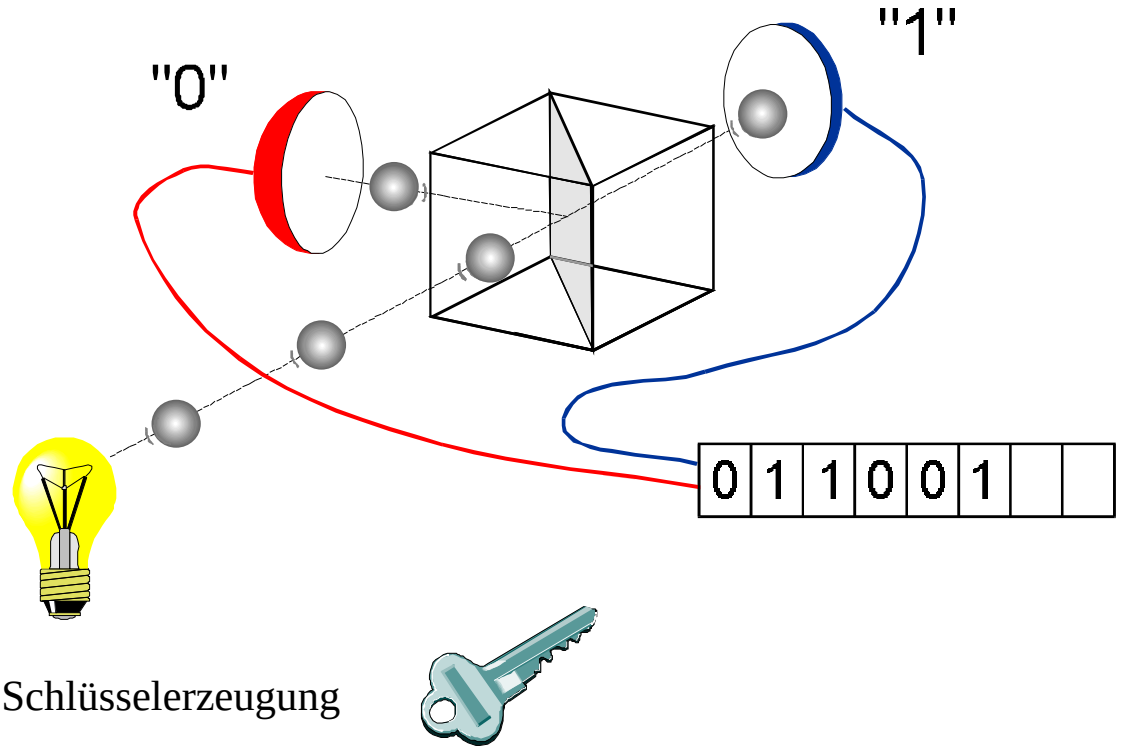
Wie kann die Quantenkryptographie zur Cyber-Sicherheit beitragen?

Nicolas Gisin, Hugo Zbinden
Mikael Afzelius und Rob Thew
GAP-Optique, Universität Genf

- **Das Zeitalter der Quantentechnologie hat begonnen!**
- **Quanten-Zufallszahlengeneratoren**
- **Quantencomputer und die Notwendigkeit eines Wechsels zur Quantenkryptographie**
- **Quantenschlüsselaustausch existiert bereits**
- **Was getan werden muss**

