doi：10.13413/j.cnki.jdxblxb.2023359

# 蜂窝物联网匿名访问用户身份认证算法

郭 文 俊

（山西大同大学 计算机与网络工程学院，山西 大同 037009）

**摘要**：针对蜂窝物联网涉及大规模设备的连接和身份认证管理，且攻击者会使用各种方法伪造身份信息，使得匿名访问用户身份认证难度增大的问题，提出一种蜂窝物联网匿名访问用户身份认证算法. 首先，以 5G 网络为蜂窝物联网系统的动态应用场景，预置系统参数；其次，根据用户的身份标识号和公钥，利用伪造名称生成用户的匿名访问信息，注册匿名存至本地；最后，基于去中心化理念，对比单元公钥与邻单元群密钥、随机数加密信息与单元 Hash 值的解密结果，认证用户身份. 实验结果表明，该算法有效缩短了身份认证与批量消息验证所需时间，减少了数据传输所需字节数，时间开销仅为 13 ms，计算开销仅为 4 ms，通信开销仅为 210 字节，且能成功抵御 15 种身份认证攻击类型.

**关键词**：蜂窝物联网；5G 网络；匿名访问；身份认证；椭圆曲线加密；Hash 函数

**中图分类号**：TP393 **文献标志码**：A **文章编号**：1671-5489(2024)03-0636-07

# Anonymous Access User Identity Authentication Algorithm for Cellular Internet of Things

GUO Wenjun

(*School of Computer and Network Engineering*, *Shanxi Datong University*, *Datong* 037009, *Shanxi Province*, *China*)

**Abstract**: Aiming at the problem that the cellular Internet of Things involved large-scale device connection and identity authentication management, and attackers cuold use various methods to forge identity information, which made the difficulty of anonymous access user identity authentication increase, the author proposed an anonymous access user identity authentication algorithm for cellular Internet of Things. Firstly, the 5G network was used as the dynamic application scenario of the cellular Internet of Things system, and the system parameters were preseted. Secondly, according to the user's identification number and public key, the forged name was used to generate the user's anonymous access information, and the registration was anonymously saved to the local. Finally, based on the concept of decentralization, the decryption results of the unit public key and the adjacent group key, the random number encryption information and the unit Hash value were compared to authenticate the user identity. The experimental results show that the proposed algorithm effectively shortens the time required for identity authentication and batch message authentication, reduces the number of bytes required for data transmission, with a time cost of only 13 ms, a computational cost of only 4 ms, and a communication cost of only 210 bytes. Moreover, it can successfully resist 15

**收稿日期**：2023-08-30.

**作者简介**：郭文俊(1986—)，男，汉族，硕士，讲师，从事网络信息安全、区块链技术和物联网的研究，E-mail：sxdtdxgwj@126.com.

**基金项目**：山西省高等学校教学改革创新项目(批准号：J2021510)和山西大同大学青年科研基金(批准号：2020Q1).

types of identity authentication attacks.

Keywords: cellular Internet of Things; 5G network; anonymous access; identity authentication; elliptic curve encryption; Hash function

物联网技术的不断发展[1-2]使得越来越多的设备和系统连接到互联网上，形成庞大的蜂窝物联网. 蜂窝物联网通过多物理设备和虚拟设备，在网络中实现信息交换与共享[3-4]. 隐私安全作为蜂窝物联网业务的首要问题已被广泛关注[5]，由于用户访问物联网认证时通常会使用用户的真实信息，一旦有内部攻击者窃取这些信息，就会泄露用户隐私. 因此，用户身份认证成为物联网的主要安全机制，匿名性访问用户身份认证成为研究热点.

为能保护用户的匿名性，研究者们提出了匿名身份认证方法. 王振宇等[6]以资源受限的轻量级物联网设备为目标，以物理不可克隆函数为基础，设计了轻量级高效匿名身份认证协议；鲁晔[7]利用基于联盟链的分布式网络模型，划分基础域、互联域，分别针对两域实施去耦处理和匿名处理；赵宗渠等[8]融合了身份标识的匿签密算法和双线性映射算法，在用户口令和智能卡的支持下，构建了适用于物联网的身份隐藏认证方法.

