计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2021.20210669
58(10):2253-2264,2021

标准模型下证明安全的可追踪属性基净化签名方案

李继国[1,2] 朱留富[1] 刘成东[3] 陆 阳[4] 韩金广[5] 王化群[6] 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](北京市信息技术应用研究所 北京 100091)
[4](南京师范大学计算机与电子信息学院/人工智能学院 南京 210023)
[5](江苏省电子商务重点实验室(南京财经大学) 南京 210003)
[6](南京邮电大学计算机学院 南京 210023)
(ljg1688@163.com)

Provably Secure Traceable Attribute-Based Sanitizable Signature Scheme in the Standard Model

Li Jiguo[1,2], Zhu Liufu[1], Liu Chengdong[3], Lu Yang[4], Han Jinguang[5], Wang Huaqun[6], 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](*Beijing Application Institute of Information Technology, Beijing* 100091)
[4](*School of Computer and Electronic Information/School of Artificial Intelligence, Nanjing Normal University, Nanjing* 210023)
[5](*Jiangsu Provincial Key Laboratory of E-Business (Nanjing University of Finance and Economics), Nanjing* 210003)
[6](*College of Computer, Nanjing University of Posts and Telecommunications, Nanjing* 210023)

Abstract Since the concept of Attribute-Based Signature(ABS) was proposed, it has attracted wide attention due to its anonymity. ABS can hide the identity of signers to support anonymity, but anonymity may enable malicious signers to abuse signatures if the signatures are not traceable. At the same time, in specific application scenarios, such as e-medical treatment or e-commerce, some personal data(e.g. medical records, trade-transfer details, etc.) should be protected to prevent the leakage of private information. In order to hide sensitive information in data transmission and prevent malicious signers from abusing signatures, a traceable attribute-based sanitizable signature scheme is proposed. The security of the scheme is reduced to the Computational Diffie-Hellman(CDH) hard problem in the standard model. The scheme not only solves the problem of sensitive information hiding, guarantees the privacy of the signer, but also prevents the signer from abusing the signature.

Key words attribute-based signature (ABS); sanitizablity; traceability; privacy; standard model

摘 要 自从属性基签名(attribute-based signature, ABS)的概念被提出后,ABS 因其匿名性特征而受到广泛关注.ABS 可以隐藏签名者的真实身份从而保护用户隐私,但其匿名性可能导致签名者滥用签名而无法进行追踪.同时在特定的应用场景,如在电子医疗或电子商务中需要保护一些敏感信息(如医疗技术、转账细节等)防止客户隐私信息泄露.为了解决数据传输中的敏感信息隐藏以及签名者滥用签名

收稿日期:2021-06-11;**修回日期**:2021-07-30
基金项目:国家自然科学基金项目(62072104,61972095,U1736112,61972190,61941116,61772009);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, U1736112, 61972190, 61941116, 61772009) and the Natural Science Foundation of the Fujian Province of China (2020J01159).
通信作者:张亦辰(zyc_718@163.com)

问题,提出了一种可追踪身份的属性基净化签名方案.方案的安全性在标准模型下规约于Computational Diffie-Hellman(CDH)困难问题假设.提出的方案不仅解决了敏感信息隐藏,保证了签名者的隐私,而且防止了签名者对签名的滥用.

关键词 属性基签名;可净化性;可追踪性;隐私性;标准模型

中图法分类号 TP391

随着云计算等新型计算模式的推广,越来越多的重要数据信息被外包存储在云服务器,此外,大量的外包计算服务也将由云服务器统一完成.然而,云计算服务运行在第三方云平台提供商,用户与云平台提供商之间无法建立可信关系,这将可能造成数据信息和用户隐私的泄露,并由此产生诸多安全问题.面对云服务提供商不断爆出的安全事故,人们对云计算环境中的用户数据安全性和隐私性的忧虑与日俱增[1-2].解决这些问题的一种常规做法是,在上传数据到云端之前先对数据进行加密,再将数据以密文的形式存储到云端.但是传统的访问控制模型、敏感数据保护方法和理论的局限性已不能满足用户对数据的安全性、机密性与细粒度访问控制的要求.用户将数据以密文的形式存储到云端后,很可能还需要对密文进行控制.而传统的公钥加密体制仅支持一对一的加密,并不能有效地实现这种数据分享.为解决这一问题,2005 年 Sahai 和 Waters 在欧密会上首次提出属性基加密(attribute-based encryption, ABE)的概念[3].在属性基加密体制中,用户的身份由一个描述性属性集标识,密文或者密钥与一个访问结构相关联,当用户的属性满足指定的访问结构的时候,用户可以成功解密密文.属性基加密体制可以实现一对多的加密以及细粒度的访问控制,可以很好地解决云计算中的访问控制、数据安全和隐私等关键问题,得到了国内外学术界和工业界的高度重视.

属性基签名方案的匿名性能保护签名者的隐私不被泄露,但恶意的签名者可能滥用签名而无法被追踪,因此追踪恶意签名者的身份是一个富有挑战性的问题.同时在特定的应用场景中,需要传输的文件包含部分敏感信息,因此如何在数据传输中保证这些信息不被泄露也亟待解决.

本文的主要贡献包括 3 个方面:

1) 提出了标准模型下安全的可追踪属性基净化签名(traceable attribute-based sanitizable signature, T-ABSS)方案.

2) 提出的方案不仅保护了签名者的隐私、提供细粒度访问控制,避免恶意签名者滥用签名,同时还解决了数据传输中的敏感信息隐藏问题.

3) 在标准模型下证明了方案的安全性,其安全性可规约到 CDH 问题的困难性假设.

1 相关工作

根据访问策略部署位置的不同,ABE[4] 可以划分为密钥策略属性基加密(KP-ABE)和密文策略属性基加密(CP-ABE).在 KP-ABE[5-7] 中,密文和一个描述性属性集合相关联,用户的私钥是由描述用户解密权限的访问结构生成.当且仅当密文的属性集合满足用户的访问结构时,用户才可以解密密文.在 CP-ABE[8-14] 方案中,密文与一个访问结构相关联,密钥由一个描述性属性集合标记,当且仅当密钥的属性集合满足密文的访问结构时用户才能成功解密.

虽然 ABE 提供数据的保密性并且支持细粒度访问控制,但是不支持完整性和认证性.属性基签名(attribute-based signature, ABS)是解决这一问题的重要密码技术.2011 年 Maji 等人首次提出 ABS 方案[15],给出了 ABS 方案的通用构造方法并在一般群模型中证明了方案的安全性.2011 年 Okamoto 等人提出一种支持非单调访问结构的高效 ABS 签名方案[16],并在标准模型下给出了方案的安全性证明.2020 年张应辉等人[17-18] 提出服务器辅助且可验证的属性基签名方案,并应用于工业物联网中.属性基签名方案具有匿名性,可以隐藏签名者的真实身份,但恶意的签名者却能利用这一特性滥用签名而无法被追踪.为了解决这一问题,2011 年 Alex 等人[19] 提出了可追踪身份的 ABS 方案.一旦恶意情况发生,私钥生成中心(Private Key Generator, PKG)可以使用追踪密钥确定签名者的真实身份.由于方案使用自同构签名并多次使用非交互证据不可区分,从而导致方案效率较低.2012 年张秋璞等人[20] 基于紧致群签名方案,提出一种可追踪身份的 ABS 方案,减少了非交互证据不可区分的使用次数且无须使用自同构签名,提高了方案的计算效率.由于

这些方案使用单一密钥授权机构,存在密钥托管问题.2014 年 Kaafarani 等人[21]提出一种可追踪身份的分布式属性基签名方案.由于用户私钥由多授权机构共同产生,因此减轻了密钥托管问题.可追踪身份的属性基签名方案不仅可以确保数据的完整性,而且可以防止恶意签名者滥用签名,能够应用于不需要完全匿名的应用场景,如电子金融交易、工程项目审批等.但在一些特殊的应用场景(电子商务或者是电子医疗系统)中,因为客户资金转账细节不能公开或是病患的诊疗结果要求保密等,需要对签名数据中的一些敏感信息进行修改使隐私部分不再公开可见,这样的方法称为"净化".可净化数字签名(sanitizable signature)允许净化者在不知道原始签名者私钥的前提下修改已签名数据的部分内容,并为净化后的数据生成有效签名[22].2005 年 Ateniese 等人[23]利用变色龙哈希函数提出一种可净化签名方案并在随机预言模型下给出了方案的安全性证明,该方案具有不变性和强透明性.2011 年 Ming 等人[24]提出了基于身份的可净化签名方案并在标准模型下证明了方案的安全性.由于该方案在验证过程中需要使用签名者身份作为公钥,因此无法提供匿名性.为了实现签名者的匿名性,2013 年 Liu 等人[25-26]提出了属性基可净化签名方案,在解决敏感信息隐藏的同时也保证了签名者的匿名性.2020 年 Samelin 等人[27]提出了一个属性基可净化签名方案,可以实现对净化者的完全审计功能.

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、拉格朗日插值、CDH 困难问题.

