Quantum Security

Dipl. Math. X. Bogomolec
Algorithms | IT-Security
Oktober 2018

Über mich

Ausbildung

Mathematik mit Nebenfach Physik

Arbeitsbereiche

Algorithmen | IT-Security

Letzte Projekte

http://ceunix.eu/ | https://tiiqu.com | SOC Helaba
... und Gründung von X4pi UG

Meine Mission

Vermittlung eines Überblick über aktuelle Entwicklungen

Kontakt: indigomind@protonmail.ch
Webseite: http://coder.tjingwan.com

Meine Perspektive

Europa (Regulierungen, Regulierungen, Regulierungen)

EU-DSGVO, PSD2,
Instant Payments, ..

Science:
Quanten Technologien,
Post-Quantum Crypto, AI, ...

Xenia Bogomolec
indigomind@protonmail.ch

Warum Post Quanten Kryptologie?

Math Master

Research
Algorithms & Implementation
Arithmetic Algebraic Geometry

Software Engineering

Web
Client-Server-Systems
Networks

Post-Quantum Cryptography

Arithmetic Algebraic Geometry
Programming
IT-Security

IT-Security

Lawful Telecommunication Interception (State)
Authentication Protocols
IT-Security Monitoring
Software Security
Cryptology

Xenia Bogomolec
indigomind@protonmail.ch

Warum Post Quanten Kryptologie?

Math Master

Research
Algorithms & Implementation
Arithmetic Algebraic Geometry

Software Engineering

Web
Client-Server-Systems
Networks

Post-Quantum Cryptography

Arithmetic Algebraic Geometry
Programming
IT-Security

IT-Security

Lawful Telecommunication Interception (State)
Authentication Protocols
IT-Security Monitoring
Software Security
Cryptology

+ Ethik

Xenia Bogomolec
indigomind@protonmail.ch

Zentrale Themen

Xenia Bogomolec
indigomind@protonmail.ch

Unsere zentralen Themen

Quanten Technologien

Benefits und Herausforderungen

Quantenkryptografie, etc. etc. etc.

Binäre Technologien

Post-Quanten Kryptografie
Sicherheit gegen Angriffe von QC

Xenia Bogomolec
indigomind@protonmail.ch

Unsere zentralen Themen

- Quanten Technologien

Benefits und Herausforderungen

Quantenkryptografie, etc. etc. etc.

Quantenkryptografie ≠ Post-Quanten Kryptografie

(Physik, Hardware) (Mathematik, Software)

Binäre Technologien

Post-Quanten Kryptografie

Sicherheit gegen Angriffe von QC

Xenia Bogomolec
indigomind@protonmail.ch

Unsere zentralen Themen

Herausforderungen

Die Sicherheit aktuell genutzter Krypto-Algorithmen beruht seit

40 Jahren

auf der Annahme, dass Primzahlfaktorisierung und der diskrete Logarithmus nicht in annehmbarer Zeit berechnet werden können.

$$n = p_1 \cdot p_2$$

$$a = r^s$$

Xenia Bogomolec
indigomind@protonmail.ch

Unsere zentralen Themen

Herausforderungen

Die Sicherheit aktuell genutzter Krypto-Algorithmen beruht seit

40 Jahren

auf der Annahme, dass Primzahlfaktorisierung und der diskrete Logarithmus nicht in annehmbarer Zeit berechnet werden können.

$$n = p_1 \cdot p_2$$

$$a = r^s$$

Genügend potente Quantencomputer werden das jedoch können!

Xenia Bogomolec
indigomind@protonmail.ch

Was heisst genügend potent?

Genügend potente Quantencomputer werden das jedoch können!
IBM schätzt, dass es 4 1/2 Jahren soweit ist.

Factoring algorithm (RSA)			EC discrete logarithm (ECC)			classical
n	$\approx$ # qubits	time	n	$\approx$ # qubits	time	time
	$2n$	$4n^3$		$f'(n)$ $(f(n))$	$360n^3$	
512	1024	$0.54 \cdot 10^9$	110	700 (800)	$0.5 \cdot 10^9$	C
1024	2048	$4.3 \cdot 10^9$	163	1000 (1200)	$1.6 \cdot 10^9$	$C \cdot 10^8$
2048	4096	$34 \cdot 10^9$	224	1300 (1600)	$4.0 \cdot 10^9$	$C \cdot 10^{17}$
3072	6144	$120 \cdot 10^9$	256	1500 (1800)	$6.0 \cdot 10^9$	$C \cdot 10^{22}$
15360	30720	$1.5 \cdot 10^{13}$	512	2800 (3600)	$50 \cdot 10^9$	$C \cdot 10^{60}$

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Quanten-Technologien

Basis-Informationseinheiten in Kommunikation und Computing

Bits

Phyikalisch repräsentiert durch ein "Two-State-Device"

