Domain-Oriented Masking

Compact Masked Hardware Implementations with Arbitrary Protection Order

Hannes Gross
Institute for Applied Information Processing and Communications
Graz University of Technology
Inffeldgasse 16a
8010, Graz, Austria

Stefan Mangard
Institute for Applied Information Processing and Communications
Graz University of Technology
Inffeldgasse 16a
8010, Graz, Austria

Thomas Korak
Institute for Applied Information Processing and Communications
Graz University of Technology
Inffeldgasse 16a
8010, Graz, Austria

ABSTRACT

Passive physical attacks, like power analysis, pose a serious threat to the security of embedded systems and corresponding countermeasures need to be implemented. In this talk, we demonstrate how the costs for protecting digital circuits against passive physical attacks can be lowered significantly. We introduce a novel masking approach called *domain-oriented masking* (DOM). Our approach provides the same level of security as threshold implementations (TI), while it requires less chip area and less randomness. DOM can also be scaled easily to arbitrary protection orders for any circuit.

To demonstrate the flexibility of our scheme, we apply DOM to a hardware design of the Advanced Encryption Standard (AES). The presented AES implementation is built in a way that it can be synthesized for any protection order. Although our AES design is scalable, it is smaller, faster, and less randomness demanding than other side-channel protected AES implementations. Our first-order secure AES design, for example, requires only 18 bits of randomness per S-box operation and 6 kGE of chip area. We demonstrate the flexibility of our AES implementation by synthesizing it up to the 15^{th} protection order. Beside our theoretical security analysis, we also evaluate the security of the AES implementation with a t-test based side-channel leakage assessments up to the second protection order.

CCS Concepts

•Security and privacy → Side-channel analysis and countermeasures;

Keywords

masking, domain-oriented masking, private circuits, threshold implementations, ISW, side-channel analysis, DPA, hardware security, AES

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

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

DOI: http://dx.doi.org/10.1145/2996366.2996426