GAP Quantique

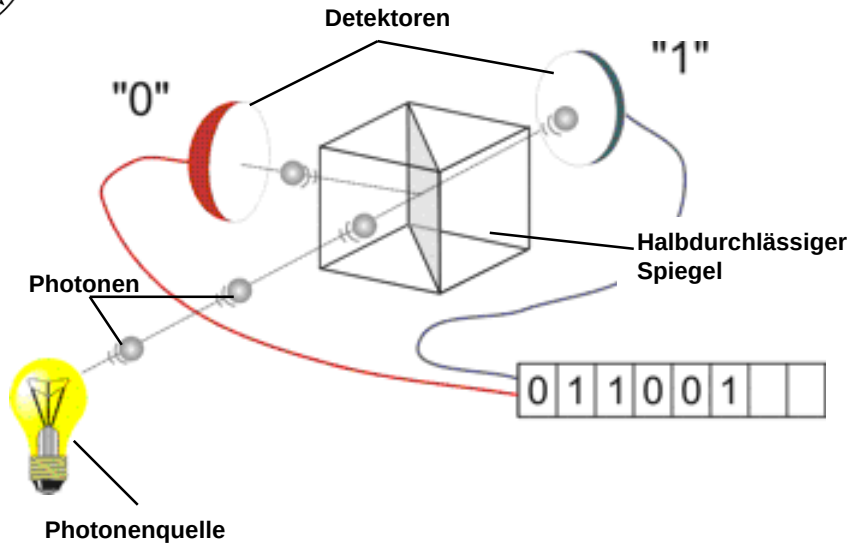
Physik eines Strahlteilers

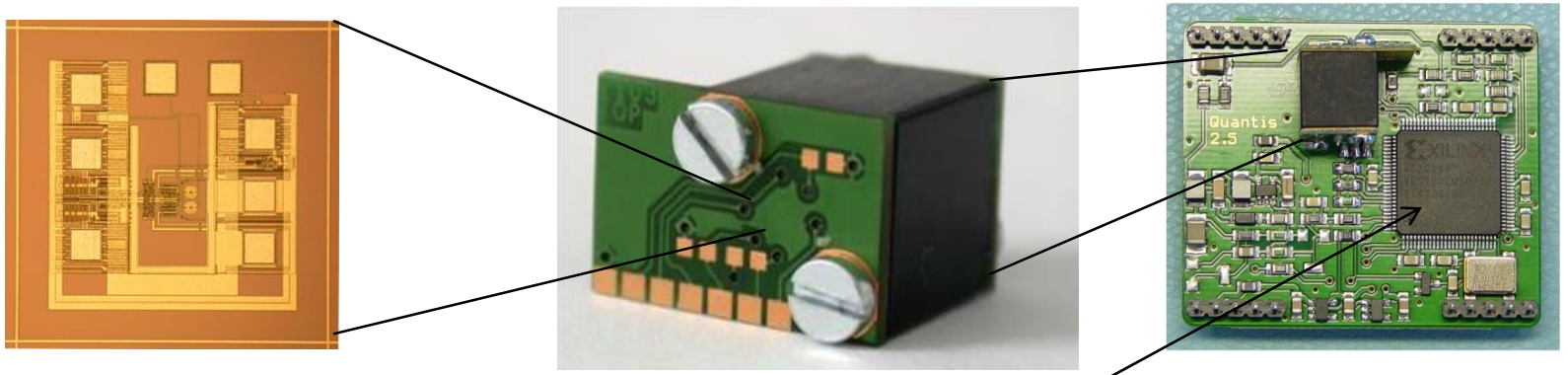


Schlüsselerzeugung

- Eine konzeptionell einfache Entropiequelle
- Nur in der Quantenphysik gibt es den fundamentalen Zufall
- Ursprung des Zufalls lässt sich einfach festlegen
- Ein praktischer Zufallszahlengenerator

Quanten-Zufallszahlengenerator





4 Mbit/s gleichverteilte Zufallszahlen

GAP Quantique

Evaluation und Zertifizierung

Nichtdeterministischer (physikalischer) RNG (Zufallsgenerator)

Bundesamt für Sicherheit in der Informationstechnik

- PTG.1

Physikalischer RNG mit internen Tests, die eine Gesamtentropiequellenstörung und nicht tolerierbare statistische Mängel der internen Zufallszahlen erfassen

- PTG.2

PTG.1, ergänzt durch ein stochastisches Modell der Entropiequelle und statistische Tests der Rohzufallsdaten

- PTG.3

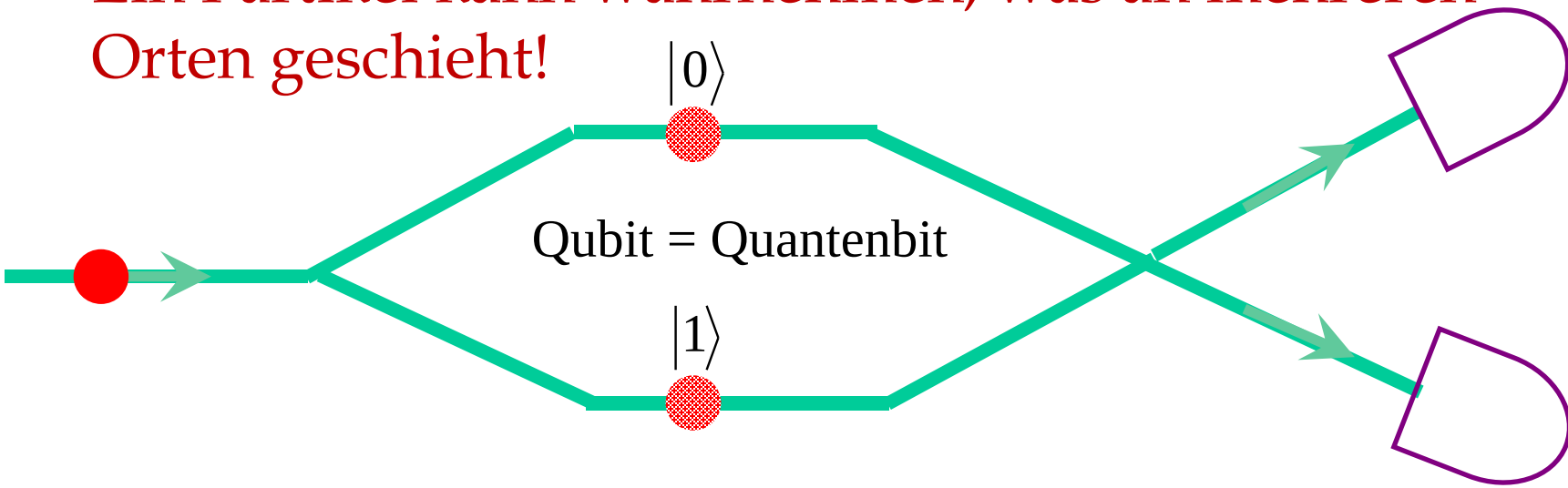
PTG.2, ergänzt durch eine krypto-graphische Nachbearbeitung (hybrider PTRNG)

GAP Quantique

Quantenmechanik

(Alle physikalische Grundlagen, die Sie kennen müssen.)

- Ein Partikel kann wahrnehmen, was an mehreren Orten geschieht!



- Ebenso möglich ist $|0\rangle+|1\rangle+|2\rangle+|3\rangle+\ldots+|n\rangle$
- 100 Qubits könnten alle Partikel im gesamten Universum nummerieren!
- Jede Messung ergibt nur ein Ergebnis.

GAP Quantique

Quantencomputing

- Informationen verarbeiten: Input x $\Rightarrow$ Output fct(x)
- Quantencomputer:
  Quantenverarbeitung einer herkömmlichen Dateneingabe:

$$|0\rangle + |1\rangle + |2\rangle + \ldots + |n\rangle \Rightarrow |fct(0)\rangle + |fct(1)\rangle + |fct(2)\rangle + \ldots + |fct(n)\rangle$$

- Eine Messung kann nur ein Ergebnis ergeben.
- Dieses eine Ergebnis kann Informationen zu einer globalen Eigenschaft der Funktion *fct* liefern.
- Zum Beispiel Maximalwert, Mittelwert oder Informationen zur Periodizität der Funktion.

