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

王小娟1,郭世泽2,赵新杰2,3,宋梅1,张帆4.基于功耗预处理优化的LED密码模板攻击研究[J].通信学报,2014,(3):157~167

基于功耗预处理优化的LED密码模板攻击研究

Research of power preprocessing optimization-basedtemplate attack on LED

投稿时间： 2012-11-10

DOI：10.3969/j.issn.1000-436x.2014.3.018

中文关键词：功耗预处理 数据对齐 数据切割 有效点选取 模板攻击 LED

英文关键词:power preprocessing data alignment data cutting interesting points selection template attack LED

基金项目:国家自然科学基金资助项目(61173191, 61272491, 61309021)

作者	单位
王小娟1，郭世泽2，赵新杰2,3，宋梅1，张帆4	1. 北京邮电大学 电子工程学院，北京 100876；2. 北方电子设备研究所，北京100083； 3. 军械工程学院 信息工程系，河北 石 050003；4. 康涅狄格大学 计算机科学与工程系，康涅狄格州 斯托斯 06269

中文摘要:

对CHES 2011会议提出的轻量级分组密码LED抗功耗模板攻击能力进行了评估，从功耗曲线预处理优化的角度对模板攻击提出了改进：利用功耗曲线频域上的相位相关性计算偏量，消除了模板构建过程中的数据干扰；利用明文片段对功耗曲线聚类划分的特征差异，提出了一种基于类间距离的特征提取方法，可实现不同泄露点的功耗数据自动切割；利用和噪声信息评估模板区分度，提出了一种基于聚类有效度的动态选点策略，提高了旁路信息利用率。实验结果表明：数据对齐和切割提高了匹配度的区分效果，降低了模板构建和所需功耗曲线数量；聚类有效度选点策略与现有策略相比，攻击数据复杂度低，2条功耗曲线即可使成功概率收敛于1。

英文摘要:

The security of LED, a lightweight block cipher proposed in CHES 2011, was evaluated by the template attack (TA). Several improvements of TA from the perspective of the preprocessing optimization was proposed. Firstly, the noise offset was calculated by using the phase-only correlation factor in the frequency view of the power trace to eliminate the data interference in the tem building phase. Secondly, a novel character extracting method was proposed based on calculating the cross-cluster offset of different clusters classified by the plaintexts to cut the different leakage from the power traces automatically. Thirdly, a dynamic effective power points choosing strategy was proposed by utilizing the mean value and the noises of the of power traces to evaluate the differences between different templates and improve the utilization of side channel information. Experiment results demonstrate that the proposed techniques of data alignment and automatically c cutting enlarge the differences of templates and reduce the number of the required power trace in both the template building and attacking phase. The proposed effective power points choosing str reduces the data complexity of the attack and only two power traces are required to launch the attack with the success rate of 100%.

查看全文 查看/发表评论 下载PDF阅读器

关闭