

Center of Excellence for Post-Quantum Cryptography

Sales Deck

Fraunhofer Institute for Applied and Integrated Security AISEC

Agenda

Sales Deck of the Center of Excellence for Post-Quantum Cryptography at Fraunhofer AISEC

Our Core Competencies and Services

Completed Projects

Current Projects

Collaborative Networks

Our Core Competencies and Services

Fraunhofer Institute for Applied and Integrated Security AISEC

Facts & Figures

- Founded: 2009
- Budget (including investments): €25.69 million (2025)
- Employees: approx. 250
- Locations: Garching near Munich (headquarters), Berlin, Weiden i.d. Opf.
- University affiliations:



Prof. Dr. Eckert
Prof. Dr. Sigl



Prof. Dr. Margraf
Prof. Dr. Wunder



Prof. Dr. Loebenberger



© Fraunhofer AISEC

“Fraunhofer AISEC translates **excellent information security research** into **application-oriented solutions** for greater reliability, trustworthiness, and tamper resistance of IT-based systems and products.”

The Center of Excellence for Post-Quantum Cryptography at Fraunhofer AISEC

From strategic consulting and technical analysis to active knowledge transfer

Goal

Secure migration of companies and government agencies to quantum-resistant IT systems – vendor-neutral, practical, and research-based.

Your added value

- ✓ Vendor-neutral and practical consulting
- ✓ Customized IT security analyses
- ✓ Excellent research as the foundation for high-quality technological solutions
- ✓ Guided transition to quantum-resistant methods



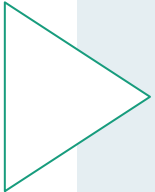
The Center of Excellence for Post-Quantum Cryptography at Fraunhofer AISEC

Our Core Competencies



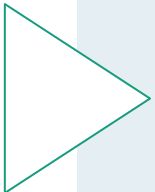
The Center of Excellence for Post-Quantum Cryptography at Fraunhofer AISEC

Our Services



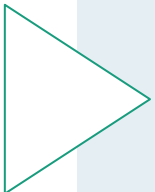
IT security analyses regarding the cryptography used

- Analysis and evaluation of external and internal application security
- Assessment of overall cryptographic risk (Cryptographic Risk Assessment)
- Conducting side-channel and error attack tests as well as firmware analyses
- Selection of suitable PQC solutions for your specific security and performance requirements



Support for migration to quantum-resistant cryptography

- Custom migration strategies (prioritization of critical systems, hybrid approaches, roadmaps)
- Design of crypto-agile target infrastructures (cryptography becomes easily interchangeable/updatable)
- Technical support for PQC implementation in software and hardware

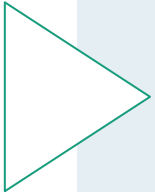


Knowledge transfer

- [pqdb database](#): Overview of PQC methods (security level, NIST standardization status, efficiency)
- [Serious Game - Charlie and the Quantum Factory](#): A playful introduction to the quantum world
- Consulting on scientific developments, the current threat landscape, and countermeasures

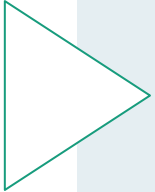
The Post-Quantum Cryptography Competence Center at Fraunhofer AISEC

Our Services



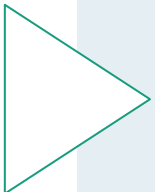
Participation in BMBFR research projects

- Shaping the future of IT security together with partners from industry and research
- Contributing to high-quality scientific publications and standardization processes
- Practical technology transfer: from research directly into real-world application scenarios



Training courses in the Cybersecurity Learning Lab

- [Fraunhofer AISEC seminar offerings](#): training formats for (quantum-resistant) cryptography, cryptoagility, and PQC migration
- Always up-to-date content, presented in a pedagogically sound manner by experienced instructors in both in-person and remote settings



Community formats & networks

- International PQC community for up-to-date exchange
- Organization of the annual “PQC Update” networking event for experts from research and industry

