

# Kompetenzzentrum für Post-Quanten Kryptografie

## Sales Deck

---

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

# Agenda

Sales Deck des Kompetenzzentrums Post-Quanten-Kryptografie am Fraunhofer AISEC

**Unsere Kernkompetenzen und Leistungen**

**Abgeschlossene Projekte**

**Aktuelle Projekte**

**Verbundnetzwerke**

# Unsere Kernkompetenzen und Leistungen

# Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)

## Zahlen & Fakten

- Gegründet: 2009
- Budget (inkl. Investitionen): 25,69 Mio. € (2025)
- Mitarbeitende: ca. 250
- Standorte: Garching bei München (Hauptsitz), Berlin, Weiden i.d. Oberpfalz
  
- Universitätsverbindungen:



© Fraunhofer AISEC



Prof. Dr. Eckert  
Prof. Dr. Sigl



Prof. Dr. Margraf  
Prof. Dr. Wunder



Prof. Dr. Loebenberger

»Das Fraunhofer AISEC überführt **exzellente IT-Sicherheitsforschung** in **anwendungsorientierte Lösungen** für mehr Zuverlässigkeit, Vertrauenswürdigkeit und Manipulationssicherheit von IT-basierten Systemen und Produkten.«

# Das Kompetenzzentrum Post-Quanten-Kryptografie am Fraunhofer AISEC

Von strategischer Beratung über technische Analyse bis zu aktivem Wissenstransfer

## Ziel

Sichere Migration von Unternehmen und Behörden hin zu quantencomputerresistenten IT-Systemen – herstellerneutral, praxisnah, forschungsbasiert.

## Ihr Mehrwert

- ✓ Herstellerunabhängige und praxisnahe Beratung
- ✓ Individuell zugeschnittene IT-Sicherheitsanalysen
- ✓ Exzellente Forschung als Grundlage für hochwertige technologische Lösungen
- ✓ Begleiteter Umstieg auf quantencomputerresistente Verfahren



# Das Kompetenzzentrum Post-Quanten-Kryptografie am Fraunhofer AISEC

## Unsere Kernkompetenzen

### Technologie- und Herstellerneutralität

Kombination aus aktueller Forschung und unabhängiger Beratung

### PQC-Migrationsstrategien

Entwicklung individueller Roadmaps zur sicheren Umstellung bestehender Systeme auf quantenresistente Verfahren

### Kryptoagilität

Design agiler IT-Sicherheitsarchitekturen, die austauschbare sichere kryptografische Verfahren ermöglichen



### IT-Sicherheitsanalysen

Umfängliche Analyse und Bewertung individueller Systemlandschaften hinsichtlich der eingesetzten Kryptografie

### Wissenstransfer & Schulungen

Vermittlung von Kryptografie- und PQC-Kenntnissen für Technik- und Managementebene in Seminaren und Community-Events

### Anwendungsnahe Forschung

Aktive Mitwirkung an BMBFR-Projekten, internationalen PQC-Gremien und Facharbeitskreisen

# Das Kompetenzzentrum Post-Quanten-Kryptografie am Fraunhofer AISEC

## Unsere Leistungen

### IT-Sicherheitsanalysen hinsichtlich der eingesetzten Kryptografie

- Analyse und Bewertung externer und interner Anwendungssicherheit
- Bewertung des kryptografischen Gesamtrisikos (Cryptographic Risk Assessment)
- Durchführung von Seitenkanal- und Fehlerangriffstests sowie Firmware-Analysen
- Auswahl geeigneter PQC-Lösungen für Ihre konkreten Sicherheits- und Performance-Anforderungen

### Unterstützung bei der Migration hin zu quantencomputerresistenter Kryptografie

- Individuelle Migrationsstrategien (Priorisierung kritischer Systeme, Hybrid-Ansätze, Roadmaps)
- Entwurf kryptoagiler Zielinfrastrukturen (Kryptografie wird leicht austauschbar/updatefähig)
- Technische Unterstützung bei der PQC-Implementierung in Software und Hardware

### Wissenstransfer

- [Datenbank pqdb](#): Überblick zu PQC-Verfahren (Sicherheitsniveau, NIST-Standardisierungsstatus, Effizienz)
- [Serious Game - Charlie und die Quantenfabrik](#): Spielerischer Einstieg in die Quantenwelt
- Beratung zu wissenschaftlichen Entwicklungen, aktueller Bedrohungslandschaft und Gegenmaßnahmen

# Das Kompetenzzentrum Post-Quanten-Kryptografie am Fraunhofer AISEC

## Unsere Leistungen

### Mitwirkung an BMBFR-Forschungsprojekten

- Gemeinsame Gestaltung der Zukunft der IT-Sicherheit mit Verbundpartnern aus Industrie und Forschung
- Beitrag zu exzellenten wissenschaftlichen Publikationen und Standardisierungsprozessen
- Praxisnaher Technologietransfer: von der Forschung direkt in reale Anwendungsszenarien

### Schulungen im Lernlabor Cybersicherheit

- [Seminarangebot des Fraunhofer AISEC](#): Schulungsformate für (quantencomputerresistente) Kryptografie, Kryptoagilität und PQC-Migration
- Stets aktuelle Inhalte, didaktisch fundiert aufbereitet von erfahrenen Referenten in Präsenz und Remote

### Community-Formate & Netzwerke

- Internationale PQC-Community für aktuellen Austausch
- Veranstaltung des jährlichen Netzwerktreffens „PQC-Update“ für Experten aus Forschung und Wirtschaft