2.1 双线性映射

假设 G 和 G_T 是 n 阶乘法循环群,其中 $n=pq$,p 和 q 是大素数.g 是 G 的生成元.一个双映射 $e:G\times G\to G_T$ 具有 3 个性质:

1) 双线性.对任意 $a,b\in Z_n$,有 $e(g^a,g^b)=e(g,g)^{ab}$.

2) 非退化性.$e(g,g)\neq 1$.

3) 可计算性.对所有 $u,v\in G$,存在多项式时间算法计算 $e(u,v)$.

2.2 拉格朗日插值

假设 p 为素数,集合 $S\subseteq Z_p$.首先定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$,$i\in Z_p$.给定 Z_p 中的 d 个点 $(1,q_1),(2,q_2),\cdots,(d,q_d)$,$d-1$ 次多项式 $q(x)$ 可以重构为

$$q(x)=\sum_{i\in S}q_i\Delta_{i,S}(x),$$

其中,$|S|=d$.

2.3 CDH 问题和困难问题假设

CDH 问题:令 G 是阶为 n 的乘法循环群,其中 $n=pq$,p 和 q 是大素数.g 是 G 的生成元.CDH 问题为对任意的 $a,b\in Z_n^*$,已知 (g,g^a,g^b),计算 g^{ab}.

CDH 困难问题假设:若不存在多项式时间算法以不可忽略的概率 ε 解决群 G 上的 CDH 问题,则称 CDH 问题在群 G 上是 (t,ε) 困难的.

3 可追踪属性基净化签名方案形式化定义和安全模型

基于文献[19]中属性基签名的形式化定义,我们提出了可追踪的属性基净化签名的形式化定义.

3.1 T-ABSS 方案的形式化定义

T-ABSS 方案包含 6 个部分:

1) 设置.给定安全参数 λ,生成公共参数 $params$、主密钥 msk 和追踪密钥 TK.

2) 密钥生成.该算法输入为用户身份 u、属性集合 ω_a、公共参数 $params$ 和主密钥 msk,输出用户私钥 D_{u,ω_a}.

3) 签名.该算法输入消息 m、签名者属性集合 ω_a 与私钥 D_{u,ω_a}、净化者属性集合 ω_b 和公共参数 $params$,输出消息 m 的签名 σ.签名者将消息 m 和签名 σ 以及秘密值集合 SI 发送给净化者.

4) 净化.签名者声明可净化的消息索引集合 $I_S\subseteq\{1,2,\cdots,l\}$.净化者输入消息 m、公共参数 $params$、m 的签名 σ、净化者的属性集合 ω_b 和签名者发送的秘密值集合 SI 进行净化操作.算法输出净化消息 m' 和净化签名 σ'.

5) 验证.该算法由验证者运行,输入净化的消息签名对 (m',σ')、公开参数 $params$、签名者属性集合 ω_a 和净化者属性集合 ω_b.若为有效签名,则算法输出 accept;否则输出 reject.

6) 追踪.该算法由 PKG 执行,输入签名 σ 和追踪密钥 TK,输出签名者的身份 u.

T-ABSS 系统模型如图 1 所示.私钥生成中心 PKG 收到签名者发送的属性集合 ω_a 和身份 u 后,为签名者产生私钥 D_{u,ω_a}.利用签名算法,签名者产生关于消息 m 的签名 σ,并将 (m,σ) 发送给净化者.净化者对可净化范围内的敏感信息进行修改,并重新生成关于净化后消息 m' 的签名 σ'.净化者将净化

签名(m',σ')发送给验证者,验证者运行验证算法判断签名是否有效.若有效,则输出 accept;否则输出 reject.最后,当发生签名者滥用签名行为时,PKG 可以执行追踪算法计算出恶意签名者的身份 u.

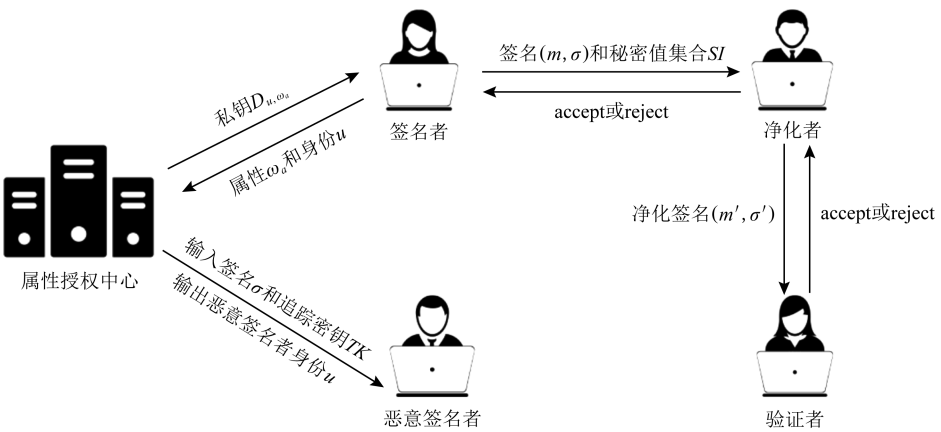

Fig. 1 The framework of T-ABSS

图 1 T-ABSS 方案框架

3.2 安全模型

3.2.1 不可伪造性

本文可追踪属性基净化签名方案使用门限签名策略(ω,d,Y),其中 ω 表示包含 n 个属性的集合,门限为 d,则 $Y=\{A\subseteq\omega:|A|\geqslant d\}$,其含义为签名者至少拥有属性集合 ω 中的 d 个属性.基于文献[18]中的安全模型,定义本文的不可伪造性游戏.

1) 初始化.敌手 A 首先声明将要挑战的签名策略(ω^*,d,Y^*).

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

3) 询问.A 自适应地进行有限次询问操作,其中包括密钥询问、签名询问.

4) 密钥询问.A 自适应地向 B 询问签名者属性集合 ω_a 对应的私钥 D_{u,ω_a},对于所有的 ω_a 都必须满足$|\omega_a\bigcap\omega^*|<d$.$B$ 执行密钥生成算法产生私钥并发送给 A.

5) 签名询问.A 自适应地选择签名者属性集合 ω_a 和净化者属性集合 ω_b,通过密钥生成算法生成签名者私钥 D_{u,ω_a},B 利用签名者的私钥、签名者的属性集合、净化者的属性集合以及消息 m 的每一位,通过签名算法生成签名并发送给 A.

6) 伪造.A 输出关于消息 m^*,属性集合 ω_a^*,ω_b^* 的签名 σ^*.若满足条件①~③,则 A 成功伪造一个有效签名:

① 将 m^*,ω_a^*,ω_b^* 以及 σ^* 输入验证算法,算法输出 accept.

② 没有对 ω_a^* 进行私钥询问.

③ 没有对 m^*,ω_a^* 和 ω_b^* 进行签名询问.

定义 1. 如果任意概率多项式时间 t 的敌手进行至多 q_k 次私钥询问和至多 q_s 次签名询问,并且以不超过 ε 的优势赢得不可伪造游戏,则 T-ABSS 方案是(t,q_k,q_s,ε)—不可伪造的.

3.2.2 不可区分性

基于文献[19]中的安全模型,定义本文的不可区分性游戏.不可区分性游戏可以通过挑战者 B 和敌手 A 之间的交互来刻画.

1) 设置.B 执行设置算法,输出公开参数 $params$ 和主密钥 msk,然后将公开参数 $params$ 发送给 A,自己保留主密钥 msk.

2) 阶段 1.同不可伪造游戏中的询问操作,A 适应性地进行有限次密钥和签名询问.

3) 挑战.A 执行完相关询问后,输出 2 个关于挑战属性集合 ω^* 和允许净化索引集 I_S^* 的消息签名对(m_0^*,σ_0^*),(m_1^*,σ_1^*),并发送给 B.B 随机选择一个位 $b\in\{0,1\}$,若 $b=0$,B 执行净化算法并将$(\overline{m}_0^*,\overline{\sigma}_0^*)$发送给 A;若 $b=1$,B 执行净化算法并将$(\overline{m}_1^*,\overline{\sigma}_1^*)$发送给 A.

4) 阶段 2. 同阶段 1 中执行的询问操作,A 可以自适应地进行有界次密钥生成询问和签名询问.

5) 猜测.最终,A 输出一个值 b',若 $b=b'$ 则赢得游戏.其中,A 赢得游戏的优势可以定义为$Adv(A)=|Pr[b=b']-1/2|$.

定义 2. 如果任意概率多项式时间 t 的敌手进行至多 q_k 次私钥询问和至多 q_s 次签名询问,并且

以不超过 ε 的优势赢得不可区分游戏,那么 T-ABSS 方案是(t,q_k,q_s,ε)—安全的.

3.2.3 不变性

不变性要求净化者只能对净化范围内的数据进行净化,而禁止对净化范围之外的数据进行任何修改.可追踪身份的属性基净化签名方案的不变性可以通过敌手 A 和挑战者 B 之间的游戏来刻画.

