Open Hiwi Position

Implementing Efficient Secure Computation

TECHNISCHE UNIVERSITÄT DARMSTADT

The *Engineering Cryptographic Protocols Group* (ENCRYPTO) is offering a Hiwi position. The number of working hours is flexible and ranges from 40 to 82 hours per month starting in October 2017. The initial contract will run for 3 months. However, a long-term cooperation is possible and desired.

Motivation & Goal

Secure computation allows mutually distrusting parties to jointly compute a function on their input data without revealing anything but the result. It can be employed on a variety of hardware platforms, ranging from mobile phones to high-end servers, and has a high number of applications, including the discovery of common contacts, genomic sequencing, or the secure processing of data in the cloud. Correspondingly, possible challenges for an applicant are wide-spread and include but are not limited to:

- Implementing new protocol designs in C/C++, as well as evaluating them and comparing them to prior art
- Running experiments for determining protocol parameters and failure probabilities on the Lichtenberg High Performance Computer (HHLR[1])
- Maintaining and extending our ABY[2] framework for efficient mixed-protocol secure two-party computation

The results emerging from this work are essential contributions to research papers that will be published at international top conferences.

Requirements

- Good programming skills in C/C++
- At least basic knowledge of cryptography
- High motivation and creativity + ability to work independently
- Flexible working hours
- Experience with reading research papers is beneficial
- Knowledge of the English language goes without saying

Contact

If you are interested, please get in touch and send your complete application (including a letter of motivation, CV, and transcript of records) to:

- M.Sc. Christian Weinert (christian.weinert@crisp-da.de)
- Dr.-Ing. Thomas Schneider (thomas.schneider@crisp-da.de)

[1] http://www.hhlr.tu-darmstadt.de/hhlr/

[2] http://encrypto.de/code/ABY/