



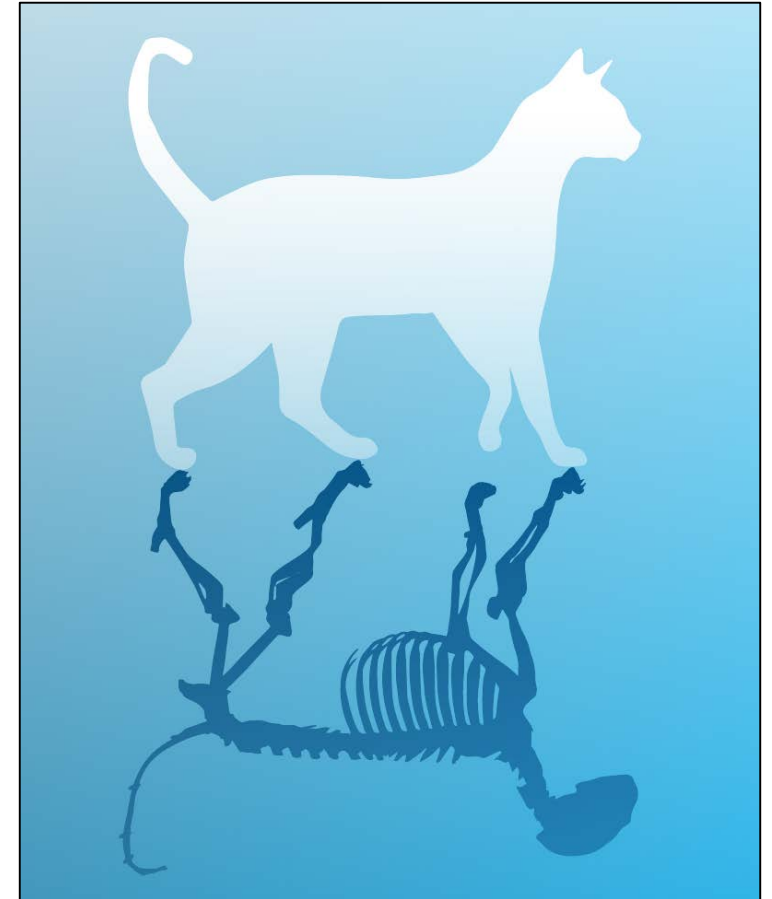
# QKD and PQC from a security perspective

Dr. Manfred Lochter

World of Quantum, 29. June 2023

# Take away message

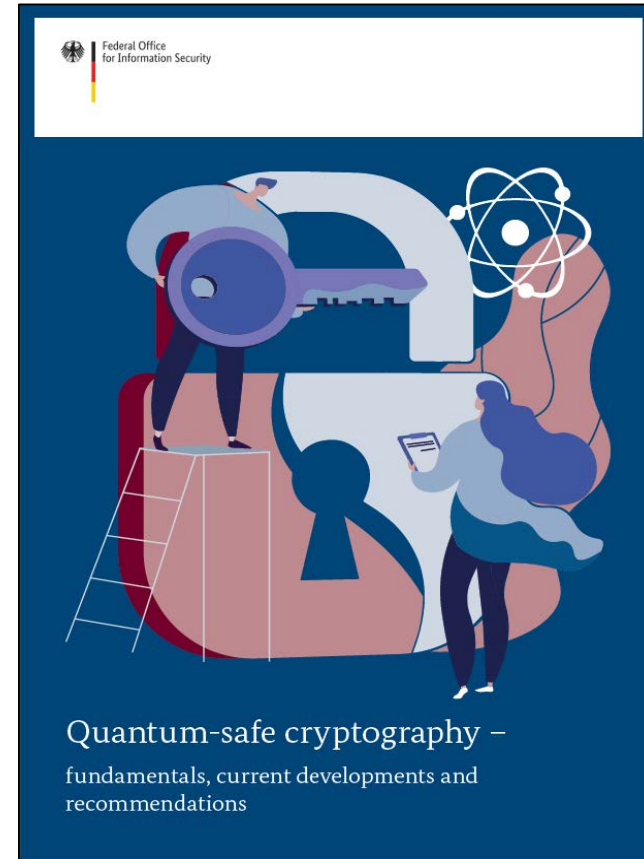
The Quantum Threat  
Two solutions: PQC & QKD  
Migration urgent  
Priority for PQ  
Lack of Awareness



The talk is from BSI's perspective, but reflects my personal views.

