
BWI
IT für Deutschland

BWI
IT für Deutschland

BWI INDUSTRY DAYS

Gemeinsam für eine resiliente IT-Zukunft

8. bis 9. August 2023, Berlin

Bildquelle: BWI/Herdieckerhoff

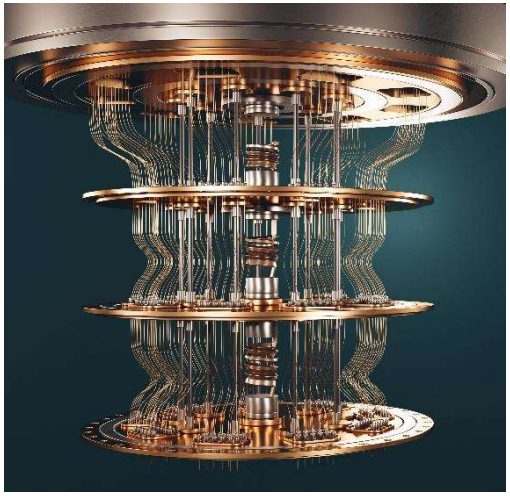
Sicher kommunizieren im Quanten-Zeitalter

Wie gelingt die Migration zu quantensicherer Kryptographie?

Adobe Stock/Digilife/267403235

01. Quantencomputer als Bedrohung der IT-Sicherheit

Gedankenexperiment: 10 Jahre in die Zukunft…



Leistungsfähige Quantencomputer existieren

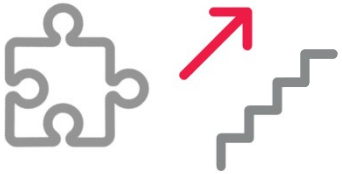
Staaten nutzen Quantencomputer, um IT-Systeme zu kompromittieren

Daten werden in großem Stil entschlüsselt Authentisierungsverfahren sind nicht mehr sicher

Risikoeinschätzung aus zwei Perspektiven

Verfügbare Quantenalgorithmen („Kochrezept“)

+



Technologischer Fortschritt bei Quantencomputern („Zutaten“)

=

Kryptographisch relevanter Quantencomputer

Breaking 256-bit Elliptic Curve Encryption with a Quantum Computer

Researchers have calculated the quantum computer size necessary to break 256-bit elliptic curve public-key cryptography:

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

IBM Extends Roadmap Up to 4,158 Qubits Using Multiprocessing and Advanced Software

Digitales Wettrüsten: Sicherheitsexperten halten praxistaugliche Quantencomputer ab 2030 für möglich

Technology

Cryptographers bet cash on when quantum computers will beat encryption

IBM Extends Roadmap Up to 4,158 Qubits Using Multiprocessing and Advanced Software - Quantum Computing Report
How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits – Quantum (quantum-journal.org)
Breaking 256-bit Elliptic Curve Encryption with a Quantum Computer - Schneier on Security
Bundeswehr erwartet praxistaugliche Quantencomputer ab 2030 (ga.de) | www.flaticon.com)

Konsequenz: Alle heute eingesetzten Verfahren der asymmetrischen Kryptographie werden gebrochen

Asymmetrische Kryptographie

Schlüsselpaar

Heute eingesetzte Verfahren sind nicht quantenresistent

RSA, Diffie-Hellman (DH), elliptische Kurven (ECC) werden vollständig gebrochen

Vertraulichkeit

Authentizität

Benötigt: Neue Verfahren für

- Schlüsselaustausch / Schlüsselverteilung
- Signaturen

Zeitskala bis zum Eintritt der Bedrohung durch Quantencomputer

„Das BSI handelt […] für den Hochsicherheitsbereich unter der Arbeitshypothese, dass kryptografisch relevante Quantencomputer **Anfang der 2030er-Jahre** zur Verfügung stehen.“

BSI (2020/2021)

Kryptografie quantensicher gestalten

Wege zu quantensicheren Lösungen

1. Schlüssel vergrößern

- ✓ Vergleichsweise einfach
- ✓ Effektiv bei AES (symmetrischer Verschlüsselung)
- x Keine Lösung für asymmetrische Kryptographie