{+, -}, {true, false},{0, 1} ≙ F_2

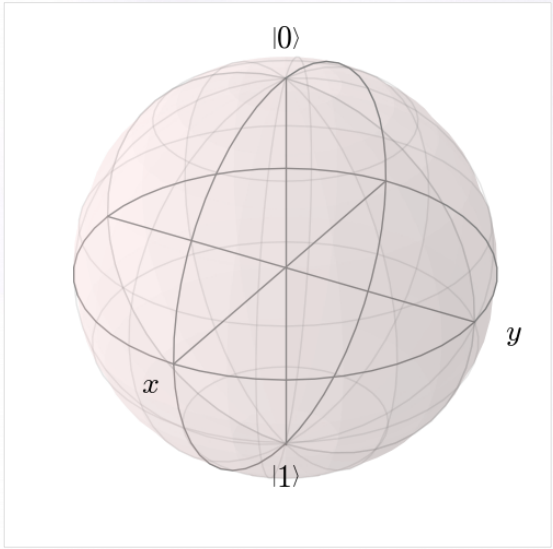
- Flip-flop (Schaltkreis mit zwei stabilen Zuständen),
- Zwei Positionen eines elektrischen Switches ("make" oder "break" in einem Schaltkreis)
- Zwei untersch. Level elektrischer Spannung oder elektrischen Flusses in einem Schaltkreis
- Zwei untersch. Level von Lichtintensität
- Zwei untersch. Richtungen von Magentisierung oder Polarisierung
- Orientierung von reversibler Doppelstrang-DNA

Bezug zu Informationstheorie in Epigenetik?

Qubits

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

$\{c_0|0\rangle + c_1|1\rangle \mid c_0, c_1 \in Z\}$ ≙



Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Basis-Informationseinheiten in Kommunikation und Computing

Bits

Phyikalisch repräsentiert durch ein "Two-State-Device"

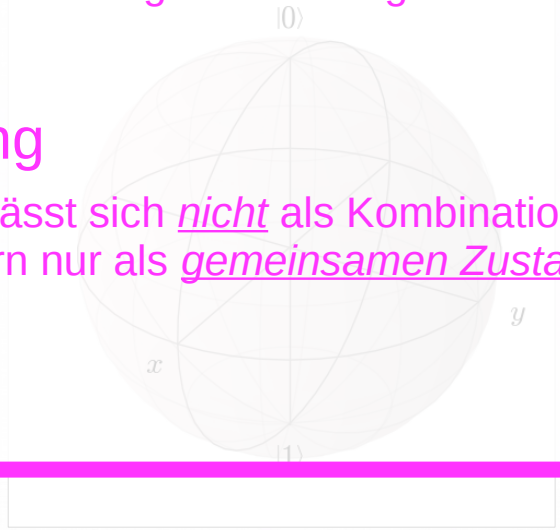
{+, -}, {true, false},{0, 1} $\triangleq$ F_2

- Flip-flop (Schaltkreis mit zwei stabilen Zuständen)
- Zwei Positionen eines elektrischen Switches ("make" oder "break" in einem Schaltkreis)
- Zwei untersch. Level elektrischer Spannung oder elektrischen Flusses in einem Schaltkreis
- Zwei untersch. Level von Lichtintensität
- Zwei untersch. Richtungen von Magentisierung oder Polarisierung
- Orientierung von Molekülen in Doppelstrang-DNA

Qubits

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

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad |c_0|^2 + |c_1|^2 = 1$$



Superposition = Addition mehrerer Zustände

Bezug zu Lösungen der (linearen) Schrödinger Gleichung

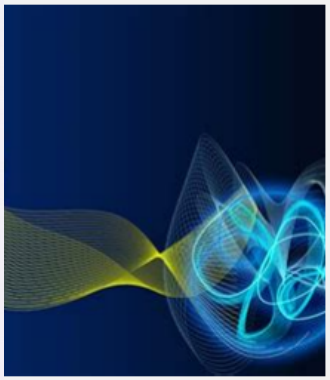
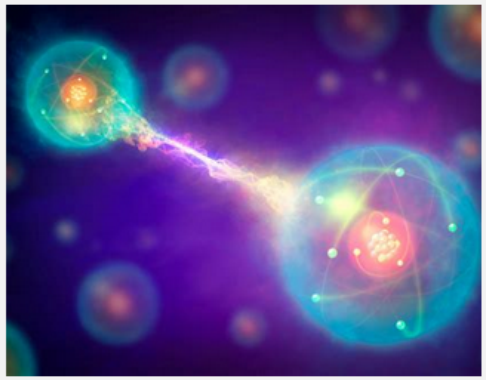
Verschränkung

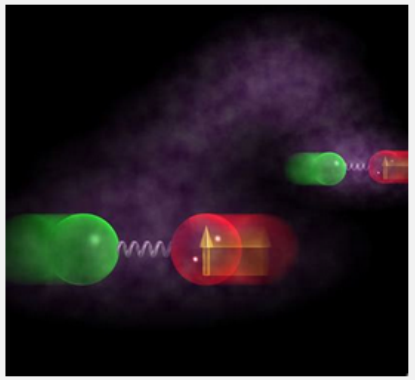
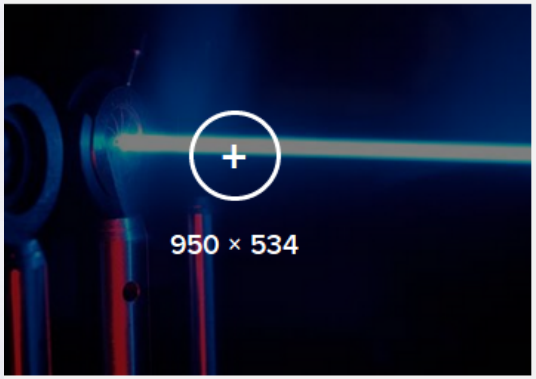
Der Zustand eines Systems mehrerer Teilchen lässt sich *nicht* als Kombination unabhängiger Einzelteilchen beschreiben, sondern nur als *gemeinsamen Zustand*.

