qQ)$, B 的目标是通过与 A 的交互找到元组$\left(c, \dfrac{1}{c+a}P\right)$, 其中 $c \in \mathbb{Z}_p^*$. A 与 B 的交互游戏为：

初始化. A 选择将要挑战的访问策略$\mathcal{A}^*$和$\mathcal{A}^*$中的 1 个属性集ω_j^*并发送给 B, B 通过算法$\varphi(\omega, U)$将$\mathcal{A}^*$,ω_j^*分别转换为二进制标识集合$I^* = \{ID_{\mathcal{A}_1^*}, ID_{\mathcal{A}_2^*}, \cdots, ID_{\mathcal{A}_n^*}\}$和二进制标识$ID_{\omega_j^*}$.

设置. B 产生公开参数. 首先令 $\mathcal{A}_k = \{\mathcal{A}_{k1}, \mathcal{A}_{k2}, \cdots, \mathcal{A}_{kn}\}$表示访问策略，$\omega_j$表示用户属性集. 随机选取 $s_1^*, s_2^*, \cdots, s_n^*, s_{i1}, s_{i2}, \cdots, s_{in} \in \mathbb{Z}_p^*$, 其中 $i \in \{0, 1, \cdots, q_s - 1\}$. 令$x_i = \dfrac{\prod\limits_{j=1}^{n} s_{kj}}{\prod\limits_{\mathcal{A}_{kj} \neq \omega_j, j \in [1,n]} s_{kj}}$, $x^* = \dfrac{\prod\limits_{i=1}^{n} s_i^*}{\prod\limits_{\mathcal{A}_i^* \neq \omega_j^*, i \in [1,n]} s_i^*}$. 生成一个 $q-1$ 阶多项式 $f(z) = \prod\limits_{i=1}^{q-1}(z + x_i) = \sum\limits_{i=0}^{q-1} c_i z^i$, 其中 c_i是 $f(z)$的系数. 利用给定的 q-SDH 困难问题实例计算 $P_2 = f(a)Q = \sum\limits_{i=0}^{q-1} c_i\left(a^iQ\right)$. 计算 $P_1 = \varphi(P_2) = f(a)P$, $P_{\text{pub}} = \sum\limits_{i=0}^{q} c_{i-1}\left(a^iQ\right) = aP_2$和$g = e(P_1, P_{\text{pub}})$; 当$i \in [1, q-1]$时，令 $f_i(z) = \dfrac{f(z)}{z + x_i} = \sum\limits_{i=0}^{q-2} d_i z^i$, 计算 $V_i = \sum\limits_{i=0}^{q-2} d_i \varphi\left(a^{i+1}Q\right) = af_i(a)P = \dfrac{af(a)}{a+x_i}P = \dfrac{a}{a+x_i}P_1$. 因此对于任意 $i \in [1, q-1]$, 元组$\left(x_i, V_i = \dfrac{a}{a+x_i}P_1\right)$是可计算的. 随机选取 1 比特密钥生成函数标识$hid$. 令主密钥$msk = a$, 公开参数 $params = (P_1, P_2, g, hid, P_{\text{pub}})$. 此时，Hash函数$H_1$, H_2被看成是由 B 控制的随机谕言机.

询问. 在询问阶段，A 可以进行H_1询问、H_2询问、密钥询问和签名询问. 具体过程为：

H_1询问. A 首先利用算法$\varphi(\omega, U)$将访问策略 $\mathcal{A}_k = \{\mathcal{A}_{k1}, \mathcal{A}_{k2}, \cdots, \mathcal{A}_{kn}\}$转换为二进制标识集合 $I = \{ID_{\mathcal{A}_{k1}}, ID_{\mathcal{A}_{k2}}, \cdots, ID_{\mathcal{A}_{kn}}\}$, 其中$k \in \{1, 2, \cdots, q_s - 1\}$. A 询问关于$ID_{\mathcal{A}_{ki}}$的 Hash 值s_{ki}. B 初始化 1 个空列表L_1并记录相关应答$(ID_{\mathcal{A}_{ki}}, s_{ki})$.若关于$ID_{\mathcal{A}_{ki}}$的询问记录已经在列表$L_1$中，$B$ 直接返回$H_1(ID_{\mathcal{A}_{ki}} \| hid, r_s) = s_{ki}$; 若$ID_{\mathcal{A}_{ki}}$是一个未经询问的二进制标识，此时令$H_1(ID_{\mathcal{A}_{ki}} \| hid, r_s) = s_{ki}$并将$(ID_{\mathcal{A}_{ki}}, s_{ki})$添加到列表$L_1$中；若 $\mathcal{A}_k = \mathcal{A}^*$, 令 $H_1\left(ID_{\mathcal{A}_i^*} \| hid, r_s\right) = s_i^*$. 然后，$B$ 将询问结果发送给 A.

