Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Post-Quanten-Kryptografie in die Anwendung bringen

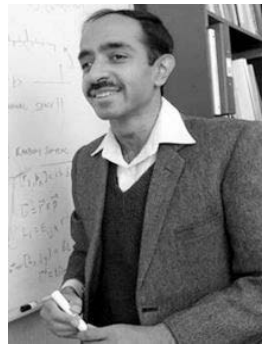
Dr. Gerhard Schabhüser

Vizepräsident BSI

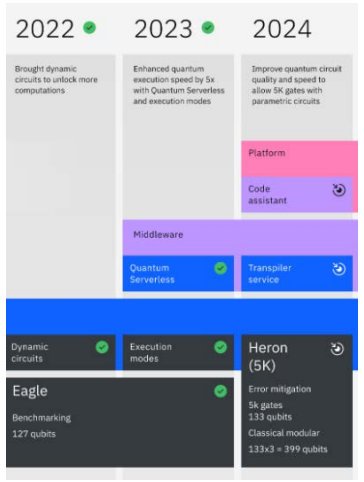
Omnisecure, 21.1.2025

Motivation

Public-Key Kryptografie und Quantencomputing



Lov Grover



A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Elliptic Curve Cryptosystems

By Neal Koblitz

1970er | 1980er | 1990er | 2020er | 2030er

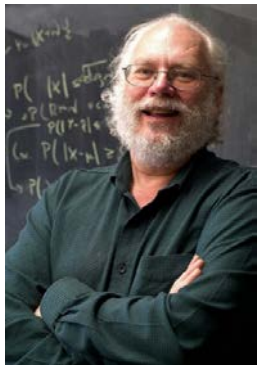
New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Use of Elliptic Curves in Cryptography

Victor S. Miller



Peter Shor

Article

Quantum supremacy using a programmable superconducting processor

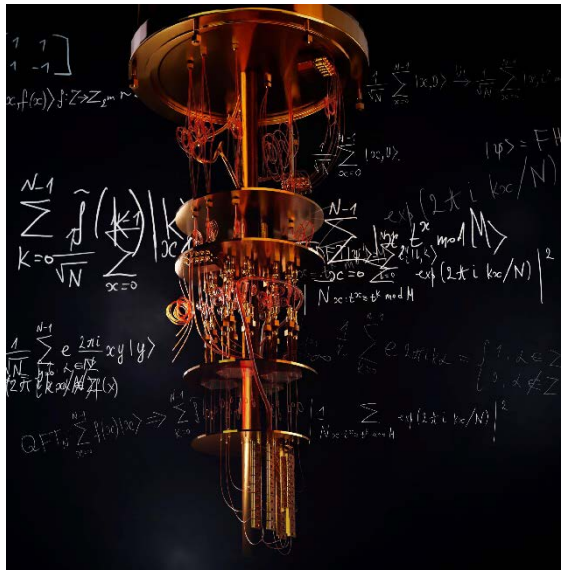
Quantum error correction below the surface code threshold