Completed Projects

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

PoQsiKom

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

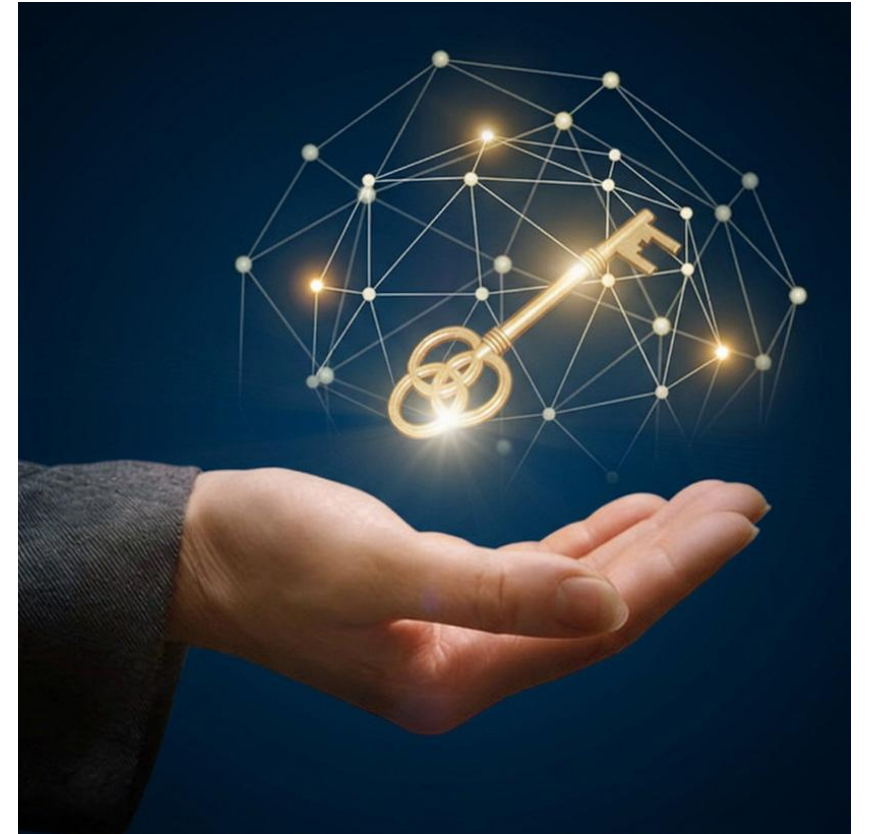
PoQsiKom

Full-Lifecycle Post-Quantum PKI (FLOQI)

Development of a PQ knowledge database, PQ-PKI implementation analysis, and demonstrators

Information and Consortium Partners

- Funding: public
- Duration: 2019–2023
- Project partners:
 - TU Berlin, SecT Chair
 - operational services GmbH & Co.KG
 - Fraunhofer AISEC
 - Robert Bosch GmbH
 - ESCRYPT GmbH
 - D-Trust GmbH
 - BMW Group



©Magnific / Fraunhofer AISEC

Full-Lifecycle Post-Quantum PKI (FLOQI)

Development of a PQ knowledge database, PQ-PKI implementation analysis, and demonstrators

Objectives and Motivation

- **Objectives:** Development of a quantum-resistant PKI (PQ-PKI) with backward compatibility to classical cryptographic methods, using the automotive sector and Industry 4.0 as examples
- **Motivation:** The need for long-lasting, secure cryptographic methods in products with decades of use (e.g., vehicles, production facilities). To ensure confidentiality and integrity today and in a future with quantum computers, current and quantum-resistant methods must be used in a hybrid manner.

Approach

- **Analysis of quantum-resistant methods:** Selection of suitable NIST PQC algorithms for use in hybrid certificates and PQ-PKIs, creation of the pqdb database for a standardized comparison of the methods
- **Architecture design:** Comparison of different PQ-PKI implementation variants, requirements analysis, and evaluation of advantages and disadvantages
- **Implementation:** Development of demonstrators in the automotive sector and Industry 4.0, taking specific requirements into account
- **Development of a migration concept** for existing PKIs

Full-Lifecycle Post-Quantum PKI (FLOQI)

Development of a PQ knowledge database, PQ-PKI implementation analysis, and demonstrators

PQDB database¹

Provision of a **public database** for post-quantum cryptographic key exchange and signature schemes



Key exchange

e.g.: CRYSTALS-KYBER

Signatures

e.g.: CRYSTALS-DILITHIUM

PQ-PKI Implementation Variants

- **Var1:** Hybrid X.509 certificates
- **Var2:** **Mixed PKI** (PKI supports both classical and PQ methods)
- **Var3:** **Parallel PKIs** (separate PKIs for classical and PQ methods, respectively)
- **Var4:** **Intelligent Composed Algorithms (ICAs)**²

PQ-PKI Demonstrators

Demonstrator for Embedded

Industry 4.0: Quantum-secure over-the-air firmware updates for I4.0 products

Demonstrators for Connected Vehicles:

- Quantum-secure authentication of electronic control units (ECUs) at WPAN gateways
- Quantum-secure in-vehicle and vehicle-to-vehicle communication between ECUs

¹<https://www.pqdb.info/> ² <https://eprint.iacr.org/2021/813.pdf>

Full-Lifecycle Post-Quantum PKI (FLOQI)

Development of a PQ knowledge base, PQ-PKI implementation analysis, and demonstrators

PQ-PKI Requirements

- **Certificate hierarchy:** Root CA, sub-CAs, EE certificates
- **Validity period:** CA certificates up to 20 years, EE certificates between 2 weeks and 20 years
- **Certificate standard:** X.509
- **Certificate management system**
- **Security level** $\geq$ 128 bits
- **Support:** in hardware (e.g., HSM) and protocols (e.g., TLS)
- **Compliance** with regulations (BSI)

Var1: Hybrid certificates

- Certificates support both classical and PQ algorithms and are backward-compatible
- To ensure hybrid compatibility, adjustments must be made:
 - In PKI standards (RFC5280, PKCS#10)
 - in the certificate management system
 - in hardware, software, and applications
 - In the authentication method (token-based procedure)

Var2: Mixed PKI

- The root CA uses the PQ signature algorithm; subordinate CAs and EEs do not necessarily have to
- Good interim solution during the transition phase: individual entities can be non-PQ-compliant without compromising the entire PKI

Full-Lifecycle Post-Quantum PKI (FLOQI)

Development of a PQ knowledge base, PQ-PKI implementation analysis, and demonstrators

Var3: Parallel PKIs

- Two parallel PKI architectures, each with its own certificate management system, hardware and software solutions, and authentication methods
- An entity requires two certificates
- Applications must define when and in what order the two certificates from the two PKIs are used

Var4: Intelligent Composed Algorithms (ICAs)

- Intelligent Composed Algorithms (ICAs) comprise cryptographic algorithms as well as control algorithms that govern the combination of the cryptographic algorithms.
- Classical and PQ methods are encapsulated in ICAs and seamlessly embedded into existing certificates.
- No changes to certificates are required. Control algorithms replace the classical algorithms. Classical and PQ methods are combined and integrated into hybrid methods.

