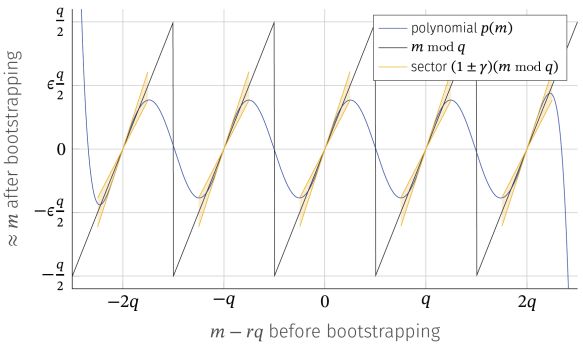
Universität Stuttgart
Institut für Systemtheorie und Regelungstechnik
Prof. Dr.–Ing. Frank Allgöwer

Open Thesis (BA/FA/MA)

Implementing a novel Encrypted Polynomial Evaluation

Description:



Homomorphic cryptosystems enable the evaluation of functions on encrypted data. This technology provides new possibilities for private cloud computing and for encrypted control. A key building block of many homomorphic cryptosystems is bootstrapping, where a polynomial approximation of the modulo function must be evaluated. We have recently developed a novel type of bootstrapping procedure. The thesis topics include the implementation of the algorithm in encryption libraries such as OpenFHE (C++) or LattiGo (Go), as well as a performance comparison with existing implementations. Furthermore, optimizing over the involved polynomials can lead to greater precision and improved performance when combined with encrypted control.

Prerequisites:

- Interest and some experience in programming.

Supervisor:

Sebastian Schlor
Room 2.234

Area:

Encrypted Control
Optimzation

Properties:

Type: **BA/FA/MA**

30% literature
20% theory
50% implementation
up to discussion

Beginning:

any time

Further information on www.ist.uni-stuttgart.de/lehre/bama

Aushang vom June 11, 2025