# Abgeschlossene Projekte

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

**PoQsiKom**

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

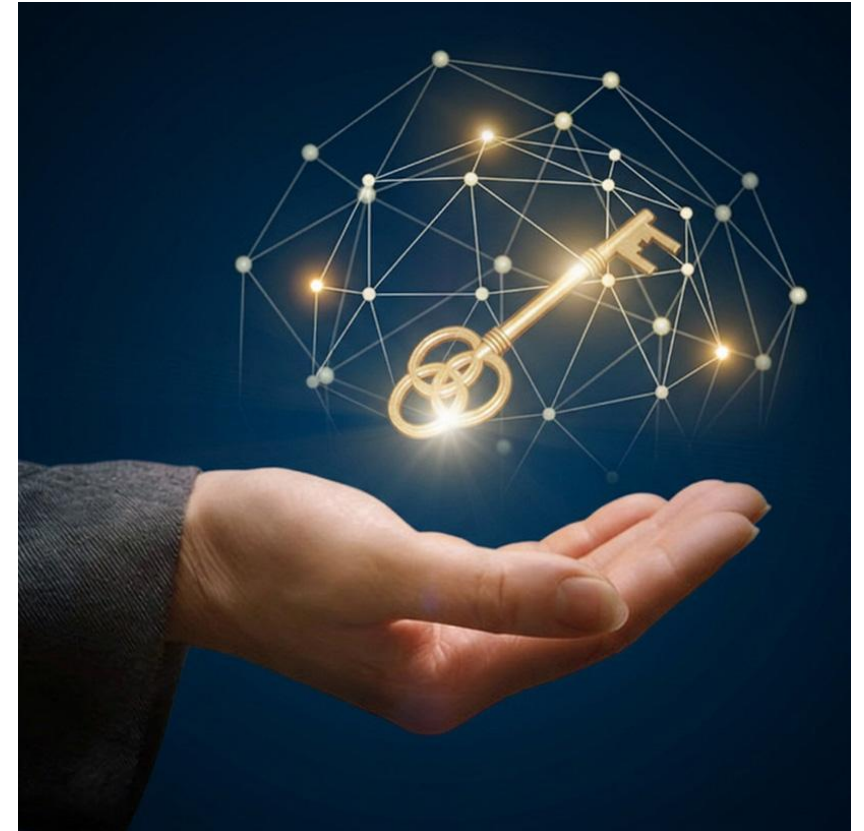
**PoQsiKom**

# Full-Lifecycle-Post-Quantum-PKI (FLOQI)

Entwicklung einer PQ-Wissensdatenbank, PQ-PKI Umsetzungsanalyse und Demonstratoren

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2019 - 2023
- Verbundpartner:
  - TU Berlin, Lehrstuhl SecT
  - 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)

Entwicklung einer PQ-Wissensdatenbank, PQ-PKI Umsetzungsanalyse und Demonstratoren

## Ziele und Motivation

- **Ziele:** Entwicklung einer quantencomputerresistenten PKI (PQ-PKI) mit Abwärtskompatibilität zu klassischen kryptografischen Verfahren am Beispiel der Automobilbranche und Industrie 4.0
- **Motivation:** Notwendigkeit langlebiger sicherer kryptografischer Verfahren in Produkten mit jahrzehntelangem Einsatz (z.B. Fahrzeug, Produktionsanlagen).  
Um Vertraulichkeit und Integrität heute und in einer Zukunft mit Quantencomputern zu gewährleisten, müssen aktuelle und quantencomputerresistente Verfahren im hybriden Einsatz eingesetzt werden.

## Vorgehen

- **Analyse quantencomputerresistenter Verfahren:** Auswahl geeigneter NIST-PQC-Algorithmen für den Einsatz in hybriden Zertifikaten und PQ-PKIs, Erstellung der Datenbank pqdb zum einheitlichen Vergleich der Verfahren
- **Konzeptionierung der Architektur:** Vergleich unterschiedlicher PQ-PKI-Umsetzungsvarianten, Anforderungsanalyse sowie Bewertung der Vor- und Nachteile
- **Implementierung:** Entwicklung von Demonstratoren in der Automobilbranche und Industrie 4.0 unter Berücksichtigung der spezifischen Anforderungen
- **Entwicklung eines Migrationskonzepts** für bestehende PKIs

# Full-Lifecycle-Post-Quantum-PKI (FLOQI)

Entwicklung einer PQ-Wissensdatenbank, PQ-PKI Umsetzungsanalyse und Demonstratoren

## Datenbank PQDB<sup>1</sup>

Bereitstellung einer öffentlichen Datenbank für post-quantenkryptografische Schlüsselaustausch- und Signaturverfahren



Schlüsselaustausch

z.B.: CRYSTALS-KYBER

Signaturen

z.B.: CRYSTALS-DILITHIUM

## PQ-PKI Umsetzungsvarianten (Var#)

- **Var1:** Hybride X.509-Zertifikate
- **Var2:** Mixed-PKI (PKI unterstützt klassische sowie PQ-Verfahren)
- **Var3:** Parallele PKIs (separate PKI jeweils für klassische und PQ-Verfahren)
- **Var4:** Intelligent Composed Algorithms (ICAs)<sup>2</sup> (Einbindung von in ICAs gekapselten kryptografischen Verfahren in bestehende Zertifikate)

## PQ-PKI Demonstratoren

**Demonstrator für Embedded Industrie 4.0:** Quantensichere Over-the-Air Firmware Updates für I4.0-Produkte

### Demonstratoren für Connected Vehicle:

- Quantensichere Authentifizierung der Steuergeräte (ECUs) bei WPAN-Gateway
- Quantensichere In-Vehicle- und Vehicle-to-Vehicle-Kommunikation zwischen ECUs

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

# Full-Lifecycle-Post-Quantum-PKI (FLOQI)

Entwicklung einer PQ-Wissensdatenbank, PQ-PKI Umsetzungsanalyse und Demonstratoren

## PQ-PKI Anforderungen

- **Zertifikathierarchie:** Root-CA, Sub-CAs, EE-Zertifikate
- **Gültigkeitsdauer:** CA-Zertifikate bis 20 Jahre, EE-Zertifikate zwischen 2 Wochen und 20 Jahren
- **Zertifikatsstandard:** X.509
- **Zertifikatsmanagementsystem**
- **Sicherheitsniveau**  $\geq$  128 Bits
- **Unterstützung:** in Hardware (z.B. HSM) und Protokollen (z.B. TLS)
- **Konformität** mit Regularien (BSI)

## Var1: Hybride Zertifikate

- Zertifikate unterstützen **klassische** sowie **PQ-Verfahren** und sind **abwärtskompatibel**
- Zur Gewährleistung der hybriden Kompatibilität müssen **Anpassungen** erfolgen:
  - In **PKI-Standards** (RFC5280, PKCS#10)
  - im **Zertifikatsmanagementsystem**
  - in **Hard- und Software** und Anwendungen
  - In der **Authentisierungsmethode** (Token-Verfahren)

## Var2: Mixed-PKI

- Root-CA benutzt **PQ-Signaturalgorithmus**, die untergeordneten CAs und EEs nicht zwingend
- **Gute Übergangslösung in der Transitionsphase:** einzelne Entitäten können nicht PQ-kompatibel sein, ohne damit die gesamte PKI zu gefährden

# Full-Lifecycle-Post-Quantum-PKI (FLOQI)

Entwicklung einer PQ-Wissensdatenbank, PQ-PKI Umsetzungsanalyse und Demonstratoren

## Var3: Parallele PKIs

- Zwei parallele PKI-Architekturen jeweils mit eigenem Zertifikatsmanagementsystem, Hard- und Softwarelösungen und Authentisierungsmethoden
- Eine Entität braucht zwei Zertifikate
- Anwendungen müssen definieren, wann und in welcher Reihenfolge die zwei Zertifikate der zwei PKIs verwendet werden

## Var4: Intelligent Composed Algorithms (ICAs)

- Intelligent Composed Algorithms (ICAs) umfassen kryptografische Algorithmen sowie Steueralgorithmen, die die Kombination der kryptografischen Algorithmen regeln.
- Klassische und PQ-Verfahren werden in ICAs gekapselt und nahtlos in bestehende Zertifikate eingebettet.
- Es müssen keine Änderungen an Zertifikaten vorgenommen werden. Steuerungsalgorithmen treten an Stelle der klassischen Algorithmen. Klassische und PQ-Verfahren werden kombiniert und zu hybriden Verfahren zusammengefasst.