GAP Quantique

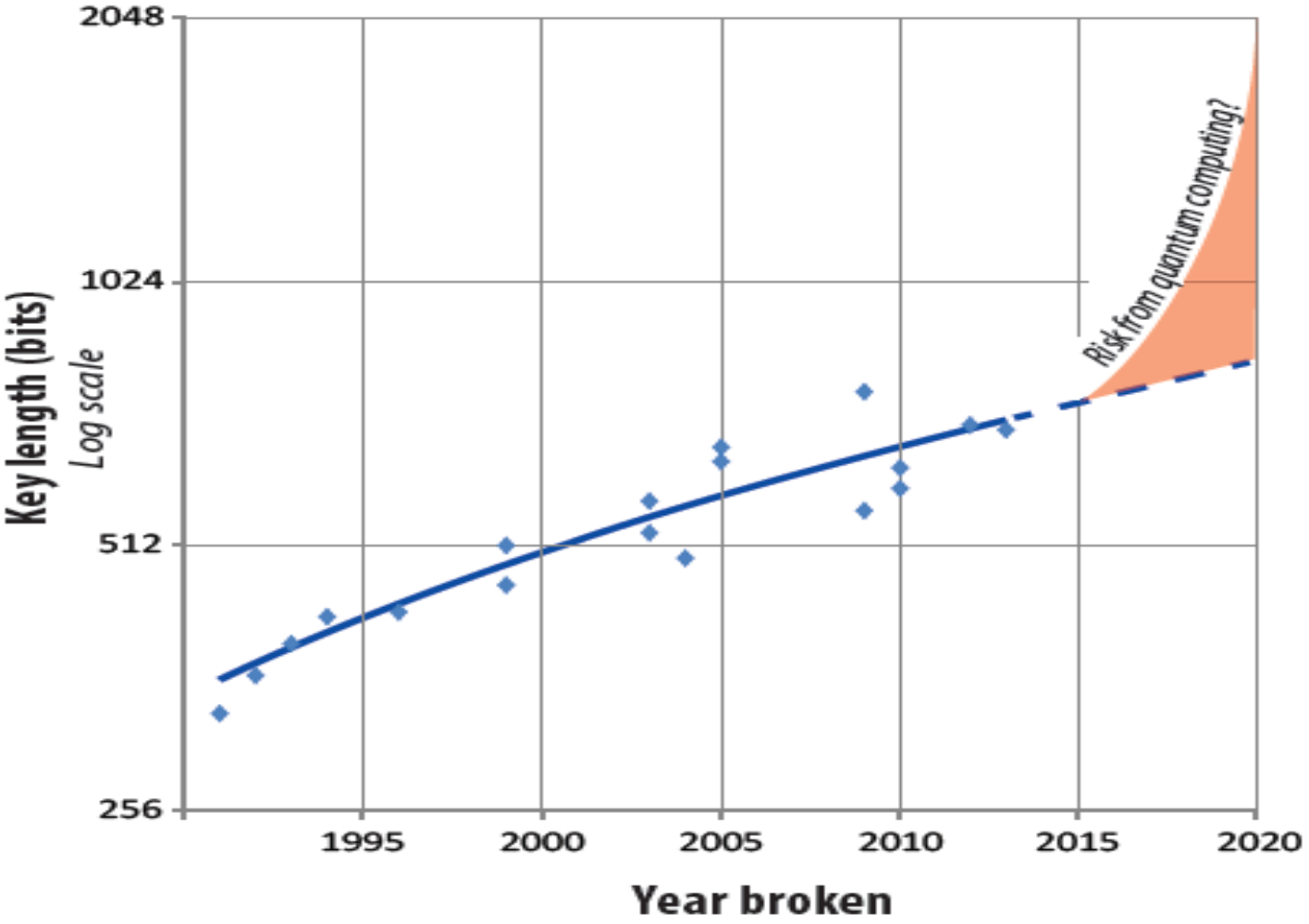
Fakt

- Periode einer Funktion + ein wenig Zahlentheorie ⇒ So können alle heutigen Public-Key-Kryptosysteme geknackt werden.
- D.h. alle verschlüsselten Nachrichten können entziffert werden.

- Ein Quantencomputer wird die heutigen Public-Key-Kryptosysteme daher obsolet machen.

