



Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

UNIVERSITÄT WIEN

UNIVERSITÄT WIEN

Quantum Communication

- # Part 1 - Basics
 - # Quantum Mechanics Basics
 - # Systems of one and two Qubits
 - # Bells Theorem and the non-locality of QM
- # Part 2 – Tools
 - # Experimental realization of photonic qubits
 - # Sources for single photons and photon pairs
 - # Transmission and detection of single photons
- # Part 3 – Experiments with Photons
 - # Quantum Cryptography
 - # Quantum Teleportation
 - # Entanglement Purification
 - # The Quantum Repeater
 - # Dense Coding

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Origins ?

“...we are going to be even more ridiculous later and consider bits written on one atom instead of the present 10E11 atoms. Such nonsense is very entertaining to professors like me. I hope you will find it interesting and entertaining also.”

Feynman, 1986

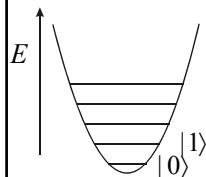
QM in a Nutshell

- The Framework
 - A system is described by a vector lying in a Hilbert space
 $|\Psi\rangle \in \mathcal{H}$ $|\psi\rangle^* = \langle\psi|$ $\langle\psi|\psi\rangle \in \mathbb{C}$
 - The inner product is written as $\langle\Psi_1|\Psi_2\rangle$
 - It's possible to define an orthonormal basis
 $\mathcal{H}^n = \{|\psi_1\rangle, \dots, |\psi_n\rangle\}$ with $\langle\psi_i|\psi_j\rangle = \delta_{ij}$
- The measurement process
 - Probability of finding the system in one of the basis states $|\psi_j\rangle$
 $P(\psi_j) = |\langle\Psi|\psi_j\rangle|^2$ Projection on one of the basis states
 - After the measurement in a certain basis, the system is in a state described by one of the basis states (depending on the measurement outcome)

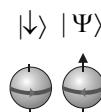
The Qubit

- Encoding of classical information in Quantum states
- Different physical systems can serve as Qubits

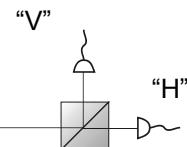
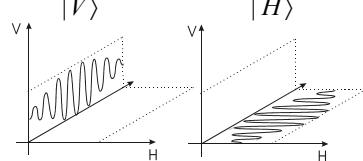
Energy Levels



Spin 1/2



Photon Polarization



Quantum Experiments and the Foundations of Physics

Prof. Anton Zeilinger

WANTED



Erwin Schrödinger

DEAD AND ALIVE

Superpositions of Single Qubits

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad |\alpha|^2 + |\beta|^2 = 1$$

Probability to find the Qubit in the state "0":

$$\begin{aligned} P(0) &= |\langle\psi|0\rangle|^2 = |\langle\alpha^*|0\rangle + \langle\beta^*|1\rangle|0\rangle|^2 \\ &= |\alpha\langle 0|0\rangle + \beta\langle 1|0\rangle|^2 = |\alpha|^2 \end{aligned}$$

$$P(1) = |\beta|^2$$

The conjugate basis:

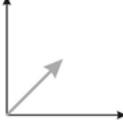
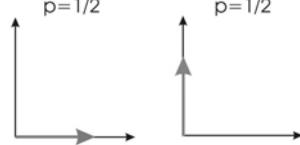
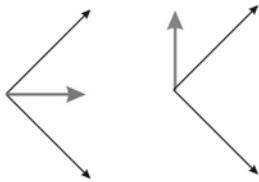
$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

A measurement of a qubit in the basis of preparation gives the correct result with certainty, while a measurement in the conjugate basis has completely random outcomes

Quantum Experiments and the Foundations of Physics

Prof. Anton Zeilinger

Superposition vs Statistical Mixture

Basis	Superposition	Mixture
HV		
45°		



Entanglement

- More than one Qubit: Tensor Product of single Qubit Spaces
 - Two Qubits: 4-dimensional Hilbertspace
- There Exist states that can not be described as a product of single qubits

