Boss, Erik; **Grosso, Vincent**; **Güneysu, Tim**; **Leander, Gregor**; **Moradi, Amir**; **Schneider, Tobias**

Strong 8-bit sboxes with efficient masking in hardware. (English) Zbl 1429.94053

Gierlichs, Benedikt (ed.) et al., Cryptographic hardware and embedded systems – CHES 2016. 18th international conference, Santa Barbara, CA, USA, August 17–19, 2016. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 9813, 171-193 (2016).

Summary: Block ciphers are arguably the most important cryptographic primitive in practice. While their security against mathematical attacks is rather well understood, physical threats such as side-channel analysis (SCA) still pose a major challenge for their security. An effective countermeasure to thwart SCA is using a cipher representation that applies the threshold implementation (TI) concept. However, there are hardly any results available on how this concept can be adopted for block ciphers with large (i.e., 8-bit) S-boxes. In this work we provide a systematic analysis on and search for 8-bit S-box constructions that can intrinsically feature the TI concept, while still providing high resistance against cryptanalysis. Our study includes investigations on Sboxes constructed from smaller ones using Feistel, SPN, or MISTY network structures. As a result, we present a set of new S-boxes that not only provide strong cryptographic criteria, but are also optimized for TI. We believe that our results will found an inspiring basis for further research on high-security block ciphers that intrinsically feature protection against physical attacks.

For the entire collection see [Zbl 1343.68009].

MSC:

94A60 Cryptography

Full Text: DOI