Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

QKD aus Sicherheitsperspektive

Dr. Manfred Lochter, BSI
13. Juli, 2022

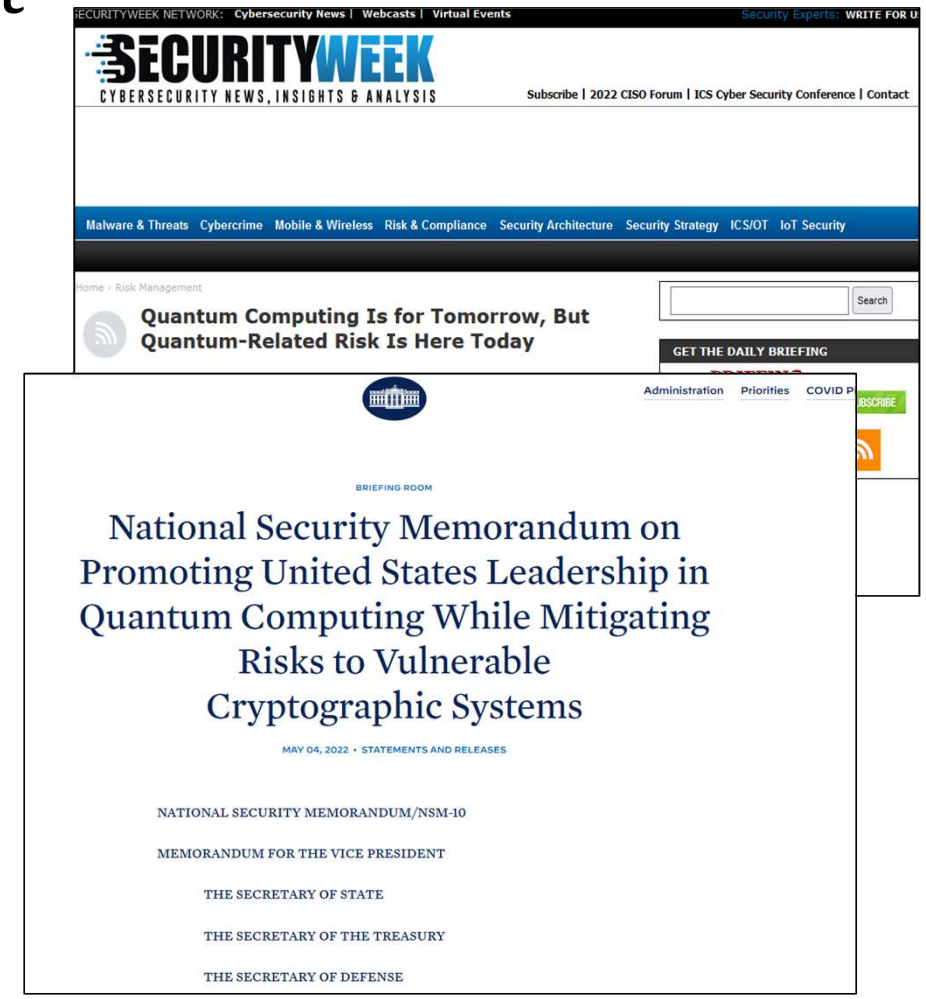
CODE Jahrestagung

Background: The Quantum Threat

BSI's Working assumption for high security applications:
A cryptographically relevant Quantum Computer will be available by the begin of the 2030ies.

.

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



What is a cryptographically relevant Quantum Computer?

