

基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法

顾天晟¹, 曾福康¹, 邵思思², 聂一君¹, 纪宗凯¹, 郑雨璐¹,
石雨辰¹, 刘尚东^{1,3,4}, 季一木^{1,3,4}

(1. 南京邮电大学计算机学院、软件学院、网络空间安全学院, 江苏 南京 210023;

2. 南京邮电大学物联网学院, 江苏 南京 210023; 3. 南京邮电大学高性能计算与大数据处理研究所, 江苏 南京 210023;

4. 国家高性能计算中心南京分中心, 江苏 南京 210023)

摘要: 智能物联网具有高灵活性、自适应性、持续演化等特性, 为用户带来更加极致的体验的同时也带来了新的挑战, 智能物联网难以杜绝的未知漏洞和后门等不确定威胁导致的物联网边域智能终端内生安全问题和安全传输问题正备受关注。为此, 提出了一种基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法。首先, 基于拟态防御理论构建了智能物联网终端安全防护架构, 以确保边域智能终端在自身存在安全基因缺陷时仍能保障系统的可靠性和鲁棒性。然后, 在该架构中设计了一种基于 Paillier 加密的安全盲签名 (SBSPE, secure blind signing with paillier encryption) 算法, 以确保边域智能终端在数据处理全流程中的数据与隐私安全。SBSPE 算法在 Paillier 半同态加密算法的基础上引入盲签名技术, 在对数据加密的同时基于盲因子技术进行盲签名, 使攻击者即使获得 Paillier 加密算法的解密密钥, 也无法解密密文信息, 有效支撑了智能物联网设备的数据高效、可靠传输。最后, 以拟态智能物联网系统为应用场景, 从性能和安全两方面对基于拟态防御的智能物联网终端半同态加密传输方法进行理论分析和实验验证, 证明所提方法的有效性和安全性。

关键词: 智能物联网; 边域智能终端; 拟态防御; DHR 架构; Paillier 加密算法

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024088

Security protection method based on mimic defense and Paillier encryption for smart IoT terminals

GU Tiansheng¹, ZENG Fukang¹, SHAO Sisi², NIE Yijun¹, JI Zongkai¹, ZHENG Yulu¹,
SHI Yuchen¹, LIU Shangdong^{1,3,4}, JI Yimu^{1,3,4}

1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

收稿日期: 2024-03-29; 修回日期: 2024-09-10

基金项目: 国家自然科学基金 (62176264); 国家重点研发计划项目 (2023YFB2904000, 2023YFB2904004); 江苏省重点发展规划项目 (BE20230042); 江苏省自然科学及高校自然科学重大项目 (20KJA520001); 中国电信江苏分公司 2023 年科技项目 (JSSGS2301022EGN00); 未来网络科学研究基金项目 (FNSRFP-2021-YB-15)

Foundation Items: The National Natural Science Foundation of China (62176264), The National Key R&D Program of China (2023YFB2904000, 2023YFB2904004), Jiangsu Key Development Planning Project (BE20230042), Natural Science Foundation of Jiangsu Province (Higher Education Institutions) (20KJA520001), 2023 Technology Project of China Telecom Co., Ltd. Jiangsu Branch (JSSGS2301022EGN00), Future Network Scientific Research Foundation Project (FNSRFP-2021-YB-15)

引用格式: 顾天晟, 曾福康, 邵思思, 等. 基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法[J]. 网络与信息安全学报, 2024, 10(6): 164-176.

Citation Format: GU T S, ZENG F K, SHAO S S, et al. Security protection method based on mimic defense and Paillier encryption for smart IoT terminals[J]. Chinese Journal of Network and Information Security, 2024, 10(6): 164-176.

2. School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

3. Institute of High Performance Computing and Big Data Processing, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

4. National High Performance Computing Center Nanjing Branch, Nanjing 210023, China

Abstract: Smart internet of things (IoT), with its high flexibility, adaptability, and continuous evolution, brings both new challenges and enhanced user experiences. In particular, the endogenous security and secure transmission issues faced by IoT edge-area smart terminals, due to uncertain threats like unknown vulnerabilities and backdoors, are of considerable concern in the realm of smart IoT. To address these challenges, a security protection method based on mimic defense and Paillier encryption for smart IoT terminals was proposed. First, a security architecture was constructed based on the mimic defense theory to ensure the reliability and robustness of the system even when the edge domain smart terminal had its own security genetic defects. Then, a secure blind signature with Paillier encryption (SBSPE) algorithm was designed in this architecture to safeguard the data and privacy of the edge-area smart terminals throughout the data processing lifecycle of edge-area smart terminals. Blind signature technology was integrated into SBSPE algorithm on the basis of Paillier semi-homomorphic encryption algorithm. During data encryption, it employed blind factor technology to execute a blind signature, rendering ciphertext information indecipherable even if an attacker obtained access to the decryption key of the Paillier encryption algorithm. It also effectively supported the efficient and reliable transmission of data of the intelligent IoT devices. Finally, taking the mimic smart IoT system as an application scenario, the proposed method was theoretically analyzed and experimentally validated for its improved performance and security.

Keywords: smart IoT, edge-area smart terminals, mimic defense, DHR architecture, Paillier encryption algorithm

0 引言

物联网^[1]作为新一代信息技术的重要浪潮,实现了“万物互联”,是人类科技史上的又一次重大革命,给人类生产、生活带来了巨大的便利。随着人工智能、大数据及边缘计算等技术的发展,物联网正进化为“万物智联”的智能物联网^[2]。许多特殊的应用场景也与智能物联网深度融合,如智能医疗^[3]、智慧家居^[4]、智能电网^[5]、智能交通^[6]、智慧城市^[7]等应用逐渐得以实现。这些应用场景中有大量的终端设备需要接入互联网并进行信息交互,因此用户在享受智能物联网带来便利性的同时也会遭受诸多的网络安全问题。

智能物联网大致分为智能终端层、边缘智能层和云计算层。智能终端层使用大量的传感器和处理器对智慧环境进行持续的信息收集。边缘智能层分布式部署了边域智能终端,用来执行数据存储、模型训练和推理任务,以缓解云端服务器的数据存储和计算压力。云计算层支持丰富多样的物联网应用,并对各分布式边域智能终端的数据进行汇总、处理和存储。在上述过程中,会生成大量的业务数据,这些数据由大量传感器与处

理器收集并上传到边域智能终端中。但是边域智能终端的安全防护体系^[8]不够完善,终端设备很容易遭受中间人攻击等安全威胁,导致数据的隐私性和机密性遭到破坏。同时,在提供智能物联网服务时产生的大量数据传输任务,也使得边域智能终端需要扮演安全网关的角色,滤掉恶意的连接和数据传输请求,进行可靠、隐蔽的安全传输^[9]。因此,智能物联网的终端内生安全脆弱性防护和安全隐蔽传输是亟须解决的问题。然而,目前业界对智能物联网环境下边域智能终端内生安全的研究尚处于探索阶段,相关成果较少。大多数研究集中在单一域内身份认证问题上,而对于不同边域智能终端的内生安全问题以及终端安全隐蔽传输的研究关注较少。

