



Potentielle Gesellschaftliche Auswirkungen von Quantentechnologien

<https://quant-x-sec.com/> | consulting@quant-x-sec.com



Unsere Expertise: Beratung, Analysen und Entwicklungen in

Informations- und IT-Sicherheit

Informationsrisikomanagement

Post-Quanten Sicherheit

Quanten Algorithmen

System- und Algorithmen Engineering



Geistige Aspekte und Motivation



Meine Mission (Heute)

Einführung in Quantentechnologien

Chancen und Risiken von Quantentechnologien aufzeigen

Kontext Informationssicherheit

Beispiele für Information:

- 1) Geld (Zahlungns-Transaktionen)
- 2) Persönliche Daten
- 3) Verträge
- 4) Zugangsdaten
- 5) ...



Quanten-Technologien

Basis-Informationseinheiten in Kommunikation und Computing

Bits

Phyikalisch repräsentiert durch ein "Two-State-Device"

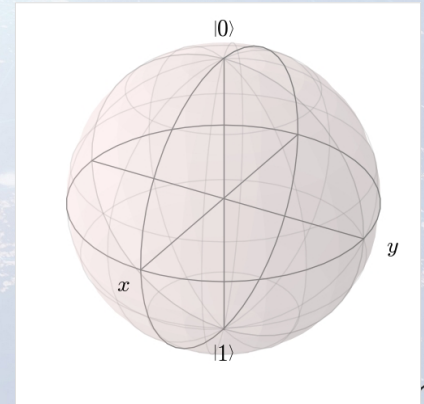
$$\{+, -\}, \{\text{true}, \text{false}\}, \{0, 1\} \cong F_2$$

- Flip-flop (Schaltkreis mit zwei stabilen Zuständen),
- Zwei untersch. Level von Lichtintensität
- Zwei untersch. Richtungen von Magnetisierung oder Polarisierung
- Orientierung von reversibler Doppelstrang-DNA

Qubits

Ein Quantensystem, das in Supersposition von zwei klassischen Bit-Werten existieren kann.

$$\{c_0|0\rangle + c_1|1\rangle \mid c_0, c_1 \in \mathbb{C}\} \cong$$



Quanten-Technologien

Basis-Informationseinheiten in Kommunikation und Computing

Bits

Physikalisch repräsentiert durch ein "State-Device"

$\{+, -\}, \{\text{true}, \text{false}\}, \{0, 1\} \cong F_2$

- Flip-flop (Schaltkreis mit zwei stabilen Zuständen),
- Zweifach-Schalter von Logikschaltung
- Zweifach-Schaltungen von
- Magnetisierung oder Polarisierung
- Orientierung von reversibler
- Doppelstrang-DNA

Qubits

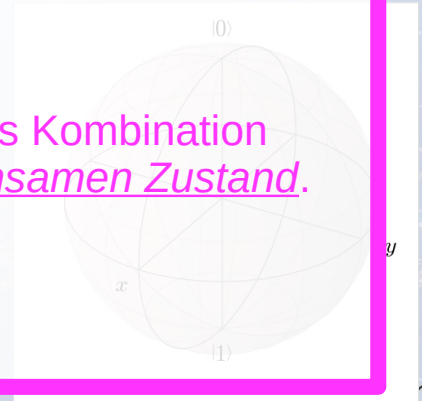
Superposition = Addition mehrerer Zustände
Bezug zu Lösungen der (linearen) Schrödinger Gleichung

kann.

Verschränkung

Der Zustand eines Systems mehrerer Teilchen lässt sich nicht als Kombination unabhängiger Einzelteilchen beschreiben, sondern nur als gemeinsamen Zustand.

$$\{c_0|0\rangle + c_1|1\rangle \mid c_0, c_1 \in \mathbb{C}\} \cong \mathbb{C}^2$$



Quanten-Technologien

Motivation für Entwicklung und Forschung

Sichere Kommunikation

Ultimative Rechenpower

Ultrapräzise Sensoren

Lösung vieler offener Probleme

Die Entwicklung der Quantentechnologien wird jedoch auch als internationaler Rüstungswettlauf bezeichnet.