# Full-Lifecycle-Post-Quantum-PKI (FLOQI)

Entwicklung einer PQ-Wissensdatenbank, PQ-PKI Umsetzungsanalyse und Demonstratoren

## Bewertung der PQ-PKI Umsetzungsvarianten

- Hybride Zertifikate (Var1) erfordern hohen Anpassungsaufwand, sind jedoch rückwärtskompatibel
- Die Mixed PKI-Infrastruktur (Var2) ermöglicht eine schrittweise PQC-Migration
- Die Verwaltung paralleler PKIs (Var3) ist sehr ressourcenintensiv und erfordert eine klare Regelung wie die zwei PKIs kombiniert werden sollen
- ICAs (Var4) schaffen eine hohe Flexibilität bei der Integration neuer Algorithmen (Kryptoagilität) und integrieren sich in bestehende Standards

## Fazit

Es gibt keine „one-fits-all“-Lösung: Auswahl abhängig von den spezifischen Gegebenheiten, Anforderungen und Rahmenbedingungen einer Organisation (Regularien, Ressourcen, Use Case)

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

**PoQsiKom**

# Kryptobibliothek Botan für langlebige Sicherheit (KBLS)

Erweiterung von Botan um PQ-Verfahren unter Wahrung von Kryptoagilität und Benutzbarkeit

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2019 - 2023
- Verbundpartner:
  - Fraunhofer AISEC
  - TU Berlin, Lehrstuhl SecT
  - neXenio GmbH
  - Rohde & Schwarz Cybersecurity GmbH



©Magnific / Fraunhofer AISEC

# Kryptobibliothek Botan für langlebige Sicherheit (KBLS)

Erweiterung von Botan um PQ-Verfahren unter Wahrung von Kryptoagilität und Benutzbarkeit

## Ziele und Motivation

- **Ziele:** Die Kryptobibliothek Botan soll durch die Integration von PQ-Verfahren erweitert werden. Die Implementierung dieser Verfahren soll effizient gestaltet werden, um auch in ressourcenbeschränkten Systemen nutzbar zu sein. Zudem soll die Bibliothek kryptoagil und leicht anwendbar sein. Die im Projekt entwickelten Ergebnisse sollen auch in anderen Kryptobibliotheken anwendbar sein.
- **Motivation:** Software-Entwickler:innen implementieren kryptographische Verfahren in der Regel nicht selbst, sondern setzen auf etablierte Kryptobibliotheken. Botan soll den einfachen und sicheren Einsatz von PQ-Kryptografie ermöglichen.

## Vorgehen

- **Analyse und Vergleich** quantencomputerresistenter Verfahren mittels der Datenbank pqdb (siehe Projekt „FLOQI“)
- **Kommunikation mit den Botan-Maintainern**, um kontinuierlich Erweiterungen abzustimmen, zu reviewen und in die offizielle Bibliothek einzuarbeiten
- **Durchführung von Usability-Tests** in Abstimmung mit Entwickler:innen

# Kryptobibliothek Botan für langlebige Sicherheit (KBLS)

Erweiterung von Botan um PQ-Verfahren unter Wahrung von Kryptoagilität und Benutzbarkeit

## Ergebnisse

- **Für Botan ausgewählte PQ-Verfahren:** Kyber (PQ-Schlüsseinigungsverfahren) und Dilithium (PQ-Signaturverfahren), da optimaler Trade-off zwischen Sicherheit und Performanz-Kriterien (Speicherbedarf, Rechenaufwand)
- **Entwerfen eines Usability-Konzepts** mit folgenden Angeboten für Entwickler:innen: Umfangreiche Dokumentationen mit Beispielen, Aussagekräftige Fehlermeldungen, Static Code-Review-Tool mit Fokus auf Seitenkanalresistenz
- **Implementierung** der ausgewählten PQ-Verfahren mit Maßnahmen für Seitenkanalresistenz und Kryptoagilität (z.B. einfacher Wechsel auf größere Schlüssellängen möglich)

## Fazit

- **Erweiterung:** Botan enthält neben klassischen Public-Key-Verfahren nun auch PQC-Verfahren
- **Einfache und sichere Anwendung** von PQC-Verfahren durch Entwickler:innen möglich
- **Kryptoagilität** erlaubt stetige Anpassungen der Bibliothek auf neue Erkenntnisse im Bereich PQC

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

**PoQsiKom**

# Post-Quanten-Kryptografie für hoheitliche Dokumente (PoQuID)

Quantencomputerresistente kryptografische Protokolle für hoheitliche Dokumente

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2020 - 2022
- Verbundpartner:
  - Bundesamt für Sicherheit in der Informationstechnik
  - Fraunhofer AISEC
  - Bundesdruckerei GmbH
  - Infineon Technologies AG



©Infineon

# Post-Quanten-Kryptografie für hoheitliche Dokumente (PoQuID)

## Quantencomputerresistente kryptografische Protokolle für hoheitliche Dokumente

### Ziele und Motivation

- **Ziele:** quantencomputerresistente Kommunikation zwischen elektronischem **Ausweisdokument** (ePass) und Inspektionssystem auf Basis eines PQ-Extended Access Control (EAC) Protokolls
- **Motivation:** Ein **elektronischer Chip** sichert die deutschen EU-Reisepässe und Personalausweise, mit denen sich Bürgerinnen und Bürger auch online authentisieren können. Die im Chip gespeicherten personenbezogenen Daten, biometrische Merkmale wie Passbild und Fingerabdrücke sowie ein Echtheitsnachweis müssen **auch im Zeitalter von Quantencomputern als Sicherheitsmerkmal genutzt** werden können.

