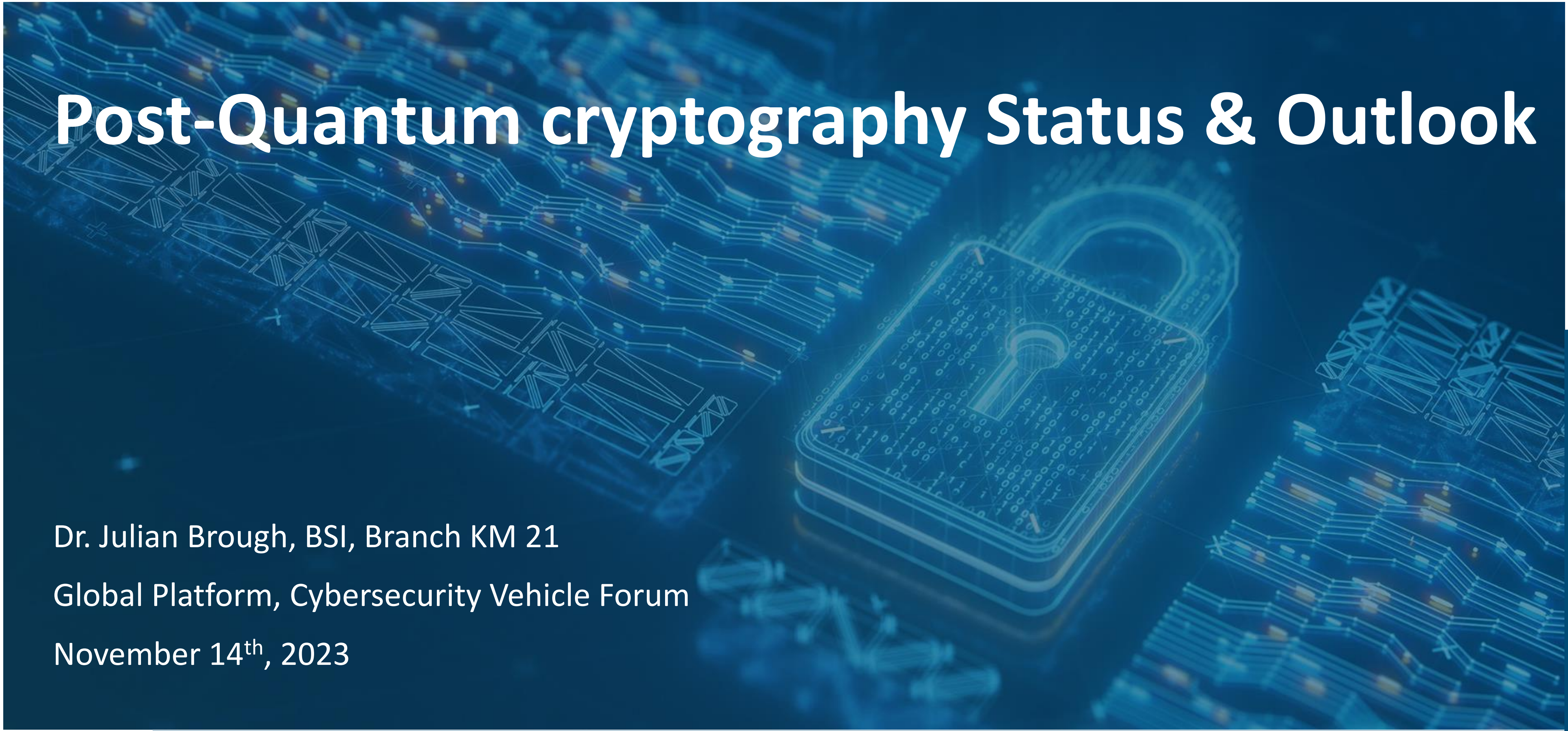
Federal Office
for Information Security

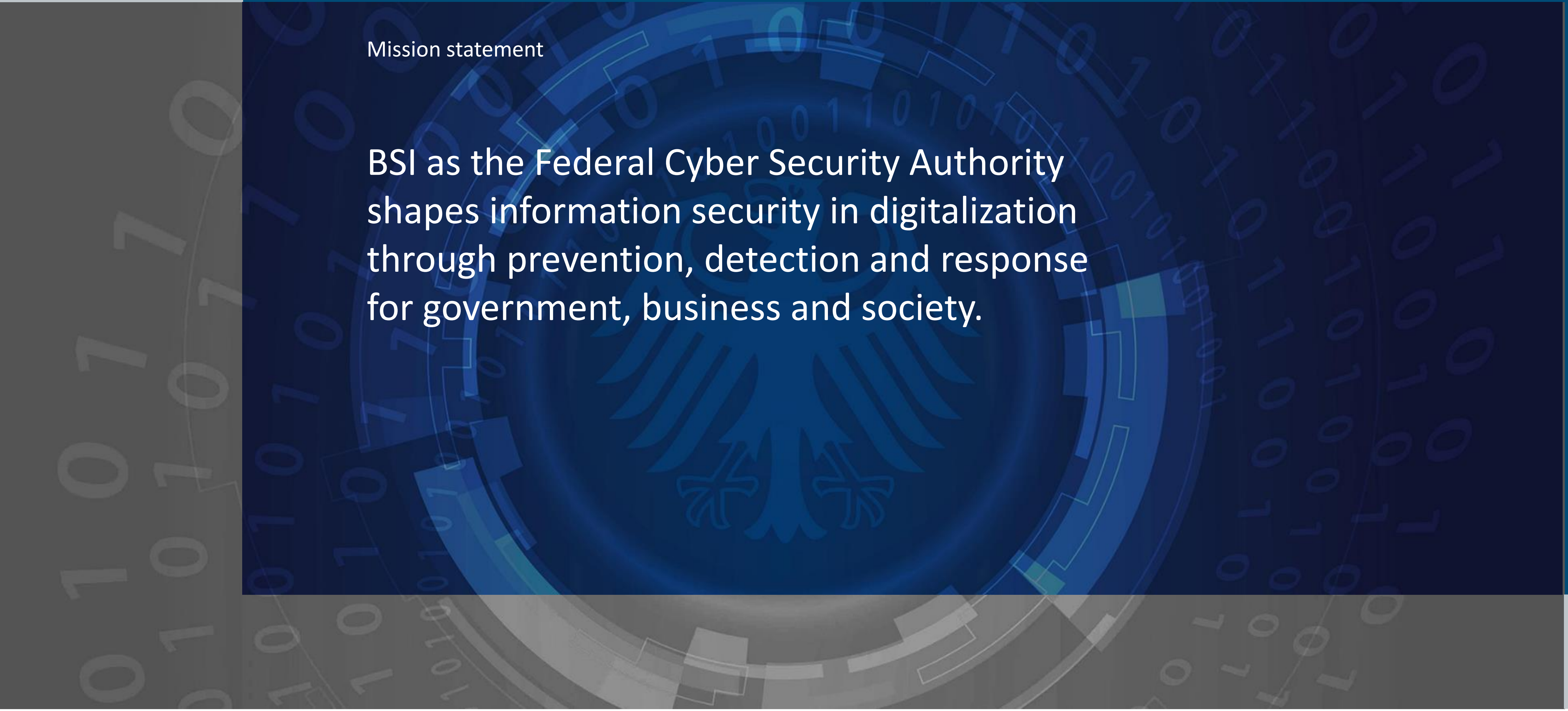


Post-Quantum cryptography Status & Outlook

Dr. Julian Brough, BSI, Branch KM 21

Global Platform, Cybersecurity Vehicle Forum

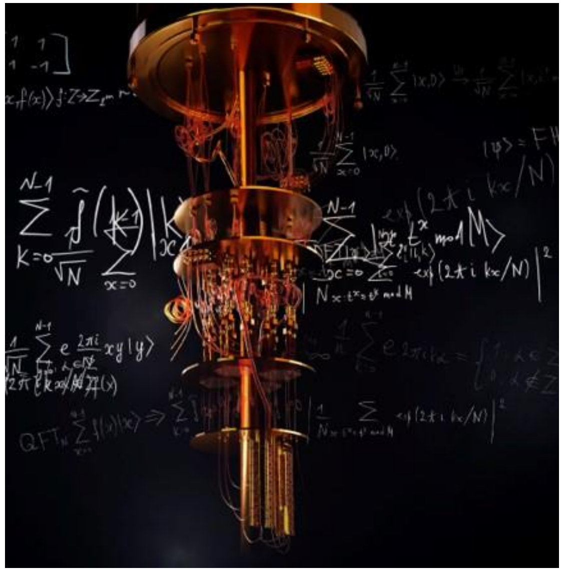
November 14th, 2023



Mission statement

BSI as the Federal Cyber Security Authority shapes information security in digitalization through prevention, detection and response for government, business and society.

The need for quantum-safe cryptography



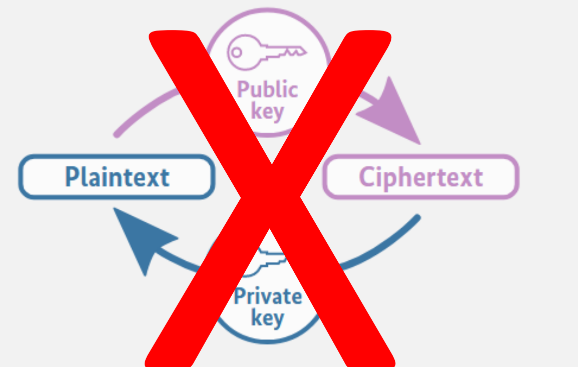
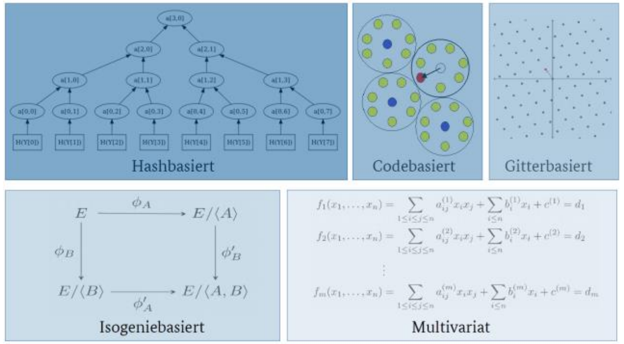