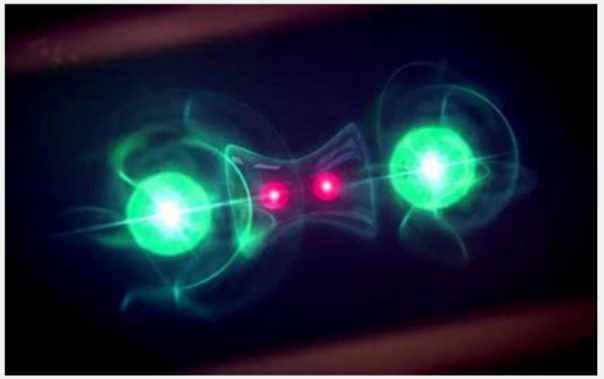
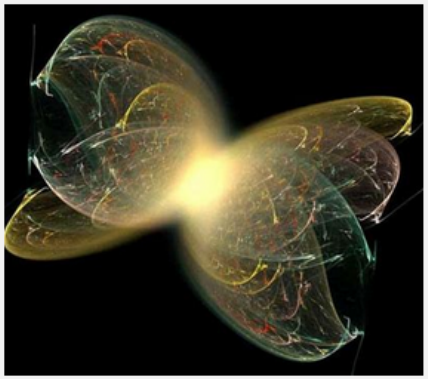
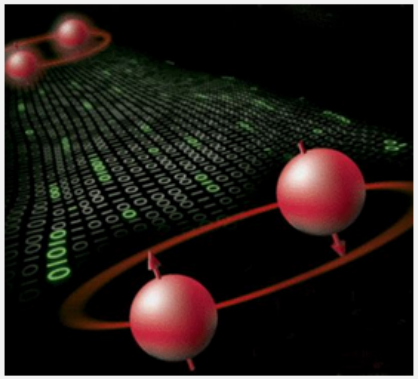
Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Verschränkung

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.

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Überblick

Kommunikation

Simulation

Sensoren und Metrologie

Computing

Quanten Technologien werden fast alle Aspekte unserer Wissenschaften, Technologien, Wirtschaft und unser Leben transformieren …

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Überblick der Technologien mit Beispielen

Kommunikation

- Quanten Repeater
  (ermöglichen rauschfreie Übermittlung von Quanteninformationen, POC)
- Sichere P2P Verbindungen
  (QRNG, QDK)
- Netzwerke

Simulation

- Elektonenbewegungen in Materialien
- Entwicklung und Design neuer Materialien
- Quantum Annealing * (gucken wir uns noch genauer an)

Sensoren und Metrology

- Gravitation
- Magnetische Felder
- Präzisere Atomuhren

Computing

- Logische Qubit Operationen und Memory
  (geschützt durch Error Correction oder Topologische Qubits)
- Algorithmen
- Prozessoren

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Überblick der Bereiche mit ausgewählten Beispielen

Quanten Simulation

Quanten Chemie

Physik

- Materialien
- Kommunikation
- Verschlüsselungen
- Differentialgeometrie

Chemie

- Klima
- Lichtsammelkomplexe
  (Effiziente Nutzung der Energie ohne Wärmeverlust durch stabile Quantenverschränkung von Photonen)

Mathematik

- Lineare Algebra
- Code Breaking
  (Primzahlfaktorisierung und Diskreter Logarithmus)

Computing

- Optimierungen
  Routenplanung
- Finanzen
- Robotics
- Suchen

Biologie

- Pharma
- Bio Moleküle
- Personalisierte Medizin

Quanten Algorithmen

Quanten Machine Learning

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Beispiele von lösbaren Problem-Typen

Big Data Probleme

“Nadel im Heuhaufen” Probleme

Protein Mapping

Wechselwirkung von Stoffen

Früherkennung von Krebs

Effiziente Energienutzung

Xenia Bogomolec
indigomind@protonmail.ch

Quanten Computer

Aktueller offizieller Stand der Entwicklungen

- IBM: 20 qubits QC kommerziell erhältlich seit 2017
- IBM, Google: 50 Qubit Prototyp in 2017
- Google: 72 Qubit Prototyp im März 2018!
- D-Wave 2048 Qubits für Quantum Annealing um Optimierungsprobleme zu lösen (seit 2016)
- D-Wave Leap Platform allows developers access to D-Wave 2048 seit OKtober 2018
- Topological Quantum Bits angekündigt in 2017

  (Lösung für Quanten Error Correction Problem)