2. Post-Quantum Cryptography (PQC)

- ✓ **Sicherheit durch (neue) mathematische Algorithmen**
- ✓ Fortgeschrittene F&E. Erste Migration in der Praxis
- ✓ Verfügbarkeit von Algorithmen für Schlüsseleinigung und Signaturen
- x Qual der (Algorithmen-)Wahl

3. Quantum Key Distribution (QKD)

- ✓ **Sicherheit durch Physik** statt durch Algorithmen
- x Spezielle Einsatzbereiche (Hochsicherheitsbereich, Militär)
- x Benötigt neuartige Hardware
- x Noch nicht ausgereift

Lucie Kogelheide
Technology Lead PQC

Dr. Maja Kierdorf
Technology Lead QKD

02. Post-Quantum Cryptography (PQC)

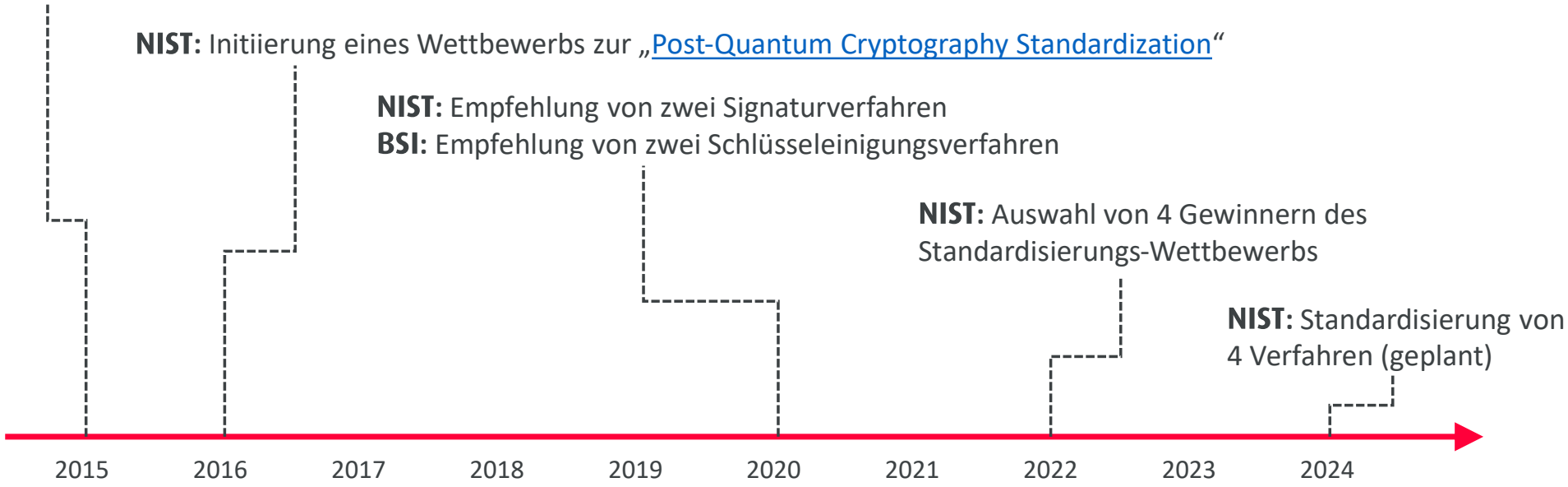
Wir benötigen **Ersatzkandidaten** für heute eingesetzte asymmetrische kryptographische Verfahren

- Sicher gegen klassische Angreifer und gegen Quanten-Angreifer
  → Shor-Algorithmus nicht anwendbar
  → Weitere Quantenalgorithmen nicht anwendbar
  → Angriffe mit klassischen Computern nicht anwendbar
- Ersatz für Signatur- und Schlüsseleinigungsverfahren
- Zeitnah verfügbar
- Lauffähig auf klassischer Hardware

→ Post-Quanten-Kryptographie (PQC)

Zeitleiste PQC-Standardisierung

NSA: "…we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."



