IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–3. DOI:XXXXXXXX

XXX for XXX Against Fault Attacks

Jiahao Xiang[1] and Lang Li[1]

Hengyang Normal University, College of Computer Science and Technology, Hengyang, China

Abstract.

Keywords: Fault attack · countermeasures

1 Introduction

1.1 Related Work

Fault Injection Techniques and Models. Recent advances in fault injection have led to sophisticated attack vectors including laser fault injection (LFI), electromagnetic fault injection (EMFI), and voltage glitching. [YCF$^+$22] introduce *Redshift*, demonstrating continuous-wave laser manipulation of signal propagation delays, enabling more precise fault injection than traditional pulsed techniques. [KO24] propose diversity algorithms for optimizing laser fault injection parameters using machine learning approaches. The work by [TNN24] provides a systematic parameterization of fault adversary models, bridging theoretical assumptions with practical attack capabilities across different injection mechanisms.

Hardware Countermeasures and Redundancy Schemes. The [THN$^+$24] formalizes the *k-fault-resistant partitioning* notion to solve the fault propagation problem when assessing *redundancy-based hardware countermeasures* in a first step. Proven security guarantees can then reduce the remaining hardware attack surface when introducing software countermeasures in a second step. [ANN24] analyze attacks against glitch detection circuits, revealing vulnerabilities in hardware-based fault detection mechanisms. [RAD21] propose RS-Mask, an integrated countermeasure combining random space masking against both power analysis and fault attacks using redundant computations.

Threshold Implementations and Masking Techniques. The [DOT24] propose StaTI, a fault countermeasure based on *threshold implementations and linear encoding techniques* that protects against both side-channel and fault adversaries in non-combined attack settings. [FRBSG24] introduce Combined Threshold Implementation, providing theoretical foundations for unified protection schemes.

Masking and Error Correction Integration. [DEG$^+$18] demonstrate statistical ineffective fault attacks on masked AES implementations, highlighting the importance of proper integration between masking schemes and fault countermeasures. [MK21] present area-efficient architectures that combine masking with fault tolerance using reduced redundancy. [BBAL22] propose RAMBAM (Redundancy AES Masking Basis for Attack Mitigation), combining multiplicative masking with redundancy for enhanced fault resistance.

Post-Quantum Cryptography and Modern Threats. Recent work addresses fault attacks in post-quantum settings. [HKM$^+$20] develop specialized fault attack countermeasures for error samplers in lattice-based cryptography, addressing unique vulnerabilities in post-quantum constructions. The [Gen23] shows both theoretically and experimentally that countermeasures based on *caching intermediate WOTS$^+$ signatures* offer enhanced protection against unintentional faults in hash-based signatures.

Formal Security Analysis. Classical results include [CM09] proving that PSS encoding is secure against random fault attacks in the random oracle model. Modern approaches focus on combined security models: [SBJ+21] analyze SCA+SIFA countermeasures against enhanced fault template attacks, demonstrating the complexity of achieving security against multiple attack vectors simultaneously.

2 Preliminary

2.1 Fault Attack Model

Consider a cryptographic computation $\mathcal{C} : \mathcal{K} \times \mathcal{M} \to \mathcal{O}$ executing on a target device, where $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{O}$ denote the key, message, and output spaces, respectively. Let $\mathcal{S} = \{s_0, s_1, \ldots, s_n\}$ represent the sequence of internal computational states during execution.

Attacker Model. The adversary $\mathcal{A}$ controls a fault injection oracle $\mathcal{F}(t, \sigma, \phi, \alpha)$ parameterized by timing $t \in [0, T]$ within execution window T, target computational domain $\sigma \in \Sigma$ where $\Sigma = \{\text{ALU}, \ldots, \text{control}\}$ represents functional units, injection mechanism $\phi \in \{\text{EM}, \ldots, \text{voltage}\}$, and intensity $\alpha \in \mathbb{R}^+$. The fault oracle induces state transitions $s_i \mapsto s_i^{\text{fault}}$ with probability $P_{\text{fault}}(t, \sigma, \phi, \alpha)$. The adversary observes output pairs $(o_{\text{clean}}, o_{\text{fault}})$ where $o_{\text{clean}} = \mathcal{C}(k, m)$ and $o_{\text{fault}} = \mathcal{C}^{\text{fault}}(k, m)$ represents computation under fault influence.

Security Assumptions. The internal states $s_i \in \mathcal{S}$ remain opaque to $\mathcal{A}$, formally expressed as $\mathcal{A}(s_i) = \perp$ for all $i \in [0, n]$. Fault effects manifest probabilistically according to $P(\Delta | t, \sigma, \phi, \alpha)$ where Δ represents the computational deviation induced by the fault oracle. The adversary cannot deterministically control fault propagation through the computational pipeline, acknowledging stochastic fault models: transient bit corruption $\Delta_{\text{bit}} \sim \text{Bernoulli}(p_\sigma)$, instruction disruption $\Delta_{\text{instr}} \sim \text{Geometric}(q_\sigma)$, or data corruption $\Delta_{\text{data}} \sim \text{Uniform}(\mathbb{F}_2^w)$ for w-bit word operations, where success probabilities p_σ, q_σ depend on the target domain σ.

This attack model aligns with practical fault injection scenarios encountered in hardware security evaluations and provides a realistic framework for analyzing the effectiveness of proposed countermeasures.

References

[ANN24] Amund Askeland, Svetla Nikova, and Ventzislav Nikov. Who watches the watchers: Attacking glitch detection circuits. *IACR TCHES*, 2024(1):157–179, 2024.

[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.

[CM09] 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.

[DEG+18] Christoph Dobraunig, Maria Eichlseder, Hannes Groß, Stefan Mangard, Florian Mendel, and Robert Primas. Statistical ineffective fault attacks on masked AES with fault countermeasures. In *Advances in Cryptology - ASIACRYPT 2018*, pages 315–342. Springer, 2018.

[DOT24] Siemen Dhooghe, Artemii Ovchinnikov, and Dilara Toprakhisar. StaTI: Protecting against fault attacks using stable threshold implementations. *IACR TCHES*, 2024(1):229–263, 2024.

[FRBSG24] Jan Feldtkeller, Jan Richter-Brockmann, Pascal Sasdrich, and Tim Güneysu. Combined threshold implementation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2024(1):118–141, 2024.

[Gen23] Aymeric Genêt. On protecting SPHINCS+ against fault attacks. *IACR TCHES*, 2023(2):80–114, 2023.

[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 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.

[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.

[YCF$^+$22] Kenji Yamashita, Benjamin Cyr, Kevin Fu, Wayne Burleson, and Russell Tessier. Redshift: Manipulating signal propagation delay via continuous-wave lasers. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(4):727–758, 2022.