# Two solutions

- PQ: Security relies on **complexity assumptions**
- QKD: Security relies on **physical assumptions**
- **Implementation security** is an issue for both solutions.
- Different maturity levels and availability of products



# Report on the Security of LWE: Improved Dual Lattice Attack

MATZOV

Many of the leading post-quantum key exchange and signature schemes rely on the conjectured hardness of the Learning With Errors (LWE) and Learning With Rounding (LWR) problems and their algebraic variants, including 3 of the 6 finalists in NIST's PQC process. The best known cryptanalysis techniques against these problems are primal and dual lattice attacks, where dual attacks are generally considered less practical.

In this report, we present several algorithmic improvements to the dual lattice attack, which allow it to exceed the efficiency

# The NIST Process

- RAINBOW-Attack
- SIKE-Attack
- Improved Lattice Attack
- Backdoor
- Keylengths?
- Products?
- Implementation security

In general there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should. So sometimes all it takes is someone who recognizes the applicability of existing theoretical math to these new cryptosystems. That is what happened here.  
**(David Jao, ars technica)**

### Signature Correction Attack on Dilithium Signature Scheme

Saad Islam <i>Worcester Polytechnic Institute</i> Worcester, MA, USA sislam@wpi.edu	Koksul Mus <i>Worcester Polytechnic Institute</i> Worcester, MA, USA kmus@wpi.edu	Richa Singh <i>Worcester Polytechnic Institute</i> Worcester, MA, USA rsingh7@wpi.edu
Patrick Schaumont <i>Worcester Polytechnic Institute</i> Worcester, MA, USA pschaumont@wpi.edu	Berk Sunar <i>Worcester Polytechnic Institute</i> Worcester, MA, USA sunar@wpi.edu	

Candidate	Required Security Level By NIST [Nat16]	Estimated Security Level	
		[DKL+21] [ABD+21] [BMD+20]	This Work
Kyber512	143	151.5	<b>137.5</b>
Kyber768	207	215.1	<b>193.5</b>
Kyber1024	272	287.3	<b>257.8</b>
Dilithium2	146	159	<b>146.3</b>
Dilithium3	207	217	<b>202.0</b>
Dilithium5	272	285	<b>263.6</b>
LightSaber	143	Unspecified	<b>138.4</b>
Saber	207	Unspecified	<b>202.7</b>
FireSaber	272	Unspecified	<b>264.9</b>

# How are BSI's recommendations impacted?

- None of the algorithms recommended by BSI was attacked
- We explicitly did not recommend RAINBOW and SIKE
- We will not adopt NIST recommendations without own analysis
- We continue to recommend FrodoKEM & Classic McEliece
- ISO standardisation of our preferred algorithms
- No plans for a German or European competition
- More research needed
- Implementation security

A notable strength of Frodo is that the random matrix  $A$  is completely unstructured, and as a consequence, the security of FrodoKEM depends on the plain LWE problem rather than on its structured variants (Module-LWE or Ring-LWE). This means that FrodoKEM could remain secure even in a future world where structured lattices are broken.

(NIST)





# Frodo

ISO Standardisation  
BSI lead editor  
Kyber/McEliece

**FrodoKEM – Preliminary Draft Standard**

**Contents**

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviations	1
5	General model for key encapsulation mechanism	2
6	FrodoKEM parameters	2
6.1	Public matrix A	2
6.2	Deterministic random bit generation	2
7	Supporting functions	3
7.1	Octet encoding of bit strings	3
7.2	Matrix encoding of bit strings	3
7.3	Packing matrices modulo $q$	3
7.4	Sampling from the error distribution	4
7.5	Matrix sampling from the error distribution	4
7.6	Pseudorandom matrix generation	4
7.6.1	Matrix A generation with AES128	4
7.6.2	Matrix A generation with SHAKE128	5
8	Key encapsulation mechanism	5
8.1	Key generation	5
8.2	Encapsulation	5
8.3	Decapsulation	6
9	Security considerations	7
9.1	Cryptanalytic attacks: the "core-SVP" hardness	7
9.1.1	Refined security estimates	7
9.2	Security reductions	7
9.3	Decryption failures	8
9.4	Backdoors and all-for-the-price-of-one attacks exploiting the matrix A	8
9.5	Security against multi-target and multi-ciphertext attacks	8
9.5.1	Multi-target attacks	8
9.5.2	Multi-ciphertext attacks	9
9.6	Ephemeral FrodoKEM	9
10	Implementation considerations	9
10.1	Reusing A	9
10.2	Side-channel resistance	9
10.2.1	Timing attacks	9
10.2.2	Other side-channel attacks	9
Annex A (informative)	Parameters	11
Annex B (informative)	FrodoKEM security estimates: core-SVP hardness	14
Annex C (informative)	Refined security analysis	15
Annex D (informative)	Security estimates for FrodoKEM derived from reductions	16
Bibliography		17