针对智能物联网环境下的智能边域终端内生安全问题和加密安全传输问题,本文提出基于拟态防御和Paillier半同态加密的智能物联网终端安全防护方法。该方法可以实现智能物联网边缘终端数据的加密安全传输,有效规避智能边缘终端自身漏洞带来的未知威胁。

本文的主要贡献如下。

1) 构建了智能物联网主动防御架构。针对智

能物联网中智能边域终端的内生安全脆弱性问题, 本文基于拟态防御动态、多样、冗余的特性, 实现了对智能物联网设备的可靠性裁定, 提高了智能物联网架构的安全性与鲁棒性, 为智能物联网环境下的隐私保护提供架构支撑。

2) 提出了基于 Paillier 加密的安全盲签名 (secure blind signing with Paillier encryption, SBSPE) 算法。针对智能物联网中的数据加密传输问题, 本文在 Paillier 半同态加密算法的基础上引入盲签名技术。SBSPE 算法在对数据加密的同时基于盲因子技术进行盲签名, 使攻击者即使获得 Paillier 加密算法的解密密钥也无法解密密文信息, 实现了智能物联网场景下隐私数据的加密处理, 支撑智能物联网设备数据高效、可靠传输。

3) 将所提方法应用到智能物联网场景中, 从性能和安全两方面对基于拟态防御的智能物联网终端半同态加密传输方法进行理论分析和实验验证, 证明了所提方法的有效性和安全性。

1 相关工作

为了最大限度地减少智能物联网基础平台可能带来的安全和隐私问题, 智能物联网必须在确保能够以简单、安全的方式执行各种用户控制操作的同时充分考虑安全性和隐私性。作为智能物联网内生安全脆弱性防护的基础, 边域智能终端的安全防护亟须加强。有效的终端安全防护机制可以防止单个边域智能终端故障导致大面积网络瘫痪事件的发生, 保证边域智能物联网安全可靠运行。另外, 作为用户和云端服务器的桥梁, 边域智能终端数据的安全隐蔽传输也非常关键。因为边域智能终端与用户侧设备、智能环境联系密切, 边域智能终端往往采集了大量有价值的信息, 这些信息如果暴露给不法分子, 可能会给用户和服务提供商带来巨大的危害。随着物联网设备自动化和智能化程度的不断提高, 物联网设备数据的加密、安全传输等问题成为业界关注的焦点。

Niu 等^[10]设计了一种高效的在边缘计算下支持关键字搜索的属性加密 (attribute-based encryption, ABE) 方案。该方案考虑到用户的计算效率, 采用外包解密方式对传统的 ABE 进行了

改进, 使得不同计算能力的用户可以独立解密, 可以在共享私有数据 (如医疗记录) 的同时保护用户信息的隐私性, 并支持在云环境下高效地实现属性撤销和密文更新。但该方案受属性数量的限制, 只适合轻量级应用场景。Wu 等^[11]提出了一种差分聚合加密 (differential aggregation encryption, DAE) 模型, 可以对边缘计算中的数据差分聚合后加密传输, 保证终端数据的安全性。Yang 等^[12]设计了一种边缘计算模式下全同态加密智能合约, 对交易数据库信息和边缘节点身份进行同态加密, 在保证交易数据可计算性的同时实现了交易信息和边缘节点身份的隐私保护。Chen 等^[13]根据边缘计算网络异构的特点, 按照移动智能私有数据结构对网络进行分层, 并采用同态加密算法对数据进行加密, 使隐私数据能够以密文的形式在边缘网络和移动终端上传输和存储。Liang 等^[14]提出了一种基于椭圆曲线密码学 (elliptic curve cryptography, ECC) 和双线性配对的隐私数据保护和身份认证方案, 通过 ECC 对终端设备的身份和生成的私有信息进行加密, 实现了匿名访问和数据传输。

也有一些学者将区块链技术防篡改和可追溯的特点应用到物联网中, 提供一个具有强大算力和安全性的网络环境, 以解决传统密码系统的密钥托管问题。Yan 等^[15]设计了一个基于区块链的分布式隐私保护架构, 并利用 Paillier 和 RSA 密码系统对数据进行同态加密, 实现了数据加密和隐私保护的目标。Xu 等^[16]设计了一种适用于边缘计算的基于区块链的无证书签名加密机制, 在边缘计算环境中利用区块链的不易篡改特性保证了信息传输的机密性和不可伪造性。Al Shahrani 等^[17]利用椭圆曲线的证书策略避免了关键的托管问题, 并采用轻量级符号加密方法, 及时阻断被攻破终端与云的联系, 保证云端接收边缘认证信息的安全性。Liao 等^[18]将区块链技术和 GSW 同态加密技术相结合, 实现了私有数据的完整性和保密性, 但该方案无法抵抗拜占庭攻击。Wang 等^[19]提出了一种结合同态加密和区块链技术的隐私保护方案。在该方案中, 基于同态加密技术设计了新的块数据结构, 敏感数据在写入区块链之前进行加密处理, 使得数据在存储和传输

的过程中都保持着密文状态，有效地解决了区块链网络中全部数据公开的隐私问题。Chen等^[20]提出了一种基于Paillier加解密的量化分布式优化算法。该算法基于有限级均匀量化器设计了一种动态编解码策略来优化通信和加密过程，并利用Paillier密码系统的同态特性来保证保密通信。

为更加直观地展现相关学者的研究进展，本文从数据安全、复杂度、通信延迟等角度总结了现有相关工作的优势和劣势。不同方案的对比如表1所示，由表可知，当前的研究虽然在一定程度上能够保证数据加密和安全传输，但是这都是建立在边域智能终端自身可信的基础上。由于软硬件在设计时可能会存在缺陷或脆弱性，网络空间中可被攻击者利用的未知漏洞和后门等威胁难以根绝，因此边域智能终端本身的安全难以保障。当系统不完全可信，如软硬件不可信或系统处于不可信网络环境中时，面对没有先验知识的威胁几乎无能为力，那在设备或系统上实施

的一切安全措施都只能起到“亡羊补牢”的作用，即使系统有数据加密、安全传输功能，攻击者仍可以采用其他方式进行攻击，如旁路攻击。

郭江兴^[21]提出的动态异构冗余（DHR, dynamic heterogeneous redundancy）架构颠覆了传统网络安全防护“被动”防御模式，提升了网络的内生安全性。该架构采用多个功能等价但实现方式各异的执行体并行工作，通过表决器比对执行体输出结果，得到系统输出^[22]。与此同时，引入了调度策略^[23]、负反馈机制和多模裁决机制^[24]，动态调度和重构执行体，阻断攻击者的信息链，使攻击者难以观察和预测系统环境，从而增强系统服务的可靠性和健壮性。随着网络攻击的不断升级，网络安全问题日益严峻，DHR架构已成为解决这些问题的重要手段之一。

