Quantenkryptographie

Vortrag im Rahmen des Seminars
„Grundlagen der Quantenmechanik“

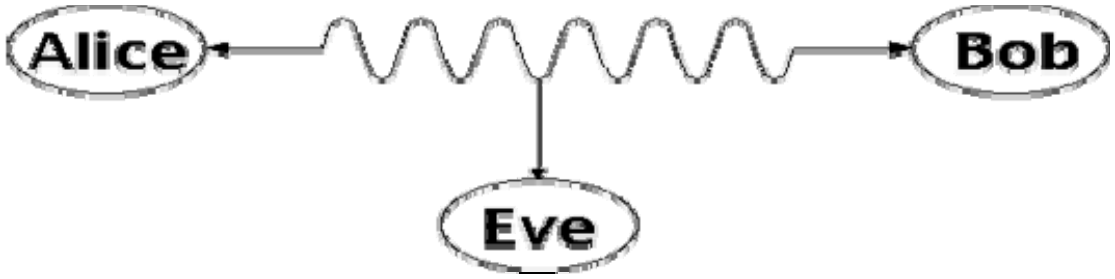
Jan Sprung

7. Januar 2009

Gliederung

- Was ist Quantenkryptographie?
- Warum ist Quantenkryptographie sicher?
- Funktionsweise
- Experimenteller Aufbau
- Technische Herausforderungen
- Stand der Technik
- Zusammenfassung

Was ist Quantenkryptographie?



- Quantum Key Distribution = abhörsichere Übertragung eines Kodierungsschlüssels
- Sicherer als asymmetrische Kodierung

  (Primfaktorzerlegung)
- Noch ungelöst:

  sichere Authentifikation sowie Übertragung trotz Abhörens

Warum ist Quantenkryptographie sicher?

- Abhörsicherheit wegen der Grundpostulate der Quantenmechanik
  1. Messprozess beeinflusst Messgröße
  2. No-cloning-Theorem

- No-cloning-Theorem

  sei U unitär mit

$$U\left(|\psi\rangle|\alpha\rangle\right)=|\psi\rangle|\psi\rangle \qquad U\left(|\varphi\rangle|\alpha\rangle\right)=|\varphi\rangle|\varphi\rangle$$

  dann folgt

$$\langle\psi\alpha|U^{+}U|\varphi\alpha\rangle=\langle\psi|\varphi\rangle\overset{!}{=}\left(\langle\psi|\varphi\rangle\right)^{2}$$

  und somit

$$|\psi\rangle=|\varphi\rangle \quad \text{oder} \quad |\psi\rangle\perp|\varphi\rangle$$

  Klonen nur bei bekannter Basis möglich!

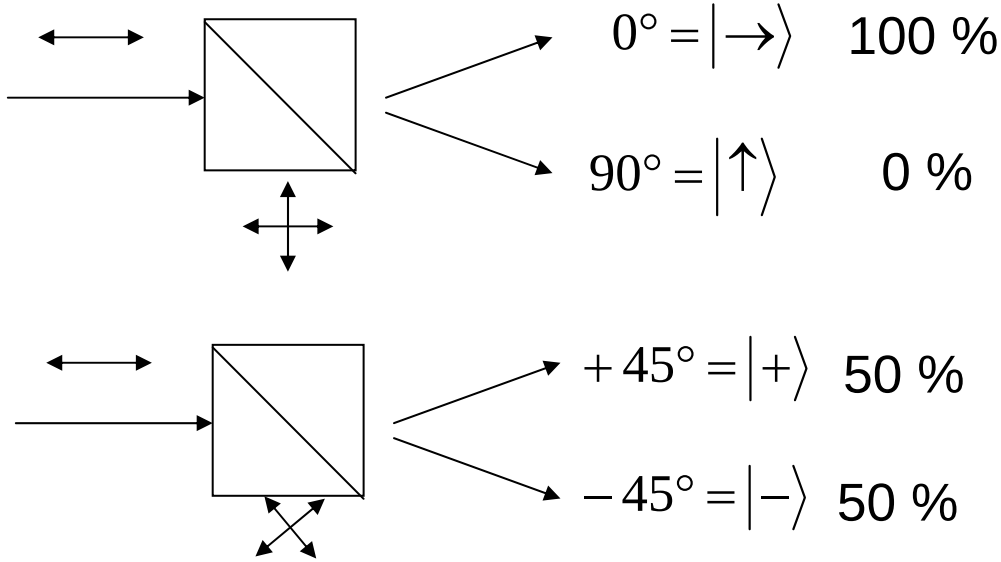
Funktionsweise am Beispiel BB84 (1)