1) 初始化.A 将挑战索引集合 I_S^* 发送给 B,I_S^* 表示净化者被允许净化的消息索引集合.

2) 设置.B 执行设置算法,输出公开参数 $params$ 和主密钥 msk,将公开参数 $params$ 发送给敌手 A,自己保留主密钥 msk.

3) 询问.同不可伪造游戏中的询问操作,A 自适应地进行有界次密钥询问和签名询问.在签名询问中,B 将秘密值集合 SI 发送给 A.

4) 伪造.A 输出消息 $m^*=(m_1^*,m_2^*,\cdots,m_l^*)$,属性集合 ω_a^*,ω_b^* 以及签名 σ^*,满足:

① σ^* 是一个有效签名.

② 没有对 ω_a^* 进行私钥询问.

③ 对于任何 $j\in\{1,2,\cdots,q_s\}$,存在 $i\notin I_S^*$ 使得 $m_{j,i}\neq m_i^*$.

定义 3. 如果任意概率多项式时间 t 的敌手进行至多 q_k 次私钥询问和至多 q_s 次签名询问,并且以不超过 ε 的优势赢得不变性游戏,则 T-ABSS 方案是(t,q_k,q_s,ε)—不变的.

4 方案构造

给出方案的具体构造.T-ABSS 方案包含6 个算法:设置、密钥生成、签名、净化、验证和追踪.

1) 设置.设 p,q 为大素数,$n=pq$,G 和 G_T 是 2 个阶为 n 的乘法循环群.$e:G\times G\to G_T$ 是双线性映射,G_p,G_q 分别为 G 的阶为 p,q 的子群.PKG 选择 $d-1$ 个缺省属性,记为集合 $\Omega=\{\omega_1,\omega_2,\cdots,\omega_{d-1}\}$,其中,$d$ 为门限值,$\omega_i\in Z_n$.设 $S\subseteq Z_n$,且 $i\in S$,定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$. PKG 随机选取$\alpha\in Z_n^*$,计算 $g_1=g^\alpha$,其中 g 是 G 的生成元;此外 PKG 随机选取 G 中的元素 g_2,G_q 的生成元 h,G 的生成元 u',一个元素为 v 的集合 $U=\{u_i\}$,其中 u_i 是 G 的生成元;定义 $K=\{1,2,\cdots,k,k+1\}$,对 $i\in K$,PKG 随机选取 $t_i\in G$,定义 $T(x)=g_2^{x^k}\prod_{i=1}^{k+1}t_i^{\Delta_{i,K}(x)}$. 最后,PKG 随机选取 $y'\in Z_n$ 以及 y_i,其中 $y_i\in Z_n^*$,$i\in\{1,2,\cdots,l\}$,计算 $w'=g^{y'}$,$W=(w_1,w_2,\cdots,w_l)=(g^{y_1},g^{y_2},\cdots,g^{y_l})$.则主密钥 msk 为 α,追踪密钥 TK 为 q,$params=(d,g,g_1,g_2,h,t_1,\cdots,t_{k+1},e,u',w',U,W,T(x))$ 为公共参数.在本文中,用户身份 u 用长为 v 的二进制字符串表示,令 $u[i]$表示 u 的第 i 个位,定义 $U\subset\{1,2,\cdots,v\}$为满足 $u[i]=1$ 的序号的集合,定义 $W(u)=u'\prod_{i\in U}u_i$.

2) 密钥生成.算法输入签名者身份 u 及其对应的属性集合 ω_a,主密钥 α 和公共参数 $params$.PKG 首先选取一个 $d-1$ 次多项式 $q(x)$,满足 $q(0)=\alpha$.然后每个用户 u 随机选取 $s\in Z_n$,计算 $D_{u,0}=g^s$,$D_{u,1}=h^s$ 对于 $i\in\omega_a$,PKG 随机选择 $r_i\in Z_n$,计算 $D_{i,0}=g_2^{q(i)}\times T(i)^{r_i}\times W(u)^s$,$D_{i,1}=g^{r_i}$.签名者私钥为 $D_{u,\omega_a}=\{s,D_{u,0},D_{u,1},D_{i,0},D_{i,1}\}$.

3) 签名.输入签名者私钥 D_{u,ω_a},消息 m 的比特 m_i,签名者属性集合 ω_a,净化者属性集合 ω_b,其中 $i\in\{1,2,\cdots,l\}$.首先,签名者随机选择 $\omega_a'\subseteq\omega_a$,再随机选择一个默认子集 $\Omega_a'\subseteq\Omega$,令 $\hat{\omega}_a=\omega_a'\cup\Omega_a'$,其中 $|\omega_a'|\geqslant d$,$\omega_a'\cap\Omega_a'=\varnothing$.对所有 $i\in\hat{\omega}_a$,签名者随机选取 $r_i'\in Z_n$.对净化者属性集合 ω_b 进行类似扩展得到 $\hat{\omega}_b$,对所有 $i\in\hat{\omega}_b$,签名者随机选取 $r_i''\in Z_n$,进行 2 项操作:

① 对任意 $u[i](i=1,2,\cdots,v)$,签名者随机选取 $\theta_i\in Z_n$,计算 $c_i=u_i^{u[i]}h^{\theta_i}$,$\pi_i=(u_i^{2u[i]-1}h^{\theta_i})^{\theta_i}$,$\theta=\sum_{i=1}^{v}\theta_i$,$c=u'\prod_{i=1}^{v}c_i\left(u'\prod_{i=1}^{v}u_i^{u[i]}\right)h^\theta=\left(u'\prod_{i=1}^{v}u_i\right)\times h^\theta=W(u)h^\theta$.

签名者随机选取 $s_1'\in Z_n$,令 $s_1=s+s_1'$.计算秘密值 $SI_i=w_i^{s_1}$,其中 $i\in I_s$.用 SI 表示秘密值集合,即 $SI=\{SI_1,SI_2,\cdots,SI_{|I_s|}\}$,$|I_s|$ 表示集合 I_s 中元素的个数,I_s 表示签名者允许净化者净化的消息索引集合.

② 签名者计算$\{\sigma_{bi}=g^{r_i''}\}_{i\in\hat{\omega}_b}$

$$\{\sigma_{ai}=D_{i,1}^{\Delta_{i,\omega_a'}(0)}g^{r_i'}\}_{i\in\omega_a'},\{\sigma_{ai}=g^{r_i'}\}_{i\in\Omega_a'}$$

$$\sigma_1=D_{u,0}\,g^{s_1'}=g^s\,g^{s_1'}=g^{s_1}.$$

$$\sigma_0=\left[\prod_{i\in\omega_a'}D_{i,0}^{\Delta_{i,\omega_a'}(0)}\right]\left[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'}\right]\times D_{u,1}^{\theta}c^{s_1'}\left(w'\prod_{j=1}^{l}w_j^{m_j}\right)^{s_1}\left[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''}\right].$$

则 $\sigma=(\sigma_0,\sigma_1,\sigma_{ai},\sigma_{bi},c,c_1,\cdots,c_v,\pi_1,\cdots,\pi_v)$ 为签名.

4) 验证.验证者通过等式验证签名的正确性为

$$\frac{e(g,\sigma_0)e\left(w'\prod_{j=1}^{l}w_j^{m_j},\sigma_1\right)^{-1}e(c,\sigma_1)^{-1}}{\left[\prod_{i\in\hat{\omega}_a}e(T(i),\sigma_{ai})\right]\left[\prod_{i\in\hat{\omega}_b}e(T(i),\sigma_{bi})\right]}=e(g_1,g_2),$$

若等式成立,则签名有效.验证算法不仅适用于非净化消息签名对,同时也适用于净化后的消息签名对.

5) 净化.净化者获得签名 σ 和从签名者获得的秘密值 $SI_i=w_i^{s_1}$,其中 $i\in I_s$.净化者首先运行验证算法来检查签名是否有效.若是有效签名,净化者定义需要净化的消息索引集合 $I\subseteq I_s$.令集合 $I_1=\{i\in I:m_i=0,m_i'=1\}$,$I_2=\{i\in I:m_i=1,m_i'=0\}$,净化者选择随机数 $\tilde{r}_i',\tilde{r}_i'',\tilde{s}_1\in Z_n$,计算:

$$\sigma_0'=\sigma_0\left[\prod_{i\in\hat{\omega}_a}T(i)^{\tilde{s}_1'}\right]\prod_{i\in I_1}SI_i\Big/\prod_{i\in I_2}SI_i\times\left(w'\prod_{j=1}^{l}w_i^{m_i'}\right)^{\tilde{s}_1}\left[\prod_{i\in\hat{\omega}_b}T(i)^{\tilde{r}_i''}\right],$$

$$\sigma_{ai}'=\sigma_{ai}g^{\tilde{r}_i'},\sigma_{bi}'=\sigma_{bi}g^{\tilde{r}_i''},\sigma_1'=\sigma_1g^{\tilde{s}_1}$$

$$\sigma'=(\sigma_0',\sigma_{ai}',\sigma_{bi}',\sigma_1',c,c_1,\cdots,c_v,\pi_1,\cdots,\pi_v)$$

为净化签名.