GAP Quantique

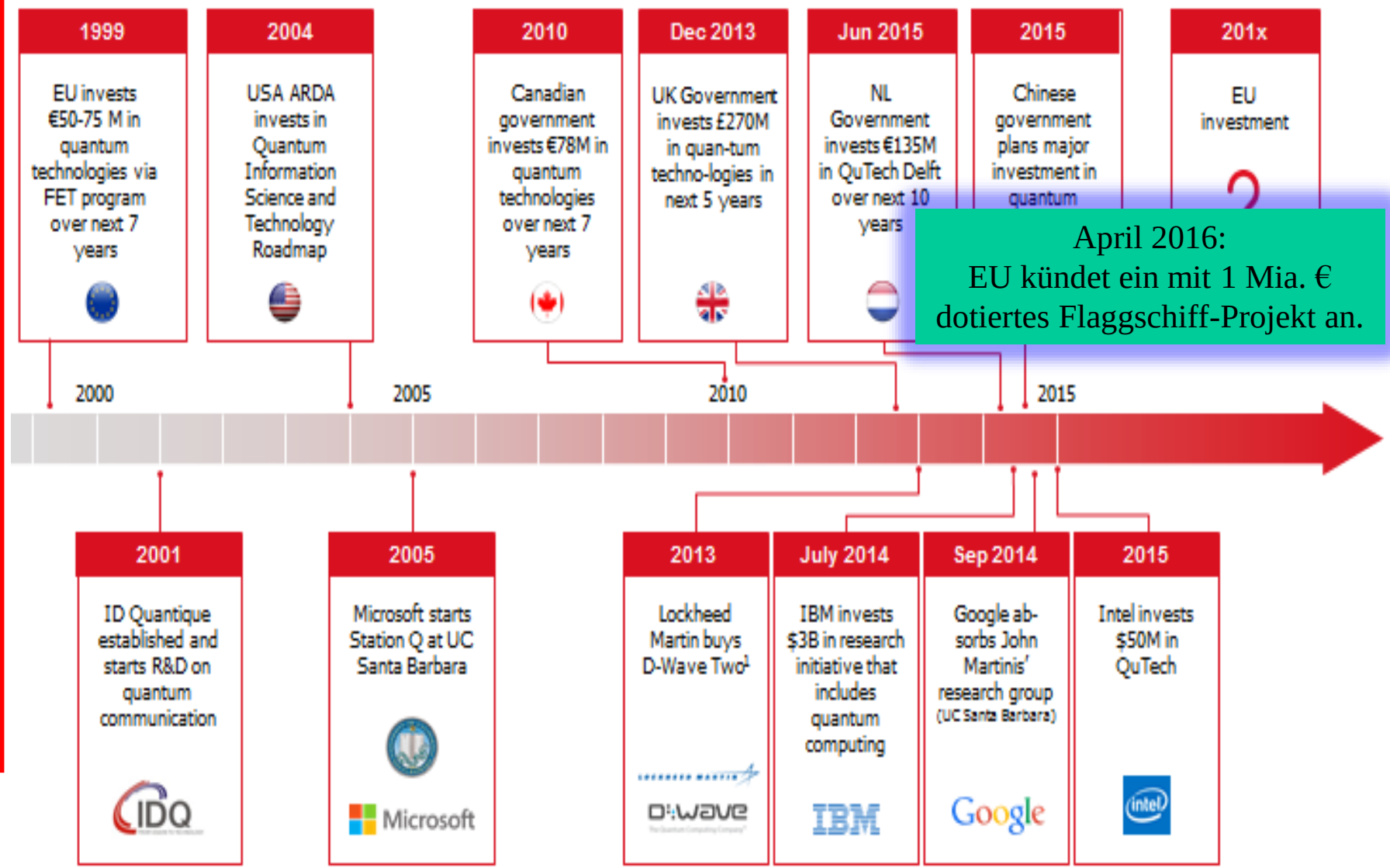
Auswirkungen von Quantencomputern auf RSA



https://downloads.cloudsecurityalliance.org/initiatives/qss/What_is_Quantum_Safe_Security_position_paper.pdf

GAP Quantique

Wann werden wir über Quantencomputer verfügen?