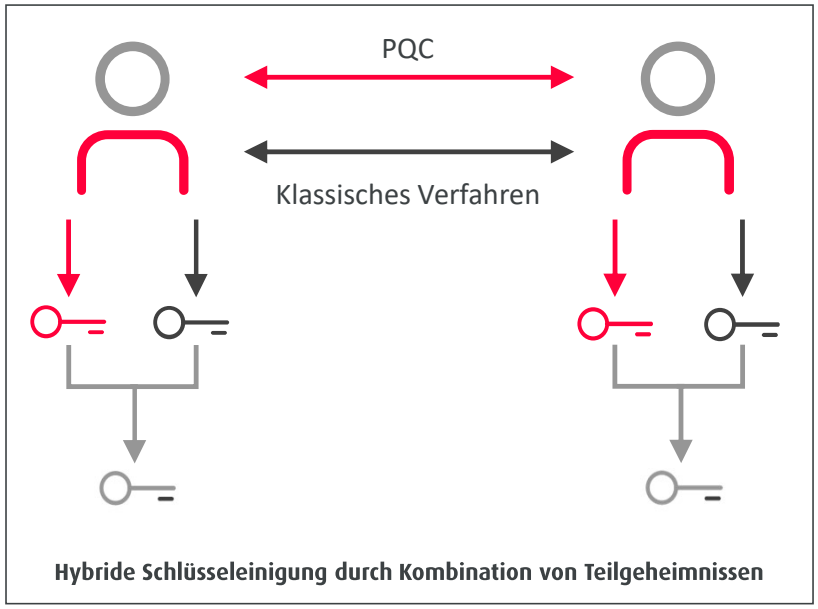
→ Post-Quanten-Kryptographie ist heute verfügbar

PQC-Algorithmen sind heute verfügbar

	Verfahren	PQC-Familie
 Schlüsseleinigung	CRYSTALS-Kyber	Gitter-basiert
	Classic McEliece	Code-basiert
	FrodoKEM	Gitter-basiert
 Signaturen	CRYSTALS-Dilithium	Gitter-basiert
	Falcon	Gitter-basiert
	XMSS	Hash-basiert Zustandsbehaftet
	LMS	Hash-basiert Zustandsbehaftet
	SPHINCS+	Hash-basiert Nicht zustandsbehaftet

Bundesamt für Sicherheit in der Informationstechnik

Die Zukunft ist hybrid und kryptoagil



Hybride Schlüsseleinigung durch Kombination von Teilgeheimnissen

„Kryptoagilität sollte […] – unabhängig von der Entwicklung von Quantencomputern – zum Designkriterium für neue Produkte werden.“

BSI (2020): Migration zu Post-Quanten-Kryptografie

Der **Erfolg der PQC-Migration** entscheidet sich heute

PQC-Algorithmen sind keine „Plug-and-play“-Lösungen → Die Zeit rennt ← Umbau einer komplexen IT-Infrastruktur dauert 5-15 Jahre