H_2询问. A 询问关于(M_i, w_i)的 Hash 值h_i. B 初始化 1 个空列表L_2并记录相关应答(M, w_i, h_i). 若关于(M_i, w_i)的询问记录已经在列表中，B 直接返回 $H_2(M_i \| w_i, p) = h_i$; 否则，B 随机选取 $h_i \in \mathbb{Z}_p^*$, 令 $H_2(M_i \| w_i, p) = h_i$, 并将(M_i, w_i, h_i)添加到列表L_2中. 然后，B 将询问结果发送给 A.

密钥询问. A 询问关于访问策略$\mathcal{A}_k = \{\mathcal{A}_{k1}, \mathcal{A}_{k2}, \cdots, \mathcal{A}_{kn}\}$和满足 $\mathcal{A}_k$的 1 个属性集ω_j的密钥，此时满足 $\mathcal{A}_k \neq \mathcal{A}^*$, $ID_{\omega_j} \in \{ID_{\mathcal{A}_{k1}}, ID_{\mathcal{A}_{k2}}, \cdots, ID_{\mathcal{A}_{kn}}\}$且 $ID_{\omega_j} \notin \{ID_{\mathcal{A}_1^*}, ID_{\mathcal{A}_2^*}, \cdots, ID_{\mathcal{A}_n^*}\}$. B 询问H_1预言机获得$(ID_{\omega_j}, s_{\omega_j})$. 在设置阶段有$x_i = \dfrac{\prod\limits_{j=1}^{n} s_{kj}}{\prod\limits_{\mathcal{A}_{kj} \neq \omega_j, j \in [1,n]} s_{kj}}$. 随机选取 $r_s \in \mathbb{Z}_p^*$, 计算 $sk_1 = r_s^{-1}V_i$, $sk_2 = r_s$并发送给 A, 其中 $V_i = \dfrac{a}{a+x_i}P_1$在设置阶段被计算.

签名询问. A 询问关于访问策略$\mathcal{A}_k = \{\mathcal{A}_{k1}, \mathcal{A}_{k2}, \cdots, \mathcal{A}_{kn}\}$, 属性集$\omega_j$和消息$M$的签名$\sigma$. B 首先询问H_1预言机获得s_{ki}并计算 $P = s_{ki}P_2 + P_{\text{pub}}$. 然后，$B$ 随机选取 $h, \tau \in \mathbb{Z}_p^*$, $S \in G_1$并计算 $w = e(\tau \cdot S, P)g^h$. 最后，$B$ 将(M, w)添加到列表L_2中. 此时，设置$H_2(M \| w, p) = h$. 需要注意的是，当$H_2(M \| w, p)$已经在记录在列表L_2中，那么 B 就无法正确模拟签名，此时 B 就终止游戏.这个事件发生的概率为$\dfrac{q_s + q_{H_2}}{2^\kappa}$, 其中$q_s$是签名询问次数，$q_{H_2}$是$H_2$询问次数.