Full-Lifecycle Post-Quantum PKI (FLOQI)

Development of a PQ knowledge database, PQ-PKI implementation analysis, and demonstrators

Evaluation of PQ-PKI implementation options

- Hybrid certificates (Var1) require significant customization effort but are backward-compatible
- The mixed PKI infrastructure (Var2) enables a phased PQC migration
- Managing parallel PKIs (Var3) is very resource-intensive and requires clear guidelines on how the two PKIs should be combined
- ICAs (Var4) provide high flexibility in integrating new algorithms (crypto-agility) and integrate into existing standards

Conclusion

There is no “one-size-fits-all” solution: Selection depends on an organization’s specific circumstances, requirements, and framework conditions (regulations, resources, use cases)

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

PoQsiKom

Botan Cryptography Library for Long-Term Security (KBLS)

Extension of Botan to include PQ schemes while maintaining cryptoagility and usability

Information and partners

- Funding: public
- Duration: 2019–2023
- Project partners:
 - Fraunhofer AISEC
 - TU Berlin, SecT Chair
 - neXenio GmbH
 - Rohde & Schwarz Cybersecurity GmbH



©Magnific / Fraunhofer AISEC

Botan Cryptography Library for Long-Term Security (KBLS)

Extension of Botan to include PQ methods while maintaining cryptoagility and usability

Goals and Motivation

- **Goals:** The Botan cryptography library is to be expanded through the integration of PQ methods. The implementation of these methods is to be designed efficiently so that they can also be used in resource-constrained systems. Additionally, the library should be crypto-agile and easy to use. The results developed in the project should also be applicable in other cryptography libraries.
- **Motivation:** Software developers typically do not implement cryptographic algorithms themselves but rely on established cryptographic libraries. Botan is intended to enable the simple and secure use of PQ cryptography.

Approach

- **Analysis and comparison of** quantum-resistant algorithms using the pqdb database (see the “FLOQI” project)
- **Communication with the Botan maintainers** to continuously coordinate, review, and integrate extensions into the official library
- **Conducting usability tests** in coordination with developers

Botan Cryptography Library for Long-Term Security (KBLS)

Extension of Botan to include PQ schemes while maintaining cryptoagility and usability

Results

- **PQ methods selected for Botan:** Kyber (PQ key exchange method) and Dilithium (PQ signature method), due to the optimal trade-off between security and performance criteria (memory requirements, computational complexity)
- **Design of a usability concept** with the following offerings for developers: Comprehensive documentation with examples, meaningful error messages, static code review tool with a focus on side-channel resistance
- **Implementation** of the selected PQ schemes with measures for side-channel resistance and cryptoagility (e.g., easy switching to longer key lengths possible)

Conclusion

- **Extension:** Botan now includes PQC schemes in addition to classic public-key schemes
- Enables developers to **use** PQC schemes **easily and securely**
- **Cryptoagility** allows for continuous adaptation of the library to new findings in the field of PQC

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

PoQsiKom

Post-Quantum Cryptography for Government Documents (PoQuID)

Quantum-computer-resistant cryptographic protocols for government documents

Information and partners

- Funding: public
- Duration: 2020–2022
- Project partners:
 - Federal Office for Information Security
 - Fraunhofer AISEC
 - Bundesdruckerei GmbH
 - Infineon Technologies AG



©Infineon

Post-Quantum Cryptography for Government Documents (PoQuID)

Quantum-computer-resistant cryptographic protocols for government documents

Objectives and Motivation

- **Objectives:** quantum-computer-resistant communication between electronic identity documents (ePassports) and inspection systems based on a PQ-Extended Access Control (EAC) protocol
- **Motivation:** An electronic chip secures German EU passports and ID cards, which citizens can also use to authenticate themselves online. The personal data stored in the chip – including biometric features such as passport photos and fingerprints, as well as a proof of authenticity – must remain usable as a security feature even in the age of quantum computers.

Approach

- **Requirements analysis and selection** of PQ methods using the pqdb database (see the "FLOQI" project)
- **Development** of hybrid authentication and PKI solutions for the EAC protocol
- **Attack analysis**, particularly regarding side channels, with security proofs
- **Implementation of a demonstrator** showing PQ-secure authentication of an e-passport at a border control. Real-world validation with tests
- **Technical specification** and standardization

Post-Quantum Cryptography for Government Documents (PoQuID)

Quantum-computer-resistant cryptographic protocols for government documents

Results

- **PQ methods selected for the PQ-EAC protocol:** Kyber (PQ key agreement method) and Dilithium (PQ signature method) (BSI recommendation)
- **Development of two PQ-EAC variants:**
 1. **SigPQEAC:** Authentication with PQ signatures based on Dilithium
 2. **KemPQEAC:** Authentication with PQ key agreement based on Kyber (Advantage: resource-efficient)
- **Development of hybrid schemes** using classical and PQ methods during the transition phase
- **Demonstrator:** Implementation of SigPQEAC in a border control scenario

