Cryptology ePrint Archive: Report 2011/697

SPONGENT: The Design Space of Lightweight Cryptographic Hashing

Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, Ingrid Verbauwhede

Abstract: The design of secure yet efficiently implementable cryptographic algorithms is a fundamental problem of cryptography. Lately, lightweight cryptography - optimizing the algorithms to fit the most constrained environments - has received a great deal of attention, the recent research being mainly focused on building block ciphers. As opposed to that, the design of lightweight hash functions is still far from being well-investigated with only few proposals in the public domain.

In this article, we aim to address this gap by exploring the design space of lightweight hash functions based on the sponge construction instantiated with PRESENT-type permutations. The resulting family of hash functions is called SPONGENT. We propose 13 SPONGENT variants -- for different levels of collision and (second) preimage resistance as well as for various implementation constraints. For each of them we provide several ASIC hardware implementations - ranging from the lowest area to the highest throughput. We make efforts to address the fairness of comparison with other designs in the field by providing an exhaustive hardware evaluation on various technologies, including an open core library. We also prove essential differential properties of SPONGENT permutations, give a security analysis in terms of collision and preimage resistance, as well as study in detail dedicated linear distinguishers.

Category / Keywords: hash function, lightweight cryptography, low-cost cryptography, low-power design, sponge construction, PRESENT, SPONGENT, RFID

Publication Info: This is an extended version of the CHES'11 paper.

Date: received 21 Dec 2011

Contact author: andrey bogdanov at esat kuleuven be