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

Seminar

Side-Channel Attacks on Code-based Cryptosystems

Established public key cryptography can be considered broken in the presence of a large scale quantum computer. In order to act on this emerging threat the National Institute of Standards and Technology (NIST) has started a competition [1] to standardize possible post-quantum cryptography algorithms.

In the third round of the contest the code-based cryptosystems “Classic McEliece”, “HQC” and “BIKE” are still under consideration from NIST. This work should give an overview of published attacks and countermeasures against code-based cryptosystems and comment on their applicability on the remaining round three candidates. As a starting point for a literature review the reference [2] should be used.

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography
[2] Sim, B.-Y.; Kwon, J.; Choi, K. Y.; Cho, J.; Park, A. & Han, D.-G.
Novel Side-Channel Attacks on Quasi-Cyclic Code-Based Cryptography
IACR Transactions on Cryptographic Hardware and Embedded Systems, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, Volume 2019, Issue 4

Prerequisites

Request Topic

Advisors

Thomas Schamberger