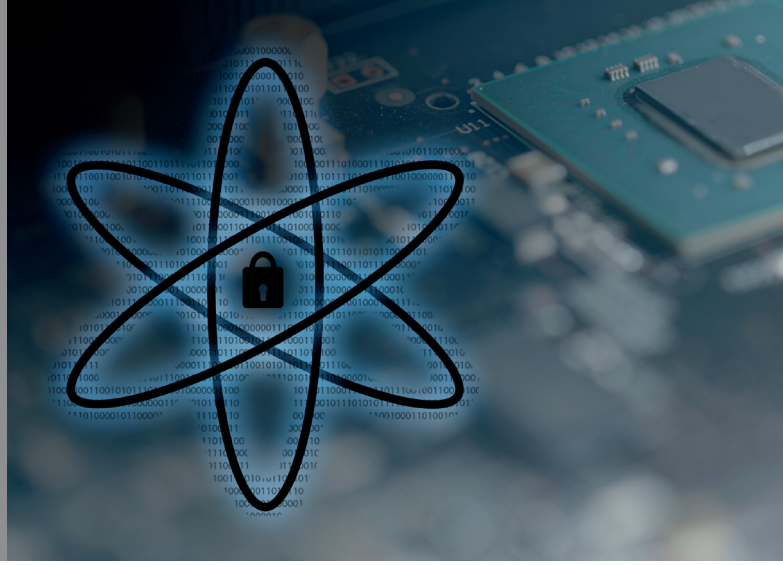
Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE



Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dr. Ruben Niederhagen
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-135
Fax 06151 869-224
ruben.niederhagen@sit.fraunhofer.de
www.sit.fraunhofer.de

QUANTUMRISC

KRYPTOGRAFIE DER NÄCHSTEN GENERATION

Die Entwicklung leistungsfähiger Quantencomputer bedroht die Sicherheit heutiger kryptografischer Verfahren. Mit einem hinreichend leistungsfähigen und stabilen Quantencomputer lassen sich viele aktuelle Verschlüsselungsverfahren brechen. Seit einigen Jahren werden deshalb alternative kryptografische Verfahren untersucht, die auch gegen Angriffe mit Quantencomputern sicher sind. Dieses Forschungsgebiet wird als Post-Quantum-Kryptografie (englisch Post-quantum Cryptography, PQC) bezeichnet. Die neuen PQC-Verfahren müssen auf ihre Praxistauglichkeit geprüft werden und in bestehende Infrastruktur integrierbar sein.

Ein Nachteil von PQC-Verfahren gegenüber derzeit benutzten Verschlüsselungsverfahren ist ihr generell höherer Ressourcenbedarf: Viele PQC-Verfahren benötigen mehr Rechenleistung, mehr Speicherplatz oder mehr Netzwerk-Bandbreite zur Übertragung von Schlüsseln oder Nachrichten. Dies ist ein Problem für eingebettete Systeme, da diese oft nur eine geringe Leistungsfähigkeit aufweisen, aber häufig in sicherheitskritischen Bereichen eingesetzt werden – wie in Industrieanlagen, in der Medizintechnik, in der Telekommunikation oder in Steuergeräten von Fahrzeugen.

Ziel des Projekts

Das Projekt QuantumRISC entwickelt PQC-Verfahren weiter, um diese auf niedrigen Stromverbrauch und geringen Speicherbedarf bei gleichzeitig hohem Sicherheitsniveau zu optimieren. Damit können PQC-Verfahren den Praxisanforderungen in eingebetteten Systemen entsprechen. Zusammen mit akademischen und industriellen Partnern wird im Anwendungsbereich „Automotive Engineering“ sowohl das Zusammenspiel mit bestehenden Fahrzeugsystemen und Architekturen erforscht als auch die Integrationsmöglichkeiten im Fahrzeug untersucht, die einen späteren Austausch der kryptografischen Verfahren (Krypto-Agilität) ermöglichen sollen. Weiterhin wird durch die Abstimmung mit weiteren assoziierten Partnern aus der Industrie die Übertragbarkeit der Ergebnisse auf andere Domänen sichergestellt..

Projektpartner

- Ruhr-Universität Bochum
- Technische Universität Darmstadt
- Hochschule RheinMain
- MTG AG
- Elektrobit Automotive GmbH
- Continental Teves AG und Co.
- Fraunhofer SIT