

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（计算机安全专业委员会）

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

# 信息安全

NETINFO SECURITY

## 等级保护

一种支持数据所有权动态管理的数据去重方案

## 技术研究

云环境下基于多密钥全同态加密的定向解密协议设计

大规模移动RFID系统Shamir's密钥共享PUF安全认证协议

GPU上SM4算法并行实现

ISSN 1671-1122



9 771671 112200 06 >

2020年 6月 第6期

总第234期

## □ 等级保护

- 1 一种支持数据所有权动态管理的数据去重方案 ..... 郎为民, 马卫国, 张寅, 姚晋芳

## □ 技术研究

- 10 云环境下基于多密钥全态加密的定向解密协议设计 ..... 李宁波, 周昊楠, 车小亮, 杨晓元
- 17 基于 SM3 与多特征值的 Android 恶意软件检测 ..... 郑东, 赵月
- 26 大规模移动 RFID 系统 Shamir's 密钥共享 PUF 安全认证协议 ..... 孙子文, 张向阳
- 36 GPU 上 SM4 算法并行实现 ..... 李秀滢, 吉晨昊, 段晓毅, 周长春
- 44 大数据环境下的本地差分隐私图信息收集方法 ..... 张佳程, 彭佳, 王雷
- 57 基于 HTTP 协议组合的隐蔽信道构建方法研究 ..... 陈骋, 罗森林, 吴倩, 杨鹏
- 65 基于果蝇优化的虚拟 SDN 网络映射算法 ..... 冉金鹏, 王翔, 赵尚弘, 高航航
- 75 面向云存储的支持范围密文搜索的属性基加密方案 ..... 施国峰, 张兴兰
- 82 基于思维进化算法优化 S-Kohonen 神经网络的恶意域名检测模型 ..... 罗峥, 张学谦

## □ 理论研究

- 90 基于 Conformal Prediction 的威胁情报繁殖方法 ..... 张永生, 王志, 武艺杰, 杜振华

## □ 网域动态

- 96 公安网安部门专项整治违法违规 APP 取得初步成效 违法收集公民个人信息十大案例发布
- 97 专家呼吁加码个人隐私保护 建立数据全生命周期管理
- 98 “中国电子工业标准化技术协会工业互联网平台生态工作委员会成立大会暨第一届委员会”成功召开
- 99 重庆大学计算机学院在软件定义异构车联网的高效数据分发研究方面取得新进展

# CONTENTS

---

1	A Data Deduplication Scheme Supporting Dynamic Management of Data Ownership .....	LANG Weimin, MA Weiguo, ZHANG Yin, YAO Jinfang
10	Design of Directional Decryption Protocol Based on Multi-key Fully Homomorphic Encryption in Cloud Environment.....	LI Ningbo, ZHOU Haonan, CHE Xiaoliang, YANG Xiaoyuan
17	Android Malware Detection Based on SM3 and Multi-feature.....	ZHENG Dong, ZHAO Yue
26	Large-scale Mobile RFID System Shamir's Key Sharing PUF Security Authentication Protocol .....	SUN Ziwen, ZHANG Xiangyang
36	Parallel Implementation of SM4 Algorithm on GPU .....	LI Xiuying, JI Chenhao, DUAN Xiaoyi, ZHOU Changchun
44	A Graph Information Collection Method Based on Local Differential Privacy in Big Data Environment.....	ZHANG Jiacheng, PENG Jia, WANG Lei
57	Research on Covert Channel Construction Method Based on HTTP Protocol Combination .....	CHEN Cheng, LUO Senlin, WU Qian, YANG Peng
65	Virtual SDN Network Embedding Algorithm Based on Fruit Fly Optimization.....	RAN Jinpeng, WANG Xiang, ZHAO Shanghong, GAO Hanghang
75	An Attribute-based Encryption Scheme for Cloud Storage Supporting Range Ciphertext Search .....	SHI Guofeng, ZHANG Xinglan
82	A Malicious Domain Name Detection Model Based on S-Kohonen Neural Network Optimized by Evolutionary Thinking Algorithm .....	LUO Zheng, ZHANG Xueqian
90	Cyber Threat Intelligence Propagation Based on Conformal Prediction .....	ZHANG Yongsheng, WANG Zhi, WU Yijie, DU Zhenhua

**敬告：**

本期所有文字和图片未经本刊书面许可，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。