### Vorgehen

- **Anforderungsanalyse und Auswahl** der PQ-Verfahren mittels der **Datenbank pqdb** (siehe Projekt „FLOQI“)
- **Entwicklung** von **hybriden** Authentifizierungs- und PKI-Lösungen für das **EAC-Protokoll**
- **Angriffsanalyse** insbesondere hinsichtlich Seitenkanälen mit Sicherheitsbeweisen
- **Umsetzung eines Demonstrators**, der eine PQ-sichere Authentifizierung eines ePasses bei einer Grenzkontrolle zeigt. Real-World-Validierung mit Tests
- **Technische Spezifikation** und Standardisierung

# Post-Quanten-Kryptografie für hoheitliche Dokumente (PoQuID)

## Quantencomputerresistente kryptografische Protokolle für hoheitliche Dokumente

### Ergebnisse

- **Für das PQ-EAC-Protokoll ausgewählte PQ-Verfahren:** Kyber (PQ-Schlüsseinigungsverfahren) und Dilithium (PQ-Signaturverfahren) (Empfehlung des BSI)
- **Entwicklung zweier PQ-EAC Varianten:**
  1. **SigPQEAC:** Authentifizierung mit PQ-Signaturen auf Basis von Dilithium
  2. **KemPQEAC:** Authentifizierung mit PQ-Schlüsseinigung auf Basis von Kyber (Vorteil: ressourceneffizient)
- **Entwicklung hybrider Schemata** durch Verwendung von klassischen und PQ-Verfahren in der Transitionsphase
- **Demonstrator:** Implementierung von SigPQEAC in einem Grenzkontrollscenario

### Fazit

- **Entwicklung und Implementierung** einer PQ-resistenten Version des für hoheitliche Dokumente verwendete Protokolls EAC<sup>1</sup>
- **Real-World Tests** zeigen eine hohe Effizienz der vorgeschlagenen Lösungen
- **Kryptoagilität:** Alternative Schlüsseinigungs- und Signaturverfahren können verwendet werden

<sup>1</sup>[https://link.springer.com/chapter/10.1007/978-3-031-30731-7\\_2](https://link.springer.com/chapter/10.1007/978-3-031-30731-7_2)

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

FLOQI

KBLS

PoQuID

Aquorypt

Laser-Fault-Injection-Angriff

QuaSiModO

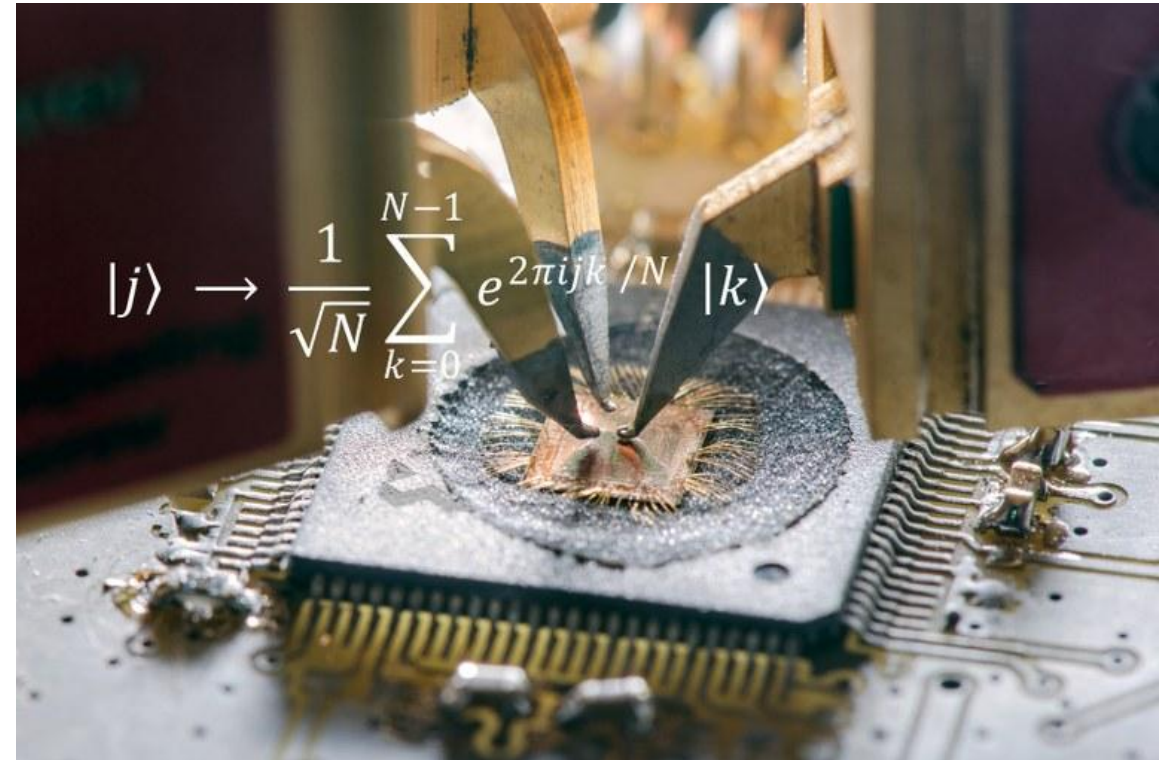
PoQsiKom

# Anwendbarkeit von PQC-Verfahren (Aquarypt)

PQC in industriellen eingebetteten Systemen und chipkartenbasierten Sicherheitsanwendungen

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2019 - 2023
- Verbundpartner:
  - Technische Universität München
  - Fraunhofer AISEC
  - Giesecke+Devrient Mobile Security GmbH
  - Infineon Technologies AG
  - Siemens AG
  - Technische Universität Darmstadt



© Andreas Heddergott / TU München

# Anwendbarkeit von PQC-Verfahren (Aquorypt)

PQC in industriellen eingebetteten Systemen und chipkartenbasierten Sicherheitsanwendungen

## Ziele und Motivation

- **Ziele:** Untersuchung der Anwendbarkeit von quantencomputerresistenten kryptografischen Verfahren in industriellen eingebetteten Systemen und chipkartenbasierten Sicherheitsanwendungen
- **Motivation:** Gewährleistung der Sicherheit eingebetteter Systeme und chipkartenbasierter Sicherheitsanwendungen im Zeitalter von Quantencomputern bei gleichbleibender Speichereffizienz und Performanz

## Vorgehen

- **Analyse und Vergleich** NIST-standardisierter PQC-Verfahren für den effizienten Einsatz in Hard- und Software
- **Implementierung** geeigneter PQC-Verfahren
- **Entwicklung von Migrationsstrategien** für die Umstellung bestehender Systeme auf quantencomputer-resistente Lösungen

# Anwendbarkeit von PQC-Verfahren (Aquorypt)

PQC in industriellen eingebetteten Systemen und chipkartenbasierten Sicherheitsanwendungen

## Ergebnisse

- Systematische **Vergleichsanalyse** geeigneter PQC-Verfahren für Hardwarebeschleuniger
- Untersuchung der **Auswirkungen von Seitenkanalangriffen auf Basis maschinellen Lernens** auf Hardwarebeschleuniger
- Entwicklung eines sicheren **Hardware-Software-Co-Designs eines PQC-Hardwarebeschleunigers** in FPGA-basierten Systemen
- Exemplarische Implementierung von **Gegenmaßnahmen zur Härtung von PQC-Implementierungen**
- Aufbau und Präsentation eines **Demonstrators** sowie Veröffentlichung mehrerer **wissenschaftlicher Arbeiten**

