

周报 向嘉豪 (2025 年 5 月 12 日)

摘要： 本周主要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**。构建了基于**电压毛刺**的故障注入实验环境，并进行了初步测试。在调整注入参数后，**成功观察到一个错误的密文输出**。下周将继续**优化故障注入参数**，提高**攻击成功率**，并尝试通过**差分故障分析**提取密钥。

下周计划： 1) 提高故障注入成功率 2) 差分故障分析出密钥

1 第四篇论文

基于对主要密码学会议和期刊 (ASIACRYPT 1990-2024, CRYPTO 1981-2024, EUROCRYPT 1982-2024、TCIES 2018-2024、ToSC 2016-2024) 的文献统计分析，我们发现了**72 篇关于故障攻击 (Fault Attack) 的论文**，其中有**12 篇 (约 16.7%) 专注于故障攻击防护技术**。在前三篇论文中，我们主要关注密码学算法的**性能优化**，而在第四篇论文中，我们将转向**安全实现**，尤其是针对**侧信道攻击**和**故障注入攻击**的防护机制。计划深入研究针对现代密码系统（特别是**后量子密码算法**）的故障攻击防护技术。**研究将聚焦于开发可验证、高效且适用于资源受限环境的故障攻击防护方法**。为此需要搭建一个**故障注入实验环境**。

1.1 实验环境

故障注入攻击的工作流程可概括为：目标设备发送**触发信号**至电压故障设备，电压故障设备向目标设备**注入电压故障**，同时示波器**捕获波形**，主机接收密文并与预期密文进行比较，从而确定故障注入是否成功。启发于老师转发的**PADNA2025**，我们建立了完整的故障注入实验环境（基于**电压毛刺**）。该环境由三个主要组件构成：目标设备（STM32F303 芯片）、电压故障注入设备和用于捕获波形的示波器。实验设置如下：

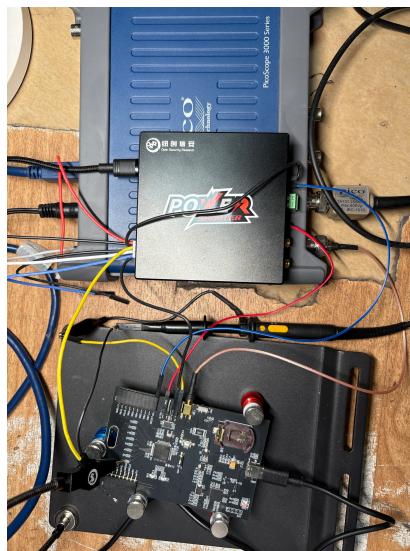


图 1：故障注入实验装置。左侧为目标设备（STM32F303 芯片），右上方为电压故障注入设备，右下方为捕获波形的示波器。

首先，我们识别了**潜在的故障注入点**。通过捕获芯片工作电源的 A 通道和 AES 加密触发信号

的 B 通道，我们观察到触发信号后第 9 轮加密的运行时间接近 4.405ms。这为故障注入提供了精确的时间窗口，如图2所示。

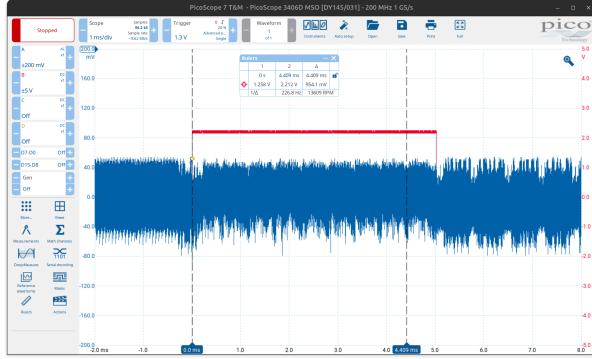


图 2：故障注入点分析的捕获波形。A 通道显示芯片工作电源，B 通道显示 AES 加密触发信号。

在攻击过程中，我们采用了电压故障攻击方法。我们在 AES 加密过程中尝试了超过 50 次电压故障注入，特别针对接近第 9 轮的时间段。如图3所示，蓝线急剧下降表示故障注入过程中的电压波动。尽管进行了多次尝试，我们未能观察到任何错误的密文输出，表明故障注入未能成功。

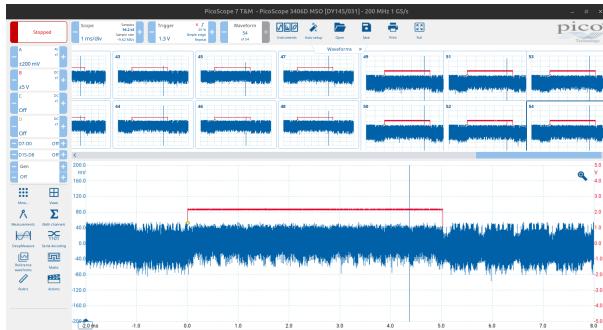


图 3：AES 加密过程中的故障注入攻击波形。蓝线急剧下降表示故障注入过程中的电压波动。

为此我们对电压毛刺的注入时间 x 和持续时间 y 进行调整，在大约 3000 次注入后，我们观察到了一条错误的密文输出，而在 PADNA2025 公众号上提供的 (x, y) 参数下，我们注入 3000 次（约 1 个小时）未观察到任何错误的密文输出。为提高注入的成功率，我们正在阅读 [BFP19]。

参考文献

- [BFP19] Claudio Bozzato, Riccardo Focardi, and Francesco Palmarini. Shaping the glitch: Optimizing voltage fault injection attacks. *IACR TCHES*, 2019(2):199–224, 2019.