Federal Office
for Information Security

Post-Quantum Policy and Activities of the BSI

European Cyber Week 2024, Rennes, November 19, 2024

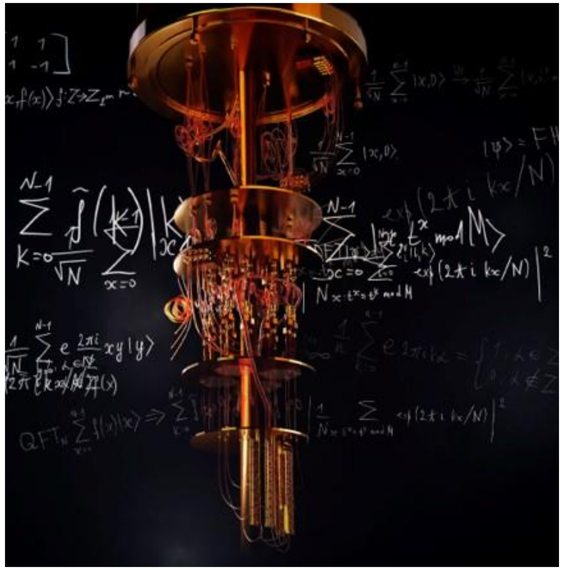
Dr. Kaveh Bashiri, BSI

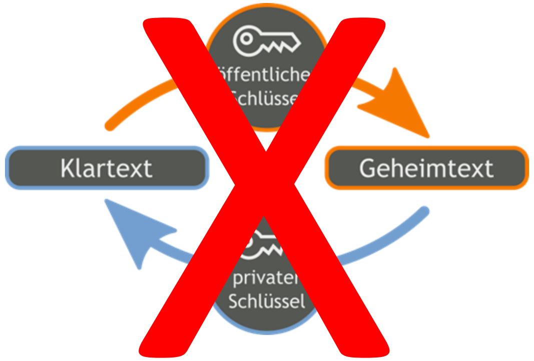
Agenda

- Motivation
- PQC@BSI
- Quantum-safe German Administration PKI
- BSI Study „Status of quantum computer development“

Motivation

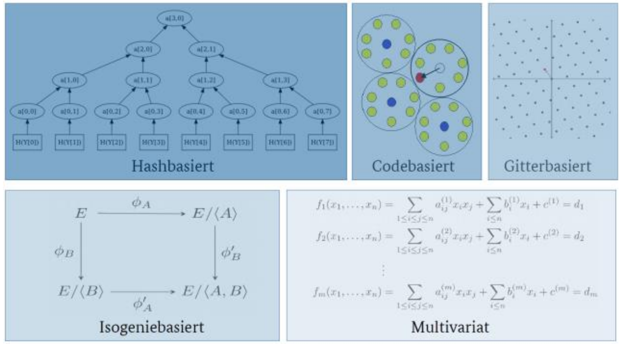
Why Quantum-safe Cryptography?





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

Post-Quantum Cryptography



Two main threat scenarios

1

- *Store now, decrypt later*

→ Quantum-safe encryption

2

- *Complex migration* (e.g. PKI)

→ Mainly quantum-safe authentication

Policies

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
Director

SUBJECT: Migrating to Post-Quantum Cryptography

Deutscher Bundestag — Drucksache 20/6610
20. Wahlperiode — 28.04.2023

Unterrichtung
durch die Bundesregierung

Handlungskonzept Quantentechnologien der Bundesregierung

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 26. April 2023.

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.

Policies

EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

"The Post-Quantum Cryptography Coordinated Implementation **Roadmap** should be available **after a period of two years** following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap."

Policies

EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

- September 2024: Kickoff PQC-Workstream
- Co-chairs: France, Germany, Netherlands
- Goal: Develop roadmap for a harmonized transition towards PQC in the EU

PQC @ BSI

Working Hypothesis

For high security systems,
BSI acts on the working hypothesis that cryptographically relevant quantum computers will be available in the early 2030s.