ii

Date: 2023-03-14

## FrodoKEM: Learning With Errors Key Encapsulation

Preliminary Draft Standard

WD/CD/DIS/FDIS stage

### Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

# Handlungskonzept Quantentechnologien

## Infokasten 2 Vision 2036

Deutscher Bundestag

Drucksache 20/6610

20. Wahlperiode

28.04.2023

### Unterrichtung

durch die Bundesregierung

Handlungskonzept Quantentechnologien der Bundesregierung

Inhaltsverzeichnis

Seite

1. Die Potenziale der Quantentechnologien für Deutschland nutzen.....	3
2. Große Herausforderungen, außerordentliches Potenzial.....	7
3. Technologie auf Spitzenniveau für Gestaltungskraft und technologische Souveränität.....	12
A. Quantentechnologien für Wirtschaft, Gesellschaft und staatliche Institutionen nutzbar machen.....	13
Wirtschaftliche Innovationskraft.....	14
Gesellschaftlichen Herausforderungen.....	15
Sicherheit und Souveränität.....	16
B. Die Technologieentwicklung mit Blick auf künftige Anwendung zielgerichtet vorantreiben.....	16
Technologische Grenzen verschieben.....	16
Standards setzen.....	17
C. Exzellente Rahmenbedingungen für ein starkes Ökosystem schaffen.....	20
Schnittstellen schaffen: Die Ökosysteme stärken.....	20
Gründerkultur und innovative Unternehmen stärken.....	20
Interesse wecken, Fachkräfte gewinnen.....	21
Auswirkungen im Blick behalten: Chancen erkennen und Auswirkungen betrachten.....	22

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

Für die Entwicklung der Quantentechnologien aus einer Zukunfts- in eine zentrale Schlüsseltechnologie ist ein Zeithorizont erforderlich, der den zeitlichen Rahmen dieses Handlungskonzepts deutlich übersteigt. Die Bundesregierung setzt daher auf eine auch von der Expertenkommission Forschung und Innovation geforderte<sup>1,12</sup> Weiterentwicklung der Maßnahmen und eine langfristige, nachhaltige Förderung und Entwicklung der Technologie. Im Fall des Quantencomputing ist ein technologieneutrales Vorgehen besonders wichtig, solange sich nicht stärker abzeichnet, welche Realisierung von Qubits für die Weiterentwicklung von Quantencomputern am vorteilhaftesten ist. Denkbar ist außerdem, dass sich unterschiedliche Hardware-Plattformen für unterschiedliche Anwendungen besonders eignen werden.

Langfristig sollen Quantentechnologien als Schlüsseltechnologie in verschiedensten Anwendungsfeldern etabliert sein. Für das Jahr 2036, zehn Jahre nach Auslaufen dieses Handlungskonzepts, ist unser Zielbild:

- Quantentechnologien sind Kernkomponenten in vielfältigen wirtschaftlichen Anwendungsbranchen. Sie leisten bedeutende Beiträge zur Wertschöpfung in Deutschland und zum Umgang mit den drängenden Zukunftsthemen unserer Gesellschaft, unter anderem:
  - o Quantensensoren haben sich in einer Vielzahl von wirtschaftlichen und gesellschaftlich relevanten Anwendungen durchgesetzt. So profitiert das Bauwesen bei der Bodenerkundung von innovativen Sensortypen, in der Medizintechnik ermöglichen Quantensensoren neuartige Diagnosemöglichkeiten und in der Informations- und Kommunikationstechnik gelingt verbesserte Signalverarbeitung durch den Einsatz hochgenauer Atomuhren.
  - o Komplexe Anwendungsfälle werden auf in Deutschland hergestellten universellen fehlerkorrigierten Quantencomputern gelöst. Quantencomputer und Spezialrechner, bspw. Quantensimulatoren oder Quantenannealer, spielen eine signifikante Rolle in mehreren Branchen, beispielsweise der chemischen und der pharmazeutischen Industrie, der Finanzbranche und dem Automobilssektor.
  - o Sensible Daten in Verwaltung und Sicherheitsbehörden werden über verwaltungsinterne Netze ausgetauscht, die auf quantencomputerresistenten Kryptografieverfahren basieren. Die verwaltungsinternen Netze besitzen sichere und definierte Übergänge zu weiteren Kommunikationspartnern. Sensible Daten kritischer Infrastrukturen und der Wirtschaft werden durch quantencomputerresistente Kryptografieverfahren geschützt und in Teilbereichen zusätzlich durch Quantenkommunikation abgesichert. Standorte von wirtschaftlicher, wissenschaftlicher oder hoheitlicher Relevanz sind über ein sicheres EU-weites Quantenkommunikationsnetzwerk verbunden.
  - o Die deutschen Aktivitäten im Bereich der Standardisierung und die signifikante Erhöhung der Präzision in Zeit-, Masse- und Stromnormalen durch die Quantenmetrologie bilden die Grundlage für ein internationales quantenbasiertes Standardisierungssystem.