Conclusion

- **Development and implementation** of a PQ-resistant version of the EAC protocol used for government documents¹
- **Real-world tests** demonstrate the high efficiency of the proposed solutions
- **Cryptoagility:** Alternative key agreement and signature schemes can be used

¹https://link.springer.com/chapter/10.1007/978-3-031-30731-7_2

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

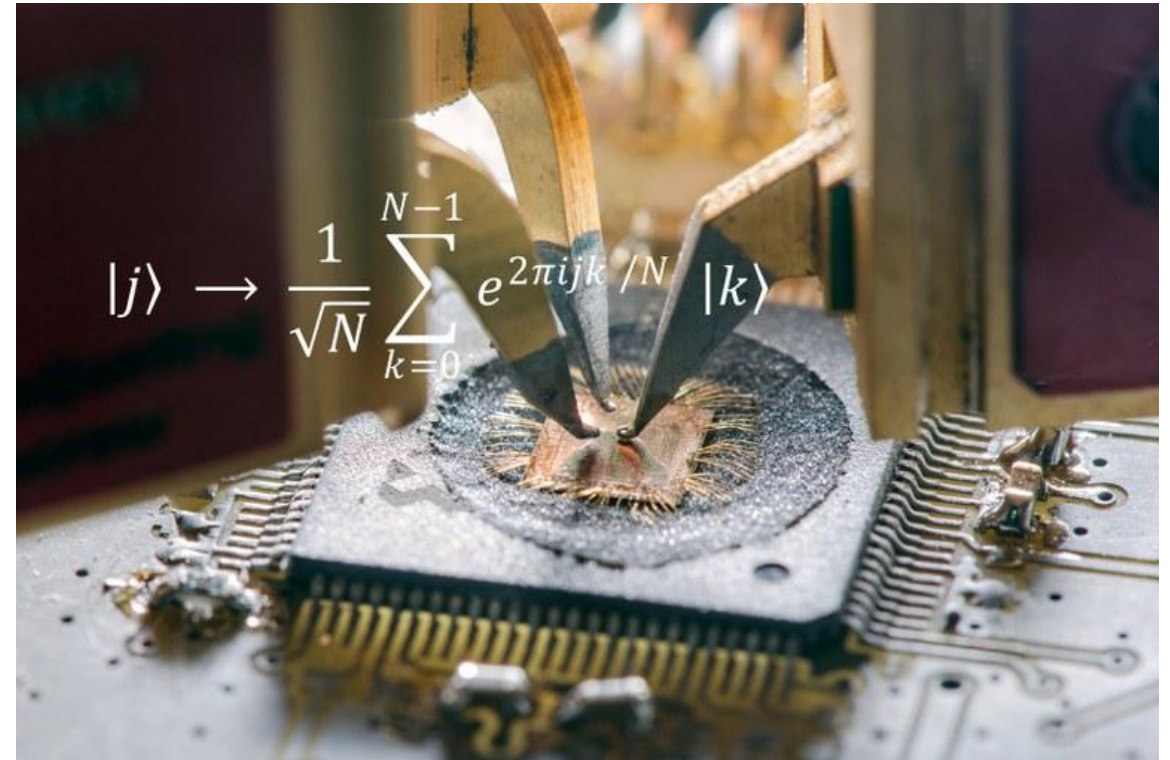
PoQsiKom

Applicability of PQC Methods (Aquorypt)

PQC in industrial embedded systems and smart card-based security applications

Information and Consortium Partners

- Funding: Public
- Duration: 2019–2023
- Project partners:
 - Technical University of Munich
 - Fraunhofer AISEC
 - Giesecke+Devrient Mobile Security GmbH
 - Infineon Technologies AG
 - Siemens AG
 - Technical University of Darmstadt



© Andreas Heddergott / TU Munich

Applicability of PQC Methods (Aquorypt)

PQC in industrial embedded systems and smart card-based security applications

Objectives and Motivation

- **Objectives:** Investigation of the applicability of quantum-computer-resistant cryptographic methods in industrial embedded systems and smart card-based security applications
- **Motivation:** Ensuring the security of embedded systems and smart card-based security applications in the age of quantum computers while maintaining storage efficiency and performance

Approach

- **Analysis and comparison of** NIST-standardized PQC schemes for efficient use in hardware and software
- **Implementation of** suitable PQC methods
- **Development of migration strategies** for transitioning existing systems to quantum-computer-resistant solutions

Applicability of PQC Methods (Aquorypt)

PQC in industrial embedded systems and smart card-based security applications

Results

- Systematic comparative analysis of suitable PQC methods for hardware accelerators
- Investigation of the effects of machine learning-based side-channel attacks on hardware accelerators
- Development of a secure hardware-software co-design for a PQC hardware accelerator in FPGA-based systems
- Exemplary implementation of countermeasures for hardening PQC implementations
- Development and presentation of a demonstrator, as well as publication of several scientific papers

Conclusion

- Quantum-resistant cryptographic methods can be implemented in hardware accelerators
- In addition to selecting suitable PQC algorithms, secure implementation, protection against side-channel attacks, and an efficient software-hardware architecture are crucial for practical deployment
- The project provides important foundations, demonstrations, and recommendations for migrating existing systems to more quantum-secure cryptographic solutions