Remark: This statement is not a forecast of the availability of quantum computers, but rather represents a timeline for risk assessment.

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:
  - Preparation/inventory
  - Cryptographic agility
  - Conservative KEMs and signature schemes
  - Hybrid solutions in general

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

BSI Technical Guidelines

- Key Encapsulation Mechanisms:
  - *FrodoKEM* and *Classic McEliece*
  - *ML-KEM* (for the 2025 update)
- Signature schemes:
  - *ML-DSA* (for the 2025 update)
  - *SLH-DSA* (for the 2025 update)
  - *LMS/HSS* and *XMSS/XMSS^MT*
- Parameters: NIST security *categories 3* and *5*
- Only *hybrid solutions*, i.e. PQC+Classical KEMs and signatures

  One exception: hash-based signatures


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

What about QKD?

Some facts:

- Theoretical security based on physical principles
- Only key agreement
- Requires specialized (and expensive) hardware
- Distance limitations
- Implementation security must also be considered
- QKD protocols need to be standardized
- Associated security proofs need to be developed
- Certification criteria for QKD products need to be further developed
- Mature European QKD products need to be developed

⟶ Migration to PQC has highest priority

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

SWEDISH ARMED FORCES

Position Paper on Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

This paper is aimed at a general audience. Technical details have therefore been left out to the extent possible. Technical terms that require a definition are printed in italics and are explained in a glossary at the end of the document.

(A selection of) Related Projects

- PQC
  - ➢ PQC in Botan cryptographic library
  - ➢ PQC in OpenPGP
  - ➢ Quantum-safe German Administration PKI ("Verwaltungs-PKI", "V-PKI")

→ Later!

- QKD
  - ➢ BSI Study "Implementation attacks against QKD systems"
  - ➢ Common Criteria Protection Profile (with ETSI QKD ISG)

- QC
  - ➢ BSI Study „Status of quantum computer development"

→ Later!

Quantum-safe German administration PKI

The public administration PKI (“Verwaltungs-PKI”, V-PKI)

- Goal: Trustworthy identity management for the public administration

Root 10y — Sub-CA 6y — Subscriber 3y

- Usage: S/MIME, TLS and other standard applications
- Scale: 6 Sub-CAs, approx. 500.000 subscribers
- Algorithm: RSA

Migration towards a quantum-safe V-PKI necessary!

Quantum-safe V-PKI – Choice of signature schemes

Important Criteria:

- Security
- Performance (especially: signature- and PK-size)
- Interoperability and compatibility with standard applications
- High Availability

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SLH-DSA	• Well-understood security properties	• Performance
ML-DSA in combination with ECDSA	• Better performance than SLH-DSA • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SLH-DSA	• Well-understood security properties	• Performance
ML-DSA in combination with ECDSA	• Better performance than SLH-DSA • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Comparison of certificate sizes

Algorithm	Signature-size in kB	PK-size in kB	(Signature + PK)-size in kB
RSA4096	0.5	0.5	1
ML-DSA & ECDSA-384	3.4	2.1	5.5
SLH-DSA-192s	16	0.05	16
SLH-DSA-Few-192s	8	0.05	8
LMS-H20-192-W8	1.1	0.05	1.1
HSS-H5/H15-192-W8	1.8	0.05	1.8

Use LMS-H20-192-W8 (or HSS-H5/H15-192-W8)?

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SLH-DSA	• Well-understood security properties	• Performance
ML-DSA in combination with ECDSA	• Better performance than SLH-DSA • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

