计算机研究与发展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202330459
60(10): 2193−2202, 2023

# 策略隐藏的高效多授权机构 CP-ABE 物联网数据共享方案

张学旺[1] 姚亚宁[1] 付佳丽[1] 谢昊飞[2]
[1](重庆邮电大学软件工程学院 重庆 400065)
[2](重庆邮电大学自动化学院 重庆 400065)
(zhangxw@cqupt.edu.cn)

# Efficient Multi-Authority CP-ABE IoT Data Sharing Scheme with Hidden Policies

Zhang Xuewang[1], Yao Yaning[1], Fu Jiali[1], and Xie Haofei[2]
[1](*School of Software Engineering*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065)
[2](*School of Automation*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065)

**Abstract** Data sharing in the IoT environment suffers from inefficiency and privacy leakage, and the CP-ABE (ciphertext policy attribute-based encryption) data sharing scheme becomes a bottleneck of system operation efficiency because it adopts a single authority, which needs to undertake heavy computational work. To solve the above problems, an efficient multi-authority CP-ABE IoT data sharing scheme with completely hidden policies is proposed in this paper. The scheme uses multi-authority CP-ABE to realize fine-grained access control of data, and uses the non-tampering property of the consortium blockchain to ensure the security of ciphertext Hash and key set ciphertext, and adopts MurmurHash3 algorithm to realize the complete hiding of policy to avoid accessing policy to leak users' private information; and the scheme combines with multi-secret sharing algorithm to improve multi-authority CP-ABE, thus enhancing efficiency of data sharing. The theoretical analysis proves that the scheme can guarantee the security of access policy and secret sharing process. The simulation experimental results show that the proposed scheme has better performance in both policy hiding and secret distribution processes.

**Key words** policy hiding; multi-secret sharing; multi-authority; Internet of things; consortium blockchain

**摘 要** 物联网环境下的数据共享存在效率低下、隐私泄露等问题,以及基于密文策略的属性基加密(ciphertext policy attribute-based encryption,CP-ABE)数据共享方案因采用单授权机构,需要承担繁重的计算工作而成为系统运行效率的瓶颈.为解决上述问题,提出一种策略完全隐藏的高效多授权机构 CP-ABE 物联网数据共享方案.该方案利用多授权机构 CP-ABE 实现数据的细粒度访问控制,利用联盟链不可篡改的特性保证密文哈希值和密钥集合密文的安全,采用 MurmurHash3 算法实现策略的完全隐藏,避免访问策略泄露用户隐私信息;并结合多秘密共享算法改进多授权机构 CP-ABE,进而提升数据共享的效率.理论分析证明该方案能够保证访问策略和秘密共享过程的安全性.仿真实验结果表明,所提方案在策略隐藏和秘密分发过程中都具有较好的性能.

**关键词** 策略隐藏;多秘密共享;多授权机构;物联网;联盟链

**中图法分类号** TP309

**收稿日期**:2023-06-05;**修回日期**:2023-08-19

**基金项目**:国家重点研发计划项目(2022YFB3204503)

This work was supported by the National Key Research and Development Program of China (2022YFB3204503).

**通信作者**:姚亚宁(S211231068@stu.cqupt.edu.cn)

物联网(Internet of things, IoT)应用广泛,包括智慧交通、智慧医疗、智慧家居等多个领域[1]. 随着物联网设备的不断增加,物联网数据共享的需求也日益增加. 然而,物联网数据共享仍存在安全和隐私保护等问题,这严重阻碍数据分享者的积极性[2]. 访问控制是确保数据不被未授权者访问的一种重要方法,区块链与访问控制的结合有2个方面:一是实现去中心化的访问控制模型,解决物联网场景下中心化访问控制的安全和效率问题;二是对基于属性的访问控制进行安全性增强,实现去中心化的授权中心[3].

Sahai 等人[4]提出属性基加密(attribute-based encryption, ABE)的概念,把如何构建多授权机构 ABE 方案作为急需要解决的问题.Chase[5]首次提出了多授权机构 CP-ABE 方案,其授权机构由1个权威机构(certification authority, CA)和多个属性机构(attribute authority, AA)组成. CA 负责为用户分发身份相关的密钥,AA 负责为用户分发属性相关的密钥,该方案中每个数据用户通过全局唯一身份标识(global unique identifier, GID)表示其唯一性;但是该方案中仍然存在一个解密能力极强的 CA,无法实现真正意义上的无中心化. 为了解决该问题,Lin 等人[6]采用密钥分发和联合零秘密共享技术,提出了一种无 CA 的多授权机构 ABE. 在 CP-ABE 方案中,数据拥有者加密数据前首先根据自身需要制定相应的访问控制策略,然后基于该策略加密明文数据(访问控制策略以明文的形式隐含在密文数据中). 但是,在物联网中的许多应用中,访问控制策略本身包含大量的隐私数据. 例如:某医院将所有注册病人的医疗信息托管给第三方存储,为了保护病人的个人隐私,使用病人姓名、身份证号、就诊医院及科室等属性字段为每个用户的医疗信息进行加密. 在这些属性中身份证号、科室相对其它属性是比较敏感的,如若得知病人所属科室为精神科,那么由属性可以判断出此病人极有可能存在精神方面的问题. 因此,实现隐藏访问策略有助于保护物联网中的隐私信息.

Zhang 等人[7]采用布隆过滤器(Bloom filter, BF)并搭配线性秘密共享方案,提出一种针对物联网数据的部分策略隐藏方案. 该方案将属性值隐藏在 BF 中,且能够抵抗访问策略猜测攻击和字典攻击. 王悦等人[8]提出一种隐藏访问策略的高效 CP-ABE 方案. 该方案利用合数阶双线性群构造了一种基于包含正负及无关值的“与门”的策略隐藏方案,使得属性隐藏和秘密共享能够同时应用到“与门”结构中;能有效地避免用户的具体属性值泄露给第三方,确保用户隐私的安全. 为了解决车联网环境下跨信任域数据共享中跨域数据泄露严重的问题,刘雪娇等人[9]提出了一种区块链架构下高效的车联网跨域数据安全共享方案. 不同信任域的可信机构构成区块链,采用改进的 CP-ABE 加密数据,结合区块链和星际文件系统(InterPlanetary file system, IPFS)进行存储,构建了基于区块链的跨域数据细粒度、安全共享方案. Dai 等人[10]提出一种新的数据访问控制策略. 首先设计基于属性的 Merkle 树结构保存用户属性,然后基于该 Merkle 树构造零知识证明,有效存储用户属性进行零知识证明验证,验证者只知道用户满足策略要求,而不知道用户拥有哪些属性,从而达到策略隐藏的目的. 访问策略隐藏的 CP-ABE 方案是研究热点,科研人员不断地提出实现方案[11-14].