以上方法均面向物联网环境的匿名身份认证，而针对蜂窝物联网的匿名身份认证研究相关报道较少，故本文将蜂窝物联网作为探索的一种网络类型，设计一种匿名访问用户的身份认证算法. 预置蜂窝物联网系统时，在 5G 通信监管模块中生成认证时与加解密相关的参数，由此自动生成密钥对，有助于确保信息在传输过程中的安全性；监管模块根据用户提交的基本信息，利用伪造名称完成匿名注册和签名，能保护用户隐私；基于去中心化理念完成匿名访问用户的身份认证，可加快身份认证效率和准确度.

# 1　匿名访问用户身份认证算法

## 1.1　蜂窝物联网参数预置

蜂窝物联网通常在资源受限(如计算能力、存储容量和能量等)的环境中运行[9]. 预置系统框架可提供有关资源约束信息，以确保匿名访问用户身份认证算法的可行性和适用性. 蜂窝物联网的系统架构如图 1 所示，其包含云服务器、核心网、基站和用户终端四部分. 各结构的功能和作用描述如下：

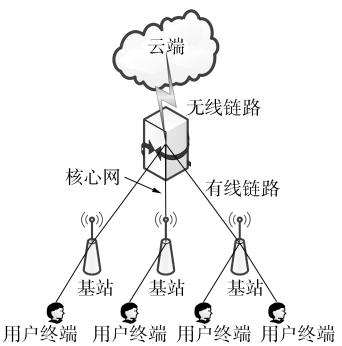



**图 1　蜂窝物联网系统架构示意图**

**Fig. 1　Schematic diagram of cellular IoT system architecture**

1) 用户终端作为蜂窝物联网的使用者与被服务者，可分为通信模组、通信权限模组、终端设备应用模组，其中通信权限模组包含核心网中终端的身份标识、编号等注册信息，是核心网进行身份认证与授权的唯一凭证；

2) 基站是用户终端与核心网之间的数据中转站，主要负责将终端的无线数据转化为有线数据后，上传至核心网；

3) 核心网既是数据与公用数据网实现交互的协议转换器，也是数据实现内部交互的路由，是蜂窝物联网运行过程中的关键节点，其根据储存的用户身份信息与通信权限签约信息，结合安全性信令进行认证、鉴权[10]；

4) 云端服务器具有远程管理用户终端界面及处理分析终端数据信息的能力，给终端下达应用控制指令.

以 5G 网络为蜂窝物联网系统的动态应用场景，在监管模块中生成认证时与加解密相关的参数，由此自动生成密钥对，确保信息在传输过程中的安全性[11-12]. 假设椭圆曲线的循环群生成元是 $G$，由其生成两个 $q$ 阶循环群，分别为 $G_1$ 和 $G_2$. 若自动生成的公钥与私钥分别为 $P_{\text{pub}}$，$s_{\text{pub}}$，则预置参数并

发送至各实体可表示为

$$X=\{G_1,G_2,q,G,s_{\text{pub}},P_{\text{pub}},H_1,H_2\},\tag{1}$$

其中 $H_1,H_2$ 分别为消息-摘要算法5和安全散列算法1两种Hash函数[13].

### 1.2 匿名访问用户注册信息整合

为实现用户的隐私保护和安全性，在实现用户身份认证前，首先匿名访问用户注册，使用户在使用蜂窝物联网服务时不需要提供真实身份信息，从而有效保护用户的隐私，防止个人敏感信息被泄露[14-15]. 监管模块根据用户提交的基本信息，利用伪造名称完成匿名注册与签名，保护用户隐私. 为避免监管模块权利集合化，利用以下步骤注册用户的匿名访问信息.

1) 假设第 $i$ 个用户的身份标识号、公钥和私钥分别为 $I_i,P_i,s_i$，则循环参数 $A_i$、标识号与公钥生成的消息-摘要算法5 Hash值 $B_i$ 及检验参数 $C_i$ 的生成公式为

$$\begin{cases}A_i=a_i\cdot\dfrac{G}{X},\\ B_i=\dfrac{H_1}{I_i\cdot G},\\ C_i=a_i\cdot s_i\cdot B_i,\end{cases}\tag{2}$$

其中 $a_i$ 表示该5G网络用户认证次数.