因此，本文提出一种基于拟态防御和Paillier半同态加密的智能物联网终端安全防护方法，旨在提升边域智能终端的内生安全性，保护消息发

表1 不同方案的对比
Table 1 Comparison of different schemes

文献	优势	劣势
[10]	只需要对服务器外包解密、共享私有数据、支持密文更新、复杂度低	有敏感信息暴露给云服务器的风险
[11]	利用聚合加密算法和具有可信权限的加密算法对端和边缘节点进行差分聚合	难以应对内部强对抗场景
[12]	用SEAL库对Fabric网络中的数据库信息和边缘节点身份信息进行同态加密	需更新智能合约中的状态数据库，并对状态数据同态加密，复杂度较高；需保证边缘节点的“无毒无菌”
[13]	设计安全集成模型，分析终端网络的异构性特点、用户面临的边界攻击，进行攻防博弈，并采用秘密共享和同态加密算法将终端数据以密文形式传输到安全集成模型	在进行攻防博弈时需数据迁移，易导致数据泄露和上下行严重拥塞
[14]	只需通过ECC算法对私有信息进行加密，复杂度较低	通信时需使用时间戳和随机数维持通信的新鲜度；在大型网络环境下面临数据聚合和安全传输问题
[15]	设计了基于区块链的分布式隐私保护架构，并引入同态加密技术	需对区块链进行维护和更新，对所有数据进行同态加密，复杂度较高；区块链网络维护和数据管理开销大
[16]	将区块链引入签名机制中，保证签名的不可抵赖性	需要注意非法节点上链和访问其他边缘节点；需对区块链进行维护和更新，且需对所有数据进行同态加密，复杂度较高
[17]	引入信任因子，用于终端的数据认证和调度；使用轻量级签名方法保证认证信息在受到威胁时能迅速传递到云端	信任因子收集时存在数据稀疏性和冷启动问题；实时收集和评估信任因子以及训练联邦学习模型会增加通信延迟
[18]	在区块链中构造Merkle哈希树以保证数据的不易篡改性	多密钥全同态加密需要处理不同密钥加密的数据，需要同时维护哈希树与区块链，复杂度较高；无法抵抗拜占庭攻击
[19]	设计了基于同态加密的新的块数据结构，使加密后的隐私数据可写入区块链	写入区块链和共识机制的计算均会增加通信延迟；无法抵御内部漏洞及侧信道攻击
[20]	设计了一种动态编解码策略来优化同态加密过程	存在数据量化误差

送者的数据隐私。该方法在拟态防御思想的基础上结合了盲签名和 Paillier 半同态加密的优势,构建了智能物联网主动防御架构。该架构基于动态、多样、冗余的特性在边缘智能层设置多个具有相同功能的非相似冗余智能终端,使得系统在部分终端存在安全威胁的情况下仍能保障安全性和可靠性;在数据传输时,通过盲化和加密处理保护消息发送者的隐私,确保签名的有效性和可验证性;能够在隐藏消息的实际内容的前提下,进行一定程度的计算,防止攻击者根据不同的输入得到相同的加密结果,从而增加了攻击者攻击系统的难度,有助于提高数据的随机性和不可预测性,增强系统的鲁棒性。

2 方案设计

2.1 架构概述

针对智能物联网边域智能终端的内生安全防护和数据传输需求,本文提出了基于拟态防御智能物联网终端安全防护架构,如图 1 所示。该架构结合拟态防御思想在智能物联网的边缘智能层进行内生安全基因改造,设计了输入输出模块、

异构终端池,供策略调度模块调度。

执行模块接收输入代理分发的盲化数据并进行验证。若证明签名有效,则接受数据以进行密文半同态加密计算,并将密文结果发送给裁决模块。若签名是无效的,则拒绝数据,记录无效签名的事件和相关信息,并且发出警报。

策略调度模块包括 Paillier 密钥生成模块、策略调度和负反馈控制器。初始时,策略调度模块从智能终端等待池中随机选择 n 个异构终端执行体,然后将其调度至执行模块组成服务体 S ,负反馈控制器对异常终端执行体进行清洗、替换,策略调度模块根据负反馈控制器动态调整调度策略。

裁决模块根据执行模块输出的密文结果进行逆同态运算后进行裁决,将裁决结果发送至输入输出模块,同时将输出结果发送给策略调度模块的负反馈控制器,由负反馈控制器对服务体进行置信度的更新。

策略调度模块是基于拟态防御智能物联网终端安全防护架构的重要组成部分。该模块需要考虑边缘智能层在引入 DHR 架构后的效益和开销

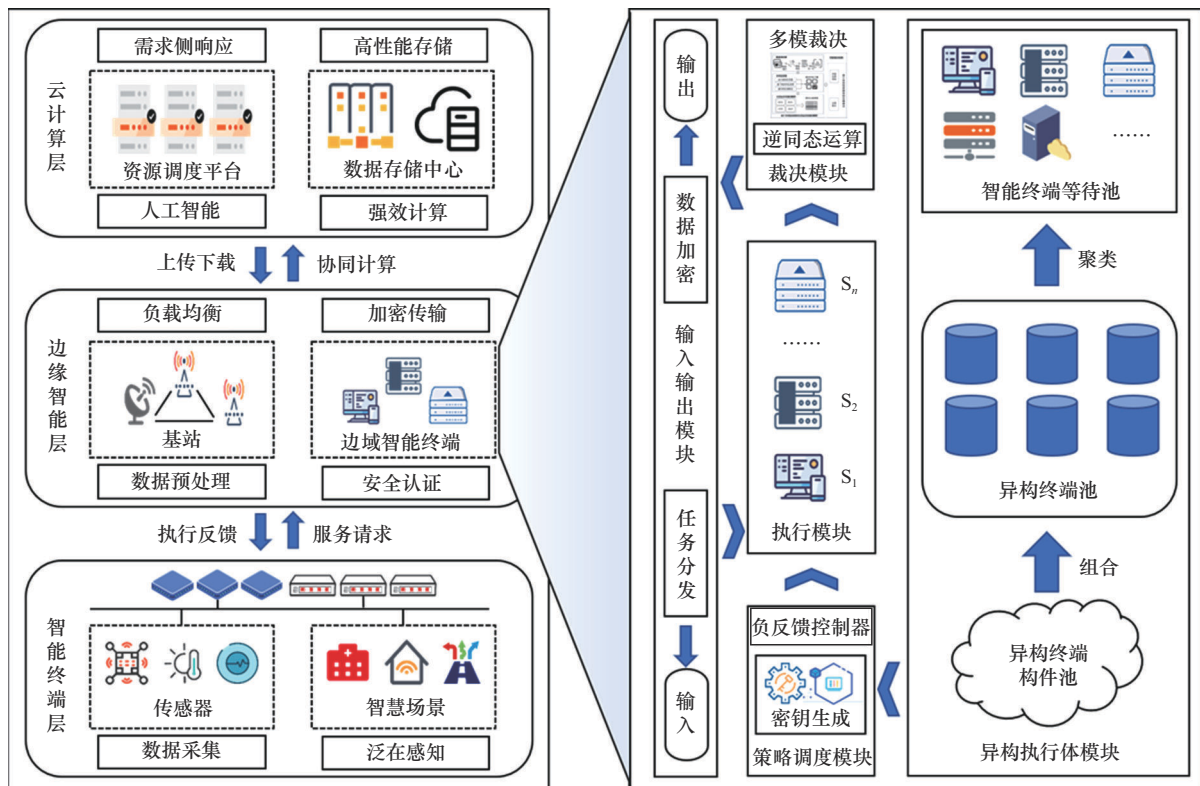


图 1 基于拟态防御智能物联网终端安全防护架构

Figure 1 Security protection architecture of intelligent IoT terminal based on mimicry defense