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

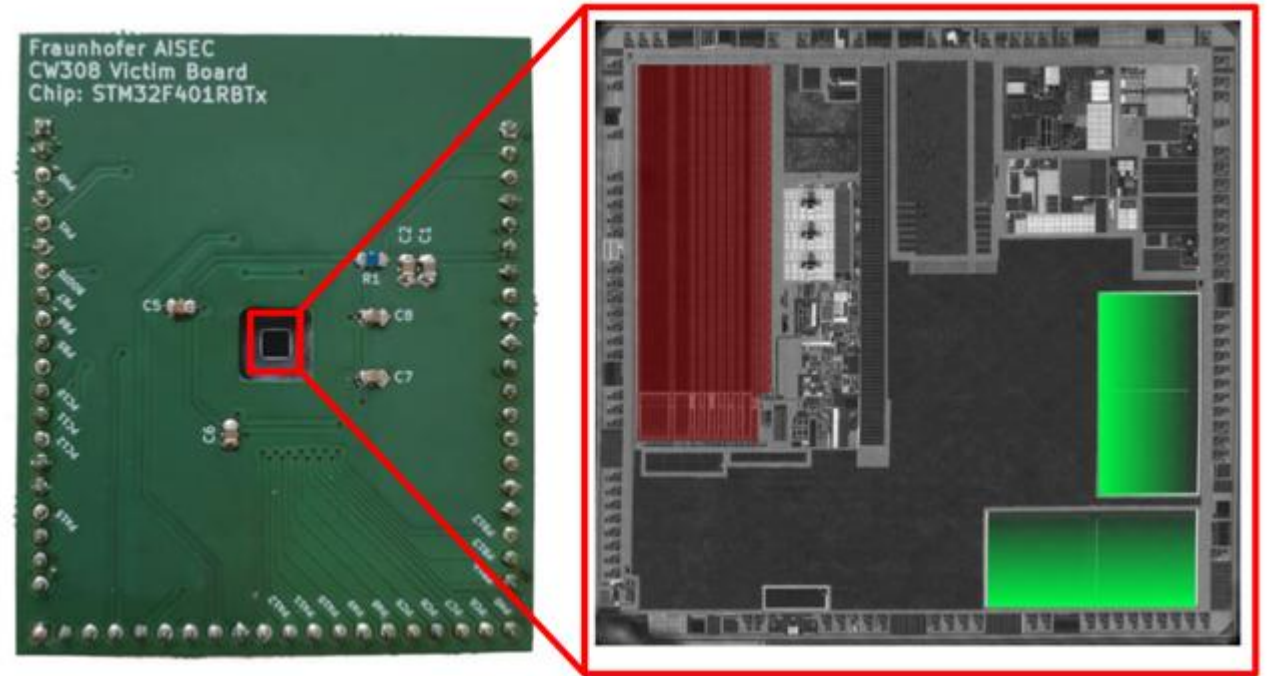
PoQsiKom

Laser Fault Injection Attack on Hash-Based Signature Schemes

BSI study on the preparation and execution of the attack

Information and partners

- Funding: public (BSI)
- Duration: 2024



© BSI

Laser Fault Injection Attack on Hash-Based Signature Schemes

BSI study on the preparation and execution of the attack

Objectives and Motivation

- **Objectives:** To investigate the practical feasibility of laser fault injection attacks against the quantum-resistant XMSS signature scheme in real-world implementations and to derive recommendations for secure implementations of hash-based signature schemes in embedded systems
- **Motivation:** To assess whether post-quantum-resistant hash-based signature schemes (e.g., XMSS) can be compromised in real-world implementations via physical hardware attacks such as laser fault injection, despite their mathematical security

Approach

- **Target:** Winternitz One-Time Signature (WOTS) scheme, which is a central component of XMSS
- **Experimental setup:** Implementation of XMSS on a standard microcontroller. Establishment of a laser attack laboratory
- **Attack method:** Generation of precise hardware errors via laser pulses in the microcontroller's calculations during signature generation -> Attacker can derive parts of the WOTS keys or generate signature forgeries
- Further information: [Download the BSI study](#)

Laser Fault Injection Attack on Hash-Based Signature Schemes

BSI study on the preparation and execution of the attack

Results

- **Practical feasibility:** Laser fault injection attacks on hash-based signatures (XMSS, LMS, SPHINCS+) are possible on real hardware. This poses a significant threat to security-critical infrastructure devices, such as HSMs or smart cards.
- **Attack conditions:** physical access to the device required, laser laboratory equipment, high level of technical expertise
- **Recommended countermeasures:** In addition to secure software, targeted hardware protection against fault injection through error detection in signature schemes and redundant computations

Conclusion

- Hash-based signature schemes can be compromised by physical attacks
- The laser fault injection attack can induce errors in signature generation that may lead to key reconstruction or signature forgery
- In addition to secure software implementation, signature security is heavily dependent on hardware hardening against physical attacks

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

PoQsiKom

Quantum-Secure VPN Modules and Operating Modes (QuaSiModO)

Quantum-secure virtual private networks

Information and Consortium Partners

- Funding: Public
- Duration: 2019–2022
- Project partners:
 - genua GmbH, Kirchheim
 - ADVA Network Security GmbH, Planegg
 - Ludwig Maximilian University of Munich
 - Fraunhofer AISEC, Weiden i.d. Opf.



