周报

2025 年 5 月 27 日

大纲

1. 防护机制分类调研

2. 故障注入效率问题分析

防护策略分类框架

系统性分类结果

基于对近年来 CHES 会议相关研究的深入分析，构建了故障攻击防护机制的系统性分类框架。根据防护策略的核心方法论差异，现有技术可归纳为三大类别：理论证明类防护、冗余校验类防护和混合类防护。以 [Gen23, DOT24, THN+24] 等近期 TCHES 文献为基础进行分析。

理论证明类防护

基于严格的数学理论构建可证明安全的防护机制。Asiacrypt 2009 的代表性工作 [CM09] 在随机预言模型下证明了 PSS 编码机制对随机故障攻击的可证明安全性，为基于编码的防护策略提供了重要的理论支撑。

防护机制技术特征分析

冗余校验类防护

通过引入冗余机制和状态校验来检测和缓解故障影响。[Gen23] 提出的基于中间 WOTS$^+$ 缓存的对策通过缓存关键中间状态实现故障检测时的安全回滚，有效控制了故障传播范围。[DOT24] 的 StaTI 方案基于阈值实现和线性编码技术，在非组合攻击场景下同时防护侧信道和故障攻击。

混合类防护

结合软硬件多层防护机制构建分层防护体系（同时具有理论分析）。TCHES 2024 的 [THN$^+$24] 形式化的 k 故障抗性分割概念通过可证明的安全保证减少硬件攻击面，并在此基础上引入软件防护层，实现了软硬件协同的鲁棒性故障防护解决方案。

实验问题诊断

成功率过低问题

尽管前期实验成功观察到错误密文输出，但电压毛刺故障注入的**成功率仅为 0.1% 且表现不稳定**，显著低于 TCHES[BFP19] 的 STM32F3xx 平台 4% 成功率。这一差异表明当前攻击流程存在系统性问题。

形式化攻击模型

建立了严格的理论分析框架。对手 $\mathcal{A}$ 控制故障注入预言机 $\mathcal{F}(t, \sigma, \phi, \alpha)$，参数化为时序 t、目标计算域 σ、注入机制 ϕ 和强度 α。故障预言机以概率 $P_{\text{fault}}(t, \sigma, \phi, \alpha)$ 诱导状态转换。

参数优化策略失效分析

优化尝试结果

尝试应用参数优化策略 [BFP19] 未能有效改善注入效率，识别出现有方法在当前实验环境中的适用性限制。实现了半自动监督搜索策略：通过随机生成并插值描述候选毛刺波形的 $(x, y) \sim (t, \alpha)$ 点集合，迭代选择参数区间内的随机样本。σ 是软件指令计算，ϕ 是电压故障注入机制。

失效原因分析

该策略在 STM32F303 实验中未达预期效果，经过约 100 次迭代仍未发现有效参数组合。由于监督搜索阶段的失效，依赖其输出作为初始种群基础的遗传算法全自动优化策略亦无法有效实施。

固件重写诊断

实验结果表明，现有参数优化方法在当前实验环境中存在适用性限制，需要深入分析故障注入失效的根本原因。计划通过重写 F303 固件暴露注入时的内部状态，进一步诊断故障注入成功率过低的技术问题。

老师评语

加快推进

下周计划

1) 重写 STM32F303 固件暴露故障注入时的内部状态，诊断注入失效根本原因
2) 完善故障攻击防护机制基础理论

参考文献 I


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


Jean-Sébastien Coron and Avradip Mandal.
PSS is secure against random fault attacks.
In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 653–666. Springer, Berlin, Heidelberg, December 2009.


Siemen Dhooghe, Artemii Ovchinnikov, and Dilara Toprakhisar.
StaTI: Protecting against fault attacks using stable threshold implementations.
IACR TCHES, 2024(1):229–263, 2024.

参考文献 II


Aymeric Genêt.
On protecting SPHINCS+ against fault attacks.
IACR TCHES, 2023(2):80–114, 2023.


Simon Tollec, Vedad Hadzic, Pascal Nasahl, Mihail Asavoae, Roderick Bloem, Damien Couroussé, Karine Heydemann, Mathieu Jan, and Stefan Mangard.
Fault-resistant partitioning of secure CPUs for system co-verification against faults.
IACR TCHES, 2024(4):179–204, 2024.