周报

2025 年 6 月 17 日

大纲

1. 相关工作技术调研

2. 当前技术挑战与研究缺口

功耗与故障攻击的联合防护

联合攻击防护的关键问题

Saha 等人 [SBJ+21] 在 COSADE 2021 上发表的"Divided We Stand, United We Fall" 深入分析了 SCA+SIFA 反措施的安全性问题，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。

统一防护机制

Miškovský 和 Kubátová [MK21] 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安全性与硬件开销的平衡。Belenky 等人 [BBAL22] 的 RAMBAM 方案将乘法掩码与冗余机制结合，增强 AES 实现的故障抗性。

集成对策方案

Ramezanpour 等人 [RAD21] 提出的 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

后量子时代的新挑战

Howe 等人 [HKM+20] 在 IEEE TC 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。

格基密码的脆弱性

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，要求重新设计针对后量子密码的故障防护机制。

故障注入参数优化的复杂性

参数空间爆炸问题

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。

理论与实践的差距

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

状态空间爆炸挑战

Tollec 等人 [THN+24] 在 TCHES 上建立了 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。

实用化瓶颈

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

联合攻击的威胁

现有研究往往独立考虑功耗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**。

老师评语

再看看最新顶刊论文，做后量子是可以的

往后量子算法实现方向深入调研

参考文献 I


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.


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.


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

参考文献 II


Viktor Miškovský 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.


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.

参考文献 III


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.


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.

参考文献 IV


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.