问题, 并通过计算服务质量和切换开销确定调度策略。调度策略大致分为两种: 例行切换和紧急切换。每隔一定时间 Δt , 策略调度模块根据调度策略中各终端执行体的相异度 $D(t)$ 、历史平均置信度 $H(t)$ 和运行开销 C_{run} 计算服务质量 Q , 并结合调度策略的切换开销 C_{switch} 确定调度策略。当调度策略的服务质量与正在运行的方案的调度策略差值超过设定的阈值 γ 且切换开销小于设定的阈值 δ 时, 则可以对当前运行策略进行例行切换。当终端执行体 i 遭受攻击或发生未知错误时, 该终端执行体的裁决结果 $y_i(t)$ 与全局裁决结果 $Y(t)$ 的输出不一致, 该终端执行体的置信度 $h_i(t)$ 将会下降, 如果低于置信度阈值 ζ , 负反馈控制器就会定位到终端执行体进行清洗、替换, 并且策略调度模块会根据上述规则紧急切换到第一个满足服务质量和切换开销的调度策略。

另外, 在上述架构中, Paillier 半同态加密技术被广泛应用。首先, 在输入输出模块中, 同态加密被用于对输入数据进行加密。使用 Paillier 加密密钥对输入数据进行加密, 可以确保数据在传输和处理过程中的机密性得到充分保护。加密后的数据在不泄露敏感信息的前提下进行传输, 可以有效防止数据被未经授权方访问和窃取。其次, 在异构执行体模块中, 异构终端池中的终端执行体利用同态加密技术进行半同态加密计算。半同态加密允许在密文状态下进行加法和乘法运算, 而无需解密数据。这种能力使得终端执行体能够对加密数据进行计算操作, 而无需暴露数据的明文内容。通过使用半同态加密, 终端执行体能够在保护数据隐私的同时, 实现对加密数据的高效计算, 确保计算结果的准确性。最后, 在裁决模块中, 执行模块输出的多个计算结果经过逆同态运算进行裁决。逆同态运算允许将加密的计算结果转换成明文的形式, 从而获得最终的计算结果。通过使用半同态加密和逆同态运算, 裁决模块能够在保护数据隐私的同时, 进行正确的计算结果裁决, 保证了系统的可靠性和安全性。

2.2 SBSPE 数据加密算法介绍

同态加密技术是一种重要的加密技术。它具有特殊的数学性质, 可在加密状态下进行计算, 而无需解密。常见的同态加密技术有半同态加密

技术和完全同态加密技术。半同态加密技术允许对特定类型的计算进行同态操作, 如加法或乘法运算。而完全同态加密技术允许对任意计算进行同态操作, 包括多次运算和不同类型的运算。

传统的 Paillier 半同态加密算法的密钥体制分为密钥生成、加密过程和解密过程。传统的 DHR 架构在读取数据时存在隐私泄露问题, 且在计算和通信时存在效率低下问题。如果攻击者通过入侵获取了 Paillier 加密算法的解密密钥, 就有可能解密用户的密文信息, 获取每个用户的私密数据, 从而导致数据泄露。考虑到解密密钥泄露会引发数据泄露问题, 本文引入了盲签名技术, 对输入数据使用 Paillier 加密的同时基于盲因子技术进行盲签名, 这样攻击者即使获得 Paillier 加密算法的解密密钥, 也无法解密密文信息, 也就不能获取每个用户的信息。本文提出的 SBSPE 算法如图2所示。

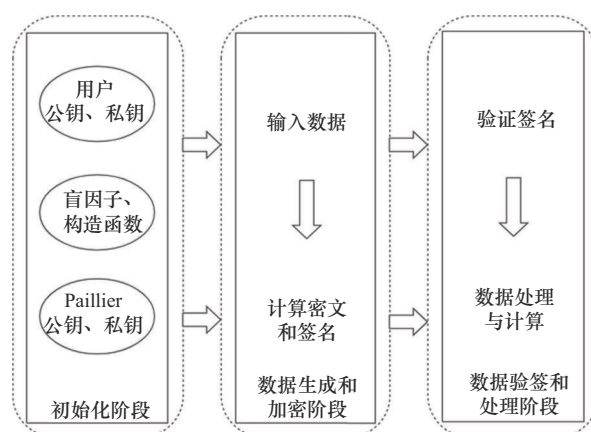


图2 SBSPE 算法

Figure 2 SBSPE algorithm

SBSPE 算法分为3个阶段, 具体如下。

(1) 初始化阶段

当前网络中存在用户 $U = \{U_1, U_2, \dots, U_n\}$, 用户 i 随机选择一个 $X_i \in Z^*$, 同时计算对应的 $Y_i = g^{X_i}$ 。其中, X_i 表示用户 i 的私钥, Y_i 表示用户 i 的公钥。假设存在可信机构随机选择 $n+1$ 个盲因子 $\{\psi_0, \psi_1, \dots, \psi_n\}$, 使得 $\psi_0 + \psi_1 + \dots + \psi_n \equiv 0$ 。将盲因子 ψ_0 发送给执行模块, ψ_i 发送给每个用户。每个用户将 ψ_i 与原始数据进行组合 (此过程称为数据盲化), 同时使用自己的私钥进行盲签名。此外, 还需要定义3个安全的 Hash 函数, 分

别为 $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: \{0,1\}^* \rightarrow Z_N^*$, $H_3: \{0,1\}^* \rightarrow Z^*$ 。生成 Paillier 密码系统的公钥 ($N = pq, g_{Ag}$) 和对应的私钥 (λ, μ), 其中 p 和 q 是 2 个大的质数, $g_{Ag} \in Z_{n^2}^*$, $\lambda = \text{lcm}(p-1, q-1)$, $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$ 。假设共有 l 个输入数据需要进行计算处理, 将其定义为 $a = (a_1, a_2, \dots, a_l)$, 则可将 Paillier 密码公钥 ($N = pq, g_{Ag}$) 定义为 $\{N, (g_1, g_2, \dots, g_l)\}$, $g_i = g_{Ag}^{a_i}$, $i = 1, 2, \dots, l$ 。

(2) 数据生成和加密阶段

输入数据为 $T = \{T_{i1}, T_{i2}, \dots, T_{il}\}$, 表示与盲因子 ψ_i 组合之后的盲化数据。输入代理首先利用 Paillier 加密算法计算密文 $CT_i = g_1^{T_{i1}} g_2^{T_{i2}} \dots g_l^{T_{il}} \bmod N^2$; 然后计算出 $h_i = H_3(CT_i)$, $W = H_1(t)$, 并根据 h_i 和 W 计算出消息签名 $\sigma_i = W^{x_{h_i}}$; 最后, 将计算出的输入数据的密文和签名 $\{CT_i, \sigma_i\}$ 发送给执行模块。