Xenia Bogomolec
indigomind@protonmail.ch

Quantum Key Distribution

Sichere Kommunikation mit Quanten-Technologien

Kurz QKD, ist ein implementiertes Kryptographisches Protokoll für Schlüsselaustausch

- Sicherheit beruht auf quantenmechanischen Komponenten
- Der Prozess der Messung eines Quanten-Systems stört i.A. das System selbst
- Jede dritte Partei welche Information während der Schlüsselübertragung zum Schlüssel zu gewinnen versucht würde von den ursprünglichen Kommunikationsparteien detektiert werden

Xenia Bogomolec
indigomind@protonmail.ch

Quantum Key Distribution

Sichere Kommunikation mit Quanten-Technologien

Etablierte QKD Netzwerke

- China (QUESS)
- Austria (SECQC)
- Japan (Tokyo QKD Network)
- Switzerland (SwissQuantum)
- USA (DARPA)

Nachteile

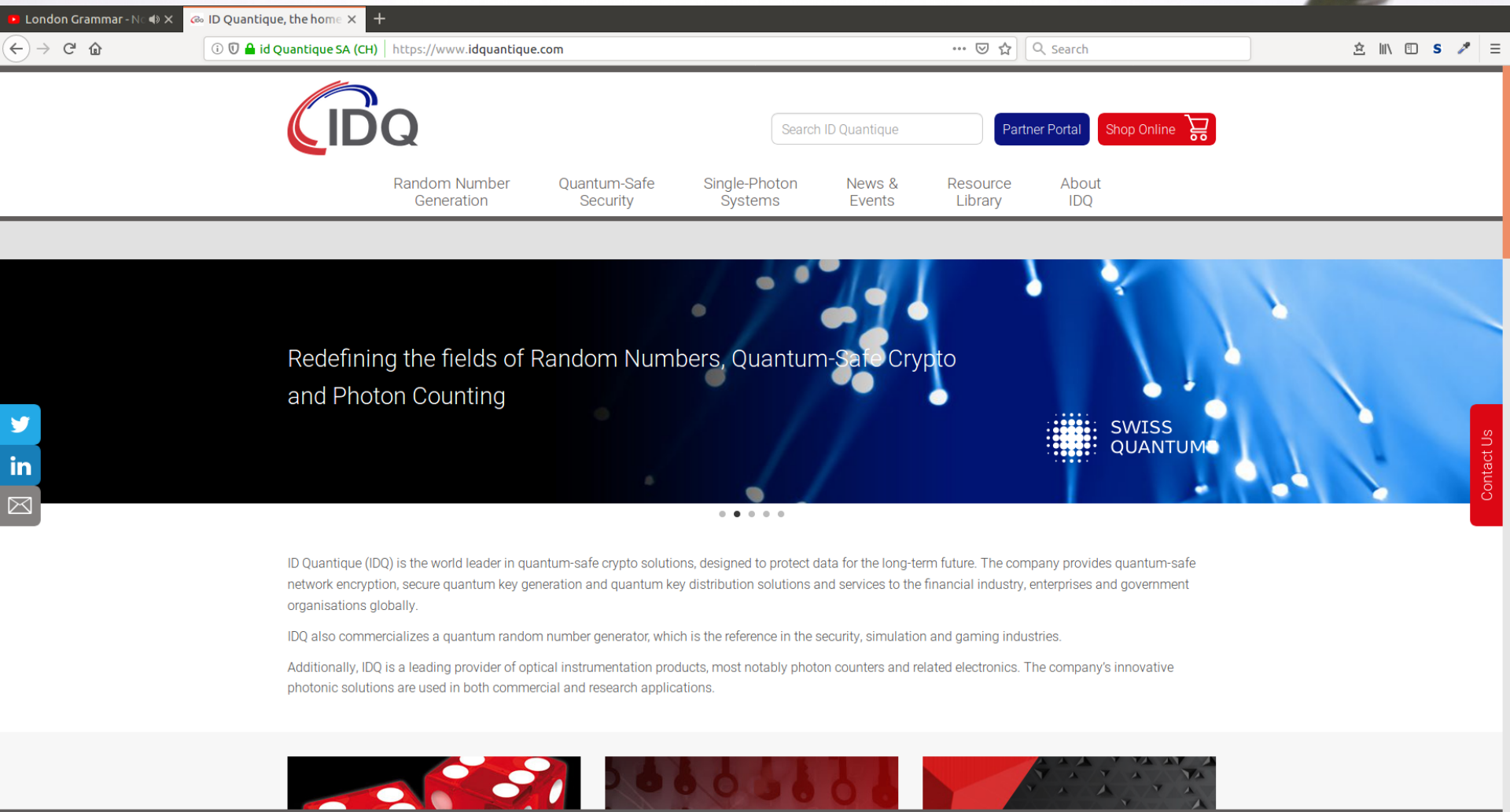
- Limitierte Distanzen zwischen Kommunikationspartnern
- Teure Hardware
- Authentifizierung der Kommunikationspartner nicht integriert

  (Man in the middle attacks sind möglich wenn sich die Kommunikationspartner vorher nicht auf ein Authentifizierungsprotokoll und ein Geheimnis einigen)

