

Connected and automated vehicles for the quantum age

To ensure the long-term safety of connected and automated vehicles, the BMBF-funded 'PARFAIT' project is researching the use of post-quantum cryptography (PQC) and crypto agility. Fraunhofer AISEC is investigating security strategies for vehicle components, analysing vulnerabilities and optimising encryption methods.

The increasing connectivity and automation of vehicles increases the risk of cyber attacks. In addition, future quantum computers could break today's encryption. That is why the UNECE R155 guideline has required a long-term security concept for vehicle approvals since 2022. To meet these requirements, post-quantum cryptography (PQC) and crypto agility must be incorporated into the development of digital and electronic vehicle components at an early stage.

The aim of the project 'Post-Quantum Cryptography for Automotive Components (PARFAIT)', funded by the German Federal Ministry of Education and Research (BMBF), is therefore to research secure procedures and methods for the use of post-quantum cryptography and crypto agility in the automotive sector. Fraunhofer AISEC is one of the cybersecurity partners among the eight participating institutions from industry and science.

Security strategies for vehicle components, vulnerability analysis and optimised encryption methods

Fraunhofer AISEC helps identify cryptographic security objectives for vehicles, such as secure boot, updates and diagnostics, which are to be secured with PQC. It also analyses 'store now, decrypt later' scenarios for implementing an attacker model as a basis for future security solutions.

Fraunhofer AISEC evaluates current technologies and assigns them to suitable applications.

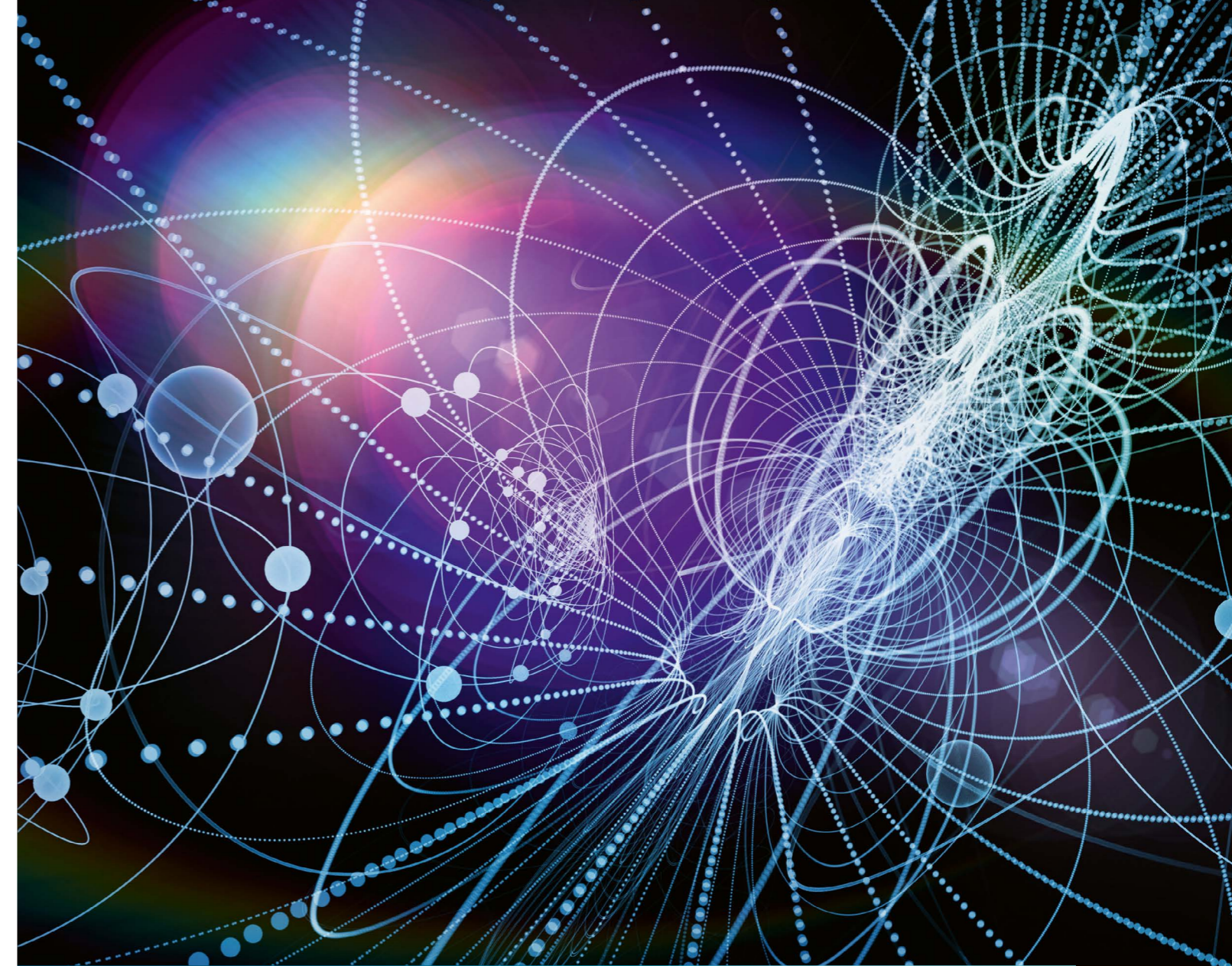
It analyses which processes are suitable for secure migration and develops migration strategies for different vehicle architectures. In doing so, it takes into account system requirements and the transition from classic to PQC-based solutions.

Researchers at Fraunhofer AISEC are analysing the PQC algorithms from the NIST competitions in terms of performance and memory requirements. They are expanding the PQDB database to include low-end devices and automotive microcontrollers so that suitable algorithms can be selected for control units. Fraunhofer AISEC is extending protocols from the automotive environment to include PQC and is examining weaknesses in existing processes and protocols. It is investigating hybridisation strategies for integrating PQC into existing systems and evaluating the best solutions in terms of performance, security and compatibility. It is also analysing the suitability of modern cryptographic approaches such as proxy re-encryption for use in the automotive sector.

Glossary

Crypto agility refers to the ability of IT systems to flexibly exchange cryptographic algorithms and protocols.

Proxy Re-Encryption (PRE) is a cryptographic technique that allows encrypted data to be passed from a sender to a recipient without the intermediary (proxy) knowing the plaintext of the data.



Strong alliance for the future viability of the automotive industry

The partners in the 'PARFAIT' consortium are: DENSO AUTOMOTIVE Deutschland GmbH, Fraunhofer AISEC, Freie Universität Berlin, Darmstadt University of Applied Sciences, RheinMain University of Applied Sciences, Infineon Technologies AG, Darmstadt Technical University and Vitesco Technologies Germany GmbH.



Project 'PARFAIT'



Contact

Prof. Dr. Marian Margraf

Head of Department
Secure Systems Engineering
Phone: +49 89 3229986-152
marian.margraf@aisec.fraunhofer.de

More Information



Center of post-quantum cryptography
excellence