- Vier Polarisationszustände eines Photons:

$$0° = \left|\rightarrow\right\rangle \mathrel{\hat{=}} 1 \quad +45° = \left|+\right\rangle \mathrel{\hat{=}} 1$$

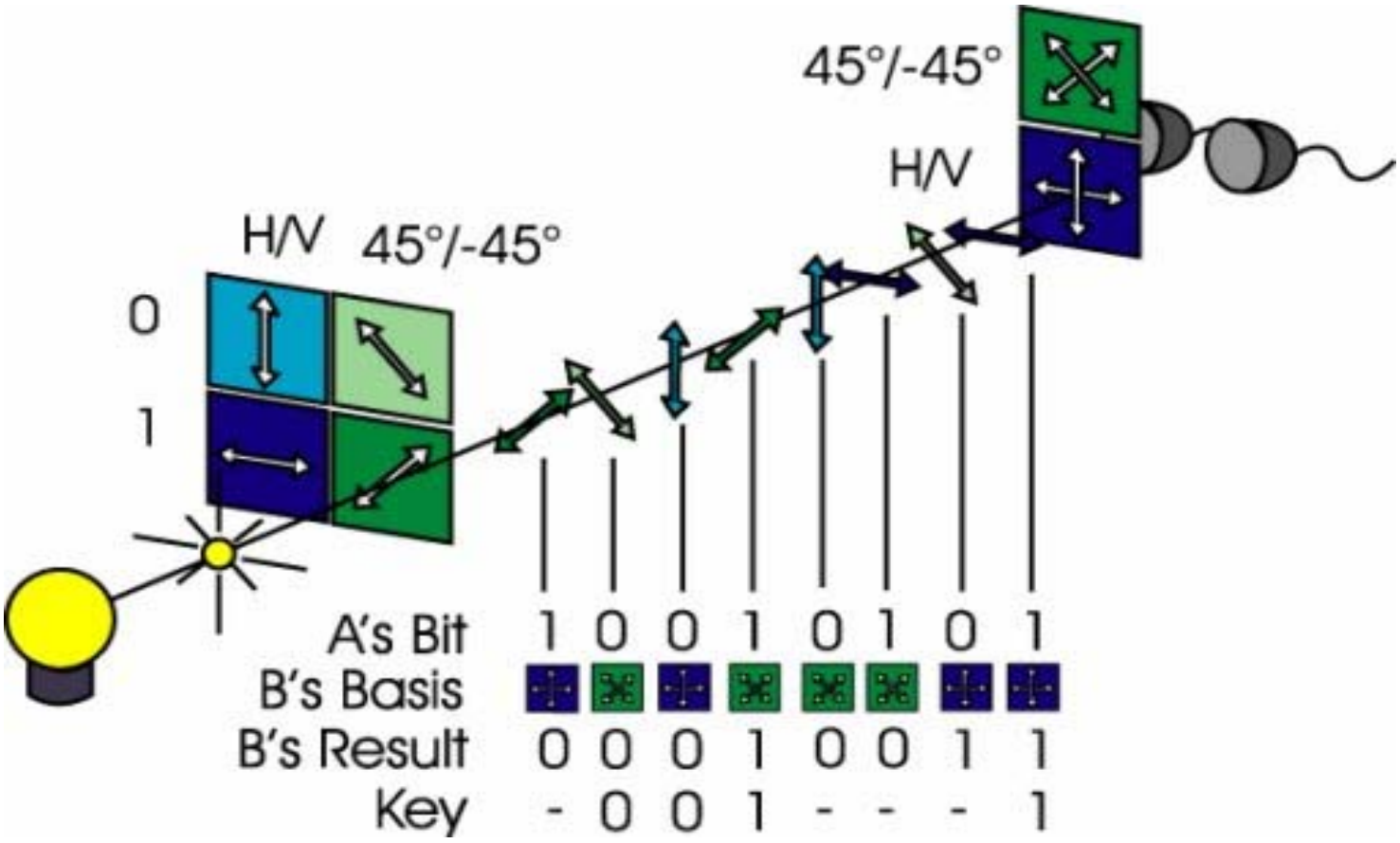
$$90° = \left|\uparrow\right\rangle \mathrel{\hat{=}} 0 \quad -45° = \left|-\right\rangle \mathrel{\hat{=}} 0$$

