Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

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).

Advisors

Julian Renner, Antonia Wachter-Zeh