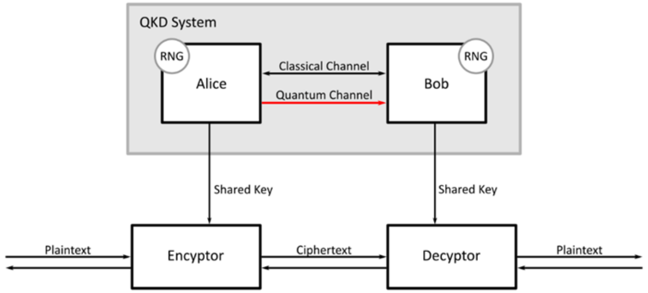
Figure: Schematic representation of asymmetric encryption and decryption

Current Public Key Cryptography
(RSA, (EC)DH, (EC)DSA)

Post Quantum Cryptography



Quantum-safe Cryptography

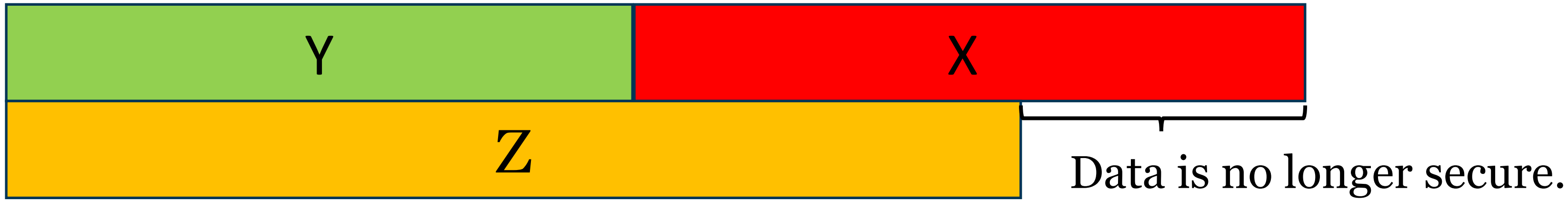


Quantum Key Distribution

How long do we have for migration?

Relevant factors:

- How long should the data stay secure? (X Years)
- How long to migrate the existing infrastructure with a large-scale quantum-safe solution? (Y Years)
- How long will it take for a large-scale quantum computer to be built? (Z Years)



Mosca: If X + Y > Z, then we have a problem!

