Design of Secondary Enhanced Encryption Method for Data Storage of IoT Hybrid Sensor Nodes*

GONG Fagen[1], HE Yongjun[2], ZHONG Shaohong[3*]
(1.Practical Training Center, Guangdong Polytechnic of Science and Technology, Zhuhai Guangdong 519090, China; 2.Computer Engineering Technical College (Artificial Intelligence College), Guangdong Polytechnic of Science and Technology, Zhuhai Guangdong 519090, China; 3.School of Computer Science and Information Engineering, Central South University of Forestry and Technology, Changsha Hu'nan 410004, China)

Abstract: IoT hybrid sensing nodes cover multiple sensors, each sensor has a large amount of data and is prone to containing a large amount of sensitive information. In order to improve the security of data storage in IoT hybrid sensor nodes, a secondary enhanced encryption method for IoT hybrid sensor node data storage is proposed. Neural networks and composite discrete chaotic systems are used to perform initial encryption of sensor node data, and AES algorithm and ECC algorithm are combined to peform secondary encryption of sensor node data. The ciphertext, AES key block, and signature block are direct transmitted to the receiving end to achieve secondary enhanced encryption of mixed sensing node data in the Internet of Things. The simulation results show that the key generation time and encryption time of the proposed method are always below 280 ms, and the storage cost is less than 1.6×10^4 byte. The information leakage ratio is less than 0.13, which can effectively reduce the execution time of the encryption process, data storage overhead, and information leakage ratio, protect the data of IoT hybrid sensor nodes, and improve the data storage security of IoT hybrid sensor nodes.

Key words: hybrid sensor node; enhanced encryption; AES algorithm; ECC algorithm; Internet of Things; data storage
EEACC: 7230 **doi**: 10.3969/j.issn.1004-1699.2025.11.022

物联网混合传感节点数据存储二次增强加密方法设计*

龚发根[1], 何拥军[2], 钟少宏[3*]
(1.广东科学技术职业学院实训中心, 广东 珠海 519090; 2.广东科学技术职业学院计算机工程技术学院(人工智能学院), 广东 珠海 519090; 3.中南林业科技大学计算机与信息工程学院, 湖南 长沙 410004)

摘 要: 物联网混合传感节点涵盖多个传感器, 每个传感器的数据量庞大, 且易包含大量敏感信息。为了提高物联网混合传感节点数据存储的安全性, 提出一种物联网混合传感节点数据存储二次增强加密方法。采用神经网络和复合离散混沌系统, 初始加密传感器节点数据, 结合 AES 算法和 ECC 算法, 二次加密传感器节点数据。将密文、AES 密钥块和签名块直接传输至接收端, 实现物联网混合传感节点数据二次增强加密。仿真结果表明, 所提方法的密钥生成时间和加密时间始终在 280 ms 以下, 存储开销低于 1.6×10^4 byte, 信息泄露比低于 0.13, 能够有效降低加密过程执行时间、数据存储开销和信息泄露比, 保护物联网混合传感节点数据, 提高物联网混合传感节点数据存储安全性。

关键词: 混合传感节点; 增强加密; AES 算法; ECC 算法; 物联网; 数据存储
中图分类号: TP309.2 **文献标识码**: A **文章编号**: 1004-1699(2025)11-2088-06

混合传感节点是物联网系统中的一种特殊节点, 它通常由多个不同类型的传感器采集而成, 可以同时感知多种环境参数。通过利用多种不同类型的传感器不间断采集和传输环境数据, 为各种应用提供实时且可靠的信息。但是随着物联网的不断发展以及广泛应用, 物联网混合传感节点收集的数据包含大量敏感信息, 如果这些数据没有得到适当的保护, 可能会被非法获取或者滥用[1-2]等。所以对物联网混合传感节点数据存储实施增强加密对保护数据隐私以及防止数据泄露具有十分重要的作用。

相关专家针对物联网混合传感节点数据存储加密方面的内容展开了大量研究。文献[3]将 OFDM 信号转换为三维信号矩阵, 采用三维 Arnold 变换对其展开置乱变换处理, 完成对数据的加密。文献[4]利用神经网络模型提取深度图像特征, 采用主成分分析将全部特征展开融合以及降维处理; 计算安全索引以及搜索陷门两者间的相似度, 获取密文图像检索结果; 将不同加密机制有效结合展开加密处理, 最终实