## Fazit

- **Quantencomputerresistente Krypto-Verfahren** können in **Hardwarebeschleunigern** implementiert werden
- Neben der Auswahl der geeigneten PQC-Algorithmen ist die **sichere Implementierung**, der **Schutz vor Seitenkanalangriffen** sowie eine **effiziente Software-Hardware-Architektur** entscheidend für den praktischen Einsatz
- Das Projekt liefert wichtige **Grundlagen, Demonstrationen und Handlungsempfehlungen** für die Migration bestehender Systeme zu quantensichereren kryptografischen Lösungen

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

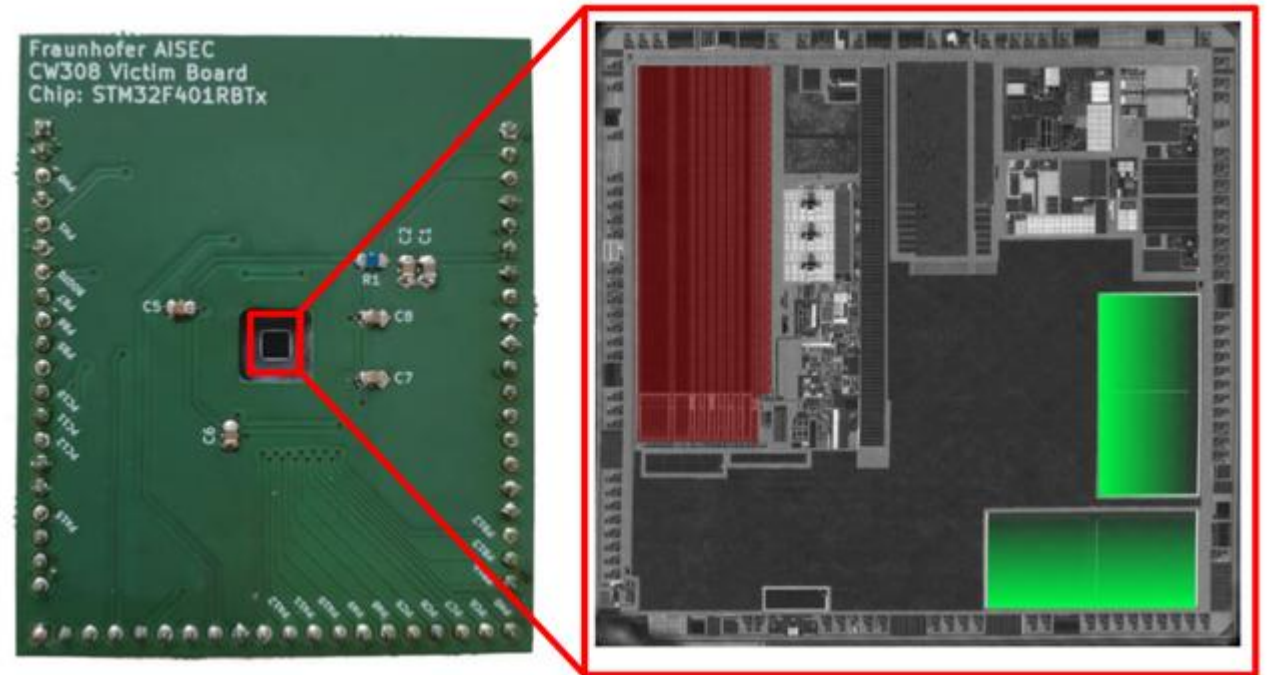
**PoQsiKom**

# Laser-Fault-Injection-Angriff auf hashbasierte Signaturverfahren

BSI-Studie zur Vorbereitung und Durchführung des Angriffs

## Infos und Verbundpartner

- Förderung: öffentlich (BSI)
- Laufzeit: 2024
- Umsetzung: Fraunhofer AISEC



© BSI

# Laser-Fault-Injection-Angriff auf hashbasierte Signaturverfahren

BSI-Studie zur Vorbereitung und Durchführung des Angriffs

## Ziele und Motivation

- **Ziele:** Untersuchung der praktischen Machbarkeit von Laser-Fault-Injection-Angriffen gegen das quantenresistente XMSS-Signaturverfahren in realen Implementierungen und Ableitung von Empfehlungen für sichere Implementierungen von hashbasierten Signaturverfahren in eingebetteten Systemen
- **Motivation:** Bewertung, ob postquantenresistente hashbasierte Signaturverfahren (z.B. XMSS) trotz mathematischer Sicherheit durch physische Hardwareangriffe wie Laser-Fault-Injection in realen Implementierungen kompromittiert werden kann

## Vorgehen

- **Angriffsziel:** Winternitz One-Time Signature (WOTS)-Verfahren, das ein zentraler Bestandteil von XMSS ist
- **Experimenteller Versuchsaufbau:** Implementierung von XMSS auf einem Standard-Mikrocontroller. Aufbau eines Laser-Angriffslabors
- **Angriffsmethode:** Erzeugung präziser Hardware-Fehler durch Laserimpulse in der Berechnung des Mikrocontrollers während der Signaturerstellung -> Angreifer kann Teile der WOTS-Schlüssel ableiten oder Signaturfälschungen erzeugen
- Nähere Informationen: [Download der BSI-Studie](#)

# Laser-Fault-Injection-Angriff auf hashbasierte Signaturverfahren

BSI-Studie zur Vorbereitung und Durchführung des Angriffs

## Ergebnisse

- **Praktische Durchführbarkeit:** Laser-Fault-Injection-Angriff auf hashbasierte Signaturen (XMSS, LMS, SPHINCS+) ist auf realer Hardware möglich. Dies stellt eine relevante Bedrohung für sicherheitskritische Infrastrukturgeräte, wie HSMs oder Smartcards, da.
- **Angriffsbedingungen:** physischer Zugriff auf das Gerät notwendig, Laser-Laboraüstung, hohe technische Expertise
- **Empfohlene Gegenmaßnahmen:** Neben sicherer Software auch gezielter Hardware-Schutz gegen Fault-Injection durch Fehlererkennung in Signaturverfahren und redundante Berechnungen

## Fazit

- Hashbasierte Signaturverfahren können durch physische Angriffe kompromittiert werden
- Der Laser-Fault-Injection-Angriff kann Fehler in der Signaturerzeugung provozieren, die zur Schlüsselrekonstruktion oder Signaturfälschung führen können
- Signatur-Sicherheit ist neben der sicheren Softwareimplementierung stark abhängig von der Hardware-Härtung gegen physische Angriffe

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

**PoQsiKom**

# Quanten-Sichere VPN-Module und –Operationsmodi (QuaSiModO)

Quantensichere virtuelle private Netzwerke

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2019 - 2022
- Verbundpartner:
  - genua GmbH, Kirchheim
  - ADVA Network Security GmbH, Planegg
  - Ludwig-Maximilians-Universität München
  - Fraunhofer AISEC, Weiden i. d. Opf.