伪造. A 输出关于M^*,$\mathcal{A}^*$, ω_j^*的 1 个有效签名σ^*. 由文献 [25] 定义的分叉引理可知，给定一个输入 $(mpk, \mathcal{A}^*, \omega_j^*)$, 可以构造另一个算法 A'以足够多的次数重放 A, 并获得 2 个有效签名$(M^*, w^*, y^*, h_1^*, \tau_1^*, S_1^*)$和$(M^*, w^*, y^*, h_2^*, \tau_2^*, S_2^*)$, 其中$h_1^* \neq h_2^*$. 然后，$B$ 运行 A'以获得关于M^*,$\mathcal{A}^*$,ω_j^*和w^*的 2 个有效伪造签名$(M^*, w^*, y^*, h_1^*, \tau_1^*, S_1^*)$和$(M^*, w^*, y^*, h_2^*, \tau_2^*, S_2^*)$. 从列表$L_1$中，$B$ 可以获得元组$(ID_{\mathcal{A}_i^*}, s_i^*)$, 并根据设置阶段 $x^* = \dfrac{\prod\limits_{i=1}^{n} s_i^*}{\prod\limits_{\mathcal{A}_i^* \neq \omega_j^*, i \in [1,n]} s_i^*}$ 获得x^*. 由于 2 个都是有效签名，因此都能通过验证算法. 可得 $w^* = e\left(\tau_1^* \times S_1^*, P^*\right)g^{h_1^*} = e(\tau_2^* \times S_2^*, P^*)g^{h_2^*}$, 其中 $P^* = y^*P_2 + P_{\text{pub}} = x^*P_2 + aP_2 = (x^* + a)P_2$. 然后计算 $e\left((\tau_1^* \times S_1^* - \tau_2^* \times S_2^*), P^*\right) = g^{h_2^* - h_1^*}$. 进一步，可以获得 $e(a^{-1}(h_2^* - h_1^*)^{-1}(\tau_1^* \times S_1^* - \tau_2^* \times S_2^*), (x^* + a)P_2) = e(P_1, P_2)$.

因此有$(h_2^*-h_1^*)^{-1}(\tau_1^*\times S_1^*-\tau_2^*\times S_2^*)=\frac{a}{x^*+a}P_1$. 令 $X^*=(h_2^*-h_1^*)^{-1}(\tau_1^*\times S_1^*-\tau_2^*\times S_2^*)$,因为$P_1=f(a)P$,有$\frac{a}{x^*+a}P_1=\frac{af(a)}{x^*+a}P=\frac{\gamma}{x^*+a}P+\sum_{i=0}^{q-1}\gamma_i a^i P$, 其中系数$\gamma_i$已知并且有$\gamma\neq 0$. B 计算$\pi^*=\frac{1}{x^*+a}P_1=\frac{1}{\gamma}\left(X^*-\sum_{i=0}^{q-1}\gamma_i\varphi\left(a^iQ\right)\right)$, 输出$(x^*,\pi^*)$作为 q-SDH 困难问题实例的 1 个解.

综上所述，若 A 能够以不可忽略的概率β伪造 1 个有效签名，那么 B 就能以不可忽略的概率ε解决 q-SDH 困难问题，其中$\varepsilon\leqslant\frac{\beta}{q_{H_1}}$, q_{H_1}是H_1询问的次数，定理 1 得证. 证毕.

6 方案分析

为了解决物联网环境中轻量级设备计算受限而无法执行高昂的计算和用户隐私保护问题，本文提出了基于商密 SM9 的属性基在线/离线签名方案(ABOOS)，提出的方案同时具有细粒度访问控制功能. 通过与已有工作[12,17,27-28]相比，分析本文方案优势. 文献 [12] 给出了支持非单调访问策略的属性基签名方案，方案具有匿名性并且实现了细粒度访问控制，但签名和验证阶段需要大量的指数运算和配对运算，计算开销大. 为了提高签名和验证算法的效率，文献 [27−28] 提出了高效的属性基签名方案，它通过减少运算中使用的配对运算提高了算法的效率，但仍无法高效地适用于轻量级设备. 为进一步降低验证过程的计算开销，文献 [17] 提出了具有服务器辅助验证的属性基签名方案，它通过将大量计算外包给云服务器降低了本地的计算开销. 文献 [12,17,27−28] 的方案是基于国外密码技术标准设计的，不符合国家网络空间安全自主可控的发展战略. 本文提出的基于商密 SM9 的属性基在线/离线签名方案，不仅具有签名者匿名性和细粒度访问控制，并且有效降低了轻量级设备的签名计算代价. 而且方案是在商密 SM9 标识签名算法标准下设计的，符合国家核心技术自主创新的发展战略. 方案性能对比如表 1 所示.