# VISION 2036

Sensible Daten in **Verwaltung und Sicherheitsbehörden** werden über verwaltungsinterne Netze ausgetauscht, die auf **quantencomputerresistenten** Kryptografieverfahren basieren. Die verwaltungsinternen Netze besitzen sichere und definierte Übergänge zu weiteren Kommunikationspartnern. Sensible Daten kritischer **Infrastrukturen und der Wirtschaft** werden durch quantencomputerresistente Kryptografieverfahren geschützt und in **Teilbereichen zusätzlich** durch **Quantenkommunikation** abgesichert. Standorte von wirtschaftlicher, wissenschaftlicher oder hoheitlicher Relevanz sind über ein sicheres EU-weites Quantenkommunikationsnetzwerk verbunden.



# Handlungskonzept Quantentechnologien

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

# When can we expect cryptographically relevant Quantum Computers?

## BSI's Working assumption for high security applications:

A cryptographically relevant Quantum Computer will be available by the begin of the 2030ies.

(BT DS 19/26340)

This is not a forecast but a **risk management assumption**

See [www.bsi.bund.de/qcstudie](http://www.bsi.bund.de/qcstudie). New version in preparation.

„Cryptographically relevant“ is undefined

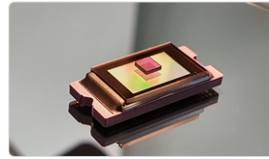
“I estimate a 1/6 chance of breaking RSA-2048 by 2026 and 1/2 chance by 2031.”

(Michele Mosca, 2017)

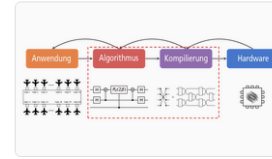
The screenshot shows the SecurityWeek website header with navigation links for Cybersecurity News, Webcasts, and Virtual Events. The main article is titled "Quantum Computing Is for Tomorrow, But Quantum-Related Risk Is Here Today" by Kevin Townsend, dated January 03, 2022. The article discusses a report by Booz Allen Hamilton on quantum computing arms race and risk management. A sidebar on the right offers a "GET THE DAILY BRIEFING" service with a search bar and social media icons.

# Initiatives

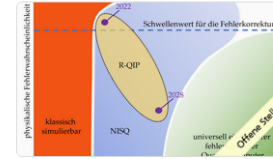
## Unsere Anwendungs-Projekte



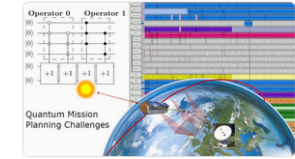
**XQI: Quantencomputer auf Basis von NV-Zentren in Diamanten**



**ALQU: Algorithmen für Quantencomputer-Entwicklung im Hardware-Software-Codesign**



**R-QIP: Reliable Quantum Information Processing**

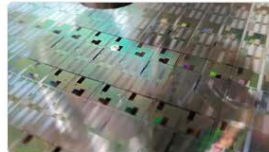


**QMPC: Quantum Mission Planning Challenges**

## Projekte



**SuNQC: Quantencomputer auf Basis von NV-Zentren in Diamanten mit Schwefel-dotierungen**



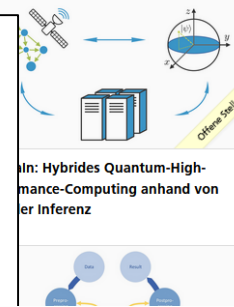
**Legato: Prototypischer Multichip-Quantencomputer mit bis zu 100 Ionenfallen-Qubits**



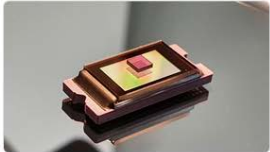
**SQuAp: Spin-Qubit-Analyseplattform für Farbzentren-basierte Quantenhardware**



