



主管：中华人民共和国公安部  
主办：公安部第三研究所  
中国计算机学会

ISSN1671-1122  
CN31-1859/TN  
中文核心期刊  
中国科技核心期刊  
中国科学引文数据库来源期刊  
CCF计算领域高质量科技期刊

# 信息安全

NETINFO SECURITY

## 等级保护

基于机器学习的匿名流量分类方法研究

## 技术研究

新形态伪随机函数研究

无线传感器网络中虚假数据途中过滤技术研究

基于可验证秘密共享的多关键词可搜索加密方案

ISSN 1671-1122



2023年 5月 第5期

总第269期



中国计算机学会会刊

万方数据

□ 等级保护

1 基于机器学习的匿名流量分类方法研究 ..... 赵小林, 王琪瑶, 赵斌, 薛静锋

□ 技术研究

- 11 新形态伪随机函数研究..... 李增鹏, 王梅, 陈梦佳
- 22 无线传感器网络中虚假数据途中过滤技术研究 ..... 冯光升, 张盈希, 任奕菲, 高素林
- 32 基于可验证秘密共享的多关键词可搜索加密方案 ..... 秦宝东, 陈从正, 何俊杰, 郑东
- 41 基于未知故障模型的多重持续故障分析 ..... 毛红晶, 程驭坤, 胡红钢
- 50 混源操作系统供应链安全风险评估方法研究 ..... 赵俊, 任怡, 李宝, 谭郁松
- 62 基于 Siamese 架构的恶意软件隐藏函数识别方法 ..... 陈梓彤, 贾鹏, 刘嘉勇
- 76 面向分组密码的高速可重构模运算单元设计 ..... 张晓磊, 戴紫彬, 刘燕江, 曲彤洲
- 85 EHR 系统中一种验证外包加密数据正确性的访问控制方案..... 张晓旭, 石润华

□ 理论研究

95 用于云存储的主动秘密共享方案 ..... 裴蓓, 张水海, 吕春利

□ 网域动态

- 105 第三届“网鼎杯”网络安全大赛暨“数字未来网络安全大会”成功举办
- 106 “第六届中国可信计算产业发展论坛”在京顺利召开
- 107 国家网信办：生成式人工智能产品提供服务前需申报安全评估
- 108 北京大学郭弘团队在经典兼容的数字化量子密钥分发中取得突破

# CONTENTS

|    |                                                                                         |                                                     |
|----|-----------------------------------------------------------------------------------------|-----------------------------------------------------|
| 1  | Research on Anonymous Traffic Classification Method Based on                            |                                                     |
|    | Machine Learning.....                                                                   | ZHAO Xiaolin, WANG Qiyao, ZHAO Bin, XUE Jingfeng    |
| 11 | Research of New Forms of Pseudorandom Random Function.....                              | LI Zengpeng, WANG Mei, CHEN Mengjia                 |
| 22 | Research on En-Route False Data Filtering Technology in                                 |                                                     |
|    | Wireless Sensor Network.....                                                            | FENG Guangsheng, ZHANG Yingxi, REN Yifei, GAO Sulin |
| 32 | Multi-Keyword Searchable Encryption Scheme Based on                                     |                                                     |
|    | Verifiable Secret Sharing .....                                                         | QIN Baodong, CHEN Congzheng, HE Junjie, ZHENG Dong  |
| 41 | Multiple Persistent Faults Analysis with Unknown Faults.....                            | MAO Hongjing, CHENG Yukun, HU Honggang              |
| 50 | Research on the Supply Chain Security Risk Assessment Methods for                       |                                                     |
|    | Mixed Source Operating System.....                                                      | ZHAO Jun, REN Yi, LI Bao, TAN Yusong                |
| 62 | Identification Method of Malicious Software Hidden Function Based on                    |                                                     |
|    | Siamese Architecture .....                                                              | CHEN Zitong, JIA Peng, LIU Jiayong                  |
| 76 | Design of High Speed Reconfigurable Modulo Arithmetic Unit for                          |                                                     |
|    | Block Cipher.....                                                                       | ZHANG Xiaolei, DAI Zibin, LIU Yanjiang, QU Tongzhou |
| 85 | An Access Control Scheme for Verifying the Correctness of Outsourcing Encrypted Data in |                                                     |
|    | EHR System .....                                                                        | ZHANG Xiaoxu, SHI Runhua                            |
| 95 | A Proactive Multi-Secret Sharing Scheme for Cloud Storage.....                          | PEI Bei, ZHANG Shuihai, LYU Chunli                  |

**敬告：** 本期所有文字和图片来经本刊书面许可，不得转载。  
本刊已被中国科技核心期刊、中国科学引文数据库来源期刊、中国学术期刊全文数据库、中文科技期刊数据库(全文版)等数据库收录,如果作者不同意文章被收录,请在来稿时向本刊声明,本刊将做适当处理。

广告



科学佩戴口罩是预防呼吸道传染病的重要措施之一，养成随身携带口罩的习惯，有需要时及时正确佩戴。

中宣部宣教局、国家卫生健康委宣传司 指导  
中国健康教育中心 制作