椭圆曲线加密[16-17]是一种基于椭圆曲线数学问题的公钥加密算法，具有相对较高的安全性、更小的密钥和数据尺寸，更适用于资源受限的蜂窝物联网环境. 因此，利用系统公钥 $P_{\text{pub}}$，通过

$$\delta=E_{P_{\text{pub}}}\{I_i,A_i,B_i,C_i\}\tag{3}$$

获取加密后的信息，并将其传输至监管模块，其中 $E_{P_{\text{pub}}}$ 表示公钥 $P_{\text{pub}}$ 的椭圆曲线加密系数，$A_i,B_i,C_i$ 为椭圆曲线加密处理参数.

2) 由于系统私钥只能由系统拥有，只有合法系统才能成功解密加密信息，并确认该请求来源合法，因此，通过使用系统私钥对加密后的信息进行解密，可以验证发送方的身份和授权，有助于防止未经授权的访问和保护系统免受恶意行为的影响[18]. 监管模块利用系统私钥 $s_{\text{pub}}$ 解密信息 $\delta$，通过下式检验信息的正确性：

$$C_i(G)=\frac{(A_i+B_i+C_i)/s_i}{\delta}.\tag{4}$$

根据上述步骤，监管模块注册信息时，匿名状态下的循环参数 $D_i$、安全散列算法1 Hash值 $E_i$ 及检验参数 $F_i$ 通过下列方程组生成：

$$\begin{cases}D_i=d_i\cdot G,\\ E_i=\dfrac{H_2}{P_{I_i}\cdot P_i/D_i},\\ F_i=\dfrac{d_i}{s_{\text{pub}}}\cdot E_i,\end{cases}\tag{5}$$

其中 $d_i$ 表示监管模块任选的随机数. 安全散列算法1 Hash值 $E_i$ 由匿名标识 $P_{I_i}$、公钥 $P_i$ 和循环参数 $D_i$ 生成. 利用公钥 $P_i$ 对参数进行椭圆曲线加密，得到加密信息 $\delta'$：

$$\delta'=E_{P_i}\{P_{I_i},D_i,E_i,F_i\}.\tag{6}$$

监管模块将用户的匿名标识 $P_{I_i}$ 和加密信息 $\delta'$ 分别传输至执法模块与对应用户后，进入下一步.

3) 通过私钥 $s_i$ 解密信息 $\delta'$ 后，根据下式检验信息的正确性：

$$F_i(G)=\frac{(D_i+E_i+F_i)/P_{\text{pub}}}{C_i(G)}\cdot\delta'.\tag{7}$$

生成注册信息为

$$\Im=A_i\cdot[F_i(G)/s_i].\tag{8}$$

将获取的参数 $\{P_{I_i},A_i,B_i,D_i,K_i,F,a_i\}$ 存至本地，完成匿名访问用户注册信息的整合.

### 1.3　用户身份认证

为加快用户身份认证的效率和准确度，基于去中心化理念[19-20]，可提高认证的安全性. 传统的中心化进行身份认证存在单点故障和攻击风险，一旦中心节点被攻击或失效，整个系统将受影响. 而通过去中心化的方式，认证过程分布在多个节点上，因此很难受单一节点的攻击和破坏[21-23]. 根据上述过程生成用户的匿名访问信息，完成匿名访问用户的身份认证，即单元对用户的认证，认证步骤如下.

1) 假设经第 $j$ 个单元公钥 $P_j$ 与群密钥 $K_j$ 加密后的用户信息为

$$M=[T,(P_i,E_{K_j}\{P_{I_i}\},E_{P_j}\{P_{I_i},a_i\}),U_{P_j}(D_i,F_i),\Im], \tag{9}$$

其中 $T$ 表示该信息的时间戳，$U_{P_j}(D_i,F_i)$表示由单元公钥生成的消息认证码. 若单元接收到此信息的时间与时间戳的时差在网络延迟的允许范围内[24-26]，则执行下一步.

2) 通过该单元公钥 $P_j$ 解密并检验信息 $E_{P_j}\{P_{I_i},a_i\}$；验证通过后，采用第$(j+1)$个单元的群密钥 $K_{j+1}$解密 $E_{K_j}\{P_{I_i}\}$.