The need for quantum-safe cryptography

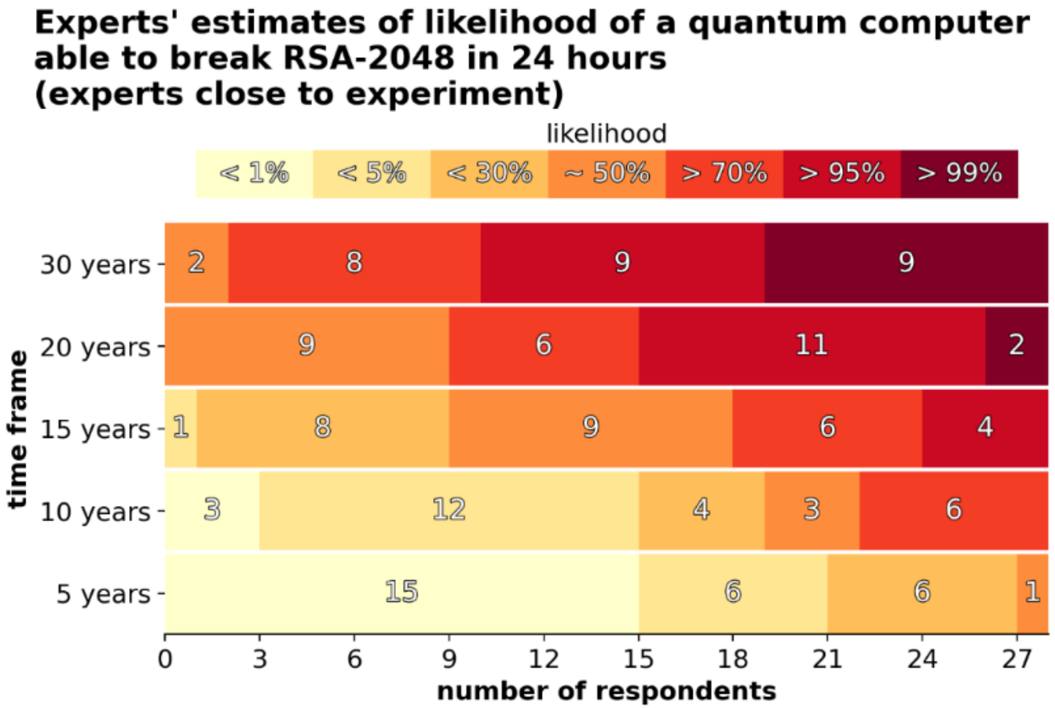


Figure 12 Estimates for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 in 24 hours—for various time frames, limited to the 28 experts deemed to be closer to experiments. Such a subset of experts appear to provide estimates that do not differ substantially from those of all respondents (see Figure 9).

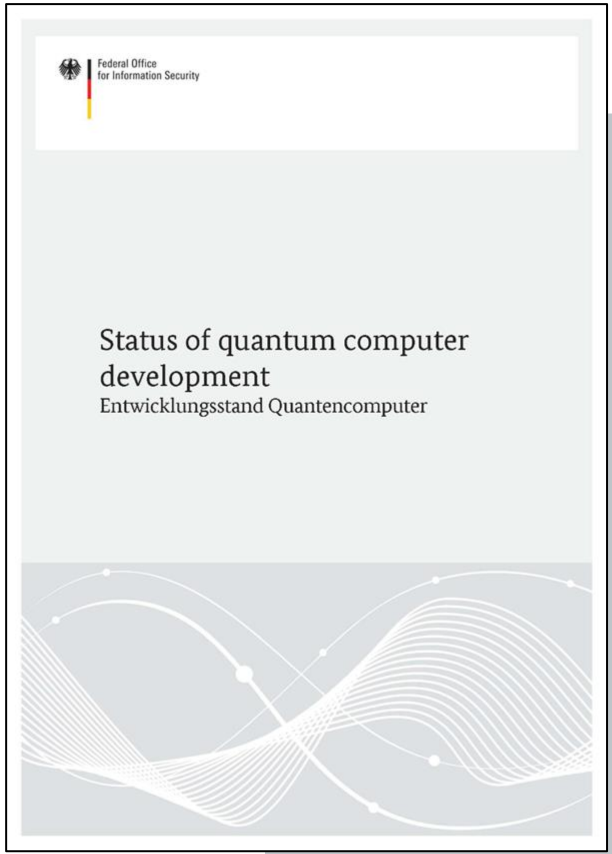
Source: Quantum Threat Timeline Report – 2021: Executive Summary, Global Risk Institute, January 24, 2022
Dr. Michele Mosca & Dr. Marco Piani
https://globalriskinstitute.org/publication/2021- quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

BSI Study „Status of quantum computer development“

- Available under www.bsi.bund.de/qcstudie
- On-going BSI project updating the study, with new developments in:
    - Algorithms in the NISQ-era (noisy intermediate-scale quantum)
    - Error correction and –mitigation
    - Hardware
- No fundamental breakthrough; however, development can accelerate significantly if heuristic results are confirmed

BSI‘s working assuption:

With non-negligible probability, **there will be a cryptographically relevant quantum computer by the beginning of the 2030s.**