Quantentechnologien – Realität

← → ↺ <https://duckduckgo.com/?q=quantum+Computer&t=newext&atb=v284-1&iax=images&ia=images> 120% ☆



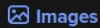
quantum Computer



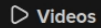
Privacy, simplified. ▾



All



Images



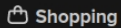
Videos



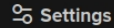
News



Maps

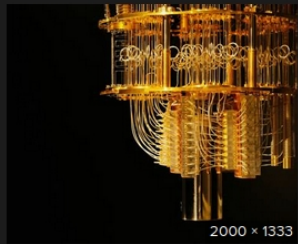


Shopping



Settings

Germany ▾ Safe search: moderate ▾ Any time ▾ All sizes ▾ All colors ▾ All types ▾ All layouts ▾ All Licenses ▾



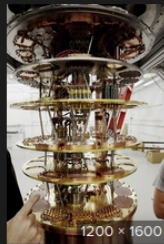
2000 × 1333

Quantum Computers Are Not Wha...
medium.com



940 × 1393

Quantum Comput...
spectrum.ieee.org



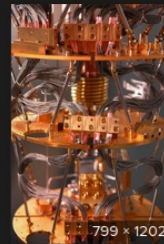
1200 × 1600

VW Group and Go...
carbobydesign.com



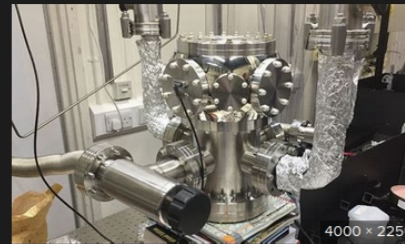
1920 × 1080

Newly Discovered State of Matter 3D Quantum Li...
trendintech.com



799 × 1202

Quantum comput...
extremetech.com



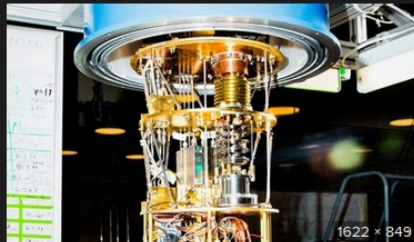
4000 × 2250

Physicists are working on 'unbelievably fast' qua...
shropshirestar.com



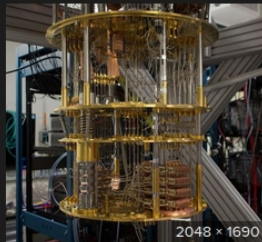
1200 × 800

Quantum computers are weirder and mo...
newsscientist.com



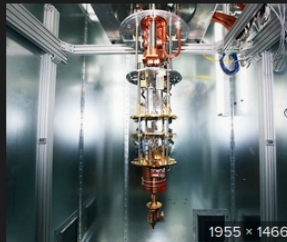
1622 × 849

Noisy Quantum Computers Could Be Good for Ch...
wired.com



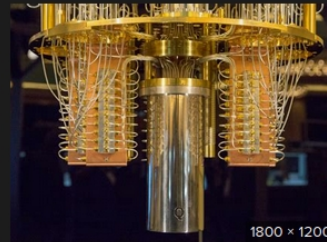
2048 × 1690

This Startup Raised \$2.7 Millio...
forbesmiddleeast.com



1955 × 1466

Application of Quantum Computer...
acontinuallearner.wordpress.com



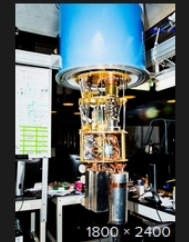
1800 × 1200

Will quantum computers doom the blo...
norbertbiedrzycki.pl



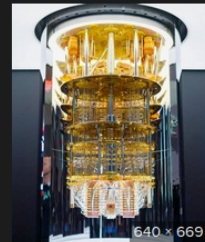
2189 × 1643

Quantum Computing, What Is It A...
mouser.com



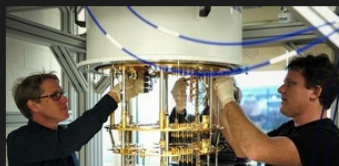
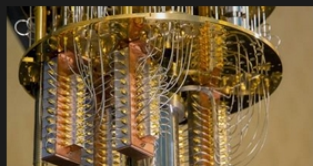
1800 × 2400