现有的策略隐藏 CP-ABE 方案分为完全隐藏[15]和部分隐藏[16]. 完全隐藏访问策略意味着不暴露访问策略中的属性信息,而部分隐藏访问策略意味着只隐藏敏感属性值. 对于物联网环境来说,访问策略的任何信息泄露都有可能对数据拥有者的隐私产生威胁. 另外,提升数据共享效率的方案大都忽略了秘密分发者的负担. 因此,本文在文献 [17] 的基础上,进一步提出一种策略完全隐藏且高效的多授权机构 CP-ABE 方案. 本文的贡献有3个方面:

1) 策略完全隐藏. 基于联盟链可以更好地保护隐私数据且更具有灵活性的特点,提出一种策略完全隐藏的高效多授权机构 CP-ABE 物联网数据共享方案.

2) 多秘密共享. 根据多秘密共享算法改进多授权机构 CP-ABE 方案提升数据共享的效率以及增强细粒度访问控制,即在一次数据共享过程中实现多份数据的共享,而且每份共享数据各有不同的门限访问结构.

3) 利用 MurmurHash3 算法实现访问策略的完全隐藏,由于哈希算法具有不可逆性,能有效防止从访问策略中推断出任何有价值的信息.

## 1 预备知识概述

### 1.1 多授权机构 CP-ABE

Lewko 等人[18]提出了一种新型的“去中心”的多授权机构属性加密(decentralized multi-authority attribute-based encryption)方案. 该方案同样不需要 CA 的参与,任何实体不需要全局合作就能成为 AA,并独立分发密钥,用户可以根据自身情况选择相信 AA. 该方案定义为:

1）$Global\ Setup(\lambda)\rightarrow GP$. 该算法为全局设置算法，由参与系统建立阶段的可信第三方执行，以安全参数$\lambda$为输入，输出系统公共参数$GP$.

2）$Authority\ Setup(GP)\rightarrow(SK, PK)$. 该算法为机构设置算法，每个属性机构以$GP$为输入进行初始化，输出该属性机构的私钥$SK$和公钥$PK$.

3）$Encrypt(M,(A,\rho),GP,\{PK\})\rightarrow CT$. 该算法为加密算法，以明文$M$、访问结构$(A,\rho)$、$GP$和相关属性机构的公钥$PK$为输入，输出密文$CT$.

4）$KenGen(GID,i,SK,GP)\rightarrow K_{i,GID}$. 该算法为密钥生成算法，以用户身份$GID$、$GP$、属性$i$和相关属性机构的私钥$SK$为输入，输出该用户的属性$i$对应的私钥$K_{i,GID}$.

5）$Decrypt\left(CT,\left\{K_{i,GID}\right\},GP\right)\rightarrow M$. 该算法为解密算法，以$GP$、$CT$和用户$GID$的私钥集合$\left\{K_{i,GID}\right\}$为输入. 若该用户的属性集合满足访问结构，则解密成功，输出明文$M$；否则，解密失败.

### 1.2 多秘密共享算法

秘密共享作为保护敏感信息的重要工具，被广泛应用于门限数字签名[19]、多方安全计算[20]和密钥协商[21]等. 对单秘密共享方案来说，参与者 1 次只能实现 1 个秘密的共享，虽然共享多个秘密可以通过多次秘密共享实现，但是这样不仅加大了秘密分发者和参与者的负担，还增加了秘密共享实现的代价. 因此，1 次共享单个秘密已经无法满足人们对于秘密共享的要求.2000 年左右，多秘密共享概念被提出，即多个秘密在 1 次秘密分发过程中实现共享，拓宽了秘密共享的应用范围. 本文采用文献 [22] 基于中国剩余定理和 Shamir 门限方案提出的一种门限可变的多秘密共享（changeable threshold multi-secret sharing, CTM-SS）方案. 该方案共享多组秘密只需 1 次秘密分发过程，且各组秘密可有不同的门限访问结构.

### 1.3 MurmurHash3 算法

MurmurHash 是一种非加密型哈希函数，适用于一般的哈希检索操作. 由 Austin Appleby 在 2008 年发明，与其它流行的哈希函数相比，MurmurHash 的随机分布特征表现更好. MurmurHash3 是 MurmurHash 的第 3 个版本，支持 128 b，碰撞概率大大降低，在 0~$10^8$ 范围内几乎不存在碰撞[23].

## 2 策略隐藏的高效多授权机构 CP-ABE 物联网数据共享方案

### 2.1 方案模型

策略隐藏的高效多授权机构 CP-ABE 物联网数据共享方案模型如图 1 所示，方案模型包含的实体主要有：可信第三方（trusted third party,TTP）、AA、数据拥有者（data owner, DO）、数据用户（data user, DU）、IPFS 和联盟链（consortium blockchain, CB）.

TTP 只参与系统初始化阶段的全局参数生成算法，为 AA 生成其对应的公钥和私钥提供参数.

AA 主要承担属性管理工作以及为 DU 生成属性私钥. 该模型中存在多个 AA，用户属性被多个 AA 共同管理，既可解决单 AA 存在的密钥托管问题而提高系统安全性，又可以提高系统性能.

DO 先使用高级加密标准（advanced encryption standard, AES）算法加密要共享的数据，1 次共享多份数据，并且每份数据的对称密钥和门限可以不同. 然后，DO 根据自身意愿制定相应的访问策略，实施以自己为中心的数据访问控制. 本文方案会自动将 DO 设置的每个属性信息通过 MurmurHash3 算法隐藏起来，即访问策略中只存储属性信息对应的哈希值，不存储明文属性信息，保护了物联网环境下访问策略的安全性和隐私性. 最后，基于隐藏属性的访问结构对密钥集合进行加密，将对称密钥集合密文、密钥和密文哈希值对应关系（每份数据加密的密钥和密文存储至 IPFS 形成的哈希值一一对应）上传至 CB，方便 DU 根据重构出的对称密钥解密对应的数据密文.

DU 根据实际情况选择相信某些 AA，并利用这些 AA 颁发的密钥解密对称密钥集合密文. 若用户属性集满足隐藏属性的访问结构，则可以从对称密钥集合密文中解密出自己所需的对称密钥，用来解密对应的数据密文，反之解密失败. DU 可以根据各自的属性集解密出 DO 共享的部分或全部数据.

