

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

信息网络安全

NETINFO SECURITY

等级保护

基于局部图匹配的智能合约重入漏洞检测方法

技术研究

基于混沌和改进广义Feistel结构的轻量级密码算法

基于twisted Edwards曲线的无证书盲签名方案

基于区块链和智能合约的双链车联网系统

ISSN 1671-1122



9 771671 112224

08>

2022年 8月 第8期

总第260期



中国计算机学会会刊

□ 等级保护

- 1 基于局部图匹配的智能合约重入漏洞检测方法 张玉健, 刘代富, 童飞

□ 技术研究

- 8 基于混沌和改进广义 Feistel 结构的轻量级密码算法 佟晓筠, 苏煜粤, 张淼, 王翥

- 19 基于 twisted Edwards 曲线的无证书盲签名方案 刘芹, 张标, 涂航

- 26 基于区块链和智能合约的双链车联网系统 胡艺, 余堃

- 36 抗温度干扰的 STT-MRAM 随机数生成器及其安全性分析 伍麟珺, 刘洋, 袁涛, 胡玉鹏

- 44 基于前后端关联性分析的固件漏洞静态定位方法 刘翎翔, 潘祖烈, 李阳, 李宗超

- 55 基于 CNN-MGU 的侧信道攻击研究 高博, 陈琳, 严迎建

- 64 基于深度森林的网络匿名流量检测方法研究与应用 魏松杰, 李成豪, 沈浩桐, 张文哲

- 72 基于 MPT 索引的高效链上 PKI 模型 黄保华, 赵伟宏, 彭丽, 谢统义

□ 理论研究

- 81 基于 GAN-Cross 的工控系统类不平衡数据异常检测 顾兆军, 刘婷婷, 高冰, 隋嵩

□ 网域动态

- 90 《2021—2022 年中国算力建设网络传播分析报告》发布

- 91 《量子“Q 波”技术白皮书》发布, 量子无线密钥分发技术得到初步验证

- 92 全球数字经济大会人工智能专场论坛举办, AI 安全受关注

- 93 2022 年北京网络安全大会举行

CONTENTS

1	Reentrancy Vulnerability Detection in Smart Contracts Based on Local Graph Matching	ZHANG Yujian, LIU Daifu, TONG Fei
8	Lightweight Cipher Algorithm Based on Chaos and Improved Generalized Feistel Structure	TONG Xiaojun, SU Yuyue, ZHANG Miao, WANG Zhu
19	Certificateless Blind Signature Scheme Based on twisted Edwards Curve	LIU Qin, ZHANG Biao, TU Hang
26	Blockchain and Smart Contract Based Dual-Chain Internet of Vehicles System	HU Yi, SHE Kun
36	STT-MRAM Random Number Generator with Anti-Temperature Interference and Security Analysis	WU Linjun, LIU Yang, YUAN Tao, HU Yupeng
44	Firmware Vulnerability Static Localization Method Based on Front-End and Back-End Correlation Analysis	LIU Lingxiang, PAN Zulie, LI Yang, LI Zongchao
55	Research on Side Channel Attack Based on CNN-MGU	GAO Bo, CHEN Lin, YAN Yingjian
64	Research and Application of Network Anonymous Traffic Detection Method Based on Deep Forest	WEI Songjie, LI Chenghao, SHEN Haotong, ZHANG Wenzhe
72	Efficient Blockchain PKI Model Based on MPT Index	HUANG Baohua, ZHAO Weihong, PENG Li, XIE Tongyi
81	Anomaly Detection of Imbalanced Data in Industrial Control System Based on GAN-Cross	GU Zhaojun, LIU Tingting, GAO Bing, SUI He

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。