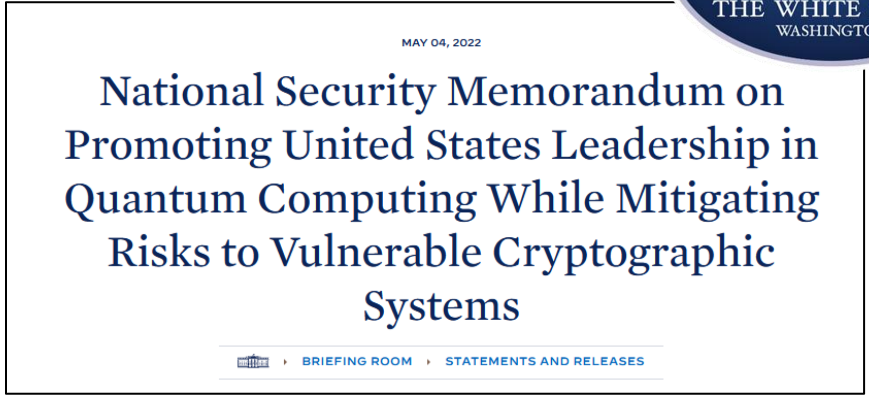
Federal Office
for Information Security

Status of quantum computer development
Entwicklungsstand Quantencomputer

Federal Office
for Information Security

Political Guidelines

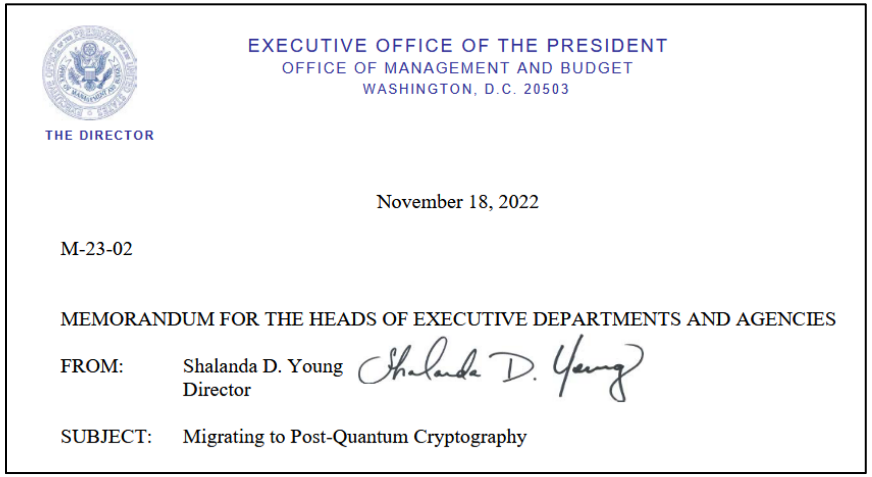
THE WHITE HOUSE
WASHINGTON



MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

› BRIEFING ROOM › STATEMENTS AND RELEASES



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

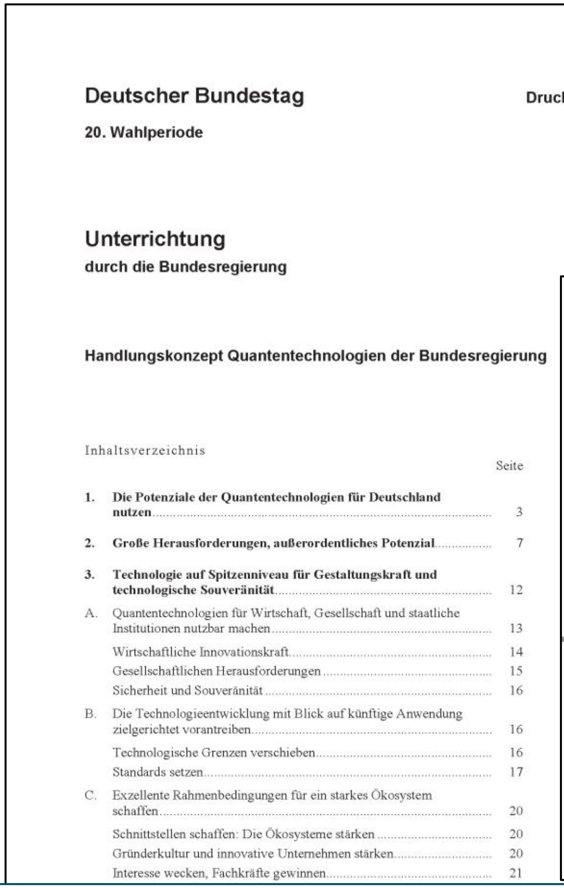
November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography



Deutscher Bundestag
20. Wahlperiode

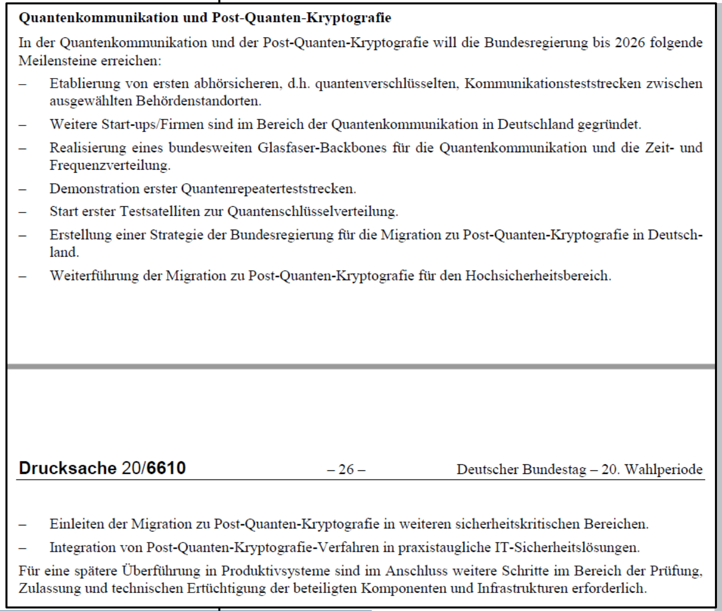
Drucksache 20/6610
28.04.2023

Unterrichtung
durch die Bundesregierung

Handlungskonzept Quantentechnologien der Bundesregierung

Inhaltsverzeichnis

Die
Bundesregierung



Quantenkommunikation und Post-Quanten-Kryptografie

In der Quantenkommunikation und der Post-Quanten-Kryptografie will die Bundesregierung bis 2026 folgende Meilensteine erreichen:

– Etablierung von ersten abhörsicheren, d.h. quantenverschlüsselten, Kommunikationsteststrecken zwischen ausgewählten Behördenstandorten.
– Weitere Start-ups/Firmen sind im Bereich der Quantenkommunikation in Deutschland gegründet.
– Realisierung eines bundesweiten Glasfaser-Backbones für die Quantenkommunikation und die Zeit- und Frequenzverteilung.
– Demonstration erster Quantenrepeaterteststrecken.
– Start erster Testsatelliten zur Quantenschlüsselverteilung.
– Erstellung einer Strategie der Bundesregierung für die Migration zu Post-Quanten-Kryptografie in Deutschland.
– Weiterführung der Migration zu Post-Quanten-Kryptografie für den Hochsicherheitsbereich.