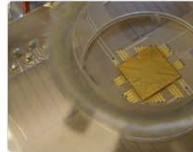
**DIAQ: Diamantmaterial für Raumtemperatur-Quantencomputer**



**Hybrides Quantum-High-Performance-Computing anhand von Inferenz**



**XQI: Quantencomputer auf Basis von NV-Zentren in Diamanten**



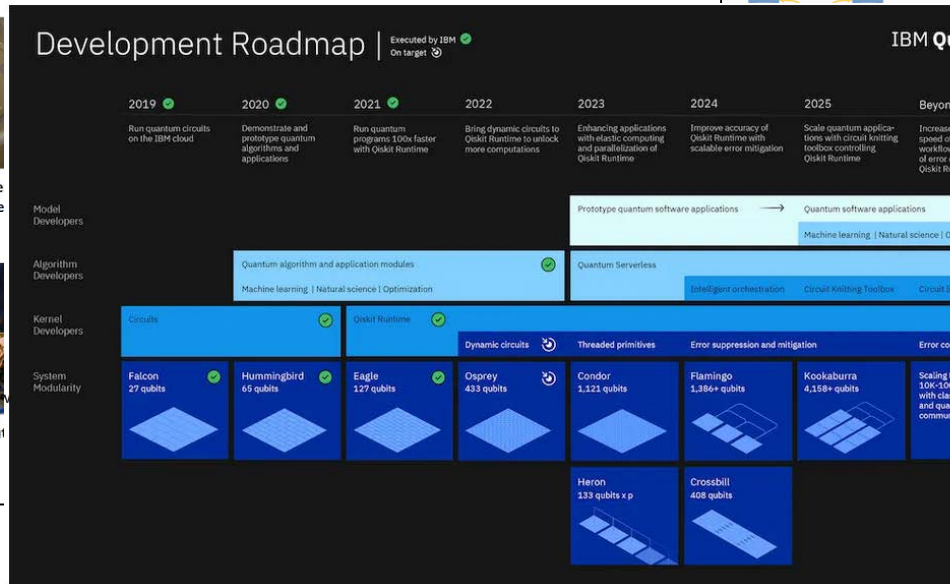
**QSea II: Modularer und skalierbarer Ionenfallen-Quantencomputer**



**REDAC: Reconfigurable Discrete Analog Computer**



**Photonischer Quantencomputer zu 64 Qubits**



## Technologie

31.05.2021

### „Mission Quantencomputer“ gestartet

Quanten und ihre Phänomene sind seit mehr als 100 Jahren bekannt. Quantentechnologie ist aber hochkomplex und ihre Effekte teilweise erst heute technologisch nutzbar. Ziel der Bundesregierung ist der strategische Ausbau der Quantentechnologie. Die Mission Quantencomputer wird mit 1,1 Mrd. Euro vom BMBF gefördert, insgesamt stehen 2 Mrd. Euro für die Entwicklung von Quantentechnologie bereit.



© BMBF/Hans-Joachim Rickel

# Migration to Quantum Safe Cryptography

HOME | PRESS ROOM | NEWS & HIGHLIGHTS | ARTICLE

**Announcing the Commercial National Security Algorithm Suite 2.0**

CYBERSECURITY ADVISORY

PRESS RELEASE | Sept. 7, 2022

**NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems**

Administration | Priorities | C

BRIEFING ROOM

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

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

MEMORANDUM FOR THE VICE PRESIDENT

THE SECRETARY OF STATE

THE SECRETARY OF THE TREASURY

THE SECRETARY OF DEFENSE

THE ATTORNEY GENERAL



- “To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of **mitigating as much of the quantum risk as is feasible by 2035.**”
- "Within 90 days of the date of this memorandum, the Secretary of Commerce, through the Director of NIST, shall initiate an **open working group** with industry, including critical infrastructure owners and operators, and other stakeholders, as determined by the Director of NIST, to further advance adoption of quantum-resistant cryptography. "
- "Within 90 days of the date of this memorandum, the Secretary of Commerce, through the Director of NIST, shall establish a “**Migration to Post-Quantum Cryptography Project**” at the National Cybersecurity Center of Excellence to work with the private sector to address cybersecurity challenges posed by the transition to quantum-resistant cryptography."
- "Within 180 days of the date of this memorandum, and annually thereafter, the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in coordination with Sector Risk Management Agencies, shall engage with **critical infrastructure** and SLTT partners regarding the risks posed by quantum computers"
- "Within 1 year of the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, the Director of OMB, in coordination with the Director of CISA and the Director of NIST, shall issue a **policy memorandum requiring** FCEB Agencies to develop a plan to upgrade their non-NSS IT systems to quantum-resistant cryptography."
- "By December 31, 2023, agencies maintaining **NSS shall implement symmetric-key protections** (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges, where appropriate and in consultation with the National Manager.“

<https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/>  
<https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>



# Migration and Awareness

Which cryptographic algorithms are used by your organisation?