(3) 数据验签和处理阶段

执行模块接收到 n 个用户传过来的某个时刻 t 产生的输入数据, 即输入数据的密文和签名 $\{CT_i, \sigma_i\}$, 执行模块同时计算出 $h_i = H_3(CT_i)$, $W = H_1(t)$ 。计算 $e(g, \delta_i)$ 和 $e(W, Y_i^{h_i})$, 对所有数据签名进行验证。如果证明签名是有效的, 那么执行模块接收数据, 进行密文同态加密计算, 并且在同态运算中加入 ψ_0 以消除盲因子的影响, 将密文结果 D_i 发送给裁决模块。如果签名是无效的, 那么拒绝数据, 记录无效签名的事件和相关信息, 并且发出警报。

综上所述, SBSPE 算法的处理流程如下所示。

算法 1 SBSPE 算法

```

1) (publicKey, privateKey) ← PaillierKey
   Generation() // 密钥生成
2) blindedMessage ← Blind(message, blind
   Factor, publicKey) // 盲化过程
3) signature ← Sign(blindedMessage, private
   Key) // 签名过程
4) isValid ← Verify(signature, blindedMessage,
   publicKey) // 验证过程
5) // 盲化函数
6) function Blind(message, blindFactor, public

```

Key):

```

7) blindedPlaintext = message + blindFactor
8) blindedCiphertext ← PaillierEncryption
   (blindedPlaintext, publicKey)
9) return blindedCiphertext
10) // 签名函数
11) function Sign(blindedMessage, private
   Key):
12) signature ← PaillierDecryption(blinded
   Message, privateKey)
13) return signature
14) // 验证函数
15) function Verify(signature, blindedMessage,
   publicKey):
16) decryptedSignature ← PaillierEncryption
   (signature, publicKey)
17) isValid ← (decryptedSignature == blinded
   Message)
18) return isValid

```

SBSPE 算法包含密钥生成、盲化过程、签名过程和验证过程。在密钥生成阶段, 通过调用 Paillier 加密算法的密钥生成函数, 生成公钥和私钥。盲化过程使用盲因子和公钥对原始消息进行盲化, 以隐藏消息内容。签名过程使用私钥对盲化后的消息进行解密, 生成签名。验证过程使用公钥对签名进行加密, 并将加密结果与盲化后的消息进行比较, 以验证签名的有效性。该算法的时间复杂度主要取决于 Paillier 加密算法的复杂度, 通常为 $O(k^2)$ 或 $O(k^3)$, 其中 k 为加密算法中使用的密钥长度。空间复杂度也主要由加密算法决定, 通常为 $O(k)$ 。

2.3 安全性分析

(1) 攻击安全性

下面分别对外部攻击和内部攻击进行分析。外部攻击者可以在输入输出模块将加密签名的数据上传到执行模块时进行窃听, 但是无法获取到其中的加密数据信息。也就是说, 虽然外部攻击者可以在数据上传阶段获取到加密数据 $T_i = g_1^{T_{i1}} g_2^{T_{i2}} \dots g_l^{T_{il}} \bmod N^2$, 但是并不知道 Paillier 的解密密钥, 从而无法获取其中的原始数据信息 (即输入数据信息) $T =$

$\{T_{i1}, T_{i2}, \dots, T_{il}\}$ 。因此, 即使受到外部攻击, 数据信息也是安全的。

执行模块中出现异常的终端执行体可以被视为内部攻击者, 异常终端执行体获取了数据的加密信息 $CT_i = g_1^{T_{i1}} g_2^{T_{i2}} \dots g_l^{T_{il}} \bmod N^2$ 以及计算处理后的值 D_i , 但是仍然无法获取用户的原始数据信息 $T = \{T_{i1}, T_{i2}, \dots, T_{il}\}$ 。因此, 即使受到内部攻击, 数据信息也是安全的。

(2) 解密安全性

本文运用 Paillier 加密算法和盲签名技术进行整体加密, 用户在加密自己的数据信息时采用了盲因子技术, 攻击者即使获得 Paillier 加密算法的解密密钥, 也无法解密每个用户的密文信息, 也就不能获取每个用户的原始数据信息。

3 实验与结果分析

3.1 实验设置

仿真实验使用本地终端模拟终端设备, 配置为 Intel Core i7 3.5 GHz 处理器、内存 8 GB、操作系统为 64 位 Ubuntu 20.04。使用阿里云服务器来模拟云计算层服务器以及边缘智能层的边域智能终端, 平台参数为 ecs.e-c1m4.xlarge (4 vCPU 16 GiB, 经济型 e)、Ubuntu 20.04 64 位操作系统, 使用基于 Java 的配对密码学库 (JPBC)。

实验评价主要是架构安全性验证和性能分

析。架构安全性验证通过模拟智能物联网中边缘智能层的数据处理流程以验证所提架构各模块的功能与安全性; 性能分析从计算效率和通信效率两个方面进行评价。

计算效率评价从本文所提方法的加密方案和签名方案的效率角度进行, 选择基于身份的同态加密系统方案、基于量子密钥系统方案以及 EPPSA 系统方案进行对比。

通信效率主要是指用户发送各种输入数据, 将其加密签名之后传送到执行模块这一过程所用的时间。通信效率的评价指标由随机生成的数据利用不同的方案加以验证。

3.2 架构安全性验证

本实验设置用户数量为 3, 异构终端池大小 $m=50$, 边域终端冗余度为 3。架构安全性验证过程如下。

首先对边缘智能层进行初始化, 用户可以输入参与初始化的用户数量, 初始化结果如图 3 所示。在初始化过程中, 密钥生成模块会生成随机的盲因子列表, 并根据每个用户的输入数据和盲因子进行盲化操作, 接着生成每个用户的私钥和公钥, 对盲化数据进行数字签名。生成的盲因子、盲化数据和数字签名将显示在相应的列表中, 并在状态标签中显示初始化完成的提示信息。初始化后, 3 位用户 $U = \{U_1, U_2, U_3\}$ 的原始数据分别为 41、-66 和 88。密钥生成模块生成的



图3 边缘智能层初始化结果

Figure 3 Initialization result of edge intelligence layer

盲因子 $\psi = \{\psi_0, \psi_1, \psi_2, \psi_3\}$ 分别为 158、-91、-70 和 3，盲因子总和为 0。使用盲因子对每个用户的原始数据进行盲化处理，处理之后的盲化数据依次为 -50、-136 和 91，盲化数据作为输入数据发送给输入输出模块。

输入输出模块获取输入数据和对应的签名，输入代理使用 Paillier 加密密钥对输入数据进行同态加密，输入数据 -50、-136 和 91 对应的密文如图 4 所示。加密后的密文以及签名都会发送至执行模块进行验证签名和密文计算。

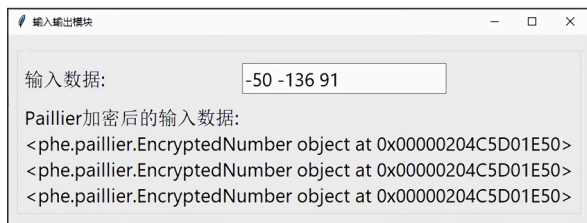


图4 输入输出结果

Figure 4 Input and output results

初始时，异构执行体模块的异构终端池中有 $m=50$ 个功能等价、结构不同的智能终端执行体处于待机状态。考虑到执行体间的差异性，设置其权重 w_1 、 w_2 和 w_3 分别为 1/3、1/3 和 1/3。使用 K -means 算法对终端执行体的特征进行聚类， K 值设置为 5，异构终端池根据聚类结果将终端执行体分为 5 组，随机从每组中调度一个终端执行体到等待池，供策略调度模块调度。本实验中进入等待池的终端执行体分别为 E24、E50、E36、E12 和 E14。