arXiv > quant-ph > arXiv:2103.06159

Search... Help | Advanc

Quantum Physics

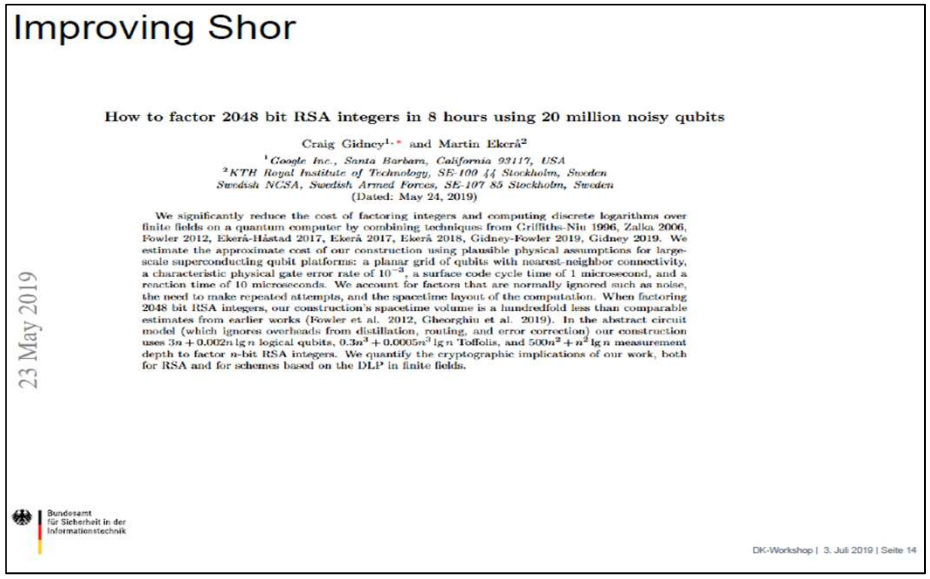
[Submitted on 10 Mar 2021 (v1), last revised 28 Sep 2021 (this version, v2)]

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.

Qubits
Physical Qubits
Gates
Memory



Improving Shor

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)

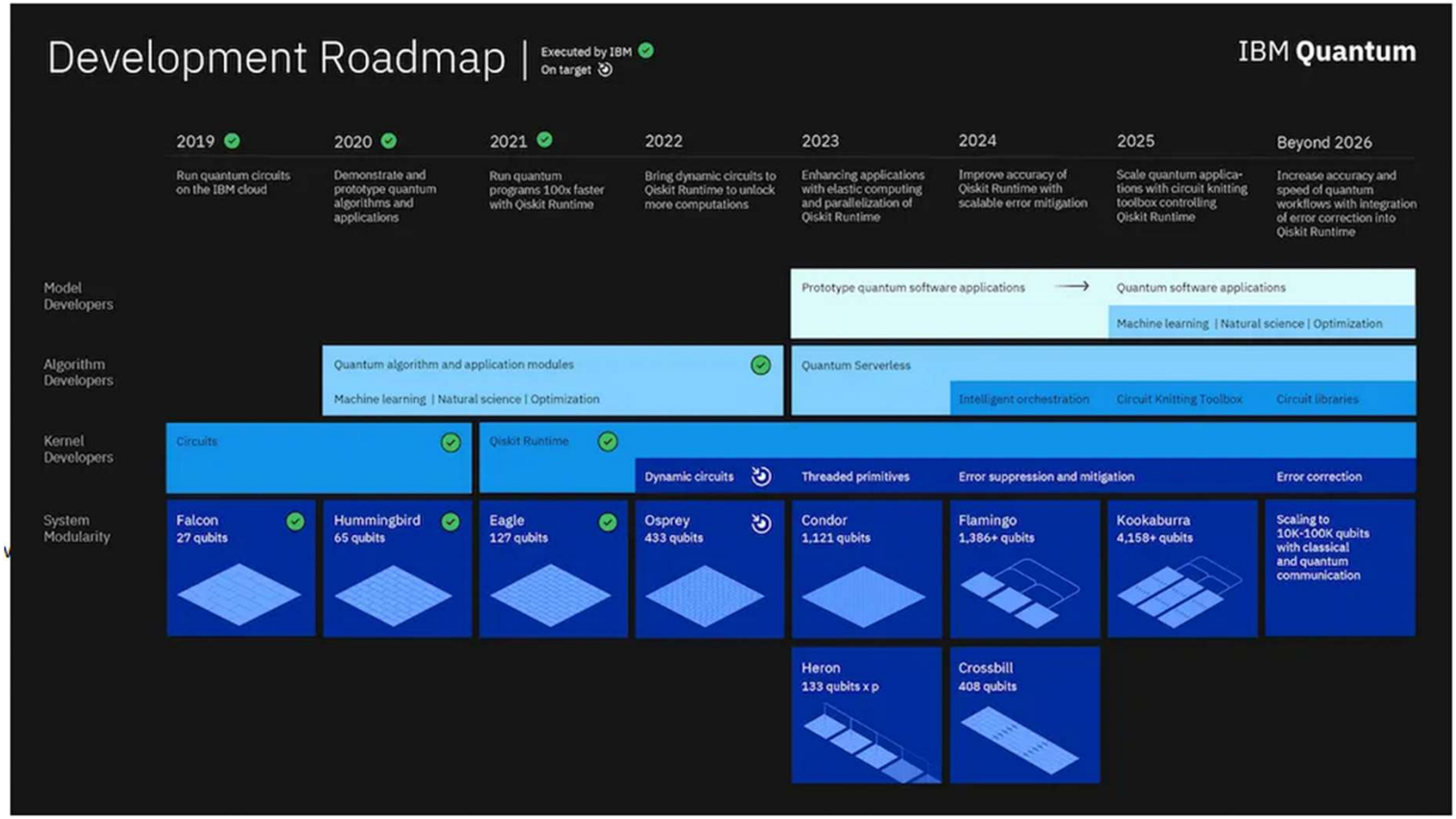
We significantly reduce the cost of factoring integers and computing discrete logarithms over finite fields on a quantum computer by combining techniques from Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate 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.