How critical are data that are cryptographically protected? Lifetime of data?

Is there an immediate need to act?

Must protocols be changed?

What could hinder the PQ migration?

Who needs to be involved?

Procurement Cycles?

Regulatory actions

**Migration is a process**

In Staat, Wirtschaft und Gesellschaft ist die Dringlichkeit des Wechsels zu quantensichererer Kryptografie akzeptiert und in kritischen Bereichen eingeleitet. Pilot-Infrastrukturen binden Partner aus den verschiedenen Bereichen ein.  
(CSS 2025)

# Awareness survey

- English version soon
- Most participants believe they will not achieve quantum-safety in time

in Zusammenarbeit mit:

**KPMG**  **Bundesamt für Sicherheit in der Informationstechnik** **Umfra­ge zu Kryptografie und Quantencomputing für CompuGlobal HyperMegaNet**

Durch die fortschreitende Digitalisierung wird ein immer größerer Anteil unserer Daten digital gespeichert, verarbeitet und übertragen. Dieser Trend eröffnet uns beachtliche neue Möglichkeiten, macht uns aber immer abhängiger von Technologie. Kryptografie ist dabei essentiell um die Authentizität, Integrität und Vertraulichkeit von Information sicher zu stellen. Von vielen Augen unbemerkt ist Kryptografie im digitalen Zeitalter geradezu omnipräsent.

Mit Quantencomputing kommt eine Technologie auf, die sich die spezifischen Gesetze der Physik der kleinsten Teilchen (Quantenmechanik) zu Nutze macht, um effiziente Berechnungen durchzuführen. Es ist unklar, wann die Reife zur praktischen Anwendung erreicht ist, jedoch existiert die Technologie bereits und wird von Monat zu Monat leistungsfähiger.

Von Biotechnologien bis zur Städteplanung hat Quantencomputing das Potential enorme Fortschritte zu bringen, aber es stehen auch Auswirkungen auf die Sicherheit von Informationen und Kommunikation bevor. Kryptographische Verfahren, die heute als sicher gelten und fest in unsere digitalen Infrastrukturen integriert sind, können in Zukunft mit Quantencomputern gebrochen werden und müssen daher bald durch neue, quantensichere Methoden, wie beispielsweise die Post-Quanten-Kryptografie, ersetzt und ergänzt werden.

Wir dürfen nicht nur auf die Möglichkeiten dieser emergenten, revolutionären Technologie schauen. Wir müssen auch für die Risiken gewappnet sein, denn die Bedrohung ist groß und geht tief. Das BSI hat dazu unlängst den Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ veröffentlicht. Um Staat, Wirtschaft und Gesellschaft bei diesem Thema bestmöglich zu unterstützen, möchten wir den aktuellen Zustand besser verstehen und Aufmerksamkeit auf das Thema lenken.

Ihre Antworten in diesem Fragebogen helfen uns beim Erreichen dieser beiden Ziele und dafür bedanken wir uns bei Ihnen. Es wird ein Ergebnisbericht erstellt, den alle Teilnehmenden erhalten.

1. **Zu welchen Zwecken werden von Ihrer Organisation kryptographische Verfahren eingesetzt?\***

- Als Bestandteil unserer Produkte
- Zum Schutz unserer Intellectual Property
- Für die Sicherheit des Kundenkontakts (Webshops, Kommunikation, etc.)
- Zur Steuerung und Schutz unserer Produktionsanlagen
- Zur Einhaltung des Datenschutzes/gesetzlicher Vorgaben
- Für die Sicherung unserer internen Kommunikation
- Gar nicht


2. **Wie sehen Sie die Auswirkung von Quantencomputing auf die Kryptografie?**

- Heutige kryptographische Verfahren werden fast vollständig obsolet.
- Spezifische kryptographische Verfahren werden gebrochen, diese sind aber weit verbreitet.
- Spezifische kryptographische Verfahren werden gebrochen, diese finden aber nur in wenigen Bereichen Verwendung.
- Die Auswirkungen bleiben auf sehr seltene, hoch spezialisierte Anwendungen beschränkt.
- Weiß ich nicht.

