TECHNISCHE UNIVERSITÄT DARMSTADT

Hiwi-Job

Implementation of cryptographic schemes and protocols

1. General Information

Lattice-based cryptography is a very promising candidate for the future, when potential quantum computers might exist.

2. Goals

Implementation of Cryptographic schemes and protocols:

- RSA, Elliptic curve, AES
- Lattice based Cryptography
- Data aggregation
- Protocols in Wireless Sensor Networks also possible
- ….

This is an opportunity to learn a lot about cryptography.

3. Required Skills

The required skills, in order of importance, are:

- Good programming skills C
- Knowledge in linear algebra
- Attendance of Introduction to cryptography desirable.

4. Contact

If you are interested, please contact
Rachid El Bansarkhani
Room: B212
EMail: elbansarkhani@cdc.informatik.tu-darmstadt.de