23 May 2019

Bundesamt für Sicherheit in der Informationstechnik

DK-Workshop | 3. Juli 2019 | Seite 14

Federal Office for Information Security



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

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

Migration to Quantum Safe Cryptography

Two solutions based on different principles:

- PQ and QKD
- **BSI‘s focus is on the migration to PQ**

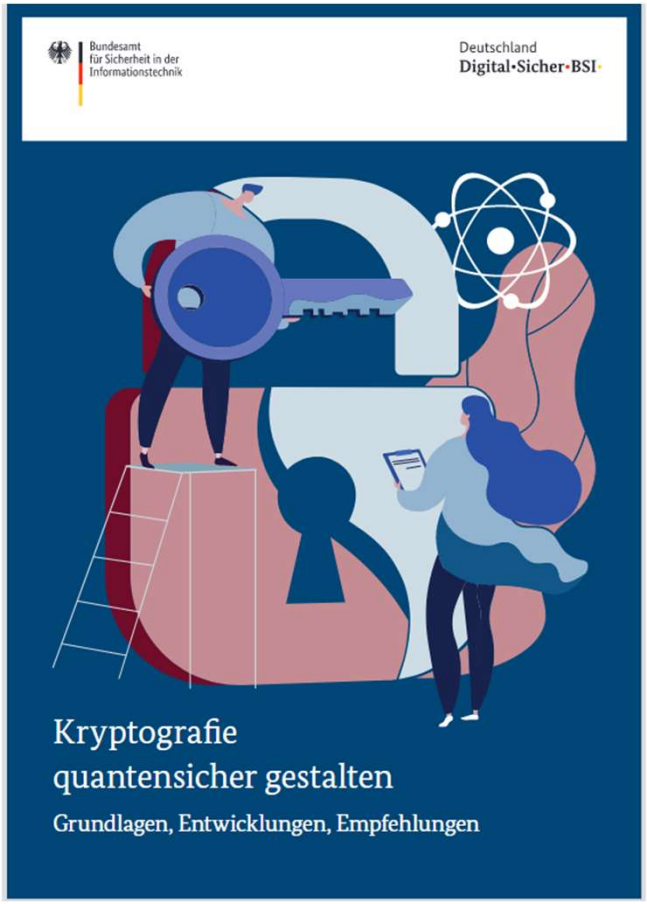
Goal: Cryptographic Agility
Building blocks:

- Hybrid key agreement and hybrid signatures
- Hashbased (stateful) signatures

Goal: International harmonisation

- Already published guidance for the migration to quantum-safe cryptography and chose algorithms.
- Awareness activities are in preparation.