State management

Root

- Moderate number of signatures
- Secure environment

→ Doable

Sub-CA

- Large number of signatures
- OCSP service

→ Challenge

Subscriber

→ Impossible

Federal Office
for Information Security

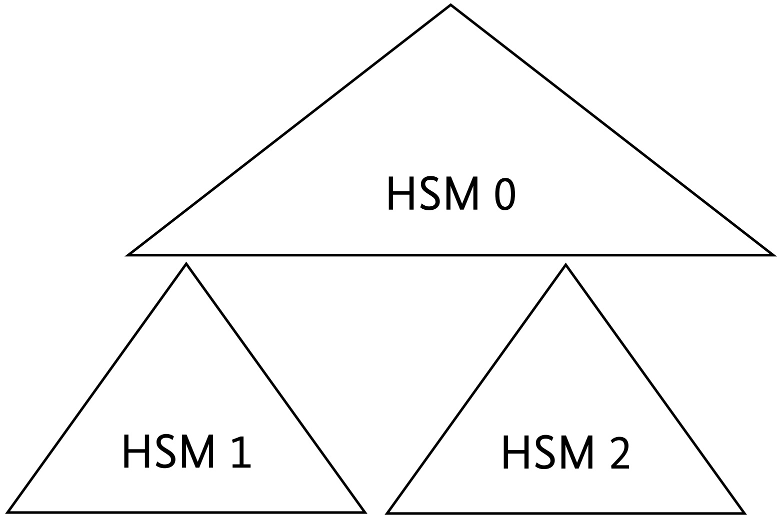
Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SLH-DSA	• Well-understood security properties	• Performance
ML-DSA in combination with ECDSA	• Better performance than SLH-DSA • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Backup management according to NIST SP 800-208, § 7

(Distributed multi-tree hash-based signatures)

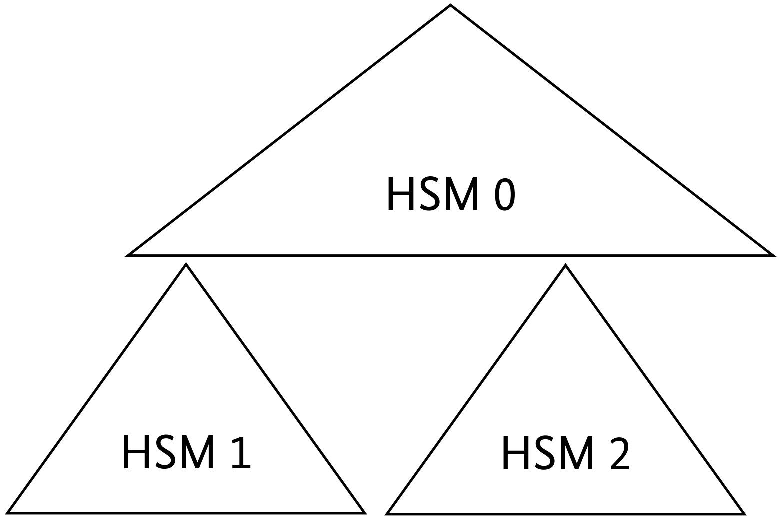


- Create top-level Merkle-tree on HSM 0
- Create bottom-level Merkle-trees on HSM 1, HSM 2
- Sign roots of the bottom-level Merkle-trees with HSM 0
- Store copies of the corresponding signatures and auth. paths outside of the cryptographic modules
- Sign messages with HSM 1 (and then with HSM 2)
- Initiate new HSM 3 as long as HSM 0 is operational

Federal Office
for Information Security

Backup management according to NIST SP 800-208, § 7

(Distributed multi-tree hash-based signatures)



Problem:

- Cryptographic modules may be operational for < 10y
- All HSMs might break at the same time
- Root-CA needs to be able to generate signatures for 10y

Federal Office
for Information Security

Backup management

→ Private key backup necessary

Problem:

- According to NIST SP 800-208 this is prohibited

Solutions:

- NIST will update NIST SP 800-208
- https://www.ietf.org/archive/id/draft-wiggers-hbs-state-00.html

→ §6: Only allow export of seeds of unused subtrees

Workgroup:	Network Working Group				
Internet-Draft:	draft-wiggers-hbs-state-00				
Published:	19 February 2024				
Intended Status:	Informational				
Expires:	22 August 2024				
Authors:	T. Wiggers *PQShield*	K. Bashiri *BSI*	S. Kölbl *Google*	J. Goodman *Crypto4A Technologies*	S. Kousidis *BSI*

Hash-based Signatures: State and Backup Management

Abstract

Stateful Hash-Based Signature Schemes (S-HBS) such as LMS, HSS, XMSS and $XMSS^{MT}$ combine Merkle trees with One-Time Signatures (OTS) to provide signatures that are resistant against attacks using large-scale quantum computers. Unlike conventional stateless digital signature schemes, S-HBS have a state to keep track of which OTS keys have been used, as double-signing with the same OTS key allows forgeries.