Xenia Bogomolec
indigomind@protonmail.ch

Quantum Key Distribution

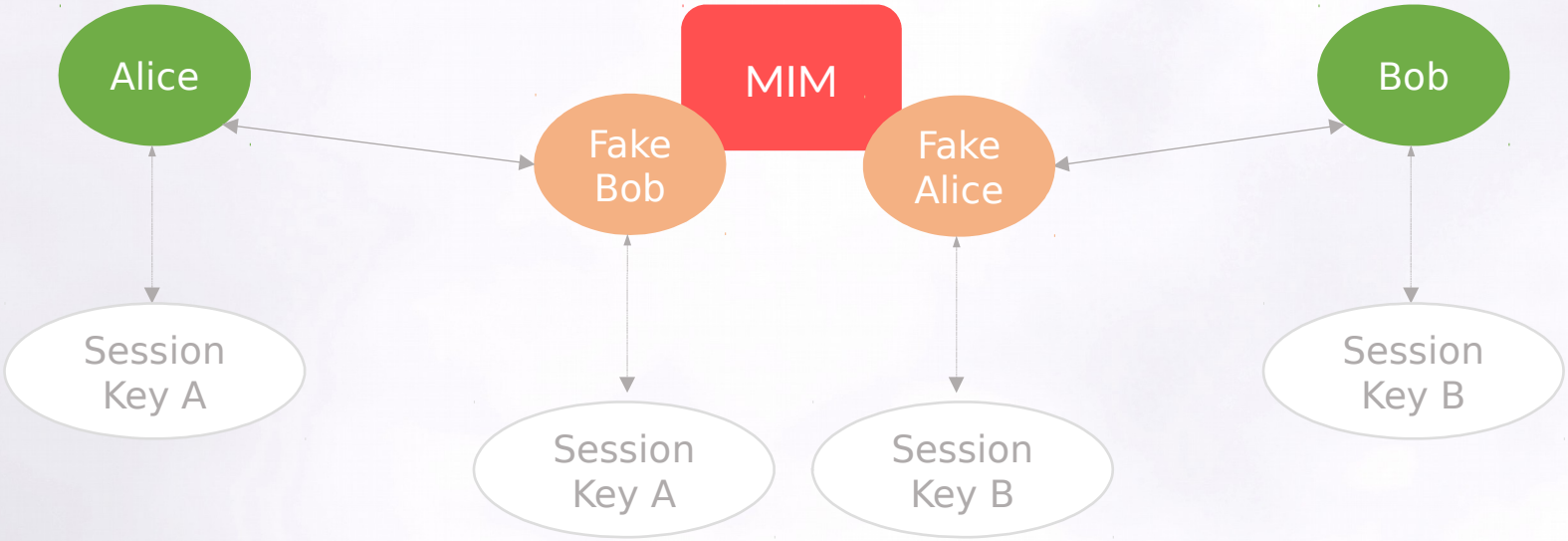
Sichere Kommunikation mit Quanten-Technologien



Xenia Bogomolec
indigomind@protonmail.ch

Quantum Key Distribution

Man in the Middle Attacken



Xenia Bogomolec
indigomind@protonmail.ch

Quanten Technologien

Konsequenzen für die Sicherheit aktuell genutzter Technologien

Das Ende klassischer Asymmetrischer Kryptografie ist absehbar

Was heisst “absehbar” in diesem Kontext?

Sobald Quanten Computer verfügbar sind, welche leistungsfähig genug sind, wird man private Schlüssel von RSA, ECC and Diffie-Hellmann private keys aus den öffentlichen Schlüsseln berechnen können.

.

Wann ist es soweit?

Wir wissen das nicht und Schätzungen sind unterschiedlich. Aber IBM schätzt dass es in 4 1/2 Jahren soweit ist:

https://www.afterdawn.com/news/article.cfm/2018/05/22/ibm-all-current-encryption-methods-will-be-broken-instantly-in-5-years-time

Was bleibt sicher?

AES-256 wird erwartungsgemäss ein Sicherheitslevel gegen Quantum Computer Attacken bieten das vergleichbar mit AES-128 gegen Attacken Binärer Computer ist.

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Adiabatische Quantencomputer

Ein quantenmechanisches System, das sich im Grundzustand (Zustand minimaler Energie) eines zeitunabhängigen Systems befindet, bleibt auch bei Veränderungen des Systems im Grundzustand, wenn die Veränderung nur hinreichend langsam (also adiabatisch) passiert.

1) Konstruktion eines Systems mit einem unbekannten Grundzustand, welcher der Lösung eines bestimmten Problems entspricht
2) Konstruktion eines weiteren Systems, dessen Grundzustand leicht experimentell zu präparieren ist
3) Das leicht zu präparierende System wird in das System überführt, an dessen Grundzustand man interessiert ist
4) Dieser Grundzustand wird gemessen
5) Wenn der Übergang langsam genug erfolgt ist, hat man so die Lösung des Problems

D-Wave Systems: https://www.dwavesys.com/

Beispiel einer Problemlösung...

