

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

第9卷 第4期 Vol.9 No.4

2022年8月

密码学报
JOURNAL OF CRYPTOLOGIC RESEARCH

第九卷

第四期

二〇二二年八月



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 9 卷第 4 期
2022 年 8 月

目 次

可否认加密技术与研究进展	郝学轩, 曹艳梅, 张方国, 陈晓峰	(579)
区块链交易内容隐私保护技术研究综述	姚 爽, 张大伟, 李 勇, 王 伟	(596)
字符串匹配的保密计算	张凯鑫, 杨 晨, 李顺东	(619)
轻量级密码 TWINE-128 的量子密码分析	李艳俊, 易子晗, 汪 振, 刘 健	(633)
一类新的代数免疫度最优的奇变元旋转对称布尔函数的构造	王 勇, 郑 东, 赵庆兰, 李路阳, 师 宇	(644)
基于通用计算平台 SM4-CTR 算法并行实现与优化	李晓东, 胡一鸣, 池亚平, 钱 榕, 张健毅	(663)
Jacobi 四次曲线的快速差分加法公式	吴宏锋, 宋贞贞	(677)
基于双线性配对的适配器签名方案	王子瑞, 张 驰, 魏凌波	(686)
Alzette 的安全性分析	许 峥, 李永强, 王明生	(698)
SNPAKA: 基于 SNTRUP 的双向认证密钥协商协议 FPGA 实现	杨亚涛, 王在舟, 曾 萍, 肖 嵩	(709)
基于模格 MLWR 的密钥封装方案优化与高效实现	郝世迪, 孙冬旎, 梁志闯, 郑婕妤, 沈诗羽, 赵运磊	(725)
基于多项式插值的多等级秘密共享方案	张 剑, 林昌露, 黄可可, 刘亚丽	(743)
AES 和 PRINCE 的 6 轮混合差分攻击	谭 林, 闫雪萍, 戚文峰	(755)
基于格的截获取签名方案	赵 勇, 杨少军, 张福泰, 黄欣沂	(767)
学术评论		(封三)

CONTENTS

A Survey on Deniable Encryption
.....HAO Xue-Xuan, CAO Yan-Mei, ZHANG Fang-Guo, CHEN Xiao-Feng (579)

A Survey on Privacy Protection of Transaction Content in Blockchain
.....YAO Shuang, ZHANG Da-Wei, LI Yong, WANG Wei (596)

Privacy Preserving String MatchingZHANG Kai-Xin, YANG Chen, LI Shun-Dong (619)

Quantum Cryptanalysis of Lightweight Cipher TWINE-128
.....LI Yan-Jun, YI Zi-Han, WANG Zhen, LIU Jian (633)

A New Construction of Odd-variable Rotation Symmetric Boolean Function with Optimal Algebraic Immunity WANG Yong, ZHENG Dong, ZHAO Qing-Lan, LI Lu-Yang, SHI Yu (644)

Parallel Implementation and Optimization of SM4-CTR Algorithm Based on General Computing Platform LI Xiao-Dong, HU Yi-Ming, CHI Ya-Ping, QIAN Rong, ZHANG Jian-Yi (663)

Efficient Differential Addition Formulae on Jacobi Quartic Curves
..... WU Hong-Feng, SONG Zhen-Zhen (677)

Adaptor Signatures from Bilinear PairingsWANG Zi-Rui, ZHANG Chi, WEI Ling-Bo (686)

Security Analysis of Alzette XU Zheng, LI Yong-Qiang, WANG Ming-Sheng (698)

SNPAKA: Authentication Key Agreement Protocol Implementation on FPGA Based on SNTRUP
..... YANG Ya-Tao, WANG Zai-Zhou, ZENG Ping, XIAO Song (709)

Optimization and Efficient Implementation of MLWR-based Key Encapsulation Mechanism
.. HAO Shi-Di, SUN Dong-Ni, LIANG Zhi-Chuang, ZHENG Jie-Yu, SHEN Shi-Yu, ZHAO Yun-Lei (725)

Polynomial Interpolation Based Hierarchical Secret Sharing Schemes.....
.....ZHANG Jian, LIN Chang-Lu, HUANG Ke-Ke, LIU Ya-Li (743)

Mixture Differential Attacks on 6 Rounds of AES and PRINCE
..... TAN Lin, YAN Xue-Ping, QI Wen-Feng (755)

A Lattice-based Extraction Signature Scheme
.....ZHAO Yong, YANG Shao-Jun, ZHANG Fu-Tai, HUANG Xin-Yi (767)