TECHNISCHE HOCHSCHULE DEGGENDORF

POST

POST-QUANTEN-SICHERE OPEN-SOURCE-SCHEMATA UND TECHNOLOGIEN FÜR AUTOMOTIVE-ANWENDUNGEN

Weitere Infos:

Abstract

Projekttitel/ Project title:

Post-Quanten-sichere Open-Source-Schemata und Technologien für Automotive-Anwendungen

Kurztitel/ Short title:

POST

Einleitung/ Introduction:

The emergence and rapid advancement of quantum computers poses a significant threat to conventional asymmetric cryptographic algorithms, as they are potentially capable of efficiently solving computational problems that are considered intractable for traditional computers. This threatens the security of modern communication systems, especially in sensitive and security-critical application areas such as vehicle communication, where protection against potential attacks is of crucial importance. The project POST addresses the urgent need to transition towards post-quantum cryptography (PQC), ensuring secure data transmission, processing, and storage in automotive systems. A key component of the subproject of the POST project at the Deggendorf Institute of Technology (DIT) is the development of a crypto-agile hardware platform using FPGA-based partial reconfiguration to support multiple PQC algorithms, evaluated and hardened against side channel attacks such as timing and power analysis attacks.

Ziel/ Aim:

The primary objectives of POST are:

1. Develop quantum-resistant cryptographic solutions tailored for automotive use cases.
2. Investigate the impact of PQC algorithms on three specific domains of automotive communication:
    - **Car2X Communication**: Securing external vehicle communication, including manufacturer backends, inter-vehicle links, and vehicle-to-device connections.
    - **Intra-Car Communication**: Ensuring the integrity and authenticity of onboard data transmission via automotive Ethernet.
    - **Sensor Network Authentication**: Authenticating sensors and their data in vehicles relying on classical bus systems like CAN and LIN.
3. Create a crypto-agile hardware platform leveraging FPGA-based partial reconfiguration to support dynamic and robust implementation of PQC algorithms.

Methode/ Method:

The project employs a multidisciplinary approach, including:

- **Algorithm Analysis**: Evaluating PQC algorithms under standardization efforts (e.g., NIST PQC competition) for automotive applicability.
- **Hardware Development**: Designing building blocks for efficient arithmetic cores to enable crypto-agility and post-quantum algorithm implementation.
- **Hardware-Software Co-Design**: Developing tightly integrated hardware-software systems for cryptographic operations, ensuring maximum acceleration and support for dynamic algorithm updates throughout the system lifecycle.
- **Protocol Development**: Enhancement of automotive communication protocols with quantum-resistant Crypto Algorithm to harden current automotive communication.
- **Side-Channel Resistance**: Implementing countermeasures to protect hardware solutions from timing and power analysis attacks.

Ergebnis/ Result:

The POST project is currently in its initial phase, therefore no scientific results are available at this stage.

Projektbeteiligte/ Project participants:

Prof. Dr. Martin Schramm
Simon Rudhart
Stephan Zitzlsperger
Mahboubeh Tajmirriahi

Projektpartner/ Project partners:

Partners:

- AED Vantage GmbH (AED)
- easycore GmbH (EC)
- Infineon Technologies AG (IFAG)
- Hochschule RheinMain (HSRM)
- Ruhr-Universität Bochum (RUB)
- Technische Hochschule Deggendorf (THD)
- Technische UniversitätMünchen (TUM)

Associated Partners:

- BMW AG
- Mercedes-Benz Group AG
- Continental AG
- Robert Bosch GmbH
- InnoRoute GmbH
-

Gefördert durch/ Funded by:

Bundesministerium für Bildung und Forschung (BMBF)

Logos/ Logos:

Bundesministerium für Bildung und Forschung

POST

AED VANTAGE

easycore

infineon

Hochschule RheinMain

TECHNISCHE HOCHSCHULE DEGGENDORF THD

RUHR UNIVERSITÄT BOCHUM RUB