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

The [Gen23] shows both in theory and experimentally that the countermeasures based on *caching the intermediate* $WOTS^{+}s$ offer a marginally greater protection against unintentional faults. For the [CM09] show that the Bellcore attack cannot be applied to the *PSS encoding*; namely we show that PSS is provably secure against random fault attacks in the random oracle model, assuming that inverting RSA is hard. 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 the software in a second step. which combines the software and hardware countermeasures to provide a more robust solution against fault attacks. The [DOT24] propose a fault countermeasure, StaTI, based on threshold implementations and linear encoding techniques. The proposed countermeasure protects the implementations of cryptographic algorithms against both side-channel and fault adversaries in a non-combined attack setting.

References

[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.

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

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

[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.