Lehrstuhl für Sicherheit in der Informationstechnik
Fakultät für Elektrotechnik und Informationstechnik
Technische Universität München

FP/BA/MA:

Statistische Fehlerattacken auf SKINNY

Beschreibung:

Fehlerattacken stellen eine ernsthafte Bedrohung für die Implementierung von kryptografischen Verfahren dar, da diese nicht das zugrunde liegende mathematische Problem angreifen, sondern dessen Implementierung [1]. Die Blockchiffre SKINNY ist eine leichtgewichtige Chiffre und eignet sich gut für den Einsatz in Systemen mit begrenzten Ressourcen [2].

Im ersten Teil dieser Arbeit soll eine statistische Fehlerattacke auf SKINNY gefunden werden.

Im zweiten Teil der Arbeit soll evaluiert werden, inwieweit man SKINNY gegen diese Art von Fehlerattacke schützen kann.

Quellen

[1] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE*, 94(2):370–382, feb 2006.

[2] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The skinny family of block ciphers and its low-latency variant mantis. Cryptology ePrint Archive, Report 2016/660, 2016. `https://eprint.iacr.org/2016/660`.

Bitte richten Sie Ihre Bewerbung an:

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
M.Sc. Michael Gruber
Theresienstraße 90
80333 München
oder per E-Mail: m.gruber@tum.de

Besuchen Sie uns auch auf https://www.sec.ei.tum.de/

June 8, 2018