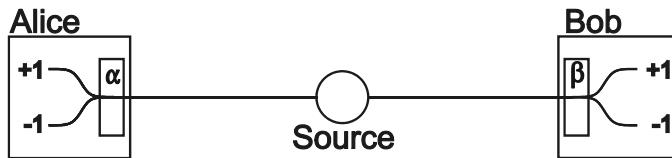
Bell Basis:

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 \pm |1\rangle_1|0\rangle_2) \quad |\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 \pm |1\rangle_1|1\rangle_2)$$

- Not a statistical mixture of 01 and 10 !!!
- Information is only encoded in joint properties.
- Individuals do not carry any information on their own.
- Correlations in joint properties
- Entanglement can not be generated by local operations on particles



Bell's inequality and the non-locality of QM

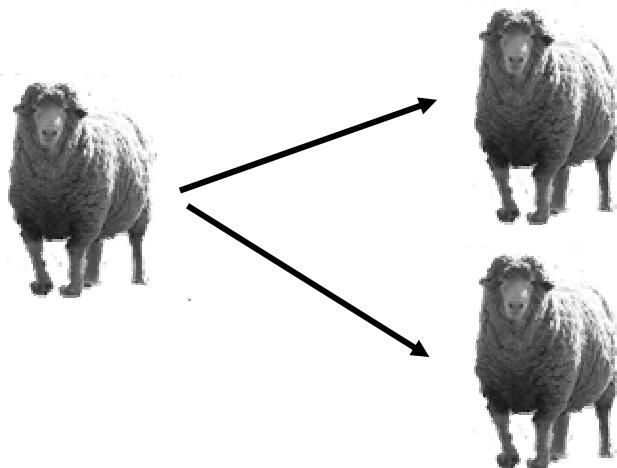


- # EPR – Paradox and Local Hidden Variable Theories
- # Locality ?
 - # Is it possible to explain the correlations by information locally encoded in the individual particles
 - # Einstein: "Spooky Action at a distance"
- # Bells Theorem and Bells Inequality

$$S(\alpha_1; \alpha_2; \beta_1; \beta_2) = |E(\alpha_1, \beta_1) + E(\alpha_2, \beta_1) + E(\alpha_1, \beta_2) - E(\alpha_2, \beta_2)| \leq 2$$

 Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Classical Cloning



 Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Quantum Cloning

Desired process:

$$|\psi\rangle_1 |b\rangle_2 |I\rangle_3 \Rightarrow |\psi\rangle_1 |\psi\rangle_2 |F_\psi\rangle_3$$

Lets assume it works for the basis states:

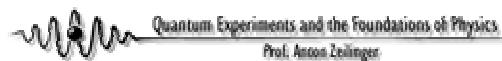
$$|0\rangle_1 |b\rangle_2 |I\rangle_3 \Rightarrow |0\rangle_1 |0\rangle_2 |F_0\rangle_3$$

$$|1\rangle_1 |b\rangle_2 |I\rangle_3 \Rightarrow |1\rangle_1 |1\rangle_2 |F_1\rangle_3$$

What about superpositions ? $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

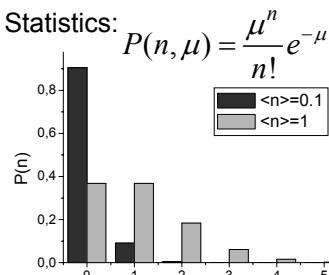
$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1) |b\rangle_2 |I\rangle_3 &\Rightarrow \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |I_0\rangle_3 + |1\rangle_1 |1\rangle_2 |F_1\rangle_3) \\ &\neq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) |F_{0+1}\rangle \end{aligned}$$

However: Imperfect cloning is Possible!



