

Scopus数据库、Abstract Journal (AJ) 等收录期刊

ISSN 2095-7025

中国科学引文数据库核心期刊 (CSCD)

CN 10-1195/TN

中国科技核心期刊 (CSTPCD)

密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

# 密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第10卷 第2期 Vol.10 No.2

2023年4月

第十卷

第二期

二〇二三年四月



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 10 卷第 2 期  
2023 年 4 月

## 目 次

后量子密码迁移趋势下应用于区块链的公钥密码安全.....	
.....胡 希, 向 宏, 丁津泰, 梁 蓓, 夏鲁宁, 向 涛	(219)
GMM 型高维输出严格几乎最优弹性密码函数构造.....	张卫国, 胡姚达, 董雪雯 (246)
基于 SM2 数字签名算法的可否认环签名.....	包子健, 何德彪, 彭 聪, 罗 敏, 黄欣沂 (264)
两方参与的隐私保护岭回归方案与应用.....	吕 由, 吴文渊 (276)
一种基于复合域的国密 SM4 算法快速软件实现方法.....	
.....陈 晨, 郭 华, 王 闯, 刘源灏, 刘建伟	(289)
基于观察等价性的协议猜测攻击形式化检测方法.....	苗旭阳, 顾纯祥, 陆思奇 (306)
半自适应性安全的双方可否认属性加密方案.....	王 蒙, 杨 波, 梁旭东 (320)
FixBranchPHT: 一种针对 BranchScope 攻击的软件防御方法.....	李永波, 唐 明 (342)
分布拟合技术及其在密码函数构造中的应用.....	朱率率, 韩益亮 (360)
KATAN 族密码的立方攻击和积分攻击.....	张贵显, 胡 斌 (372)
一种抗差分计算分析的白盒 SM4 方案.....	原梓清, 陈 杰 (386)
基于区块链的远程医疗认证协议.....	邵晓伟, 郭亚军 (397)
聚合认证加密方案.....	刘 刚, 王 鹏, 叶顶锋 (415)
针对 RIAC 同态加密算法的攻击.....	刘易简, 石 冰 (433)
《密码学报》投稿指南.....	(封三)

CONTENTS

Security of Public Key Cryptography in Blockchain under the Trend on Post-quantum Cryptography  
Migration.....HU Xi, XIANG Hong, DING Jin-Tai, LIANG Bei, XIA Lu-Ning, XIANG Tao (219)

Constructions of GMM Type Strictly almost Optimal Resilient Vectorial Boolean Functions with High-  
dimension..... ZHANG Wei-Guo, HU Yao-Da, DONG Xue-Wen (246)

Deniable Ring Signature Scheme Based on SM2 Digital Signature Algorithm.....  
..... BAO Zi-Jian, HE De-Biao, PENG Cong, LUO Min, HUANG Xin-Yi (264)

Two-party Privacy-preserving Ridge Regression Scheme with Applications.....  
.....LYU You, WU Wen-Yuan (276)

A Fast Software Implementation of SM4 Based on Composite Fields.....  
.....CHEN Chen, GUO Hua, WANG Chuang, LIU Yuan-Hao, LIU Jian-Wei (289)

Formal Analysis Method of Protocol Guessing Attack Based on Observation Equivalence.....  
..... MIAO Xu-Yang, GU Chun-Xiang, LU Si-Qi (306)

Semi-adaptive Secure Bi-deniable Attribute Based Encryption.....  
.....WANG Meng, YANG Bo, LIANG Xu-Dong (320)

FixBranchPHT: A Software Defense Against BranchScope Attacks.....LI Yong-Bo, TANG Ming (342)

Distribution Fitting and Its Applications in Construction of Cryptographic Functions.....  
.....ZHU Shuai-Shuai, HAN Yi-Liang (360)

Cube Attacks and Integral Attacks on KATAN Family Ciphers.....ZHANG Gui-Xian, HU Bin (372)

A White-box SM4 Scheme Against Differential Computation Analysis.....YUAN Zi-Qing, CHEN Jie (386)

A Blockchain-based Authentication Protocol for Telemedicine.....SHAO Xiao-Wei, GUO Ya-Jun (397)

Design of New Aggregate Authenticated Encryption Schemes.....  
..... LIU Gang, WANG Peng, YE Ding-Feng (415)

An Attack on RIAC Homomorphic Encryption Algorithm.....LIU Yi-Jian, SHI Bing (433)

## 密码学报

Mima Xuebao  
(双月刊, 2014年创刊)  
第10卷 第2期 2023年4月

## Journal of Cryptologic Research (Bimonthly)

(Started in 2014)  
Vol.10 No.2 Apr. 2023

编辑 《密码学报》编辑部  
(北京市海淀区丰德中路9号 邮编100878)  
电话: 86-10-82789618  
传真: 86-10-82789618  
E-mail: [jcr@cacnet.org.cn](mailto:jcr@cacnet.org.cn)  
<http://www.jcr.cacnet.org.cn>

主编 冯登国  
主办单位 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

主管单位 中国科学技术协会  
出版 中国科学技术出版社  
印刷 北京科信印刷有限公司  
发行 《密码学报》编辑部

Edited by Editorial Board of Journal of Cryptologic Research  
(No. 9, Fengde Middle Road, Haidian District,  
Beijing 100878, P. R. China)  
Tel: 86-10-82789618  
Fax: 86-10-82789618  
E-mail: [jcr@cacnet.org.cn](mailto:jcr@cacnet.org.cn)  
<http://www.jcr.cacnet.org.cn>

Editor-in-Chief FENG Deng-Guo  
Sponsored by Chinese Association for Cryptologic  
Research (CACR) and Beijing Academy of Information  
Science & Technology (BAIST) and China Science and  
Technology Press  
Supervised by China Association for Science and  
Technology (CAST)  
Published by China Science and Technology Press  
Printed by Beijing Kexin Printing Co., Ltd.

ISSN 2095-7025  
CN 10-1195/TN

邮发代号: 80-918  
公开发行

定价: 60.00元