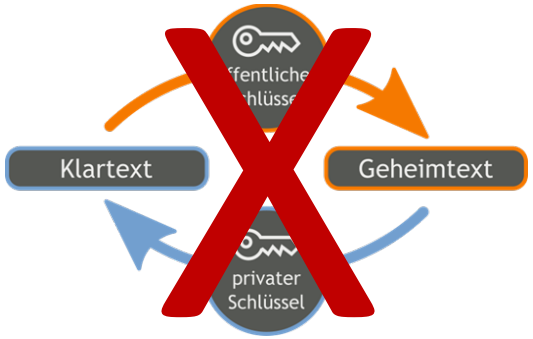
Google Quantum AI and Collaborators

Bundesamt für Sicherheit in der Informationstechnik

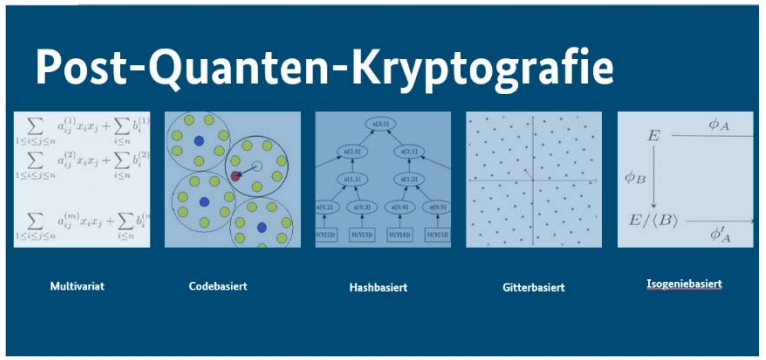
Deutschland Digital•Sicher•BSI•

Motivation



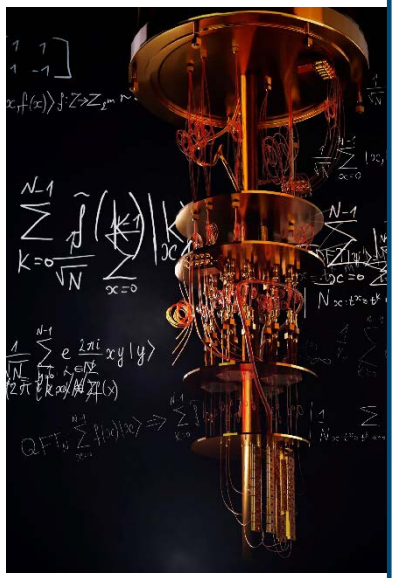


Derzeit eingesetzte Public-Key-Kryptografie



Quantensichere Kryptografie

Motivation



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

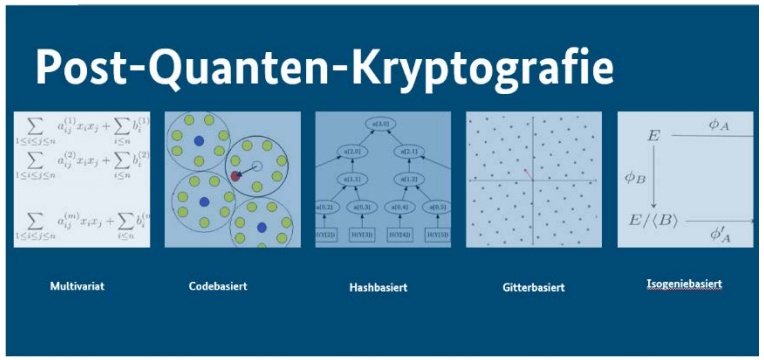
Swedish National Communications Security Authority,

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.



Quantensichere Kryptografie

Die Priorität sollte klar auf der **Migration zu PQC** liegen

[BSI-Position zu QKD]

Die wichtigsten Bedrohungsszenarien

1

Store now, decrypt later

→ Quantensichere Verschlüsselung

2

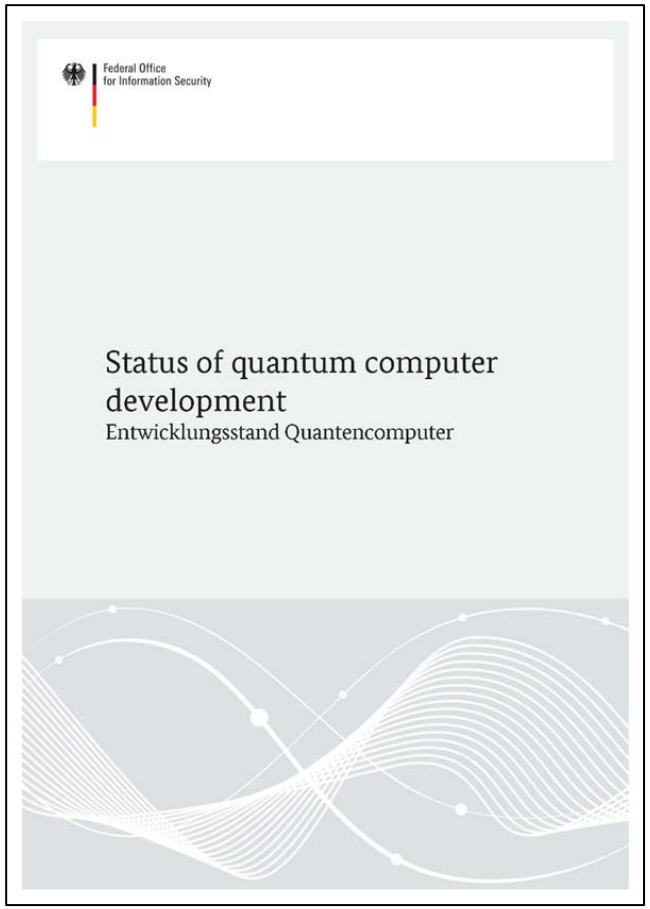
Komplexe oder langwierige Migration (z.B. PKI)

→ haupts. quantensichere Authentisierung

BSI Studie „Status of quantum computer development“

Neuerungen aus dem Update Januar 2025 (Version 2.1):

- Grundannahme Quantenfehlerkorrektur in 2024 bestätigt
- Es ist wahrscheinlich, dass ein kryptografisch relevanter Quantencomputer **in den nächsten 16 Jahren realisierbar** wird.
- Neue Entwicklungen in der Fehlerkorrektur und –mitigation und Hardware: mögliche Beschleunigung auf **knapp 10 Jahre**.



Verfügbar unter www.bsi.bund.de/qcstudie.