Noisy Quantum C...
wired.com



640 × 669

IBM and Fraunhofer br...
electronicsmaker.com



QUANTUM
COMPUTER



Klassen von Quantentechnologien

QRNG

Quantum Random Number Generator. Erzeugt idealerweise echte Zufallswerte.

Quanten Kommunikation (QKD)

Aka Quantum Key Distribution. Schlüsselaustausch auf quantenmechanischen Prinzipien.

Quantum Sensing und Metrologie

Hochpräzise Messungen und Metriken auf Basis von quantenmechanischen Effekten.

Quantum Imaging (Erweiterung von Quantum Sensing)

Hochauflösende Abbildung eines Objekts mit quantenmechanischen Effekten.

Quanten Simulation

Simulation auf quantenmechanischen Prinzipien zur Lösung eines spezifischen Problems

Quantum Computing

- Quantum Annealing (für wenige Klassen von Problemen)
- Gate-based Quantum Computing (im Idealfall ein universeller Computer)



Quantentechnologien in Anwendung – Beispiele

QRNG

Quantum Random Number Generator. Erzeugt idealerweise echte Zufallszahlen.

Quanten Kommunikation (QKD)

Aka Quantum Key Distribution. Schlüsselaustausch auf quantenmechanischen Prinzipien.

Quantum Sensing und Metrologie

Hochpräzise Messungen und Metriken auf Basis von quantenmechanischen Effekten.

Quantum Imaging (Erweiterung von Quantum Sensing)

Hochauflösende Abbildung eines Objekts mit quantenmechanischen Effekten.

Quanten Simulation

Simulation auf quantenmechanischen Prinzipien zur Lösung eines spezifischen Problems

Quantum Computing

- Quantum Annealing (für wenige Klassen von Problemen)
- Gate-based Quantum Computing (im Idealfall ein universeller Computer)

Kommerzielle Anwendung in QKD Geräten

Wien (seit 2004), DARPA, Regierung Genf, ...

Tests für Militär und Medizinische Anwendungen

Protein Folding / Materialwissenschaften

D-Wave's Advantage > 5000 qubits
Google, IBM, Terraquantum, Quantinuum, ...



Quantentechnologien – Ethische Aspekte



Quantum Machine Learning

Diskriminierende Algorithmen

Medizin

Personalisierte Medizin

Logistik

Effiziente Routen

...

Projektförderungen

Politische Aspekte

Diskriminierung von Experten

Zerrissener Westen



Quantentechnologien – Ethische Aspekte



Marketing - Illusionen - Machbarkeit

Quantum Machine Learning

Diskriminierende Algorithmen

Medizin

Personalisierte Medizin

Logistik

Effiziente Routen

Projektförderungen

Politische Aspekte

Diskriminierung von Experten

Zerrissener Westen



Quantentechnologien und Informationssicherheit

QRNG

Quantum Random Number Generator. Erzeugt idealerweise echte Zufallswerte.

Quanten Kommunikation (QKD)

Aka Quantum Key Distribution. Schlüsselaustausch auf quantenmechanischen Prinzipien.

CHANCEN

Quantum Sensing und Metrologie

Hochpräzise Messungen und Metriken auf Basis von quantenmechanischen Effekten.

Quantum Imaging (Erweiterung von Quantum Sensing)

Hochauflösende Abbildung eines Objekts mit quantenmechanischen Effekten.

