# 周报 向嘉豪 (2025 年 6 月 16 日)

**摘要：** 本周我们基于第四篇论文的研究进展，深入分析了故障注入攻击防护方向。通过对比分析相关工作的研究现状，我们识别了五个关键技术挑战：故障注入参数优化的复杂性、形式化验证的扩展性问题、多重攻击向量的统一建模挑战、硬件软件协同设计的理论缺失，以及后量子时代的新挑战。基于现有的电压故障注入平台、FPGA 设备，我们制定了分阶段的研究规划，重点突破中等复杂度问题，为解决 SCA+VFA 联合攻击防护和 k-故障扩展性提供实践路径。

**下周计划：** 1) 完成电压故障注入参数空间的系统性映射，建立参数-故障效果数据库 2) 在 FPGA 平台上实现 AES 加密电路，开始 k-故障的硬件验证实验

## 1 研究进展分析

### 1.1 相关工作技术调研

**侧信道与故障攻击的联合防护**。[SBJ+21] 在 COSADE 2021 上发表了针对 SCA+SIFA 联合攻击的防护方案分析，题为 “Divided We Stand, United We Fall”。该工作深入分析了某些 SCA+SIFA 反措施在面对 SCA 增强的故障模板攻击时的安全性问题，揭示了单独设计的防护措施在联合攻击下可能失效的关键问题。Miškovský 和 Kubátová [MK21] 在 IEEE TVLSI 上提出了面积高效的掩码与故障容错架构，通过减少冗余度实现了安全性与硬件开销的平衡。Belenky 等人 [BBAL22] 提出了 RAMBAM 方案，将乘法掩码与冗余机制结合，增强了 AES 实现的故障抗性。Ramezanpour 等人 [RAD21] 提出了 RS-MASK 方案，作为针对功耗分析和故障分析的集成对策，使用随机空间掩码技术同时抵御两类攻击。

**后量子密码学的故障攻击防护**。Howe 等人 [HKM+20] 在 IEEE HOST 上提出了针对格基密码学中误差采样器的故障攻击对策。这项工作专门解决了后量子密码构造中的独特漏洞，为后量子时代的安全芯片设计提供了重要的理论基础。

### 1.2 当前技术挑战与研究缺口

**故障注入参数优化的复杂性**。Krček 和 Ordas [KO24] 的研究表明，激光故障注入的参数空间极其庞大，传统的穷举搜索方法效率低下。他们提出了基于遗传算法的多样性优化策略，但仍然面临收敛速度和全局最优解的挑战。同时，Toprakhisar 等人 [TNN24] 在 ESORICS 2024 上系统梳理了故障对手模型的参数化问题，强调了理论模型与实际攻击能力之间的差距。

**形式化验证的扩展性问题**。Tollec 等人 [THN+24] 在 TCHES 上发表的工作虽然建立了 k-故障抗性分区的理论基础，但在复杂系统中的扩展性仍然有限。当系统规模增大时，状态空间爆炸问题变得严重，需要开发更加高效的符号执行和模型检验技术。特别是对于现代处理器中包含的数百万门电路，现有方法的计算复杂度呈指数级增长，这是限制 k-故障抗性分区实用化的核心瓶颈。

**多重攻击向量的统一建模挑战**。现有研究往往独立考虑侧信道攻击和故障攻击的防护，对于两类攻击联合实施时的安全性分析相对薄弱。Saha 等人 [SBJ+21] 的工作 “Divided We Stand, United We Fall” 深刻揭示了这一问题：许多单独设计的 SCA+SIFA 防护措施在面对联合攻击时会失效。这表明我们需要从根本上重新思考安全防护的设计理念，建立真正统一的威胁模型。

