计算机工程　2010 36 (1): 189-190,200　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

安全技术

AES差分故障攻击的建模与分析

刘上力，赵劲强，聂勤务

(湖南科技大学网络信息中心，湘潭 411201)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　研究高级加密标准(AES)密码算法对差分故障攻击的安全性。攻击采用针对密钥扩展算法的单字节随机故障模型，通过对比正确和错误密文的差异恢复种子密钥。该攻击方法理论上仅需104个错误密文和2个末轮子密钥字节的穷举搜索就可完全恢复AES的128比特种子密钥。故障位置的不均匀分布使实际攻击所需错误密文数与理论值略有不同。

关键词　高级加密标准；差分故障攻击；故障诱导；故障模型

分类号　TP309.7

DOI:

通讯作者:

作者个人主页: 刘上力;赵劲强;聂勤务