This document provides guidance and documents security considerations for the operational and technical aspects of deploying systems that rely on S-HBS. Management of the state of the S-HBS, including any handling of redundant key material, is a sensitive topic, and we discuss some approaches to handle the challenges. We also describe the challenges that need to be resolved before certain approaches should be considered.

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SLH-DSA	• Well-understood security properties	• Performance
ML-DSA in combination with ECDSA	• Better performance than SLH-DSA • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Hybrid Digital Signatures

- Independent signatures, e.g. PQC & ECC
- Signature is valid if and only if all signatures verify
- Concrete proposals @IETF:
  - draft-ietf-lamps-pq-composite-sig
  - draft-ietf-openpgp-pqc
  - Composite construction, e.g. identifier for „ML-DSA-65 + ECDSA-brainpoolP256r1“

Quantum-safe V-PKI – Further criteria

Design of certificates:

- Separate signing- and KEM- certificates
- Standardisation of post-quantum schemes in common certificate formats

→ Cooperation BSI & Cisco Systems & CryptoNext Security & genua GmbH

for X.509 certificates: draft-ietf-lamps-x509-shbs draft-ietf-lamps-x509-slhdsa

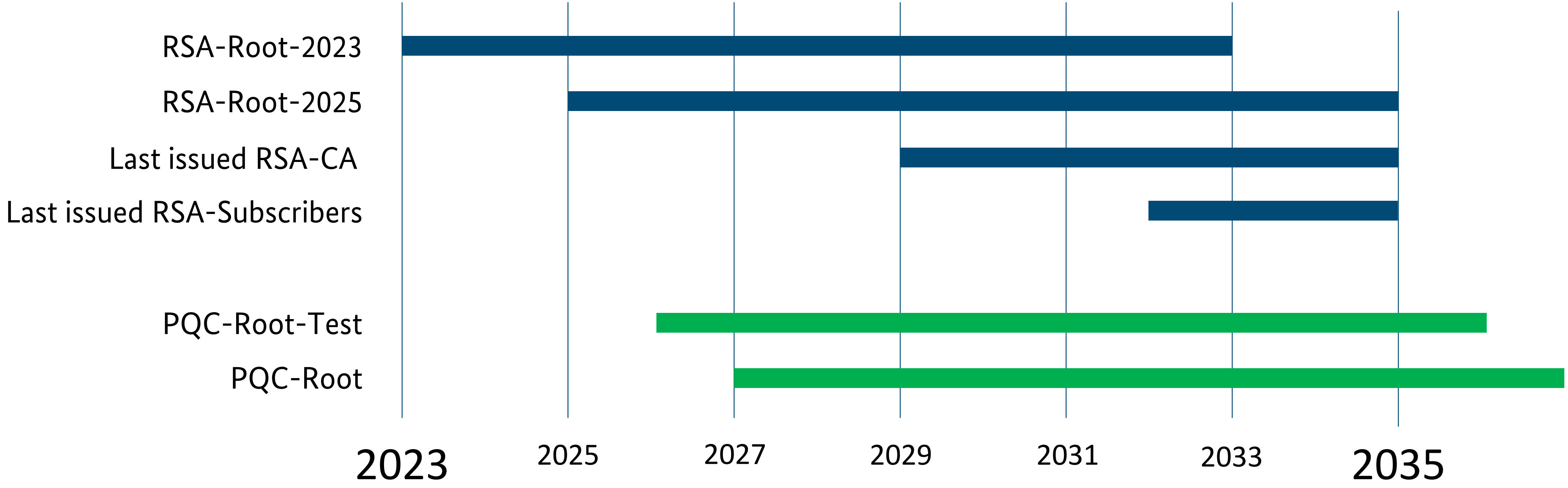
Quantum-safe V-PKI – Further criteria

Migration concept:

- *Parallel approach*:

→ Smooth transition in order to guarantee business continuity

Migration – What it looks like in validity periods

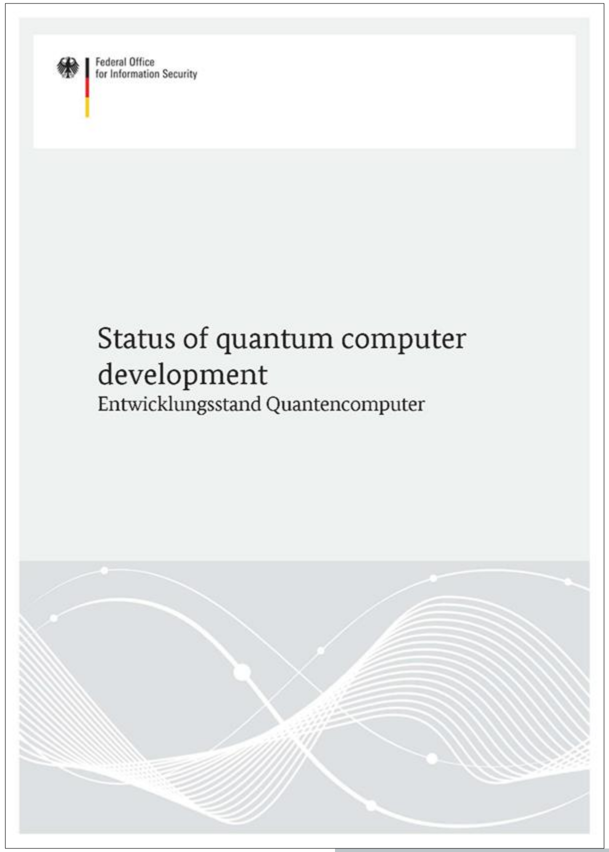


(The bars represent the validity periods of the corresponding certificates)

BSI Study „Status of quantum computer development“

BSI Study “Status of quantum computer development”

- Available under www.bsi.bund.de/qcstudie
- First version published in 2018
- Updated 2019, 2020, and 2023
- Next update: December 2024
- Project lead: Prof. Frank Wilhelm-Mauch (FZ Jülich)
  with subcontractor: Prof. Rainer Steinwandt (University of Alabama in Huntsville)
- Two evaluation schemes:
  - one for quantum computing hardware and
  - another for quantum algorithms.
- Separate evaluation scheme for the field of NISQ algorithms



Some Insights from the Newest Update

- Regev's Factoring Algorithm:
  - Alternative to Shor's algorithm
  - Asymptotic improvement
  - Detailed analysis needed on efficiency gains for concrete cryptographically relevant factorization instances
  - Extended to DLP by Ekerå and Gärtner (but not for ECC)