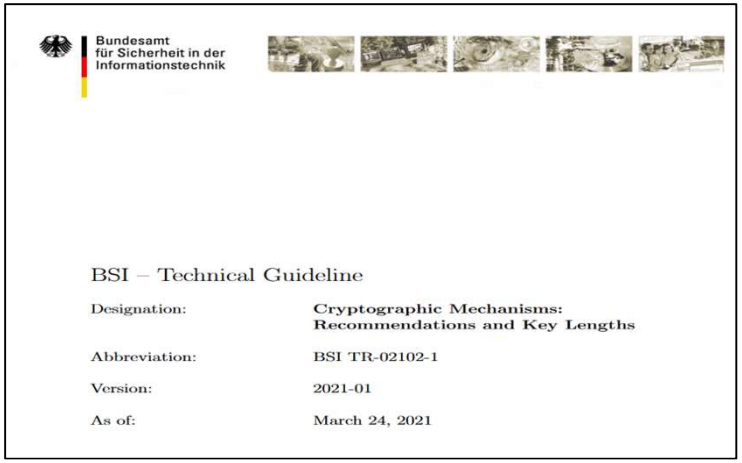
BSI‘s positions are similar to ANSSI‘s and NLNCSA‘s
(https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/, https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers)



www.bsi.bund.de/Quanten

Recommendations in Technical Guideline TR-02102-1

Recommended mechanisms: FrodoKEM-976 (Section 2.5 in [5]), FrodoKEM-1344 (Section 2.5 in [5]) and Classic McEliece with the parameters listed in Section 7 of [14] in the categories 3 and 5 are viewed as cryptographically suitable for long-term confidentiality protection at the security level aimed at by this Technical Guideline.
This is a fairly conservative assessment which leaves a significant security margin with regards to possible future cryptanalytic progress. It is possible that future revisions of this document will assess other parameter choices and PQC schemes as technically suitable as well.
FrodoKEM has not been included among the finalists for the third round of the NIST PQC project, but as an alternative candidate. This is primarily due to considerations about the efficiency of the scheme; there are no doubts about its security. The BSI therefore maintains its recommendation of FrodoKEM as a PQC scheme with a high security margin against future attacks. More details can be found in [12].


Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technical Guideline

Designation:	Cryptographic Mechanisms: Recommendations and Key Lengths
Abbreviation:	BSI TR-02102-1
Version:	2021-01
As of:	March 24, 2021

Overall assessment. In terms of security, Frodo's conservative design choices are laudable. At the same time, these choices mean that Frodo's performance is significantly worse than schemes based on structured lattices.

IT-Sicherheit durch Quantentechnologie gewährleisten

Woran lassen wir uns messen?
Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

Im Bereich des Quantencomputing stehen bis 2025 Rechner mit mindestens 100 Qubits auf der Basis souveräner Technologie aus Deutschland und Europa bereit und stehen für Anwendungsuntersuchungen aus dem Sicherheitsbereich zur Verfügung.

Im Hochsicherheitsbereich hat der Wechsel zu quantensicherer Kryptografie begonnen.

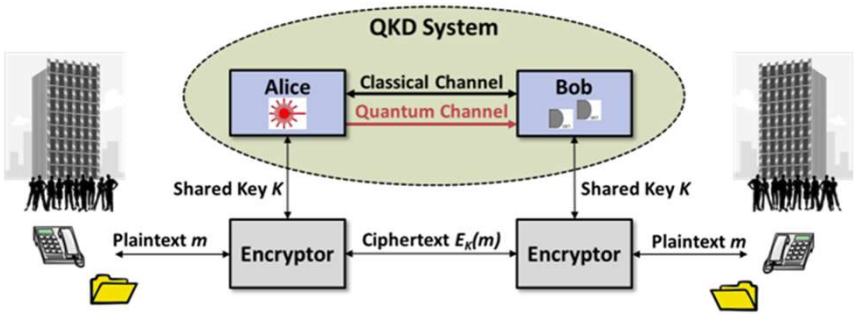
In Staat, Wirtschaft und Gesellschaft ist die Dringlichkeit des Wechsels zu quantensicherer Kryptografie akzeptiert und in kritischen Bereichen eingeleitet. Pilot-Infrastrukturen binden Partner aus den verschiedenen Bereichen ein.