GAP Quantique

Veränderung der Technologien

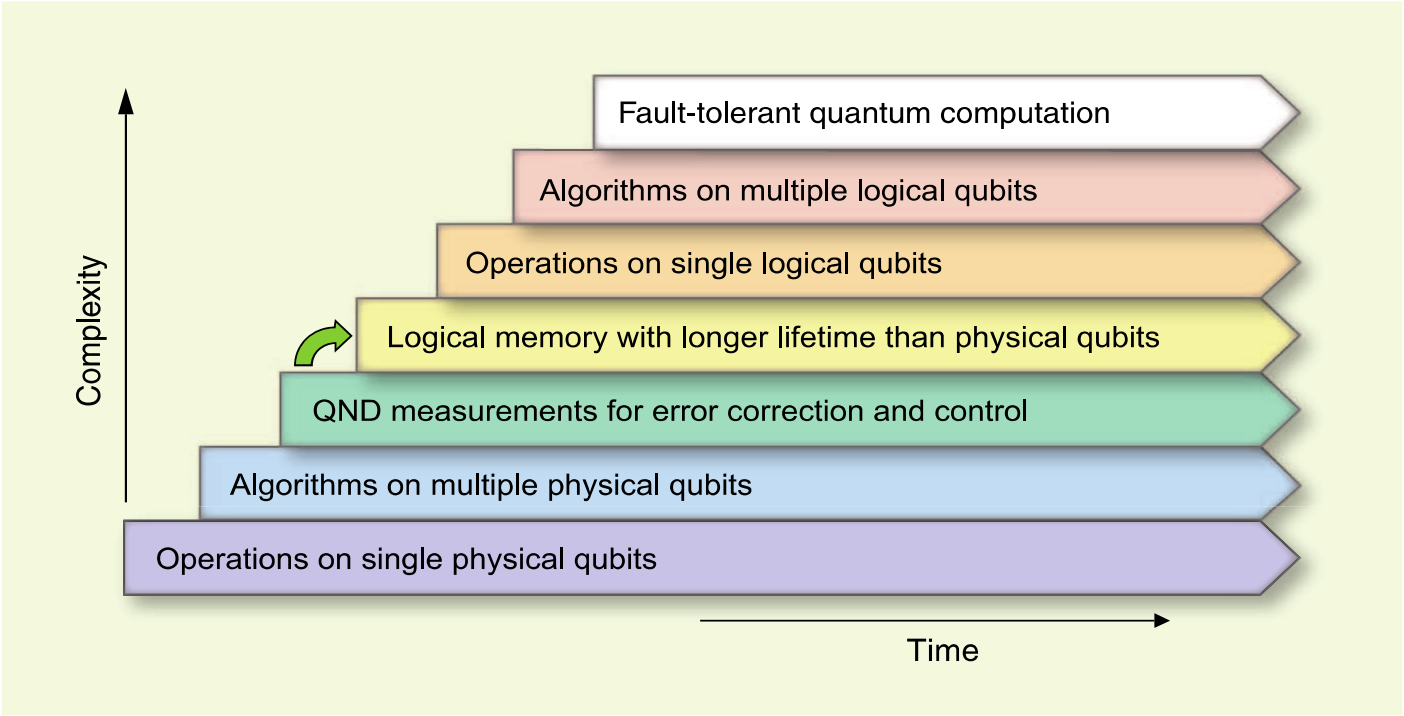


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

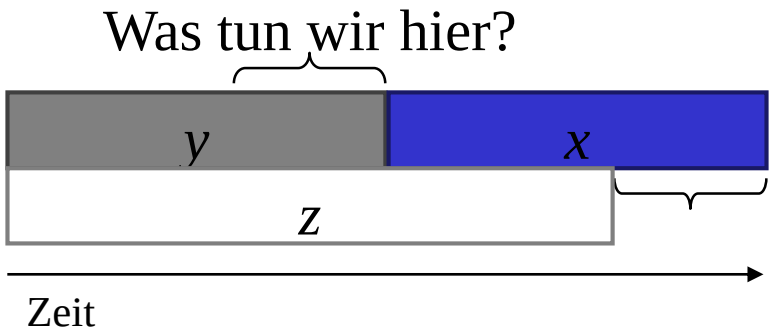
Veränderung der Wahrnehmung

Wie bald müssen wir uns Sorgen machen?

Abhängig von folgenden Faktoren:

- Wie lange muss die Verschlüsselung sicher sein? (x Jahre)
- Wie lange wird es dauern, um die bestehenden Infrastrukturen mit einer umfassenden quanten-kryptografischen Lösung neu auszurüsten? (y Jahre)
- Wie lange wird es dauern, bis ein grosser Quanten-computer gebaut wird (oder andere entsprechende Fortschritte erzielt werden)? (z Jahre)

Theorem 1: Wenn $x + y > z$, dann muss man sich Sorgen machen.



GAP Quantique

Quantenkryptographie

- Post-Quanten-Kryptographie
  = *auf Komplexität basierende klassische Algorithmen, resistent gegen bekannte Quantenangriffe*

+ keine grosser Veränderung für Sicherheitsfachleute
- eine Art «Schuss ins Blaue»
- gefährdete Backward Security

- Quantenschlüsselaustausch (QKD)
  = *physikbasiert, erwiesener-massen resistent gegen Quantenangriffe*

+ nachweisbare Sicherheit
+ Backward Security
- teuer
- grosse Veränderung bezüglich Infrastruktur und Mentalität

- Wahrscheinlich werden beide Verfahren ihre Anwendungs-bereiche finden; entscheidend ist die Frage nach der Grösse des jeweiligen Marktes.
- Beide erfordern echte Zufallsbits.

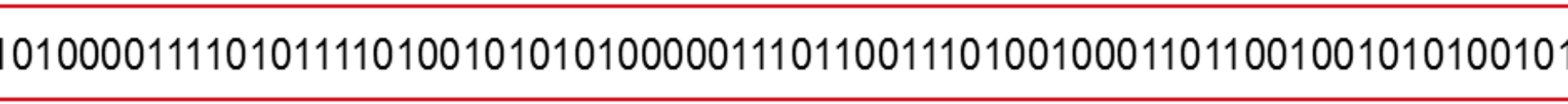
Beispiel Quantenkryptographie

OSI Model

Application	⟷	Application
Presentation	⟷	Presentation
Session	⟷	Session
Transport	⟷	Transport
Network	⟷	Network
DataLink	⟷	DataLink
Physical	⟷	Physical

