Dokumenttyp: Konferenzbeitrag
Art des Konferenzbeitrags: Vortrag / Präsentation
Autor(en) des Beitrags: De Santis, Fabrizio and Bauer, Tobias and Sigl, Georg
Seitenangaben Beitrag: 10 pages
Abstract: Polynomial masking is a glitch-resistant and higher-order masking scheme based upon Shamir’s secret sharing scheme and multi-party computation protocols. Polynomial masking was first introduced at CHES 2011, while a 1st-order implementation of the AES S-box on FPGA was presented at CHES 2013. In this latter work, the authors showed a 2nd-order univariate leakage by side-channel collision analysis on a tuned measurement setup. This negative result motivates the need to evaluate the performance, area-costs, and security margins of combined shuffled and higher-order polynomially masking schemes to counteract trivial univariate leakages. In this work, we provide the following contributions: first, we introduce additional principles for the selection of efficient addition chains, which allow for more compact and faster implementations of cryptographic S-boxes. Our 1st-order AES S-box implementation requires approximately 27% less
registers, 20% less clock cycles, and 5% less random bits than the CHES 2013 implementation. Then, we propose a lightweight shuffling countermeasure, which inherently applies to polynomial masking schemes and effectively enhances their univariate security at negligible area expenses. Finally, we present the design of a combined shuffled and higher-order polynomially masked AES S-box in hardware, while providing ASIC synthesis and side-channel analysis results in the Electro-Magnetic (EM) domain.

Stichworte:
Shuffling; Polynomial Masking; Multi-Party Computation; Secret Sharing; Side-Channel Analysis; AES

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
Theory of Implementation Security Workshop (TIs 2016), ACM CCS

Kongress / Zusatzeinformationen:
Vienna, Austria

Jahr:
2016

Quartal:
4. Quartal

Jahr / Monat:
2016-10

Monat:
Oct

Revid:
ja

Sprache:
en

WWW:

Occurences:
- Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016

entries: