

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5卷 第1期 Vol.5 No.1

2018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

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5卷第1期
2018年2月

目次

针对诱骗态量子密钥分发方案的 PNS 攻击研究	李宏欣, 迟洋广, 韩宇, 闫宝, 王伟 (1)
一种基于格签名算法的数字证书方案	李子臣, 梁澜, 孙亚飞 (13)
基于LWE的全同态身份广播加密方案	冯翰文, 刘建伟, 伍前红 (21)
基于区块链的密钥更新和可信定位系统	李大伟, 刘建伟, 关振宇, 秦煜瑶, 伍前红 (35)
弱半 bent 正交序列集的构造	夏婷婷, 孙玉娟, 解春雷 (43)
无双线性对的基于证书多域条件代理重加密方案	徐洁如, 陈克非, 沈忠华, 徐晓栋 (55)



认证加密算法专栏	专栏责任编辑: 胡磊
认证加密算法专栏序言	胡磊 (68)
认证加密算法研究进展	吴文玲 (70)
认证加密算法 FASER 的安全性分析	冯秀涛, 张凡 (83)
Grain-128a 认证机制的安全性分析	王鹏, 郑凯燕 (94)
征稿启事	(封三)

CONTENTS

Analysis on Photon-number-splitting Attack Against Decoy-state Quantum Key Distribution Schemes ···
····· LI Hong-Xin, CHI Yang-Guang, HAN Yu, YAN Bao, WANG Wei (1)

Digital Certificate Scheme Based on Lattice Signature Algorithm ···········
····· LI Zi-Chen, LIANG Lan, SUN Ya-Fei (13)

Identity-based Broadcast Fully Homomorphic Encryption Scheme from LWE ·········
····· FENG Han-Wen, LIU Jian-Wei, WU Qian-Hong (21)

Key Update and Trusted Positioning System Based on Blockchain··········
····· LI Da-Wei, LIU Jian-Wei, GUAN Zhen-Yu, QIN Yu-Yao, WU Qian-Hong (35)

Constructions of Weakly Semi-bent Orthogonal Sequences Sets ···········
····· XIA Ting-Ting, SUN Yu-Juan, XIE Chun-Lei (43)

Pairing-free Certificate-based Multi-domain Conditional Proxy Re-encryption Scheme ·······
····· XU Jie-Ru, CHEN Ke-Fei, SHEN Zhong-Hua, XU Xiao-Dong (55)



Special Column: Authenticated Encryption Algorithms **HU Lei**

Preface ··········· HU Lei (68)

Research Advances on Authenticated Encryption Algorithms ··········· WU Wen-Ling (70)

Research on Cryptanalysis on Authenticated Cipher FASER··········
····· FENG Xiu-Tao, ZHANG Fan (83)

Security Analysis of Authentication Mechanism in Grain-128a··········
····· WANG Peng, ZHENG Kai-Yan (94)