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

Die Kommunikation im, vom und zum Fahrzeug ist insbesondere hinsichtlich der Entwicklung von autonomen Fahrfunktionen sicherheitskritisch und muss entsprechend gegen Cyberangriffe abgesichert werden. Quantencomputer haben das Potential, derzeit verwendete kryptografische Algorithmen zu brechen, weshalb diese zukünftig nicht mehr ausreichen werden. Aufgrund der langen Lebensdauer von Fahrzeugen ist es wichtig, potenzielle Schwachstellen weit im Voraus zu identifizieren, um die Sicherheit ihrer Systeme langfristig gewährleisten zu können.

Eckdaten

Kurztitel

POST

Laufzeit

01.08.2024 - 31.07.2027

Fördergeber

Bundesministerium für Bildung und Forschung (BMBF)

Projektträger

VDI/VDE/IT

Projektleitung

Prof. Dr. Martin Schramm

Ziele

Moderne Fahrzeugbordnetze lassen sich in drei Ebenen gliedern:

- Car2X-Kommunikation: Fahrzeuge kommunizieren mit ihrer Umgebung.
- Intra-Car-Kommunikation: Die Steuergeräte eines Fahrzeugs kommunizieren miteinander.
- Sensornetzwerk-Authentifikation: Sensoren registrieren sich an Steuergeräten und übertragen Daten.

Die Leistungsfähigkeit der verwendeten Komponenten ist in den drei Ebenen sehr unterschiedlich. Im Rahmen des Projekts sollen jedoch alle Ebenen mit jeweils geeigneten Post-Quanten-Kryptografischen (PQK) Verfahren abgesichert werden, also Verfahren, bei denen davon ausgegangen wird, dass sie nicht mit Hilfe eines Quantencomputers zu brechen sind. Das System soll dabei kryptoagil sein, so dass kryptografische Verfahren während der Lebensdauer der Fahrzeuge aktualisiert werden können, falls dies nötig wird. Außerdem soll ein hybrider Ansatz verwendet werden, bei dem klassische kryptografische Verfahren mit PQK-Verfahren kombiniert werden, um eine nahtlose Integration in bestehende Systeme zu gewährleisten.