- Messung:



Bennett, C.H. and G. Brassard, 1984, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York), pp 175-179

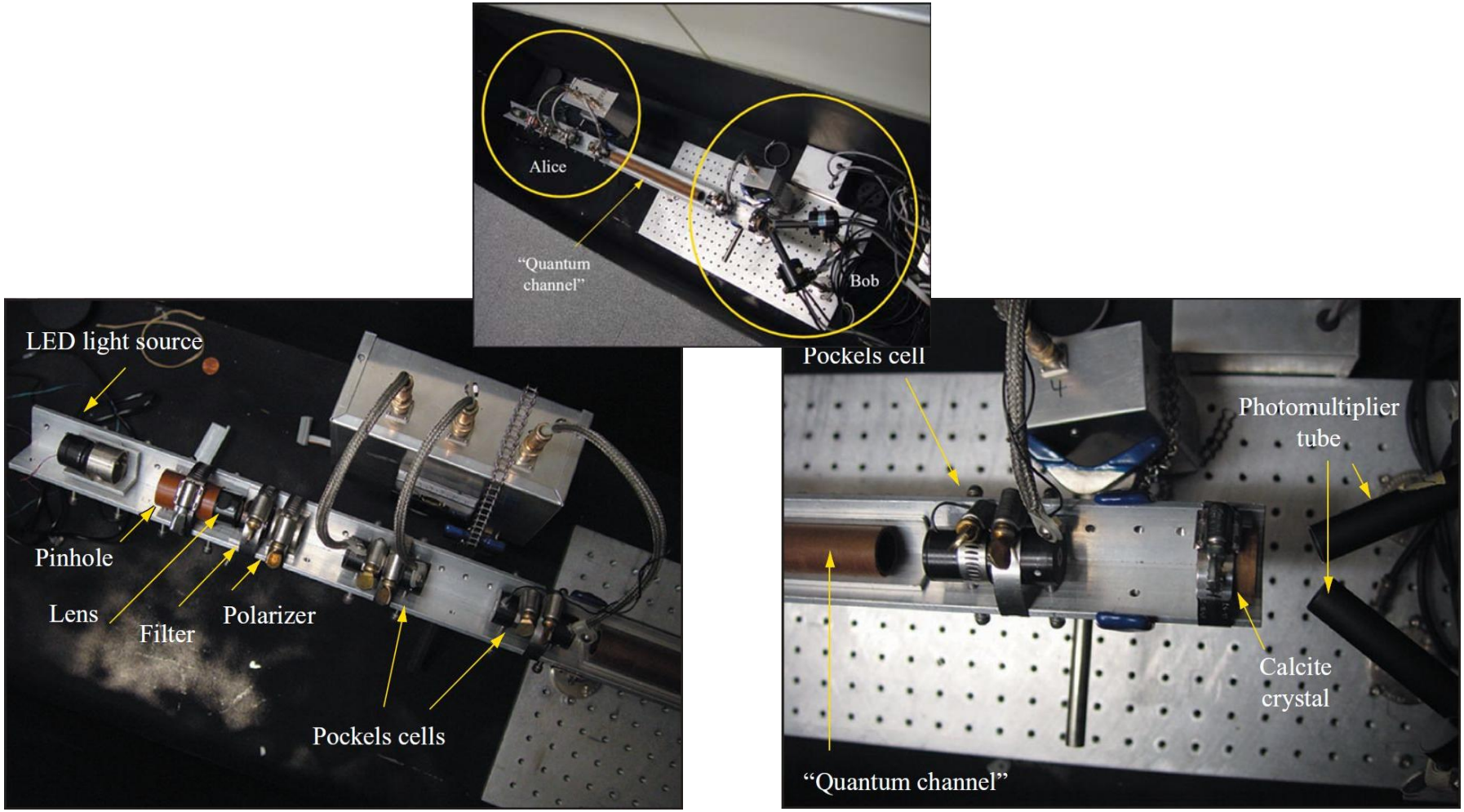
Funktionsweise am Beispiel BB84 (2)



