

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10卷 第1期 Vol.10 No.1

2023年2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 1 期
2023 年 2 月

目 次

基于格的数字签名及其聚合类变体的综述	陈新坚, 黄建业, 黄 琼	(1)
NIST 抗量子密码标准候选算法中基于格的公钥加密与密钥封装机制介绍
.....	向斌武, 张 江, 邓 毅	(20)
基于杂凑函数 SM3 的后量子数字签名
.....	孙思维, 刘田雨, 关 志, 何逸飞, 荆继武, 胡 磊, 张振峰, 闫海伦	(46)
基于 BLISS 签名的不经意电子信封	杜育松, 庄少华, 伍春晖	(61)
基于标记配对相干态光源的实用化诱骗态量子随机数发生器
.....	李元昊, 费洋洋, 王卫龙, 孟祥栋, 王 洪, 段乾恒, 马 智	(73)
基于身份体制下多密文等值测试加密方案的一般性构造
.....	花锦国, 张 磊, 杨 波, 陈立全, 吴 戈	(87)
分布式多重集众数及重数的保密计算	家珠亮, 赵雪玲, 李顺东	(102)
针对分组密码工作模式的基于持久性故障的碰撞攻击	臧首金, 郑世慧	(118)
云存储中高效可追踪可撤销的属性基加密方案	郭丽峰, 邢晓敏, 郭 慧	(131)
基于 Feistel-NFSR 结构的 16 比特 S 盒设计方法	武小年, 豆道饶, 韦永壮, 张润莲, 李灵琛	(146)
实现高阶安全的一阶掩码与乱序方法研究	肖 冲, 唐 明, 严 飞	(155)
对基于深度学习的密钥恢复攻击的分析与改进	陈 怡, 申焱天, 于红波	(168)
基于 MILP 的相关密钥差分分析安全评估算法改进	周春宁, 张文涛, 曹文芹	(181)
通用可重组安全的多方求解 Top- k 协议设计
.....	栾明学, 张秉晟, 杨国正, 臧 铨, 陈嘉俊, 李泽昊, 吴泽成, 任 奎	(195)
一种基于乘法掩码的 AES 防护方案	郭 箬, 杨正文, 张效林, 卢 岩, 原义栋	(209)

CONTENTS

An Overview of Lattice-based Signature and Its Variants Supporting Aggregation
..... CHEN Xin-Jian, HUANG Jian-Ye, HUANG Qiong (1)

An Overview on Lattice-based Public Key Encryption and Key Encapsulation Mechanism in Candidate
Schemes for Post Quantum Cryptography Standard of NIST.....
..... XIANG Bin-Wu, ZHANG Jiang, DENG Yi (20)

SM3-based Post-quantum Digital Signature Schemes
..... SUN Si-Wei, LIU Tian-Yu, GUAN Zhi, HE Yi-Fei, JING Ji-Wu, HU Lei, ZHANG Zhen-Feng, YAN Hai-Lun (46)

An Oblivious Envelope Based on Bimodal Lattice Signature Scheme
..... DU Yu-Song, ZHUANG Shao-Hua, WU Chun-Hui (61)

Practical Decoy-state Quantum Random Number Generator with Heralded Pair-coherent Source
· LI Yuan-Hao, FEI Yang-Yang, WANG Wei-Long, MENG Xiang-Dong, WANG Hong, DUAN Qian-Heng, MA Zhi (73)

General Construction of Identity-based Encryption with Multi-ciphertext Equality Test.....
..... HUA Jin-Guo, ZHANG Lei, YANG Bo, CHEN Li-Quan, WU Ge (87)

Secure Distributed Multiset's Mode and Multiplicity Computation.....
..... JIA Zhu-Liang, ZHAO Xue-Ling, LI Shun-Dong (102)

Persistent Fault-based Collision Attack on Block Cipher Mode ZANG Shou-Jin, ZHENG Shi-Hui (118)

An Efficient Traceable and Revocable Attribute-based Encryption Scheme in Cloud Storage.....
..... GUO Li-Feng, XING Xiao-Min, GUO Hui (131)

A 16-bit S-box Design Method Based on Feistel-NFSR Structure.....
..... WU Xiao-Nian, DOU Dao-Rao, WEI Yong-Zhuang, ZHANG Run-Lian, LI Ling-Chen (146)

First Order Masking Combined with Shuffling to Reach Higher-order Security.....
..... XIAO Chong, TANG Ming, YAN Fei (155)

Analysis and Improvements of Deep Learning-based Key Recovery Attack
..... CHEN Yi, SHEN Yan-Tian, YU Hong-Bo (168)

Improvement of MILP-aided Security Evaluation Algorithm of Related-key Differential Cryptanalysis ·
..... ZHOU Chun-Ning, ZHANG Wen-Tao, CAO Wen-Qin (181)

Universally Composable Secure Multi-party Computation of the Top- k Element..... LUAN Ming-Xue,
ZHANG Bing-Sheng, YANG Guo-Zheng, ZANG Cheng, CHEN Jia-Jun, LI Ze-Hao, WU Ze-Cheng, REN Kui (195)

A Side-channel Countermeasure for AES Based on Multiplication Mask.....
..... GUO Zheng, YANG Zheng-Wen, ZHANG Xiao-Lin, LU Yan, YUAN Yi-Dong (209)