©Magnific / Fraunhofer AISEC

Quantum-Secure VPN Modules and Operating Modes (QuaSiModO)

Quantum-secure virtual private networks

Objectives and Motivation

- **Objectives:** Integration of quantum-resistant algorithms into VPN standards and implementations at Layers 2 and 3 of the TCP/IP reference model. Focus on the PQ adaptation of IKEv2 in IPsec at Layer 3.
- **Motivation:** Ensuring VPN security against attacks by powerful quantum computers

Approach

- **Selection and analysis** of suitable PQC algorithms based on practical requirements
- **Development of hybrid approaches** for the key agreement procedure in the MACsec (Layer 2) and IPsec (Layer 3) protocols
- **Implementation** of schemes in established VPN software suites
- **Security analysis** of the protocols and their implementations
- Exchange within international **standardization bodies**

Quantum-Secure VPN Modules and Operating Modes (QuaSiModO)

Quantum-Secure Virtual Private Networks

Results

- **Development of quantum-secure extensions** for the key agreement procedure in the MACsec (Layer 2) and IPsec (Layer 3) protocols
- **Contribution to Internet Drafts of** international standardization bodies

Conclusion

- **Contribution** to the creation of **robust and future-proof VPN standards**

Completed Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

FLOQI

KBLS

PoQuID

Aquorypt

Laser Fault Injection Attack

QuaSiModO

PoQsiKom

Post-Quantum Secure Communication for Industry 4.0 (PoQsiKom)

PQ-secure communication for Industry 4.0 with internationally standardized trust anchors

Information and Consortium Partners

- Funding: public
- Duration: 2021–2024
- Project partners:
 - Fraunhofer AISEC
 - Technical University of Munich
 - Siemens
 - TRUMPF Machine Tools GmbH



Post-Quantum Secure Communication for Industry 4.0 (PoQsiKom)

PQ-secure communication for Industry 4.0 with internationally standardized trust anchors

Objectives and Motivation

- **Objectives:** Development of an Industry 4.0 platform for the secure and trustworthy remote acknowledgment of safety devices. This enables remote real-time monitoring and confirmation of safety states, thereby reducing response times.
- **Motivation:** Increasing connectivity and the exchange of data across trust boundaries require robust security solutions that go beyond traditional authentication methods. Given the threats posed by quantum computers, it is crucial to establish long-term security standards.

Approach

- **Definition of requirements and system architecture** for the industrial platform (operating system, trust anchors, ...)
- **Development of a trust anchor** based on the open-source security chip OpenTitan with hardware accelerators for the post-quantum cryptographic algorithms Dilithium and Falcon
- **Integration of the trust anchor** into the industrial platform using the Generic Trust Anchor (GTA) API
- **Analysis of suitable communication protocols and authentication methods** for remote acknowledgment, including QUIC, BRSKI, and MFA
- Integration of the system components into a platform demonstrator

Post-Quantum Secure Communication for Industry 4.0 (PoQsiKom)

PQ-secure communication for Industry 4.0 with internationally standardized trust anchors

Results

- **Publication of project results** at scientific conferences and as open-source projects
- **Participation in the DIN NA 043-01-41-02 working group** "Generic Application Programming Interface for IoT and Industrial Devices" for the standardization of the GTA-API
- **Prototype implementation** of the project results in the form of a demonstrator and presentation at the Hannover Messe 2024
- **Cooperation with a Korean sister project** to integrate the national demonstrators, including the connection of the Korean crypto module to the German demonstrator

Conclusion

- **Significant progress** in the development of secure communication solutions for Industry 4.0.
- **The AISEC demonstrator** serves as a clear example of secure remote acknowledgment and raises awareness among companies and students about post-quantum security and safety in industrial environments

Current Projects

Current Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

PARFAIT

AMiQuaSy

TRUSTED

Current Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

PARFAIT

AMiQuaSy

TRUSTED

Post-Quantum Cryptography for Automotive Components (PARFAIT)

Application of post-quantum cryptography and cryptoagility in the automotive sector

Information and partners

- Funding: public
- Duration: 2024–2027
- Project partners:
 - Infineon Technologies AG
 - DENSO AUTOMOTIVE Deutschland GmbH
 - Vitesco Technologies Germany GmbH
 - Fraunhofer AISEC
 - Freie Universität Berlin
 - Darmstadt University of Applied Sciences
 - RheinMain University of Applied Sciences
 - Technical University of Darmstadt



Post-Quantum Cryptography for Automotive Components (PARFAIT)

Application of post-quantum cryptography and cryptoagility in the automotive sector

Objectives and Motivation

- **Objectives:** Establishment of post-quantum cryptography (PQC) and cryptoagility in the automotive sector
- **Motivation:** PQC and cryptoagility support the implementation of the UNECE R155 regulation to ensure the long-term security of vehicle registrations

Approach

- **Identification of requirements** arising for automotive applications
- **Conducting threat analyses**
- **Analysis and comparison** of NIST-standardized PQC methods for use in automotive components in terms of performance, memory requirements, and robustness
- **Development of hybrid approaches** and suitable migration strategies with practical demonstration
- **Extension of automotive protocols** with regard to PQC and cryptoagility

Current Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

PARFAIT

AMiQuaSy

TRUSTED

Agile Migration to Quantum-Resistant Systems (AMiQuaSy)

Secure Software Development in the Post-Quantum World

Information and Partners

- Funding: public
- Duration: 2023–2026
- Project partners:
 - Xitaso GmbH IT & Software Solutions, Augsburg
 - genua GmbH, Kirchheim
 - OTH Amberg-Weiden, Amberg
 - Fraunhofer AISEC, Weiden i.d. Opf.