Technologien und Lösungen der Quantenkommunikation von Anbietern aus Deutschland und Europa stehen für Staat, Wirtschaft und Gesellschaft zur Verfügung.

Die Studie zur Realisierbarkeit von Quantencomputern wird fortgeführt und aktualisiert.

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

businesswire
A BERKSHIRE HATHAWAY COMPANY

HOME SERVICES NEWS EDUCATION ABOUT US

Search

INVESTOR ALERT: Arqit Quantum Inc. f/k/a Centricus Acquisition Corp. Investors Substantial Losses Have Opportunity to Lead the Arqit Class Action Lawsuit - AR 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 Centricus Acquisition Corp. (NASDAQ: ARQQ; ARQQW) securities between September 7, 2021 and April 18, 2022, inclusive (t Period") and/or all holders of Centricus securities as of the record date for the special meeting of shareholders held on August 3 to consider approval of the merger between Arqit and Centricus (the "Merger") and entitled to vote on the Merger have until July 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 Securities Exchange Act of 1934.

If you suffered significant losses and wish to serve as lead plainti *Arqit* class action lawsuit, please provide your information by clicking here. You can also contact attorney J.C. Sanche Robbins Geller by calling 800/449-4900 or via e-mail at jsanchez@rgrdlaw.com. Lead plaintiff motions for the *Arqit* clas 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 technolo alleged its quantum encryption technology would be secure against current and future forms of cyberattacks, including from a q computer. Centricus was a special purpose acquisition corporation ("SPAC" or blank check company) formed for the purpose of a merger, capital stock exchange, asset acquisition, stock purchase, reorganization, or similar business combination with one o businesses. Prior to the Merger, Centricus shares traded on the NASDAQ under the ticker symbol CENHU.

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.

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

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, …

Key Points from BSI‘s recommendations

- QKD is feasible with technology available today and provides key agreement schemes whose security is based on quantum mechanical principles and which are expected to be information-theoretically secure at the protocol level.
- In addition to theoretical security, implementation security must also be considered.
- QKD is subject to some restrictions and is therefore only suitable for certain application scenarios.
- Standards, for example on protocols, and certified products are still lacking.
- QKD should only be used in hybrid mode with classical and post-quantum key agreement schemes.
- Using the one-time pad alone for encryption is not recommended.

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."*

Some Buzzwords

- **Certification** (Commoncriteriaportal.org, ISO 15408)
- **Approval** (https://www.bsi.bund.de/DE/Themen/OeffentlicheVerwaltung/Zulassung/zulassung_node.html)
- **Accreditation**
- Digital Sovereignty
- **Supply chain** security: Can components be used? Are components available?

For government use Certification is often not sufficient. There may be additional requirements, not only on the product itself, but also on its lifecycle and origin.

CC-Evaluation criteria – a first step

- PP-QKD funded by BSI, cooperation with ETSI
- Goal: An internationally accepted ETSI-Standard
- Draft available at 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.

