Lehrstühle und Professuren

Dokumenttyp: Konferenzbeitrag
Art des Konferenzbeitrags: Vortrag / Präsentation
Autor(en) des Beitrags: Seuschek, Hermann and Guillen, Oscar and De Santis, Fabrizio
Titel des Beitrags: Side-Channel Leakage Aware Instruction Scheduling
Abstract:
Speed-optimized side-channel protected software implementations of block ciphers are important for the security of embedded IoT devices based on general-purpose microcontrollers. The recent work of Schwabe et al. published at SAC 2016 introduced a bit-sliced implementation of AES and a first-order Boolean-masked version of it, targeting ARM Cortex-M CPU cores. The authors claim to be secure against timing as well as first-order power and electromagnetic side-channel attacks. However, the author's security claims are not taking the actual leakage characteristics of the underlying CPU architecture into account, hence making the scheme potentially vulnerable to first-order attacks in practice. In this work we show indeed that such a masking scheme can be attacked very easily by first-order electromagnetic side-channel attacks. In order to fix the issue and provide practical first-order security, we provide a strategy to schedule program instructions in way that the specific leakage of the CPU does not impair the side-channel countermeasure.

Stichworte: Side-Channel Countermeasures; Masking; Bit-sliced; Compilers

Dewey Dezimalklassifikation (Liste):