项目来源: 广东省教育厅科研重点专项项目(2020ZDZX3118); 广东省普通高校重点领域专项项目(2022ZDZX1056); 广东省教育厅科研重点专项项目(2023ZDZX1060)
收稿日期: 2023-11-13 **修改日期**: 2023-12-26

现属性基加密。文献[5]在不可信的 BSN 环境中重新定义了选择性加密方案,以保护体感数据免受攻击者的非法分类,从而进一步保护数据隐私。文献[6]使用具有伪随机序列的遗传算法的概念来加密和解密数据流。经验证,该方法在商业多媒体传输应用集成中,具有较高的可行性,可以提高实时数据保护的吞吐率。文献[7]利用基于 RC6 的轻量级混沌分组加密算法对传感器网络分组展开加密处理。但在上述方法中,仅对数据实施一次加密,未提供数据完整性和可信性的保证。攻击者可能篡改、删除或伪造数据,使得数据的可靠性受到威胁。

在以上几种加密方法的基础上,提出一种物联网混合传感节点数据存储二次增强加密方法。利用神经网络和复合离散混沌系统,初始加密传感器节点数据,压缩原始数据,以此降低数据存储开销。结合 AES 算法和 ECC 算法的优势,二次加密传感器节点数据,选取合适的椭圆曲线的域参数,以抵挡不同类型的网络攻击,从而保护物联网混合传感节点数据,提高物联网混合传感节点数据存储安全性。

1　传感节点数据存储二次加密方法设计

结合神经网络和复合离散混沌系统展开节点数据的初始加密,保护数据在传输过程中的安全性,降低传感节点数据被未经授权的人员窃取或篡改。采用高级加密标准(Advanced Encryption Standard, AES)和椭圆曲线密码学(Elliptic Curve Cryptography, ECC)算法相结合的方式,二次加密物联网混合传感节点数据,有效保护数据中的敏感信息。

1.1　物联网混合传感节点数据初始加密

为了使物联网混合传感节点数据存储具有比较高的安全性,在物联网混合传感节点数据传输过程中,采用神经网络和复合离散混沌系统相结合的方式对传感节点数据展开初始加密[8-9]。通过 Logistic 映射 L 和 Sine 映射 S 可以将对应的映射方程表示为式(1)的形式:

$$\begin{cases} L=\chi a_\kappa(1-a_\kappa) \\ S=\chi\sin(\pi a_\kappa) \end{cases} \tag{1}$$

式中:a_κ 代表第 κ 次的迭代值;χ 代表控制参数。将带有不同取值参数的 Logistic 混沌系统和 Sine 混沌系统展开线性变换以及非线性运算处理,并将系统形成的混沌序列 $A=\{A_1,A_2,\cdots,A_n\}$ 转换为二值序列 $P=\{P_1,P_2,\cdots,P_n\}$,详细的计算式如下:

$$P=\begin{cases} 0 & 0\leqslant A<\bar{A} \\ 1 & \bar{A}\leqslant A\leqslant 1 \end{cases} \tag{2}$$

式中:$\bar{A}$ 代表混沌序列的平均值。Lyapunov 指数 β 是验证混沌序列随机性以及混沌特性的指标,对应的计算式如下所示:

$$\beta=\frac{1}{i}\lim_{i\to\infty}\left[P\sum_{\kappa=1}|g'(a_\kappa)|\right] \tag{3}$$

式中:i 代表常数;g'代表变换处理后的映射方程。神经网络主要是由三个不同层组成[10-11],每个层的神经元之间以全连接的形式连接。设定输出层为 B,主要是由 B_1 和 B_2 构成。B_1 和 B_2 经过进一步处理为 $\boldsymbol{B}_1'$和 $\boldsymbol{B}_2'$,分别代表置乱矩阵的行值以及列值。网络中的传输函数主要由多个不同的函数组成,通过其可以完成输入数据的处理,如式(4)所示:

$$\boldsymbol{N}=[A_1,A_2,A_3,A_4] \tag{4}$$

式中:$\boldsymbol{N}$ 代表物联网混合传感节点数据矩阵。神经网络每运行一次,就会形成 2 个随机的 B_1 和 B_2,同时更新 C 值,采用更新后的值循环运行神经网络计算全新的输出值 B_1 和 B_2。如果所要生成的置乱矩阵大小为 $m\times n$,需要通过神经网络对应输出 B_1 和 B_2 展开下一步操作,进而得到置乱矩阵的行值 $\boldsymbol{B}_1'$ 和列值 $\boldsymbol{B}_2'$,如式(5)所示:

$$\begin{cases} \boldsymbol{B}_1'=L\bmod[\mathrm{ceil}(NB_1\times10^5),m] \\ \boldsymbol{B}_2'=S\bmod[\mathrm{ceil}(NB_2\times10^5),n] \end{cases} \tag{5}$$

采用神经网络和复合离散混沌系统对传感器节点数据展开初始加密[12-13],详细的操作步骤如下所示:

①设定置乱矩阵大小为 $m\times n$,读取位于前 $m\times n$ 位的二进制数据,将其应用于混沌系统的参数 ϕ 以及初始值 a_0,两者对应的计算式如下所示:

$$\begin{cases} \phi=\boldsymbol{B}_1'\bmod(\mathrm{sum},4) \\ a_0=\boldsymbol{B}_2'\bmod(\mathrm{sum},10)\times0.1 \end{cases} \tag{6}$$

通过复合离散混沌系统的初始值以及参数形成混沌序列。

②在步骤①组成的混沌序列中选取随机数值作为传感节点输入数据;其中,取值以及偏置矩阵分别从序列 A_s 和 A_q 中选取。通过神经网络[14]形成 B_1 和 B_2,经过处理后形成 $\boldsymbol{B}_1'$和 $\boldsymbol{B}_2'$,并且将其存储于矩阵中。假设 $\boldsymbol{B}_1'$、$\boldsymbol{B}_2'$和已经产生数值完全不同,则保留该数值,直至形成行矩阵和列矩阵的长度为 m 和 n 则停止计算。

③利用置乱矩阵对应的行列索引对系统内的星座图展开置乱变换处理,矩阵经过转换处理后为 m 行 n 列矩阵,将星座图矩阵设定为 $\boldsymbol{H}$,置乱后的矩阵为 $\boldsymbol{F}$,对应的置乱公式如下所示:

$$\boldsymbol{F}_k(i,j)=\boldsymbol{H}_k[\phi Z_k(i),a_0U_k(i)] \tag{7}$$

式中:$\boldsymbol{F}_k(i,j)$代表第 k 个置乱后的矩阵;$\boldsymbol{H}_k$ 代表第

k 个星图矩阵;$U_k(i)$代表列矩阵中的不同数值。

④完成第一次置乱处理后,将 k 个置乱后的矩阵转换为行值为 1 的矩阵。

⑤选取混沌序列中的值,将得到的数字按照取值大小排列,将其组成的数组表示为 E,以数组中各个传感节点数据的顺序确定物联网混合传感节点数据在原始数组中的具体坐标位置,得到用于加密的位置矩阵 $\boldsymbol{E}'$。

⑥重复步骤⑤,形成物联网混合传感节点数据加密所需要的全部位置矩阵。

⑦对串并转换插入导频后的物联网混合传感节点数据通过步骤⑥形成的位置矩阵展开置乱加密处理,直至串并转换循环结束,至此完成物联网混合传感节点数据初次加密处理。

1.2 物联网混合传感节点数据存储进行二次加密

在物联网混合传感节点数据存储中,进行初始加密是为了保护传感节点数据在传输过程中的安全性,防止传感节点数据被未经授权的人员窃取或篡改。然而,仅仅进行初始加密可能还不足以提供足够的安全性保障。为了进一步增强传感节点数据的安全性,需要进一步采用增强加密方法,以增加破解难度和抵抗各种攻击手段的能力。通过增强加密,可以对传感节点数据进行多次加密和混淆处理,增加攻击者破解密码的成本和难度。完成物联网混合传感节点数据初次加密[15]处理后,采用 AES 和 ECC 算法相结合的方式对物联网混合传感节点数据存储进行二次加密。

1.2.1 AES 算法

AES 算法是一种对称的分组加密技术,使用 128 位分组加密数据,广泛应用于保护敏感数据的加密和解密过程中。

AES 算法[16-17]的详细操作步骤如下所示:

①初始轮:和扩展秘钥展开异或运算。

②重复轮:主要包含四个变换,分别:

A. 字节替代操作,实际上就是以字节为单位将各个元素全部都利用一个 S 盒映射为一个新的元素,如图 1 所示。

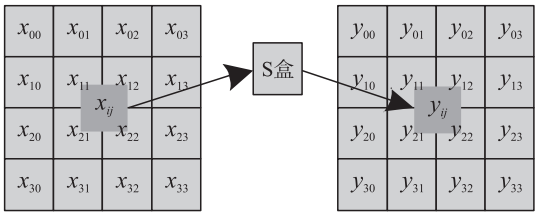


图 1 字节替代处理示意图

B. 行位移变换属于线性变换,将其和混合变换有效结合后确保传感节点加密数据能够得到更好的混淆,如图 2 所示。

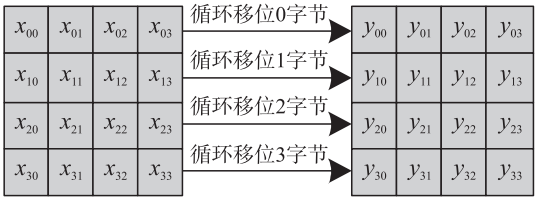


图 2 行位移变换示意图

C. 列混合变换是利用线性映射将列上的元素映射为另外一个值,使其可以达到一定程度的混淆。

D. 轮密钥加是将 128 位轮密钥同状态矩阵中的传感节点数据进行逐位异或操作,轮密钥加即将完成混淆变换时,对 state 和轮密钥矩阵中的字节分别展开异或操作。

③最终轮:

重复步骤 B 中的四个变换,最终输出密文。

在加密端,轮处理的步骤主要有字节替代、行位移、列混合以及轮密钥加,经过 10 轮处理得到密文展开传输;在解密端,轮处理的步骤主要有逆向行位移、逆向字节替代、逆向列混合和轮密钥加,密文经过解密段的 10 轮处理可以获取对应的明文。在 AES 的轮处理过程中,每轮均需要展开轮密钥加处理,解密过程实际上就是对轮变换对应加密算法的逆变换,同时解密过程中轮密钥加和加密过程是完全相同的。

1.2.2 ECC 算法

ECC 算法是一种公钥加密体制,利用椭圆曲线数学问题的难解性而构建,具有比传统 RSA 算法更小的密钥尺寸和更高的安全性。

在 ECC 算法中,很难确定椭圆曲线上全部点和其局限性,所以椭圆曲线为传感节点数据加密提供了大量良好的属性。椭圆线上的点均为一些离散点,如果遇到攻击者攻击,也无法将离散点连接成正确的曲线,也无法了解曲线参数之间的关系。所以椭圆曲线的域参数选取十分重要,只有可以抵抗不同类型的攻击手段,才能够有效确保密码系统的安全性。

椭圆曲线的域参数选取以及验证是保证密码系统安全性的关键,为了使密码系统具有良好的安全属性,域参数的选取需要满足以下条件:①参数 p 的取值越大,则说明系统的安全性越高。通常情况下,p 大约 200 位的取值即可达到安全需求。②可以抵抗大小步算法(Baby-Step-Giant-Step,BSGS)的攻击。

当满足以上条件后,结合置乱后的矩阵 $\boldsymbol{F}_k(i,$

j),增加传感节点数据的随机性和复杂性,使得破解者难以对其中的椭圆曲线点进行逐个尝试和计算。经过求解可以获取一对正确的密钥(K_s,K_p)。设定待加密的明文传感节点数据为 M,在展开传感节点数据处理前期需要展开映射变换,将 M 映射到 $N_p(a,b)$的随机一个点上。假设明文传感节点数据较长,则需要对其展开分组处理。完成上述操作后,需要选择一个随机数,经过计算得到另外一个椭圆曲线点,最终完成传感节点数据加密处理。

通过上述分析,采用 AES 算法和 ECC 算法相结合的方式展开物联网混合传感节点数据存储二次加密处理,详细的操作步骤如下所示:①读取明文,采用 AES 算法对物联网混合传感节点数据展开加密处理,获取通过 AES 加密处理后的密文 c 和加密密钥 s_a,同时密钥的设计可以利用函数展开配置。②利用 ECC 加密算法对加密密钥 s_a 展开加密处理,获取 AES 密钥块。③引入 MD5 算法对物联网混合传感节点数据展开加密处理,形成明文摘要,同时通过 ECC 签名算法展开签名处理获取签名块。④将密文、AES 密钥块和签名块直接传输至接收端,完成物联网混合传感节点数据存储二次加密处理。

2　仿真分析

2.1　仿真环境和仿真参数

为了确保仿真环境的一致性,全部的仿真都在同一台机器上展开。设置神经网络层数为 3 层,各层中神经元的数量分别为 64、128、64,置乱矩阵大小为 8×8,采用 QPSK 星座图,即 4 个星点,使用 128 位的二进制数据共 5 GB 进行仿真分析。物联网混合传感节点数据存储架构如图 3 所示。

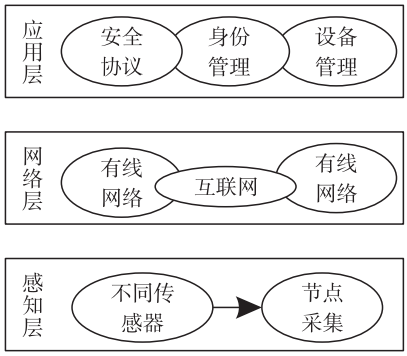


图 3　物联网混合传感节点数据存储架构

2.2　仿真结果

2.2.1　加密速度分析

将基于混沌映射的加密方法(文献[3]方法)、可检索的加密方法(文献[4]方法)和基于监督机器学习的加密方法(文献[5]方法)作为对比方法。不同方法的密钥生成时间和对物联网混合传感节点数据存储二次加密处理的执行时间变化如图 4 和图 5 所示。

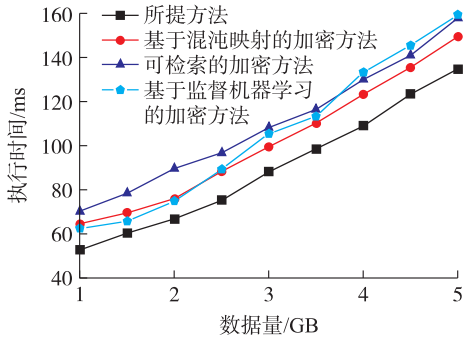


图 4　各个方法的密钥生成时间比较

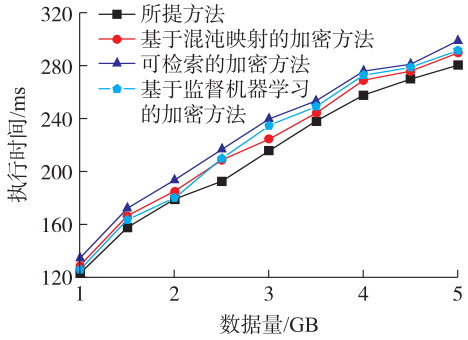


图 5　各个方法的执行时间比较

通过图 4 和图 5 可以看出,在加密数据量比较低的情况下,各个加密方法的密钥生成时间和执行时间也就相对较低。在数据量较大的情况下,可检索的加密方法的密钥生成时间和执行时间最高,在相同加密数据量下,不同方法的密钥生成时间和执行时间存在比较大的差距。但是所提方法的密钥生成时间和加密时间明显更低一些,且始终在 280 ms 以下,说明所提方法具有比较高的执行速度,适用于解决物联网混合传感节点数据存储二次加密问题。这是因为所提方法结合 Logistic 混沌系统和 Sine 混沌系统进行非线性运算处理,增强混沌序列的不可预测性和随机性,降低了加密过程的执行时间。

2.2.2　存储开销分析

由于内存的稀疏性,主要分析内存在执行过程中的开销,各个方法在物联网混合传感节点数据存储二次加密过程中的存储开销变化情况如图 6 所示。

通过图 6 可以看出,在相同的加密数据量下各个方法的存储开销存在比较明显的差异。经过比较可知,所提方法的存储开销始终在 1.6×10^4 byte 以下,充分验证了所提方法的优越性。因为所提方法采用神经网络和复合离散混沌系统实施传感器节点