http://www.whitehat.ch/cissp/krypto/Kryptographie-Dateien/image001.png

Bennett, C.H. and G. Brassard, 1984, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York), pp 175-179

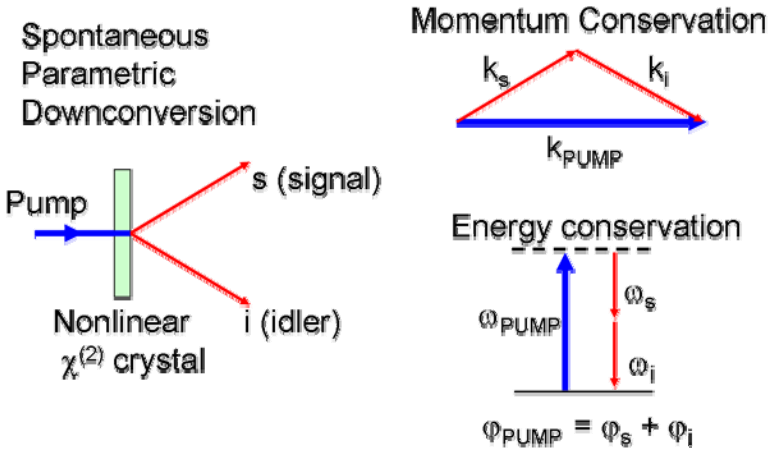
Erste experimentelle Umsetzung



Smolin, J. A. 2004. *The early days of experimental quantum cryptography*. *IBM J. Res. Dev.* 48, 1 (Jan. 2004), 47-52.

Technische Herausforderungen

- Erzeugung von einzelnen Photonen
  - Schwache Laserpulse
    - sehr geringe Bitrate
  - Parametrische Fluoreszenz
  - Quantenpunkte
- Tatsächliche Übermittlung
  - Glasfaserkabel
    - Dispersion
  - Freier Raum
    - abhängig von äußeren Bedingungen

