Scopus数据库、Abstract Journal（AJ）等收录期刊
中国科学引文数据库核心期刊（CSCD）
中国科技核心期刊（CSTPCD）

ISSN 2095-7025
CN 10-1195/TN

密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第9卷 第1期 Vol.9 No.1
2022年2月

密码学报 JOURNAL OF CRYPTOLOGIC RESEARCH 第9卷 第1期 2022年2月

ISSN 2095-7025 02>
9 772095 702220

主办
中国密码学会
北京信息科学技术研究院
中国科学技术出版社

Scopus 数据库、Abstract Journal (AJ)等收录期刊
中国科学引文数据库核心期刊(CSCD)
中国科技核心期刊(CSTPCD)

密 码 学 报
(Mima Xuebao)

第 9 卷第 1 期
2022 年 2 月

目 次

复杂语义可搜索加密研究 …… 刘晋璐, 秦 静, 汪 青, 赵 博, 张 茜, 苏 烨 (1)

发布订阅系统中的隐私保护研究综述 …… 石瑞生, 冯庆玲, 兰丽娜, 时金桥 (23)

Subterranean-SAE 算法的条件立方攻击 …… 刘 勇, 陈思维, 张莎莎, 向泽军, 曾祥勇 (45)

不可否认协议分析的扩展 ZQZ 逻辑方法 …… 韩志耕, 石青山, 杨 鹏, 陈 耿, 范远哲 (60)

面向无人机空地通信的无线信道密钥生成技术研究 …… 高玉威, 熊 俊, 郭登科, 马东堂 (76)

基于 BTM 主题模型的对称可搜索加密方案 …… 薛玉洁, 陈兰香, 穆 怡 (88)

可复用 Garbling 的效率分析及简化方案 …… 胡予濮, 刘 君, 王保仓 (106)

Android 应用内第三方支付协议的形式化分析 …… 李 晖, 范立岩, 潘雪松, 冯皓楠 (113)

轻量级迭代 MDS 矩阵的构造 …… 王 丽, 陈 媛, 王 石, 曾祥勇 (126)

TLS1.3 后量子安全迁移方案、实现和性能评测 …… 张 枫, 潘天雨, 赵运磊 (143)

MIBS-64 算法的三子集中间相遇攻击 …… 许星霖, 李艳俊, 欧海文, 孙启龙 (164)

基于中继器的无线侧信道分析方法 …… 张弘毅, 谷大武, 张 驰, 卢 岩, 原义栋 (175)

《密码学报》投稿指南 …… (封三)

Journal of Cryptologic Research Vol.9 No.1 Feb. 2022

CONTENTS

On Complex Semantic Searchable Encryptions
LIU Jin-Lu, QIN Jing, WANG Qing, ZHAO Bo, ZHANG Xi, SU Ye (1)
A Survey on Privacy Protection for Publish/Subscribe Systems
SHI Rui-Sheng, FENG Qing-Ling, LAN Li-Na, SHI Jin-Qiao (23)
Conditional Cube Attacks on Subterranean-SAE
LIU Yong, CHEN Si-Wei, ZHANG Sha-Sha, XIANG Ze-Jun, ZENG Xiang-Yong (45)
Extended ZQZ Logic Method for Analysis of Non-repudiation Protocols
HAN Zhi-Geng, SHI Qing-Shan, YANG Peng, CHEN Geng, FAN Yuan-Zhe (60)
Design of Key Generation Schemes for Aerial Communication Scene of UAVs
GAO Yu-Wei, XIONG Jun, GUO Deng-Ke, MA Dong-Tang (76)
BTM Topic Model Based Searchable Symmetric Encryption
XUE Yu-Jie, CHEN Lan-Xiang, MU Yi (88)
Efficiency Analysis and Simplified Scheme of Reusable Garbling
HU Yu-Pu, LIU Jun, WANG Bao-Cang (106)
Formal Analysis of Third-party Payment Protocol in Android Applications
LI Hui, FAN Li-Yan, PAN Xue-Song, FENG Hao-Nan (113)
Constructions of Lightweight Iterative MDS Matrix
WANG Li, CHEN Yuan, WANG Shi, ZENG Xiang-Yong (126)
Design, Implementation and Performance Evaluation of Migrating Post-quantum Safe Schemes to TLS1.3
ZHANG Feng, PAN Tian-Yu, ZHAO Yun-Lei (143)
3-subset Meet-in-the-middle Attack on Block Cipher MIBS-64
XU Xing-Lin, LI Yan-Jun, OU Hai-Wen, SUN Qi-Long (164)
Wireless Side-channel Analysis Method Based on Repeater
ZHANG Hong-Yi, GU Da-Wu, ZHANG Chi, LU Yan, YUAN Yi-Dong (175)