Xenia Bogomolec
indigomind@protonmail.ch

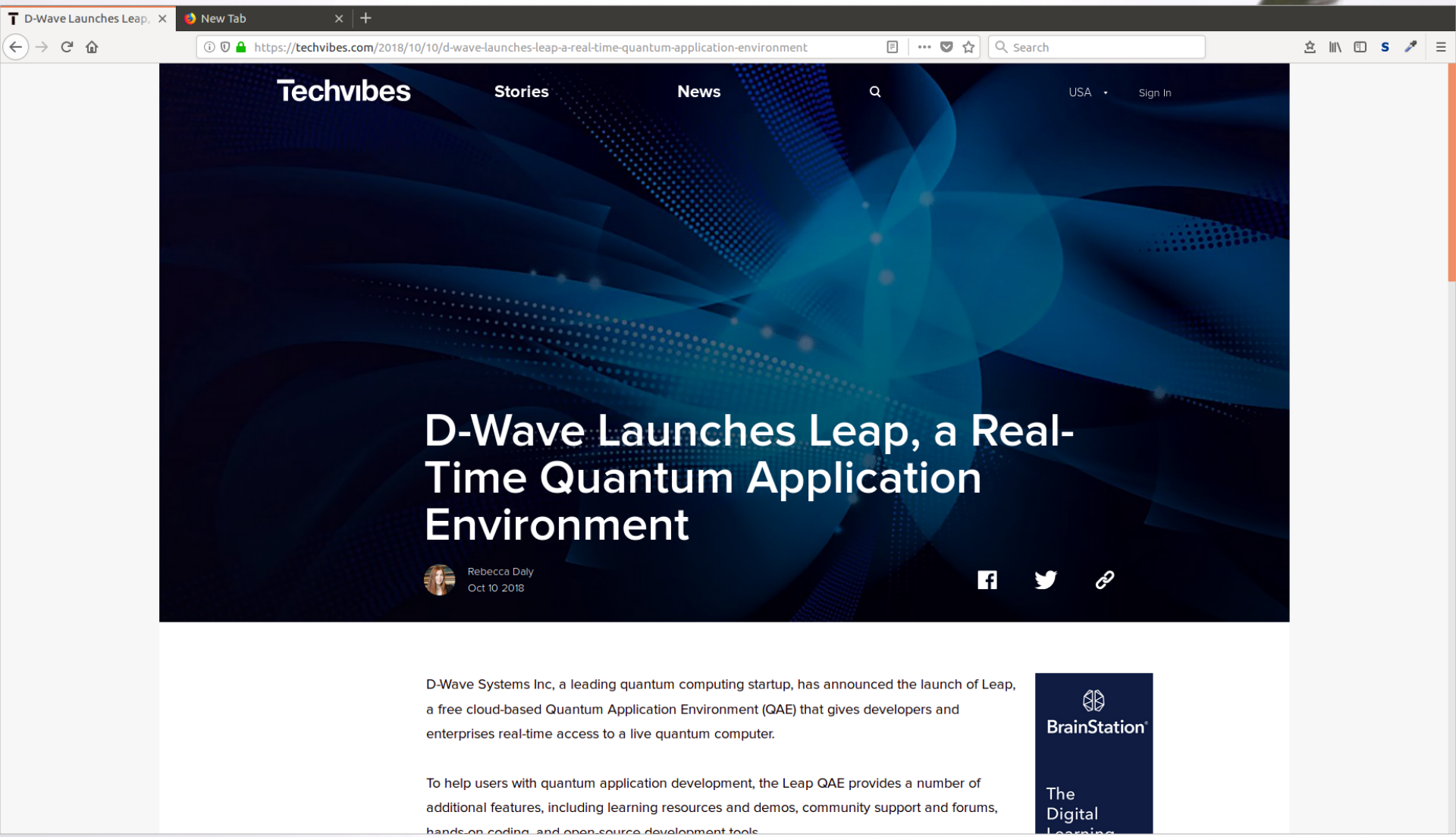
Quanten-Technologien

Adiabatische Quantencomputer | D-Wave Systems Investoren

Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

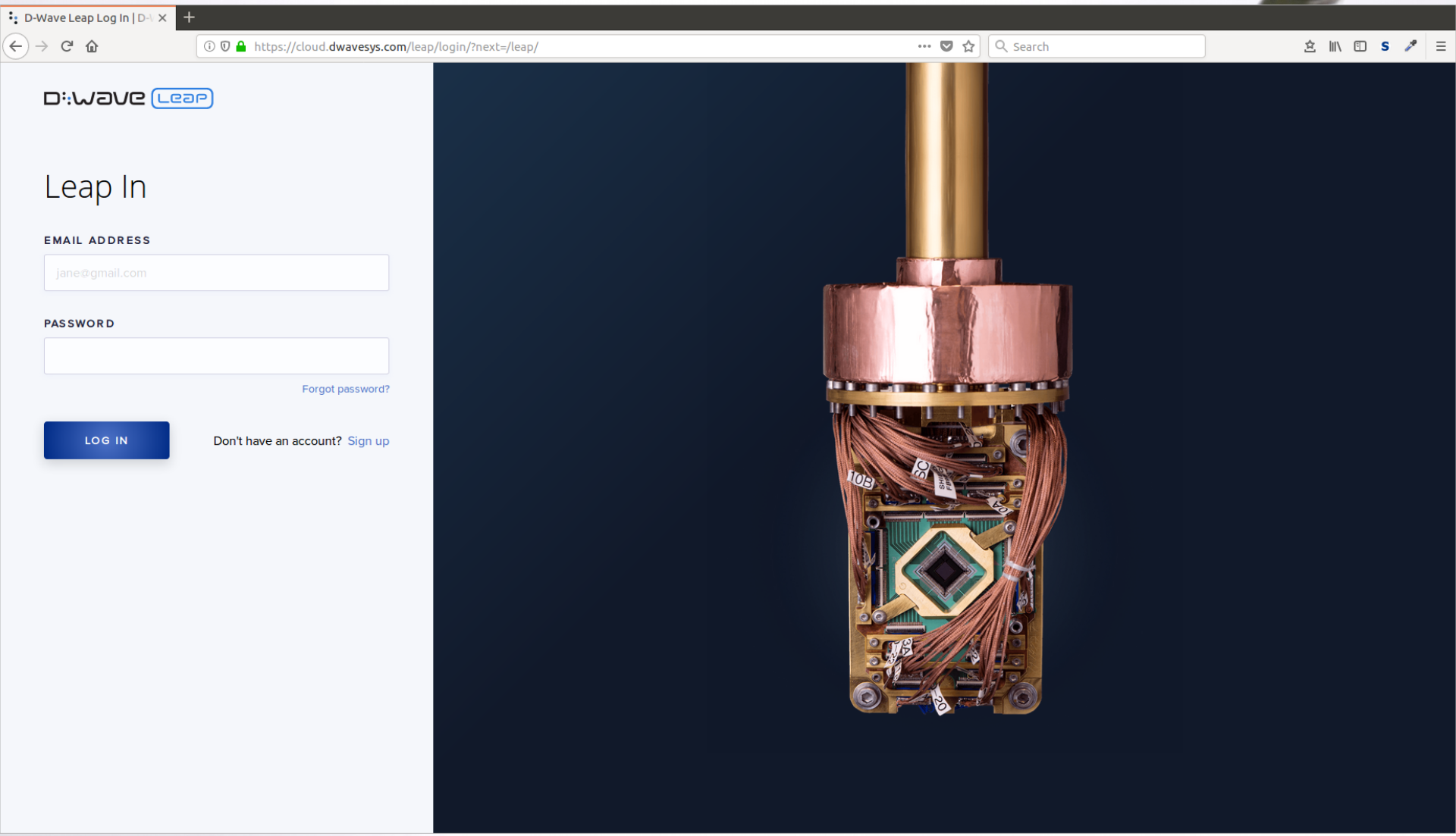
Adiabatische Quantencomputer | Leap



Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

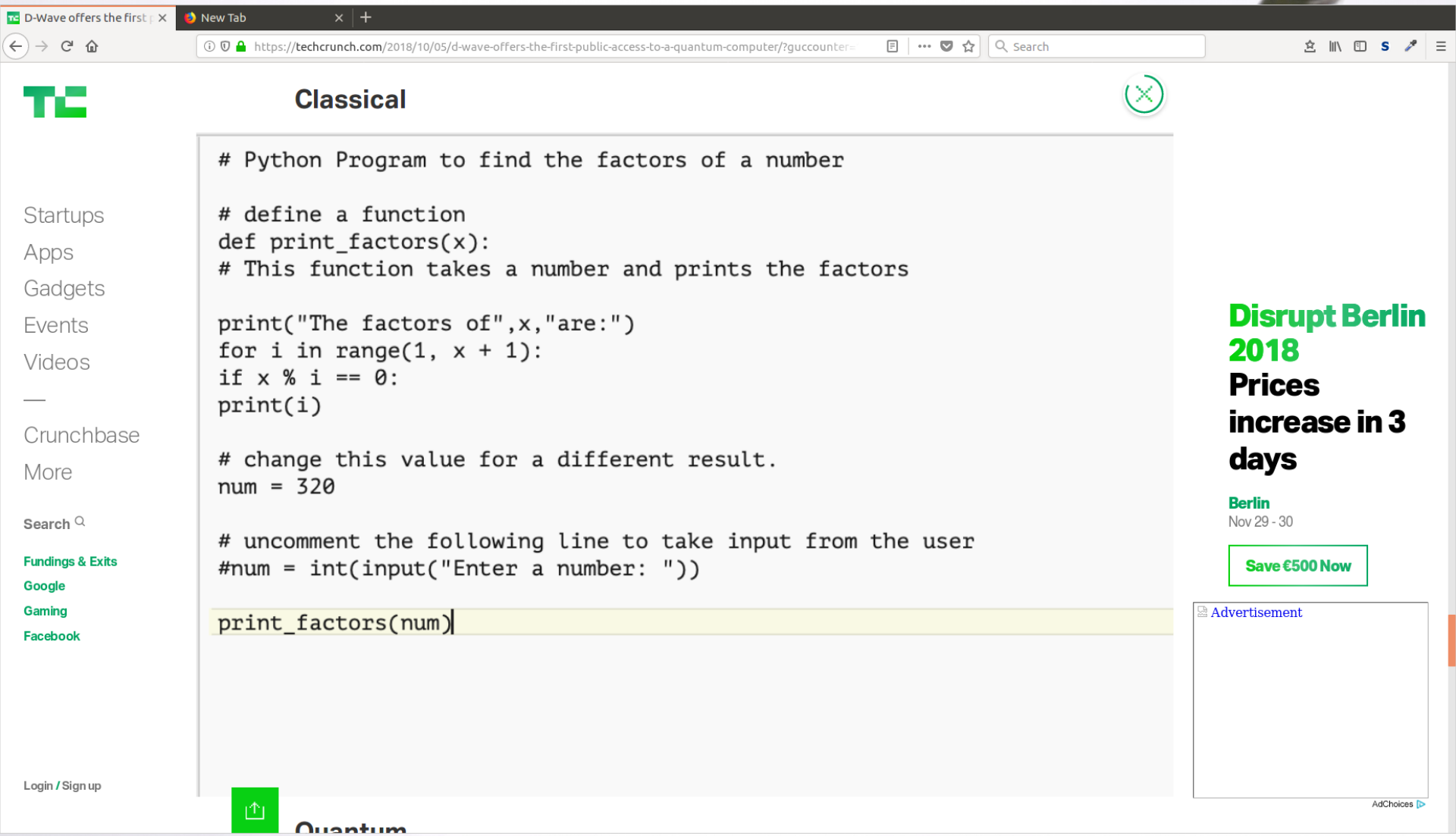
Adiabatische Quantencomputer | Leap



Xenia Bogomolec
indigomind@protonmail.ch

Quanten-Technologien

Adiabatische Quantencomputer | Leap



Xenia Bogomolec
indigomind@protonmail.ch

Quanten Computer

Aktueller offizieller Stand der Entwicklungen

- IBM: 20 qubits QC kommerziell erhältlich seit 2017
- IBM, Google: 50 Qubit Prototyp in 2017
- Google: 72 Qubit Prototyp im März 2018
- D-Wave 2048 Qubits für Quantum Annealing um Optimierungsprobleme zu lösen (seit 2016)
- D-Wave Leap Platform allows developers access to D-Wave 2048 seit Oktober 2018
- Topological Quantum Bits angekündigt in 2017
  (Lösung für Quanten Error Correction Problem)
  https://www.quantum-bits.org/?p=2226

Xenia Bogomolec
indigomind@protonmail.ch

Post-Quanten Verschlüsselungen

Mathematische Lösungen gegen Angriffe durch QC

NIST Standardisierungsprozess für asymmetrische Kryptografie

Kryptografie, deren Sicherheit auf der "Hardness" der Berechnung der Inversen einer Einweg-Funktion beruht.

Bereiche

- Code-Based
- Hash-Based
- Lattice-Based
- Multivariate
- Isogeny-Based

Vorteile gegenüber QKD

- Reine Software Updates
- Effektive Performance auf Smart Phones, Desktops and IoTs

Überblick zu Entwicklungen

https://arxiv.org/abs/1809.00371
(Kooperation mit Dr. Jochen Gerhard von Bearingpoint)

Xenia Bogomolec
indigomind@protonmail.ch

Vergleich

Ersatz für bis 40 Jahre alten Algorithmen

Quantum Key Distribution

Schlüsselaustausch basierend auf Quantenmechanischen Effekten

- Teure neue hardware (ID Quantique)
- Bisher nur für kurze Distanzen (300-1200km in 2017)
- Keine integrierte Message Authentifizierung, MIM möglich wenn nicht zusätzlich implementiert

QUESS: 2000km quantum communication network between Shanghai and Bejing

SwissQuantum

SECQC Austria

Tokyo QDK Network

DARPA USA

Post-Quanten Kryptographie

Alternative Algorithmen für Schlüsselaustausch basierend auf der Hardness von anderem mathematischen Problemen als Primzahlfaktorisierung

- NIST Standardisierungsprozes läuft (2017-2021)
- Manche wurden schon jahrelang genutzt und nicht gebrochen
- Laufen effektiv auf aktuellen Geräten
- Reine Software Updates

Isara USA

KPN in Netherlands

Infineon

Microsofts experimental VPNs with algorithms that haven't been exposed publicly

Einige Beispiele etablierter Lösungen

Xenia Bogomolec
indigomind@protonmail.ch

Nützliche Links

- https://hpcwire.com/2018/10/29/europe-launches-ten-year-e1b-quantum-flagship-project/
- https://twitter.com/quantumflagship?lang=de
- https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/fetflag-03-2018.html
- https://quantumfrontiers.com/2017/08/16/topological-qubits-arriving-in-2018/amp/
- https://pqcrypto.org
- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
- http://latticehacks.cr.yp.to/

Chinas Quantum Communication Network besteht aus drei Teilen:

- Quantum Communication (Schlüsselaustausch per Satellit QUESS)
- Traditional Network (Glasfaser?)
- Management System

Auch interessant:

Wassenaar Abkommen für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien: https://www.wassenaar.org

Xenia Bogomolec
indigomind@protonmail.ch