初始时，策略调度模块从智能终端等待池中随机选择 3 个终端执行体作为服务体 S ，并将服务体 S 调度至执行模块进行计算。每个终端执行体都具有异构度、置信度、运行开销和切换开销这几个属性。服务体集合 $S = \{E50, E24, E12\}$ ，初始置信度都为 0.5。

策略调度基于终端执行体的属性和预设的阈值选择进行例行切换或紧急切换。本文只列举例行切换的情况，例行切换如图 5 所示，图中调度方案按照成本增益降序排序，方案 1 的成本增益为 0.448，所以当发生例行切换时，则会将 E14、E41 和 E9 作为新服务体，调度至执行模块。假如存在服务体的置信度低于系统置信度阈值，就会触发紧急切换，选择合适的方案进行调度。

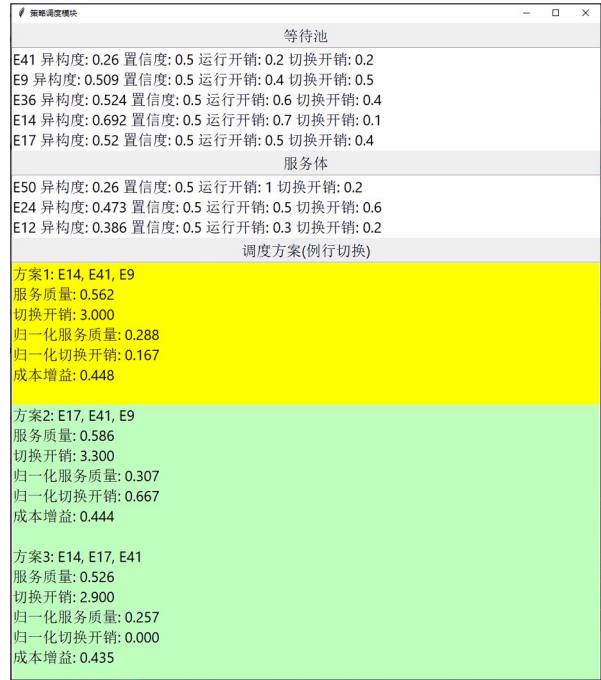


图5 例行切换

Figure 5 Routine switching

执行模块将对数据签名进行验证。如图 6 所示，服务体 S 为 E50、E24 和 E12，使用状态属性代表该服务体是否被攻击（0 代表正常，1 代表异常）。服务体 S 对所有数据签名进行验证。若证明签名有效，则执行模块接收数据，进行密文同态加密计算，并且在同态运算中加入 ψ_0 以消除盲因子的影响，将密文结果 D_i 发送给裁决模块。若签名无效，则拒绝数据，记录无效签名的事件和相关信息，并且发出警报。由图 3 可知，初始时加密数据明文依次为 -50、-136 和 91， ψ_0 的明文为 158。执行结果如图 6 所示，3 个服务体计算结果明文都为 63。执行模块将每个服务体计算的密文结果发送给裁决模块，由裁决模块进行裁决。

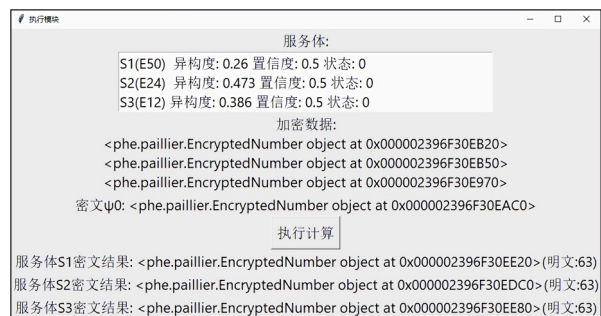


图6 执行结果

Figure 6 Execution results

接下来, 裁决模块将进行裁决。在服务体未受攻击时的情况, 裁决模块在接收到执行模块发送的密文结果后便进行裁决, 裁决策略采用大数裁决, 由于3个服务体的执行结果都为63, 则裁决成功, 裁决结果如图7所示, 为密文的63。此时所有计算正确的服务体的置信度上升。

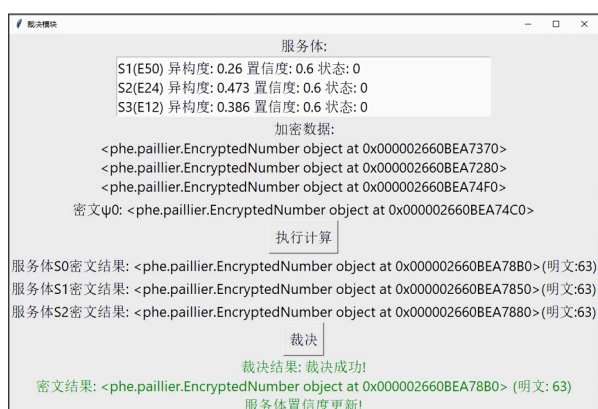


图7 裁决结果(服务体正常)

Figure 7 Verdict results (normal service body)

图8展示了服务体受到攻击时的情况, 可以看出, 服务体 S_3 此时的状态为1, 表示受到了攻击者的入侵, 执行结果受到了影响, 执行结果为64, 与全局裁决结果63不一致, 置信度下降。



图8 裁决结果(服务体异常)

Figure 8 Verdict results (Abnormal service body)

3.3 性能分析

实验选取了EPPSA (efficient client privacy-preserving statistical aggregation) 系统^[25]、基于身份的同态加密系统^[26]、基于量子密钥系统^[27]与本文方法进行对比。选取的3种方案均能保障隐私数据的机密性与安全性。传统的EPPSA系

统采用超增序列对多维数据进行结构化, 并以Paillier加密技术对结构化的数据进行加密, 从而能够抵抗安全威胁, 保护用户隐私。而文献^[25]中的EPPSA系统改进了Montgomery指数算法, 从而提高了边缘聚合器对多维数据的聚合效率, 同时具有更低的通信负荷。基于身份的同态加密方案在考虑到签名密钥暴露的现实威胁后, 采用完全子树技术构建一种分层可撤销的基于身份的全同态签名方案, 并在公共通道中定期更新密钥, 在有效抵抗签名密钥暴露的同时实现了可扩展性和上下文隐藏特性。基于量子密钥系统将经典密码学中的混淆和扩散概念引入量子加密, 将量子态作为密文、量子态创建过程作为密钥, 在保护信息完整性的同时提供了密钥的可重用性, 且对密码分析攻击具有很强的抵抗能力。