©Magnific / Fraunhofer AISEC

# Quanten-Sichere VPN-Module und –Operationsmodi (QuaSiModO)

## Quantensichere virtuelle private Netzwerke

### Ziele und Motivation

- **Ziele:** Integration quantenresistenter Algorithmen in VPN-Standards und -Implementierungen auf den Schichten 2 und 3 des TCP/IP-Referenzmodells. Fokus auf die PQ-Anpassung von IKEv2 in IPsec auf Ebene 3.
- **Motivation:** Gewährleistung der VPN-Sicherheit gegen Angriffe durch leistungsfähige Quantencomputer

### Vorgehen

- **Auswahl und Analyse** geeigneter PQC-Algorithmen basierend auf praktischen Anforderungen
- **Entwicklung hybrider Ansätze** für das Schlüsseleinigungsverfahren im MACsec- (Schicht 2) sowie IPsec-Protokoll (Schicht 3)
- **Implementierung** von Schemata in etablierten VPN-Software-Suiten
- **Sicherheitsanalyse** der Protokolle sowie der Implementierungen
- Austausch in internationalen **Standardisierungsgremien**

# Quanten-Sichere VPN-Module und VPN-Operationsmodi (QuaSiModO)

## Quantensichere virtuelle private Netzwerke

### Ergebnisse

- **Entwicklung quantensicherer Erweiterungen** für das Schlüsseleinigungsverfahren im MACsec- (Schicht 2) sowie IPsec-Protokoll (Schicht 3)
- **Mitwirkung an Internet Drafts** internationaler Standardisierungsgremien

### Fazit

- **Beitrag** zur Schaffung **robuster und zukunftssicherer VPN-Standards**

# Abgeschlossene Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**FLOQI**

**KBLS**

**PoQuID**

**Aquorypt**

**Laser-Fault-Injection-Angriff**

**QuaSiModO**

**PoQsiKom**

# Post-Quanten-sichere Kommunikation für Industrie 4.0 (PoQsiKom)

PQ-sichere Kommunikation für Industrie 4.0 mit international standardisierten Vertrauensankern

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2021 - 2024
- Verbundpartner:
  - Fraunhofer AISEC
  - Technische Universität München
  - Siemens
  - TRUMPF Werkzeugmaschinen GmbH



# Post-Quanten-sichere Kommunikation für Industrie 4.0 (PoQsiKom)

PQ-sichere Kommunikation für Industrie 4.0 mit international standardisierten Vertrauensankern

## Ziele und Motivation

- **Ziele:** Entwicklung einer Industrie 4.0-Plattform zur Durchführung einer sicheren und vertrauenswürdigen Quittierung von Sicherheitseinrichtungen aus der Ferne. Dies ermöglicht eine Remote-Echtzeitüberwachung sowie Remote-Bestätigung von Sicherheitszuständen, wodurch die Reaktionszeit verkürzt werden kann.
- **Motivation:** Die zunehmende Vernetzung und der Austausch von Daten über Vertrauensgrenzen hinweg erfordern robuste Sicherheitslösungen, die über traditionelle Authentifizierungsmethoden hinausgehen. Angesichts der Bedrohungen durch Quantencomputer ist es entscheidend, langfristige Sicherheitsstandards zu etablieren.

## Vorgehen

- **Definition der Anforderungen und Systemarchitektur** der Industrieplattform (Betriebssystem, Vertrauensanker, ...)
- **Entwicklung eines Vertrauensankers** auf Basis des Open-Source Sicherheitschips OpenTitan mit Hardware-Beschleunigern für die Post-Quantum-Krypto-Algorithmen Dilithium und Falcon
- **Anbindung des Vertrauensankers** an die Industrie-Plattform mittels der Generic Trust Anchor (GTA) API
- **Analyse geeigneter Kommunikationsprotokolle sowie Authentifizierungsmethoden** für die Fernquittierung u.a. QUIC, BRSKI, MFA
- Integration der Systembausteine in einen **Plattform-Demonstrator**

# Post-Quanten-sichere Kommunikation für Industrie 4.0 (PoQsiKom)

PQ-sichere Kommunikation für Industrie 4.0 mit international standardisierten Vertrauensankern

## Ergebnisse

- **Veröffentlichung der Projektergebnisse** auf wissenschaftlichen Konferenzen und als Open-Source-Projekte (mehr Infos unter <https://poqsikom.de/>)
- **Mitwirkung in dem DIN NA 043-01-41-02 Arbeitskreis** „Generische Anwendungs-Programmierschnittstelle für IoT- und Industriegeräte“ zur Standardisierung der GTA-API
- **Prototypische Umsetzung** der Projektergebnisse in Form eines Demonstrators und Präsentation auf der Hannovermesse 2024
- **Kooperation mit einem koreanischen Schwesterprojekt** zur Integration der nationalen Demonstratoren, einschließlich der Anbindung des koreanischen Krypto-Moduls an den deutschen Demonstrator

## Fazit

- **Wesentliche Fortschritte** in der Entwicklung sicherer Kommunikationslösungen für die Industrie 4.0.
- **AISEC-Demonstrator** dient als anschauliches Beispiel für sichere Fernquittierung und sensibilisiert Unternehmen sowie Studierende für Post-Quanten-Sicherheit und Safety in industriellen Umgebungen

# Aktuelle Projekte

# Aktuelle Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**PARFAIT**

**AMiQuaSy**

**TRUSTED**

# Aktuelle Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**PARFAIT**

**AMiQuaSy**

**TRUSTED**

# Post-Quanten-Kryptografie für Automotive-Komponenten (PARFAIT)

Einsatz von Post-Quanten-Kryptografie und Kryptoagilität im Automobilbereich

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2024 - 2027
- Verbundpartner:
  - Infineon Technologies AG
  - DENSO AUTOMOTIVE Deutschland GmbH
  - Vitesco Technologies Germany GmbH
  - Fraunhofer AISEC
  - Freie Universität Berlin
  - Hochschule Darmstadt
  - Hochschule RheinMain
  - Technische Universität Darmstadt



# Post-Quanten-Kryptografie für Automotive-Komponenten (PARFAIT)

Einsatz von Post-Quanten-Kryptografie und Kryptoagilität im Automobilbereich

## Ziele und Motivation

- **Ziele:** Etablierung von Post-Quanten-Kryptografie (PQC) und Kryptoagilität im Automobilbereich
- **Motivation:** PQC und Kryptoagilität unterstützen die Umsetzung der UNECE R155-Richtlinie zur Gewährleistung von Langzeitsicherheit von Fahrzeugzulassungen

