Threshold Implementations in Industry: A Case Study on SHA-256

Michael Hutter
Cryptography Research
425 Market Street
San Francisco, CA 94105
michael.hutter@cryptography.com

ABSTRACT

Implementing efficient countermeasures against side-channel attacks is a challenge since two decades. Especially in hardware, many masking countermeasure implementations failed due to first-order leakages caused by glitches or other effects such as early evaluation and unbalanced routing. The Threshold Implementation (TI) countermeasure was proposed a decade ago and it provides provable security even in the presence of such effects. In this talk, I discuss different state of the art secure logic styles and TIs from an industry perspective. As a case study, we consider SHA-256 which is especially interesting to mask due to its ARX-based design. I present various techniques for efficient mask conversion that can be applied to SHA-256 and discuss solutions for higher-order security.

CCS Concepts

•**Security and privacy** → **Side-channel analysis and countermeasures;** *Security in hardware;*

Keywords

Side-channel analysis; Threshold Implementation; Boolean-to-arithmetic masking; DPA; hardware security

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

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

DOI: http://dx.doi.org/10.1145/2996366.2996373

BIOGRAPHY

Michael Hutter is Principal Engineer at Cryptography Research, a division of Rambus Inc. He is currently working on secure hardware implementations of cryptographic algorithms. His research interests include all types of side-channel analysis related topics, fault and physical attacks, embedded system security, and RFID/IoT security. Previously, he served at the faculty of Computer Science at Graz University of Technology, Austria, at the Institute for Applied Information Processing and Communication Technologies (IAIK). He holds a Master of Science, a PhD degree, and a "venia docendi" (Habilitation) for the subject "Applied Information Processing". Michael has published more than 50 papers in international conferences, workshops, and journals and served as program committee member in numerous security conferences.