Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware

In this paper, we present a novel lightweight authenticated cipher optimized for hardware implementations called Fides. It is an online nonce-based authenticated encryption scheme with authenticated data whose area requirements are as low as 793 GE and 1001 GE for 80-bit and 96-bit security, respectively. This is at least two times smaller than its closest competitors Hummingbird-2 and Grain-128a. While being extremely compact, Fides is both throughput and latency efficient, even in its most serial implementations. This is attained by our novel sponge-like design approach. Moreover, cryptographically optimal 5-bit and 6-bit S-boxes are used as basic nonlinear components while paying a special attention on the simplicity of providing first order side-channel resistance with threshold implementation.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Stichting Katholieke Universiteit, NXP Semiconductors Belgium, Graz University of Technology
Contributors: Bilgin, B., Bogdanov, A., Knezevic, M., Mendel, F., Wang, Q.
Pages: 142-158
Publication date: 2013

Host publication information
Title of host publication: Cryptographic Hardware and Embedded Systems - CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-40348-4
ISBN (Electronic): 978-3-642-40349-1
(Lecture Notes in Computer Science, Vol. 8086).
Keywords: Lightweight cryptography, Authenticated encryption, Keyed sponge, Glitch-free masking, APN permutation, Almost bent permutation
DOIs: 10.1007/978-3-642-40349-1_9
Source: dtu
Source-ID: n:oai:DTIC-ART:inspec/391644794::31716
Research output: Research - peer-review > Article in proceedings – Annual report year: 2013