Master's Thesis

Protected Code-based Post-Quantum Security

The foreseeable breakthrough of quantum computers represents a risk for communication which uses public-key cryptography. In order to prepare for such an event, embedded devices must integrate post-quantum cryptography, a set of algorithms based on mathematical problems that remains secure even in the presence of the quantum computers. Code-based is one of the most promising post-quantum cryptography. However, the implementation of code-based cryptography has two main challenges: i) satisfy performance and power constraints; and ii) resist side-channel attacks, which uses leakages derived from the implementation (timing, power or electromagnetic characteristics) to retrieve the secret information. The goal of this thesis is to implement a protected version (resistant to side-channel attack) of the newest version of the Gabidulin-Paramonov-Tretjakov code-based post-quantum cryptosystem. This Master thesis will be supervised by Dr. Johanna Sepúlveda (Chair of Security in Information Technology) and Prof. Dr.-Ing. Antonia Wachter-Zeh (Professorship for Coding for Communications and Data Storage).

Some of the following tasks might be covered:

- Getting familiar with Code-based Post-quantum security
- Getting familiar with Gabidulin codes
- Getting familiar with secure implementation
- Secure C/VHDL implementations
- Performance evaluation
- Security evaluation

The thesis can be done in German or English language.

Literature:

Mail: johanna.sepulveda@tum.de, tel.: +49 89 289 28256, room N1009.
Prof. Dr.-Ing. Antonia Wachter-Zeh
Mail: antonia.wachter-zeh@tum.de, tel.: +49 89 289 23495, room N4402.

Prerequisites

- VHDL/Verilog or C/C++ programming skills
- Basic knowledge in security concepts
- Basic knowledge in channel coding or information theory
Contact

Dr. Johanna Sepúlveda (Doutora em Ciencias, Microeletrônica, University of São Paulo). Mail: johanna.sepulveda@tum.de, tel.: +49 89 289 28256, room N1009.
Prof. Dr.-Ing. Antonia Wachter-Zeh
Mail: antonia.wachter-zeh@tum.de, tel.: +49 89 289 23495, room N4402.

Advisors

Antonia Wachter-Zeh
Johanna Sepúlveda (Chair of Security in Information Technology, TUM)