ParTI – Towards Combined Hardware Countermeasures against Side-Channel and Fault-Injection Attacks

Tobias Schneider
Ruhr-Universität Bochum, Germany
Horst Görtz Institute for IT Security
tobias.schneider-a7a@rub.de

Amir Moradi
Ruhr-Universität Bochum, Germany
Horst Görtz Institute for IT Security
amir.moradi@rub.de

Tim Güneysu
University of Bremen and DFKI, Germany
tim.gueneysu@uni-bremen.de

ABSTRACT

Side-channel analysis and fault-injection attacks are known as major threats to any cryptographic implementation. Protecting cryptographic implementations with suitable countermeasures is thus essential before they are deployed in the wild. However, countermeasures for both threats are of completely different nature: Side-channel analysis is mitigated by techniques that hide or mask key-dependent information while resistance against fault-injection attacks can be achieved by redundancy in the computation for immediate error detection. Since already the integration of any single countermeasure in cryptographic hardware comes with significant costs in terms of performance and area, a combination of multiple countermeasures is expensive and often associated with undesired side effects.

In this work, we introduce a countermeasure for cryptographic hardware implementations that combines the concept of a provably-secure masking scheme (i.e., threshold implementation) with an error detecting approach against fault injection. As a case study, we apply our generic construction to the lightweight LED cipher. Our LED instance achieves first-order resistance against side-channel attacks combined with a fault detection capability that is superior to that of simple duplication for most error distributions at an increased area demand of 4.3%.

CCS Concepts

•**Security and privacy** → **Hardware attacks and countermeasures;**

Keywords

side-channel analysis; fault injection; threshold implementation; error-detecting codes

1. ACKNOWLEDGMENTS

The research in this work was supported in part by the DFG Research Training Group GRK 1817/1.

Tis'16 October 24-24 2016, Vienna, Austria

ACM ISBN 978-1-4503-4575-0/16/10.

DOI: http://dx.doi.org/10.1145/2996366.2996427