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

Seminar

Differential Computation Analysis

Differential Computation Analysis (DCA) is the software counterpart of the Differential Power Analysis (DPA) that uses the power consumption of a device to extract secret information.
A DCA can be mounted on white-box implementations of cryptographic algorithms, i.e., an attacker has full access to the internal state and can extract software traces containing the read and write accesses made to memory.

This work should give an insight into DCA. Moreover, the limitations of DCA should be discussed as well as possible countermeasures.

References

- Bos, Joppe W., Hubain, Charles, Michiels, Wil, Teuwen, Philippe. 'Differential Computation Analysis: Hiding Your White-Box Designs is Not Enough'. Cryptographic Hardware and Embedded Systems -- CHES 2016. Springer Berlin Heidelberg. 2016.

Contact

Request Topic

Advisors

Manuel Brosch