Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

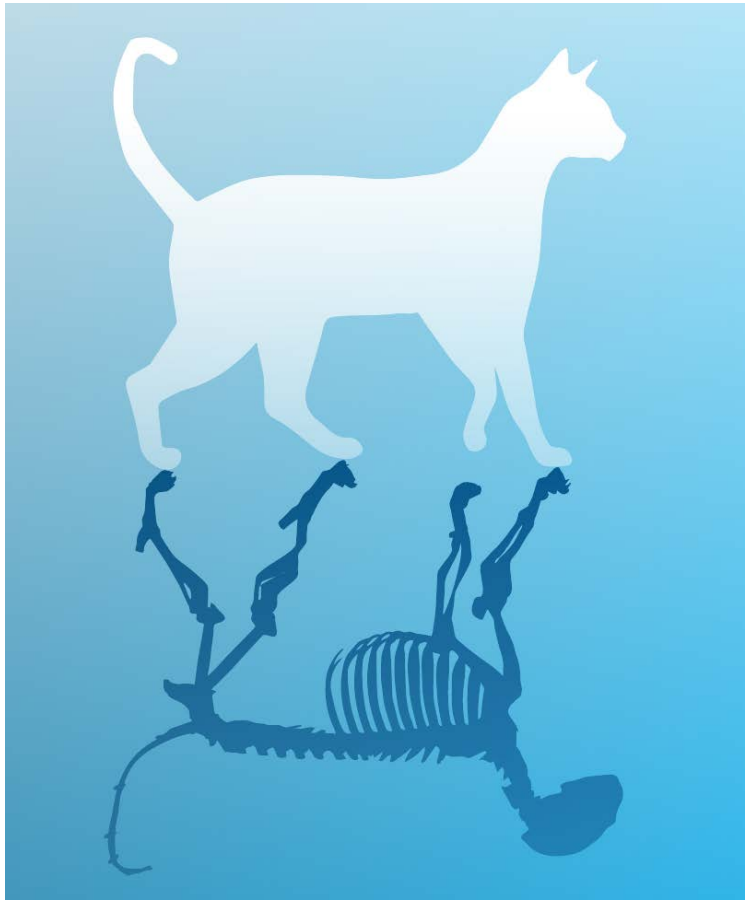
Quantum Safe Cryptography

Dr. Manfred Lochter
BSI

CA/B Forum, 25. October 2022

Topics

Background: The Quantum Threat
Two solutions: PQC & QKD
BSI's recommendations & open questions



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

Use of cryptography

Past
Mostly government

Today
TLS, MRTDs, HealthCard, Banking, electronic identities, …
Often with Smartcards as „Security-Anchor“

Tomorrow
Ubiquitous, cheap products, longlived (IoT, Industrie 4.0, C2C, Blockchain, 6G, ...)

The quantum threat

CNSS Advisory 2015

NIST-Standardisation

Impact of Quantum Computers on today‘s Cryptography

- **Symmetric cryptographic algorithms**: Sender and reveiver use the same key (e.g. AES)
- **Asymmetric** (or „Public-Key“) algorithms (e.g. RSA, ECC): Communication partners use different keys, one is public, one is private
- Security relies on **complexity assumptions**

- Quantum Computers would break traditional asymmetric cryptography (Shor‘s algorithm)
- Quantum Computers would roughly halve symmetric key lengths (Grover‘s algorithm)

- Typical applications (e.g. TLS) combine an asymmetric key agreement and symmetric encryption
- **Store-now-Decrypt-later** scenario: An adversary stores your full communication and is able to decrypt when Quantum Computers are available
- Role of digital signatures

- Change is necessary – independent from the quantum threat
- Two solutions PQC and QKD – with different assumptions

BSI‘s focus is on the migration to PQ cryptography

Mosca‘s Theorem

How much time is left for migration?

To estimate when the migration to quantum-safe cryptography is necessary, the following consideration by theoretical physicist M. Mosca from [Mos15] is very illustrative.

Let

- *x* be the number of years that the data to be protected must remain secured,
- *y* be the number of years needed to convert the corresponding system to quantum computer-resistant cryptography, and
- *z* be the number of years it will take for quantum computers to exist that threaten the cryptography currently in use.

Then, if x+y > z, you have a problem!

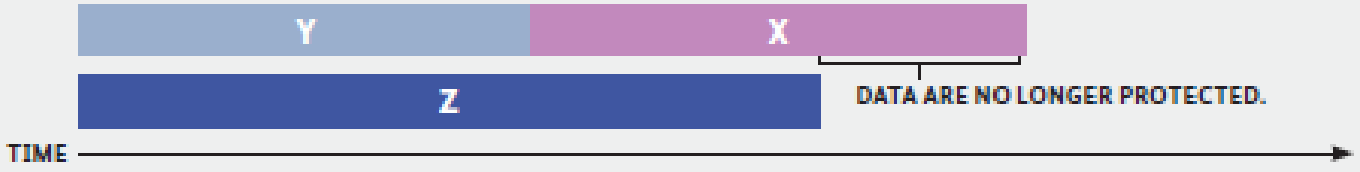
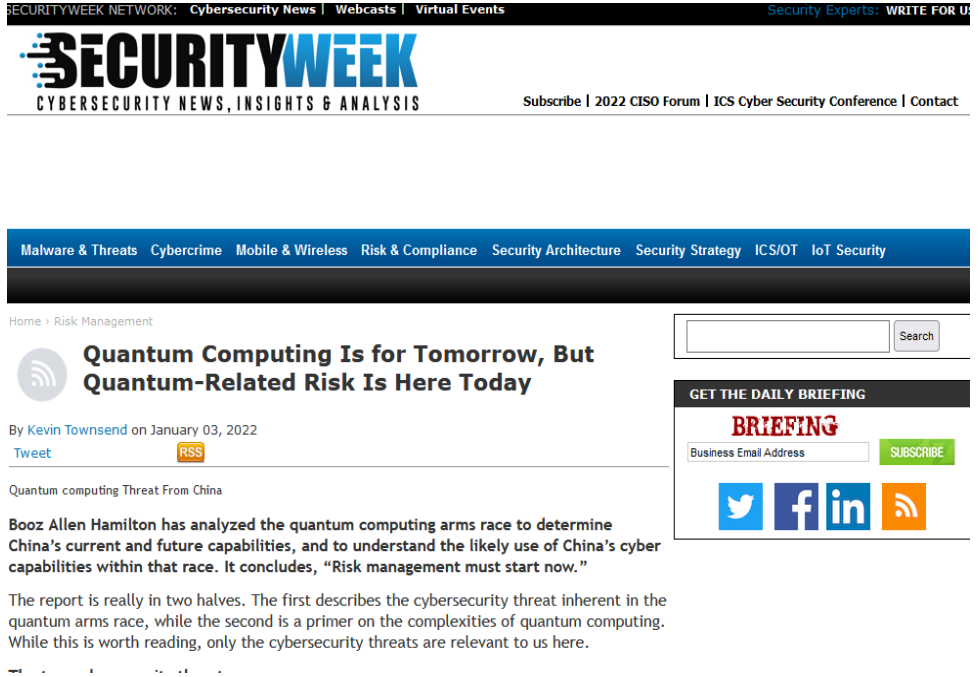


Figure: Illustration of "Mosca's Theorem"

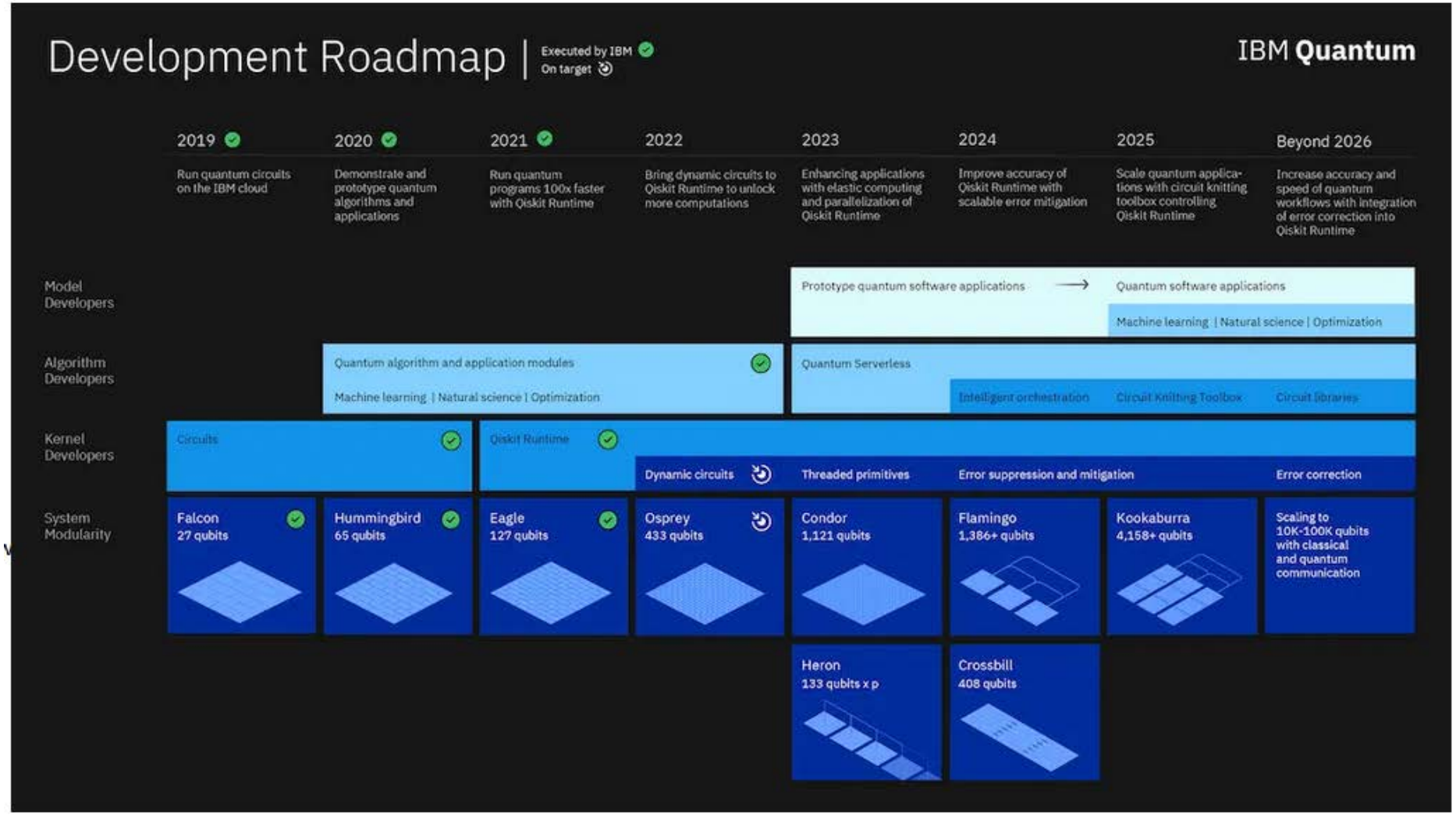
When can we expect cryptographically relevant Quantum Computers?

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)



https://research.ibm.com/blog/ibm-quantum-roadmap-2025

What does cryptographically relevant mean?

Most people only talk about Shor/Grover and full breaks
What about HHL?
Algorithms that need less qubits?
Algorithms that work only for a fraction of instances?
Quantum Coprocessors?
Application to Sidechannel analysis
Cofactoring in the NFS
Special purpose QC?

Lots of open research questions

Cryptosystems	N_k	N_r	#Vars	#Eqs	T	Complexity
AES-128	4	10	4288	10616	252288	$2^{69.26}c\kappa^2$
AES-192	6	12	7488	18096	421248	$2^{71.83}c\kappa^2$
AES-256	8	14	11904	29520	696384	$2^{74.38}c\kappa^2$
Trivium		1152	3543	4407	24339	$2^{55.50}c\kappa^2$
Trivium		2304	6999	9015	49683	$2^{59.06}c\kappa^2$
	N_h	N_r	#Vars	#Eqs	T	Complexity
Keccak	384	24	76800	77160	611023	$2^{73.12}c\kappa^2$
Keccak	512	24	76800	77288	611540	$2^{73.12}c\kappa^2$

Table 1: Complexities of the quantum algebraic attack

Structured lattices vs. unstructured lattices

eprint 2018/008, Chen, Gao: Quantum algorithms for boolean equation solving and quantum algebraic attacks on cryptosystems (see also arxiv 1712.06239
and 1802.03856)

Which ressources do we need?

arXiv > quant-ph > arXiv:2103.06159

Search... Help | Advanc

Quantum Physics

[Submitted on 10 Mar 2021 (v1), last revised 28 Sep 2021 (this version, v2)]

Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory

Élie Gouzien, Nicolas Sangouard

We analyze the performance of a quantum computer architecture combining a small processor and a storage unit. By focusing on integer factorization, we show a reduction by several orders of magnitude of the number of processing qubits compared with a standard architecture using a planar grid of qubits with nearest-neighbor connectivity. This is achieved by taking advantage of a temporally and spatially multiplexed memory to store the qubit states between processing steps. Concretely, for a characteristic physical gate error rate of 10^{-3}, a processor cycle time of 1 microsecond, factoring a 2048-bit RSA integer is shown to be possible in 177 days with 3D gauge color codes assuming a threshold of 0.75 % with a processor made with 13436 physical qubits and a memory that can store 28 million spatial modes and 45 temporal modes with 2 hours' storage time. By inserting additional error-correction steps, storage times of 1 second are shown to be sufficient at the cost of increasing the run-time by about 23 %. Shorter run-times (and storage times) are achievable by increasing the number of qubits in the processing unit. We suggest realizing such an architecture using a microwave interface between a processor made with superconducting qubits and a multiplexed memory using the principle of photon echo in solids doped with rare-earth ions.

Improving Shor

23 May 2019

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

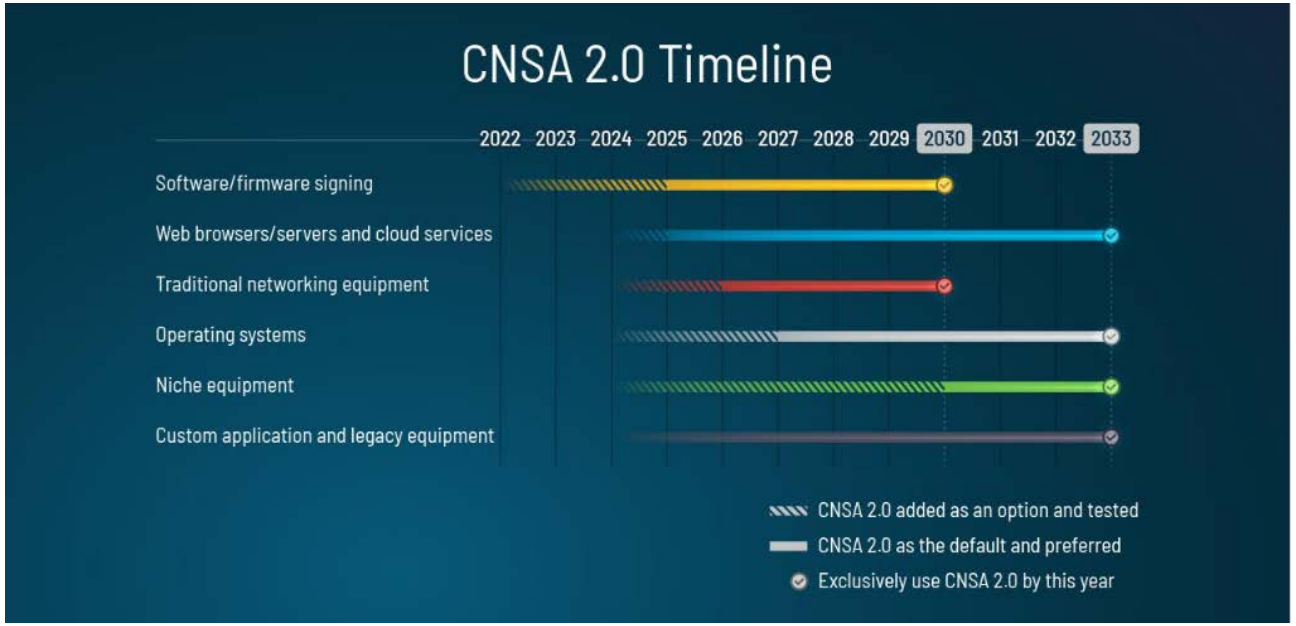
Craig Gidney[1,*] and Martin Ekerå[2]

[1] *Google Inc., Santa Barbara, California 93117, USA*
[2] *KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden*
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

(Dated: May 24, 2019)

We significantly reduce the cost of factoring integers and computing discrete logarithms over finite fields on a quantum computer by combining techniques from Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n-bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

Qubits
Physical Qubits
Gates
Memory



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

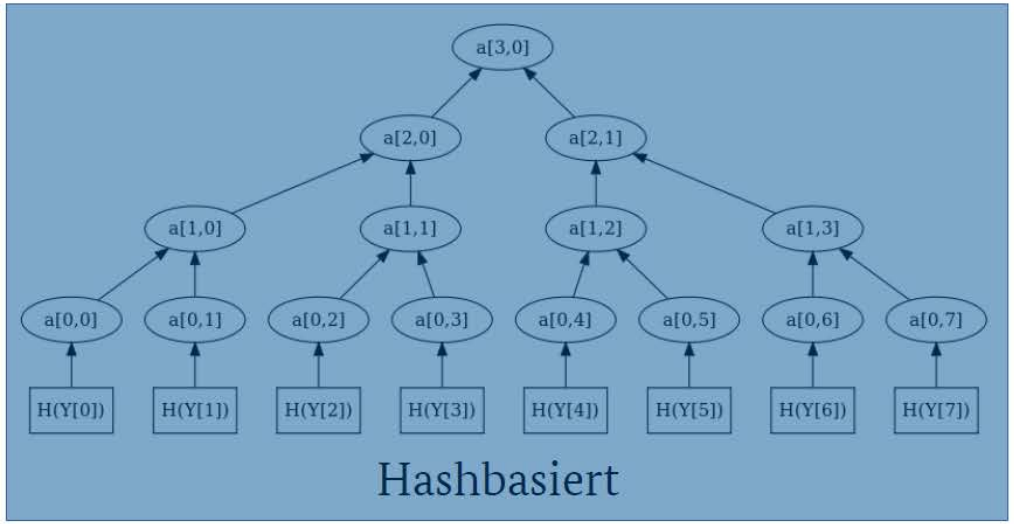
THE SECRETARY OF DEFENSE

THE ATTORNEY GENERAL

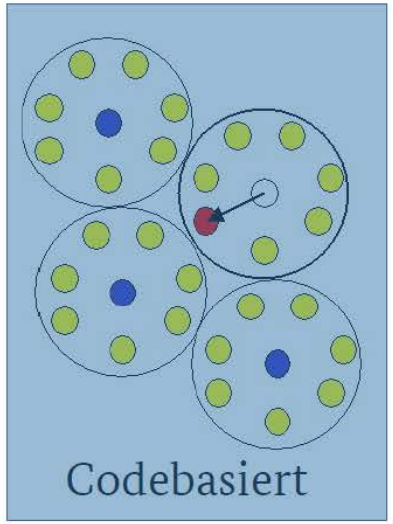
- “To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of **mitigating as much of the quantum risk as is feasible by 2035**."
- "Within 90 days of the date of this memorandum, the Secretary 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.“

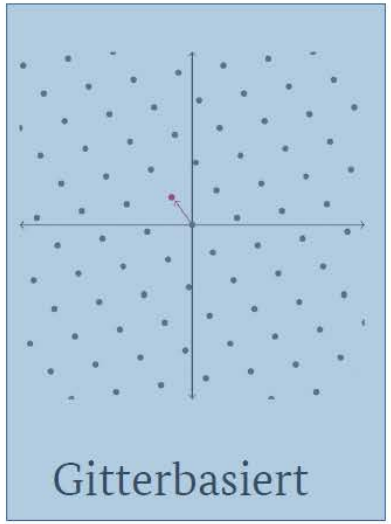
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerabl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

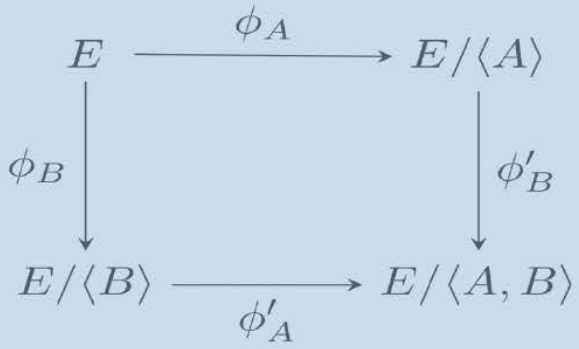
Post-Quantum-Cryptography



Hashbasiert


Codebasiert


Gitterbasiert



Isogeniebasiert

$$f_1(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{i\le n} b_i^{(1)} x_i + c^{(1)} = d_1$$
$$f_2(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(2)} x_i x_j + \sum_{i\le n} b_i^{(2)} x_i + c^{(2)} = d_2$$
$$\vdots$$
$$f_m(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{i\le n} b_i^{(m)} x_i + c^{(m)} = d_m$$

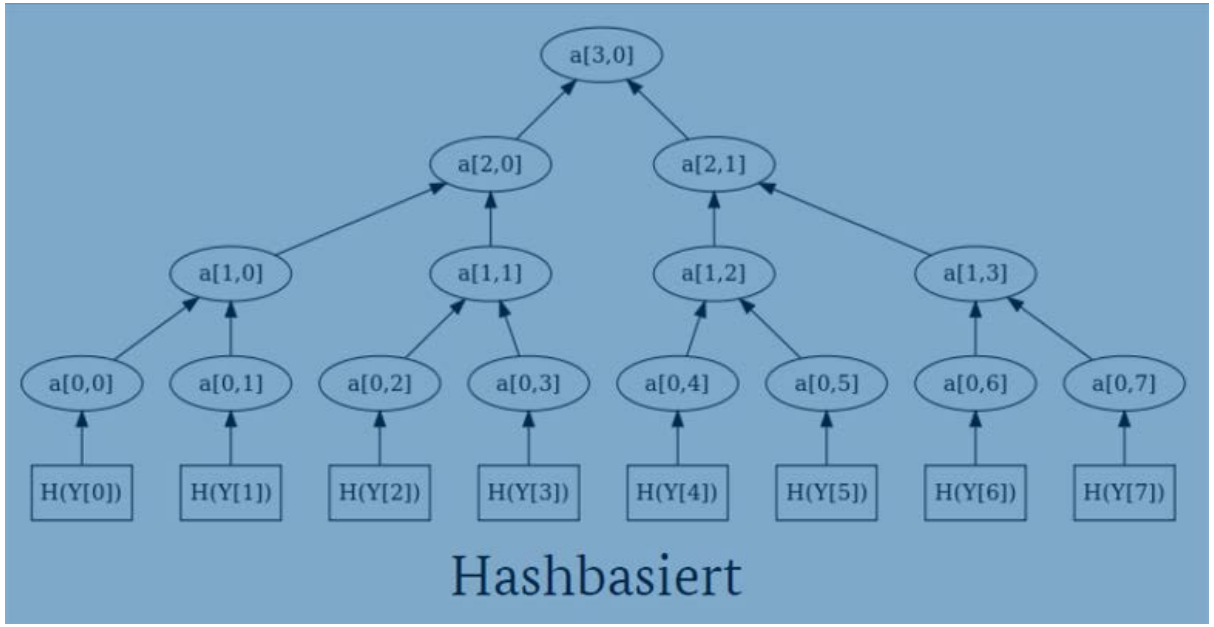
Multivariat

Hashbased Signatures

- Fundamental building block for agile solutions
- XMSS [RFC 8391], LMS [RFC 8553]
- NIST SP 800-208
- BSI TR02102-1

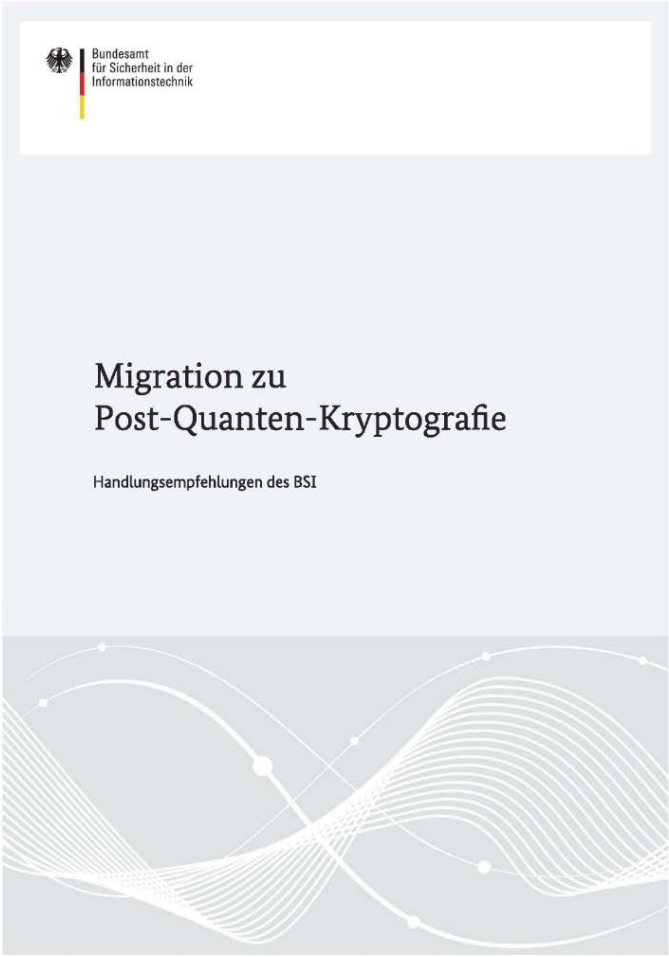
Agility does not necessarily guarantee long term security

Agility can get lost



Migration to Post Quantum Cryptography

- BSI has published (conservative) algorithm recommendations (TR-02101) and recommendations for the migration to PQ-algorithms.
- FRODO-KEM, Classic McEliece
- Focus: **agility** and **hybrid** key-agreement.
- Hash based signatures.
- Why were recommendations made before the NIST has finished?
- Strong cooperation with security industry and science.



Migration to Quantum Safe Cryptography

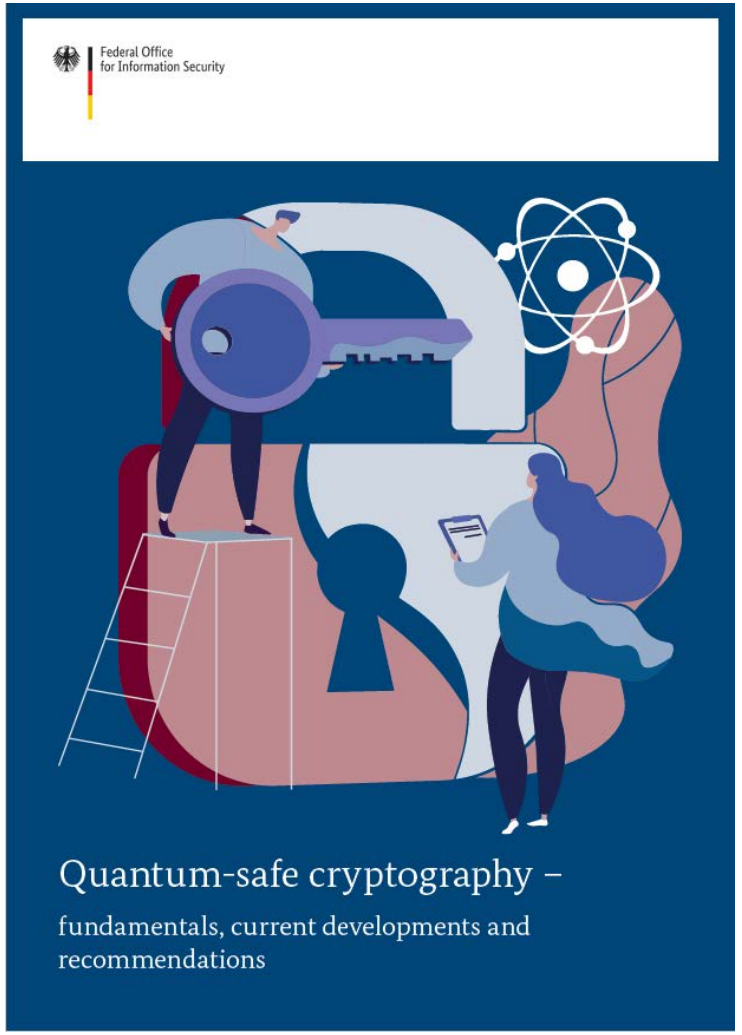
Two solutions based on different principles:
- PQ and QKD
- BSI‘s focus is on PQ

Goal: Cryptographic Agility
Building blocks:
- Hybrid key agreement and hybrid signatures
- Hashbased (stateful) signatures

Goal: International harmonisation

- Awareness activities

BSI‘s positions are similar to ANSSI‘s and NLNCSA‘s
(https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/, https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers)



www.bsi.bund.de/Quanten

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 of primal attacks. In the improved attack, we enumerate over more coordinates of the secret and use an improved distinguisher based on FFT. In addition, we incorporate improvements to the estimates of the cost of performing a lattice sieve in the RAM model, reducing the gate-count of random product code decoding and performing less inner product calculations.

Combining these improvements considerably reduces the security levels of Kyber, Saber and Dilithium, the LWE/LWR based finalists, bringing them below the thresholds defined by NIST.

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**

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

The NIST process

Start 2016
Several rounds

July 5, 2022
1 KEM selected
3 Signatures selected
New call for signatures soon

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8413

NIST expects to execute the various agreements prior to publishing the standard. If the agreements are not executed by the end of 2022, NIST may consider selecting NTRU instead of KYBER. NTRU was proposed in 1996, and U.S. patents were dedicated to the public in 2007

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)

SIKE

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)

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 required
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

- Joint Project BSI/KPMG
- Publication soon
- Most companies 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 Stadtplanung 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

Hybrid Solutions and QRNGS

This is a generic picture
Protocol specific solutions possible
Hybrid should remain after transition to PQ

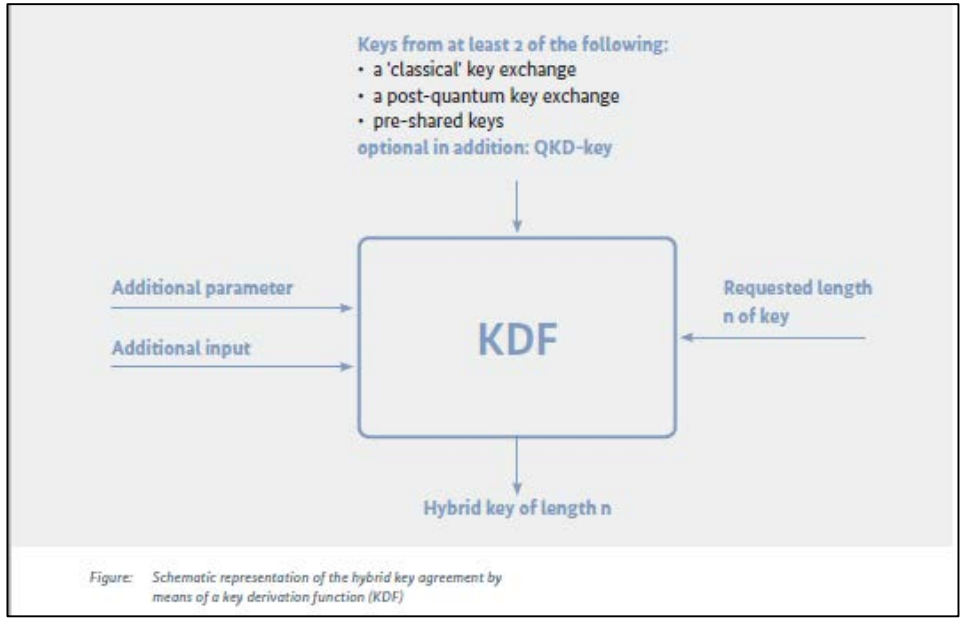
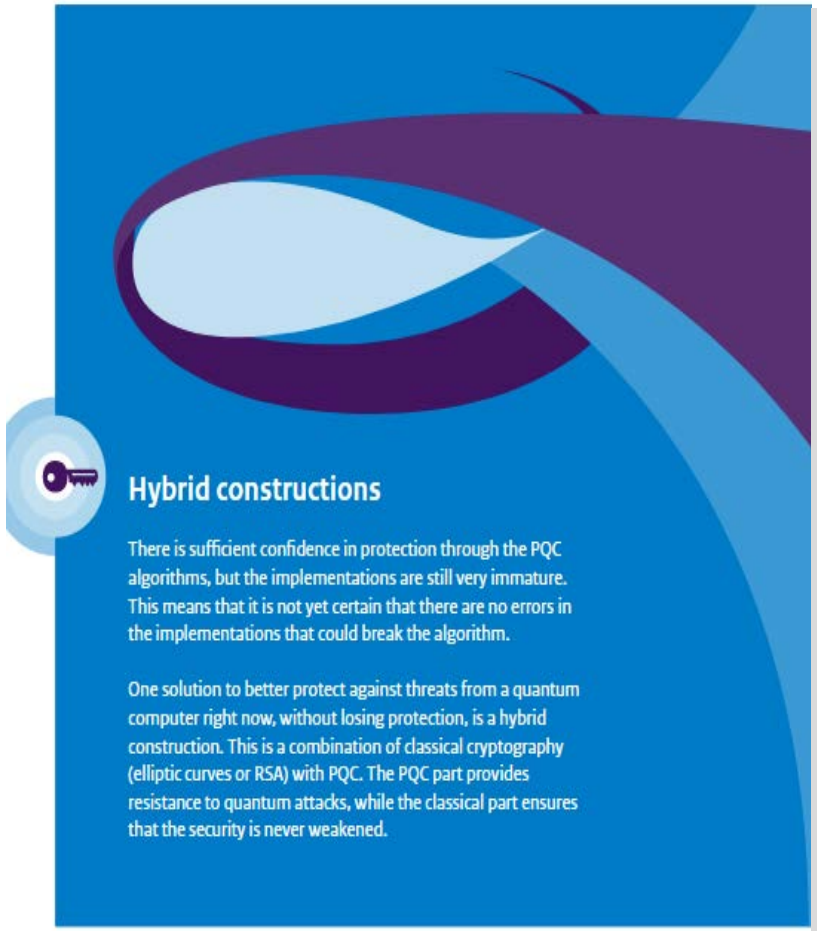


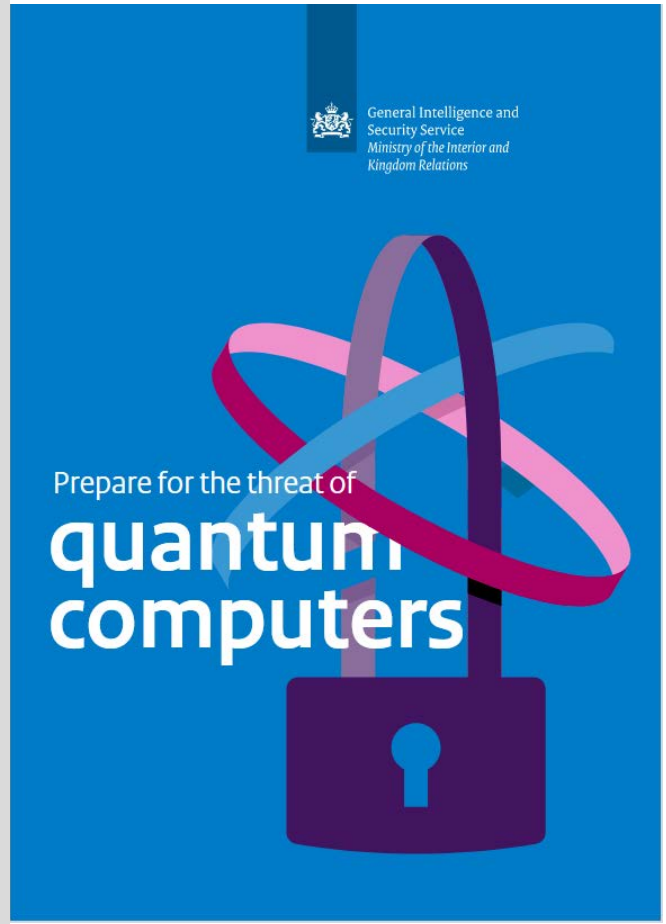
Figure: *Schematic representation of the hybrid key agreement by means of a key derivation function (KDF)*

QRNGs fit into the approach taken by AIS31
However: No QRNG with security proof known

Acknowledging the immaturity of PQC is important: **ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term.** However, this immaturity should not serve as an argument for postponing the first deployments. ANSSI encourages all industries to progress towards an initiation of a gradual overlap transition in order to progressively increase trust on the post-quantum algorithms and their implementations while ensuring no security regression as far as classical (pre-quantum) security is concerned.

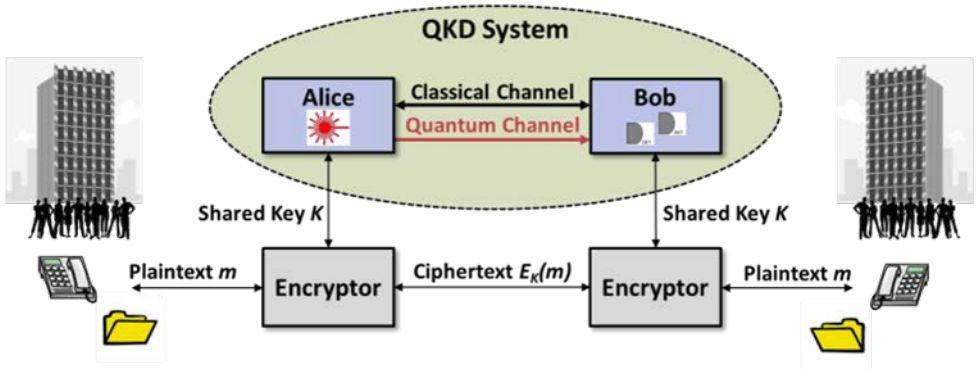


If this not possible, or is your information so sensitive that an extra layer of symmetric cryptography does not provide sufficient security, then switch to PQC in a hybrid construction (see page 7). You can use many different algorithms that vary in performance, efficiency and security.
For PQC, we recommend the most secure algorithms, such as Frodo or McEliece.
This is in line with what BSI, the German equivalent of the NLNCSA, recommends, among others. These algorithms provide the most protection against new attacks in the future, but are not the most efficient.



Alternative solution: Quantum Communication

Derive cryptographic keys by using quantum mechanical effects: **QKD**



Warning: This picture is oversimplified

PQ cryptography and Quantum Communication can complement each other in hybrid solutions

BSI's current focus is on the migration to PQ cryptography

What do other security agencies say?

National Cyber Security Centre

NCSC – Whitepaper: Quantum Security Technologies (2020)

*"Given the **specialised hardware requirements** of QKD over classical cryptographic key agreement mechanisms and the **requirement for authentication** in all use cases, the NCSC does not endorse the use of QKD for any government or military applications […]."*

Federal Office for Information Security

ANSSI - Technical Position Paper: QKD (2020)

*"Security guarantees provided in principle by QKD come with **significant deployment constraints** which reduce the scope of the services offered and compromise in practice QKD security assurances, particularly in scenarios where communications travel through a network of interconnected QKD links."*

NSA – Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

*"NSA **does not recommend** the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations […] are overcome."*

Key Projects (EU&Germany)

The participating member states Plan to work together to establish a cooperation framework – EuroQCI – for exploring within the next 12 months, the possibility of developing and deploying in the Union, within the next 10 years, a ***certified*** *secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored* ***ultra-securely*** *and capable of linking critical public communication assets all over the Union.*

(QCI Declaration)

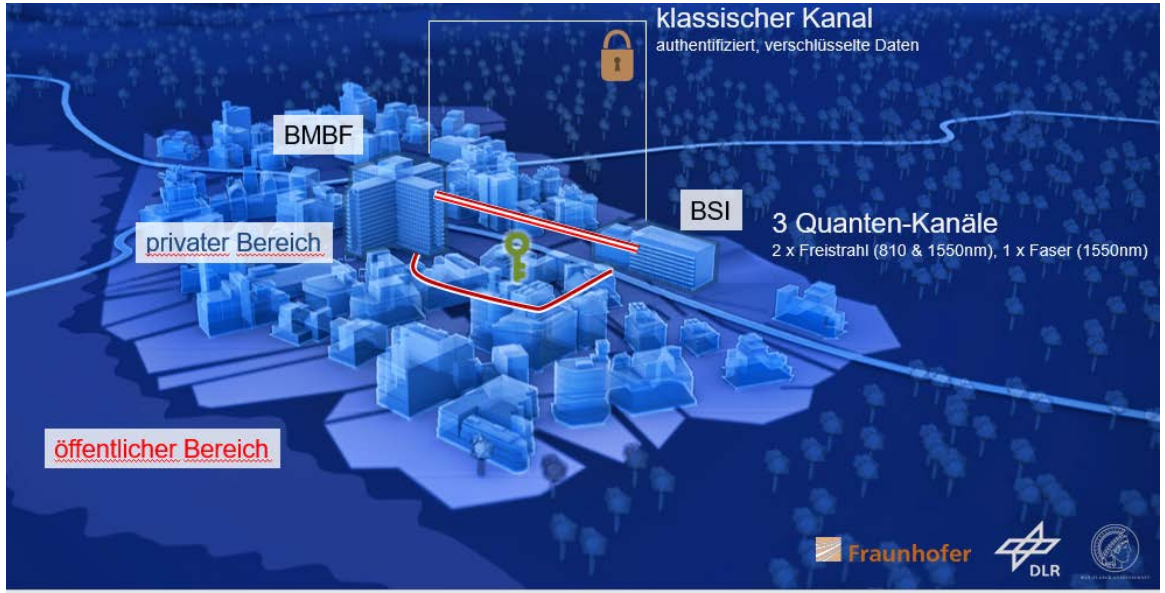
QuNET *(BMBF, scientific societies, industry, BSI)*
Basis for a German Quantum Communication Network (165 Million €). Demonstration August 2021. Video conference between BMBF and BSI, secured by QKD and PQC.

Federal Office for Information Security

QuNET

— The quantum communication networks would link institutional users to their critical infrastructures

QuNET-Demonstration



MAX PLANCK INSTITUTE
FOR THE SCIENCE OF LIGHT

NEWS & EVENTS DIVISIONS RESEARCH AT M

HOME | NEWS & EVENTS | NEWS FROM THE INSTITUTE | **NEWS-DETAIL**

First quantum-secured video conference between two federal agencies

10.08.2021

Initiative QuNET demonstrates highly secure and practical quantum communication

Photo: BMBF

Photo: Fraunhofer IOF

Today, two German federal authorities communicated via video for the first time in a quantum-secure manner. The QuNET project, an initiative funded by the German Federal Ministry of Education and Research (BMBF) to develop highly secure communication systems, is thus demonstrating how data sovereignty can be guaranteed in the future. This technology will not only be important for governments and public authorities but also to protect everyday data.

It was a foretaste of the communication of the future - or rather, the "data security" of the future. Because when Federal Research Minister Anja Karliczek invited members of the Federal Office for Information Security (BSI) to a video conference today, everything looked the same, at least for outsiders. Together with Andreas Könen, Head of Department CI "Cyber and IT Security" at the Federal Ministry of the Interior, Building and Community (BMI) and BSI Vice President Dr. Gerhard Schabhüser, the minister talked via video stream.

Where are we now?

Physicists always have a habit of taking the simplest example of any phenomenon and calling it "physics," leaving the more complicated examples to become the ***concern of other fields****—say of applied mathematics, electrical engineering, chemistry, or crystallography. Even solid-state physics is almost only half physics because it worries too much about special substances.*

(Feynman Lectures on Physics)

QKD: Concerns of other fields

Implementation security, network aspects, remote access, key management, key use, protocols, randomization, standardization, qualification, quantitative security proofs, hybridization, …

CC-Evaluation criteria – 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
- Draft available on ETSI webpage
- Next Step: Certification of the PP
- 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.

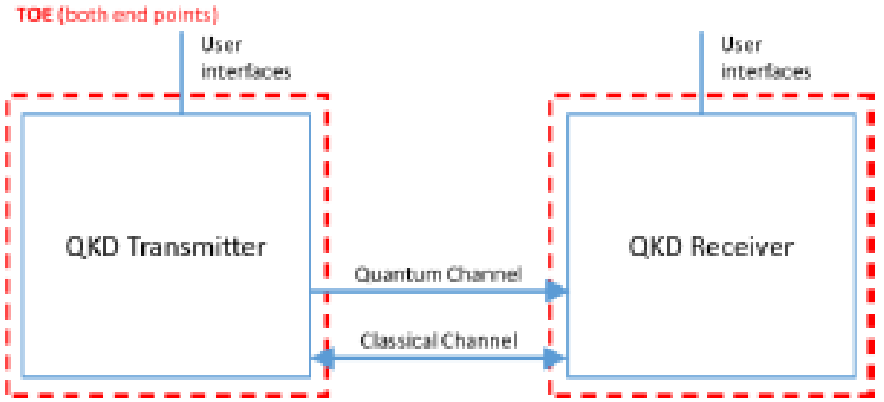
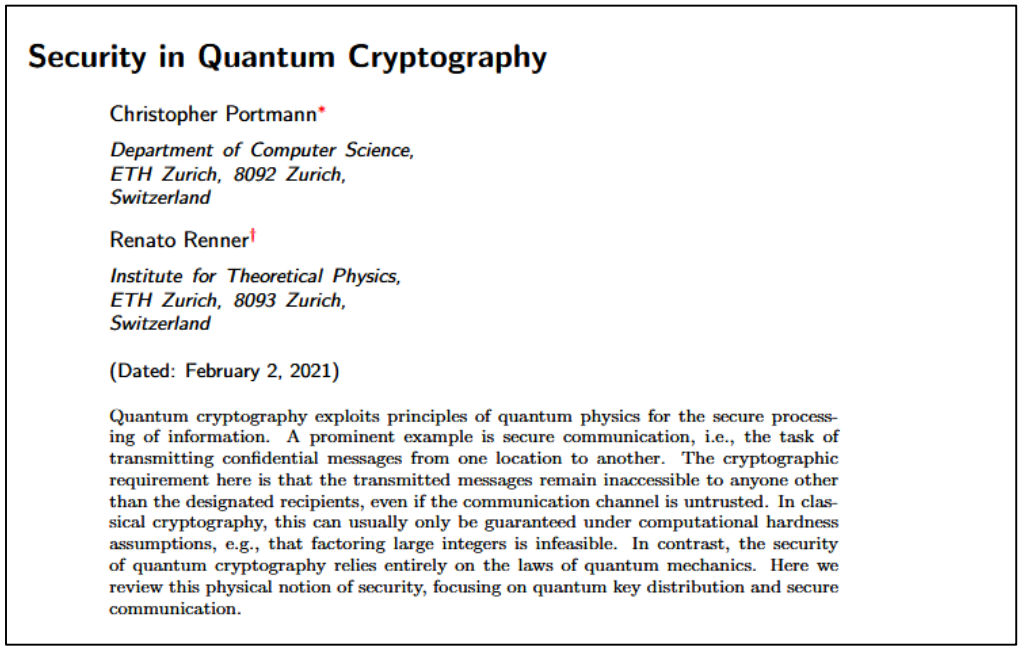


Figure 1: The TOE-boundary, i.e. the two QKD modules

Theoretical Security

- Trace distance criterion (Renner-Portmann-Model)
- Classical Authentication between modules needed, but key-depletion
- ITS vs. Computational security
- Wegman-Carter-Authentication: Parts of QKD-Key needed for Key-Updates (DoS); security guarantee decreases with each key-agreement; external input needed
- Quantitative security statements for **standardized** protocols



Security in Quantum Cryptography

Christopher Portmann*

Department of Computer Science,
ETH Zurich, 8092 Zurich,
Switzerland

Renato Renner†

Institute for Theoretical Physics,
ETH Zurich, 8093 Zurich,
Switzerland

(Dated: February 2, 2021)

Quantum cryptography exploits principles of quantum physics for the secure processing of information. A prominent example is secure communication, i.e., the task of transmitting confidential messages from one location to another. The cryptographic requirement here is that the transmitted messages remain inaccessible to anyone other than the designated recipients, even if the communication channel is untrusted. In classical cryptography, this can usually only be guaranteed under computational hardness assumptions, e.g., that factoring large integers is infeasible. In contrast, the security of quantum cryptography relies entirely on the laws of quantum mechanics. Here we review this physical notion of security, focusing on quantum key distribution and secure communication.

There are various choices that can lead to different security levels for a QKD system

Central Part: FCS_QKD

Security in Quantum Cryptography

Christopher Portmann*

Department of Computer Science,
ETH Zurich, 8092 Zurich,
Switzerland

Renato Renner†

Institute for Theoretical Physics,
ETH Zurich, 8093 Zurich,
Switzerland

(Dated: February 2, 2021)

Quantum cryptography exploits principles of quantum physics for the secure processing of information. A prominent example is secure communication, i.e., the task of transmitting confidential messages from one location to another. The cryptographic requirement here is that the transmitted messages remain inaccessible to anyone other than the designated recipients, even if the communication channel is untrusted. In classical cryptography, this can usually only be guaranteed under computational hardness assumptions, e.g., that factoring large integers is infeasible. In contrast, the security of quantum cryptography relies entirely on the laws of quantum mechanics. Here we review this physical notion of security, focusing on quantum key distribution and secure communication.

Scientific review needed!

5 Extended component definition

5.1 Quantum Key Distribution (FCS_QKD)

This section describes the security functional requirements for the generation of QKD keys, which may be used as secrets for cryptographic purposes. The IT security functional requirements for a TOE are defined in an additional family Quantum Key Distribution (FCS_QKD) of the Class FCS (Cryptographic support).

Family Behaviour

Quantum Key Distribution relates to two or more end points (modules) establishing a confidential, shared, random bit string. It uses a communication channel carrying quantum states, which by quantum physical principles cannot be eavesdropped on without introducing anomalies with high probability. The establishment is achieved using a protocol that limits the joint probability that the protocol does not abort and that

- any entity outside the modules has gained knowledge about the bit strings, or
- the shared bit strings are not identical in both modules, or
- the distribution of bit strings has statistical properties different from uniform distribution

to a well defined value. This value is called the security parameter of the quantum key distribution protocol.

Component levelling:

FCS_QKD: Quantum Key Distribution	1

FCS_QKD.1 Prepare and Measure Quantum Key Distribution requires quantum key distribution in between two modules to be established using a Prepare and Measure protocol including information reconciliation and privacy amplification. The actual protocols and the algorithms for their application shall be chosen in accordance with the underlying security proof to support the claimed value of the security parameter. The SFR depends on local random numbers to choose physical and cryptographic protocol parameters, and to randomly partition measurement data into private and public data. The SFR furthermore depends on an authenticated classical communication channel.

Management: FCS_QKD.1

There are no management activities foreseen.

Proofs

No convincing proofs available
BSI Project on Security Proofs: No contractor found

Proofs are necessary for certification and approval of QKD-devices

Importance of security proofs

Upper security bounds for coherent-one-way quantum key distribution

Javier González-Payo,[1] Róbert Trényi,[1] Weilong Wang,[1,2,3] and Marcos Curty[1,*]

[1]*Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, 450001, China*
[3]*Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan, 450001, China*

(Dated: July 1, 2020)

The performance of quantum key distribution (QKD) is severely limited by multi-photon pulses emitted by laser sources due to the photon-number splitting attack. Coherent-one-way (COW) QKD has been introduced as a promising solution to overcome this limitation, and thus extend the achievable distance of practical QKD. Indeed, thanks to its experimental simplicity, the COW protocol is already used in commercial applications. Here, we derive simple upper security bounds on its secret key rate, which suggest that it scales quadratically with the system's transmittance, thus solving a long-standing problem. That is, in contrast to what has been claimed, this approach does not seem to be appropriate for long-distance QKD transmission. Our findings imply that all long-distance implementations of the COW protocol performed so far are actually insecure.

Gonzalez-Payo et al., arXiv:2006.16891 (2020)

Limited security proof for COW known to community. Other QKD protocols (e.g. BB84 decoy) offer more advanced security proofs.

Maybe son

businesswire
A BERKSHIRE HATHAWAY COMPANY

HOME SERVICES NEWS EDUCATION ABOUT US

Search

INVESTOR ALERT: Arqit Quantum Inc. f/k/a Centricus Acquisition Corp. Investors with Substantial Losses Have Opportunity to Lead the Arqit Class Action Lawsuit - ARQQ; ARQQW

May 09, 2022 04:41 PM Eastern Daylight Time

SAN DIEGO--(BUSINESS WIRE)--**Robbins Geller Rudman & Dowd LLP** announces that purchasers of Arqit Quantum Inc. f/k/a Centricus Acquisition Corp. (NASDAQ: ARQQ; ARQQW) securities between September 7, 2021 and April 18, 2022, inclusive (the "Class Period") and/or all holders of Centricus securities as of the record date for the special meeting of shareholders held on August 31, 2021 to consider approval of the merger between Arqit and Centricus (the "Merger") and entitled to vote on the Merger have until July 5, 2022 to seek appointment as lead plaintiff in *Glick v. Arqit Quantum Inc. f/k/a Centricus Acquisition Corp.*, No. 22-cv-02604 (E.D.N.Y.). Commenced on May 6, 2022, the *Arqit* class action lawsuit charges Arqit and certain of its top executive officers with violations of the Securities Exchange Act of 1934.

If you suffered significant losses and wish to serve as lead plaintiff of the *Arqit* class action lawsuit, please provide your information by clicking here. You can also contact attorney J.C. Sanchez of Robbins Geller by calling 800/449-4900 or via e-mail at jsanchez@rgrdlaw.com. Lead plaintiff motions for the *Arqit* class action lawsuit must be filed with the court no later than July 5, 2022.

CASE ALLEGATIONS: Arqit is a cybersecurity company that has purportedly pioneered a unique quantum encryption technology. Arqit alleged its quantum encryption technology would be secure against current and future forms of cyberattacks, including from a quantum computer. Centricus was a special purpose acquisition corporation ("SPAC" or blank check company) formed for the purpose of effecting a merger, capital stock exchange, asset acquisition, stock purchase, reorganization, or similar business combination with one or more businesses. Prior to the Merger, Centricus shares traded on the NASDAQ under the ticker symbol CENHU.

What‘s missing? The Ecosystem!

- A Technical Domain: Impact of the CSA?
- CSA-Level „High“
- Industry Working Groups necessary
- Accompanying documentation (e.g. on Sidechannels)
- Security proofs
- Standards for Protocols/Interfaces
- Standards for the use of QKD keys
- Distribution of authentication keys
- OTP or AES? Or both?
- Hybrid solutions
- End-to-end security?

> “For assurance level ‘substantial’, the evaluation, in addition to the requirements for assurance level ‘basic’, should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.” (CSA)

> “…for assurance level ‘high’, the evaluation, in addition to the requirements for assurance level ‘substantial’, should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.” (CSA)

Practical Security – Projekt 575

https://www.evergabe-online.de/tenderdetails.html?0&id=465272&cookieCheck

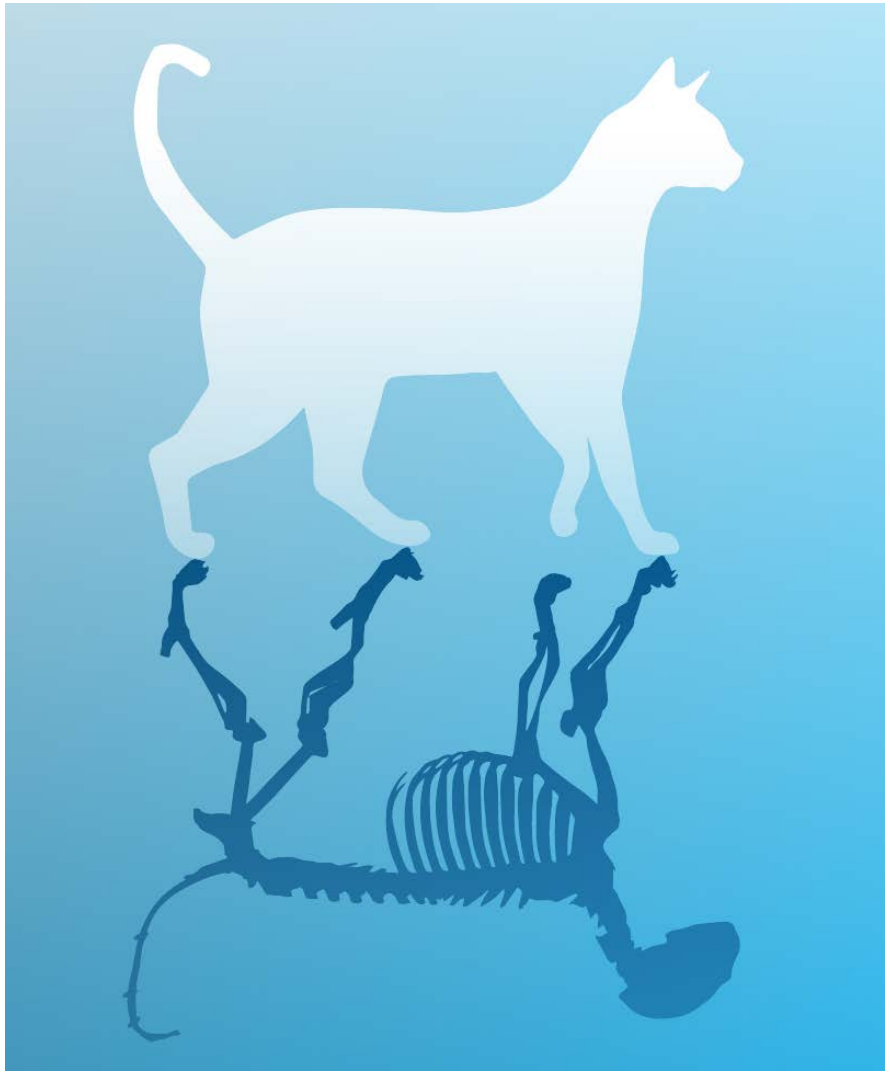
No offer for Security-Proof project
SCA project: Contract awarded recently
Certification of PP pending

Conclusion

Don‘t panic!

(Corporal Jones)

Change is coming!
Agility must be a design criterion.
QKD in hybrid solutions
Many open questions



Thank you for your attention!

Contact

Dr. Manfred Lochter
Requirements for and design of cryptographic mechanisms

Manfred.lochter@bsi.bund.de
Tel. +49 (0) 228 9582 5643
Fax +49 (0) 228 10 9582 5643

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de