Quanten Simulation

Simulation auf quantenmechanischen Prinzipien zur Lösung eines spezifischen Problems

Quantum Computing

- Quantum Annealing (für wenige Klassen von Problemen)
- Gate-based Quantum Computing (im Idealfall ein universeller Computer)

RISIKEN



Quantentechnologien und Informationssicherheit

LÖSUNGEN

QRNG – HARDWARE basiert

Quantum Random Number Generator. Erzeugt idealerweise echte Zufallswerte.

Quanten Kommunikation (QKD) – HARDWARE basiert

Aka Quantum Key Distribution. Schlüsselaustausch auf quantenmechanischen Prinzipien.

+++ Post-Quanten-Kryptografie – SOFTWARE basiert

Quantenresistente Kryptografie für klassische digitale Kommunikation, als offizieller Standard verfügbar.

Quantum Imaging (Erweiterung von Quantum Sensing)

Hochauflösende Abbildung eines Objekts mit quantenmechanischen Effekten.

Quanten Simulation

Simulation auf quantenmechanischen Prinzipien zur Lösung eines spezifischen Problems

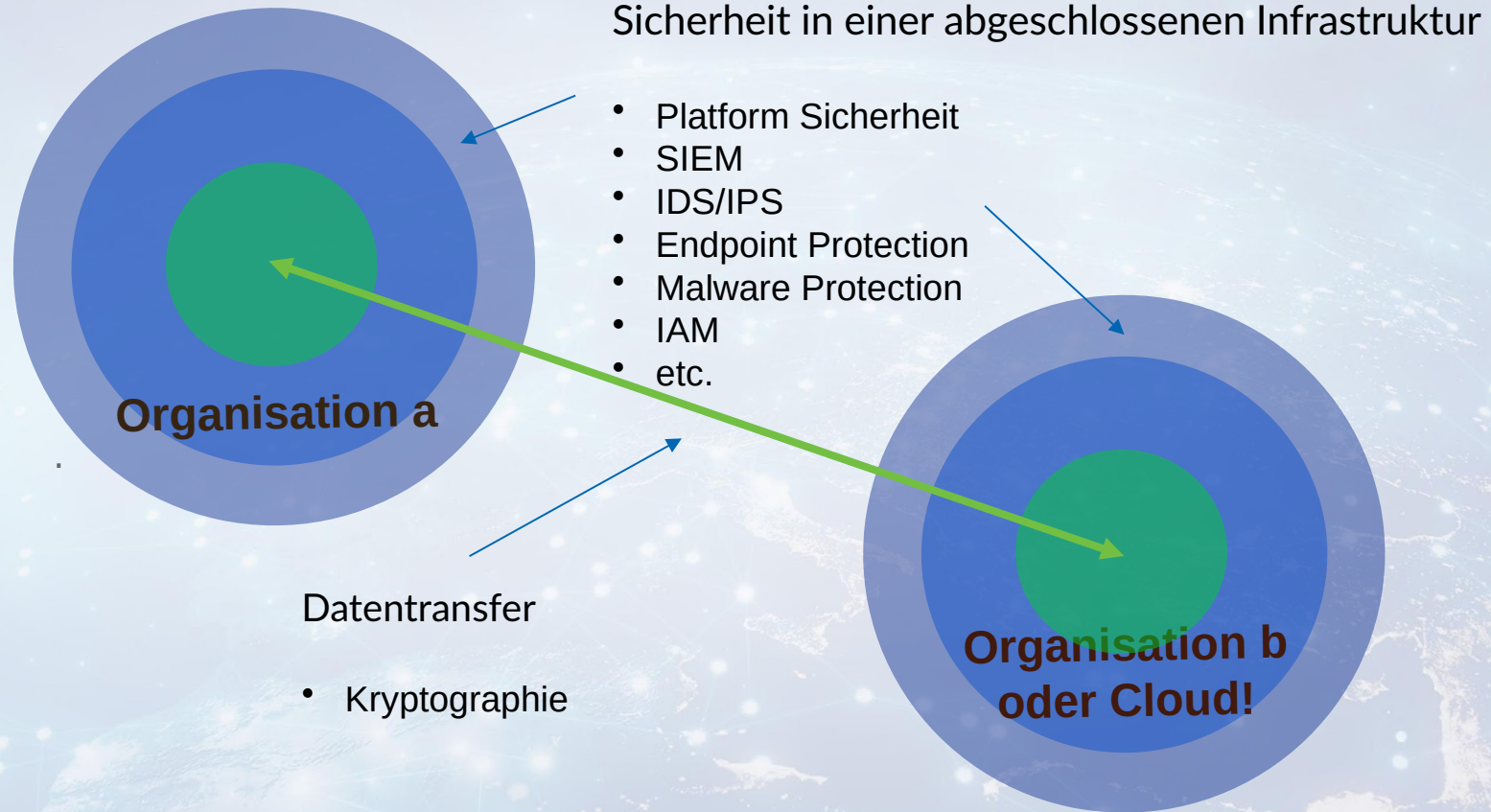
Quantum Computing

BEDROHUNG

- Quantum Annealing (für wenige Klassen von Problemen)
- Gate-based Quantum Computing (im Idealfall ein universeller Computer)



Sonderstellung Kryptografie



Bedrohung für Kryptografie durch Quanten-basierte Angriffe

Full Cryptanalysis

Bei asymmetrischer Kryptografie kann der private Schlüssel direkt aus dem öffentlichen Schlüssel berechnet werden.

Effiziente Brute Force Methoden

Private Schlüssel symmetrischer Kryptografie können mit effizienten Suchalgorithmen gefunden werden.



Weitere Bedrohungen für Klassische Kryptografie

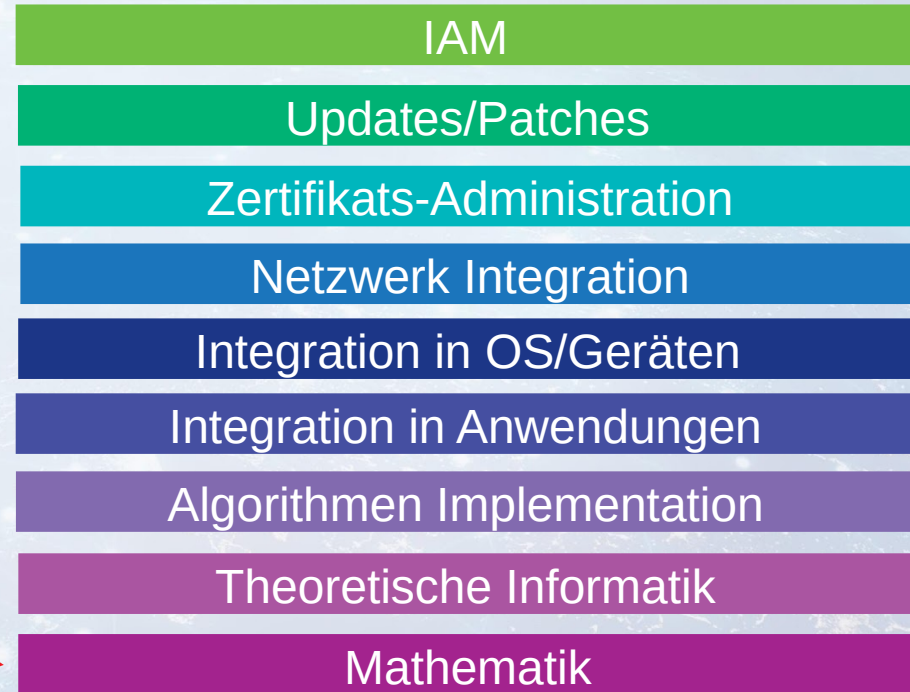
BEDROHUNGEN

High Performance Anwendungen
(Binäre Technologien)

Neue Mathematische Lösungen

Quantum
Computing

Kryptografie Stack



Post-Quantum Cryptography

Software-basierte Sicherheitslösungen
Standardisiert (NIST, ANSI, etc.)