3) 对比所得的两个解密结果，若二者相等，则认为该访问是合法的，匿名访问用户通过认证，结束流程；反之，则为非法用户，不允许进行匿名访问，进入下一阶段.

4) 令第 $j$ 个单元选取随机数 $b_j$，将下列信息发送给第 $i$ 个用户：

$$M'=[E_{b_j}\{I_j,Q_j\},U_{b_j}(D_i,F_i),M], \tag{10}$$

其中 $I_j$,$Q_j$ 分别表示该单元的真实身份和认证参数，$U_{b_j}(D_i,F_i)$表示由随机数 $b_j$ 生成的消息认证码. 若其通过式(7)的检验，则进行解密[27]，并发送下列信息给该单元：

$$M''=[T,P_i,E_{b_j}\{P_{I_i},I_i,Q_i,B_i\},U_{b_j}(D_i,F_i),M'], \tag{11}$$

其中 $Q_i$ 表示该用户的身份认证参数.

5) 重复步骤 3)和 4)，得到加密信息 $E_{b_j}\{P_{I_i},I_i,Q_i,B_i\}$解密结果中的 $B_i$ 值，利用

$$B_j=\frac{H_1\cdot M''}{(a_iQ_i,P_l)\cdot(a_is_j,I_i)} \tag{12}$$

解密单元的安全散列算法 1 Hash 值 $B_j$，若 $B_i$ 和 $B_j$ 相等，则匿名访问用户身份合法，实现用户身份认证，其中 $P_l$ 表示执法部门的公钥.

## 2　算法性能验证

为验证匿名访问用户身份认证算法的性能，设计对比实验. 选取包含 3 个基站和 10 个终端设备的典型蜂窝物联网作为实验环境，利用具有低功耗、长距离特点的 LoRa 通信技术连接智能终端设备与蜂窝物联网. 选择自由空间路径损耗模型(free space path loss，FSPL)模拟蜂窝物联网中的无线信号传输特性，以确保验证消息的顺利传输. 利用支持多种通信协议(如 MQTT，HTTP)的 Google Cloud IoT 收集匿名访问请求数据，在真实的运行场景内部署网关固件代码与终端程序，使实验数据更贴合实际. 为深入分析该算法的优势与劣势，选取高效匿名身份认证协议、基于联盟链的匿名交易方案、基于身份匿签密的认证方法作为试验活动的对比项.

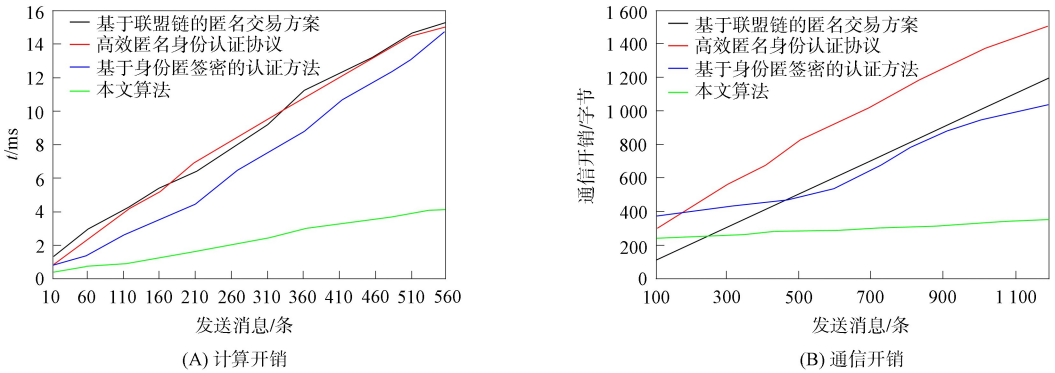
### 2.1　算法开销对比测试

计算开销和通信开销是算法性能的重要评估标准. 当身份认证时间或批量消息验证过程所需时间过长或数据传输所需字节数过多时，都会降低用户体验感，不利于算法的普及使用. 选取 1 100 个并发用户，560 条批量验证消息及 1 200 条发送消息，用这 3 个评估标准为指标，得到匿名访问用户身份认证算法的开销实验数据，结果如图 2 所示. 由图 2 中并发用户数、计算开销与批量验证消息条数、通信开销与消息发送条数变化关系可见，所有方法均使其呈现了一定的线性关系，但本文认证算法不仅线性函数斜率始终远小于对比方法，且初始开销也低于部分对比方法，计算开销仅为 4 ms，通信开销仅为 210 字节，具有显著优势. 这是因为本文算法通过蜂窝物联网系统预置、匿名访问用户注册、用户身份认证 3 个阶段，有效缩短了身份认证与批量消息验证所需时间，并减少了数据传输所需字节数.