Sources for Single Photons

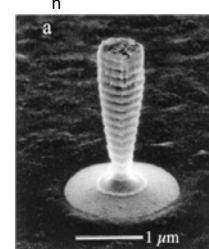
Poisson Statistics:



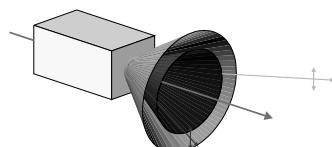
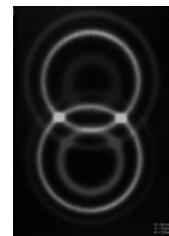
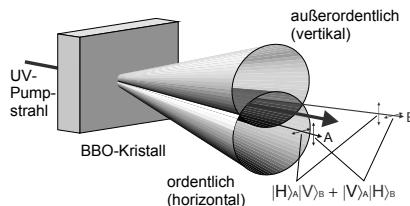
- “real” single photon sources
 - Color Centers in Crystals
 - Quantum Dots (“artificial Atoms”)
- Weak coherent pulses (attenuated laser pulses)
- SPDC Pair Sources

Single Quantum Dot in a Microcavity

Solomon, Pelton, Yamamoto,
PRL 86 (2001) 3903



Entanglement Sources I - SPDC

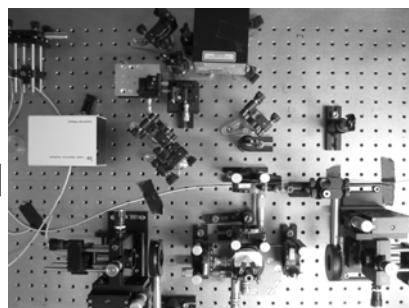
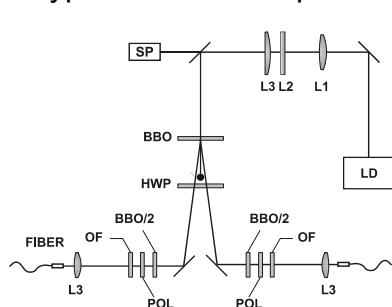


Type-I Parametric Down-conversion

by Guido Czeija, Gregor Weihs and Alipasha Vaziri
 Quantum Experiments and Foundational Physics
 Prof. Anton Zeilinger
 Institut für Experimentalphysik
 University of Vienna

Quantum Experiments and the Foundations of Physics
 Prof. Anton Zeilinger

A type-II SPDC setup:



Pairs detected: >20.000 1/s (> 1300 events/(s.mW))
 Visibility of entanglement: > 96%

Quantum Experiments and the Foundations of Physics
 Prof. Anton Zeilinger

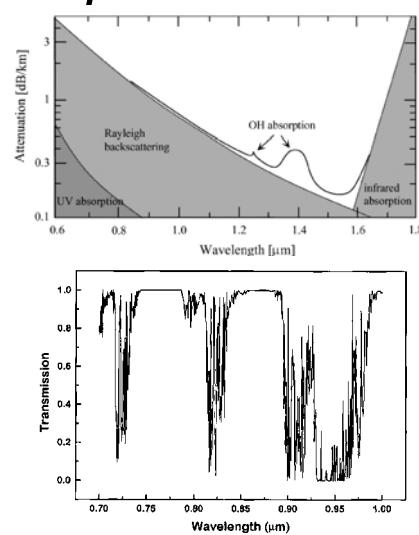
Detectors

- Avalanche Photo Diodes (APD)
 - Si
 - visible & near infrared / -20°C / high efficiency / low noise
 - Ge
 - ~1300nm / -200°C / low efficiency / high noise
 - InGaAs
 - ~1550nm / -50°C / low efficiency / high noise
- Other photon counting devices
 - Superconducting
 - any optical wavelength / 500mK / high efficiency
 - Photo Multiplier Tubes

 Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

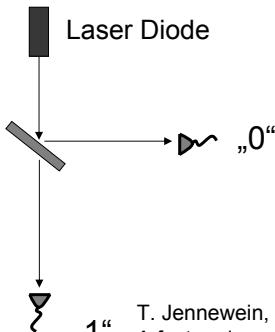
Transmission Systems

- Fibers
 - Loss
 - Dispersion
 - Decoherence
- Telescopes - Atmosphere
 - Line of Sight
 - Environmental Light



 Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Random Number Generator



Bit Rate: 1 Mbit/s

Noncyclic Random Sequence

T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger
A fast and compact quantum random number generator
Rev. Sci. Inst. 71, 1675-1680 (2000)

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Classical Cryptography

Rather old:

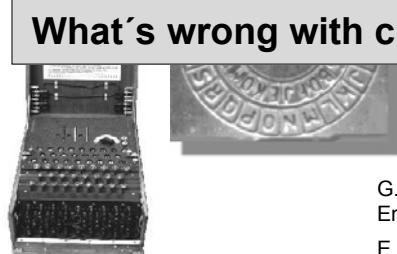


Today:

Symmetric Ciphers:

- DES
- AES
- One Time Pad
- Perfectly secure

What's wrong with classical Cryptography?



Public Key Cryptosystems:

- RSA

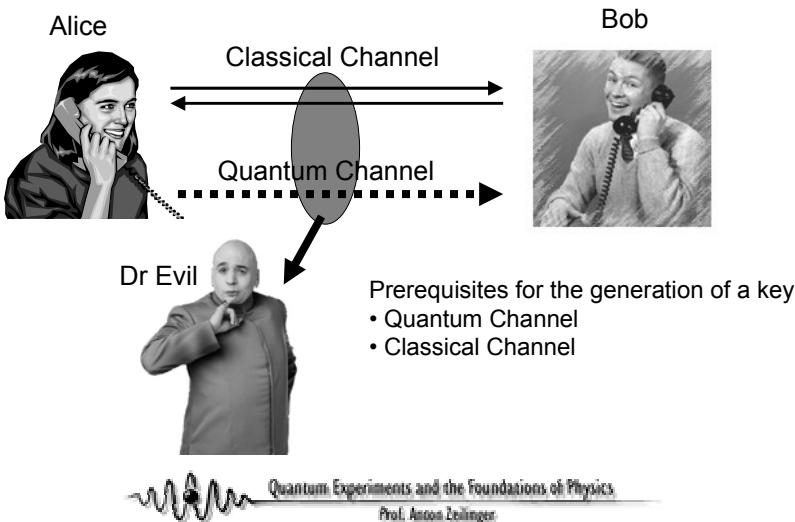
G. Vernam J. Am. Institute of Electrical Engineering Vol XLV, 109 (1926)

E.C. Shannon, Bell Systems Technical Journal 28 656 (1949)