Table 1 Performance Comparison of Schemes

表 1 方案性能比较

方案	匿名性	商密 SM9	轻量级	访问控制
文献 [12] 方案	√	×	×	√
文献 [17] 方案	√	×	√	√
文献 [27] 方案	√	×	×	√
文献 [28] 方案	√	×	×	√
本文方案	√	√	√	√

注: “√”表示方案支持该性能; “×”表示方案不支持该性能.

7 性能分析

本方案与文献 [27−28] 的计算开销和通信开销比较如表 2 和表 3 所示. 基于 Ubuntu 18.4, 本文在 Charm0.5 框架下实现了所提的方案. 使用 Intel(R) Core(TM) i5-3230M CPU @2.60GHz, 4GB RAM 性能计算机，利用 Charm 库中的超奇异椭圆曲线 (SS512) 测试方案. 实验中群的阶 p为 512b 的大素数. 在计算机上测试主要密码学操作开销，经过 1 000 次测量取平

Table 2 Comparison of Computation Cost of Schemes

表 2 方案计算开销比较

方案	密钥生成	离线签名	在线签名	验证
文献 [27] 方案	$\left(\lvert\omega_j\rvert+3\right)\times \mathrm{E}_{G_1}+\mathrm{T}$		$3\left(\lvert\omega_j\rvert+6\right)\times \mathrm{E}_{G_1}+7\mathrm{T}$	$\left(\lvert\omega_j\rvert+3\right)\times \mathrm{P}+4\mathrm{T}$
文献 [28] 方案	$2\lvert\omega_j\rvert\times \mathrm{E}_{G_1}+\lvert\omega_j\rvert\times \mathrm{T}$		$\mathrm{H}+\mathrm{T}+(\lvert\omega_j\rvert+1)\times \mathrm{E}_{G_1}$	$\mathrm{H}+3\mathrm{P}+\lvert\omega_j\rvert\times \mathrm{E}_{G_1}+\mathrm{T}$
本文方案	$2n\mathrm{T}+(2n-1)\times \mathrm{H}$	$\mathrm{E}_{G_T}+2\mathrm{T}$	$2\mathrm{H}+\mathrm{T}$	$\mathrm{H}+\mathrm{P}+\mathrm{E}_{G_T}+\mathrm{E}_{G_1}+\mathrm{E}_{G_2}+\mathrm{T}$

注：ω_j 表示签名者属性集；n表示访问策略中授权属性集的数量；P表示双线性对运算；H表示Hash运算；T表示群$\mathbb{Z}_p^*$中的乘法运算；E_{G_1}表示群G_1中的指数运算；E_{G_2}表示群G_2中的指数运算；E_{G_T}表示群G_T中的指数运算.

Table 3 Comparison of Communication Cost of Schemes

表 3 方案通信开销比较

方案	密钥	离线签名	在线签名
文献 [27] 方案	$(\lvert\omega_j\rvert+2)\times\lvert G_1\rvert$		$(2\lvert\omega_j\rvert+2)\times\lvert G_1\rvert$
文献 [28] 方案	$\lvert\omega_j\rvert\times\lvert G_1\rvert$		$2\lvert G_1\rvert+\lvert\mathbb{Z}_p^*\rvert$
本文方案	$\lvert G_1\rvert+\lvert\mathbb{Z}_p^*\rvert$	$\lvert G_1\rvert+\lvert G_T\rvert+2\lvert\mathbb{Z}_p^*\rvert$	$\lvert G_1\rvert+3\lvert\mathbb{Z}_p^*\rvert$

注：$\lvert\omega_j\rvert$表示属性集ω_j的大小；$\lvert G_1\rvert$,$\lvert G_2\rvert$,$\lvert G_T\rvert$,$\lvert\mathbb{Z}_p^*\rvert$分别表示各个群元素的大小.