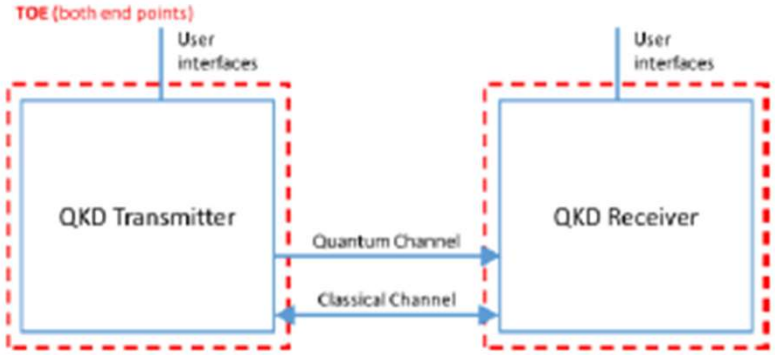
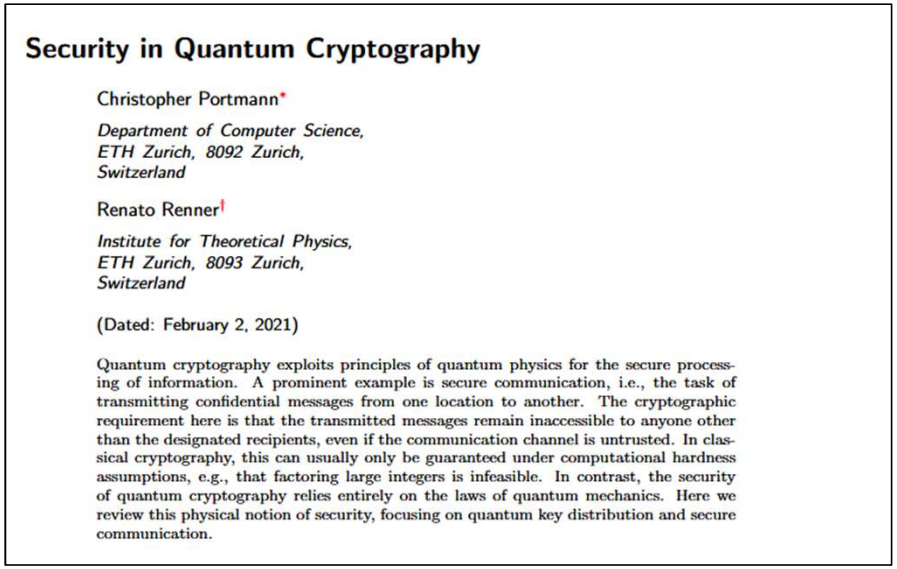


Figure 1: The TOE-boundary, i.e. the two QKD modules

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

Practical Security – Projekt 575

Seitenkanalangriffe auf QKD-Systeme
Angebotsfrist verlängert bis zum 16.08.2022

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

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.

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
- 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)

Use of QKD?

- BSI‘s position: QKD only in hybrid solutions as **optional additional input**. Hybrid solutions support End-to-End security and may mitigate the Store-now-Decrypt-Later threat
- Encryption: AES (*Additional* use of the OTP possible-> How many key bits can be generated?)
- Management of Authentication Keys has to be solved? PKI and ITS?
- **Availability** of certified/approved Products? XXX years?