6) 追踪.输入 σ(或是 σ')和追踪密钥 q,返回签名者的身份 u,首先验证签名是否有效.若签名有效,则 PKG 对每一个 c_i 计算 $(c_i)^q$,若 $(c_i)^q=g^0$,则 $u[i]=0$;若 $(c_i)^q=(u_i)^q$,则 $u[i]=1$,从而可以恢复出签名者身份 u.

身份 u 的每一个比特 $u[i]$,有 $e(c_i,u_i^{-1}c_i)=e(h,\pi_i)$ 成立.由 $h\in G_q$,则 $e(h,\pi_i)$ 在 G_T 中的阶为 q,因此有 $c_i\in G_q$ 或 $u_i^{-1}c_i\in G_q$.若 $c_i\in G_q$,有 $(c_i)^q=g^0$;若 $c_i\notin G_q$,有 $u_i^{-1}c_i\in G_q$,可表示为 $u_i^{-1}c_i=h^{\theta_i}$,$c_i=u_ih^{\theta_i}$,其中 θ_i 未知.此时,$(c_i)^q=(u_ih^{\theta_i})^q=(u_i)^q$.因此,追踪算法能够确定签名者的身份.

5 正确性和安全性分析

5.1 正确性分析

通过证明等式成立表明 T-ABSS 方案满足正确性要求.

$$\frac{e(g,\sigma_0)e\left(w'\prod_{j=1}^{l}w_j^{m_j},\sigma_1\right)^{-1}}{\left[\prod_{i\in\hat{\omega}_a}e(T(i),\sigma_{ai})\right]\left[\prod_{i\in\hat{\omega}_b}e(T(i),\sigma_{bi})\right]e(c,\sigma_1)}=$$

$$e\left(g,\left[\prod_{i\in\omega_a'}D_{i,0}^{\Delta_{i,\omega_a'}(0)}\right]\left[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'}\right]\times\left[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''}\right]\left(w'\prod_{j=1}^{l}w_j^{m_j}\right)^{s_1}D_{u,1}^{\theta}\times c^{s_1'}\right)\times\left[\prod_{i\in\hat{\omega}_a}e(T(i),\sigma_{ai})\right]^{-1}e(c,g^{s_1})\times\left[\prod_{i\in\hat{\omega}_b}e(T(i),g^{r_i''})\right]^{-1}e\left(w'\prod_{j=1}^{l}w_j^{m_j},g^{s_1}\right)^{-1}=$$

$$e(g,g_2^{\alpha})=e(g_1,g_2).$$

净化性.当获得净化签名 $\sigma=(\sigma_0',\sigma_{ai}',\sigma_{bi}',\sigma_1',c_1,\cdots,c_v,\pi_1,\cdots,\pi_v)$ 后,当 $i\in I_1$ 时,$m_i'-m_i=1$,记为 1;当 $i\in I_2$ 时,$m_i'-m_i=-1$,记为 0.因此有:

$$\sigma_0'=\sigma_0\left[\prod_{i\in\hat{\omega}_a}T(i)^{\tilde{r}_1'}\right]\left[\prod_{i\in\hat{\omega}_b}T(i)^{\tilde{r}_i''}\right]\times\prod_{i\in I_1}SI_i\Big/\prod_{i\in I_2}SI_i\left(w'\prod_{j=1}^{l}w_i^{m_i'}\right)^{\tilde{s}_1}=\left[\prod_{i\in\omega_a'}D_{i0}^{\Delta_{i,\omega_a'}(0)}\right]\left[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'+\tilde{r}_i'}\right]c^{s_1'}\times\left(w'\prod_{j=1}^{l}w_i^{m_i'}\right)^{s_1+\tilde{s}_1}\left[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''+\tilde{r}_i''}\right]D_{u,1}^{\theta},$$

$$\{\sigma_{ai}=D_{i,1}^{\Delta_{i,S(0)}}g^{r_i'+\tilde{r}_i'}\}_{i\in\omega_a'},\{\sigma_{ai}=g^{r_i'+\tilde{r}_i'}\}_{i\in\Omega_a'},\{\sigma_{bi}=g^{T(i)r_i''+r_i''}\}_{i\in\hat{\omega}_b},\sigma_1'=g^{\tilde{s}_1+s_1}.$$

通过分析可知净化签名的分布和原始签名的分布是一样的,因此净化签名也能通过验证等式.

5.2 安全性分析

5.2.1 不可伪造性

定理 1. 在选择签名策略和选择消息攻击模型下,如果敌手 A 以不可忽略的概率 ε 攻方案,那么挑战者 B 以不可忽略的优势:

$$\varepsilon'\geqslant\frac{\varepsilon}{8q_s(q_k+q_s)(l+1)(v+1)}$$

解决 CDH 问题.

证明. 如果存在一个敌手 A 可以伪造签名,则挑战者 B 可以通过与敌手 A 交互解决 CDH 困难问题假设.令 p,q 为 2 个大素数,$n=pq$,G 和 G_T 是 2 个阶为 n 的乘法循环群,$e:G\times G\to G_T$ 为双线性映射.G_p,G_q 分别为 G 的阶为 p,q 的子群,h 为 G_q 的生成元.给定一个 CDH 困难问题实例:(g,g^{α},g^{β}),其中 g 是 G_p 的生成元,$\alpha,\beta\in Z_p^*$.若 A 可以攻破方案,则 B 可以利用与 A 的交互解决 G_p 子群中的 CDH 问题.

1) 初始化.A 选择要挑战的签名策略 (ω_a^*,d,Y^*).

2) 设置.B 接收到 (g,g^{α},g^{β}),令 $g_1=g^{\alpha}$,$g_2=g^{\beta}$.随机选择 k 次多项式 $f(X)$,计算 k 次多项式 $\varphi(X)$:当 $X\in\omega^*$ 时,令 $\varphi(X)=-X^k$;否则,令 $\varphi(X)\neq-X^k$.所以当且仅当 $X\in\omega^*$ 时,有 $\varphi(X)=-X^k$.

对 $i=1,2,\cdots,k+1$,令 $t_i=g_2^{\varphi(i)}g^{f(i)}$,此时有

$T(i)=g_2^{i^k+\varphi(i)}g^{f(i)}$.假设 A 最多进行 q_k 次密钥询问,q_s 次签名询问.令 $l_u=2(q_s+q_k)$,$l_m=2q_s$,有 $l_u(v+1)<p$,$l_m(l+1)<p$.B 随机选择整数 k_u 和 k_m,其中 $0\leqslant k_u\leqslant v$,$0\leqslant k_m\leqslant l$;$B$ 随机选择 $x'\in Z_{l_u}$ 和一个 v 维向量 $\boldsymbol{X}=(x_i)$,其中 $x_i\in Z_{l_u}$;B 随机选择 $z'\in Z_{l_m}$ 以及一个 k 维向量 $\boldsymbol{Z}=(z_i)$,其中 $z_i\in Z_{l_m}$;B 随机选择 $\mu'\in Z_p$ 和一个 v 维向量 $\boldsymbol{Y}=(\mu_i)$,其中 $\mu_i\in Z_p$;B 随机选择 $\eta'\in Z_p$ 以及一个 l 维向量 $\eta=(\eta_i)$,其中 $\eta_i\in Z_p$.关于身份 u 和消息 m 的函数定义为

$$F(u)=-l_uk_u+x'+\sum_{i\in U}x_i;$$

$$J(u)=\mu'+\sum_{i\in U}\mu_i;$$

$$K(m)=z'-l_mk_m-\sum_{i\in M}z_im_i;$$

$$J(m)=\eta'+\sum_{i\in M}\eta_im_i.$$

设置参数:$u'=g_2^{x'-l_uk_u}$,$u_i=g_2^{x_i}g^{\mu_i}$,$1\leqslant i\leqslant v$;$w'=g_2^{z'-l_mk_m}$,$w_i=g_2^{z_i}g^{\eta_i}$,$1\leqslant i\leqslant l$,并发送给 A.

对任意消息 m 和身份 u 都有:

$$w'\prod_{j=1}^{l}w_j^{m_j}=g_2^{K(m)}g^{J(m)};$$

$$W(u)=u'\prod_{i=1}^{v}u_i=g_2^{F(u)}g^{J(u)}.$$

3) 密钥询问.A 最多进行 q_k 次密钥生成询问.对于用户 u,令其属性为 ω_a.若 $|\omega_a\cap\omega_a^*|\geqslant d$,则终止;否则,$A$ 对属性 ω_a 询问,在不知道主密钥的情况下 B 模拟私钥方式为:

B 首先定义 3 个集合 Γ,Γ',S,令 $\Gamma=(\omega_a\cap\omega_a^*)\cup\Omega_a^*$,$\Gamma\subseteq\Gamma'\subseteq S$,$|\Gamma'|=d-1$,令集合 $S=\Gamma'\cup\{0\}$.