Grundlage: Mathematische Probleme, die nicht effizient durch Quantenalgorithmien gelöst werden können.

Post-Quantum Cryptography PQC

Overview

The Candidates to be Standardized and Round 4 Submissions were announced July 5, 2022. NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is now available. NIST has developed Guidelines for Submitting Tweaks for Fourth Round Candidates.

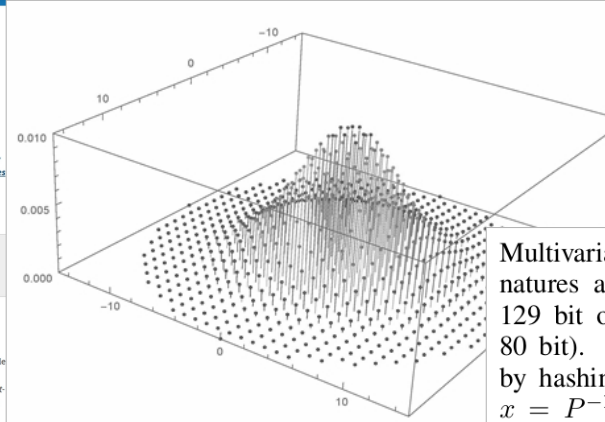
NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the [Post-Quantum Cryptography Standardization page](#).

[Post-Quantum Encryption: A Q&A With NIST's Matt Scholl](#)

[Post-Quantum Cryptography: the Good, the Bad, and the Powerful \(video\)](#)

Background

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.



Multivariate signature schemes provide the shortest signatures amongst post-quantum algorithms (GUI [20] 129 bit over $GF(2)$ for a quantum security level of 80 bit). The signature x of a message m is created by hashing m into a vector $y \in F^n$ and computing $x = P^{-1}(y) = T^{-1}(P'(S^{-1}(y)))$. The receiver can simply compute the hash y and check if $P(x) = y$.



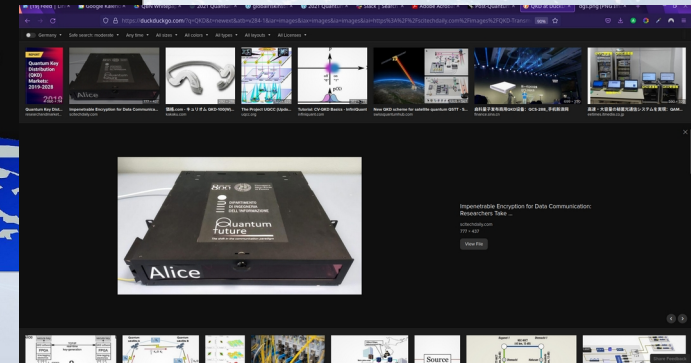
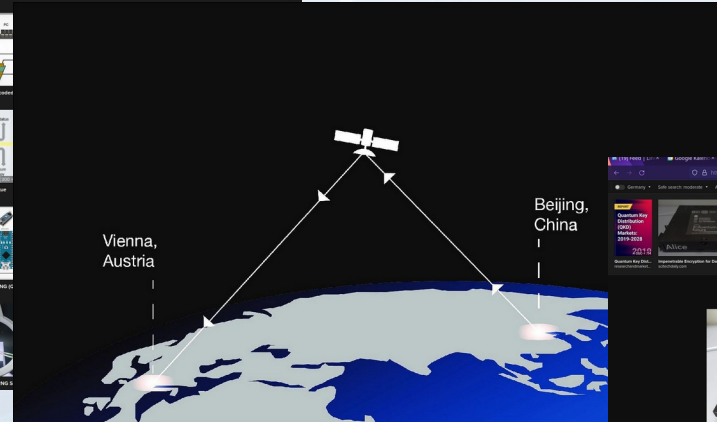
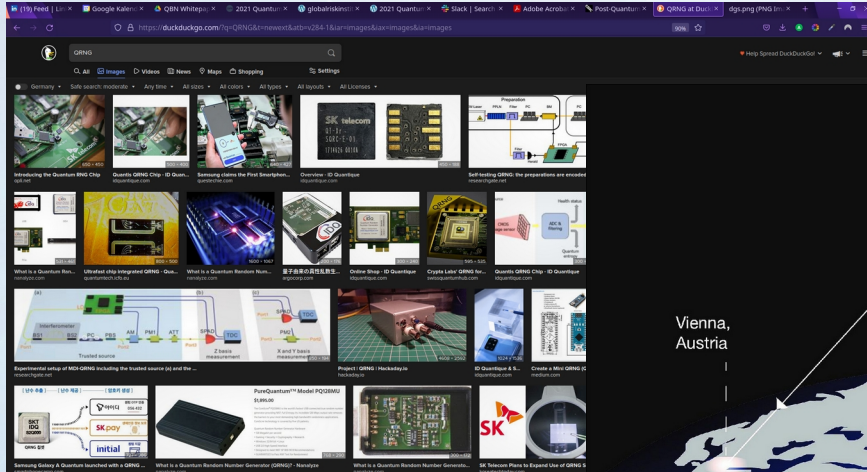
Quanten Kommunikation (aka QKD) und QRNG