IPFS 可能会对用户的数据内容感到好奇，甚至擅自将数据泄露给 DO 的竞争对手以获取不当利益. 因此，本文方案只存储数据密文至 IPFS.

CB 是指由多个机构共同参与管理的区块链，用户节点只有满足指定 CB 的准入机制才能加入区块链. 与公有链相比，CB 可以更好地保护隐私数据且更具灵活性. 由于区块链上空间有限，CB 只存储密钥和密文哈希值的对应关系及对称密钥集合密文. 密钥和密文哈希值的对应关系是利用哈希表来存储的，其中键为密文哈希值索引、值为对应的密文哈希值. 本方案中密文哈希值索引是自增的，不会出现键冲突的情况，因此可以根据密文哈希值索引得到对应的密文哈希值.

### 2.2 方案构造

现有的基于 CP-ABE 算法的数据共享方案中，采

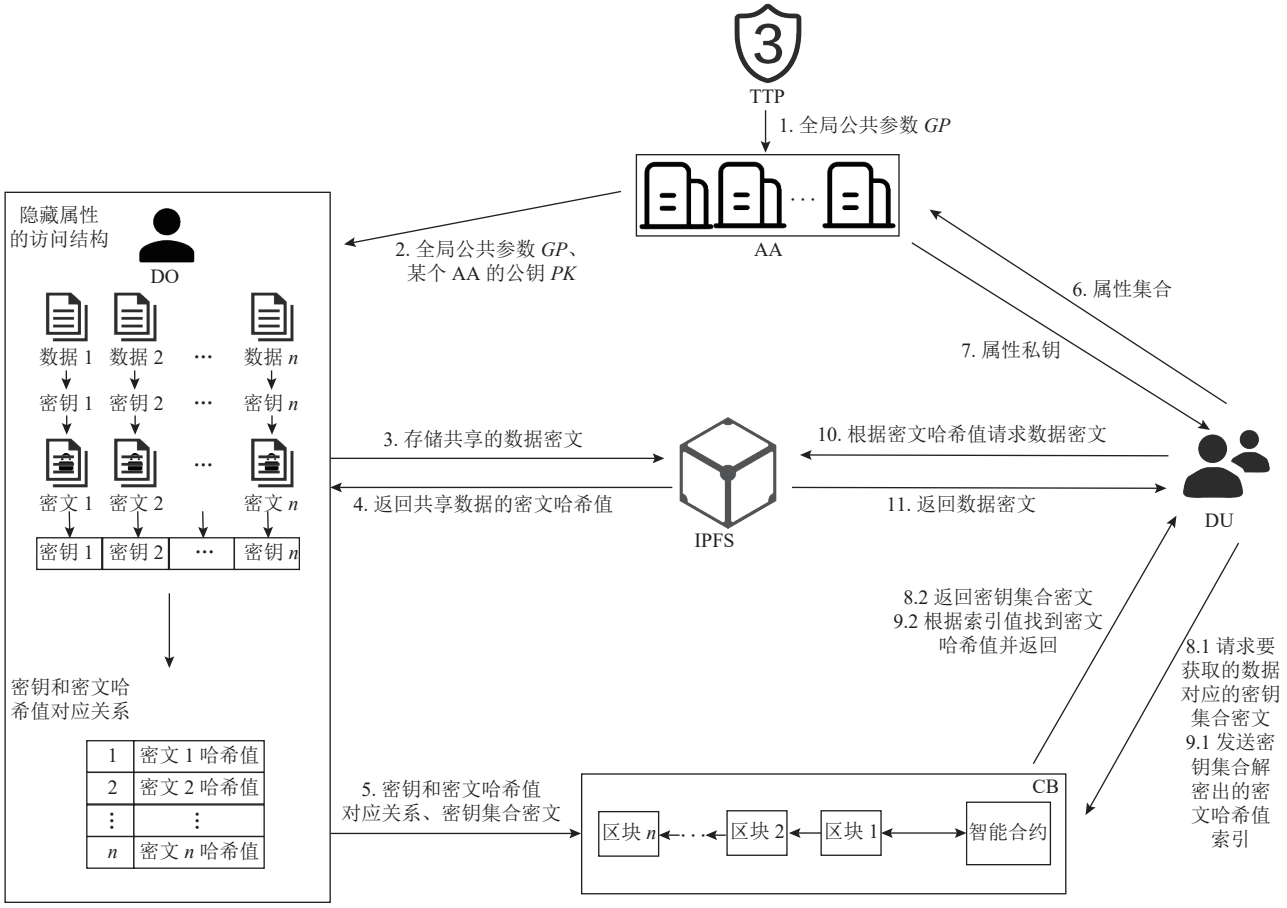



Fig. 1 IoT data sharing scheme model

图 1 物联网数据共享方案模型

用的都是单秘密共享算法，即 1 次秘密共享过程只能共享 1 个秘密. 如果要共享另一个秘密，秘密分发者必须为所有的参与者重新分配新的秘密份额，而且多次秘密分发会加重秘密分发者的计算开销. 本文采用多秘密共享算法，不仅实现 1 次数据共享过程共享多个秘密，而且秘密份额也得到了重用，数据共享效率更高. 本文方案分为：系统初始化、数据加密和数据解密 3 个阶段.

2.2.1 系统初始化

1) 全局参数生成

TTP 执行全局设置算法$Global\ Setup(\lambda)\rightarrow GP$，以安全参数$\lambda$为输入，输出系统全局公共参数$GP$.

① 选择一个阶为$N=p_1p_2p_3$的双线性群$G$，其中$p_1, p_2, p_3$为 3 个素数；

② 选择一个将全局身份$GID$映射到群$G$中的哈希函数$H:\{0,1\}^*\rightarrow G$；

③ 输出全局公共参数$GP=\{N, g_1, G_{p_1}, H\}$，其中$g_1$为$G_{p_1}$的生成元，$G_{p_1}$为$G$的子群.

2) AA 参数生成

每个 AA 执行机构生成算法$AuthoritySetup(GP)\rightarrow(SK, PK)$进行初始化，生成该 AA 的公钥$PK$和私钥$SK$.

① 对于每一个属性$i$，AA 随机选取 2 个指数$\alpha_i, y_i\in Z_N$；

② 输出该 AA 的公钥$PK=\{e(g_1,g_1)^{\alpha_1}, g_1^{y_i}\forall i\}$和私钥$SK=\{\alpha_i, y_i\forall i\}$.