### 2.2　算法安全性验证

基于匿名访问用户身份认证算法的设计目标及算法的攻击抵御能力，评估本文算法的安全性能.

4种不同方法的认证安全程度列于表1，其中“√”表示能抵御该类攻击，“×”表示不能抵御该类攻击.




(A) 计算开销 (B) 通信开销

**图2 匿名访问用户身份认证算法开销**

**Fig. 2 Anonymous access user identity authentication algorithm cost**

**表1 不同方法的匿名身份认证安全程度**

**Table 1 Degree of safety of anonymous identity authentication for different methods**

| 攻击属性 | 高效匿名身份认证协议 | 基于联盟链的匿名交易方案 | 基于身份匿签密的认证方法 | 本文算法 |
|---|---|---|---|---|
| 重放攻击 | √ | × | √ | √ |
| 中间人攻击 | × | √ | × | √ |
| 撞库攻击 | √ | √ | √ | √ |
| 会话劫持 | × | √ | × | √ |
| 注入攻击 | √ | × | √ | √ |
| 暴力攻击 | √ | √ | √ | √ |
| 字典攻击 | √ | √ | √ | √ |
| 凭据填充 | √ | √ | √ | √ |
| 非约束委派攻击 | √ | √ | × | √ |
| 约束委派攻击 | × | √ | √ | √ |
| 伪装攻击 | √ | √ | √ | √ |
| 匿名性 | × | × | × | √ |
| 前向保密性 | √ | √ | √ | √ |
| 后向保密性 | × | × | × | √ |
| 抗别名去同步攻击 | √ | √ | √ | √ |

由表1可见，3种对比方法只能抵御部分常见的身份认证攻击类型，对于匿名性与后向保密性两个安全性能则无效；而本文算法利用伪造名称完成匿名注册与签名，认证时无需发送真实的身份信息，确保了用户的匿名性，成功抵御了15种常见身份认证攻击类型，安全性更高.

综上所述，针对蜂窝物联网涉及大规模设备的连接和身份认证管理，且攻击者会使用各种方法伪造身份信息，使得匿名访问用户身份认证难度增大的问题，本文提出了一种蜂窝物联网匿名访问用户身份认证算法. 首先，以5G网络为蜂窝物联网系统的动态应用场景，预置系统参数；其次，根据用户的身份标识号和公钥，利用伪造名称生成用户的匿名访问信息，注册匿名存至本地；最后，基于去中心化理念，对比单元公钥与邻单元群密钥、随机数加密信息与单元Hash值的解密结果，认证用户身份. 实验结果表明，该算法有效缩短了身份认证与批量消息验证所需时间，减少了数据传输所需字节数，时间开销仅为13 ms，计算开销仅为4 ms，通信开销仅为210字节，且能成功抵御15种身份认证攻击类型.

## 参 考 文 献

[1] DOGANI J, FARAHMAND M, DARYANAVARD H. A New Method to Detect Attacks on the Internet of Things (IoT) Using Adaptive Learning Based on Cellular Learning Automata [J]. Etri Journal, 2021, 44(11): 155-167.

[2] 闫攀，周莉，闫会峰. 混合云存储下物联网隐私数据保护模型研究 [J]. 计算机仿真，2023，40(2)：530-534.（YAN P，ZHOU L，YAN H F. Research on Privacy Data Protection Model of Internet of Things under Hybrid Cloud Storage [J]. Computer Simulation，2023，40(2)：530-534.）

[3] 李鹏程，张文胜，郭栋，等. 基于物联网通信协议的车辆信息系统开发 [J]. 计算机工程与设计，2022，43(3)：646-653.（LI P C，ZHANG W S，GUO D，et al. Development of Vehicle Information System Based on IoT Communication Protocol [J]. Computer Engineering and Design，2022，43(3)：646-653.）

[4] ZHENG Z H，DONG L，ZHANG Y F，et al. WeBrain 1.0：A Web-Based Big EEG Data Management and Cloud Computing Platform [J]. International Journal of Psychophysiology，2021，168：S198-S199.