Hardware Lösung - basiert auf Quantum-mechanischen Prinzipien

Standardisierung läuft (Global, EU und national)

QKD - nicht berechenbare Sicherheit für Schlüsselaustausch

QRNG - echte Zufallswerte (idealerweise, theoretisch)



12/04/22

xb@quant-x-sec.com



Quanten Kommunikation (aka QKD) und QRNG

Hardware Lösung - basiert auf Quantum-mechanischen Prinzipien

Standardisierung läuft (Global, EU und national)

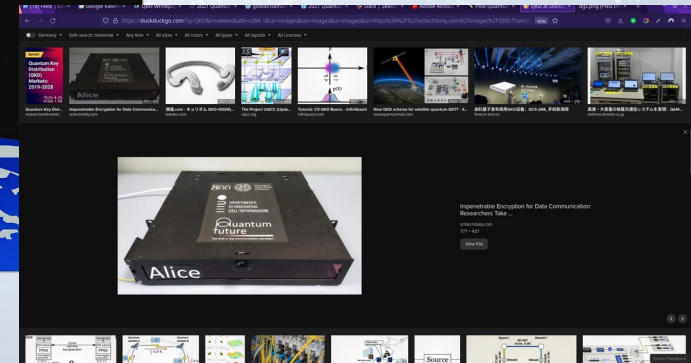
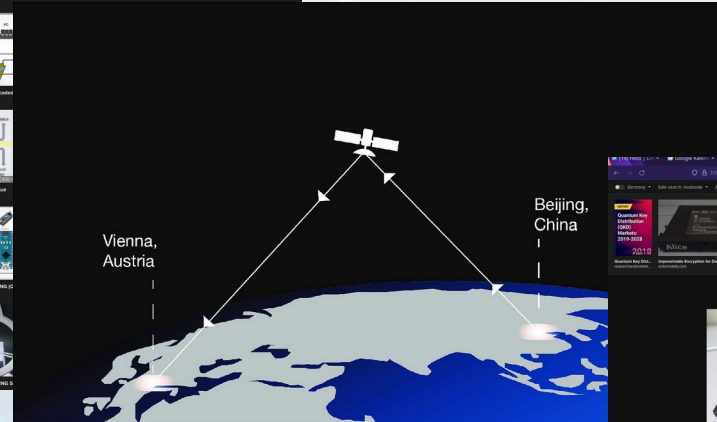
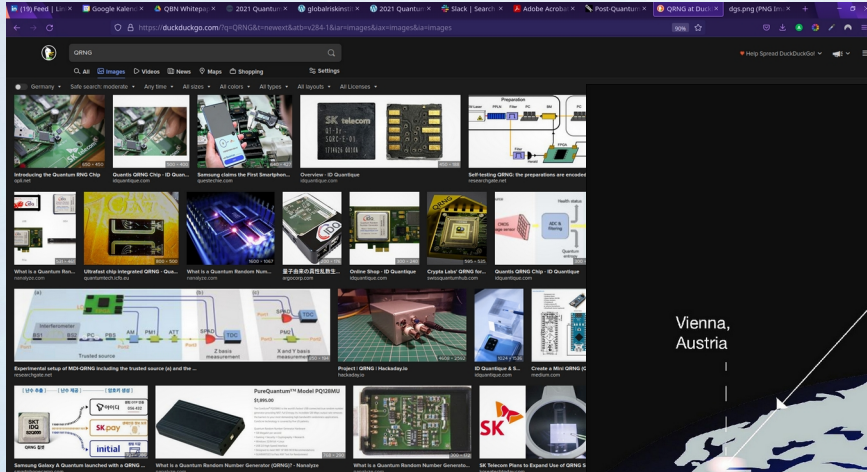
QKD - nicht berechenbare Sicherheit für Schlüsselaustausch