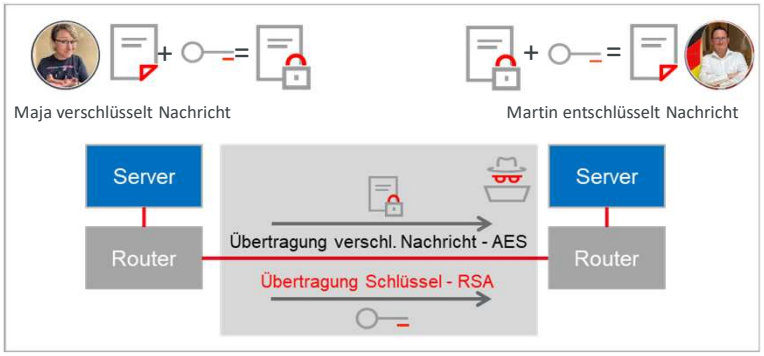
BWI Vision

„Wir sorgen für die digitale Zukunftsfähigkeit unseres Landes.“

03. Quantum Key Distribution (QKD)

Das **Prinzip** von QKD

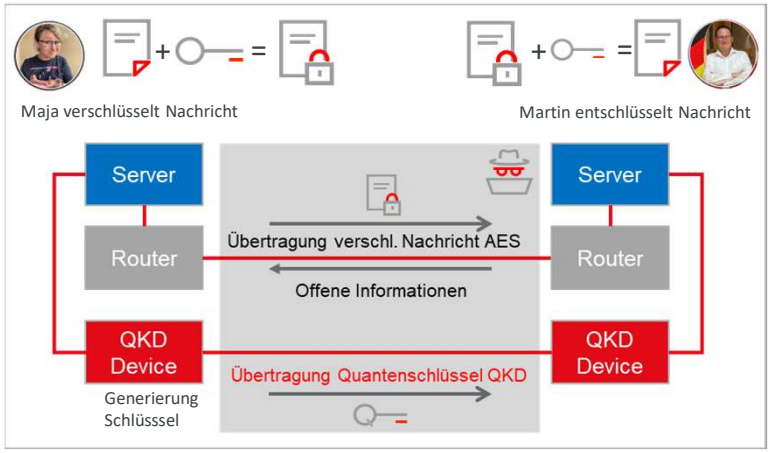
Klassisches Verfahren



Verschlüsselung ohne QKD

- Verschlüsselung mit symmetrischem Algorithmus (AES)
- Problem: unsichere Schlüsselübermittlung – Eve hört ab

QKD



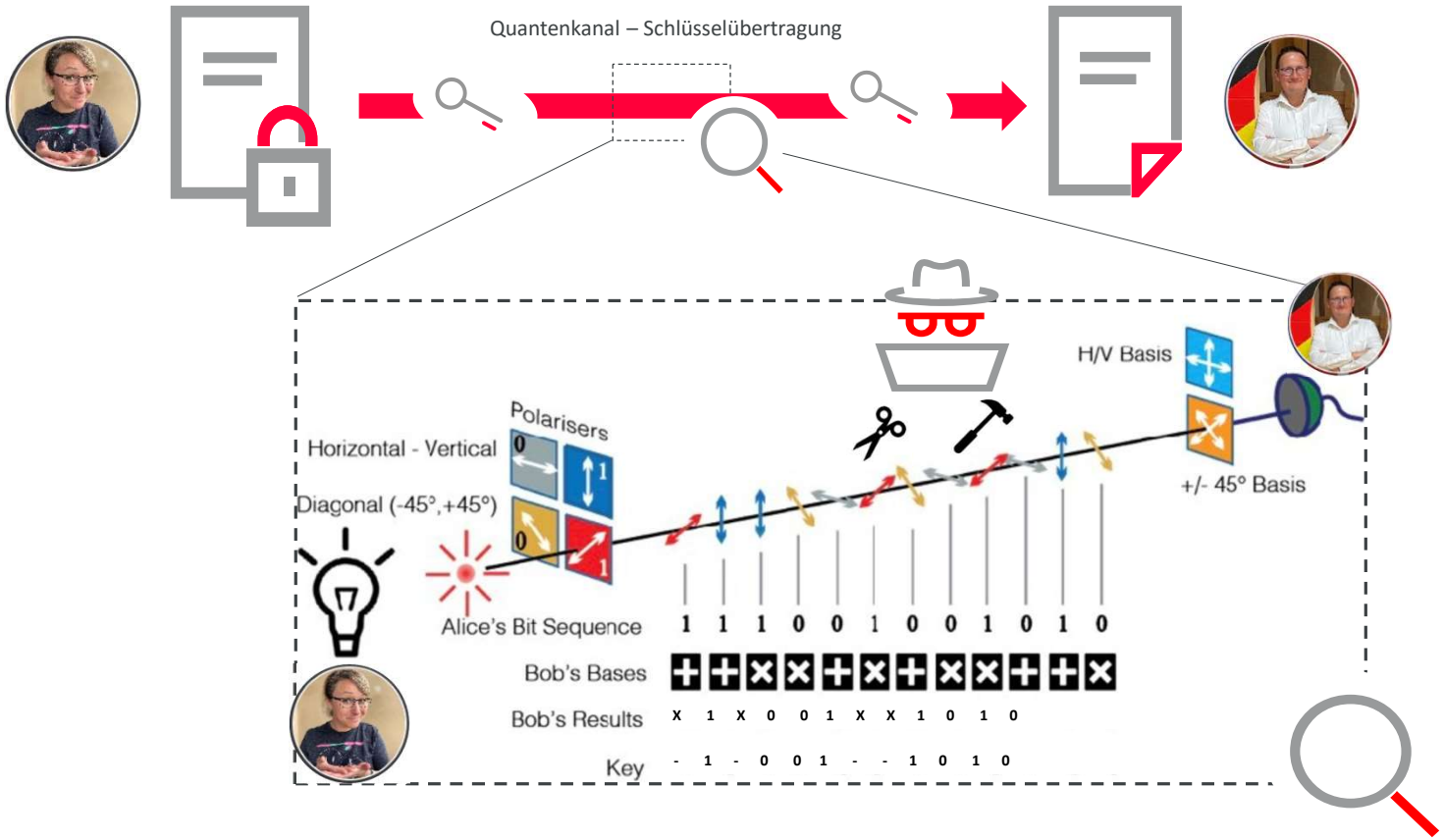
Lösung:

- Sichere Schlüsselübermittlung über QKD
- Bei Eingriffsversuch von Eve bricht Schlüsselübertragung ab und ein neuer Schlüssel wird erzeugt

Bildquelle: https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd

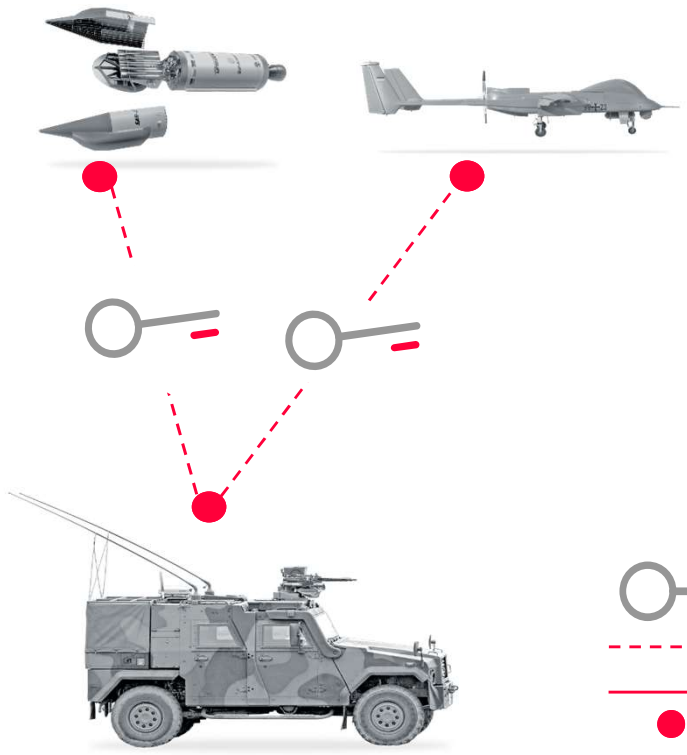
QKD Funktionsweise

Sichere Kommunikation auf Basis physikalischer Gesetze



Bildquelle: https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd

Einsatzszenarien von QKD



BWI GmbH

Ludwig-Maximilians-Universität

ZITiS

Schlüsselübertragung

Freistrahl

Glasfaserleitung

QKD-Hardware

Maja Kierdorf, Lucie Kogelheide - Sicher kommunizieren im Quanten-Zeitalter: Wie gelingt die Migration zu quantensicherer Kryptographie? – v1.0 – BWI intern – Eine Weitergabe an Auftraggeber ist erlaubt

bundeswehr.de
Bwi.de
https://www.bmi.bund.de/SharedDocs/behoerden/DE/zitis.html
tripadvisor.de/Attractions-g187309-Activities-c47-t275-Munich_Upper_Bavaria_Bavaria.html