均值后得到实验中配对运算所需时间为 12.58 ms, 在群G_1和G_2中执行指数运算所需时间分别为 4.97 ms 和 5.02 ms, 在群G_T执行指数运算的时间为 8.37 ms, 在群$\mathbb{Z}_p^*$中执行乘法运算的时间为 0.24 ms, 执行 Hash 运算的时间为 0.02 ms. 实验结果如图 2 所示.

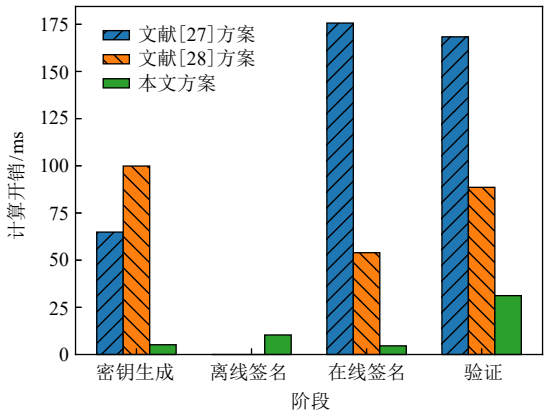

Fig. 2 Computation cost comparison of schemes in different phases

图 2 方案在各阶段的计算开销比较

实验仿真分析结果表明提出的 ABOOS 方案采用在线/离线签名技术使得签名过程的各计算开销均低于文献 [27−28] 提出的高效属性基签名方案的. 在签名验证过程中, 本文提出的方案使用固定数量的配对运算和指数运算验证计算开销也远小于文献 [27−28] .

8 结束语

本文在 SM9 标识签名方案的基础上首次提出基于商密 SM9 的属性基在线/离线签名方案(ABOOS). 该方案不仅适用于物联网环境, 同时还实现了细粒度访问控制功能. 基于 q-SDH 困难问题, 本文在随机谕言机模型下证明了该方案的安全性. 通过与现有属性基签名方案的对比分析可知, 提出的方案更适用于物联网环境.

作者贡献声明: 朱留富负责提出初步方案, 实验设计、论文初稿撰写和修改; 李继国负责论文思路构建、理论指导、方案分析和论文修改; 赖建昌、黄欣沂和张亦辰负责论文方案分析、论文润色和修改.

参 考 文 献

[1] Even S, Goldreich O, Micali S. On-line/off-line digital signatures[C] //Proc of the 9th Conf on the Theory and Application of Cryptology. Berlin: Springer, 1990: 263-275

[2] Sahai A, Waters B. Fuzzy identity-based encryption[C] //Proc of the 24th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473

[3] Zhang Ruyuan, Li Jiguo, Lu Yang, et al. Escrow-free attribute based encryption with user revocation[J]. Information Sciences, 2022, 600(1): 59−72

[4] Li Jiguo, Chen Ningyu, Zhang Yichen. Extended file hierarchy access control scheme with attribute based encryption in cloud computing[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(2): 983−993

[5] Li Jiguo, Wang Yao, Zhang Yichen, et al. Full verifiability for outsourced decryption in attribute based encryption[J]. IEEE Transactions on Services Computing, 2020, 13(3): 478−487

[6] 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)

[7] 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

[8] Chen Ningyu, Li Jiguo, Zhang Yichen, et al. Efficient CP-ABE scheme with shared decryption in cloud storage[J]. IEEE Transactions on Computers, 2022, 71(1): 175−184

[9] Li Jiguo, Zhang Yichen, Ning Jianting, et al. Attribute based encryption with privacy protection and accountability for CloudIoT[J]. IEEE Transactions on Cloud Computing, 2020, 10(2): 762−773

[10] Goyal V, Pandey O, Saha 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

[11] 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

[12] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model[C] //Proc of the 14th Int Conf on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2011: 409-421

[13] Liu J K, Baek J, Zhou Jianying, et al. Efficient online/offline identity-based signature for wireless sensor network[J]. International Journal of Information Security, 2010, 9(4): 287−296

[14] Liu Dan, Zhang Shun, Zhong Hong, et al. An efficient identity-based online/offline signature scheme without key escrow[J]. International Journal of Network Security, 2017, 19(1): 127−137