2.2.2 数据加密

1)数据对称加密

DO 使用 AES 算法加密要共享的物联网数据，由于 1 次共享过程可以共享多份数据，因此用来加密数据的对称密钥也就存在多个. 数据密文会被存储到 IPFS 中，DO 会接收到 IPFS 返回的数据密文哈希值.

2)隐藏属性的访问策略构建

访问策略是整个秘密共享算法的访问控制中心，用于表明哪些参与者(属性)可以合作恢复所共享的秘密. 哪些参与者合作不能恢复秘密. 在访问结构中，叶子节点表示参与者，非叶子节点表示门限. 例如(2, 3)门限，表示任何 2 个及以上参与者联合才可以恢复

所共享的秘密. 使用 128 b MurmurHash3 算法隐藏属性的访问策略如图 2 所示.

在构建访问策略过程中, 需要将根节点的秘密值(对称密钥集合)递归地分发给每个节点, 分发采用 CTM-SS[22] 方案中的秘密分发算法来实现. 该秘密分发算法如算法 1 所示. 设$n$个参与者构成的集合为$P=\{P_1, P_2, \cdots, P_n\}$, $S$表示秘密集合, 设$G_1=\{k_{1,1}, k_{1,2}, \cdots, k_{1,p_1}\}$, $G_2=\{k_{2,1}, k_{2,2}, \cdots, k_{2,p_2}\}$, $G_m=\{k_{m,1}, k_{m,2}, \cdots, k_{m,p_m}\}\subset S$为$m$组需要共享的秘密. 每组$G_i$包含的秘密个数可以不同, 这里假设$1\leqslant p_1\leqslant p_2\leqslant\cdots\leqslant p_m$, 并根据不同的$(t_i, n)(1\leqslant i\leqslant m)$门限结构进行共享, 其中门限值满足$1\leqslant t_1\leqslant t_2\leqslant\cdots\leqslant t_m$.

**算法 1.** 秘密分发算法.

输入: $S, p_i, t_i, m, n$;

输出: 每个参与者分配的子份额$y_i$.

① 选择$m$个素数$q_1<q_2<\cdots<q_m$, 满足$k_{i,j}<q_i$ $(1\leqslant i\leqslant m, j=1, 2, \cdots, p_i)$, $n<q_1$和$p_m<q_1$;

② 若$p_m>t_1$, 还需$p_m-t_1+1+n<q_1$;

③ if$(p_m>t_1)$

④ 选择$n$个不同的整数$x_1, x_2, \cdots, x_n$作为参与者$P$的公开身份标识信息, $x_i\in[p_m-t_1+1, q_1)$;

⑤ else

⑥ 选择$n$个不同的整数$x_1, x_2, \cdots, x_n$作为参与者$P$的公开身份标识信息, $x_i\in[1, q_1]$;

⑦ end if

⑧ 令$a_0, a_1, \cdots, a_{p_m-1}$分别为$p_m$组恒等式的解;

⑨ $for\ (i=0; i<p_m-1; i++)$

⑩
$$\begin{cases} a_i\equiv k_{1,i+1} \bmod q_1, \\ a_i\equiv k_{2,i+1} \bmod q_2, \\ \quad\vdots \\ a_i\equiv k_{m,i+1} \bmod q_m, \end{cases}$$

若$k_{1,i+1}, k_{2,i+1}, \cdots, k_{m,i+1}$不存在, 令$k_{1,i+1}, k_{2,i+1}, \cdots, k_{m,i+1}=0$;

⑪ end for

⑫ if$(p_m>t_1)$

⑬ 计算$b_j=c_j r_j\prod_{k=1}^{i}q_k \bmod M$, 其中 $i\in[1, m-1], j\in[t_1, t_{i+1}-1]$, $M=\prod_{i-1}^{m}q_i$, $c_j\in[1, q_i)$, $r_j\in N^*$;

⑭ 以$a_0, a_1, \cdots, a_{p_m-1}, b_{t_1}, b_{t_1+1}, \cdots, b_{t_m-1}$为系数, 构造一个$p_m+t_m-t_1-1$阶多项式: $H(x)=a_0+a_1x+\cdots+a_{p_m-1}x^{p_m-1}+b_{t_1}x^{p_m}+\cdots+b_{t_m-1}x^{p_m+t_m-t_1-1}$;

⑮ else

⑯ 在$(1, M)$上选择$t_1-p_m$个整数, 其中$M=\prod_{i=1}^{m}q_i$;

⑰ 计算$a_j=c_j r_j\prod_{k=1}^{i}q_k \bmod M$, 其中 $i\in[1, m-1], j\in[t_1, t_{i+1}-1]$, $c_j\in[1, q_i), r_j\in N^*$;

⑱ 以$a_0, a_1, \cdots, a_{t_m-1}$为系数, 构造一个$t_m-1$阶多项式: $H(x)=a_0+a_1x+\cdots+a_{t_m-1}x^{t_m-1}$;

⑲ end if

⑳ 计算参与者$P_i, i\in[1, n]$的子份额: $y_i=H(x_i)\bmod M$;

㉑ if$(p_m>t_1)$

㉒ 对$i=1, 2, \cdots, p_m-t_1$, 先计算公共值$d_i=H(i) \bmod M$, 再公布$d_i$;

㉓ end if

㉔ 将$y_i$分配给相应的参与者$P_i$, 公布$q_1, q_2, \cdots, q_m$, 返回每个参与者的子份额$y_i$.

3) 密钥集合加密以及信息上链

DO 使用隐藏属性的访问策略加密对称密钥集合(对称密钥集合就是要共享的多个秘密), 然后将对称密钥集合密文、密钥和密文哈希值对应关系通过智能合约上传至 CB.

