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

Seminar

Hardware Acceleration of Hommorphic Encryption

With the rapid increase in cloud computing, solutions for protecting the privacy of the data in the cloud should be deployed.
One of them is hommorphic encryption, a paradigm which allow computations on encrypted data without having to decrypt it.
The implementation of such encryption schemes is challenging and usually slow on general purpose computers. With the raise of FPGAs in the cloud, hommorphic encryption can be accelerated via these platforms [1, 2, 3].

This work should introduce the concept of hommorphic encryption and its possible acceleration via FPGA platforms.

References

[1]: Pöppelmann et al., **Accelerating HomomorphicEvaluation on Reconfigurable Hardware**, CHES 2015
[2]: Sinha Roy et al., **FPGA-based High-Performance ParallelArchitecture for Homomorphic Computing on Encrypted Data**, HPCA 2019
[3]: M. Sadegh Riaz et al., **HEAX: An Architecture for Computing on Encrypted Data**, ASPLOS 20

Contact

Request Toppic

Advisors

Mathieu Gross