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

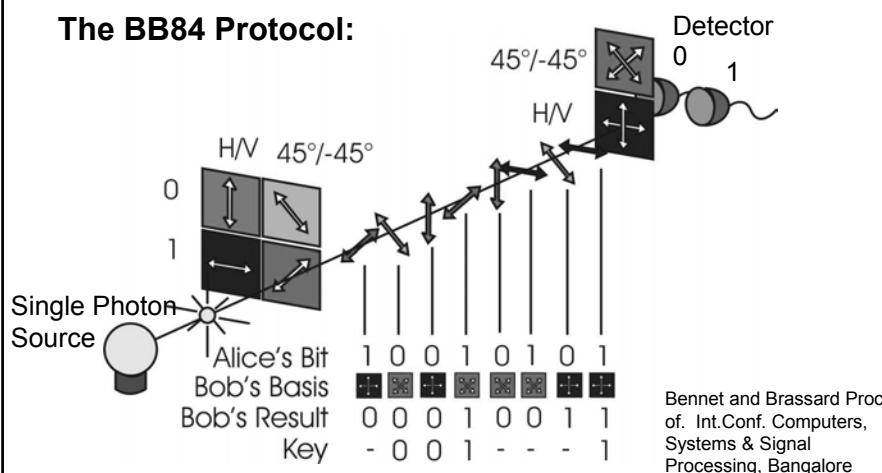
Quantum Key Distribution

Creation of a secure shared secret

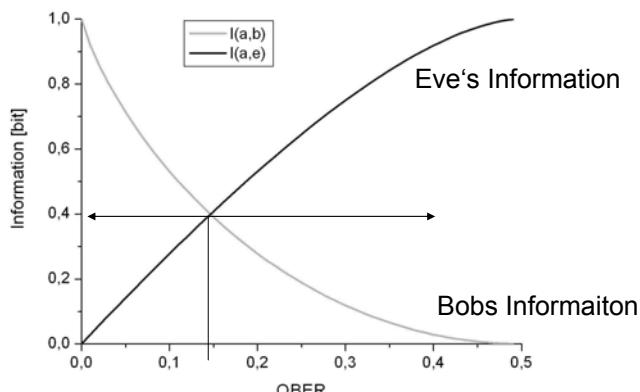


Quantum Cryptography (QKD)

The BB84 Protocol:



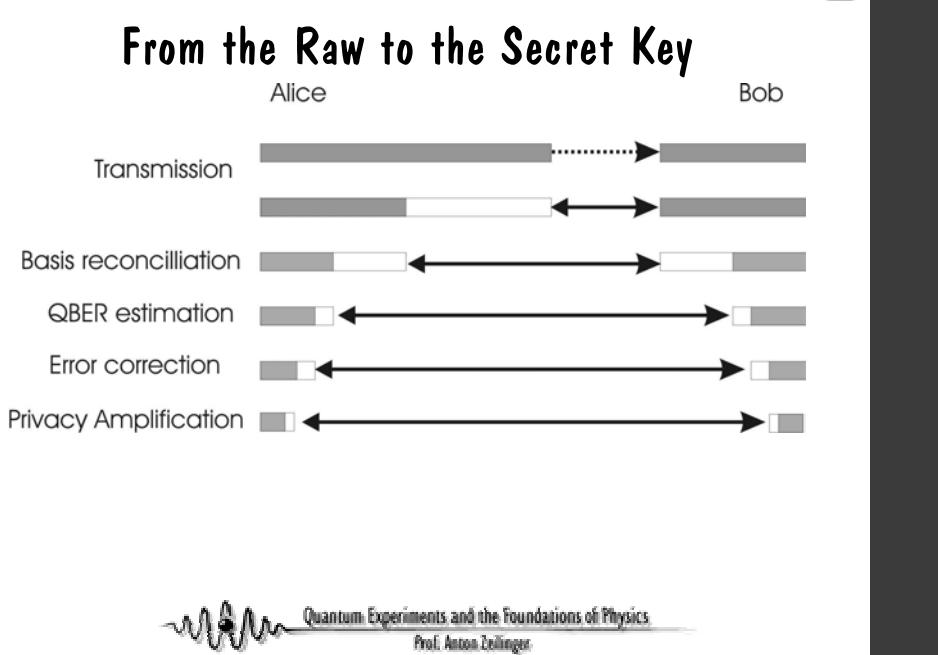
What about noise ?



$$R_{\text{net}} = R_{\text{sifted}}(I(a,b) - I(a,e))$$

$$QBER_{\max} = \frac{1-\sqrt{2}}{2} \approx 15\%$$

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

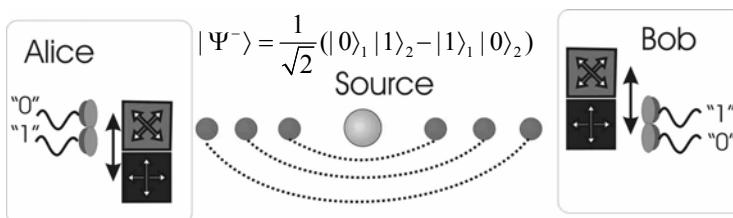


Attacks on QKD

- # Individual Attacks
 - # Intercept resend
- # Coherent Attacks
- # Photon Number Splitting attacks