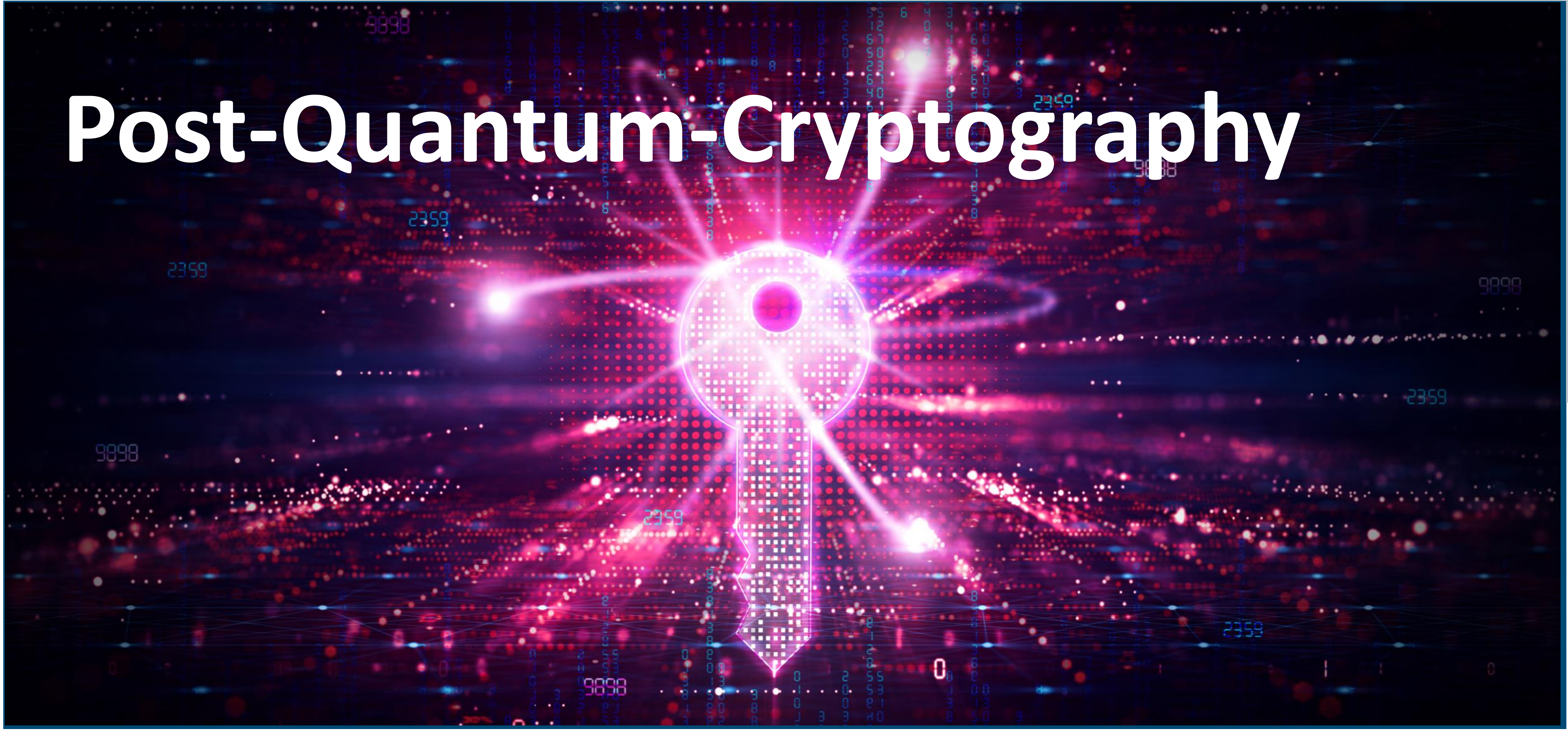
Drucksache 20/6610 – 26 – Deutscher Bundestag – 20. Wahlperiode

– Einleiten der Migration zu Post-Quanten-Kryptografie in weiteren sicherheitskritischen Bereichen.
– Integration von Post-Quanten-Kryptografie-Verfahren in praxistaugliche IT-Sicherheitslösungen.

Für eine spätere Überführung in Produktivsysteme sind im Anschluss weitere Schritte im Bereich der Prüfung, Zulassung und technischen Ertüchtigung der beteiligten Komponenten und Infrastrukturen erforderlich.

Milestones (until 2026):

- Create a strategy of the federal government for the migration to post-quantum cryptography.
- …