2.2.3 数据解密

1)根据隐藏属性的访问策略使用属性集重构秘密. DU 从 CB 上得到对称密钥集合密文, DU 使用自身的属性集合来重构某个对称密钥, 重构采用 CTM-SS[22] 方案中的秘密重构算法来实现. 若 DU 的属性

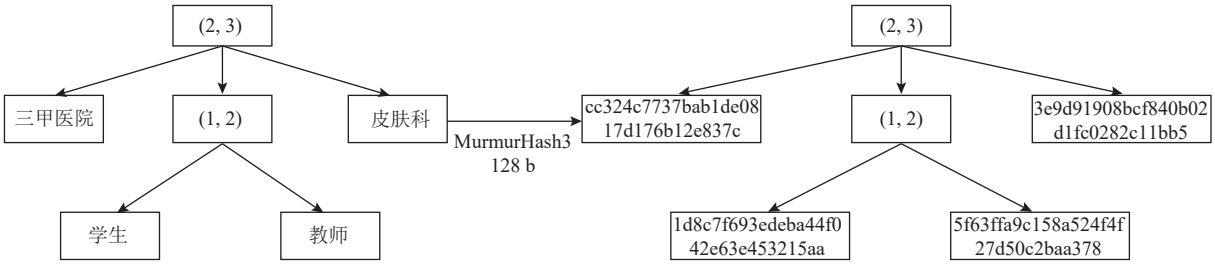



Fig. 2 Access policy for hidden attributes

图 2 隐藏属性的访问策略

集合为授权集合, 则解密成功; 否则, 解密失败. 该秘密重构算法如算法 2 所示. 算法 2 中, 以授权集合 $A=\{P_1, P_2, \cdots, P_{t_i}\}$为例来说明秘密重构的过程, 假设$A$要重构第$i(1\leqslant i\leqslant m)$组秘密$\{k_{i,1}, k_{i,2}, \cdots, k_{i,p_i}\}$, 其门限值为$t_i$.

**算法 2.** 秘密重构算法.

输入: $A, i, t_i$,

输出: $\{k_{i,1}, k_{i,2}, \cdots, k_{i,p_i}\}$.

① 每个参与者$P_j$, $j\in[1, t_i]$出示他们的子份额$y_j$;

② 计算$y_{i,j}=y_j \bmod q_i$, 得到$t_i$个点
$(x_1, y_{i,1}), (x_2, y_{i,2}), \cdots, (x_{t_i}, y_{i,t_i})$;

③ if$(p_m>t_1)$

④ 由公共值$d_i$, $i\in[1, p_m-t_1]$, 计算$d_i'\equiv d_i \bmod q_i$;

⑤ 得到$p_m-t_1$个点$(1, d_1'), (2, d_2'), \cdots,$
$(p_m-t_1, d'_{p_m-t_1})$;

⑥ 利用$p_{\mathrm{m}}-t_1+t_i$个点, 通过 Lagrange 插值多项式重构多项式$H_i(x)=a_0+a_1x+\cdots+a_{p_m-1}x^{p_m-1}+b_{t_1}x^{p_m}+b_{t_2}x^{p_{m+1}}+\cdots+b_{t_i-1}x^{p_m+t_i-t_1-1} \bmod q_i$;

⑦ else

⑧ 利用$t_i$个点, 通过 Lagrange 插值多项式重构多项式$H_i(x)=a_0+a_1x+\cdots+a_{p_i-1}x^{p_i-1}+a_{p_m}x^{p_m}+\cdots+a_{t_i-1}x^{t_i-1} \bmod q_i$;

⑨ end if

⑩ 已知$H_i(x)$的前$p_i$个系数, 求出秘密
$\{k_{i,1}, k_{i,2}, \cdots, k_{i,p_i}\}=\{a_0 \bmod q_i, a_1 \bmod q_i, \cdots, a_{p_i-1} \bmod q_i\}$;

⑪ 返回秘密$\{k_{i,1}, k_{i,2}, \cdots, k_{i,p_i}\}$.

2)根据 DU 重构出的秘密$\{k_{i,1}, k_{i,2}, \cdots, k_{i,p_i}\}$可知, 对称密钥为$\{k_{i,1}, k_{i,2}, \cdots, k_{i,p_{i-1}}\}$、对称密钥对应的密文哈希值索引为$k_{i,p_i}$. 通过密钥和密文哈希值的对应关系, 即可从 CB 上获取到数据对应的密文哈希值, 进而得到密文. 最后, DU 根据密钥解密出相应的数据.

### 2.3 智能合约设计

本文方案设计数据共享智能合约(data sharing smart contract, DSSC), 采用 Solidity 语言进行编写. DO 和 DU 通过调用 DSSC 合约实现共享数据的存储和获取. DSSC 合约的基本业务设计如表 1 所示.

DSSC 合约定义了 2 个引用类型的状态变量 *secretKeyAndHash* 和 *secretKeySetCiphertext*, 分别表示映射和字符串. 为了验证合约方法的正确性, 基于 Remix 环境对 3 种合约方法进行了编译部署. 3 种合约方法的具体代码实现如图 3 所示.

**Table 1 DSSC Contract Business Design**

**表 1 DSSC 合约业务设计**

| 功能 | 合约方法 | 调用者 |
|---|---|---|
| 密文哈希值上链 | *uploadCTHashs*( ) | DO |
| 由索引值获取对应的密文哈希值 | *getCTHash*( ) | DU |
| 获取密钥集合密文 | *getSKSet*( ) | DU |

## 3 方案分析

### 3.1 安全性分析

**定理 1.** 隐藏属性的访问策略不会泄露任何有价值的信息.

证明. 在隐私保护设计中, 摒弃可能泄露隐私信息的明文访问策略, 以经过 MurmurHash3 128 b 哈希算法处理后的访问策略实现策略的完全隐藏. 因为哈希算法所计算出来的哈希值具有不可逆性, 即使攻击者得到了访问策略, 也就只能看到无数个属性哈希值, 无法逆向演算回原本的属性信息, 因此任何人都不可能知道属性和其对应的属性哈希值之间的对应关系. 故该策略可有效地保护属性信息. 证毕.

**定理 2.** 在多秘密共享过程中, 不同的门限访问结构不会影响系统的安全性.

证明. 由算法 1 可知, 当$P_m>t_1$时, 会构造一个$P_m+t_m-t_1-1$阶的多项式$H(x)$. 因此, 至少需要知道$P_m+t_i-t_1(1\leqslant i\leqslant m)$个满足$H_i(x)$的点, 才能重构$H_i(x)$. 由于公布了$P_m-t_1$个点, 至少还需要$t_i$个参与者合作才能重构$H_i(x)$, 从而恢复秘密, 而$t_i-1$个或更少的参与者将不能合作重构$H_i(x)$, 这满足 Shamir 门限方案的安全性. 当$P_m\leqslant t_1$时, 会构造一个$t_m-1$阶的多项式$H(x)$. 因此, 至少还需要$t_i$个参与者合作才能重构$H_i(x)$, 从而恢复秘密, 而$t_i-1$个或更少的参与者将不能合作重构$H_i(x)$, 这也满足了 Shamir 门限方案的安全性. 本文方案中, 每组秘密可以根据不同的门限访问结构进行共享, 每次秘密重构过程都会根据上述 2 种情况进行分类讨论, 若要重构出所共享的秘密, 必须重构$t_i-1$次 Lagrange 插值多项式$H_i(x)$. 而对于$t_i-1$个或更少的参与者来说, 想要计算出所共享的秘密, 等价于攻破 Shamir 门限方案, 这在计算上是不可行的. 证毕.