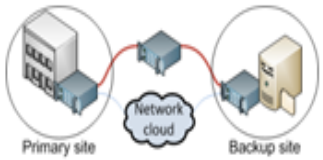
Use Quantum Resistant algorithms here

Use QKD here

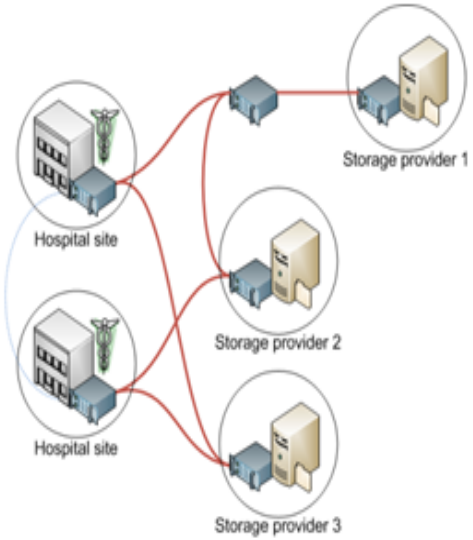


Beispiele von Anwendungsfällen

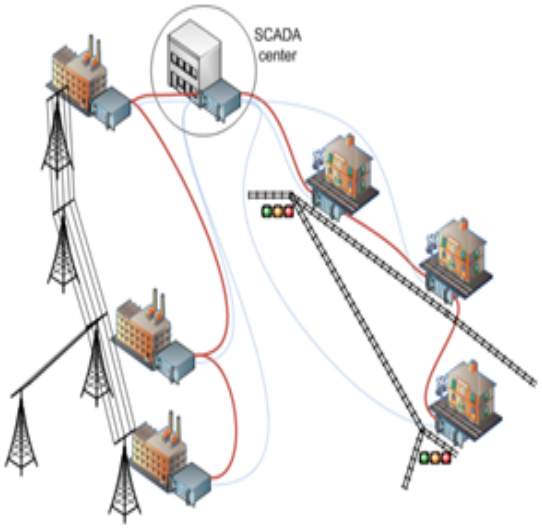
Off-site backup



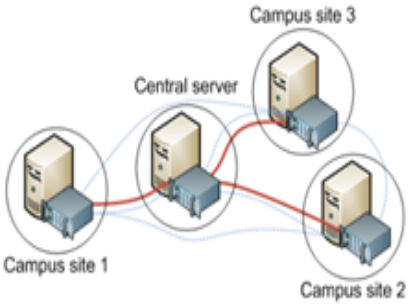
High security cloud storage



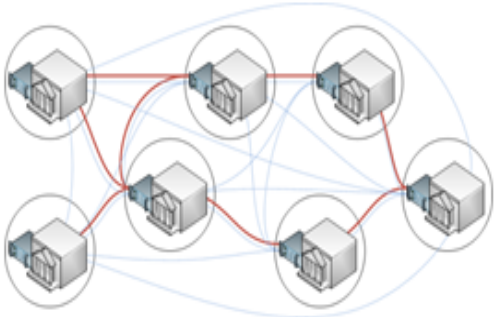
Critical infrastructure protection



Key and signature server



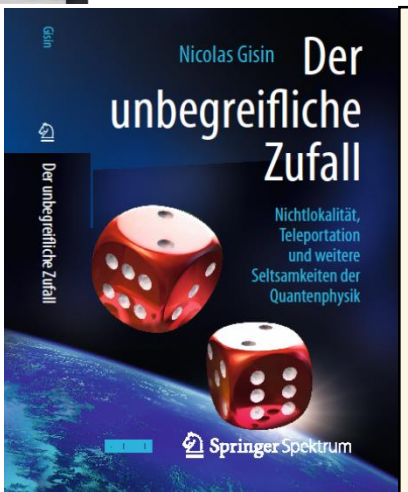
High security private networks

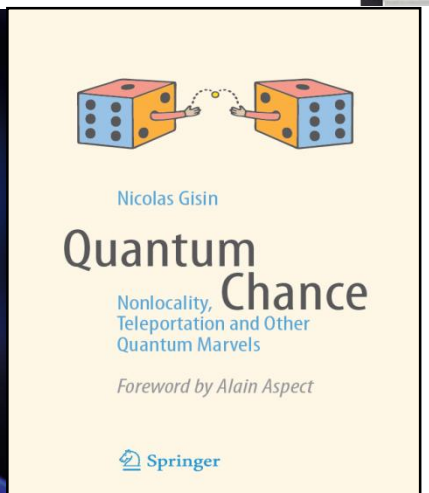


Backbone link protection

In der Natur gibt es den echten lokalen & nichtlokalen geheimen Zufall.

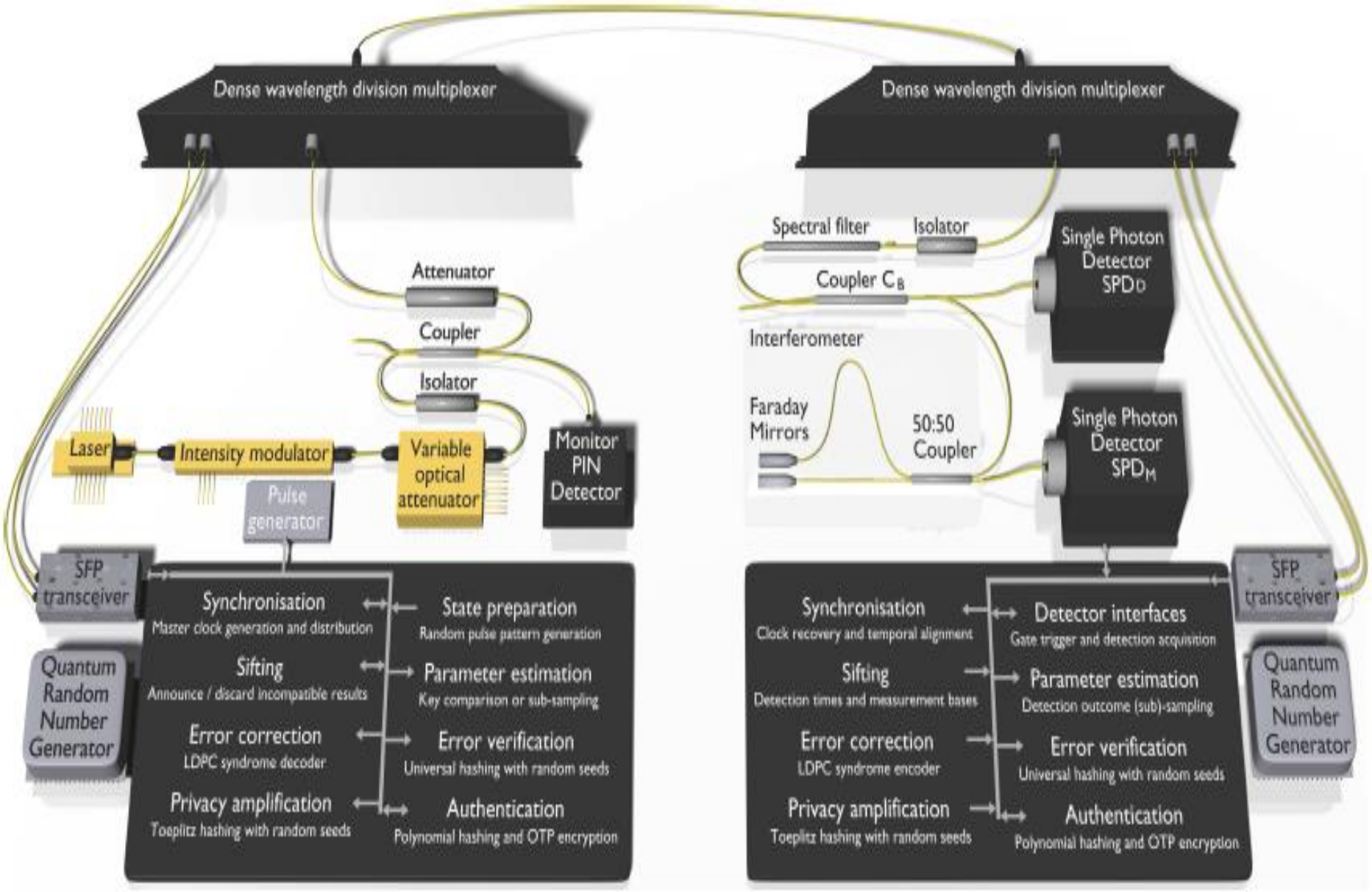
- Nehmen wir an, dass Distanzen tatsächlich existieren.
- Nehmen wir an, dass Alice & Bob sicherstellen können, dass keine Informationen an die Aussenwelt durchsickern.
- Nehmen wir an, dass $a \oplus b = x \cdot y$ mit hoher Wahrscheinlichkeit zutrifft. (Zu beachten: Das kann überprüft werden.)





