Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Algebraic Side-Channel Analysis

Side-Channel Analysis (SCA) exploits information leaked by a device over its timing behavior, power consumption or EM emanations to reveal, e.g., the secret key of a cryptographic algorithms is retrieved. “Classical” SCA methods such as Differential Power Analysis (DPA) or Correlation Power Analysis (CPA) collect a number of measurements for different input values of the algorithm under attack and combine the leakage of different measurements to conduct the attack.

Instead, Algebraic SCA [1] makes use of the internal state of the attacked algorithm to formulate a SAT problem and thus allows for combining different leakages. Furthermore, attacks on a single measurement are possible, an attacker does not need to know inputs and outputs and even countermeasures such as masking schemes can circumvented.

The goal of this topic is to provide an overview over existing approaches on algebraic side-channel analysis that exceeds the seminal works in [1-2] and to outline current trends and applications ofalgebraic attacks.

[1] Renauld, M. & Standaert, F.-X.: Algebraic Side-Channel Attacks. Information Security and Cryptology, Springer Berlin Heidelberg, 2010, 393-410
[2] Renauld, M.; Standaert, F.-X. & Veyrat-Charvillon, N.: Algebraic Side-Channel Attacks on the AES: Why Time also Mtters in DPA Cryptographic Hardware and Embedded Systems - CHES 2009, Springer Berlin Heidelberg, 2009, 97-111

Contact

Request Topic

Advisors

Lars Tebelmann