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

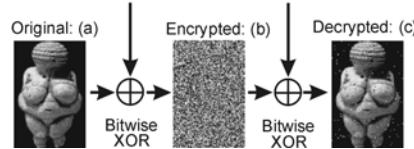
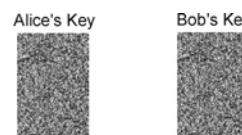
Entangled State Cryptography



Different Schemes possible:

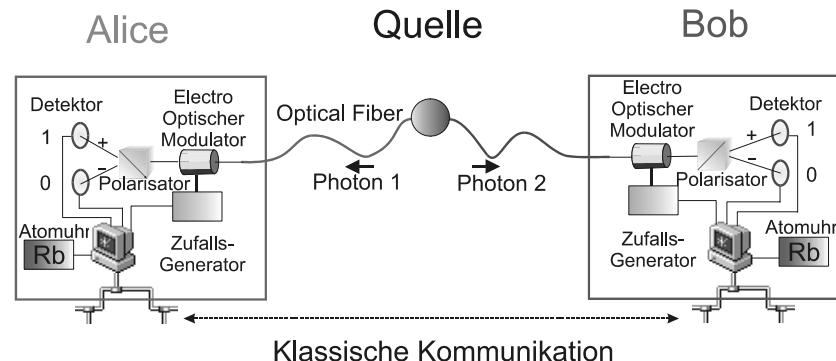
- # Eckert
- # Modified BB84
- # CHSH

Jennewein et al. PRL 2001



Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Entangled State QKD II



Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Long Distance Fiber QKD

Over 100km:

System: Weak Pulse – Phase

Distance: >100 km

QBER ?

? kbit/s (raw)

Kosaka et al. quant-ph/0306066
Yuan et al. Proc. CLEO 2003



Geneva: System: Weak Pulse – Phase
Distance: 67 km
QBER < 6%
160 bit/s (raw)

Stucki et al. New Journal of Physics 4 (2002) 41.1-41.8

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Free-Space QKD with Single Photons

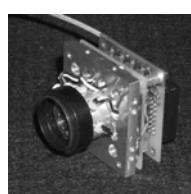


System: Weak Pulse - Polarization

Distance: 23.4 km

QBER < 5%

1.5-2 kbit/s (raw)

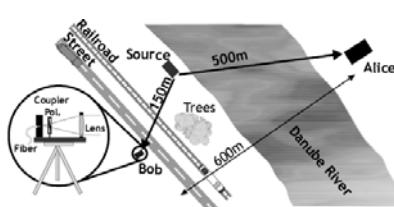


Kurtsiefer, Zarda, Halder, Weinfurter, Gorman, Tapster, Rarity
Nature 419 (2002) 450

Quantum Experiments and the Foundations of Physics

Prof. Anton Zeilinger

Free Space Distribution of Entangled Photons I



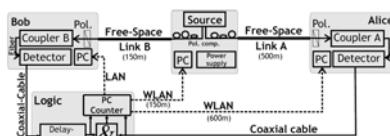
System: EP – Polarization

Distance: 600 m

QBER ~ 8%

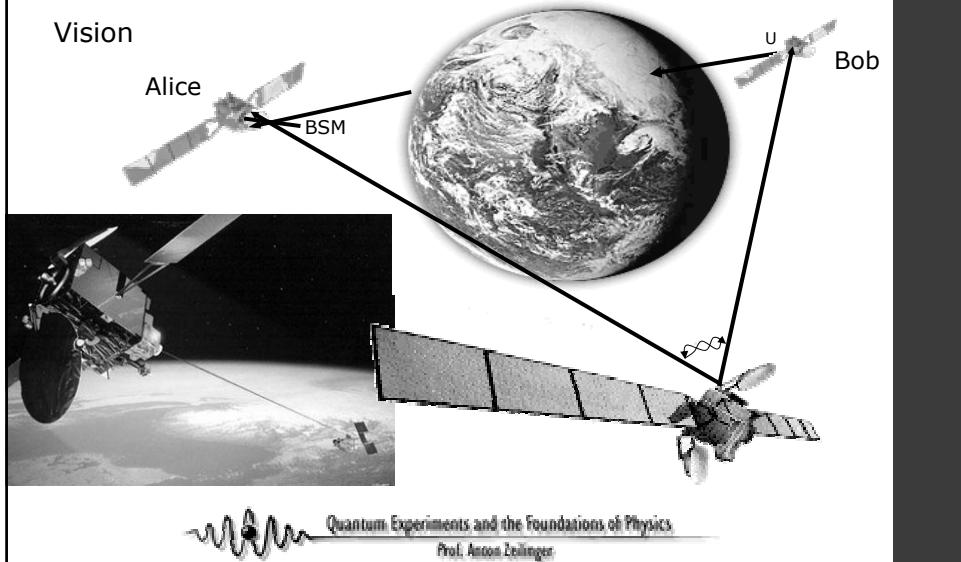
< 100 bit/s (raw)