3. **Welche Relevanz von Quantencomputing für die Sicherheit von kryptographischen Verfahren erwarten Sie generell?**

- Hohe Relevanz
- Eher hohe Relevanz
- Eher niedrige Relevanz
- Niedrige Relevanz
- Keine Meinung

\* Mehrfachnennung möglich

**KPMG**  **Bundesamt für Sicherheit in der Informationstechnik**

## Marktumfrage Kryptografie und Quantencomputing





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

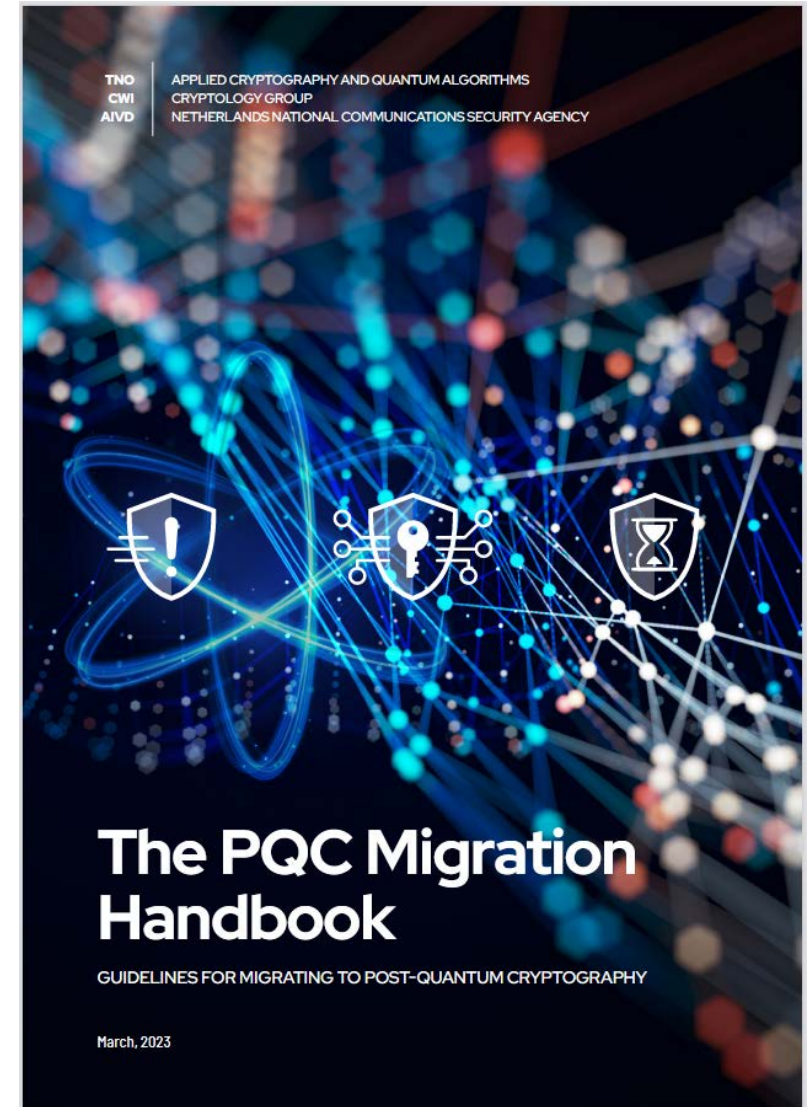
This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).<sup>1</sup>

**I. OVERVIEW**

Federal agencies<sup>2</sup> (“agencies”) are moving to a zero trust architecture, as directed by Executive Order 14028, *Improving the Nation’s Cybersecurity* (May 12, 2021)<sup>3</sup> and Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).<sup>4</sup> This paradigm shift relies in part on the ubiquitous use of strong encryption throughout agencies.

As outlined in NSM-10, the threat posed by the prospect of a cryptanalytically relevant quantum computer (CRQC)<sup>5</sup> requires that agencies prepare now to implement post-quantum cryptography (PQC). Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure Federal data and information systems.

<https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf>



<https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook>

# CC-Evaluation criteria for QKD – a first step

- PP-QKD funded by BSI, cooperation with ETSI
- Goal: An internationally accepted ETSI-Standard
- Included in Workplan of the ETSI ISG QKD
- Untypical approach
- Certification of the PP in progress
- Limited Scope: Point-to-Point Prepare & Measure QKD
- EAL4+AVA\_VAN.5+ALC\_DVS.2
- Packages to address different environments
- Options to address national policies, e.g. on randomisation

QKD often claims ITS: This will not be achieved in real Networks.

