Abschlussarbeit Quantum Key Distribution Post-Processing

Anna-Katharina Wickert ✉ **wickert@st.informatik.tu-darmstadt.de**
Maximilian Tippmann ✉ **maximilian.tippmann@physik.tu-darmstadt.de**

TECHNISCHE UNIVERSITÄT DARMSTADT

Start after agreement
Bachelorthesis or masterthesis

Motivation

Quantum key distribution provides a means for cryptographic applications to exchange a symmetric key between different parties in a provably secure manner. The security of this method is based on the errors generated during information exchange by an eavesdropping attack - based on principles of quantum mechanics - which are noticeable by the involved parties. Therefore, it is important that the keys are post-processed before they are used. Post-processing consists of error correction of the key and subsequent privacy enhancement.

Integration into Collaborative Research Center CROSSING

As part of the Collaborative Research Center CROSSING, project P4 [1] from the Department of Physics is researching such quantum key exchange methods, while from the Department of Computer Science project E1 [2] is researching secure integration of cryptographic methods into code. As an interface between both departments, various post-processing methods, in particular error correction, will be adapted to the current quantum system of P4 and further investigated in this thesis.

Thesis Objectives

The work of the thesis include, for example, performance (minimizing the necessary key compression) and runtime investigations. Existing methods can be investigated more deeply for optimal block lengths - the key is split into blocks for post-processing - and achievable Shannon efficiencies. For testing, P4 provides quantum keys of the experiment. Finally, the implementation will be integrated into the open-source Eclipse plugin CogniCrypt.

Additional Information

The topic can be worked on as a bachelor's or master's thesis. For working on the thesis, a simple knowledge of quantum key exchange protocols is advantageous. The willingness to familiarize oneself with the topic is a prerequisite. To achieve the goals of the thesis, it is necessary to have programming experience in Java and Python. In addition, knowledge of other programming languages is beneficial, as well as experience with open source projects. The work can start promptly after consultation with the supervisors. In the case of very good work, there is a possibility of publication of the results. If you are interested in the work, please contact Anna-Katharina Wickert or Maximilian Tippmann.

[1] https://www.crossing.tu-darmstadt.de/research_crossing/project_areas/primitives/p4/index.en.jsp
[2] https://www.crossing.tu-darmstadt.de/research_crossing/project_areas/engineering/e1/index.en.jsp