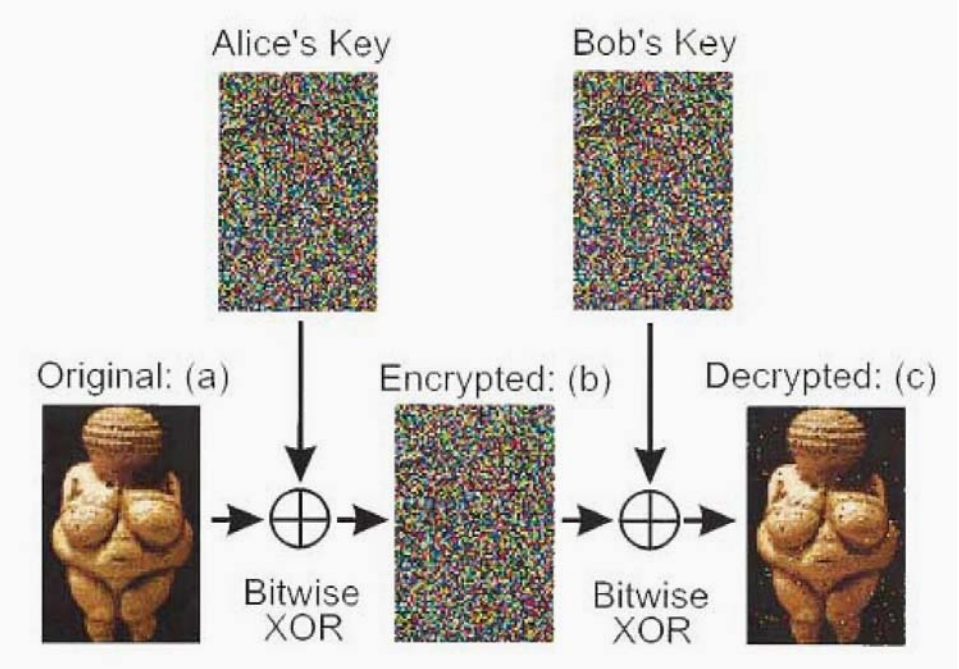


http://en.wikipedia.org/wiki/Spontaneous_parametric_down_conversion

http://thomas-aichele.de/qoptik/qoptik.html

Beispiel 1: Übertragung per Glasfaser (BB84)

- 1999:
  - Entfernung: 360m
  - Datenrate: 400-800 b/s
  - Fehlerrate: ca. 3 %
- Steigerung der Entfernung bis 200 km erprobt
- Bei schweizer Nationalratswahl 2008 eingesetzt

