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

Seminar

Frequency-Based Differential Side-Channel Attack

Most Side-Channel attacks, like DPA, are executed in the timing domain. As a result, the measurements need to be aligned in order to mount a successfull attack.
Shifting the attack to the frequency domain overcomes the requirement of aligned measurements, and allows also to attack secured implementations.

The goal is to give an insight into the topic of side-channel attacks that operate in the frequency domain. Furthermore, the advantages or disadvantages compared to well known techniques like DPA should be drawn.

References

- Gebotys, Catherine H., Ho, Simon, Tiu, C. C.. "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA". Cryptographic Hardware and Embedded Systems -- CHES 2005. Springer Berlin Heidelberg. 2005.
- Y. Lu, K. H. Boey, M. O'Neill, J. V. McCanny and A. Satoh, "Is the differential frequency-based attack effective against random delay insertion?," 2009 IEEE Workshop on Signal Processing Systems, Tampere, 2009.

Contact

Request Topic

Advisors

Manuel Brosch