Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

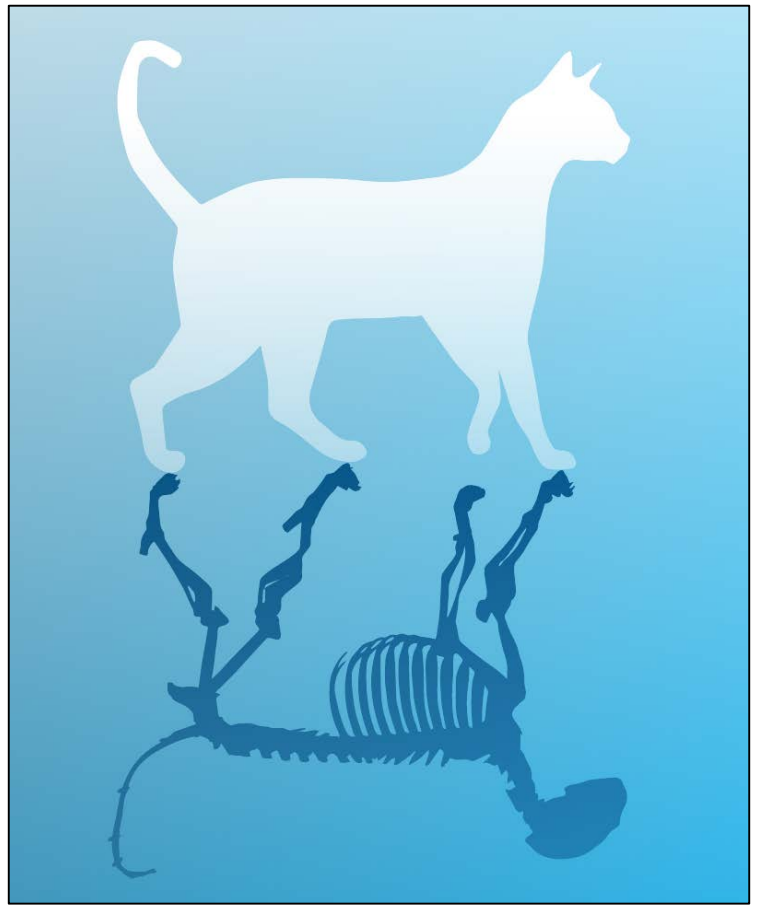
QKD and PQC from a security perspective

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

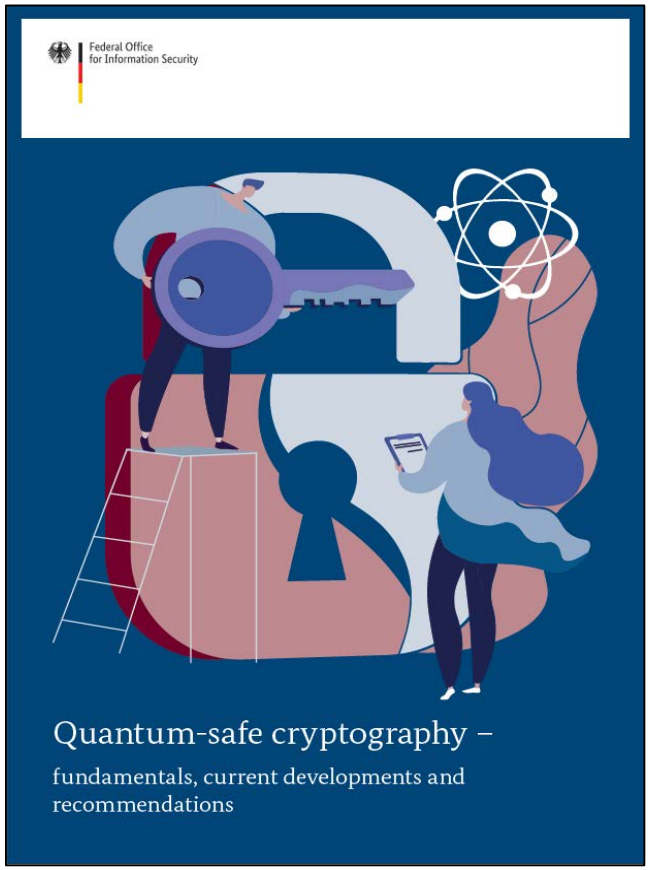


The talk is from BSI‘s perspective, but reflects my personal views.

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



Federal Office
for Information Security

BSI‘s focus is on the migration to PQ cryptography

The NIST Process

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

April 4, 2022 Report Open Access

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

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
Worcester Polytechnic Institute
Worcester, MA, USA
sislam@wpi.edu

Koksal Mus
Worcester Polytechnic Institute
Worcester, MA, USA
kmus@wpi.edu

Richa Singh
Worcester Polytechnic Institute
Worcester, MA, USA
rsingh7@wpi.edu

Patrick Schaumont
Worcester Polytechnic Institute
Worcester, MA, USA
pschaumont@wpi.edu

Berk Sunar
Worcester Polytechnic Institute
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	**137.5**
Kyber768	207	215.1	**193.5**
Kyber1024	272	287.3	**257.8**
Dilithium2	146	159	**146.3**
Dilithium3	207	217	**202.0**
Dilithium5	272	285	**263.6**
LightSaber	143	Unspecified	**138.4**
Saber	207	Unspecified	**202.7**
FireSaber	272	Unspecified	**264.9**

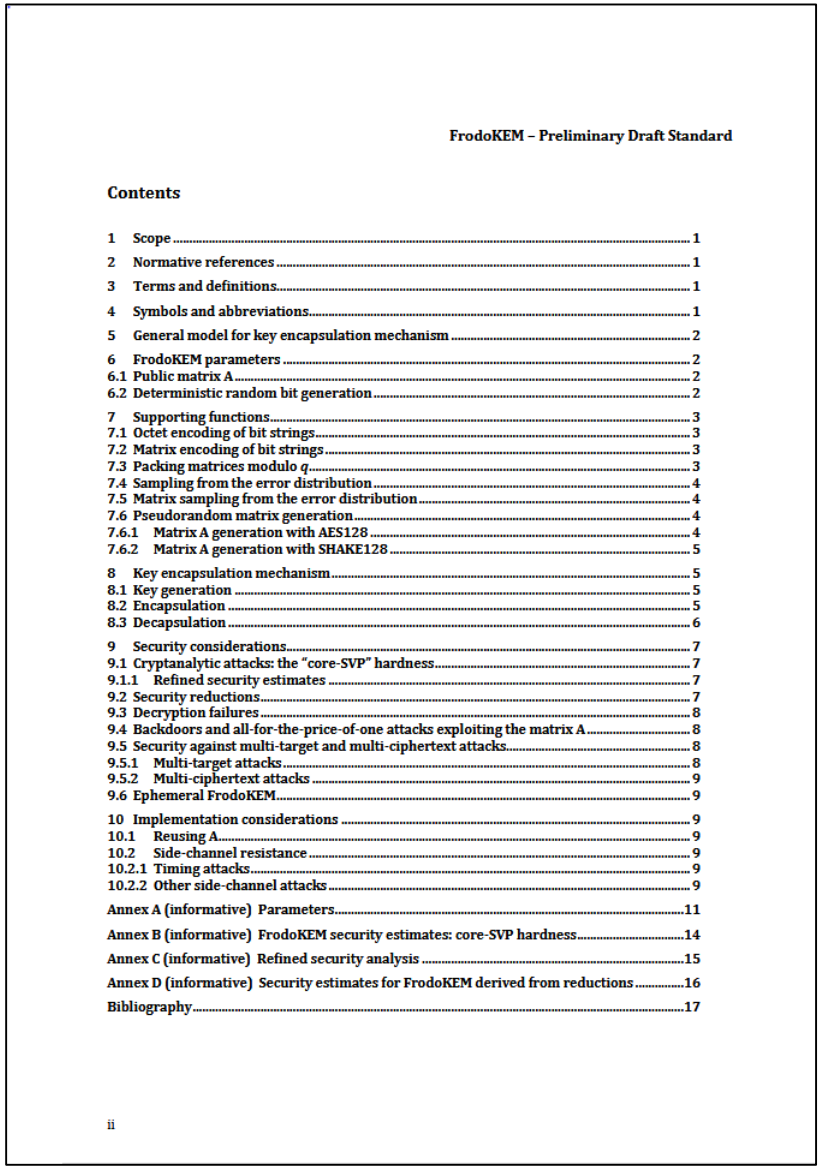
How are BSI‘s recommendations impacted?

- None of the algorithms recommended by BSI was attacked
- We explicitely 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)

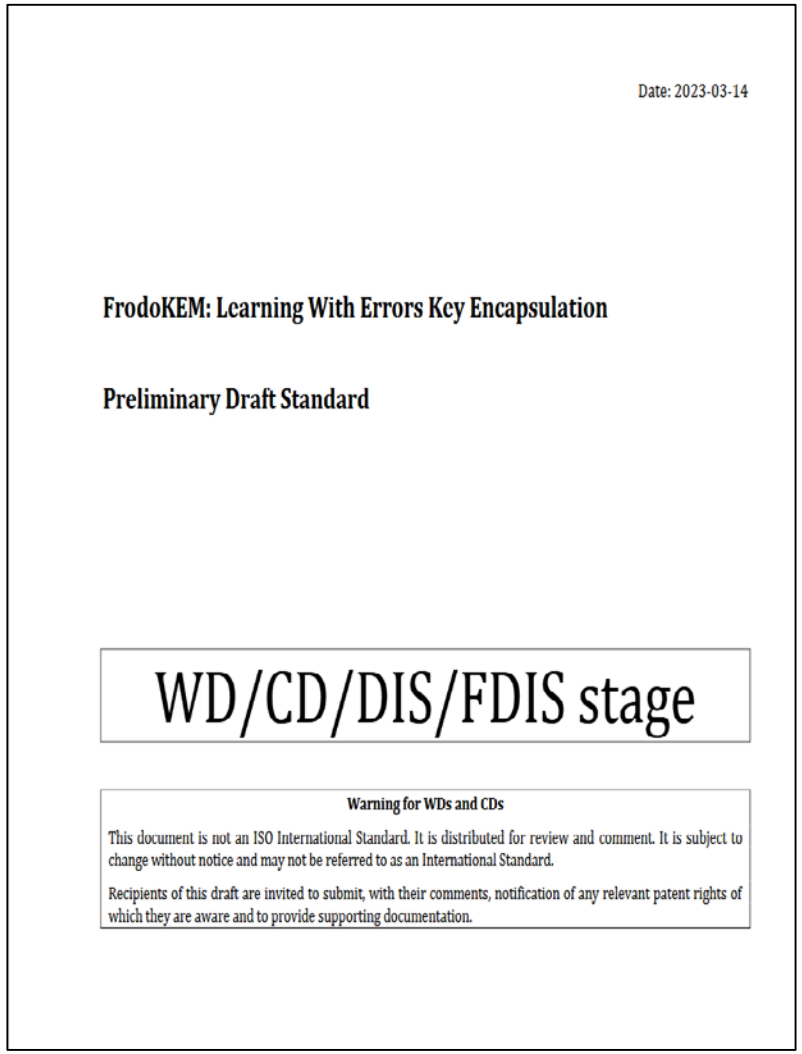
Frodo

ISO-Standardisation
BSI lead editor
Kyber/McEliece



FrodoKEM – Preliminary Draft Standard

Contents



Date: 2023-03-14

FrodoKEM: Learning With Errors Key Encapsulation

Preliminary Draft Standard

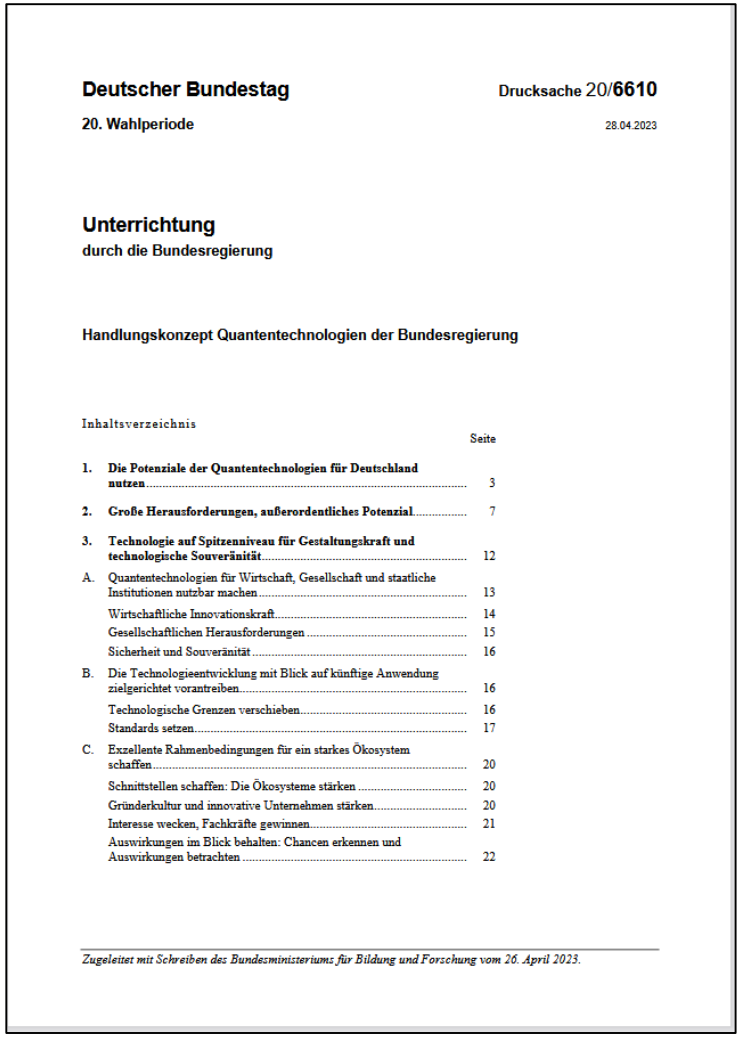
WD/CD/DIS/FDIS stage

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



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.

Infokasten 2 Vision 2036

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[1,12] 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:
  - 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.
  - 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 Automobilsektor.
  - 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.
  - 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.

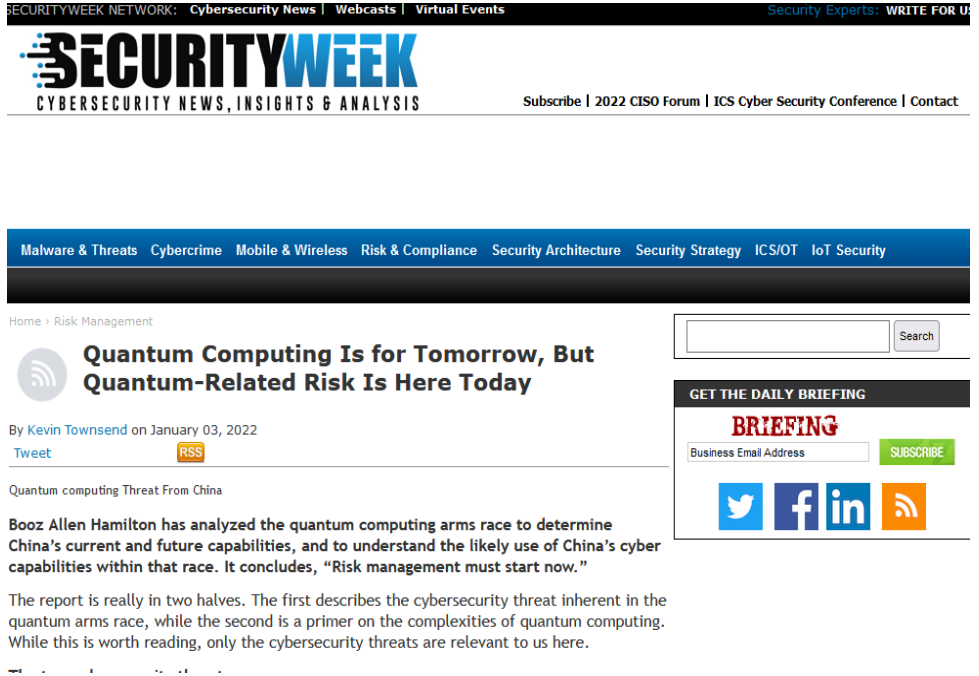
Handlungskonzept Quantentechnologien

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?

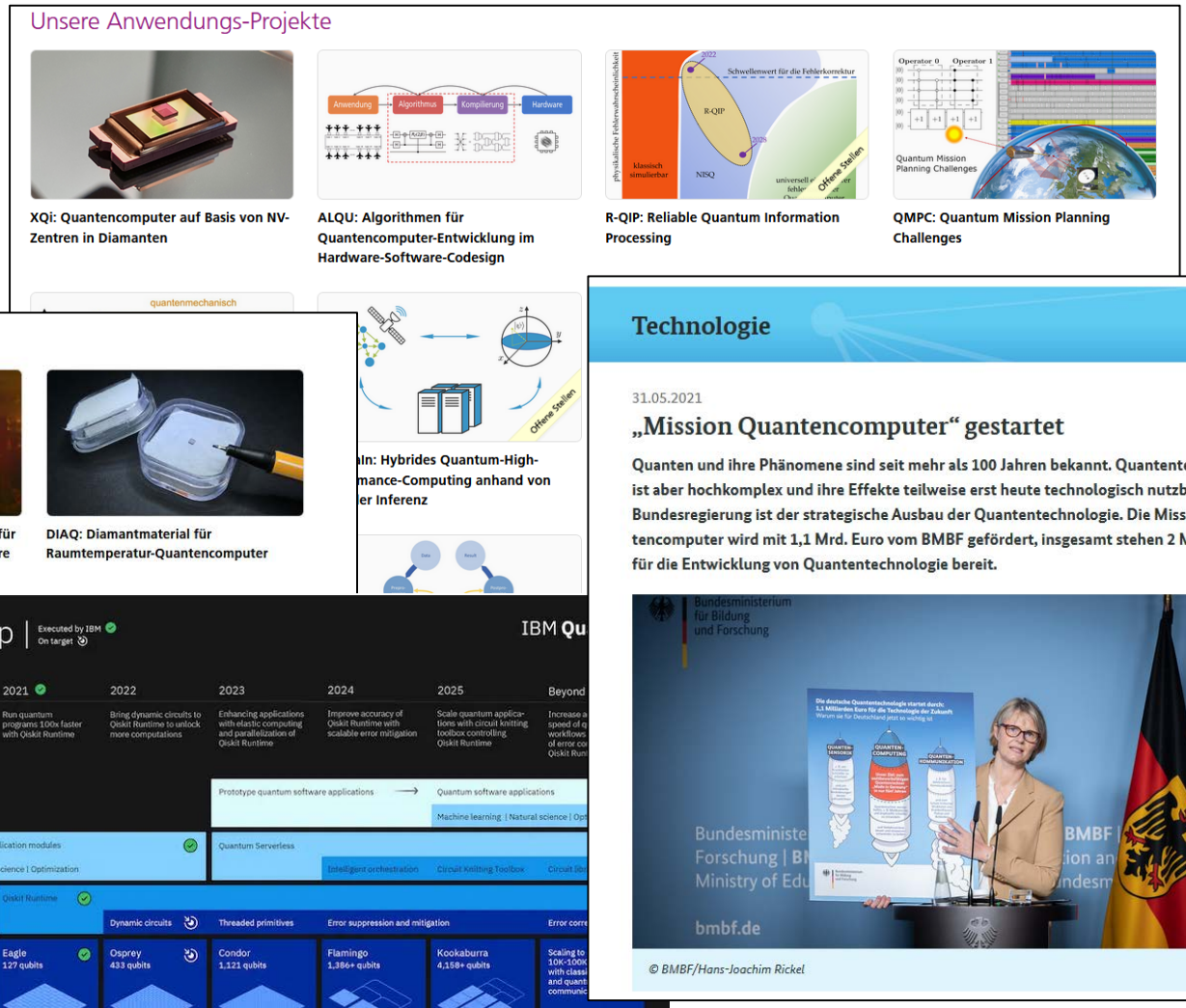
BSI's Working assumption for high security applications:
A cryptographically relevant Quantum Computer will be available by the begin of the 2030ies.
(BT DS 19/26340)

This is not a forecast but a **risk management assumption**
See www.bsi.bund.de/qcstudie. New version in preparation.
„Cryptographically relevant" is undefined

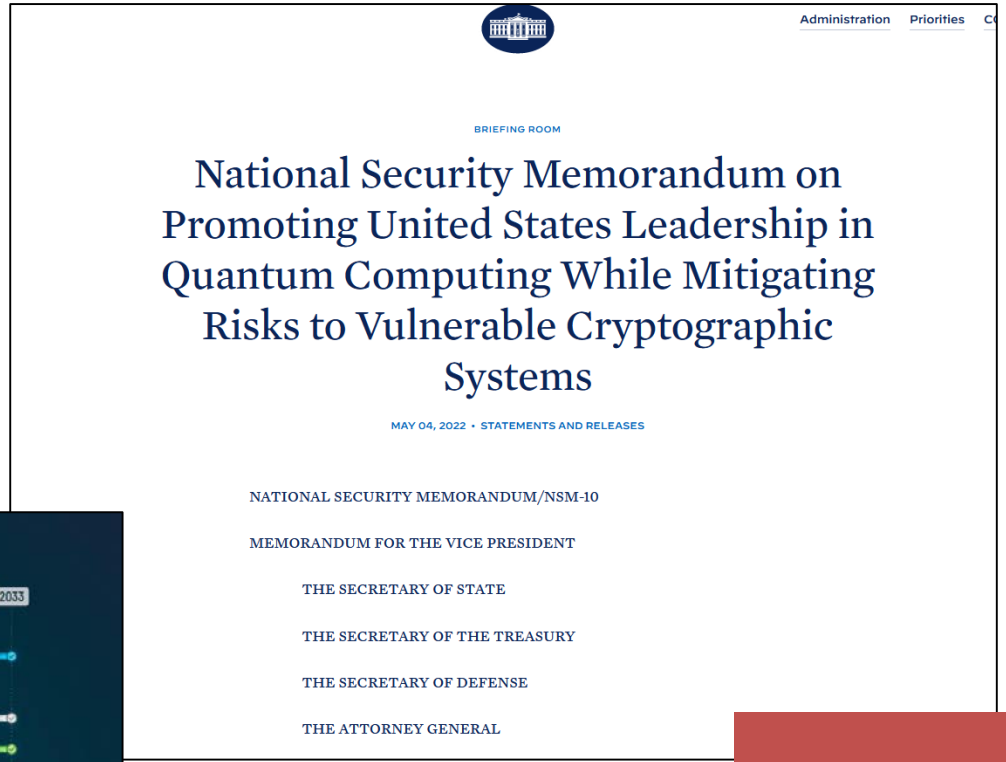


"I estimate a 1/6 chance of breaking RSA-2048 by 2026 and ½ chance by 2031."
(Michele Mosca, 2017)

Initiatives



Migration to Quantum Safe Cryptography



- “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 Kryptographie 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. Kryptographie ist dabei essentiell um die Authentizität, Integrität und Vertraulichkeit von Information sicher zu stellen. Von vielen Augen unbemerkt ist Kryptographie 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.

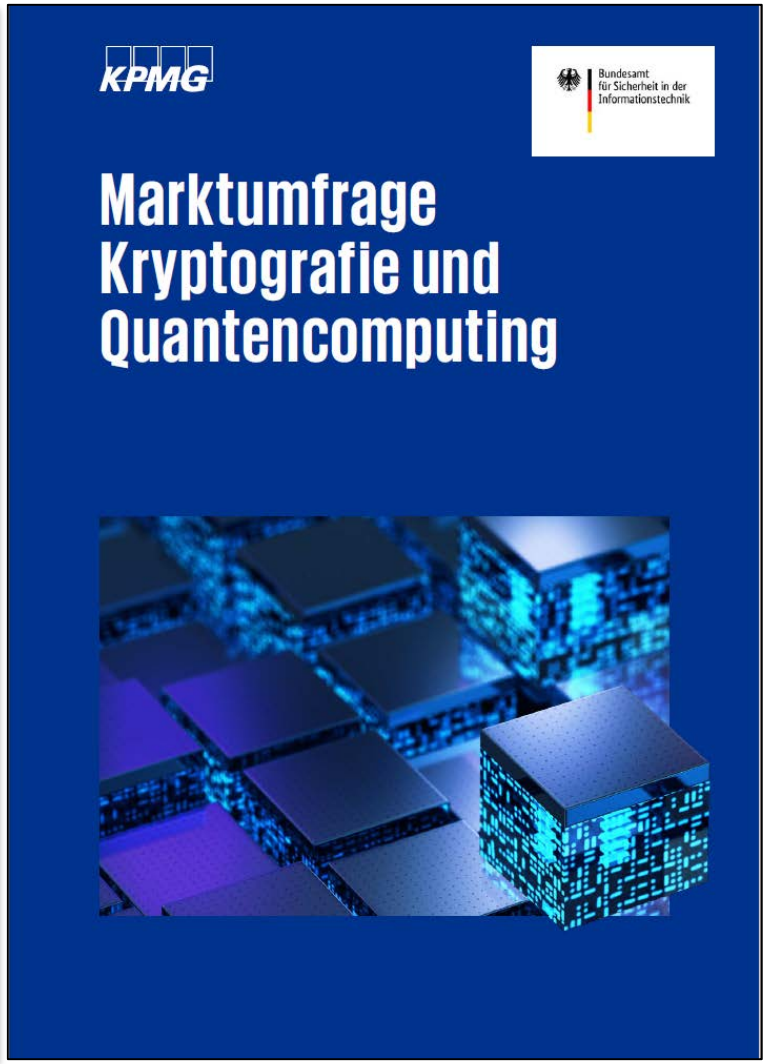
Von Biotechnologien bis zur Städteplanung hat Quantencomputing das Potential enorme Fortschritte zu bringen, aber es stehen auch Auswirkungen auf die Sicherheit von Informationen und Kommunikation bevor. Kryptographische Verfahren, die heute als sicher gelten und fest in unsere digitalen Infrastrukturen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



Federal Office for Information Security

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

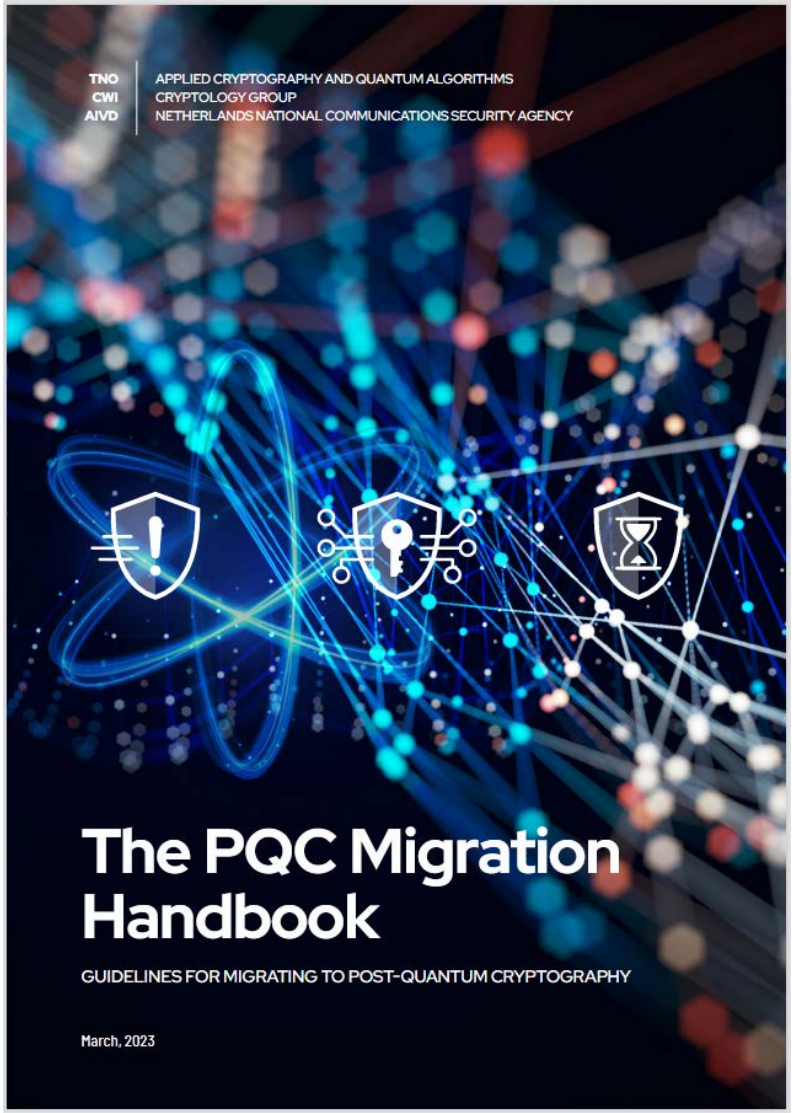
This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

I. OVERVIEW

Federal agencies[2] ("agencies") are moving to a zero trust architecture, as directed by Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)[3] and Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).[4] 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)[5] 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 aproach
- 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.

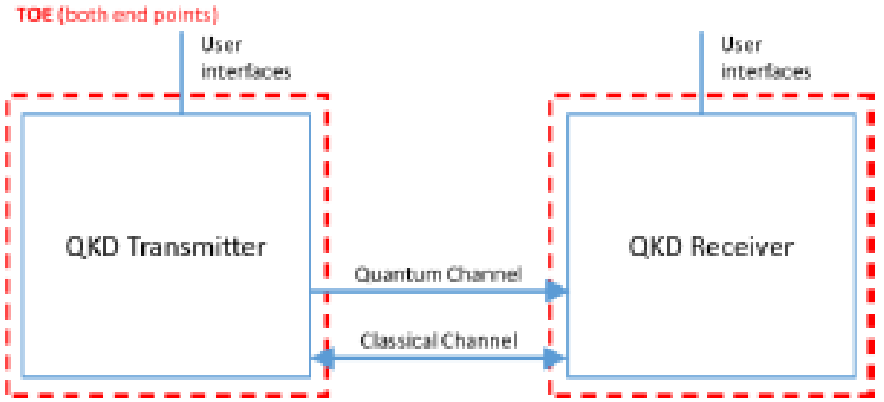


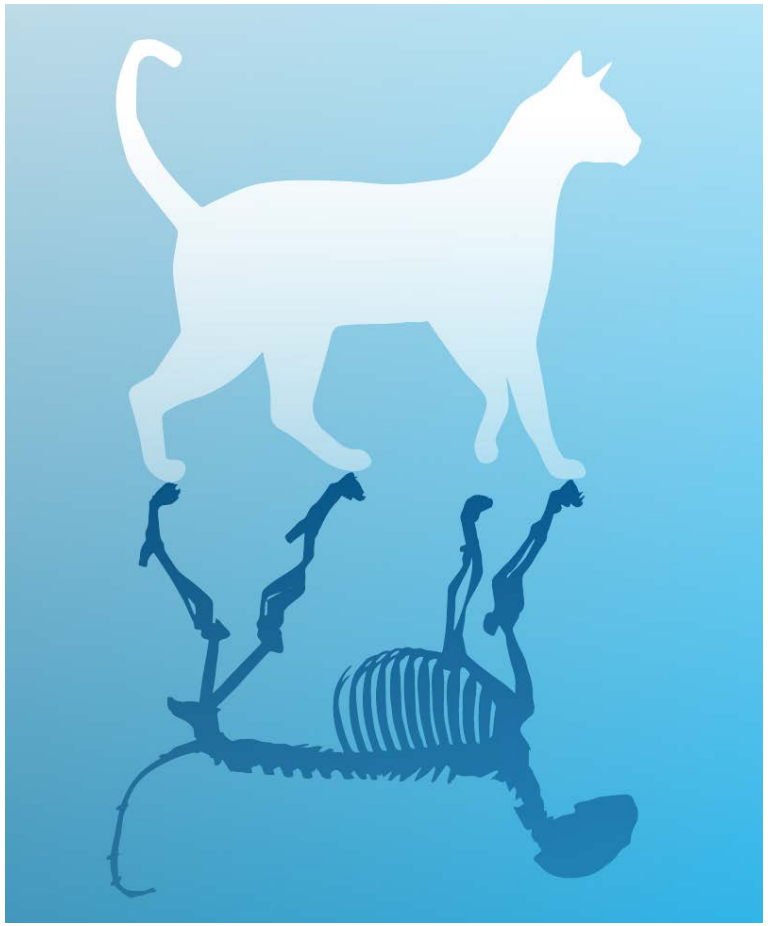
Figure 1: The TOE-boundary, i.e. the two QKD modules

Practical Security

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

Conclusion

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



Vielen Dank für Ihre Aufmerksamkeit!

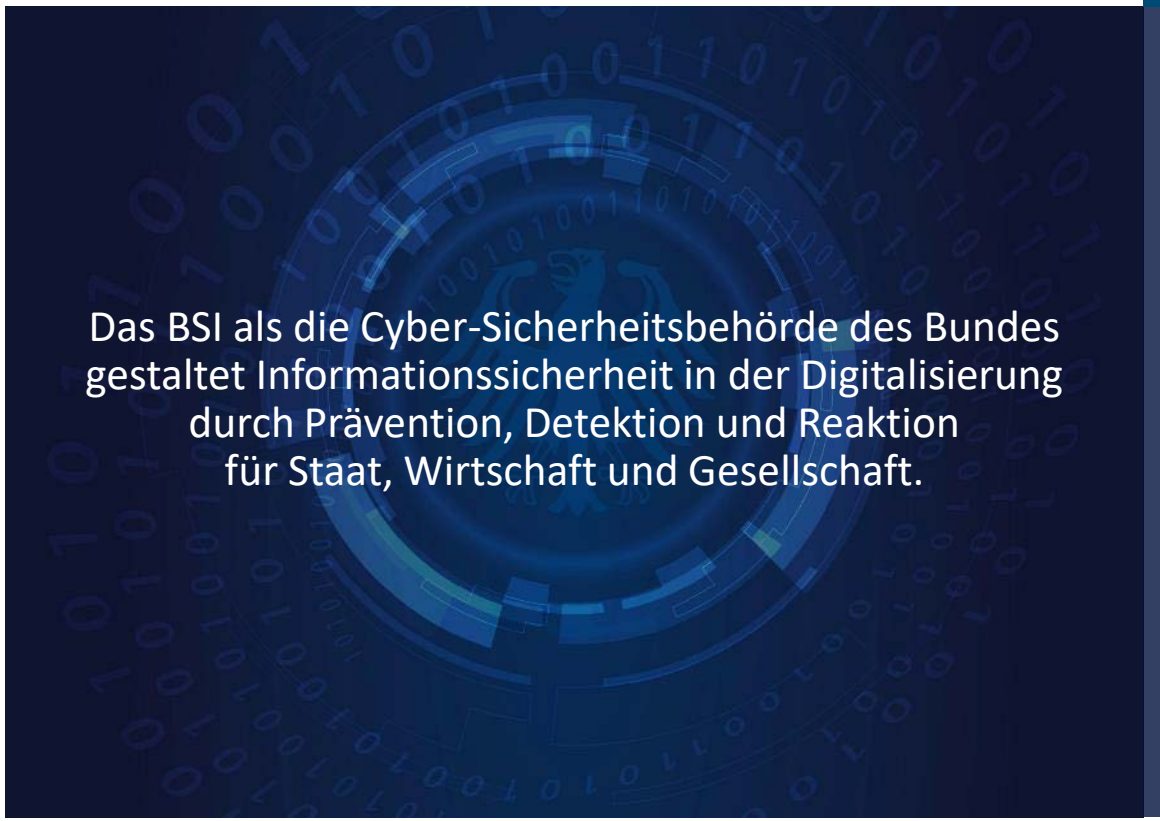
Deutschland
Digital•Sicher•BSI•

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



Bundesamt
für Sicherheit in der
Informationstechnik