04. Was macht die BWI?

Das Competence Center Quantum Enabled Technologies

Aufbau eines interdisziplinären Teams

QUANTENSICHERE KOMMUNIKATION

Dr. Maja Kierdorf
Technology Lead QKD

Lucie Kogelheide
Technology Lead PQC

QUANTENSENSORIK

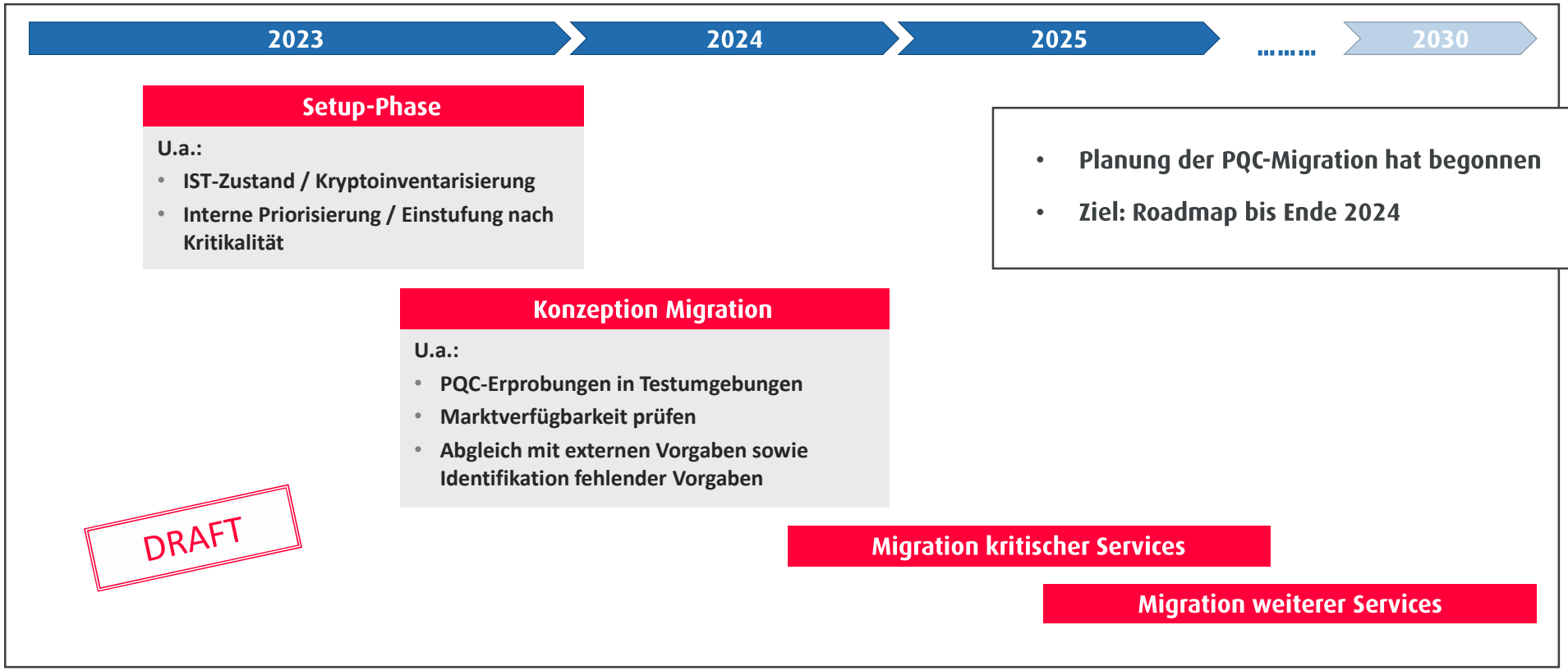
Dr. Timo Weggler
Technology Lead Quantum Sensing

METHODIK, GESCHÄFTSMODELLE UND STRATEGIE

Frank Völker
Leiter CC QET

Sascha Noack
Innovation Lead

Migration zu PQC als Projekt der Architektur-Entwicklung



Einführung von PQC auf allen Ebenen der Organisation

01

Innerhalb einzelner Services.

- Fortsetzung (bereits begonnener) Erfolgsgeschichten
- Soweit möglich dezentral über direkte Ansprechpartner BWI/Hersteller

02

Übergeordnete Steuerung.

- Zentrale Architektur und CC Quantum Enabled Technologies
- Erprobung neuer Lösungen (bereichsübergreifend)
- Einordnung von (antizipierten) externen Vorgaben
- Steuerung über Vorgaben u.a. für Einkauf

→ Projektstart Sommer 2023

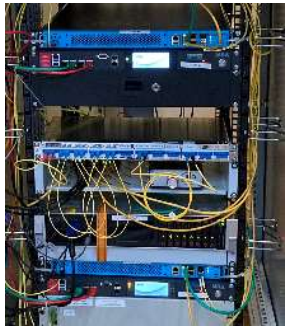
→ Roadmap Ende 2024

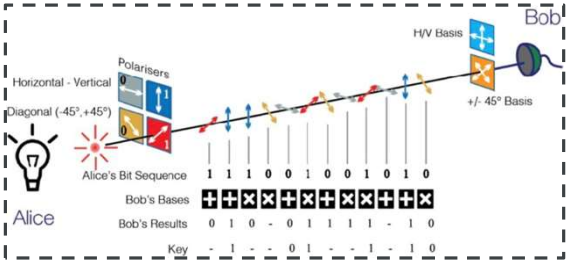
QKD Erprobung in zwei Phasen

01

Testphase.