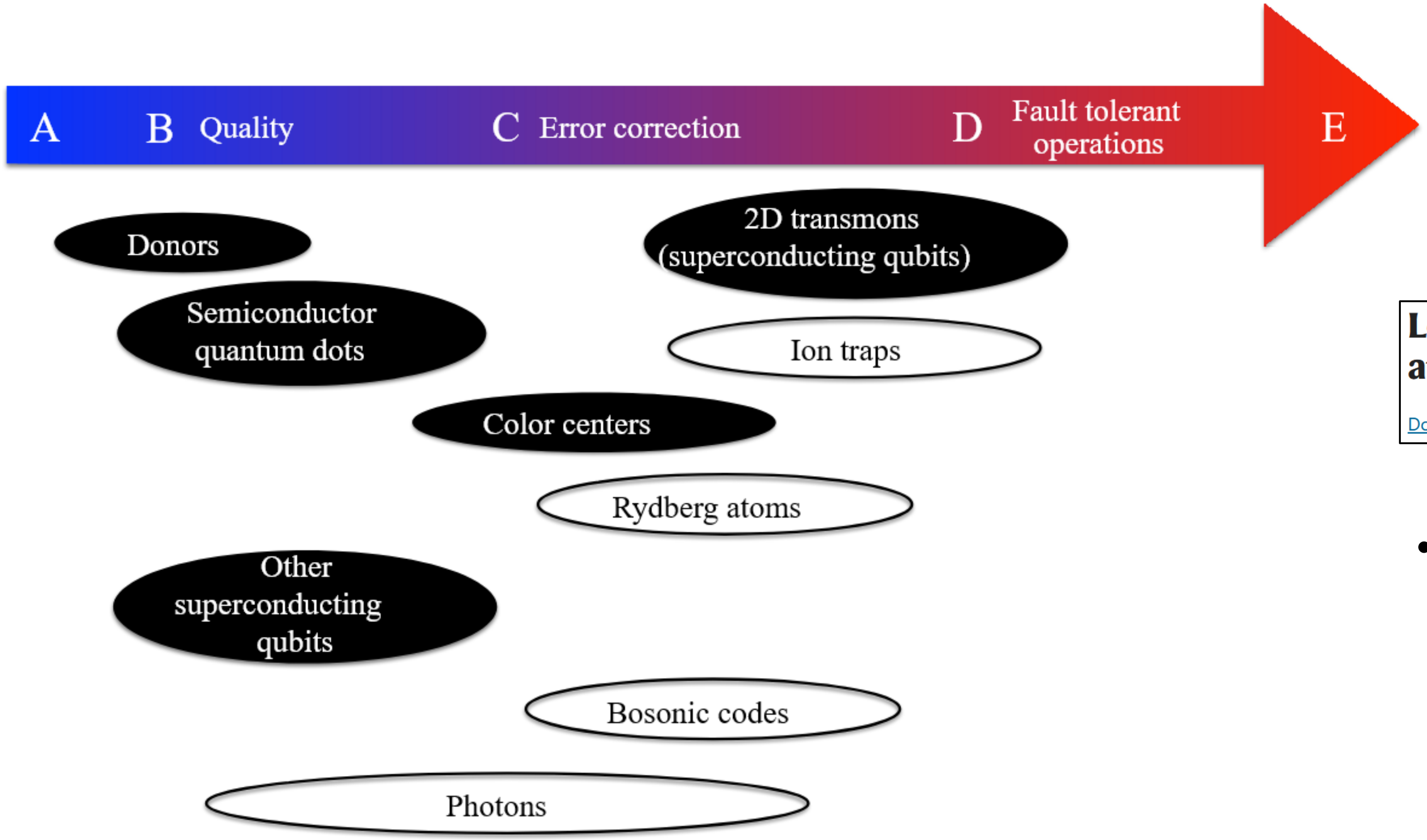
An Efficient Quantum Factoring Algorithm

Oded Regev*

Abstract

We show that n-bit integers can be factorized by independently running a quantum circuit with $\tilde{O}(n^{3/2})$ gates for $\sqrt{n}+4$ times, and then using polynomial-time classical post-processing. The correctness of the algorithm relies on a number-theoretic heuristic assumption reminiscent of those used in subexponential classical factorization algorithms. It is currently not clear if the algorithm can lead to improved physical implementations in practice.