**硬件软件协同设计的理论缺失**。当前的硬件软件协同防护缺乏统一的理论框架。虽然如 RS-MASK [RAD21] 等方案试图同时抵御 SCA 和故障攻击，但这些方案主要基于经验设计，缺乏形式

化的安全保证。我们需要建立能够跨越硬件和软件边界的统一安全分析方法，以实现真正的端到端安全保证。

**后量子时代的新挑战**。随着后量子密码学的广泛部署，传统的故障攻击防护方法面临新的挑战。Howe 等人 [HKM+20] 针对格基密码的研究表明，后量子算法的独特结构引入了新的攻击面。特别是在误差采样和格运算过程中，故障可能导致格结构的破坏，从而暴露私钥信息。这要求我们重新审视和设计针对后量子密码的故障防护机制。

## 2 可行性分析与研究规划

### 2.1 基于现有资源的可行性评估

**硬件实验能力**。我们拥有电压故障注入平台和 FPGA 设备，具备进行实际故障注入实验的硬件基础。电压故障注入技术相对成熟，可以实现精确的时序控制，为验证理论结果提供实验支撑。虽然缺乏激光故障注入设备，但电压故障注入能够覆盖大部分基础攻击场景，为参数优化算法的验证提供了充分的实验平台。

**软件开发能力**。具备中等程度的编程技能，能够开发所需的分析工具和实验软件。可以实现故障仿真器、分区算法、以及实验数据处理工具等关键软件组件。这种能力水平足以应对中等复杂度的技术挑战，特别是在故障传播建模和参数优化方面。

### 2.2 近期目标（未来 1-2 个月）

**电压故障注入参数空间映射**。基于现有的电压故障注入设备，系统性地探索和记录不同参数组合的故障效果。建立参数到故障结果的映射数据库，为后续的智能优化算法提供训练数据。重点改进时序控制精度和故障参数的自动化调节功能，直接响应参数优化复杂性的技术挑战。

**FPGA 上的 AES 电路 k-故障验证**。在 FPGA 平台上实现标准的 AES 加密电路，作为 k-故障抗性理论的验证目标。通过实际硬件实现，验证 3-故障安全性分析。

**故障传播模型与 SCA 联合分析基础**。针对多重攻击向量统一建模挑战，开发能够同时考虑故障传播和侧信道泄露的基础分析框架。利用 FPGA 平台收集故障注入实验中的功耗特征，为后续的 SCA+VFA 联合防护研究奠定实验基础。

## 参考文献


[BBAL22] Yossi Belenky, Vadim Bugaenko, Liron Azriel, and Itamar Levi. RAMBAM: Redundancy AES masking basis for attack mitigation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(3):748–778, 2022.

[HKM+20] James Howe, Ayesha Khalid, Marco Martinoli, Francesco Regazzoni, and Elisabeth Oswald. Fault attack countermeasures for error samplers in lattice-based cryptography. *IEEE Trans. Comput.*, 69(4):564–569, 2020.

[KO24] Martin Krček and Thomas Ordas. Diversity algorithms for laser fault injection. In *Computer Security - ESORICS 2024*, pages 159–178. Springer, 2024.

[MK21] Viktor Mišković and Hana Kubátová. Secure and dependable: Area-efficient masked and fault-tolerant architectures. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 29(10):1788–1801, 2021.

[RAD21] Keyvan Ramezanpour, Paul Ampadu, and William Diehl. RS-MASK: Random space masking as an integrated countermeasure against power and fault analysis. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 40(6):1087–1099, 2021.

[SBJ+21] Sayandeep Saha, Arnab Bag, Dirmanto Jap, Debdeep Mukhopadhyay, and Shivam Bhasin. Divided we stand, united we fall: Security analysis of some SCA+SIFA countermeasures against SCA-enhanced fault template attacks. In *Constructive Side-Channel Analysis and Secure Design - COSADE 2021*, pages 50–78. Springer, 2021.

[THN+24] 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.

[TNN24] Dilara Toprakhisar, Svetla Nikova, and Ventzislav Nikov. SoK: Parameterization of fault adversary models connecting theory and practice. In *Computer Security - ESORICS 2024*, pages 350–370. Springer, 2024.