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

冀可可1,王韬1,郭世泽2,赵新杰1,刘会英1.基于汉明重的LED代数旁路攻击研究[J].通信学报,2013,(7):134~142

基于汉明重的LED代数旁路攻击研究

Research of Hamming weight-based algebraicside-channel attack on LED

投稿时间： 2012-01-09

DOI：10.3969/j.issn.1000-436x.2013.07.015

中文关键词：汉明重 LED 代数旁路攻击 可满足性 伪布尔优化 线性编程

英文关键词:Hamming weight LED ASCA satisfiability pseudo-Boolean optimization linear programming

基金项目:国家自然科学基金资助项目(61173191)

作者	单位
冀可可1，王韬1，郭世泽2，赵新杰1，刘会英1	1. 军械工程学院 信息工程系,河北 石家庄 050003；2. 北方电子设备研究所，北京 100083

摘要点击次数: **280**

全文下载次数: **188**

中文摘要:

对CHES 2011会议提出的LED轻型分组密码抗代数旁路攻击能力进行了评估。给出了密码算法代数旁路攻击模型及LED密码代数方程表示方法；利用示波器采集微控制器ATMEGA324P上的LED实现功耗泄露，选取功耗特征较为明显的部分泄露点，基于Pearson相关系数方法推断加密中间状态汉明重；分别基于可满足性问题、伪布尔优化问题、线性编程问题给出了LED密码和汉明重泄露的3种代数方程表示方法；使用CryptoMinisat和SCIP 2种解析器对建立的代数方程求解恢复密钥，在已知明文、未知明密文、容错等场景下进行了大量的攻击实验。结果表明，LED易遭受代数旁路攻击，一条功耗曲线的1轮汉明重泄露分析即可恢复64 bit完整密钥。

英文摘要:

The security of LED against the algebraic side-channel attack (ASCA)was evaluated, which is a lightweight block cipher proposed in CHES 2011. Firstly, the attack model of ASCA was analyzed, and then the design and algebraic representations of LED were described. Secondly, the power leakages of LED on ATMEGA324P microcontroller were measured by a digital oscilloscope; some leakage points with obvious power patterns were chosen as the targeted points and used to deduce the Hamming weight via computing the Pearson correlation factor; satisfiability-based, Pseudo-Boolean optimization-based, linear programming-based methods were used to representing Hamming weights with algebraic equations. Finally, the CryptoMinisat and the SCIP solver were applied to solve for the key and many attacks are conducted under different scenarios. Experiment results demonstrate that LED is vulnerable to ASCA, full 64 bit master key can be derived via analyzing the HW leakages of the first round in LED.

查看全文 查看/发表评论 下载PDF阅读器

关闭