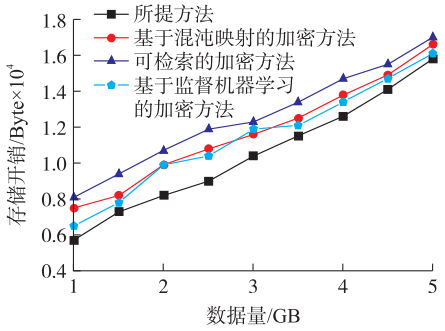


图 6 不同加密数据量下各个方法的存储开销比较

数据的初始加密,将原始数据进行压缩,降低了数据存储开销。

2.2.3 信息泄露比分析

为了验证所提方法的加密性能,选取信息泄露比作为仿真指标,该项指标取值越大,则说明物联网混合传感节点数据存储二次加密性能越差,无法有效确保数据的安全性。分析不同方法的信息泄露比变化情况,如图 7 所示。

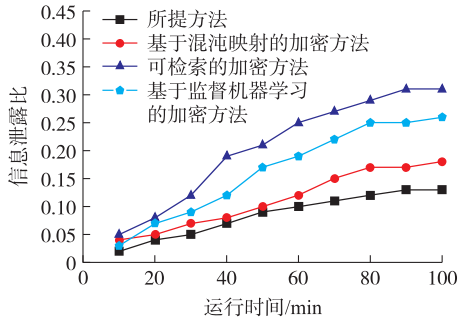


图 7 不同方法的信息泄露比

通过分析图 7 可知,随着时间的不断变化,各个方法对应的信息泄露比也发生了比较明显的变化。但是相比另外两种方法而言,所提方法的信息泄露比取值低于 0.13,可以更好地保护物联网混合传感节点数据存储的安全性,也充分证明所提方法展开初始加密和二次加密是可行且有效性的,可以达到增强加密的目的。这是因为所提方法引入了 MD5 算法,进一步加密了传感节点数据,形成了明文摘要,传输密文、AES 密钥块和签名块至接收端,实现了二次加密,降低了信息泄露比。

2.2.4 综合性能分析

通过上述仿真分析,对各个加密方法的综合性能展开比较,具体如表 1 所示。

通过表 1 可知,所提方法可以更好地实现物联网混合传感节点数据存储二次加密处理,可以更好保护物联网混合传感节点数据;该方法结合了 AES 算法和 ECC 算法的优势,选取合适的椭圆曲线的域参数,以抵挡不同类型的网络攻击。而另外两种方法的加密性能需要进一步提升。

表 1 不同加密方法的功能比较

功能	所提方法	基于混沌映射的加密方法	可检索的加密方法	基于监督机器学习的加密方法
存储开销	较低	高	较高	较高
效率性	高	较高	较低	高
安全性	高	低	较低	较高
可扩展性	高	较低	低	低
易用性	高	较低	较低	高
加密强度	高	低	低	较高

3 结束语

在物联网中,混合传感节点数据存储增强加密技术具有十分重要的意义。为此,提出一种物联网混合传感节点数据存储二次增强加密方法。仿真结果表明,所提方法可以有效降低密钥生成时间和执行时间,同时还可以有效减少信息泄露比和存储开销,可以更好地保护物联网混合传感节点数据的安全性。未来阶段,将致力于相关领域的研究工作,为全面推动物联网技术进步和发展做出更大的贡献。

参考文献:

[1] 方友志,张云凤. 高速网络多段支持度数据自动加密算法仿真[J]. 计算机仿真,2021,38(12):237-240.

[2] 王峥,孙泉. 雾计算中支持计算外包的微型属性加密方案[J]. 计算机工程与科学,2022,44(3):427-435.

[3] 周玉鑫,毕美华,滕旭阳,等. 基于混沌映射的 OFDM-PON 物理层加密及系统性能增强算法[J]. 光学学报,2021,41(16):33-40.

[4] 赵博,李春亮,孙碧颖,等. 一种智能电网敏感图像可检索的属性基加密方案[J]. 西安交通大学学报,2021,55(11):136-146.

[5] Qiu H,Qiu M,Lu Z. Selective Encryption on ECG Data in Body Sensor Network Based on Supervised Machine Learning[J]. Information Fusion,2020,55:59-67.