对于用户 u,B 随机选取 $s\in Z_p$,计算 $D_{u,0}=g^s$,$D_{u,1}=h^s$;

对于属性 $i\in\Gamma'$,B 随机选取 $r_i,\eta_i\in Z_p$,计算 $D_{i,0}=g_2^{\eta_i}T(i)^{r_i}W(u)^s$,$D_{i,1}=g^{r_i}$;即当属性 $i\in\Gamma'$ 时,PKG 选取 $d-1$ 次多项式 $q(x)$ 上的 $d-1$ 个点 $q(i)=\eta_i$,此外多项式 $q(x)$ 满足 $q(0)=\alpha$.

对于属性 $i\in\omega_a-\Gamma'$,B 随机选取 $r_i'\in Z_p$,计算:

$$D_{i,0}=\Big(\prod_{j\in\Gamma'}g_2^{q(i)\Delta_{j,S}(i)}\Big)W(u)^s\times$$
$$(g_1^{f(i)/(i^k+\varphi(i))}(g_2^{i^k+\varphi(i)}g^{f(i)})^{r_i'})^{\Delta_{j,S}(i)}$$

$$D_{i,1}=(g_1^{1/(i^k+\varphi(i))}g^{r_i'})^{\Delta_{j,S}(i)}.$$

令 $r_i=(r_i'-\alpha/(i^k+\varphi(i)))\Delta_{0,S}(i)$,因为 $q(i)=q(0)\Delta_{0,S}(i)+\sum_{j\in\Gamma'}(q(i)\Delta_{0,S}(i))$,所以有 $D_{i,0}=g_2^{q(i)}T(i)^{r_i}W(u)^s$,$D_{i,1}=g^{r_i}$.因此,对于敌手而言模拟的私钥与真实的私钥不可区分.

4) 签名询问.假设 A 最多进行 q_s 次签名询问,其中签名者的身份为 u,属性集合为 ω_a,签名策略为 (ω,d,Y).若 $|\omega_a\cap\omega|<d$,则不满足签名策略,模拟终止;否则,模拟签名方式为:

当 $|\omega_a\cap\omega_a^*|<d$ 时,挑战者使用模拟的私钥按原方案步骤生成签名;

当 $|\omega_a\cap\omega_a^*|\geqslant d$ 时,若 $K(m)=0 \bmod p$,则模拟终止;否则进行计算:

对 u 的每一个位 $u[i]$ $(i=1,2,\cdots,v)$,B 随机选取 $\theta_i\in Z_p$,$s_1\in Z_p$,计算 $c_i=u_i^{u[i]}h^{\theta_i}$,$\theta=\sum_{i=1}^{v}\theta_i$,

$$c=u'\prod_{i=1}^{v}c_i=\Big(u'\prod_{i=1}^{v}u_i^{u[i]}\Big)h^{\theta}=\Big(u'\prod_{i\in U}u_i\Big)\times h^{\theta}=W(u)h^{\theta};$$

计算 $\sigma_1=g^{s_1}$;然后 B 随机选择 $r_i,r_i',r_i'',s_1',\tilde{s}_1\in Z_p$,计算为

$$\sigma_0=g_1^{-\frac{J(m)}{K(m)}}\Big[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'}\Big]c^{s_1'}D_{u,1}^{\theta}(g^{J(m)}g_2^{K(m)})^{\tilde{s}_1}\times$$
$$\Big[\prod_{i\in\omega_a'}(T(i)^{r_i})^{\Delta_{i,\omega_a'}(i)}\Big]\Big[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''}\Big]=$$
$$g_2^{\alpha}\Big[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'}\Big](g^{J(m)}g_2^{K(m)})^{\tilde{s}_1-\frac{\alpha}{K(m)}}\times$$
$$\Big[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''}\Big]c^{s_1'}D_{u,1}^{\theta}\Big[\prod_{i\in\omega_a'}(T(i)^{r_i})^{\Delta_{i,\omega_a'}(i)}\Big]=$$
$$g_2^{\alpha}\Big[\prod_{i\in\omega_a'}(T(i)^{r_i})^{\Delta_{i,\omega_a'}(i)}\Big]c^{s_1'}D_{u,1}^{\theta}\times$$
$$\Big[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''}\Big]\Big[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'}\Big](g^{J(m)}g_2^{K(m)})^{\tilde{s}_1}=$$
$$\Big[\prod_{i\in\omega_a'}D_{i,0}^{\Delta_{i,\omega_a'}(i)}\Big]\Big[\prod_{i\in\hat{\omega}_a}T(i)^{r_i'}\Big]\times$$
$$\Big(w'\prod_{j=1}^{l}w_i^{m_i'}\Big)^{\tilde{s}_1}\Big[\prod_{i\in\hat{\omega}_b}T(i)^{r_i''}\Big]c^{s_1'}D_{u,1}^{\theta}$$

$$\sigma_{ai}=\{D_{i1}^{\Delta_{i,S}(i)}g^{r_i'}\}_{i\in\omega_a'},$$

$$\sigma_{ai}=\{g^{r_i'}\}_{i\in\Omega_a'}\sigma_{bi}=\{g^{r_i''}\}_{i\in\hat{\omega}_b},$$

$$\sigma_1=g_1^{-\frac{1}{K(m)}}g^{\tilde{s}_1}.$$

模拟签名为 $\sigma=(\sigma_0,\sigma_1,\sigma_{ai},\sigma_{bi},c,c_1,\cdots,c_v,\pi_1,\cdots,\pi_v)$.

5) 追踪询问.B 直接按原方案运算并返回相关结果给 A.

6) 伪造.若 B 在上述过程中没有终止,A 将伪造消息 m^* 的签名 σ^*.B 知道追踪密钥 TK 并通过追踪算法计算出 u^*,检查 A 没有询问过 u^* 和 ω_a^* 的私钥以及没有对消息 m^* 进行签名询问.由 $\varphi(x)$ 的构造,对所有 $i\in\omega^*$,有 $i^k+\varphi(i)=0$,此时,$T(i)=g_2^{i^k+\varphi(i)}g^{f(i)}=g^{f(i)}$.

若 $F(u^*)\neq 0 \bmod p$ 或者 $K(m^*)\neq 0 \bmod p$，则模拟终止.因此，当 $F(u^*)=0 \bmod p, K(m^*)=0 \bmod p$ 时，有 $W(u^*)=g^{J(u^*)}, c^*=g^{J(u^*)}h^{\theta}$.

B 计算输出：

$$\frac{\sigma_0^*}{\left[\prod_{i\in\hat{\omega}_a}(\sigma_{ai}^*)^{f(i)}\right]\left[\prod_{i\in\hat{\omega}_b}(\sigma_{bi}^*)^{f(i)}\right]\left[(\sigma_1^*)^{J(u^*)+J(m^*)}\right]}=g^{\alpha\beta},$$

其中

$$\sigma_0^*=g^{\alpha_2}\prod_{i\in\hat{\omega}_b}g^{r_i''}\times(g^{J(m^*)})^{s_1}\times$$

$$\prod_{i\in\hat{\omega}_a}(g^{f(i)r_i\Delta_{i,S}(i)}g^{f(i)r_i'}(g^{J(u^*)})^{s_1})$$

$$\sigma_{ai}^*=g^{r_i\Delta_{i,S}(i)+r_i'},\sigma_{bi}^*=g^{r_i''},\sigma_1^*=g^{s_1}.$$

因此，如果 A 能够伪造一个消息的有效签名，那么 B 就能成功地解决 CDH 问题. 证毕.

5.2.2 概率分析

分析在 5.2.1 节模拟中挑战者 B 没有发生终止的概率.若 B 不发生终止，需要以下事件成立.在签名询问时询问了 q_m 个不同的消息.

1) $E_{1i}: K(m_i)\neq 0 \bmod l_m$，其中，$i=1,2,\cdots,q_m$；

2) $E_2: K(m^*)\neq 0 \bmod p$；

3) $E_3: F(u^*)\neq 0 \bmod p$.

则 B 不发生终止的概率为

$$Pr(\overline{abort})\geqslant Pr(\bigwedge_{i=1}^{q_m}E_{1i}\wedge E_2\wedge E_3).$$

$$Pr(E_2)=1/l_m(l+1),$$

$$Pr(E_3)=1/l_u(v+1).$$

同时，对于所有的 $i=1,2,\cdots,q_m$，事件 E_{1i} 和事件 E_2 是相互独立的，因此有：

$$Pr(\overline{abort})\geqslant Pr(\bigwedge_{i=1}^{q_m}E_1\wedge E_2\wedge E_3)=$$

$$Pr(\bigwedge_{i=1}^{q_m}E_1\wedge E_2)Pr(E_3)=$$

$$Pr(E_2)Pr(\bigwedge_{i=1i=1}^{q_m\ q_m}E_1\mid E_2)Pr(E_3)\geqslant$$

$$Pr(E_2)\left(1-\sum_{i=1}^{q_m}Pr(\bar{E}_1\mid E_2)\right)Pr(E_3)\geqslant$$

$$\frac{1}{2q_s(l+1)}\left(1-\frac{q_s}{2q_s}\right)\frac{1}{2(q_k+q_s)(v+1)}=$$

$$\frac{1}{8q_s(q_k+q_s)(l+1)(v+1)}.$$

因此解决 CDH 问题的概率为

$$\varepsilon'\geqslant\frac{\varepsilon}{8q_s(q_k+q_s)(l+1)(v+1)}.$$

5.2.3 不可区分性

定理 2. 提出的 T-ABSS 方案在适应性选择消息攻击下是不可区分的.