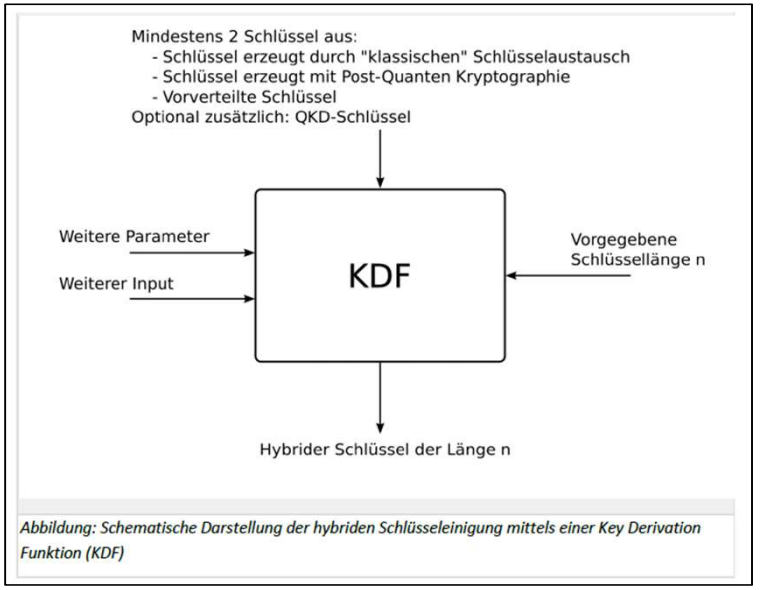
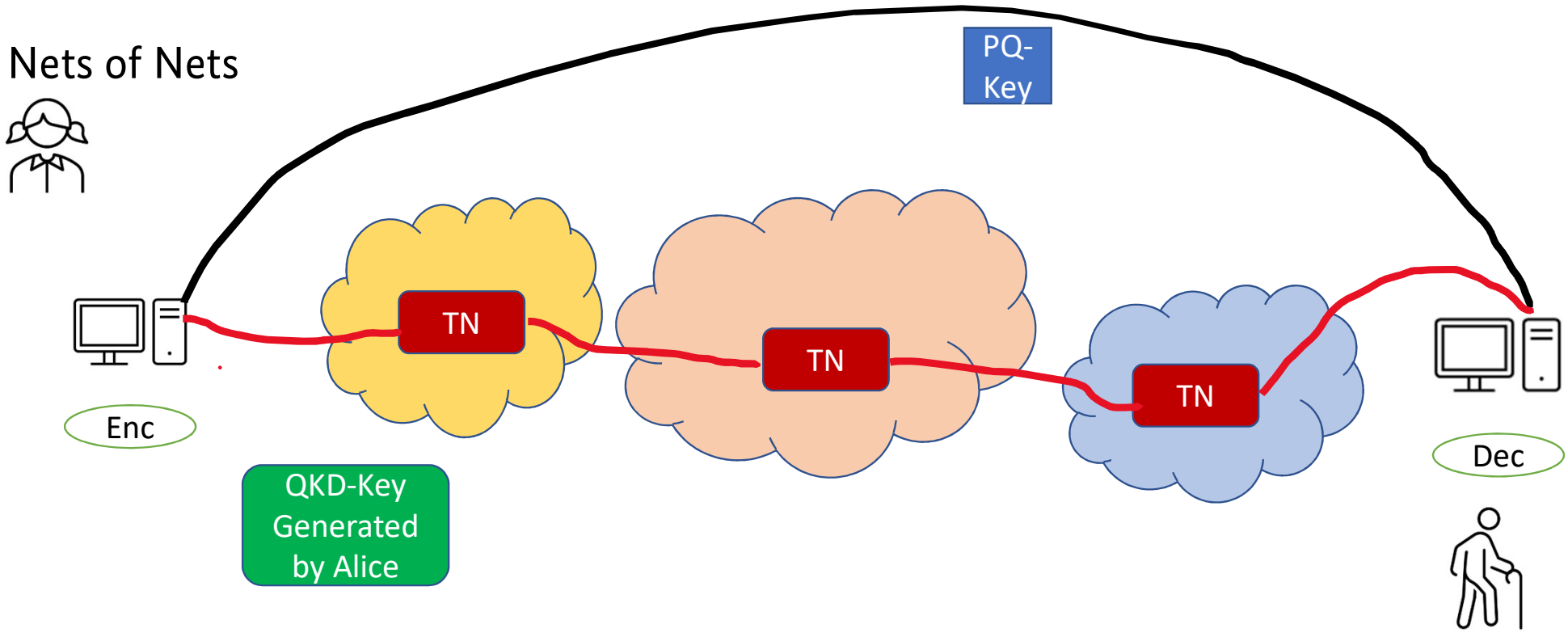


Abbildung: Schematische Darstellung der hybriden Schlüsseleinigung mittels einer Key Derivation Funktion (KDF)

Nets of Nets



- In Trusted Nodes QKD-Keys are visible. No End-to-End Security from QKD
- Trust in all networks needed where your QKD-Key passes through a TN
- Net of networks?
- Hybrid use of PQ and QKD gives End-to-End Security based on PQ
- How can different security levels be handled?
- Omitting infrastructure needed for authentication
- What happens at borders?
- When will Quantum-Repeaters be available?

Some open questions

- Key-Updates for authentication keys
- How to build a net? Use PQ-certificates?
- Man-in-the-middle attacks
- Stability (new nodes, out of phase nodes, ...)
- How many bits should be generated during an QKD key-agreement?
- Protection of generated QKD-Keys
- Export of keys (via TLS?) and remote access?
- Standardisation (BB84 Decoy state?) & proofs
- RNGs with ITS guarantees
- Handling of different security levels
- Hybridization

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

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