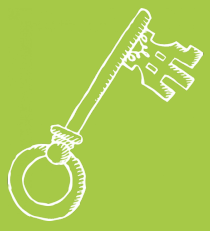


Feasibility of Fully Homomorphic Encryption on Embedded Devices

Advisor: **Daniel Kales**

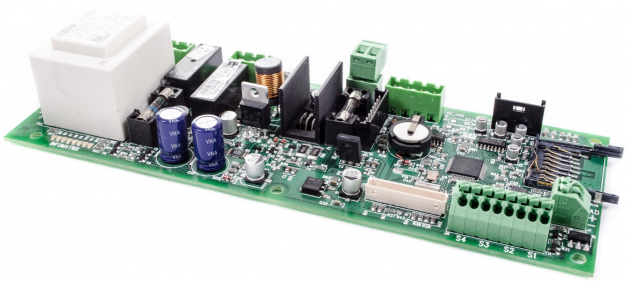
Motivation

Small IoT devices are omni-present in todays times, ranging from wearable devices to sensor node networks. However, many of the data that is recorded by these devices is sent to a central server, where it is stored in the clear. Many use-cases might want to hide this information from a cloud server, but still want to compute statistics over this data. One approach that can enable this functionality is fully homomorphic encryption (FHE). Using FHE, devices can encrypt their data and send them to a cloud server, and, due to the properties of the FHE scheme, the server can still perform calculations using this data. The result of these computations is still encrypted and can then be sent to another party to decrypt.

However, FHE schemes come with a considerable overhead in both computation time and communication size. Especially on resource-constrained devices, like the IoT devices mentioned before, even something as simple as encryption and decryption can, for some applications, be too costly.

Goals and Tasks

- Get familiar with FHE schemes and libraries
- Port/Implement FHE encryption and decryption on embedded devices
- Evaluate the performance of FHE and alternatives on embedded devices



Literature

- Z. Brakerski, C. Gentry, and V. Vaikuntanathan
  (Leveled) Fully Homomorphic Encryption without Bootstrapping
  TOCT 2014
- J. H. Cheon et al.
  Homomorphic Encryption for Arithmetic of Approximate Numbers
  ASIACRYPT (1)

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, …
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Programming: C, C++
- Interest in FHE

Advisor / Contact

daniel.kales@iaik.tugraz.at