GAP Quantique

QKD-System @ 625 MHz



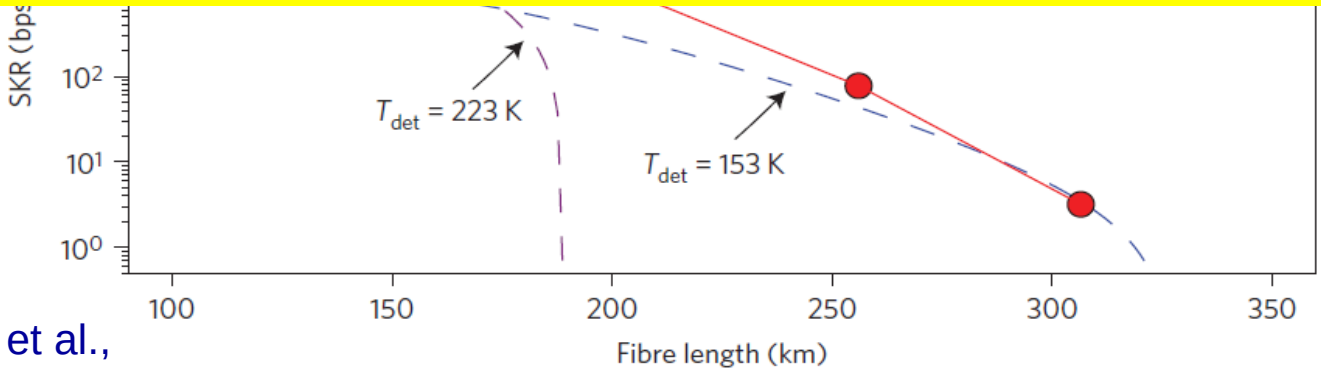
Integriertes QKD-System

- Aufgebaut auf der Advanced Telecommunication Computing Architecture (ATCA).
- Bietet standardisierte mechanische Schnittstellen sowie Stromversorgungs- und Datenschnitt-stellen.
- Umfasst Netzwerk-dienstleistungen, Kühlung, Netzteile.
- Skalierbare Architektur, ist potenziellen Kunden vertraut.

GAP Quantique

QKD über 307 km mit Echtzeit-Erzeugung von geheimen Schlüsseln und Sicherheitsanalyse solcher Verfahren

- Integration in ATCA-Blades
- Ein Modell eines QKD-Systems, das 1 Gb/s nachweisbar geheime Bits produziert, ist absehbar.



B. Korzh, C. W. Lim et al.,
Nature Photonics
9, 163-168 (2015)

GAP Quantique

Beispiel einer kommerziellen Verbindung, die seit 2011 ununterbrochen besteht

Lausanne

Nyon

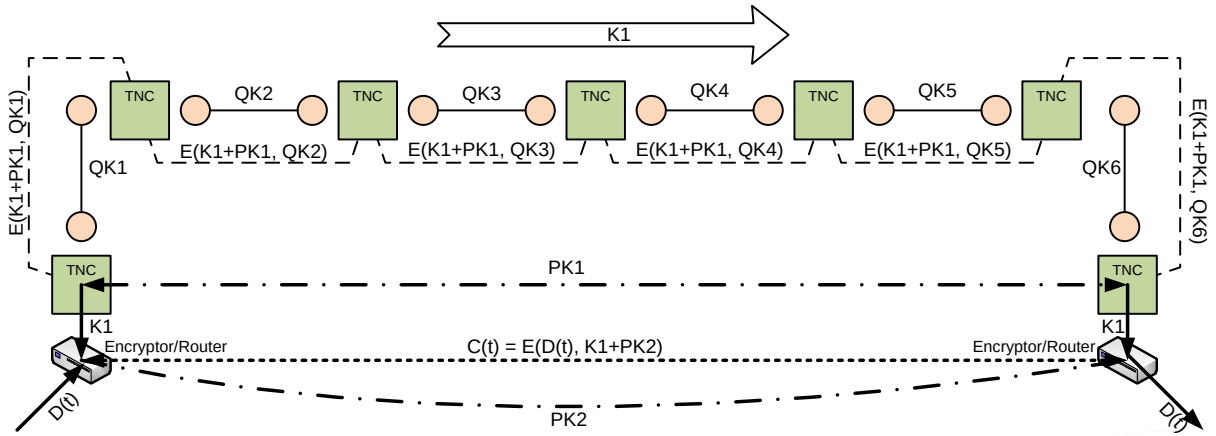
67 km

Gemultiplexter Quantenkanal für kommerzielle Nutzer.