[5] LIANG W，NING Z B，XIE S Y，et al. Secure Fusion Approach for the Internet of Things in Smart Autonomous Multi-robot Systems [J]. Information Sciences，2021，579：468-482.

[6] 王振宇，郭阳，李少青，等. 面向轻量级物联网设备的高效匿名身份认证协议设计 [J]. 通信学报，2022，43(7)：49-61.（WANG Z Y，GUO Y，LI S Q，et al. Design of Efficient Anonymous Identity Authentication Protocol for Lightweight IoT Devices [J]. Journal on Communications，2022，43(7)：49-61.）

[7] 鲁晔. 一种基于联盟链的物联网匿名交易方案 [J]. 计算机应用研究，2021，38(1)：23-27.（LU Y. IoT Anonymous Transaction Scheme Based on Alliance Chain [J]. Application Research of Computers，2021，38(1)：23-27.）

[8] 赵宗渠，郭小杰，殷明辉，等. 物联网环境下基于身份匿签密的认证方法研究 [J]. 重庆邮电大学学报(自然科学版)，2023，35(2)：343-351.（ZHAO Z Q，GUO X J，YIN M H，et al. Research on Authentication Method of Identity-Based Higncryption in IoT [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)，2023，35(2)：343-351.）

[9] LU Y G，WANG X W，LI F L，et al. RLbR：A Reinforcement Learning Based V2V Routing Framework for Offloading 5G Cellular IoT [J]. IET Communications，2022，16(4)：303-313.

[10] GUENDOGAN C，KIETZMANN P，SCHMIDT T C，et al. A Mobility-Compliant Publish-Subscribe System for an Information-Centric Internet of Things [J]. Computer Networks，2022，203：108656-1-108656-14.

[11] 严翰致，许小龙，代飞，等. 车联网环境下基于强化学习的边缘服务器部署策略 [J]. 计算机集成制造系统，2022，28(10)：3146-3155.（YAN H Z，XU X L，DAI F，et al. Edge Server Deployment Strategy with Reinforcement Learning in Internet of Vehicles [J]. Computer Integrated Manufacturing Systems，2022，28(10)：3146-3155.）

[12] 张艺与，赵海军，贺春林，等. 基于椭圆曲线的 RFID 电子标签加密算法研究 [J]. 云南大学学报(自然科学版)，2021，43(1)：60-67.（ZHANG Y Y，ZHAO H J，HE C L，et al. The Research of RFID Tag Encryption Algorithm Based on ECC [J]. Journal of Yunnan University (Natural Sciences Edition)，2021，43(1)：60-67.）

[13] RIAD K，CHENG J R. Adaptive XACML Access Policies for Heterogeneous Distributed IoT Environments [J]. Information Sciences，2021，548(1)：135-152.

[14] 王静怡，刘百祥，方宁，等. 基于区块链与属性密码体制的匿名数据共享访问控制 [J]. 计算机工程，2023，49(10)：41-52.（WANG J Y，LIU B X，FANG N，et al. Anonymous Data Sharing and Access Control Based on Blockchain and Attribute-Based Cryptography [J]. Computer Engineering，2023，49(10)：41-52.）

[15] 甘臣权，杨宏鹏，祝清意，等. 基于访问控制的可验证医疗区块链数据搜索机制 [J]. 重庆邮电大学学报(自然科学版)，2023，35(5)：873-887.（GAN C Q，YANG H P，ZHU Q Y，et al. A Verifiable Medical Blockchain Data Search Mechanism with Access Control [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)，2023，35(5)：873-887.）

[16] 蓝永胜，冯文健，黄力. 基于 ECC 和 AES 的区块链云存储框架设计 [J]. 计算机工程与设计，2022，43(6)：1534-1540.（LAN Y S，FENG W J，HUANG L. Design of Blockchain Cloud Storage Framework Based on ECC and AES [J]. Computer Engineering and Design，2022，43(6)：1534-1540.）

[17] 张超，彭长根，丁红发，等. 基于国密 SM9 的可搜索加密方案 [J]. 计算机工程，2022，48(7)：159-167.（ZHANG C，PENG C G，DING H F，et al. Searchable Encryption Scheme Based on China State Cryptography Standard SM9 [J]. Computer Engineering，2022，48(7)：159-167.）

[18] 李莉，杜慧娜，李涛. 基于群签名与属性加密的区块链可监管隐私保护方案 [J]. 计算机工程，2022，48(6)：132-138.（LI L，DU H N，LI T. Blockchain Supervisable Privacy Protection Scheme Based on Group Signature

and Attribute Encryption [J]. Computer Engineering, 2022, 48(6): 132-138.)

