

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

基于Polar码改进的McEliece密码体制

技术研究

隐私保护集合交集计算协议

多机构授权下可追踪可隐藏的属性基加密方案

云计算平台基于角色的权限管理系统设计与实现

ISSN 1671-1122



2020年 第1期

总第229期

□ 等级保护

- 1 基于 Polar 码改进的 McEliece 密码体制 韩益亮, 李喆, 李鱼

□ 技术研究

- 9 隐私保护集合交集计算协议 唐春明, 林旭慧
- 16 面向属性迁移状态的 P2P 网络行为分析方法研究 荆涛, 万巍
- 26 抗量子本原格上高效的属性基消息恢复签名方案 张建航, 曹泽阳, 宋晓峰, 徐庆征
- 33 多机构授权下可追踪可隐藏的属性基加密方案 许盛伟, 王飞杰
- 40 基于功率控制与中继协作的抗窃听攻击模型 李瑞兴, 许力, 方禾
- 46 基于知识图谱驱动的网络安全等级保护日志审计分析模型研究 陶源, 黄涛, 李末岩, 胡巍
- 52 基于复杂网络的智能电网网络攻击影响分析研究 董威, 李永刚
- 61 一种基于 PUF 的物理层安全认证方法 胡蝶, 马东堂, 龚旻, 马召
- 67 融合多特征的 Android 恶意软件检测方法 侯留洋, 罗森林, 潘丽敏, 张笈
- 75 云计算平台基于角色的权限管理系统设计与实现 白嘉萌, 寇英帅, 刘泽艺, 查达仁
- 83 具有数据上传管控的无证书可证明数据持有方案 李晓冉, 郝蓉, 于佳

□ 理论研究

- 89 基于可信计算和 UEBA 的智慧政务系统 吴宏胜

□ 网域动态

- 94 “第 14 届政府 / 行业信息化安全年会” 在京顺利召开
- 95 公安部“云剑”行动成效明显
- 96 “国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求》(报批稿) 试点工作启动会” 在京召开
- 97 “2019 新一代人工智能院士高峰论坛” 在深圳举办

CONTENTS

1	An Improved McEliece Cryptosystem Based on Polar Code.....	HAN Yiliang, LI Zhe, LI Yu
9	Protocol of Privacy-preserving Set Intersection Computation.....	TANG Chunming, LIN Xuhui
16	Research on a P2P Network Communication Behavior Analytical Method for Status Migration Attribute-oriented.....	JING Tao, WAN Wei
26	Quantum-resistant Efficient Identity-based Signature Scheme with Message Recovery over Primitive Lattices ...	ZHANG Jianhang, CAO Zeyang, SONG Xiaofeng, XU Qingzheng
33	Attribute-based Encryption Scheme Traced Under Multi-authority.....	XU Shengwei, WANG Feijie
40	Anti-eavesdropping Attack Model Based on Power Control and Relay Cooperation.....	LI Ruixing, XU Li, FANG He
46	Research on Log Audit Analysis Model of Cyberspace Security Classified Protection Driven by Knowledge Map	TAO Yuan, HUANG Tao, LI Moyan, HU Wei
52	Research on Analysis of Attacks on Smart Grid Network Based on Complex Network.....	DONG Wei, LI Yonggang
61	A Physical Layer Security Authentication Method Based on PUF	HU Die, MA Dongtang, GONG Ming, MA Zhao
67	Multi-feature Android Malware Detection Method.....	HOU Liuyang, LUO Senlin, PAN Limin, ZHANG Ji
75	Docker-based RBAC Task Management System	BAI Jiameng, KOU Yingshuai, LIU Zeyi, ZHA Daren
83	Certificateless Provable Data Possession with Data Uploading Control.....	LI Xiaoran, HAO Rong, YU Jia
89	Intelligent Government System Based on Trusted Computing and UEBA.....	WU Hongsheng

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。