**定理 3.** 本文方案可以确保数据共享的安全性.

证明. 本文方案以文献 [18] 中的 CP-ABE 算法为原型, 使用多秘密共享算法替换传统的单秘密共享

```
function uploadCTHashs(string[] memory hashs, string memory _secretKeySetCiphertext) public {
    uint256 j = 0;
    /*将密文哈希值存入mapping中*/
    for (j = 0;  j < hashs.length; j++) {
        secretKeyAndHash[j] = hashs[j];
    }
    /*密钥集合密文上链*/
    secretKeySetCiphertext = _secretKeySetCiphertext;
}

function getCTHash(uint256 _key) public view returns (string memory) {
    /*获取密钥集合密文*/
    getSKSet();
    if (bytes(secretKeyAndHash[_key]).length > 0) {
        return secretKeyAndHash[_key];
    }
    /*若mapping中不存在_key，则返回"No Found Hash"*/
    return "No Found Hash";
}
function getSKSet() public view returns (string memory) {
  return secretKeySetCiphertext;
}
```

Fig. 3 Contract methods

图 3 合约方法

算法，提出一种新型的多授权机构 CP-ABE 算法，CP-ABE 算法的安全性并未降低. 首先，DO 所共享的数据皆已加密；其次，使用改进后的多授权机构 CP-ABE 算法加密对称密钥集合；最后，只有授权用户方可解密出数据. 在本文方案中，即使攻击者得到了密钥和密文哈希值的对应关系，也不会降低本文方案的安全性，因为在密钥和密文哈希值的对应关系中，并不存储真正的密钥，而是以密钥的索引值和密文哈希值形成的键值对. 攻击者不能从对应关系中反推出密钥，只能获得密文哈希值，根据密文哈希值从 IPFS 中检索出密文，由于缺乏密钥，也不会对方案的安全性造成威胁. 证毕.

### 3.2 性能分析

在共享多组秘密(数据加密阶段描述的$m$组秘密$G_1, G_2, \cdots, G_m$)的情况下，将本文方案使用到的秘密共享算法和文献 [24] 中使用到的秘密共享算法进行分析.

文献 [24] 中，在$(t_i, n)$门限访问结构上共享一组秘密$G_i$，秘密分发过程需要构造一个$n$阶的 Lagrange 插值多项式，若共享$m$组秘密，就需要进行$m$次秘密分发，重复计算量较大. 而对于本文方案，在$(t_i, n)$门限访问结构上共享$m$组秘密时，秘密分发过程只需构造一个$t_m-1$(当 $p_m \leqslant t_1$时)阶或 $p_m+t_m-t_1-1$(当 $p_m > t_1$时)阶的 Lagrange 插值多项式，即秘密分发仅需 1 次，就可以实现$m$组秘密共享. 因此，本文方案中使用到的秘密共享算法实现简单、计算量小，对于共享多组秘密具有优势.

### 3.3 功能对比分析

将本文方案与文献 [7,10−11,24] 中提出的数据共享方案就各项功能特性进行对比，结果如表 2 所示. 由表 2 可知，文献 [7,11,24] 都是采用单授权机构的 CP-ABE 方案，而且文献 [7,11] 只实现了策略部分隐藏，文献 [24] 不具有策略隐藏功能. 文献 [10] 虽然支持多授权机构和策略完全隐藏，但其使用到的秘密共享算法为单秘密共享. 多秘密共享算法可以一次共享多个秘密信息，所消耗的计算量远小于重复多次使用单秘密共享算法造成的开销. 因此，本文方案在联盟链环境下实现了数据细粒度访问控制，采用多授权机构和多秘密共享算法提高了系统运行的性能和数据共享的效率，也保证了策略的安全性.

**Table 2 Function Comparison**

**表 2 功能对比**

| 方案 | 授权机构数量 | CP-ABE | 区块链 | 秘密共享算法类型 | 策略隐藏 |
|---|---|---|---|---|---|
| 文献 [7] | 少 | √ | × | 单秘密共享 | 部分隐藏 |
| 文献 [10] | 多 | √ | √ | 单秘密共享 | 完全隐藏 |
| 文献 [11] | 少 | √ | √ | 单秘密共享 | 部分隐藏 |
| 文献 [24] | 少 | √ | × | 单秘密共享 | × |
| 本文方案 | 多 | √ | √ | 多秘密共享 | 完全隐藏 |

注：“×”表示未使用某种技术；“√”表示使用某种技术.

## 4 仿真实验

仿真实验使用 JPBC(Java pairing-based cryptography)库和 Google Guava 工具包进行代码编写，在 8 GB 内存、Intel® Core™ i7-7700HQ CPU、Windows10 操作系统环境下运行，结果均采用 10 次实验的平均运行时间.

### 4.1 策略隐藏性能

为验证本文方案中策略隐藏方法较文献 [7] 所具有的优势，对其时间开销进行对比实验. 实验结果如图 4 和表 3 所示：当属性个数为 1.2 万时，文献 [7] 采取的策略隐藏方法耗时几乎是本文方案的 2 倍.

### 4.2 秘密分发性能

秘密分发性能以秘密个数和属性个数为变量，测试各个方案的运行时间. 图 5(a)(b)(c)(d)分别以属性个数为 4, 8, 16 和 32 时测试秘密分发阶段的时间开销. 由于本文方案使用的秘密共享算法为多秘密共享，多个秘密共享只需要 1 次秘密分发过程；而文献 [7, 24] 要想实现多个秘密共享，则需要多次秘密分发过程. 从图 5 和表 4 可以看出，随着属性个数和秘密个数的增大，本文方案秘密分发过程的计算量将远低于文献 [7, 24].