©Magnific / Fraunhofer AISEC

Agile Migration to Quantum-Resistant Systems (AMiQuaSy)

Secure Software Development in the Post-Quantum World

Objectives and Motivation

- **Objectives:** Development of agile security mechanisms that allow **cryptographic algorithms** to be easily replaced with new secure algorithms (crypto-agility)
- **Motivation:** In the future, **cryptographic methods** must be quickly **replaceable** in order to respond to a **constantly changing threat landscape** with minimal risk and low downtime

Approach

- Collaboration with industry and research to **identify practical requirements** and current migration barriers
- Investigation of various **migration scenarios** and development of technical **implementation approaches**
- Development of an LLM-based approach for **the semi-automatic identification of cryptographic software packages**
- Development of an IT security-focused Architecture Tradeoff Analysis Method (SATAM) to derive **Cryptographic Bills of Materials (CBOMs)** from IT architectures, thereby placing cryptographic migration planning **within an architectural context**

Current Projects: Overview

Analysis, design, and implementation of secure solutions for the post-quantum era

PARFAIT

AMiQuaSy

TRUSTED

Enabling Trustworthy European Data Spaces (TRUSTED)

Trustworthy European Data Space for Personal Data

Information and partners

- **Funding:** public (European Commission)
- **Duration:** 2025–2028
- **Project partners:**
 - Gradient
 - Tree Technology, Fundación Cibervoluntarios (Spain)
 - Infocert SPA, Cybersocial Lab, Fondazione Mondo Digitale (Italy)
 - Fraunhofer AISEC, Fraunhofer ISST (Germany)
 - Promptly, University Hospital of Coimbra (Portugal)
 - Sestek (Turkey)



© Gradient

Enabling Trustworthy European Data Spaces (TRUSTED)

Trustworthy European Data Space for Personal Data

Goals and Motivation

- **Goals:** Establishing a **trusted data space** that enables AI applications on personal data through **privacy-enhancing technologies**, as well as **AI-supported identity and authorization management** for self-managed identities.
- **Motivation:** Innovations based on AI drive valuable progress, e.g., in medicine. To **apply AI methods to personal data in a trustworthy manner**, it must be ensured that users retain control over their data.

Approach

- **Analysis of existing technologies for self-sovereign identities** and definition of **requirements** for a trustworthy data space
- **Development and integration of privacy-enhancing technologies**
- Future-proofing the data space through **quantum-resistant cryptographic methods**
- **Active participation in shaping international standards** for tools and regulations

Collaborative Networks

Collaborative Networks: Overview

AISEC is part of other consortia working together to develop solutions for the post-quantum era

BayQS

Other collaborative networks

Collaborative Networks: Overview

AISEC is part of other consortia working together to develop solutions for the post-quantum era

BayQS

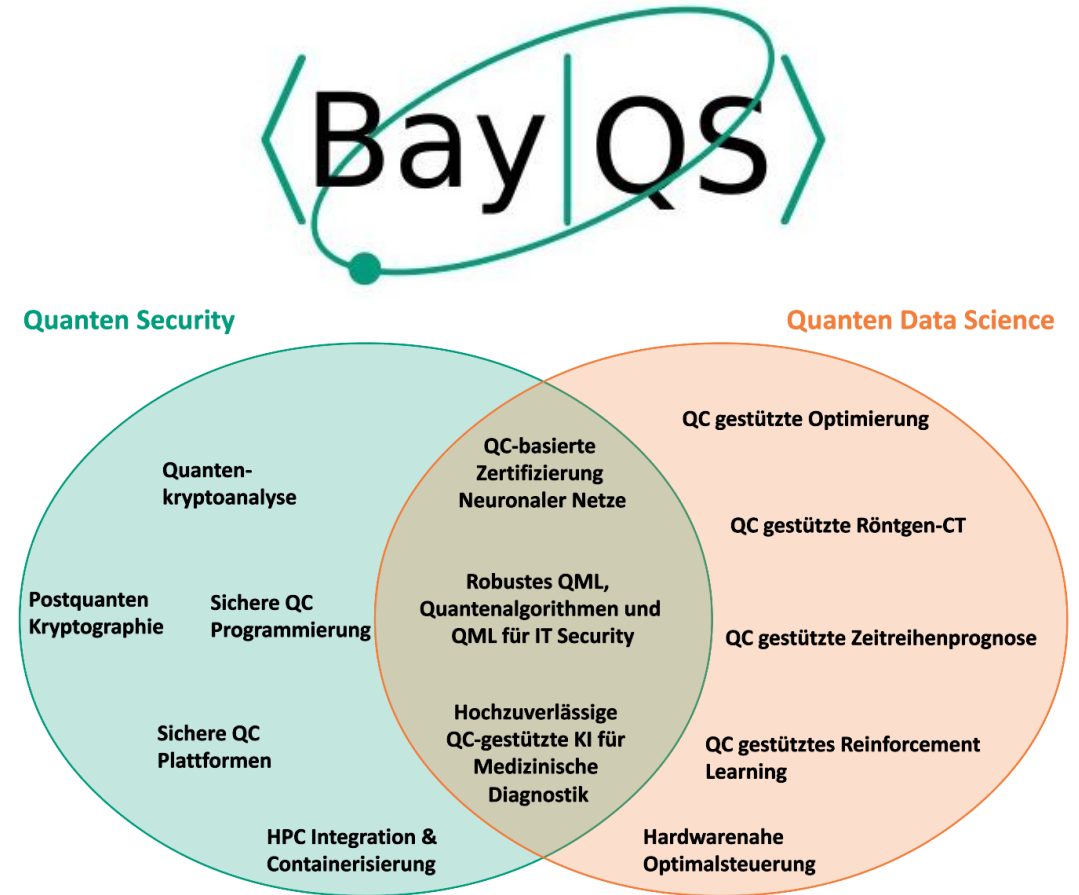
Other collaborative networks

Bavarian Competence Center for Quantum Security and Data Science (BayQS)