## Vorgehen

- **Identifizierung von Anforderungen**, die sich für Automotive-Anwendungen ergeben
- **Durchführung von Bedrohungsanalysen**
- **Analyse und Vergleich** der im NIST-standardisierten PQC-Verfahren für den Einsatz in Automotive-Komponenten unter den Aspekten Performance, Speicherbedarf, Robustheit
- **Entwicklung hybrider Ansätze** und geeigneter Migrationsstrategien mit praktischer Demonstration
- **Erweiterung der Automotive-Protokollen** hinsichtlich PQC und Kryptoagilität

# Aktuelle Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**PARFAIT**

**AMiQuaSy**

**TRUSTED**

# Agile Migration auf quantenresistente Systeme (AMiQuaSy)

Sichere Softwareentwicklung in der Post-Quanten-Welt

## Infos und Verbundpartner

- Förderung: öffentlich
- Laufzeit: 2023 - 2026
- Verbundpartner:
  - Xitaso GmbH IT & Software Solutions, Augsburg
  - genua GmbH, Kirchheim
  - Ostbayerische Technische Hochschule Amberg-Weiden, Amberg
  - Fraunhofer AISEC, Weiden i.d.Opf.



©Magnific / Fraunhofer AISEC

# Agile Migration auf quantenresistente Systeme (AMiQuaSy)

## Sichere Softwareentwicklung in der Post-Quanten-Welt

### Ziele und Motivation

- **Ziele:** Entwicklung agiler Sicherheitsmechanismen, mit denen **kryptografische Verfahren leicht gegen neue sichere Verfahren ausgetauscht** werden können (Kryptoagilität)
- **Motivation:** Kryptografische Verfahren müssen in Zukunft schnell **austauschbar** sein, um auf eine **sich ständig ändernde Bedrohungslandschaft** mit minimalem Risiko und geringer Ausfallzeit reagieren zu können

### Vorgehen

- Austausch mit Industrie und Forschung zur **Erfassung praxisnaher Anforderungen** und aktueller Migrationshemmnisse
- Untersuchung verschiedener **Migrationsszenarien** und Entwicklung technischer **Umsetzungsansätze**
- Erarbeitung eines LLM-basierten Ansatzes zur **semi-automatischen Identifikation kryptografischer Softwarepakete**
- Entwicklung einer IT-Sicherheit-fokussierten Architecture-Tradeoff-Analyse-Methode (SATAM), um aus IT-Architekturen **Cryptographic Bills of Materials (CBOMs)** abzuleiten, sodass die kryptografische Migrationsplanung **in einen architektonischen Kontext** gebracht wird

# Aktuelle Projekte: Übersicht

Analyse, Konzeptionierung und Umsetzung sicherer Lösungsansätze für die Post-Quanten-Ära

**PARFAIT**

**AMiQuaSy**

**TRUSTED**

# Enabling Trustworthy European Data Spaces (TRUSTED)

Vertrauenswürdiger europäischer Datenraum für personenbezogene Daten

## Infos und Verbundpartner

- Förderung: öffentlich (Europäische Kommission)
- Laufzeit: 2025 - 2028
- Verbundpartner:
  - Gradient
  - Tree Technology, Fundación Cibervoluntarios (Spanien)
  - Infocert SPA, Cybersocial Lab, Fondazione Mondo Digitale (Italien)
  - Fraunhofer AISEC, Fraunhofer ISST (Deutschland)
  - Promptly, Centro Hospitalar Universitário de Coimbra (Portugal)
  - Sestek (Türkei)



© Gradient

# Enabling Trustworthy European Data Spaces (TRUSTED)

Vertrauenswürdiger europäischer Datenraum für personenbezogene Daten

## Ziele und Motivation

- **Ziele:** Aufbau eines vertrauenswürdigen Datenraums, der KI-Anwendungen auf personenbezogene Daten durch Privacy Enhancing Technologies sowie ein KI-gestütztes Identitäts- und Berechtigungsmanagement für selbstverwaltete Identitäten ermöglicht.
- **Motivation:** Innovationen auf Basis von KI schaffen wertvolle Fortschritte, z.B. in der Medizin. Um KI-Methoden vertrauenswürdig auf personenbezogene Daten anzuwenden, muss sichergestellt werden, dass Nutzerinnen und Nutzer die Kontrolle über ihre verwendeten Daten behalten.

## Vorgehen

- **Analyse bestehender Technologien für Self Sovereign Identities** und Definition der Anforderungen an einen vertrauenswürdigen Datenraum
- **Entwicklung und Integration von Privacy Enhancing Technologies**
- Zukunftsorientierte Absicherung des Datenraums durch **quantenresistente kryptografische Verfahren**
- **Aktive Mitgestaltung von internationalen Standards** für Tools und Regelwerke

# Verbundnetzwerke

# Verbundnetzwerke: Übersicht

Das AISEC ist Teil weiterer Konsortien, um gemeinsam Lösungen für die Post-Quanten-Ära zu schaffen

**BayQS**

**Weitere Verbundnetzwerke**

# Verbundnetzwerke: Übersicht

Das AISEC ist Teil weiterer Konsortien, um gemeinsam Lösungen für die Post-Quanten-Ära zu schaffen

**BayQS**

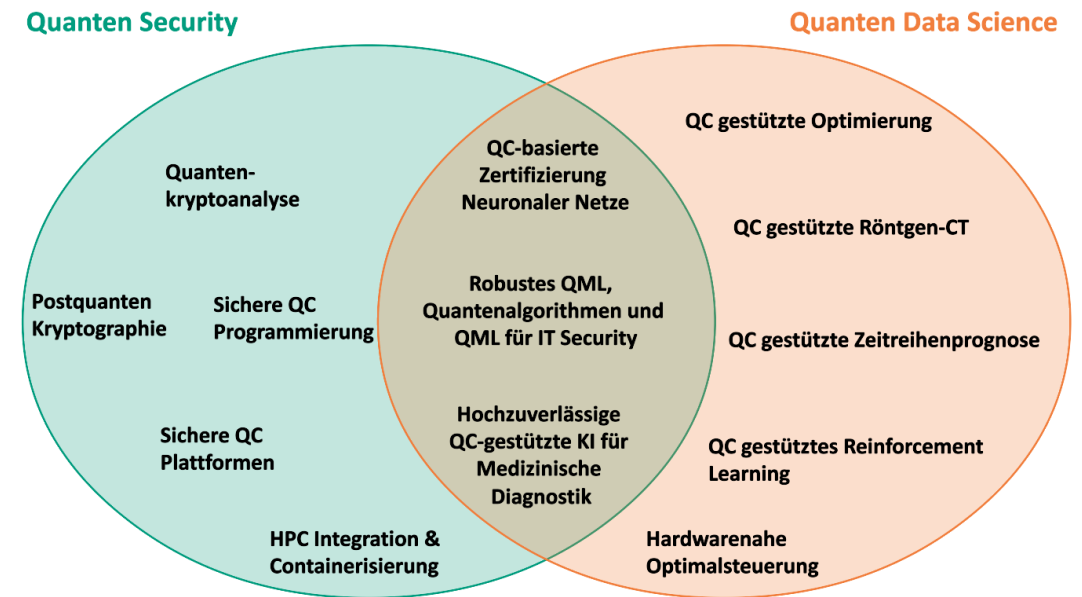
**Weitere Verbundnetzwerke**

# Bayerisches Kompetenzzentrum Quanten Security und Data Science (BayQS)

Entwicklung von Grundlagenkonzepten, Lösungen und Prototypen im Quantencomputing (QC)