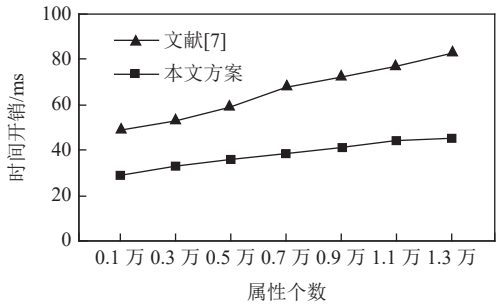



Fig. 4 Policy hiding performance

图 4 策略隐藏性能

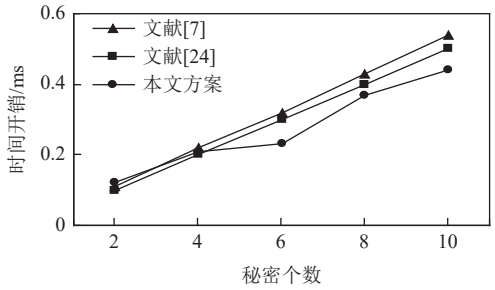
**Table 3 Policy Hiding Performance**

**表 3 策略隐藏性能**

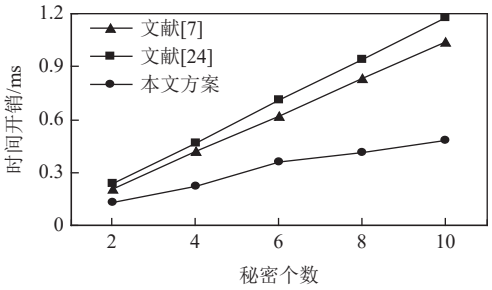
| 属性个数 | 时间开销/ms | |
|---|---|---|
| | 文献 [7] | 本文方案 |
| 1 000 | 50.0 | 28.9 |
| 3 000 | 55.0 | 35.0 |
| 6 000 | 69.0 | 39.0 |
| 9 000 | 74.6 | 43.6 |
| 12 000 | 84.0 | 45.0 |

## 5 结束语

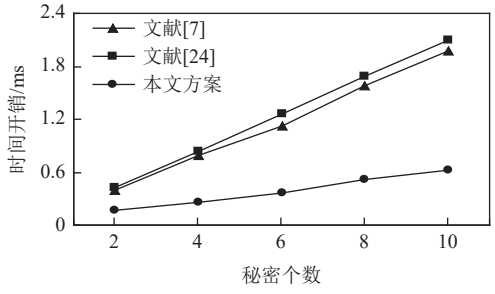
本文使用多授权机构 CP-ABE 算法设计了一种支持访问策略完全隐藏的物联网数据共享方案. 该方案不但解决了单属性机构 CP-ABE 方案导致的系统运行瓶颈的弊端，还使用 MurmurHash3 算法对访问策略进行完全隐藏，保护了访问策略的隐私安全.



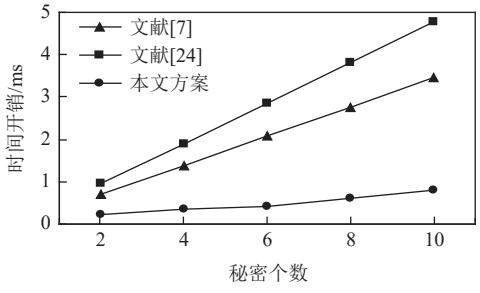

(a) 属性个数为 4 时的时间开销




(b) 属性个数为 8 时的时间开销




(c) 属性个数为 16 时的时间开销




(d) 属性个数为 32 时的时间开销

Fig. 5 Secret distribution performance

图 5 秘密分发性能

**Table 4 Secret Distribution Performance**

**表 4 秘密分发性能**

| 属性个数 | 秘密个数 | 时间开销/ms | | |
|---|---|---|---|---|
| | | 文献 [7] | 文献 [24] | 本文方案 |
| 4 | 2 | 0.11 | 0.10 | 0.12 |
| | 4 | 0.22 | 0.20 | 0.21 |
| | 6 | 0.32 | 0.30 | 0.23 |
| | 8 | 0.43 | 0.40 | 0.37 |
| | 10 | 0.54 | 0.50 | 0.44 |
| 8 | 2 | 0.21 | 0.24 | 0.13 |
| | 4 | 0.42 | 0.47 | 0.22 |
| | 6 | 0.62 | 0.71 | 0.36 |
| | 8 | 0.83 | 0.94 | 0.41 |
| | 10 | 1.04 | 1.18 | 0.48 |
| 16 | 2 | 0.40 | 0.42 | 0.16 |
| | 4 | 0.79 | 0.84 | 0.26 |
| | 6 | 1.12 | 1.26 | 0.37 |
| | 8 | 1.58 | 1.68 | 0.51 |
| | 10 | 1.98 | 2.10 | 0.62 |
| 32 | 2 | 0.69 | 0.95 | 0.21 |
| | 4 | 1.38 | 1.90 | 0.34 |
| | 6 | 2.08 | 2.86 | 0.42 |
| | 8 | 2.77 | 3.81 | 0.61 |
| | 10 | 3.46 | 4.76 | 0.81 |

不仅如此，本文引入多秘密共享算法代替传统的单秘密共享算法，做到一次共享过程可以共享多份数据，且每份数据可以具有不同的门限访问结构. 本文方案不但提高了资源利用率，而且为物联网数据共享方案提供了新思路. 安全性分析验证了本文方案的有效性，仿真实验结果表明了本文方案的高效性. 为进一步拓展策略隐藏的多授权机构 CP-ABE 数据共享方案的功能，未来将考虑实现可搜索加密.

**作者贡献声明**：张学旺指导选题，设计研究方案、论文结构，修改完善论文；姚亚宁负责搜集、整理实验数据，调研、整理文献，设计研究方案，实施研究过程，以及撰写论文；付佳丽协助收集、整理实验数据，参与研究过程；谢昊飞指导选题，修改论文.

## 参 考 文 献

[1] Liu Qixu, Jin Ze, Chen Canhua, et al. Survey on Internet of things access control security[J]. Journal of Computer Research and Development, 2022, 59(10): 2190−2211 (in Chinese)
(刘奇旭, 靳泽, 陈灿华, 等. 物联网访问控制安全性综述[J]. 计算机研究与发展, 2022, 59(10): 2190−2211)

[2] Cai Ting, Lin Hui, Chen Wuhui, et al. Efficient blockchain-empowered data sharing incentive scheme for Internet of things[J]. Journal of Software, 2021, 32(4): 953−972 (in Chinese)
(蔡婷, 林晖, 陈武辉, 等. 区块链赋能的高效物联网数据激励共享方案[J]. 软件学报, 2021, 32(4): 953−972)

[3] Liu Mingda, Chen Zuoning, Shi Yijuan, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1−27 (in Chinese)
(刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1−27)

[4] 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

[5] Chase M. Multi-authority attribute based encryption[C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2007: 515−534

