通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

赵新杰,郭世泽,王 韬,刘会英.针对AES和CLEFIA的改进Cache踪迹驱动攻击[J].通信学报,2011,(8):101~110

针对AES和CLEFIA的改进Cache踪迹驱动攻击

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
赵新杰	
郭世泽	
王 韬	
刘会英	

摘要点击次数： 289

全文下载次数： 125

中文摘要：

通过分析“Cache失效”踪迹信息和S盒在Cache中不对齐分布特性，提出了一种改进的AES和CLEFIA踪迹驱动攻击方法。现有攻击大都假定S盒在Cache中对齐分布，针对AES和CLEFIA的第一轮踪迹驱动攻击均不能在有限搜索复杂度内获取第一轮扩展密钥。研究表明，在大多数情况下，S盒在Cache中的分布是不对齐的，通过采集加密中的“Cache失效”踪迹信息，200和50个样本分别经AES第一轮和最后一轮分析可将128bit AES主密钥搜索空间降低到216和1，80个样本经CLEFIA第一轮分析可将12

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭

版权所有：通信学报
地址：北京东城区广渠门内大街80号通正国际大厦6层602室 电话：010-67110006-869/878/881 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司