## Infos und Verbundpartner

- Verbundpartner:
  - Fraunhofer-Institute:
    - Fraunhofer AISEC (Angewandte und Integrierte Sicherheit)
    - Fraunhofer IKS (Kognitive Systeme)
    - Fraunhofer IIS (Integrierte Schaltungen)
  - Akademische Partner:
    - Technische Universität München (TUM)
    - Ludwig-Maximilians-Universität München (LMU)
    - Leibniz-Rechenzentrum (LRZ)
  - Netzwerkanbindung:
    - Teil des Fraunhofer-Kompetenznetzwerks Quantencomputing
    - Teil des Munich Quantum Valley



# Bayerisches Kompetenzzentrum Quanten Security und Data Science (BayQS)

Entwicklung von Grundlagenkonzepten, Lösungen und Prototypen im Quantencomputing (QC)

## Ziele und Motivation

- **Ziele:** Entwicklung und Erforschung von Grundlagenkonzepten, Lösungen und Prototypen für QC und Unterstützung der Industrie bei der Identifikation von Quantenvorteilen für praxisrelevante Probleme. Fokus auf drei Themenschwerpunkte:
  - Sichere QC-Programmierung & Plattformen
  - Robustes QC
  - QC-gestützte (hybride) Optimierung
- **Motivation:** QC ermöglicht disruptive Veränderungen und neue Anwendungen in vielen Branchen. BayQS schafft eine wissenschaftliche Grundlage zur Unterstützung der Innovationsfähigkeit und technologischen Souveränität der bayerischen Wirtschaft.

## Aktivitäten

- Entwicklung und Evaluation von Architekturen für sichere und robuste QC-Anwendungen
- Untersuchung sicherer Zugangskonzepte und Ausführungsumgebungen für QC-Anwendungen
- Forschung an Sicherheitskonzepten für Quantenalgorithmen und hybride Berechnungsmodelle
- QC-basierte Optimierung von Systemen (Prozesse, Materialien, etc.)

# Verbundnetzwerke: Übersicht

Das AISEC ist Teil weiterer Konsortien, um gemeinsam Lösungen für die Post-Quanten-Ära zu schaffen

**BayQS**

**Weitere Verbundnetzwerke**

# Weitere Verbundnetzwerke

## Munich Quantum Valley und das Fraunhofer Kompetenznetzwerk Quantencomputing

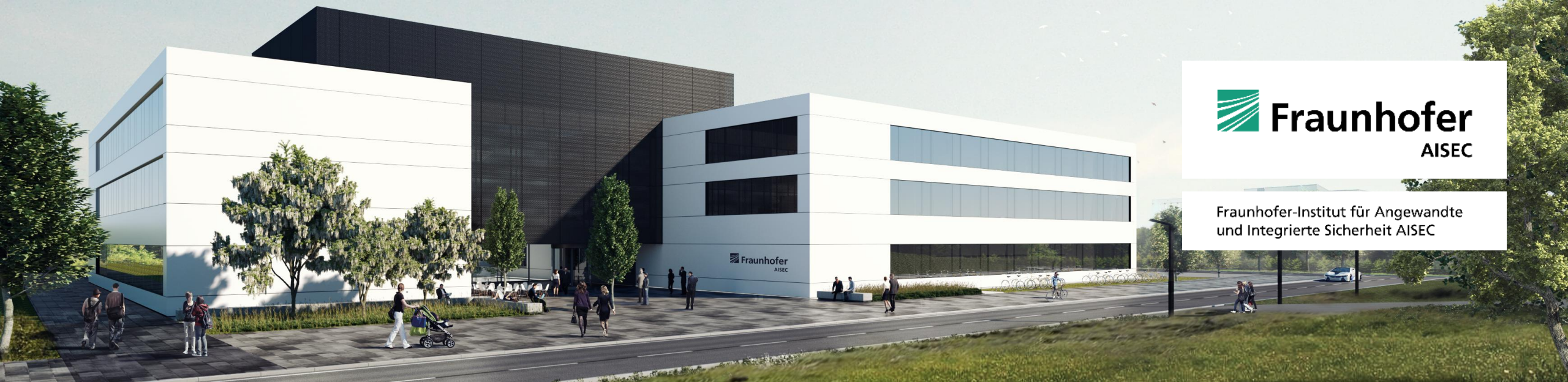
### Munich Quantum Valley

- Koordination und Steuerung der Entwicklung, des Betriebs und der Förderung **wettbewerbsfähiger Quantencomputer** sowie des **Ausbaus von Quantentechnologien in Bayern**.
- Forschung, Ausbildung und Transfer von **Quantenwissenschaft und -technologie** in die Praxis. Bündelung der Aktivitäten führender bayerischer Forschungsinstitutionen und Kooperationen mit Unternehmen.



### Fraunhofer Kompetenznetzwerk Quantencomputing

- Das nationale Fraunhofer-Netzwerk bestehend aus regionalen Kompetenzzentren verfolgt ein gemeinsames Ziel: Die **Erforschung und Entwicklung** von neuen technologischen **Lösungen auf dem Gebiet des Quantencomputings**.
- Es steht für den **Aufbau eines Quantenökosystems** innerhalb der Fraunhofer-Gesellschaft wie auch mit Partnern und Kunden aus Forschung und Industrie.



 **Fraunhofer**  
AISEC

Fraunhofer-Institut für Angewandte  
und Integrierte Sicherheit AISEC

# Kontakt

---

Prof. Dr. Marian Margraf  
Fraunhofer-Institut für Angewandte und  
Integrierte Sicherheit AISEC (Standort Berlin)  
Breite Straße 12  
14199 Berlin  
[marian.margraf@aisec.fraunhofer.de](mailto:marian.margraf@aisec.fraunhofer.de)



[Vcard Marian Margraf](#)



[Anmeldung zum  
POC-Newsletter](#)



[Kompetenzzentrum  
Post-Quanten-  
Kryptografie](#)