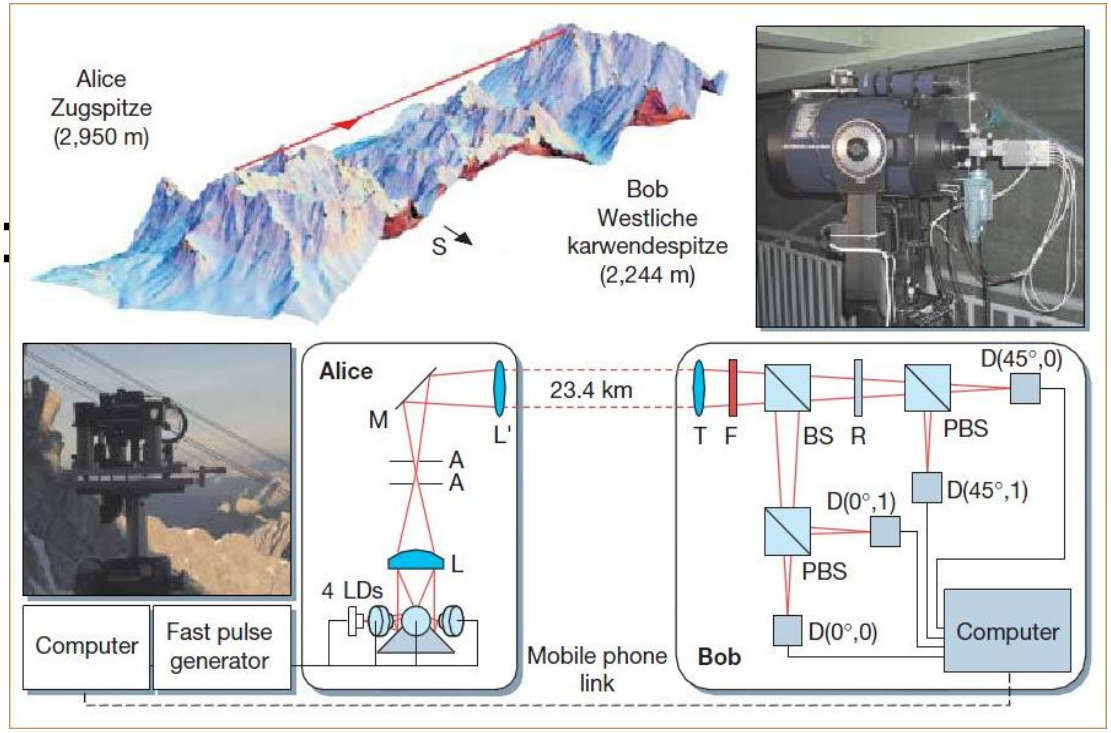


Übertragung eines Bildes der Venus von Willendorf

T. Jennewein et al., *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett. 84 4729 (2000)

Beispiel 2: Übertragung im freien Raum

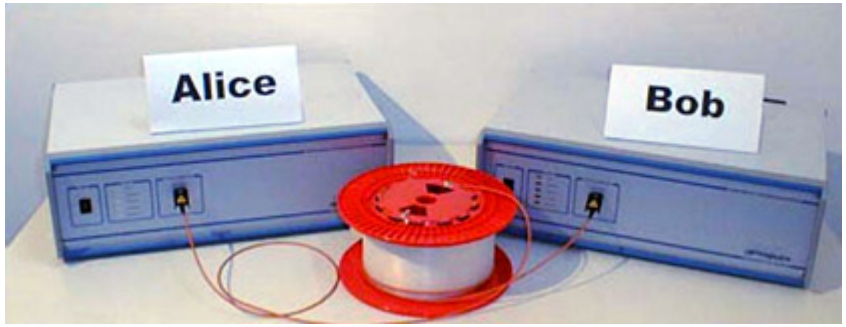
- Entfernung: 23.4 km
- Datenrate: 1.5-2 kb/s
- Fehlerrate: 5 %
  (nachts)
- Derzeitiger Rekord:
  144 km zwischen
  La Palma und
  Teneriffa
- Perspektive:
  Satelliten-
  kommunikation



Kurtsiefer, C. et al., *Quantum cryptography: A step towards global key distribution*, Nature 419, 450-450 (2002)

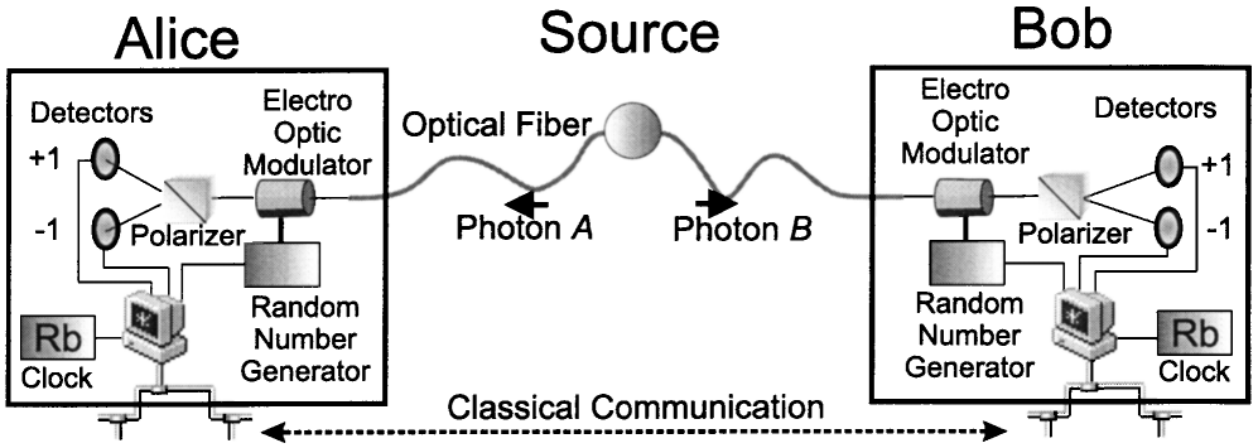
Zusammenfassung

- Quantenkryptographie ist absolut sicher (wenn keiner lauscht)
- Trotzdem bleiben klassische Hürden
- Technische Umsetzung schon erprobt und genutzt



http://www.iqis.org/media/html/macgregor_files/macgregor03.jpeg

EPR-Protokoll



T. Jennewein et al., *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett. 84 4729 (2000)

- Benutzt verschränkte Photonen
  - Quelle sendet verschränkte Photonenpaare an A und B
  - Beide messen unabhängig
  - Einer kehrt alle Bits um
- Vorteil:
  - Aussortierte Bits müssen Bell‘sche Ungleichung verletzen

Ekert, A.K., Quantum cryptography based on Bell‘s theorem, Phys. Rev. Lett. 67, 661-663, (1991)