

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SM2签名的批验签高效实现方案

### 技术研究

以太坊智能合约定理证明中的形式化规约研究综述

基于跨链交互的网络安全威胁情报共享方案

基于事件的群组密钥协商协议形式化分析研究

ISSN 1671-1122



9 771671 112224

# 2022年 5月 第5期

## 总第257期



中国计算机学会会刊

### □ 等级保护

- 1 基于 SM2 签名的批验签高效实现方案..... 李莉, 白鹭, 涂航, 张标

### □ 技术研究

- 11 以太坊智能合约定理证明中的形式化规约研究综述..... 华景煜, 黄达明
- 21 基于跨链交互的网络安全威胁情报共享方案..... 冯景瑜, 张琪, 黄文华, 韩刚
- 30 基于事件的群组密钥协商协议形式化分析研究..... 沈延, 姚萌萌
- 37 基于模拟退火和粒子群混合改进算法的数据库水印技术..... 孔嘉琪, 王利明, 葛晓雪
- 46 一种基于集成学习的列车控制系统入侵检测方法..... 王浩洋, 李伟, 彭思维, 秦元庆
- 54 基于区块链的隐私信用数据受限共享技术研究..... 刘嘉微, 马兆丰, 王姝爽, 罗守山
- 64 基于时间微分博弈的网络安全防御决策方法..... 孙鹏宇, 谭晶磊, 李晨蔚, 张恒巍
- 75 针对 PMU 测量的虚假数据注入攻击检测方法..... 周婧怡, 李红娇

### □ 理论研究

- 84 基于区块链的属性加密多授权机构安全模型研究..... 崔皓宇, 马利民, 王佳慧, 张伟

### □ 网域动态

- 94 首届网络空间内生安全发展大会召开
- 95 国家计算机病毒应急处理中心监测发现十七款违法移动应用
- 96 中国教育和科研计算机网 CERNET 全面实现国际“路由安全相互协议规范”
- 97 南京大学提出量子密钥分发新协议, 提升城际传输距离与密钥率

# CONTENTS

---

1	Efficient Implementation Scheme of Batch Verification Based on SM2 Signatures.....	LI Li, BAI Lu, TU Hang, ZHANG Biao
11	Survey of Formal Specification Methods in Theorem Proving of Ethereum Smart Contract .....	HUA Jingyu, HUANG Daming
21	A Cyber Threat Intelligence Sharing Scheme Based on Cross-Chain Interaction.....	FENG Jingyu, ZHANG Qi, HUANG Wenhua, HAN Gang
30	Research on Formal Analysis Based on Event of Group Key Agreement Protocol .....	SHEN Yan, YAO Mengmeng
37	Simulated Annealing and Particle Swarm Enhanced Relational Database Watermark.....	KONG Jiaqi, WANG Liming, GE Xiaoxue
46	An Intrusion Detection Method of Train Control System Based on Ensemble Learning.....	WANG Haoyang, LI Wei, PENG Siwei, QIN Yuanqing
54	Research on the Restricted Sharing Technology of Private Credit Data Based on Blockchain.....	LIU Jiawei, MA Zhaofeng, WANG Shushuang, LUO Shoushan
64	Network Security Defense Decision-Making Method Based on Time Differential Game.....	SUN Pengyu, TAN Jinglei, LI Chenwei, ZHANG Hengwei
75	False Data Injection Attack Detection Method against PMU Measurements .....	ZHOU Jingyi, LI Hongjiao
84	Research on the Security Model of Multi-Authority for Attribute Encryption Based on Blockchain.....	CUI Haoyu, MA Limin, WANG Jiahui, ZHANG Wei

**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。