Genève

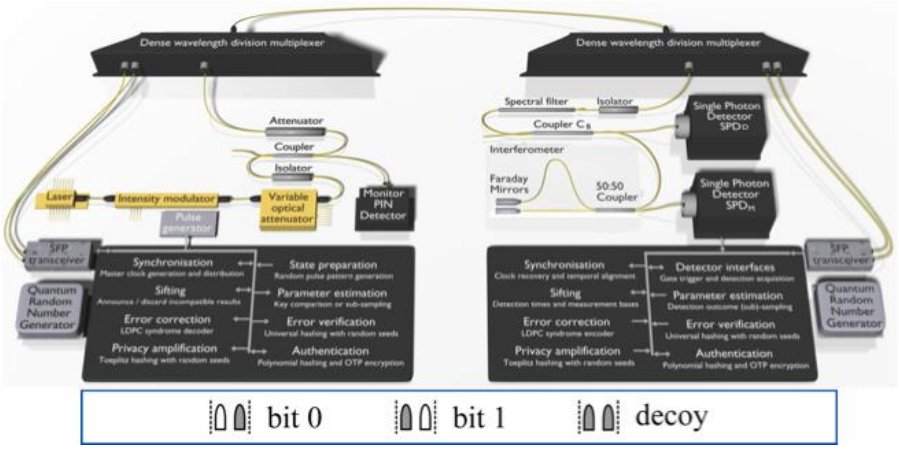
GAP Quantique

QKD Vertrauenswürdiger Knoten



Schlüssel bewegen sich sicher Schritt um Schritt durch das Netzwerk.

COW(Coherent One-Way)-Protokoll



Telecom-kompatible Architektur (ATCA), bis zu 8 Quanten-Blades pro Chassis

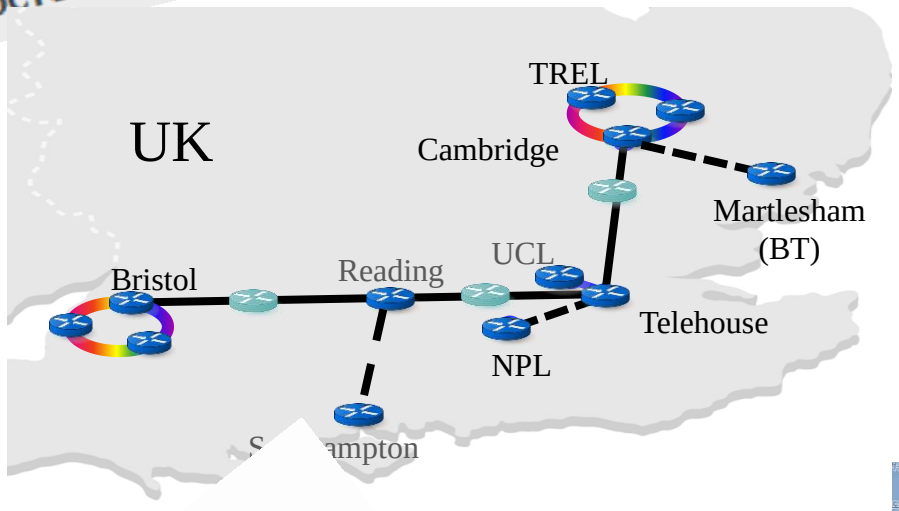
FIPS 140-2-Zertifizierung (geplant)
CC-Evaluation (geplant)

GAP Quantique

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

ADD THIS TO MY CALENDAR

5-7 OCTOBER 2015



Quantique

Battelle

The Business of Innovation

Was erreicht QKD

1. Angriffe müssen vor Ort lanciert werden
   ⇒ immun gegen zukünftige Fortschritte
2. Nur unter der Annahme einer korrekten Umsetzung
   ⇒ Schlüsselexpansion
3. Ausgehend von kurzfristig sicherer Einweg-Funktion
   ⇒ Verteilung von kryptographischen Schlüsseln mit langfristiger Sicherheit

I. QKD mit Einmalverschlüsselung (limitiert durch Übertragungsrate der QKD)
   ⇒ ermöglicht eine langfristige informationstheoretische Sicherheit

II. QKD ermöglicht einen sehr häufigen Wechsel des Seed Keys (Startwerts) des Advanced Encryption Standards (AES)
   ⇒ limitierte Daten für die Kryptoanalyse und limitierte Motivation für einen Gegner

GAP Quantique

Was noch getan werden muss

- Heute arbeiten Physiker und Kryptographen nicht zusammen.

➔ Eine Gemeinschaft von Physikern und Kryptographen bilden, die gemeinsam an der Quantenkryptographie arbeiten.

➔ Herausfinden, wo Post-Quanten-Algorithmen sinnvoll sind, z.B. Mobiltelefonie, Anwendungen in öffentlichen Bereichen, fast im ganzen E-Commerce usw.

➔ Herausfinden, wo Quantenkryptographie (QRNG & QKD) sinnvoll ist, z.B. **Schweizer Quanten-Datenübertragungs-leitung** für kritische Infrastrukturen und umfassende aggregierte Daten.

GAP Quantique

Was noch getan werden muss

- Heute arbeiten Physiker und Kryptographen nicht zusammen.

➔ Eine Gemeinschaft von Physikern und Kryptographen bilden, die gemeinsam an der Quantenkryptographie arbeiten.

➔ Herausfinden, wo Post-Quanten-Algorithmen sinnvoll sind, z.B. Mobiltelefonie, Anwendungen in öffentlichen Bereichen, fast im ganzen E-Commerce usw.

➔ Herausfinden, wo QKD sinnvoll ist, z.B.

Schweizer Quanten-Datenübertragungs-leitung für kritische Infrastrukturen und umfassende aggregierte Daten.

GAP Quantique