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,王 韬,郑媛媛.针对SMS4密码算法的Cache计时攻击[J].通信学报,2010,(6):89~98

针对SMS4密码算法的Cache计时攻击

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
赵新杰	
王 韬	
郑媛媛	

中文摘要：

分别提出并讨论了针对SMS4加密前4轮和最后4轮的访问驱动Cache计时分析方法，设计间谍进程在不干扰SMS4加密前提下采集加密前4轮和最后4轮查表不可能访问Cache组集合信息并转化为索引值，然后结合明文或密文对密钥的不可能值进行排除分析，最终恢复SMS4初始密钥。实验结果表明多进程共享Cache存储器空间方式和SMS4查找表结构决定其易遭受Cache计时攻击威胁，前4轮和最后4轮攻击均在80个样本左右恢复128bit SMS4完整密钥，应采取一定的措施防御该类攻击。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