QRNG - echte Zufallswerte (idealerweise, theoretisch)

Integration in digitale Infrastrukturen
in experimentellen Projekten

Zertifizierungen noch nicht möglich

Nachweis-Methoden noch
nicht ausgearbeitet



12/04/22

xb@quant-x-sec.com



Informationssicherheit - Bereiche



Informationssicherheit – Immense Last für Organisationen



Cybercrime

Stetige Steigerung der Angriffe
Angriffe sind immer intelligenter

Last auf IT, Business und Management

Erdrückende Arbeitslast
Perfekter Schutz wird niemals erreicht

Ethische Lösungsansätze

Klare Kommunikation
Respektvoller Austausch
Akzeptanz von Diversität
Umgang mit Kritik



Warum jetzt handeln?

Weiteren Bedrohungen vorbeugen

- Passwort und Krypto Cracking Tools (Hashcat und ähnliche Tools)
- Aggregierte Computing Ressourcen und Parallelisierung von Angriffs-Prozessen
- Neue mathematische Lösungen betreffen Parameter und Konfiguration von klassischer Kryptografie

Potentiell Katastrophale Auswirkungen

- Die Folgen des Eintritts von Quantenbedrohungen sind katastrophal! Die Entwicklung von Quanten-prozessoren wird von Experten als “internationales Kriegssrennen” bezeichnet.
- Datensammler können in der Vergangenheit gesammelte Daten entschlüsseln, sobald entsprechende Quantenprozessoren verfügbar sind.

Herausforderung Reaktionszeit

- *Migrationen können Jahre dauern. - Wir kennen das alle!!!*



Handlungsempfehlungen / Roadmaps

Handlungsempfehlungen / Roadmaps

1. BSI: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf>
2. NIST: <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions>
3. ANSSI: <https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/>

Information zu Quanten Kommunikation/QKD

Es gibt weltweit seit vielen Jahren etablierte QKD Netzwerke, z. B. QUESS: 2000km quantum communication channel between Shanghai and Beijing, SwissQuantum, SECQC Austria, Tokyo QDK Network, DARPA USA. Es gibt jedoch noch keine vom BSI zertifizierte oder zugelassene QRNG und QKD Geräte- Mehr Information zu Empfehlungen des BSI und der NIST:

- [BSI | Quantenkryptografie](#)
- [NIST | Quantum Networks](#)



Fazit

Quantentechnologien kommen mit Chancen und Risiken.

Wir müssen darauf vorbereitet sein, dass Erwartungen in beide Richtungen nicht eintreffen.

Gute Lösungen bestimmen wir Menschen, nicht die Technologien selbst.

Die besten Lösungen finden wir mit respektvoller Zusammenarbeit!

Unsere Webseite: <https://quant-x-sec.com/>
Slides: <https://quant-x-sec.com/published.htm>

<https://quant-x-sec.com/> | consulting@quant-x-sec.com