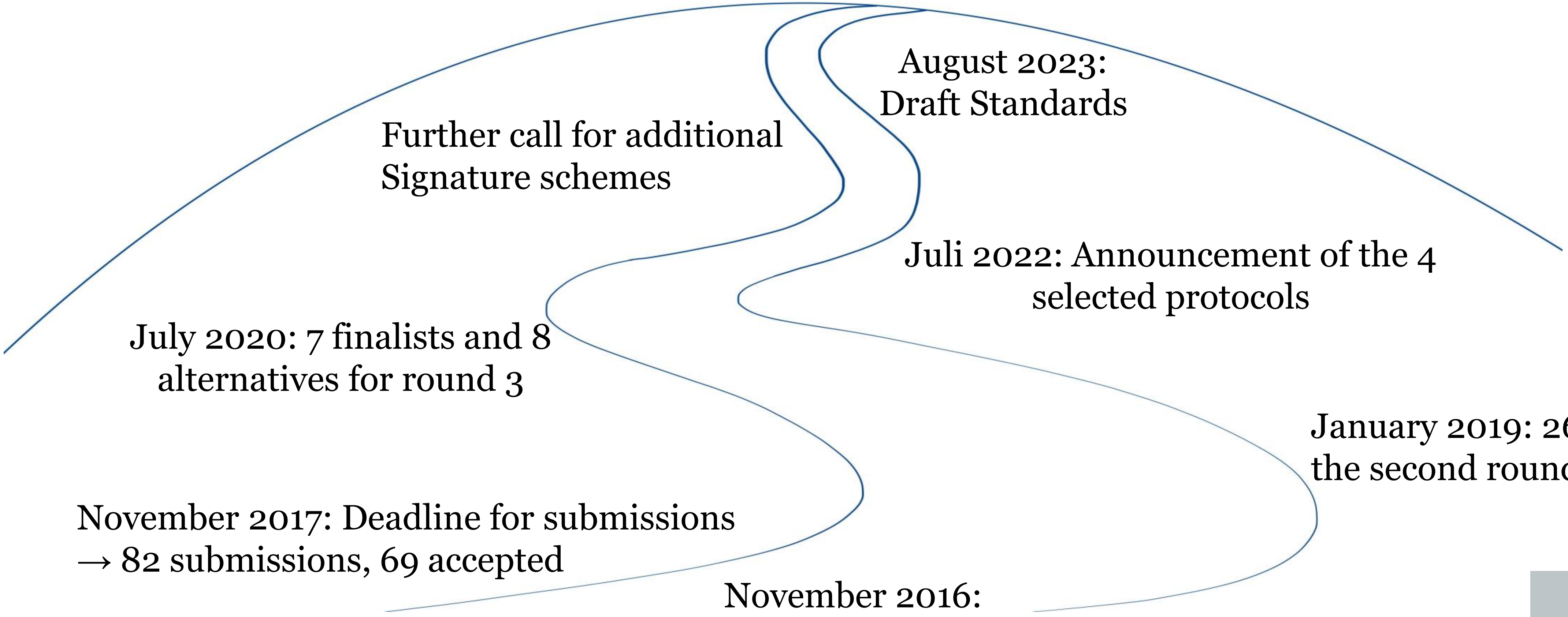


Post-Quantum-Cryptography

Federal Office
for Information Security

Standardisation: NIST-Process („A long and winding road“)

First Standards: 2024



November 2016:
Call for Proposals

November 2017: Deadline for submissions
→ 82 submissions, 69 accepted

January 2019: 26 selected for
the second round

July 2020: 7 finalists and 8
alternatives for round 3

Juli 2022: Announcement of the 4
selected protocols

Further call for additional
Signature schemes

August 2023:
Draft Standards

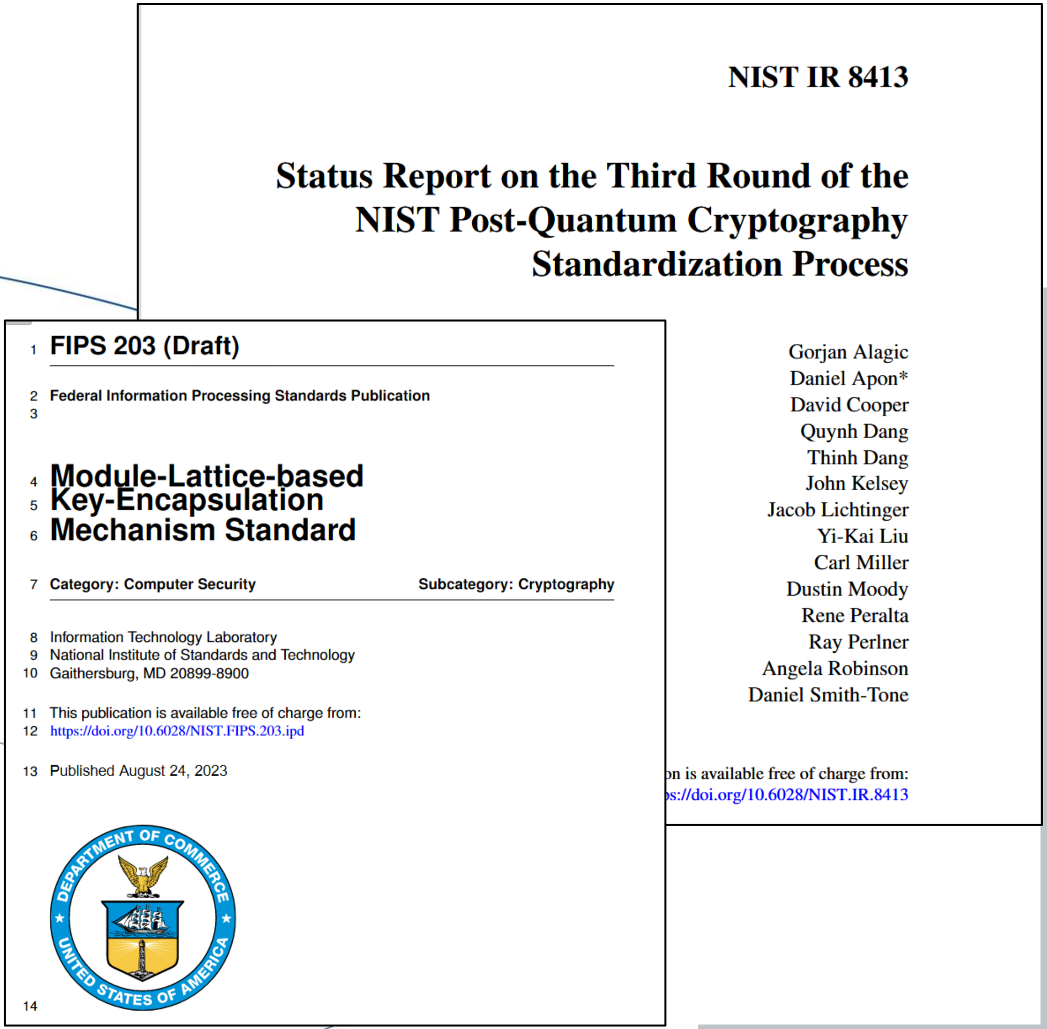
Standardisation: NIST-Process

August 2023: Drafts for FIPS 203, 204, 205:

1 KEM: **ML-KEM** (CRYSTALS-Kyber)

3 Signature schemes:

ML-DSA (CRYSTALS-Dilithium**)**, **SLH-DSA** (SPHINCS+), **Falcon** (later)



NIST IR 8413

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Daniel Apon*
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone

on is available free of charge from:
s://doi.org/10.6028/NIST.IR.8413

FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203.ipd

Published August 24, 2023

Standardisation: ISO/IEC, IETF/IRTF

- ISO/IEC 18033-2: Standardisation project for PQ-KEMs
  - FrodoKEM
  - Classic McEliece
  - ML-KEM (CRYSTALS-Kyber)
- Multiple standardisation projects for PQC in IETF/IRTF
  - OpenPGP
  - Cryptographic Message Syntax (CMS)
  - X.509
  - TLS 1.3
  - IKEv2
  - …

BSI Guide „Quantum-safe cryptography“

In 2021 BSI published the guideline
Quantum-safe cryptography – fundamentals, current developments and recommendations:

- Background on *quantum computers*, *PQC*, *protocols*, *QKD*
- Developments in politics, research and industry
- Recommendations for actions (excerpt):
  - Preparation: cryptographic inventory
  - Hybrid solutions for KEMs and signature schemes
  - Cryptographic agility (the ability to switch between multiple cryptographic primitives)

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sich

Migration to Post Quantum Cryptography

Recommendations for action by the BSI

Federal Office for Information Security

Quantum-safe cryptography – fundamentals, current developments and recommendations