[6] Lin Huang, Cao Zhenfu, Liang Xiaohui, et al. Secure threshold multi-authority attribute based encryption without a central authority[J]. Information Sciences, 2010, 180(13): 2618−2632

[7] Zhang Leyou, Wang Jun, Mu Yi. Privacy-preserving flexible access control for encrypted data in Internet of things[J]. IEEE Internet of Things Journal, 2021, 8(19): 14731−14745

[8] 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)

[9] Liu Xuejiao, Cao Tiancong, Xia Yingjie. Research on efficient and secure cross-domain data sharing of IoV under blockchain architecture[J]. Journal on Communications, 2023, 44(3): 186−197 (in Chinese)
(刘雪娇, 曹天聪, 夏莹杰. 区块链架构下高效的车联网跨域数据安全共享研究[J]. 通信学报, 2023, 44(3): 186−197)

[10] Dai Weiqi, Tuo Shuyue, Yu Liangliang, et al. HAPPS: A hidden attribute and privilege-protection data-sharing scheme with verifiability[J]. IEEE Internet of Things Journal, 2022, 9(24): 25538−25550

[11] Zhao Zhiyuan, Wang Jianhua, Zhu Zhiqiang, et al. Attribute-based encryption for data security sharing of Internet of things[J]. Journal of Computer Research and Development, 2019, 56(6): 1290−1301 (in Chinese)
(赵志远, 王建华, 朱智强, 等. 面向物联网数据安全共享的属性基加密方案[J]. 计算机研究与发展, 2019, 56(6): 1290−1301)

[12] Lin Li, Chu Zhenxing, Liu Zimeng, et al. A policy-hidden big data access control method based on blockchain[J]. Acta Automatica Sinica, 2023, 49(5): 1031−1049 (in Chinese)
(林莉, 储振兴, 刘子萌, 等. 基于区块链的策略隐藏大数据访问控制方法[J]. 自动化学报, 2023, 49(5): 1031−1049)

[13] Wu Qing, Lai Taotao, Zhang Leyou, et al. Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud[J]. Journal of Systems Architecture, 2022,

129: 102569

[14] Wang Huiyong, Liang Jialing, Ding Yong, et al. Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health[J]. Computer Standards & Interfaces, 2023, 84: 103696

[15] Zhang Zhaoqian, Zhang Jianbiao, Yuan Yilin, et al. An expressive fully policy-hidden ciphertext policy attribute-based encryption scheme with credible verification based on blockchain[J]. IEEE Internet of Things Journal, 2021, 9(11): 8681−8692

[16] Zhang Zhishuo, Zhang Wei, Qin Zhiguang. A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted cloud computing[J]. Future Generation Computer Systems, 2021, 123: 181−195

[17] Zhang Xuewang, Yao Yaning, Li Zhihong, et al. Data scheme based on consortium blockchain and Asmuth-Bloom secret sharing algorithm[J]. Netinfo Security, 2022, 22(11): 17−23 (in Chinese)
(张学旺, 姚亚宁, 黎志鸿, 等. 基于联盟链和Asmuth-Bloom秘密共享算法的数据共享方案[J]. 信息网络安全, 2022, 22(11): 17−23)

[18] Lewko A, Waters B. Decentralizing attribute-based encryption[C] // Proc of the 30th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568−588

[19] Li Yahong, Wang Caifen, Zhang Yulei, et al. Security obfuscation for encrypted threshold signatures[J]. Journal on Communications, 2020, 41(6): 61−69 (in Chinese)
(李亚红, 王彩芬, 张玉磊, 等. 安全加密的门限签名混淆[J]. 通信学报, 2020, 41(6): 61−69)

[20] Chen Lüjun, Xiao Di, Yu Zhuyang, et al. Communication-efficient federated learning based on secret sharing and compressed sensing[J]. Journal of Computer Research and Development, 2022, 59(11): 2395−2407 (in Chinese)
(陈律君, 肖迪, 余柱阳, 等. 基于秘密共享和压缩感知的通信高效联邦学习[J]. 计算机研究与发展, 2022, 59(11): 2395−2407)

[21] Shen Jian, Zhou Tianqi, Cao Zhenfu. Protection method for cloud data security[J]. Journal of Computer Research and Development, 2021, 58(10): 2079−2098 (in Chinese)
(沈剑, 周天祺, 曹珍富. 云数据安全保护方法综述[J]. 计算机研究与发展, 2021, 58(10): 2079−2098)

[22] Pang Liaojun, Pei Qingqi, Li Huixian, et al. Secret sharing technology and its applications[M]. Beijing: post & Telewm press, 2017: 104−112 (in Chinese)
(庞辽军, 裴庆祺, 李慧贤, 等. 秘密共享技术及其应用[M]. 北京: 人民邮电出版社, 2017: 104−112)

[23] Zhu Enguo, Ye Fangbin, Dou Jian, et al. A comparison method of massive power consumption information collection test data based on improved merkle tree[C] //Proc of the 4th Int Conf of Pioneering Computer Scientists, Engineers and Educators. Berlin: Springer, 2018: 401−415

[24] Li Ruixuan, Shen Chenglin, He Heng, et al. A lightweight secure data sharing scheme for mobile cloud computing[J]. IEEE Transactions on Cloud Computing, 2018, 6(2): 344−357

**Zhang Xuewang**, born in 1974. PhD, associate professor, master supervisor, Senior member of CCF. His main research interests include blockchain and Internet of things, and data security and privacy protection.

**张学旺**, 1974 年生. 博士, 副教授, 硕士生导师. CCF 高级会员. 主要研究方向为区块链与物联网、数据安全与隐私保护.

**Yao Yaning**, born in 1998. Master candidate. Student member of CCF. His main research interests include blockchain, Internet software, and security technologies.

**姚亚宁**, 1998 年生. 硕士研究生. CCF 学生会员. 主要研究方向为区块链、互联网软件、安全技术.

**Fu Jiali**, born in 1998. Master candidate. Student member of CCF. Her main research interests include blockchain, Internet software, and security technologies.

**付佳丽**, 1998 年生. 硕士研究生. CCF 学生会员. 主要研究方向为区块链、互联网软件、安全技术.

**Xie Haofei**, bom in 1978. PhD, professor, master supervisor. His main research interests include networked control systems, wireless sensing, and the industrial Internet of things.

**谢昊飞**, 1978 年生. 博士, 教授, 硕士生导师. 主要研究方向为网络化控制系统、无线感知、工业物联网.