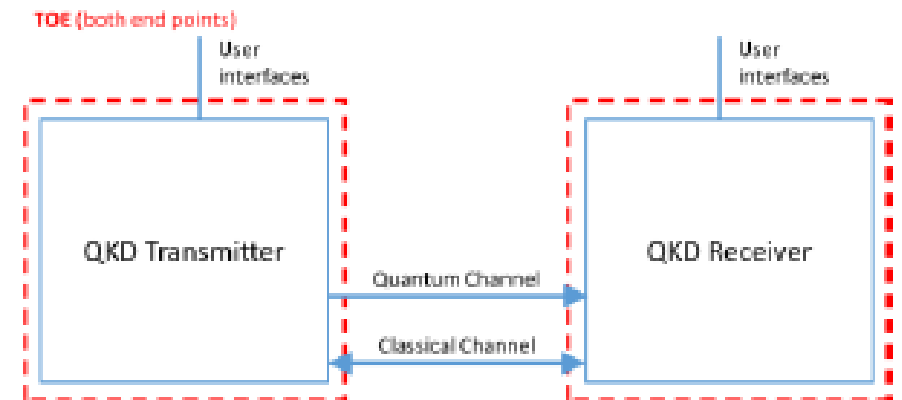


Figure 1: The TOE-boundary, i.e. the two QKD modules

# Practical Security

- No offer for Security-Proof project
- SCA project: Draft soon available for public comment
- PP- Certification almost complete
- No protocol standard



 Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI**

**Projekt 575**

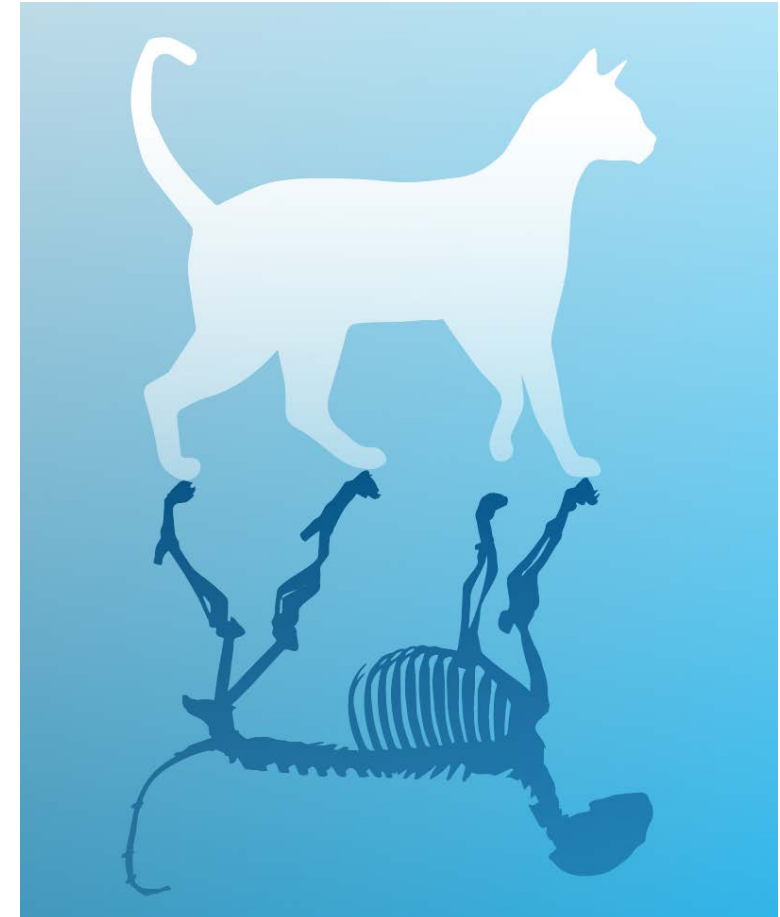
**Seitenkanalangriffe auf QKD-  
Systeme (QKD-Seitenkanalstudie)**

**Leistungsbeschreibung  
und Besondere Bewerbungsbedingungen**



# Conclusion

Urgency of migration  
Different maturity levels of PQ and QKD  
Awareness still missing



# Vielen Dank für Ihre Aufmerksamkeit!

Deutschland  
**Digital•Sicher•BSI**

## Kontakt

Dr. Manfred Lochter  
Principal Adviser Cryptography

Manfred.Lochter@bsi.bund.de  
Tel. +49 (0) 228 9582 5643

Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Godesberger Allee 185-189  
53175 Bonn  
[www.bsi.bund.de](http://www.bsi.bund.de)

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.