通过敌手 A 和挑战者 B 的交互游戏给出不可区分性证明：

1) 设置.B 选择与不可伪造游戏中相同的系统参数 $params$，并随机选择 $u', u_1, \cdots, u_k\in G_p$，将系统参数 $params$ 发送给 A；

2) 阶段 1. B 知道主密钥，因此它可以运行密钥生成算法、签名算法来回应 A 的密钥询问和签名询问.

3) 挑战.在该阶段中，A 对挑战属性集 ω_a^* 生成 2 个签名 $\sigma_0^*=(\sigma_{0,0}^*,\sigma_{0,ai}^*,\sigma_{0,bi}^*,\sigma_{0,1}^*)$ 以及 $\sigma_1^*=(\sigma_{1,0}^*,\sigma_{1,ai}^*,\sigma_{1,bi}^*,\sigma_{1,1}^*)$，其中 σ_0^* 对应消息 $m_0^*=\{m_{0,0}^*,m_{0,1}^*,\cdots,m_{0,l}^*\}$ 的签名；σ_1^* 对应消息 $m_1^*=\{m_{1,0}^*,m_{1,1}^*,\cdots,m_{1,l}^*\}$ 的签名.此外，A 选择一个被允许净化消息索引的集合 $I_S=\{l-k+1,l-k+2,\cdots,l\}$，其中 $|I^*|=k$.令 $I_1^*=\{i\in I^*, j\in\{0,1\}: m_{j,i}^*=0, m_i^*=1\}$，$I_2^*=\{i\in I^*, j\in\{0,1\}: m_{j,i}^*=1, m_i^*=0\}$.有 $I_1^*\cup I_2^*=I^*$，$I_1^*\cap I_2^*=\Phi$.B 随机选择 $\tau\in\{0,1\}$.

若 $\tau=0$，B 随机选择 $(r_0'^*, r_0''^*, s_{0,1}^*, \tilde{s}_{0,1}^*)$，令 $SI_i=u_i^{s_{0,1}^*}$，计算，

$$\bar{\sigma}_{0,0}^*=\sigma_{0,0}^*\left[\prod_{i\in\hat{\omega}_a}T(i)^{r_0'^*}\right]\prod_{i\in I_1}SI_i\Big/\prod_{i\in I_2}SI_i\times$$

$$\left(w'\prod_{j=1}^{l}w_i^{m_i'}\right)^{\tilde{s}_{0,1}^*}\left[\prod_{i\in\hat{\omega}_b}T(i)^{r_0''^*}\right]$$

$$\bar{\sigma}_{0,ai}^*=\sigma_{0,ai}^*g^{r_0'^*},\bar{\sigma}_{0,bi}^*=\sigma_{0,bi}^*g^{r_0''^*},$$

$$\bar{\sigma}_{0,1}^*=\sigma_{0,1}^*g^{\tilde{s}_{0,1}^*}.$$

令 $\bar{\sigma}^*=\bar{\sigma}_0^*=(\bar{\sigma}_{0,0}^*,\bar{\sigma}_{0,ai}^*,\bar{\sigma}_{0,bi}^*,\bar{\sigma}_{0,1}^*)$.

若 $\tau=1$，B 随机选择 $(r_1'^*, r_1''^*, s_{1,1}^*, \tilde{s}_{1,1}^*)$，令 $SI_i=u_i^{s_{1,1}^*}$，计算：

$$\bar{\sigma}_{1,0}^*=\sigma_{1,0}^*\left[\prod_{i\in\hat{\omega}_a}T(i)^{r_1'^*}\right]\prod_{i\in I_1}SI_i\Big/\prod_{i\in I_2}SI_i\times$$

$$\left(w'\prod_{j=1}^{l}w_i^{m_i'}\right)^{\tilde{s}_{1,1}^*}\left[\prod_{i\in\hat{\omega}_b}T(i)^{r_1''^*}\right]$$

$$\bar{\sigma}_{1,ai}^*=\sigma_{1,ai}^*g^{r_1'^*},\bar{\sigma}_{1,bi}^*=\sigma_{1,bi}^*g^{r_1''^*},$$

$$\bar{\sigma}_{1,1}^*=\sigma_{1,1}^*g^{\tilde{s}_{1,1}^*}.$$

令 $\bar{\sigma}^*=\bar{\sigma}_1^*=(\bar{\sigma}_{1,0}^*,\bar{\sigma}_{1,ai}^*,\bar{\sigma}_{1,bi}^*,\bar{\sigma}_{1,1}^*)$.

最终 B 将 $\bar{\sigma}^*=(\bar{\sigma}_0^*,\bar{\sigma}_{ai}^*,\bar{\sigma}_{bi}^*,\bar{\sigma}_1^*)$ 发送给 A.

4) 阶段 2.当接收到消息签名对后，A 仍可以进行密钥询问和签名询问.

通过计算分析可知下面 2 个分布是相同的，因此可以表明 2 个净化签名是不可区分的.

$$Pr(\bar{\sigma}^*=\bar{\sigma}_0^*)=Pr(\bar{\sigma}_0^*=\bar{\sigma}_{0,0}^*,\bar{\sigma}_{1,bi}^*=\bar{\sigma}_{0,bi}^*,$$

$$\bar{\sigma}_{ai}^*=\bar{\sigma}_{0,ai}^*,\bar{\sigma}_1^*=\bar{\sigma}_{0,1}^*)=Pr(r_0'^*=r'^*,r_0''^*=r''^*,$$

$$s_{0,1}^*=s_1^*,\tilde{s}_{0,1}^*=\tilde{s}_{,1}^*)=\frac{1}{p^4}Pr(\bar{\sigma}^*=\bar{\sigma}_1^*)=$$

$Pr(\bar{\sigma}_0^* = \bar{\sigma}_{1,0}^*, \bar{\sigma}_{ai}^* = \bar{\sigma}_{1,ai}^*, \bar{\sigma}_{1,bi}^* = \bar{\sigma}_{1,bi}^*, \bar{\sigma}_1^* = \bar{\sigma}_{1,1}^*) =$

$Pr(r_1'^* = r'^*, r_1''^* = r''^*, s_{1,1}^* = s_1^*, \bar{s}_{1,1}^* = \bar{s}_{,1}^*) = \frac{1}{p^4}$.

综上所述,2 个分布的概率是相同的,因此 A 能区分 2 个签名的优势也是可以忽略的,所以提出的方案具有不可区分性. 证毕.

5.2.4 不变性

定理 3. 如果 ε'-CDH 假设在群 G 中成立,则提出的 T-ABSS 方案具有 ε-不变性,其中 $\varepsilon < \psi\varepsilon'$,$\psi$ 为一常数.

证明. 假设可净化集合为 $I_S \subseteq \{1,2,\cdots,l\}$,净化者在已知秘密值$\{SI_i : i \in I_S\}$的情况下无法对可净化集合之外的数据进行修改.可以通过证明下面关于不变性的引理 1 来证明定理 3.

引理 1. 如果对于任何概率多项式时间的敌手 A_1 可以对净化部分 I_S 中的 k 长度消息进行净化,并且能够以 ε_b 的优势赢得游戏,那么就存在一个概率多项式敌手 A 能够以 $\varepsilon_a \geqslant \varepsilon_b$ 的优势在不可伪造游戏中对 $l-k$ 长度的消息伪造一个有效签名.根据文献[28]给出证明过程.

证明. 假设存在敌手 A_1 在不变性游戏中可以对 l 长度的消息可净化部分 I_S 中的 k 长度进行净化,并且能够以 ε_b 的优势进行游戏.我们考虑敌手 A 对 $l-k$ 长度的消息进行不可伪造游戏.下面我们可以将 A 模拟成挑战者与 A_1 交互从而使得 A 在不可伪造游戏中获得 $\varepsilon_a \geqslant \varepsilon_b$ 的优势.在设置阶段,A 和 A_1 以及在不可伪造游戏中的挑战者 B 进行交互:

1) 首先 A_1 将可净化索引集合 I_S 发送给 A,为了简化表述我们令 $I_S = \{l-k+1, l-k+2, \cdots, l\}$,其中 l 表示消息的长度,$k = |I_S|$.

2) B 将公开参数 $params = \{d, g, g_1, g_2, h, t_1, \cdots, t_{k+1}, e, u', U, w', w_1, \cdots, w_{l-k}\}$发送给 A.

3) A 随机选择 $\delta_i \in Z_p$,$i = l-k+1, l-k+2, \cdots, l$.$A$ 计算 $w_i' = g^{\delta_i}$,$i = l-k+1, l-k+2, \cdots, l$.

