Contribution ID: **63** Type: **Talk (15min + 5min)**

Privacy-preserving scientific computing with fully homomorphic encryption

Tuesday 25 February 2025 17:15 (20 minutes)

With the rise of cloud computing in many areas of industry, commercial services, or science, data privacy is a growing concern for researchers and practitioners alike. In addition, with more data being processed in the cloud, the impact of a potential data breach increases as well, especially when sensitive information such as engineering, financial, or medical data is concerned. The use of fully homomorphic encryption (FHE) can provide a solution to this issue: Since all data is encrypted before being sent to the cloud, all information remains secure even if a malicious party is able to gain access to the cloud computing environment.
In this talk, we will take a look at homomorphic encryption for securely processing numerical data and assess its potential for privacy preserving applications in the context of scientific computing. After a brief introduction to the CKKS scheme for FHE, we will discuss the accuracy and performance implications of its basic operations for computations with floating point numbers. Finally, we will evaluate the potential of FHE for scientific computing by demonstrating the secure numerical simulation of partial differential equations with a finite difference approach.

I want to participate in the youngRSE prize

no

Primary author: SCHLOTTKE-LAKEMPER, Michael (University of Augsburg)

Presenter: SCHLOTTKE-LAKEMPER, Michael (University of Augsburg)

Session Classification: Security of Research Software

Track Classification: Research Software: Cloud Technologies