ISSN 2095-7025
CN 10-1195/TN

密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第3卷 第5期 Vol.3 No.5
2016年10月

密码学报 JOURNAL OF CRYPTOLOGIC RESEARCH 第3卷 第5期 2016年10月

ISSN 2095-7025 10>
9 772095 702169

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

密 码 学 报　　第 3 卷第 5 期
(Mima Xuebao)　　2016 年 10 月

目 次

格上可编程杂凑函数的新构造……张　江 (419)

无线通信设备的射频指纹提取与识别方法 …… 俞佳宝, 胡爱群, 朱长明, 彭林宁, 姜　禹 (433)

CRT-RSA 算法的选择明文攻击 ……李增局, 彭　乾, 史汝辉, 李　超, 马志鹏, 李海滨 (447)

输出反馈模式在量子随机数提取器中的应用 ……刘翼鹏, 郭建胜, 崔竞一 (462)

隐藏树型访问结构的属性加密方案……李　新, 彭长根, 牛翠翠 (471)

全同态加密具体安全参数分析……陈智罡, 石亚峰, 宋新霞 (480)

对约减轮数 Skein-1024 的 Boomerang 区分攻击 ……吴广辉, 于红波, 郝泳霖 (492)

信息集攻击算法的改进 ……李梦东, 蔡坤锦, 邵玉芳 (505)

REESSE3+算法抵抗差分攻击的分析 ……董大强, 殷新春, 苏盛辉 (516)

《密码学报》投稿指南 …… (封三)