[6] Baagyere E Y,Agbedemnab P A N,Qin Z,et al. A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers[J]. IEEE Access,2020,8:100438-100447.

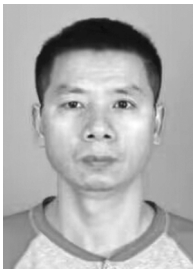
[7] 葛仕杰,汪烈军,李永明. 基于混沌的无线传感器网络分组加密算法[J]. 计算机工程与设计,2022,43(9):2456-2463.

[8] 陈思伟,高翠云,沈庆伟,等. 面向智能家居的生理参数密钥加密方法研究[J]. 电子测量与仪器学报,2021,35(3):173-180.

[9] 赵梓婷,徐银,宋祥福,等. 基于差分隐私的多模式隐藏动态对称可搜索加密方案[J]. 计算机研究与发展,

2021,58(10):2287-2299.
[10] 杨鹤标,胡惊涛,刘芳. 基于神经网络语言模型的动态层序 Softmax 训练算法[J]. 江苏大学学报(自然科学版),2020,41(1):67-72,80.
[11] 张勇,郭永存,陈伟,等. 高效移动端煤矸识别方法[J]. 中国粉体技术,2023,29(1):61-70.
[12] 郭威,李信红,林晓宁,等. 基于属性规则的复合电力数据权限加密算法[J]. 电网与清洁能源,2023,39(4):76-82,90.
[13] 王小龙,张黎明,闫浩文,等. 利用哈尔变换和高斯随机数进行矢量空间数据坐标加密[J]. 武汉大学学报(信息科学版),2022,47(11):1946-1955.
[14] 李孟奇,屈美娇,何卫锋,等. 基于 BP 神经网络的力学行为模型构建方法[J]. 兵器材料科学与工程,2022,45(3):1-7.
[15] 宋翔飞,王化群. 一个具有前向安全和后向安全的可验证多关键字可搜索加密方案[J]. 计算机学报,2023,46(4):727-742.
[16] 赵秉宇,王柳生,张美玲,等. 针对重用掩码 AES 算法的随机明文碰撞攻击[J]. 计算机工程,2022,48(6):139-145,153.
[17] 王淑梅,宋佳宝,刘广哲,等. 基于交替量子随机行走的改进 AES 和离散余弦变换的图像加密算法[J]. 北京工业大学学报,2023,49(6):647-655.

龚发根(1970—),男,汉族,江西永丰人,硕士,广东科学技术职业学院计算机科学与技术副教授,研究方向:云计算、大数据、人工智能、信息安全。从事竞赛管理、计算机网络技术专业的教学和研究工作 27 年,主持和主要参与科研和教改项目 7 项,发表论文 20 余篇;其中 EI 收录 1 篇;主讲课程《活动目录的规划、实现和管理》《网络安全的实现与管理》《路由与交换技术》《公有云技术与实施》等。工作以来,多次组织学生参加"全国职业院校技能大赛"等学科竞赛,指导的学生获得国家级一等奖 1 项、二等奖 2 项,省级一等奖 3 项;多次荣获"优秀教师""学生最满意课程"等荣誉 gongfagen2023@163.com;



钟少宏(1976—),男,汉族,湖南衡阳人,博士,副教授,硕士生导师。计算机应用技术专业工学博士。主要研究方向为工业物联网、5G 与深度学习和信息年龄等。中国计算机学会会员,IEEE 会员,IEEE CS 会员,湖南省计算机学会理事。湖南省自然科学基金评审专家、江西省自然科学基金评审专家、湖南省发改委项目评审专家。现任中南林业科技大学计算机与信息工程学院软件工程系主任。主持教育部产学研协同育人项目 2 项,指导学生主持国家级大学生创新训练项目 2 项,主持湖南省自然科学基金项目 1 项,主持湖南省教育厅教学改革项 1 项,主持湖南省教育厅科学研究重点项目 1 项,主持湖南省教育厅科学研究面上项目 2 项,作为第一参与人参与国家自然科学基金项目 1 项。发表论文 20 余篇(其中 SCI、EI 检索 7 篇),授权发明专利 1 项,软件著作权 5 项,zhongshaohong1976@163.com。

何拥军(1976—),男,汉族,湖南邵阳人,硕士研究生,教授,研究方向:区块链、云计算、数据存储;