本文将从计算效率和通信效率两个方面对上述4个方案的性能进行对比评估。

(1) 计算效率

计算效率包含加密效率和签名效率两部分。

1) 加密效率。本实验将随机生成整数信息并分别用4种方案进行加密, 然后计算出各方案加密所用的时间。加密效率实验结果如图9所示, 当 $n < 30$ 时, 本文方案加密效率更高; 当 $n > 30$ 时, 基于量子密钥系统方案加密效率更高, 基于身份的同态加密系统方案次之。本文方案加密时需要多个执行体将盲因子和Paillier加密算法进行混合整体加密并裁决, 花费的时间较多, 因此更适合用户数量小于30的场景。基于量子密钥系统方案和基于身份的同态加密系统方案在加密过程中都需要创建并维持新的数据结构(完全子树和密码块链)。假设每个用户所产生的各种类型的计算数据大小相等, 当用户数量较少时, 创建并维持新的数据结构花费的时间较多, 但随着用户数量的增加, 这些数据结构将大幅提升数据加密的效率, 因此这两种方案更适合用户数量多的场景。

2) 签名效率。本实验也将随机生成整数信息并分别用4种方案进行签名, 然后计算出各方案签名所用的时间。签名效率实验结果如图10所示, 不管用户多少, 本文方案的签名效率均高于其他方案。这是因为本文方案在签名过程仅需使

用 Paillier 私钥对盲化后的消息进行解密即可生成签名, 复杂度低, 效率更高。

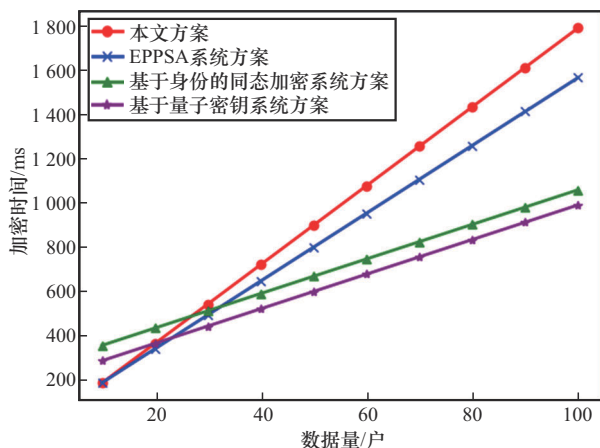


图9 加密效率实验结果

Figure 9 Experimental results of encryption efficiency

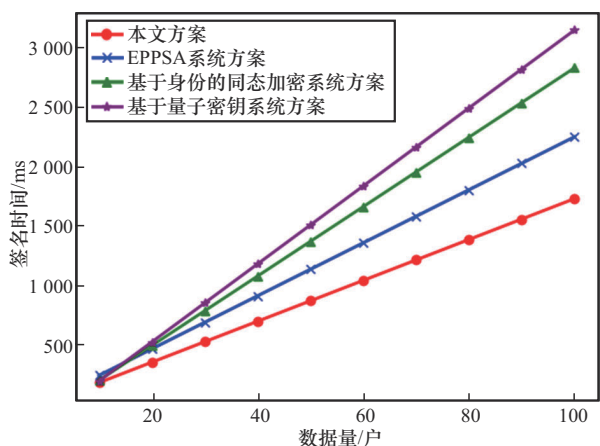


图10 签名效率实验结果

Figure 10 Experimental results of signature efficiency

(2) 通信效率

本文所述的通信效率指用户与输入输出模块之间所用的时间。实验使用加密签名后的数据上传到输入输出模块的时间进行对比。通信效率实验结果如图 11 所示, 本文方案的通信效率高与其他方案。这是因为本文方案只需要传输加密和签名后的数据, 没有额外操作或其余数据结构需要传输, 所以本文方案所需的通信时间最少, 通信效率相对较高。

在轻量级智能物联网环境下 (用户数为 40), 不同方案的时间指标数据对比如表 2 所示, 相比其他方案, 本文方案在签名时间、通信时间上表现更优, 而在加密时间上略逊色。

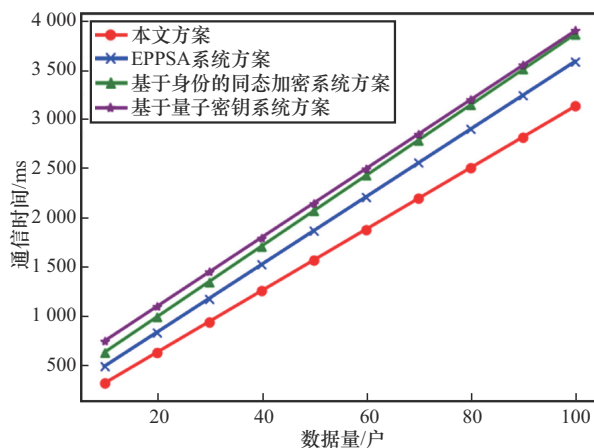


图11 通信效率实验结果

Figure 11 Experimental results of communication efficiency

表2 不同方案的时间指标数据对比

Table 2 Comparison of time index data of different schemes

方案	加密 时间/ms	签名 时间/ms	通信 时间/ms
基于身份的同态加密系统方案 ^[26]	698	1 101	1 812
基于量子密钥系统方案 ^[27]	670	1 490	2 124
EPPSA系统方案 ^[25]	794	977	1 799
本文方案	823	865	1 564

4 结束语

针对智能物联网环境下边域智能终端的内生安全问题以及传输安全问题, 本文提出了一种基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法。该方法通过在智能物联网架构中引入拟态防御理论, 从而确保智能物联网在面对自生的未知威胁或漏洞时仍然可以安全、可靠地提供服务; 利用具有盲签名功能的 Paillier 半同态加密算法保护边域智能终端数据的隐私安全。本文从计算效率和通信效率两个方面开展实验以评估所提方法的性能, 实验结果表明, 所提方法能够有效解决智能物联网中用户私密数据在上传、通信以及计算过程中存在的随机攻击、传输不安全、泄露用户隐私等问题, 并具有较好的计算效率和通信效率。

本文提出的基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法将动态、异构、冗余的特性和盲签名的思想引入智能物联网架构, 提高了智能物联网数据的安全性。然而, 这种方

法通过加冗余的方式实现整体架构的异构性和动态性, 在系统开销和部署成本方面存在一定的局限性。因此, 未来需进一步优化该方法的架构和加密算法, 以解决系统冗余和异常执行体再利用问题, 使其拥有更广阔的应用空间。

参考文献:

- [1] LAGHARI A A, WU K, LAGHARI R A, et al. A review and state of art of internet of things (IoT)[J]. Archives of Computational Methods in Engineering, 2021: 1-19.
- [2] 郭斌, 刘思聪, 刘琰等. 智能物联网: 概念、体系架构与关键技术[J]. 计算机学报, 2023, 46(11): 2259-2278.
GUO B, LIU S C, LIU Y, et al. AIoT: the concept, architecture and key techniques[J]. Chinese Journal of Computers, 2023, 46(11): 2259-2278.
- [3] QADRI Y A, NAUMAN A, ZIKRIA Y B, et al. The future of health-care internet of things: a survey of emerging technologies[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1121-1167.
- [4] DAVIS B D, MASON J C, ANWAR M. Vulnerability studies and security postures of IoT devices: a smart home case study[J]. IEEE Internet of Things Journal, 2020, 7(10): 10102-10110.
- [5] 顾伟, 沈剑, 任勇军. 基于智能电网的安全密钥共享算法[J]. 网络与信息安全学报, 2021, 7(4): 141-146.
GU W, SHEN J, REN Y J. Secure key-sharing algorithm based on smart grid[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 141-146.
- [6] 何智旺, 王化群. 面向车联网的匿名组密钥分发方案[J]. 网络与信息安全学报, 2023, 9(5): 127-137.
HE Z W, WANG H Q. Anonymous group key distribution scheme for the internet of vehicles[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 127-137.
- [7] ABADIA J J P, WALTHER C, OSMAN A, et al. A systematic survey of Internet of things frameworks for smart city applications[J]. Sustainable Cities and Society, 2022, 83: 103949.
- [8] HOU R, REN G, ZHOU C, et al. Analysis and research on network security and privacy security in ubiquitous electricity internet of things[J]. Computer Communications, 2020, 158: 64-72.
- [9] LETAFATI M, KUHESTANI A, WONG K K, et al. A lightweight secure and resilient transmission scheme for the internet of things in the presence of a hostile jammer[J]. IEEE Internet of Things Journal, 2020, 8(6): 4373-4388.
- [10] NIU S F, HU Y, ZHOU S W, et al. Attribute-based searchable encryption in edge computing for lightweight devices[J]. IEEE Systems Journal, 2023, 17(3): 3503-3514.
- [11] WU J H, SHENG X F, LI G S, et al. An efficient and secure aggregation encryption scheme in edge computing[J]. China Communications, 2022, 19(3): 245-257.
- [12] 杨亚涛, 林天祥, 陈剑源等. 边缘计算模式下全同态加密智能合约设计[J]. 信息安全学报, 2022, 7(2): 150-162.
YANG Y T, LIN T X, CHEN J Y, et al. Smart contract with fully homomorphic encryption under edge computing mode[J]. Journal of Cyber Security, 2022, 7(2): 150-162.
- [13] CHEN X. A security integration model for private data of intelligent mobile communication based on edge computing[J]. Computer Communications, 2020, 162: 204-211.
- [14] LIANG W, XIE S, CAI J, et al. Novel private data access control scheme suitable for mobile edge computing[J]. China Communications, 2021, 18(11): 92-103.
- [15] YAN X, WU Q, SUN Y. A homomorphic encryption and privacy protection method based on blockchain and edge computing[J]. Wireless Communications and Mobile Computing, 2020, 2020: 1-9.
- [16] XU G, DONG J, MA C, et al. A certificateless signcryption mechanism based on blockchain for edge computing[J]. IEEE Internet of Things Journal, 2023, 10(14): 11960-11974.
- [17] AL SHAHRANI A M, RIZWAN A, SANCHEZ-CHERO M, et al. Blockchain-enabled federated learning for prevention of power terminals threats in IoT environment using edge zero-trust model[J]. The Journal of Supercomputing, 2023: 1-27.
- [18] LIAO J, WANG H, WU J. A multikey fully homomorphic encryption privacy protection protocol based on blockchain for edge computing system[J]. Concurrency and Computation: Practice and Experience, 2023, 35(4): e7539.
- [19] 王瑞锦, 唐榆程, 张巍琦, 等. 基于同态加密和区块链技术的车联网隐私保护方案[J]. 网络与信息安全学报, 2020, 6(1): 46-53.
WANG R J, TANG Y C, ZHANG W Q, et al. Privacy protection scheme for internet of vehicles based on homomorphic encryption and block chain technology[J]. Chinese Journal of Network and Information Security, 2020, 6(1): 46-53.
- [20] CHEN W, WANG Z, GE Q, et al. Quantized distributed economic dispatch for microgrids: paillier encryption - decryption scheme[J]. IEEE Transactions on Industrial Informatics, 2024, 20(4): 6552 - 6562.
- [21] 郭江兴. 网络空间内生安全: 拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020: 587 - 588.
WU J X. Endogenous security in cyberspace: mimetic defense and generalized robust control[M]. Beijing: China Science Publishing & Media Ltd, 2020: 587 - 588.
- [22] ZHENG Y, LI Z, XU X, et al. Dynamic defenses in cyber security: techniques, methods and challenges[J]. Digital Communications and Networks, 2022, 8(4): 422-435.
- [23] 普黎明, 卫红权, 李星, 等. 面向云应用的拟态云服务架构[J]. 网络与信息安全学报, 2021, 7(1): 101-112.
PU L M, WEI H Q, LI X, et al. Mimic cloud service architecture for cloud applications[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 101-112.
- [24] SHAO S S, JI Y M, ZHANG W L, et al. A DHR executor selection algorithm based on historical credibility and dissimilarity clustering[J]. Science China Information Sciences, 2023, 66(11): 212304.
- [25] TAO Y, KONG F, YU J, et al. EPPSA: efficient privacy-preserving statistical aggregation scheme for edge computing-enhanced wireless sensor networks[J]. Security and Communication Networks,

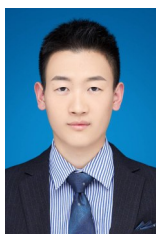
2022, 2022(1): 7359134.

- [26] XIE C, WENG J, ZHOU D H. Revocable identity-based fully homomorphic signature scheme with signing key exposure resistance [J]. Information Sciences, 2022, 594: 249-263.
- [27] HU Z X, KAIS S. A quantum encryption design featuring confusion, diffusion, and mode of operation[J]. Scientific Reports, 2021, 11(1): 23774.

[作者简介]



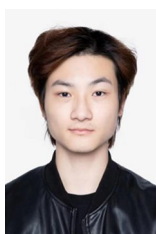
顾天晟 (2000-), 男, 江苏南通人, 南京邮电大学硕士生, 主要研究方向为拟态防御、网络安全。



曾福康 (1999-), 男, 江苏扬州人, 南京邮电大学硕士生, 主要研究方向为网络安全、公钥密码学。



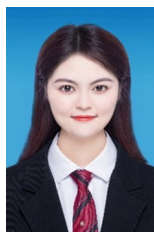
邵思思 (1997-), 女, 江苏东海人, 南京邮电大学博士生, 主要研究方向为内生安全、主动防御。



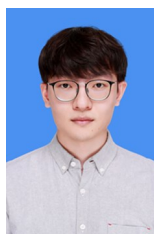
聂一君 (2000-), 男, 河南周口人, 南京邮电大学硕士生, 主要研究方向为内生安全、网络安全。



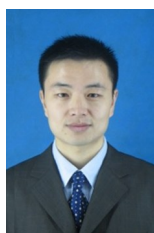
纪宗凯 (2001-), 男, 江苏盐城人, 南京邮电大学硕士生, 主要研究方向为网络安全。



郑雨璐 (2001-), 女, 河南鹤壁人, 南京邮电大学硕士生, 主要研究方向为内生安全、拟态防御和纠错编码通信。



石雨辰 (2000-), 男, 山西临汾人, 南京邮电大学硕士生, 主要研究方向为网络安全。



刘尚东 (1979-), 男, 江苏南京人, 博士, 南京邮电大学讲师, 主要研究方向为网络行为分析、大数据与人工智能。



季一木 (1978-), 男, 安徽无为, 博士, 南京邮电大学教授、博士生导师, 主要研究方向为云计算、大数据、物联网和人工智能安全及应用。