4) A 将公开参数:$params = \{d, g, g_1, g_2, h, t_1, \cdots, t_{k+1}, e, u', U, w', w_1, \cdots, w_{l-k}, w'_{l-k+1}, \cdots, w'_l\}$发送给 A_1.

模拟阶段中,在 $j = 1,2,\cdots,q_s$ 次询问中,A 通过与 B 的交互来回答 A_1 的签名询问:

1) A_1 向 A 进行关于消息 $m_j = m_{j,1}, m_{j,2}, \cdots, m_{j,l}$的签名询问.

2) A 向 B 进行关于消息 $m_j = m_{j,1}, m_{j,2}, \cdots, m_{j,l-k}$的签名询问.

3) B 将签名 $\sigma = (\sigma_{j,0}, \sigma_{j,1}, \sigma_{j,a}, \sigma_{j,b}, c, c_1, \cdots, c_v, \pi_1, \cdots, \pi_v)$发送给 A.A 计算 $\sigma'_{j,0} = \sigma_{j,0} \prod_{i=l-k+1}^{l} \sigma_{j,1}^{\delta_i m_{j,i}}$, $\sigma'_{j,1} = \sigma_{j,1}$, $\sigma'_{j,a} = \sigma_{j,a}$, $\sigma'_{j,b} = \sigma_{j,b}$, $c'_j = c_j$, $c'_{j,\zeta} = c_{j,\zeta}$, $\pi'_{j,\zeta} = \pi_{j,\zeta}$($\zeta = 1,2,\cdots,v$).

4) A 将签名$(\sigma'_{j,0}, \sigma'_{j,1}, \sigma'_{j,a}, \sigma'_{j,b}, c'_j, c'_{j,\zeta}, \pi'_{j,\zeta})$以及秘密值$\{\sigma_{j,1}^{\delta_i m_{j,i}} \mid i = l-k+1, l-k+2, \cdots, l\}$发送给 A_1.

在挑战阶段,如果 A_1 能成功伪造一个消息 $m^{*\prime}$ 的签名 $\sigma^{*\prime}$,那么 A 就能通过以下方法获得一个有效签名:

1) A_1 将成功伪造的消息签名对$((m_1^{*\prime} m_2^{*\prime} \cdots m_l^{*\prime}), (\sigma_0^{*\prime}, \sigma_1^{*\prime}, \sigma_a^{*\prime}, \sigma_b^{*\prime}, c^{*\prime}, c_\zeta^{*\prime}, \pi_\zeta^{*\prime}))$发送给 A.可以看出 $\forall j \in \{1,2,\cdots,q_s\}$, $\exists i \notin \{l-k+1, l-k+2, \cdots, l\}$:$m_{j,i} \neq m_i^{*\prime}$.

2) 令消息 $m^* = (m_1^* m_2^* \cdots m_l^*)$,当 $i = 1,2,\cdots,l-k$,有 $m_i^{*\prime} = m_i^*$.A 计算:

$$\sigma_0^* = \sigma_0^{*\prime} \Big/ \prod_{i=l-k+1}^{l} \sigma_1^{\delta_i m_i^{*\prime}}, \sigma_1^* = \sigma_1^{*\prime}, \sigma_a^* = \sigma_a^{*\prime}$$

$$\sigma_b^* = \sigma_b^{*\prime}, c^* = c^{*\prime}, c_\zeta^* = c_\zeta^{*\prime}, \pi_\zeta^* = \pi_\zeta^{*\prime}.$$

3) A 将有效的消息签名对$(m^*, \sigma^* = (\sigma_0^*, \sigma_1^*, \sigma_a^*, \sigma_b^*, c^*, c_\zeta^*, \pi_\zeta^*))$发送给 B.易知 $\forall j \in \{1,2,\cdots,q_s\}$, $\exists i \in \{l-k+1, l-k+2, \cdots, l\}$:

$m_{j,i} \neq m_i^{*\prime}$.如果 A_1 伪造的签名能通过验证,那么 A 计算生成的签名也能通过验证.因此敌手 A 赢得不可伪造游戏的优势 $\varepsilon_a \geqslant \varepsilon_b$,其中 ε_b 是敌手 A_1 赢得不变性游戏的优势. 引理 1 证毕.

从定理 1 中可知,在 CDH 困难问题假设下敌手赢得不可伪造游戏的概率是可以忽略的.通过证明引理 1 可得,在 CDH 困难问题假设下,任何概率多项式时间算法赢得不变性游戏的优势也是可以忽略的. 定理 3 证毕.

6 方案分析

为了解决特定应用场景中的敏感信息隐藏、用户隐私保护以及签名者身份追踪问题,我们提出了可追踪身份的属性基净化签名方案(T-ABSS).本节我们将 T-ABSS 与已有的文献相比较,分析方案优势.文献[29]给出了标准模型下安全的基于身份的签名方案,该方案避免了公钥证书的产生和分发但不能保护签名者的隐私和细粒度访问控制,同时该方案不具有可净化性.文献[20]给出了一种标准模型下安全的属性基可追踪签名方案,该方案在提供

签名者身份隐私保护和细粒度访问控制功能的同时也能追踪签名者的身份,但是该方案不具有可净化性.文献[24]方案给出了标准模型下安全的基于身份的可净化签名方案,实现了敏感信息的隐藏,但由于使用签名者公开信息作为公钥不能保护身份隐私同时也不具有细粒度访问控制.文献[25]给出了标准模型下安全的属性基净化签名方案,但是不能追踪签名者的身份防止签名者滥用签名.我们提出的T-RABS不仅实现了签名者隐私保护和细粒度访问控制,同时也提供了敏感信息隐藏和签名者身份追踪功能,在标准模型下我们给出了方案的安全性证明.方案对比如表1所示:

Table 1 Comparison of Schemes

表1 方案比较

方案	匿名	净化	追踪	透明	安全	访问控制
文献[29]	√	×	√	×	CDH	×
文献[20]	×	×	√	×	CDH	√
文献[24]	×	√	√	√	CDH	×
文献[25]	√	√	×	√	CDH	√
本文方案	√	√	√	√	CDH	√

注:"√"表示满足该性质;"×"表示不满足该性质.

7 性能分析

令 $\hat{\omega}_a$,$\hat{\omega}_b$ 分别表示签名者和净化者属性数量,ω'_a 为用户非缺省属性集,l 表示消息长度,v 表示用户身份长度,I 表示需要净化消息索引集合.BP表示双线性对运算,EXP表示指数运算.T-ABSS方案计算开销如表2所示.与方案[20]可追踪属性基签名(T-ABS)比较开销如表3所示.

基于Ubuntu 18.4,我们在Charm0.5框架下实现了提出的方案.使用Intel® Core™ i5-3230M CPU @2.60 GHz,4 GB RAM性能计算机,利用Charm库中的超奇异椭圆曲线(SS1024)测试方案.实验中群 G 的阶为 n,其中 $n=pq$,p 和 q 为512 b的大素数.在实验计算机上测试主要密码学操作开销,经过1 000次测量取平均值后得到实验中计算双线对所需时间为0.053 s,在群 G 和 G_T 中执行指数运算所需时间分别为0.028 s和0.002 s.实验结果表明在T-ABSS方案中,签名长度随着签名者属性数量的增加而增加,密钥生成、签名产生、验证签名和净化所需时间也与签名者属性数量线性相关.T-ABSS方案及其比较实验结果如图2~4所示.

Table 2 Computation Cost of T-ABSS

表2 T-ABSS方案计算开销

设置	密钥生成	签名	验证	净化	追踪
$(1+l)$EXP	$(3+3\lvert\hat{\omega}_a\rvert)$EXP	$(2\lvert\hat{\omega}_a\rvert+2\lvert\hat{\omega}_b\rvert+\lvert\omega'_a\rvert+l+4v+6)$EXP	$(\lvert\hat{\omega}_a\rvert+\lvert\hat{\omega}_b\rvert+3)$BP+$l$EXP	$(\lvert\hat{\omega}_a\rvert+\lvert\hat{\omega}_b\rvert+\lvert I\rvert+l+4)$EXP	vEXP

Table 3 Comparison of Computation Cost

表3 计算开销比较

方案	签名	验证
T-ABSS	$(2\lvert\hat{\omega}_a\rvert+2\lvert\hat{\omega}_b\rvert+\lvert\omega'_a\rvert+l+4v+6)$EXP	$(\lvert\hat{\omega}_a\rvert+\lvert\hat{\omega}_b\rvert+3)$BP+$l$EXP
T-ABS	$(2\lvert\hat{\omega}_a\rvert+\lvert\omega'_a\rvert+4v+5)$EXP	$(\lvert\hat{\omega}_a\rvert+3)$BP