Development of fundamental concepts, solutions, and prototypes in quantum computing (QC)

Information and partners

- Partners:
 - Fraunhofer Institutes:
 - Fraunhofer AISEC (Applied and Integrated Security)
 - Fraunhofer IKS (Cognitive Systems)
 - Fraunhofer IIS (Integrated Circuits)
 - Academic partners:
 - Technische Universität München (TUM)
 - Ludwig-Maximilians-Universität München (LMU)
 - Leibniz-Rechenzentrum (LRZ)
 - Network affiliation:
 - Part of the Fraunhofer Quantum Computing Competence Network
 - Part of Munich Quantum Valley



Bavarian Center of Excellence for Quantum Security and Data Science (BayQS)

Development of fundamental concepts, solutions, and prototypes in quantum computing (QC)

Goals and Motivation

- **Goals:** Development and research of fundamental concepts, solutions, and prototypes for QC, and support for industry in identifying quantum advantages for practical problems. Focus on three key areas:
 - Secure QC Programming & Platforms
 - Robust QC
 - QC-based (hybrid) optimization
- **Motivation:** QC enables disruptive changes and new applications across many industries. BayQS establishes a scientific foundation to support the innovative capacity and technological sovereignty of the Bavarian economy.

Activities

- Development and evaluation of architectures for secure and robust QC applications
- Investigation of secure access concepts and execution environments for QC applications
- Research on security concepts for quantum algorithms and hybrid computational models
- QC-based optimization of systems (processes, materials, etc.)

Collaborative Networks: Overview

AISEC is part of other consortia working together to develop solutions for the post-quantum era

BayQS

Other collaborative networks

Other collaborative networks

Munich Quantum Valley and the Fraunhofer Quantum Computing Competence Network

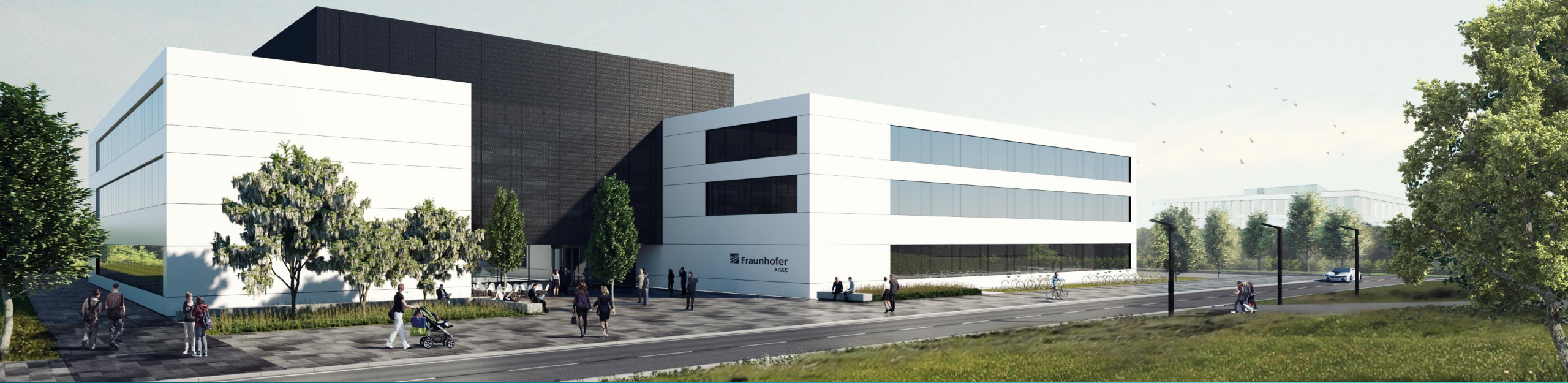
Munich Quantum Valley

- Coordination and management of the development, operation, and promotion of **competitive quantum computers**, as well as the **expansion of quantum technologies in Bavaria**.
- Research, education, and the practical application of **quantum science and technology**. Consolidation of activities by leading Bavarian research institutions and collaborations with companies.



Fraunhofer Quantum Computing Competence Network

- The national Fraunhofer network, consisting of regional centers of excellence, pursues a common goal: the **research and development of new technological solutions in the field of quantum computing**.
- It is dedicated to **building a quantum ecosystem** within the Fraunhofer Society as well as with partners and customers from research and industry.



Contact

Prof. Dr. Marian Margraf
Fraunhofer Institute for Applied and
Integrated Security AISEC
Breite Straße 12
14199 Berlin
marian.margraf@aisec.fraunhofer.de



Vcard Marian Margraf



[Subscribe to the
PQC Newsletter](#)



[Center of Excellence
for Post-Quantum
Cryptography](#)