[15] Rao Y S. Attribute-based online/offline signcryption scheme[J]. International Journal of Communication Systems, 2017, 30(16): 3322−3342

[16] 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)

[17] Chen Yu, Li Jiguo, Liu Chengdong, et al. Efficient attribute-based server-aided verification signature[J/OL]. IEEE Transactions on Services Computing, 2021 [2022-05-24]. https://ieeexplore.ieee.org/abstract/document/9483637

[18] Li Jiguo, Chen Yu, Han Jinguang, et al. Decentralized attribute-based server-aid signature in the internet of things[J]. IEEE Internet of Things Journal, 2021, 9(6): 4573−4583

[19] 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[J]. 计算机研究与发展, 2021, 58(10): 2253−2264)

[20] Cheng Zhaohui. Security analysis of SM9 key agreement and encryption[C] //Proc of the 14th Int Conf on Information Security and Cryptology. Berlin: Springer, 2018: 3-25

[21] Wang Song, Fang Liguo, Han Lianbing, et al. Fast implementation of SM9 digital signature and verification algorithms[J]. Communication Technology, 2019, 52(10): 2524−2527 (in Chinese)
(王松, 房利国, 韩炼冰, 等. 一种SM9数字签名及验证算法的快速实现方法[J]. 通信技术, 2019, 52(10): 2524−2527)

[22] Lai Jianchang, Huang Xinyi, He Debiao, et al. Provably secure scheme based on SM9[J]. The Computer Journal, 2022, 65(7): 1692−1701

[23] Lai Jianchang, Huang Xinyi, He Debiao. An efficient identity-based broadcast encryption scheme based on SM9[J]. Chinese Journal of Computers, 2021, 44(5): 897−907 (in Chinese)
(赖建昌, 黄欣沂, 何德彪. 一种基于商密SM9的高效标识广播加密方案[J]. 计算机学报, 2021, 44(5): 897−907)

[24] Lai Jianchang, Huang Xinyi, He Debiao, et al. An efficient identity-based signcryption scheme based on SM9[J]. Journal of Cryptologic Research, 2021, 8(2): 314−329 (in Chinese)
(赖建昌, 黄欣沂, 何德彪, 等. 基于商密SM9的高效标识签密[J]. 密码学报, 2021, 8(2): 314−329)

[25] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361−396

[26] Fan C I, Tseng Y F, Lin C W. Attribute-based encryption from identity-based encryption[EB/OL]. 2017 [2022-05-24]. https://eprint.iacr.org/2017/219

[27] Zhang Jinxin, Chen Jiageng, Meng Weizhi. Efficient attribute-based signature for monotone predicates[C] //Proc of the 15th Int Conf on Provable Security. Berlin: Springer, 2021: 346−362

[28] Gu Ke, Jia Weijia, Wang Guojun, et al. Efficient and secure attribute-based signature for monotone predicates[J]. Acta Informatica, 2017, 54(5): 521−541.

Zhu Liufu, born in 1995. Master candidate. Member of CCF. His main research is public key cryptography.
朱留富, 1995 年生. 硕士研究生. CCF 会员. 主要研究方向为公钥密码学.

Li Jiguo, born in 1970. PhD, professor. Member of CCF. His main research interests include public key cryptography and cloud computing security.
李继国, 1970 年生.博士, 教授. CCF 会员. 主要研究方向为公钥密码学、云计算安全.

Lai Jianchang, born in 1988. PhD, associate professor. His main research interests include public key cryptography and information security.
赖建昌, 1988 年生. 博士, 副教授. 主要研究方向为公钥密码学、信息安全.

Huang Xinyi, born in 1981. PhD, professor. Member of CCF. His main research interest includes public key cryptography.
黄欣沂, 1981 年生. 博士, 教授. CCF 会员. 主要研究方向为公钥密码学.

Zhang Yichen, born in 1971. PhD, associate professor. Her main research interests include public key cryptography and cloud computing security.
张亦辰, 1971 年生. 博士, 副教授. 主要研究方向为公钥密码学、云计算安全.