Reference: www.bsi.bund.de/dok/pqmigration-en

Federal Office for Information Security

BSI Technical Guideline TR-02102-1

„Cryptographic Recommendations for PQC“

- Key Encapsulation Mechanisms:
    - *FrodoKEM*
    - *Classic McEliece*
- Stateful hash-based signatures:
    - *LMS/HSS*
    - *XMSS/XMSS^MT*
- PQC only in a *hybrid format*, i.e. PQC + “Classical”, except for HBS

Federal Office
for Information Security

BSI – Technical Guideline

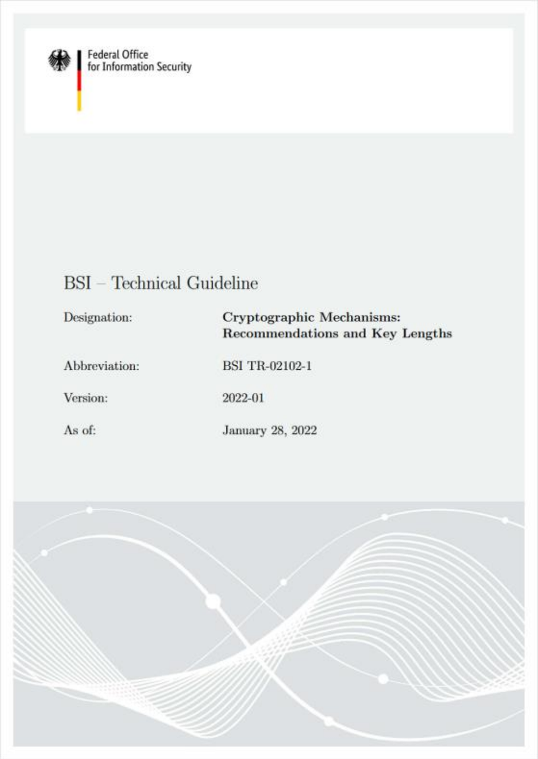
Designation:	**Cryptographic Mechanisms: Recommendations and Key Lengths**
Abbreviation:	BSI TR-02102-1
Version:	2022-01
As of:	January 28, 2022

Reference: www.bsi.bund.de/TR-02102

BSI Technical Guideline TR-02102-1

Outlook (2024/2025) for PQC:

- Key Encapsulation Mechanisms:
  - *FrodoKEM*
  - *Classic McEliece*
  - *ML-KEM (after standard becomes available)*
- Digital Signature Schemes:
  - *ML-DSA (after standard becomes available)*
  - *SLH-DSA (after standard becomes available)*
  - *LMS/HSS* and *XMSS/XMSS^MT*
- *Parameter sets: NIST security categories 3 and 5*
- PQC only in a *hybrid format*, i.e. PQC + “Classical”, except for HBS



Federal Office
for Information Security

BSI – Technical Guideline

Designation: Cryptographic Mechanisms: Recommendations and Key Lengths

Abbreviation: BSI TR-02102-1

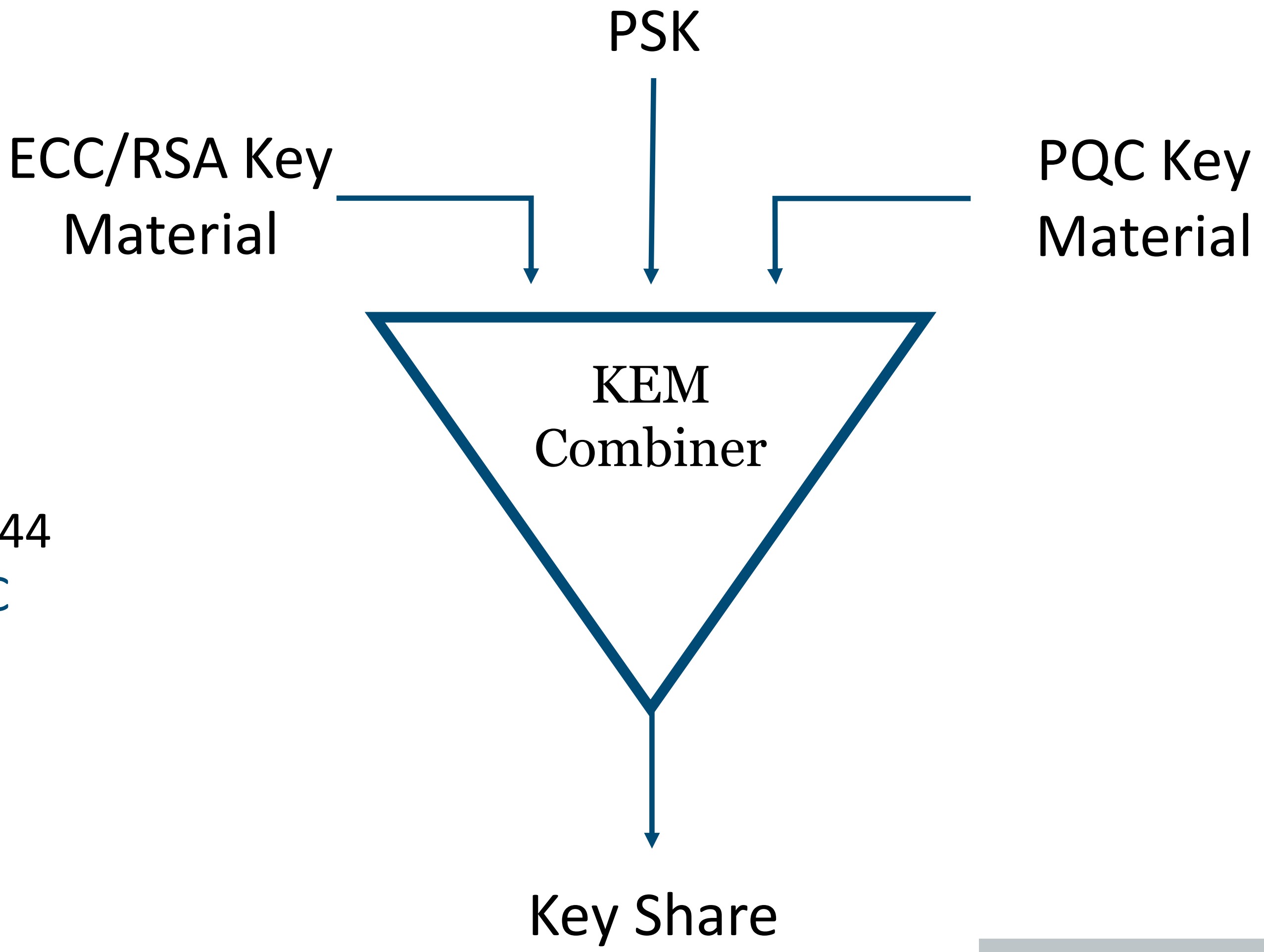
Version: 2022-01

As of: January 28, 2022

Key Exchange: KEM Combiner

- Goal:
  Construction is secure as long as at least one of the inputs is secure.