Empfehlungen des BSI

TR-02102: Update 2025

Public-Key-Verschlüsselung und Schlüsseleinigung

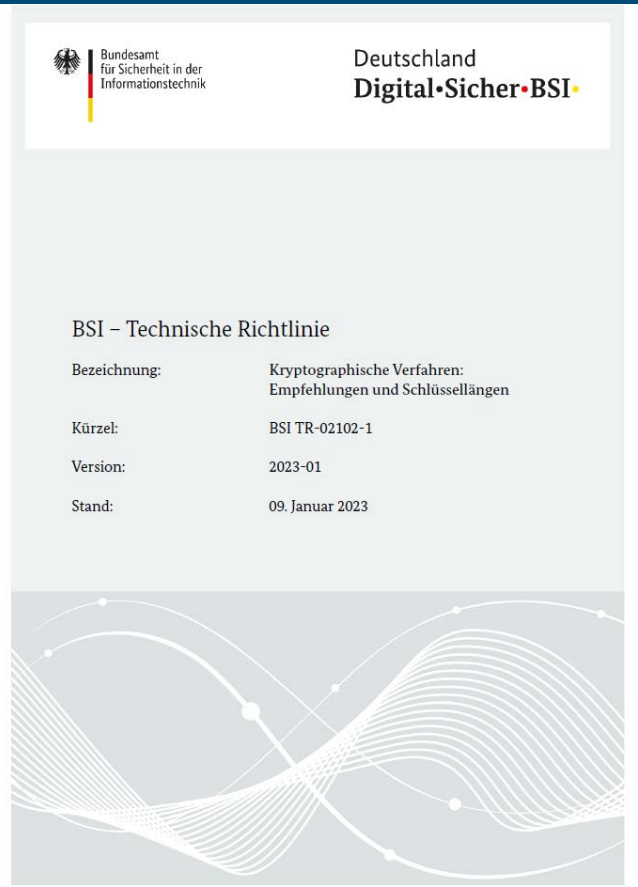
- **Neu:** Empfehlung von ML-KEM-768 und ML-KEM-1024
- FrodoKEM und Classic McEliece weiterhin empfohlen

Signaturverfahren

- **Neu:** Empfehlung von ML-DSA und SLH-DSA
- Konkretisierung der empfohlenen Parametersätze für LMS/HSS und XMSS/XMSS^MT

Migration zu quantensicheren Verfahren

- Hybrider Einsatz von traditioneller Krypto und PQC empfohlen
- Empfehlungen für konkrete Verfahren aktualisiert
- **Ankündigung:** in einer zukünftigen Version werden keine nicht-quantensicheren Verfahren mehr für den nicht-hybriden Einsatz empfohlen
- **Ankündigung**: Abkündigung von nicht-quantensicheren Verfahren ggf. mit Frist < 7 Jahre



„Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography“

We urge public administration, critical infrastructure providers, IT providers, as well as all of industry, to **make the transition to post-quantum cryptography a top priority.** For the reasons outlined above, organizations and governments should **start the transition now** […]

[…] protection of the **most sensitive use cases**. To ensure an acceptable level of readiness, we recommend that these should be protected against ‘store now, decrypt later’ attacks as soon as possible, **latest by the end of 2030**.

Securing Tomorrow, Today

PQ-Migration in der Praxis

Was muss jetzt getan werden?

Schritte nicht strikt nacheinander ausführen. Hochpriorisierte Aufgaben sofort angehen.

Inventarisierung

- Welche Verfahren verwenden Kryptografie?
- Sensibilität der Daten, Lebensdauer
- Abhängigkeiten

Priorisierung

- Abwägung: Kosten der Migration vs. Schäden bei gebrochener Sicherheitsleistung → **Risikoorientierte Priorisierung**
- Wie lange dauert die Migration?

Umsetzung/ Planung

- Programmsteuerung aufsetzen
- Verantwortlichkeit festlegen, Kosten einkalkulieren
- Nötige ad-hoc-Maßnahmen sofort umsetzen

Rücksprache mit Dienstleistern, Softwarelieferanten, bei Einkauf auf Kryptoagilität achten etc.

Weitere Migrations-Aktivitäten

- Standardisierung bei *IETF/IRTF, ETSI*:
  - CFRG KEM combiners design team
  - OpenPGP
  - Hash-basierte Signaturen in X.509 Zertifikaten
  - Hybride KEMs in TLS 1.3
  - Multiple Schlüsselaushandlungen in IKEv2
  - PQUIP
  - Hybride Schlüsseleinigung
  - …
- BSI-Projekte:
  - PQC in Kryptobiblitohek Botan
  - PQC in OpenPGP
  - Quantensichere Verwaltungs-PKI (“V-PKI”)
- Veranstaltungen & Ressourcen zum Thema PQ-Migration
- …

Fazit

- Der kryptografische Umbruch hin zu quantensicherer Kryptografie hat begonnen: Es gibt Standards, Empfehlungen und erste Produkte
- Die Migration zu quantensicherer Kryptografie wird kompliziert und langwierig
- **Maßnahmen sind bereits jetzt möglich und nötig: Inventur, Risikobewertung und Planung**
- Handlungsempfehlungen:
  - Kryptoagilität
  - Hybride Lösungen
- **Awareness** muss weiter gesteigert werden

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Gerhard Schabhüser
Vizepräsident

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de