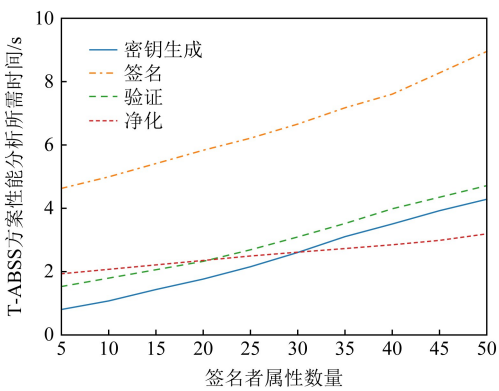

Fig. 2 Analysis of T-ABSS

图2 T-ABSS方案性能分析

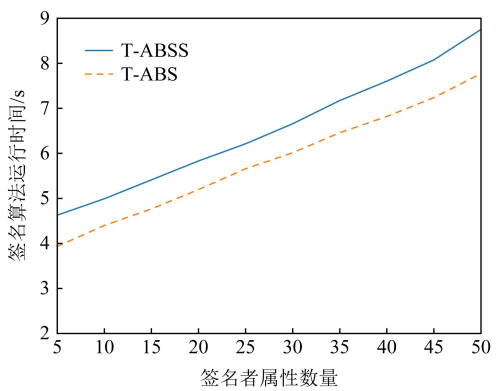

Fig. 3 Analysis of signing algorithm

图3 签名算法性能分析

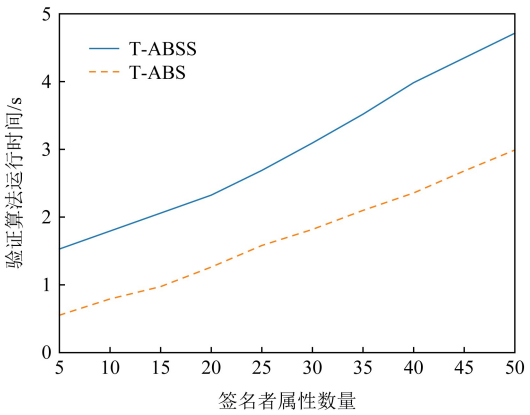

Fig. 4 Analysis of verifying algorithm

图 4 验证算法性能分析

分析结果表明:提出的 T-ABSS 方案由于增加了净化功能,所以随着签名者属性数量的线性增长,在签名产生和签名验证过程所需要的时间高于张秋璞等人[20]提出的可追踪属性基签名方案所需时间.接下来,我们将对如何提高方案的效率做出进一步研究.

8 结束语

本文在属性基签名方案的基础上提出了一种可追踪身份的属性基净化签名方案,不仅解决了敏感信息隐藏问题,同时还避免了签名者滥用签名.在现有安全模型的基础上,我们给出了方案的安全模型和详细构造,并在标准模型下给出了方案的安全性证明.通过与现有方案的对比分析可知,我们的方案更适用于电子医疗、电子政务等特殊应用场景中.

参 考 文 献

[1] Feng Dengguo, Zhang Min, Zhang Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
(冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83)

[2] Zhang Lei, Xiong Hu, Huang Qiong, et al. Cryptographic solutions for cloud storage: Challenges and research opportunities [J]. IEEE Transactions on Services Computing. doi:10.1109/TSC.2019.2937764

[3] Sahai A, Waters B. Fuzzy identity-based encryption [C] // Proc of Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

[4] Su Jinshu, Cao Dan, Wang Xiaofeng, et al. Attribute-based encryption schemes [J]. Journal of Software, 2011, 22(6): 1299-1315 (in Chinese)
(苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J].软件学报, 2011, 22(6): 1299-1315)

[5] 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

[6] Han Jinguang, Susilo W, Mu Yi, et al. Privacy-preserving decentralized key-policy attribute-based encryption [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 3(11): 2150-2162

[7] Li Jiguo, Yu Qihong, Zhang Yichen. Key-policy attribute-based encryption against continual auxiliary input leakage [J]. Information Sciences, 2019, 470: 175-188

[8] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 2007 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2007: 321-334

[9] Li Jiguo, Yu Qihong, Zhang Yichen. Hierarchical attribute based encryption with continuous leakage-resilience [J]. Information Sciences, 2019, 484: 113-134

[10] Li Jiguo, Yao Wei, Zhang Yichen, et al. Flexible and fine-grained attribute-based data storage in cloud computing [J]. IEEE Transactions on Services Computing, 2017, 10(5): 785-796

[11] Li Jiguo, Yao Wei, Zhang Yichen, et al. Full verifiability for outsourced decryption in attribute based encryption [J], 2020, 13(3): 478-487

[12] 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

[13] Li Jiguo, Zhang Yichen, Ning Jianting, et al. Attribute based encryption with privacy protection and accountability for cloudIoT [J]. IEEE Transactions on Cloud Computing, doi:10.1109/TCC.2020.2975184

[14] Chen Ningyu, Li Jiguo, Zhang Yichen. Efficient CP-ABE scheme with shared decryption in cloud storage [J]. IEEE Transactions on Computers, doi:10.1109/TC.2020.3043950

[15] Maji K, Prabhakaran M, Rosulek M. Attribute-based signatures [C] //Proc of Cryptographers' Track at the RSA Conf. Berlin: Springer, 2011: 376-392

[16] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model [C] //Proc of Public Key Cryptography. Berlin: Springer, 2011: 409-421

[17] 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)

[18] Chen Yu, Li Jiguo, Liu Chengdong, et al. Efficient attribute-based server-aided verification signature [J]. IEEE Transactions on Services Computing, doi: 10.1109/TSC.2021.3096420

[19] Alex E, Javier H, Paz M. Revocable attribute-based signatures with adaptive security in the standard model [C] // Proc of the 4th Int Conf on Progress in Cryptology in Africa. Berlin: Springer, 2011: 224-241

[20] Zhang Qiupu, Xu Zhen, Ye Dingfeng. Identity traceable attribute-based signature scheme [J]. Journal of Software, 2012, 23(9): 2449-2464 (in Chinese)
(张秋璞, 徐震, 叶顶锋. 一个可追踪身份的基于属性签名方案[J]. 软件学报, 2012, 23(9): 2449-2464)

[21] Kaafarani A E, Ghadafi E, Khader D. Decentralized traceable attribute-based signatures [C] //Proc of Cryptographers' Track at the RSA Conf. Berlin: Springer, 2014: 327-348

[22] Ma Jinhua, Liu Jianghua, Wu Wei, et al. Survery on redactable signatures [J]. Journal of Computer Research and Development, 2017, 54(10): 2144-2152 (in Chinese)
(马金花, 刘江华, 伍玮, 等. 可修订数字签名研究综述[J]. 计算机研究与发展, 2017, 54(10): 2144-2152)

[23] Ateniese G, Chou D H, De Medeiros B, et al. Sanitizable signatures [C] //Proc of European Symp on Research in Computer Security. Berlin: Springer, 2005: 159-177

[24] Ming Yang, Shen Xiaoqin, Peng Yamian. Provably security identity-based sanitizable signature scheme without random oracles [J]. Journal of Software, 2011, 6(10): 1890-1897

[25] Liu Ximeng, Ma Jianfeng, Xiong Jinbo, et al. Attribute based sanitizable signature scheme [J]. Journal on Communications, 2013, 34(S1): 148-155 (in Chinese)
(刘西蒙, 马建峰, 熊金波, 等. 基于属性的可净化签名方案[J]. 通信学报, 2013, 34(增 1): 148-155)

[26] Mo Ruo, Ma Jianfeng, Liu Ximeng, et al. An attribute-based sanitizable signature supporting dendritic access structure [J]. Acta Electronica Sinica, 2017, 45(11): 2715-2720 (in Chinese)
(莫若, 马建峰, 刘西蒙, 等. 一种支持树形访问结构的属性基可净化签名方案[J]. 电子学报, 2017, 45(11): 2715-2720)

[27] Samelin K, Slamanig D. Policy-based sanitizable signatures [C] //Proc of Cryptographers' Track at the RSA Conf. Berlin: Springer, 2020: 538-563

[28] Agrawal S, Kumar S, Shareef A, et al. Sanitizable signatures with strong transparency in the standard model [C] //Proc of Information Security and Cryptology. Berlin: Springer, 2009: 93-107

[29] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model [C] //Proc of Australasian Conf on Information Security and Privacy. Berlin: Springer, 2006: 207-222

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.

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

Liu Chengdong, born in 1979. BS, associate professor. His main research interests include information security.
刘成东,1979 年生.本科,副研究员.主要研究方向为信息安全.

Lu Yang, born in 1977. PhD, professor. His main research interests include information security and cryptography, network security, and cloud computing security.
陆 阳,1977 年生.博士,教授.主要研究方向为信息安全与密码学、网络安全、云计算安全.

Han Jinguang, born in 1979. PhD, professor. His main research interests include cryptography and information security.
韩金广,1979 年生.博士,教授.主要研究方向为密码学与信息安全.

Wang Huaqun, born in 1974. PhD, professor. His main research interests include applied cryptography, blockchain, and cloud computing security.
王化群,1974 年生.博士,教授.主要研究方向为应用密码学、区块链、云计算安全.

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.