- Recommendations:
  - CatKDF & CasKDF from ETSI TS 103 744
  - The Keccac (SHA3, KMAC) and HMAC based KDFs from NIST SP 800-56Cr2

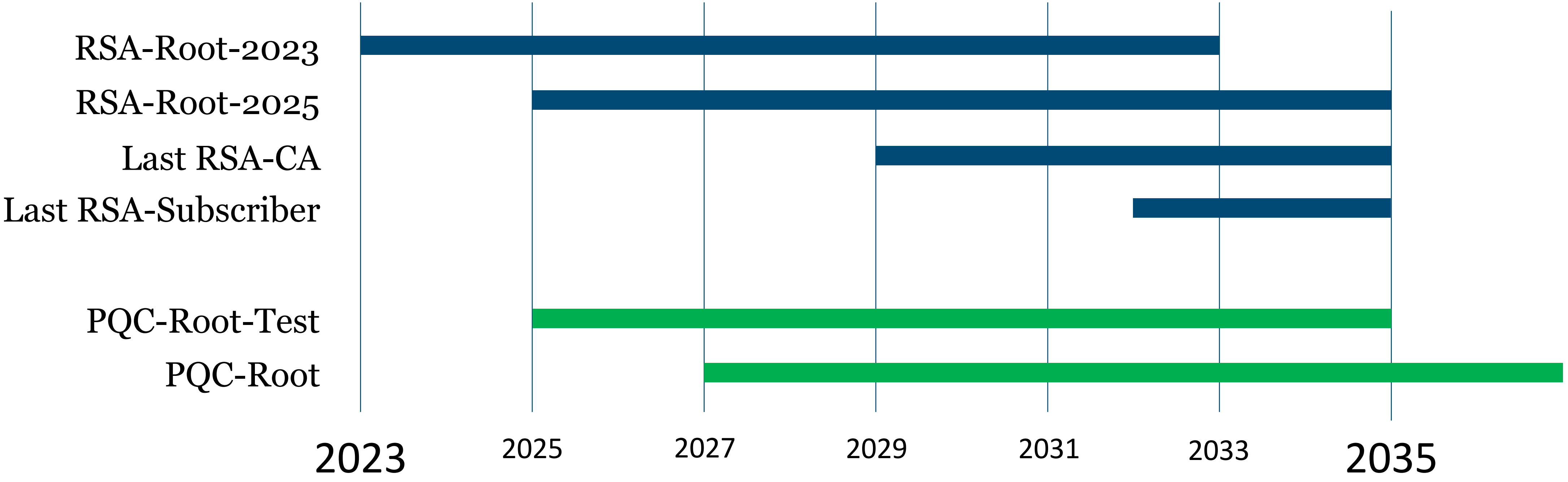


Federal Office for Information Security

BSI-activities and projects on PQC

Cryptographic library Botan	Integration of PQC in Thunderbird and OpenPGP	Migration of German administrative Public Key Infrastructure to PQC
• Botan 3.x • Implementation of PQC in Botan: SPHINCS+, FrodoKEM, Classic McEliece, Kyber, Dilithium, XMSS, LMS/HSS • Hybrid Key Agreement in TLS 1.3	• PQC+ECC for E-Mail-encryption and signatures • IETF I-D “PQC for OpenPGP” (coming soon) • Implementation in GnuPG/libgcrypt	• Hybrid solution (PQC+ECC) for Subscriber-Certificates • Root-CA: BSI is examining the use of hash-based signature scheme

Migration of German administrative Public Key Infrastructure



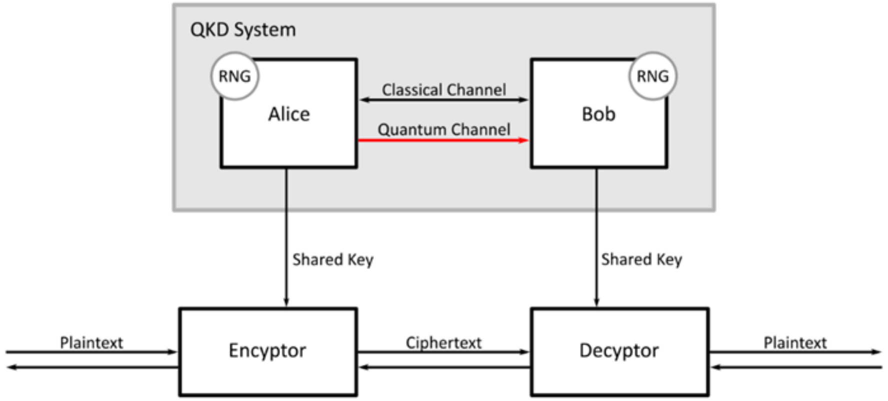
Quantum Key Distribution

Quantum Key Distribution (QKD)

Some facts:

- Theoretical security is based on quantum-physical principles
- Only works for key agreement
- Requires specialized (and expensive) hardware
- Implementation security must also be considered

  (in addition to theoretical security)
- Limitations of QKD make it only applicable for specific use cases



BSI‘s policy:

- **Migration to PQC has highest priority**
- QKD could potentially complement or backup PQC in the future

Summary

- Public-key cryptography deployed today **will be broken** by large-scale quantum computers.
- *„Store now, decrypt later“* is a real threat & considerable migration times are to be expected.
  → PQC-migration has to be initiated **now**!
- Cryptographic agility should become a design criterion.
- In general, PQC should be used in a hybrid format together with RSA or ECC.
- QKD is not sufficiently mature from a security perspective.

Thank you for your attention!

Contact

Dr. Julian Brough
KM 21 – Information Assurance Technology Requirements

Federal Office for Information Security (BSI)
Godesberger Allee 185-189
53175 Bonn

julian.brough@bsi.bund.de