Some Insights from the Newest Update



Logical quantum processor based on reconfigurable atom arrays

Dolev Bluvstein orcid.org/0000-0002-9934-9530[1], Simon J. Evered orcid.org/0000-0001-8986-1103[1],

- Neutral atoms using Rydberg states became a TOP candidate among ion traps and 2D transmons (superconducting qubits)

Some Insights from the Newest Update

Quantum error correction below the surface code threshold

Google Quantum AI and Collaborators
(Dated: August 27, 2024)

- Quantum error correction beyond break-even point:
  - Error-corrected quantum memory with surface codes of increasing distance (up to distance 7)
  - Logical qubit error is under the physical qubit error threshold

    → Increasing code distance leads to better results
  - Achieved by a number of engineering improvements
  - A main insight is that the background of rare correlated “catastrophic” events has been significantly reduced
- Further results in this direction:

Hardware-efficient quantum error correction using concatenated bosonic qubits

Harald Putterman,[1,*] Kyungjoo Noh,[1] Connor T. Hann,[1] Gregory S. MacCabe,[1] Shahriar Aghaeimeibodi,[1] Rishi N.

Demonstration of quantum computation and error correction with a tesseract code

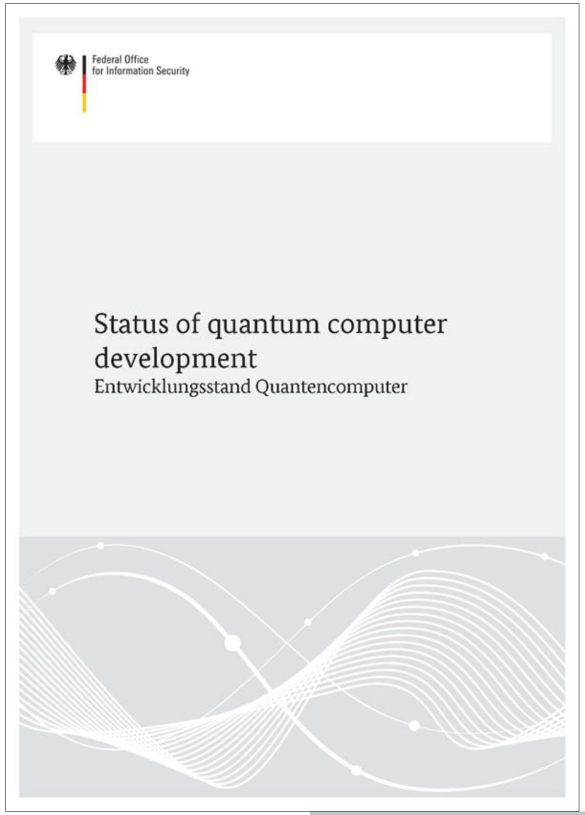
Ben W. Reichardt,[1] David Aasen,[1] Rui Chao,[1] Alex Chernoguzov,[2] Wim van Dam,[1] John P. Gaebler,[2] Dan Gresh,[2] Dominic Lucchetti,[2] Michael Mills,[2] Steven A. Moses,[2] Brian Neyenhuis,[2] Adam Paetznick,[1] Andres Paz,[1] Peter E. Siegfried,[2] Marcus P. da Silva,[1] Krysta M. Svore,[1] Zhenghan Wang,[1] and Matt Zanner[1]
[1] *Microsoft Azure Quantum*
[2] *Quantinuum*

Quantum Error Correction of Qudits Beyond Break-even

Benjamin L. Brock,[*] Shraddha Singh, Alec Eickbusch,[†] Volodymyr V. Sivak,[†] Andy Z. Ding, Luigi Frunzio, Steven M. Girvin, and Michel H. Devoret[‡]
Departments of Applied Physics and Physics, Yale University, New Haven, CT, USA
Yale Quantum Institute, Yale University, New Haven, CT, USA
(Dated: October 10, 2024)

Some Insights from the Newest Update

- Conclusions:
  - Steady progress towards cryptographic relevance
  - Estimated time horizon: Decision pending
  - However, huge step forward is expected as soon as heuristic claims become rigorous



Summary

- Most of the public-key cryptography deployed today is threatened 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 hybrid mode together with RSA or ECC.
- QKD is not sufficiently mature from a security perspective. Once it is, it could be an addition to post-quantum cryptography for a limited set of use cases.

Deutschland
Digital•Sicher•BSI•

Dr. Kaveh Bashiri

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

Email:
quantum@bsi.bund.de

Image by Maedeh Amini-Bashiri