

周报

2025-05-12

大纲

1. 研究方向与进展

2. 实验环境搭建

3. 实验结果与分析

第四篇论文研究方向

研究聚焦

本周确定了第四篇论文的研究方向，聚焦于故障攻击防护技术研究。通过对主要密码学会议和期刊的文献统计，发现 72 篇关于故障攻击的论文，其中 **12 篇专注于防护技术**。本论文将从以往的性能优化转向 **安全实现**，重点关注侧信道攻击与故障注入攻击的防护机制，尤其针对后量子密码算法。研究目标为开发高效、可验证且适用于资源受限环境的防护方法。

能有机合成硕士大论文不？

大论文 **软硬件优化实现包含抗故障攻击的安全实现**，可以和第二篇论文软件实现工作结合，实现更快更安全。

故障注入实验环境

环境构建. 构建了基于电压毛刺的故障注入实验环境, 包括目标设备 (STM32F303 芯片)、电压故障注入设备和示波器。实验流程为: 目标设备发送触发信号, 电压故障设备**注入电压故障**, 示波器捕获波形, 主机对比密文以判定注入效果。



图 1: 故障注入实验装置。左侧为目标设备 (STM32F303 芯片), 右上方为电压故障注入设备, 右下方为捕获波形的示波器。

注入点分析

注入点分析

通过捕获芯片电源与 AES 加密触发信号，确定第 9 轮加密的**精确时间窗口**（约 4.405ms），为故障注入提供了依据。

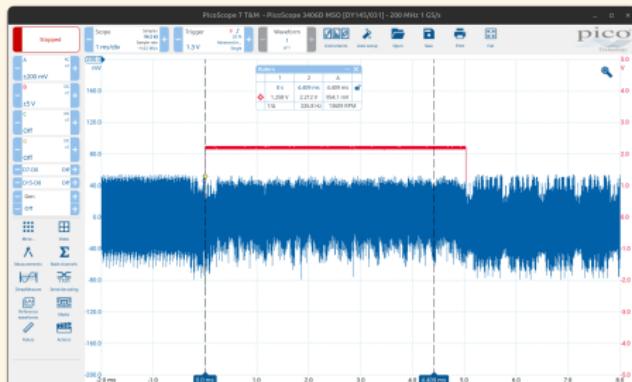


图 2：故障注入点分析的捕获波形。A 通道显示芯片工作电源，B 通道显示 AES 加密触发信号。

实验结果

初步测试

在 AES 加密过程中，尝试了超过 50 次电压故障注入，未观察到错误的密文输出。随后调整电压毛刺的注入时间 x 和持续时间 y ，在约 3000 次注入后，成功观察到一条错误的密文输出。而在[公众号](#)参考参数下，注入 3000 次未见异常。阅读 CHES 论文 [BFP19]，以提高注入成功率。

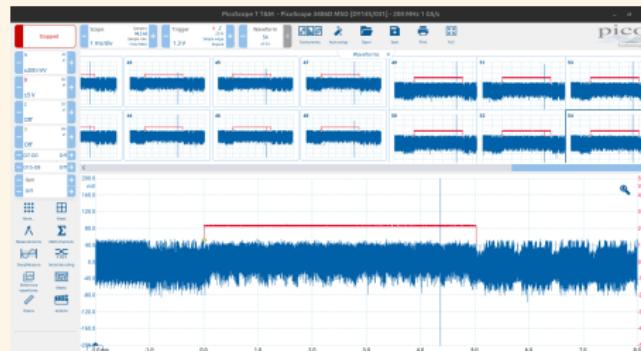


图 3: AES 加密过程中的故障注入攻击波形。蓝线急剧下降表示故障注入过程中的电压波动。

老师评语

故障攻击这些实验都是自己做出来的 ??

是自己做的，其中大部分是实验室设备，电压毛刺是淘宝买的。

下周计划

1) 优化故障注入参数，提升**攻击成功率**，并尝试通过差分故障分析提取密钥。2) 跑通攻击流程后，阅读**抗故障攻击的实现**文献。

参考文献

-  Claudio Bozzato, Riccardo Focardi, and Francesco Palmarini.
Shaping the glitch: Optimizing voltage fault injection attacks.
IACR TCHES, 2019(2):199–224, 2019.