- Testumgebung Labor in Nürnberg
- Was kann die Technologie (nicht)?
- Erfahrungen sammeln über
  - Parameter
  - Rahmenbedingungen
  - Key Management System

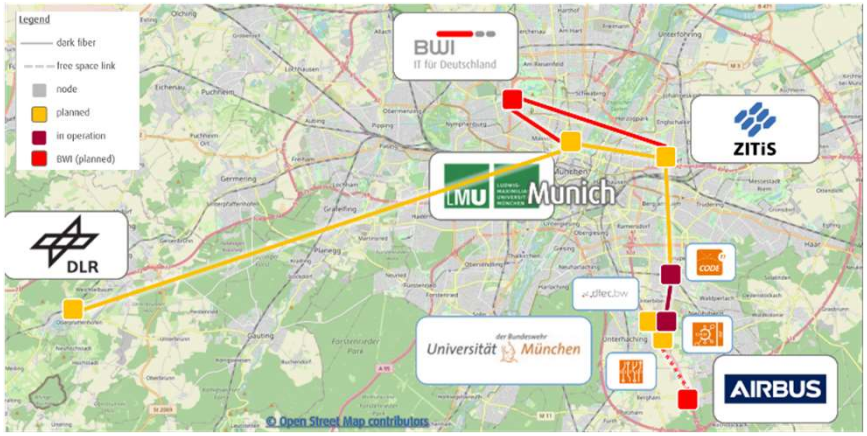




02

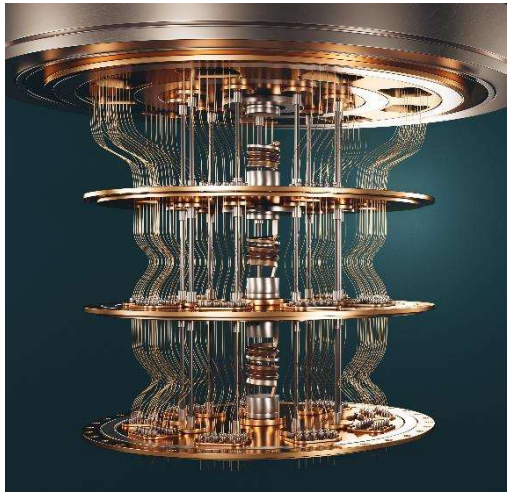
MuQuaNet Phase.

- Testumgebung Münchener Quantennetzwerk (MuQuaNet)
- Wissenstransfer mit Partnern
  - UniBw, ZiTiS, AIRBUS, DLR, LMU, TU Ilmenau
- Konkrete Anwendungsfälle entwickeln und erproben

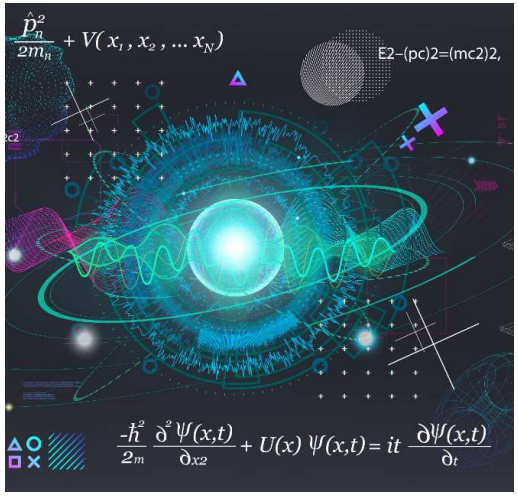


Bildquelle: https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd
Openstreetmap.de

Gedankenexperiment: 10 Jahre in die Zukunft…



Leistungsfähige Quantencomputer existieren



IT-Systeme sind durch quantenresistente Kryptographie abgesichert

Kryptoagilität ermöglicht uns, auch auf neue Bedrohungen schnell zu reagieren