[19] 刘云, 宋凯, 陈路遥, 等. 最小损失算法在区块链物联网中的优化研究 [J]. 四川大学学报(自然科学版), 2022, 59(2): 84-90. (LIU Y, SONG K, CHEN L Y, et al. Optimization of Minimum Loss Algorithm in Blockchain Internet of Things [J]. Journal of Sichuan University (Natural Science Edition), 2022, 59(2): 84-90.)

[20] 蒋沥泉, 秦志光. 基于属性隐藏的高效去中心化的移动群智数据共享方案 [J]. 电子科技大学学报, 2023, 52(6): 915-924. (JIANG L Q, QIN Z G. Attribute-Hiding Based Efficient and Decentralized Scheme for Mobile Crowdsensing Data Sharing [J]. Journal of University of Electronic Science and Technology of China, 2023, 52(6): 915-924.)

[21] 蒋成满, 华保健, 樊淇梁, 等. Python 虚拟机本地代码的安全性实证研究 [J]. 计算机科学, 2022, 49(增刊 1): 474-479. (JIANG C M, HUA B J, FAN Q L, et al. Empirical Security Study of Native Code in Python Virtual Machines [J]. Computer Science, 2022, 49(Suppl 1): 474-479.)

[22] 丁奕文, 鲁若愚, 周冬梅. LoRa 在合法性演进中的时间同步: 多网关场景下的移动感知 [J]. 电子科技大学学报, 2023, 52(2): 224-231. (DING Y W, LU R Y, ZHOU D M. Time Synchronization of Emerging Technology LoRa in the Evolution of Legitimacy: Mobility Awareness in Multi-gateway Scenarios [J]. Journal of University of Electronic Science and Technology of China, 2023, 52(2): 224-231.)

[23] 查煜坤, 智慧, 房小彤. 基于区块链的物联网智能终端协作计算方案 [J]. 北京邮电大学学报, 2021, 44(2): 89-94. (ZHA Y K, ZHI H, FANG X T. Blockchain-Based Cooperative Computing Scheme for IoT Intelligent Terminals [J]. Journal of Beijing University of Posts and Telecommunications, 2021, 44(2): 89-94.)

[24] 李望. 采用区块链技术的卫星编队组网安全认证设计 [J]. 电讯技术, 2022, 62(7): 859-864. (LI W. Design of Security Certification of Satellite Formation Using Blockchain Technology [J]. Telecommunication Engineering, 2022, 62(7): 859-864.)

[25] 张利华, 刘季, 曹宇, 等. 双共识混合链跨异构域身份认证方案 [J]. 应用科学学报, 2022, 40(4): 666-680. (ZHANG L H, LIU J, CAO Y, et al. Dual Consensus Hybrid Blockchain Cross Heterogeneous Domain Identity Authentication Scheme [J]. Journal of Applied Sciences, 2022, 40(4): 666-680.)

[26] 苏瑞国, 阳建, 秦继伟, 等. 基于物联网区块链的轻量级共识算法研究 [J]. 计算机工程, 2023, 49(2): 175-180. (SU R G, YANG J, QIN J W, et al. Research on Lightweight Consensus Algorithm Based on IoT Blockchain [J]. Computer Engineering, 2023, 49(2): 175-180.)

[27] 何建江, 陈玉玲. 基于 DLIN 加密的可监管联盟链隐私保护方案 [J]. 计算机工程, 2023, 49(6): 170-179. (HE J J, CHEN Y L. DLIN Encryption-Based Auditable Privacy-Preserving Scheme for Consortium Blockchain [J]. Computer Engineering, 2023, 49(6): 170-179.)

(责任编辑: 韩 啸)