Aspmeyer, Böhm et al. Science 301
(2003) p621



Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

The Future of QKD ?

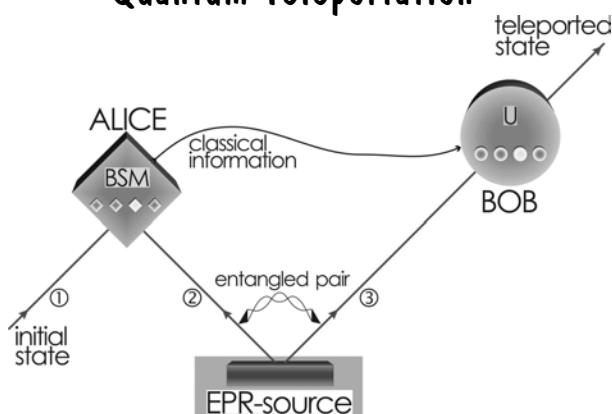


Predicting the Future

“Where a calculator on the Eniac is equipped with 18.000 vacuum tubes and weighs 30 tons, computers in the future may have only 1000 tubes and weigh only 1½ tons “

Popular Mechanics, March 1949

Quantum Teleportation



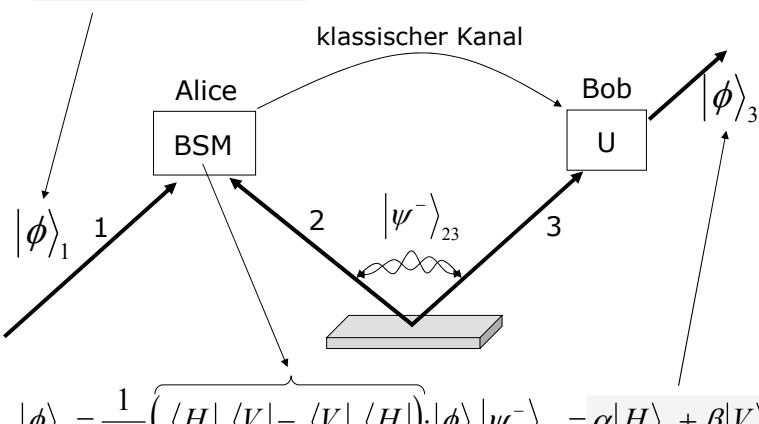
Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl,
Harald Weinfurter & Anton Zeilinger, Nature vol.390, 11 Dec
1997, pp.575.

C.H. Bennett, G. Brassard, C. Crepeau, R.
Jozsa, A. Peres, and W. Wootters, *Phys.
Rev. Lett.* vol. **70**, pp 1895-1899 (1993)

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Teleportationsprotokoll

$$|\phi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1 \quad |\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|H\rangle_2|V\rangle_3 - |V\rangle_2|H\rangle_3)$$



$$|\phi\rangle_3 = \frac{1}{\sqrt{2}}(|H\rangle_2|V\rangle_3 - |V\rangle_2|H\rangle_3) \cdot |\phi\rangle_1 |\psi^-\rangle_{23} = \alpha|H\rangle_3 + \beta|V\rangle_3$$

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Teleportation

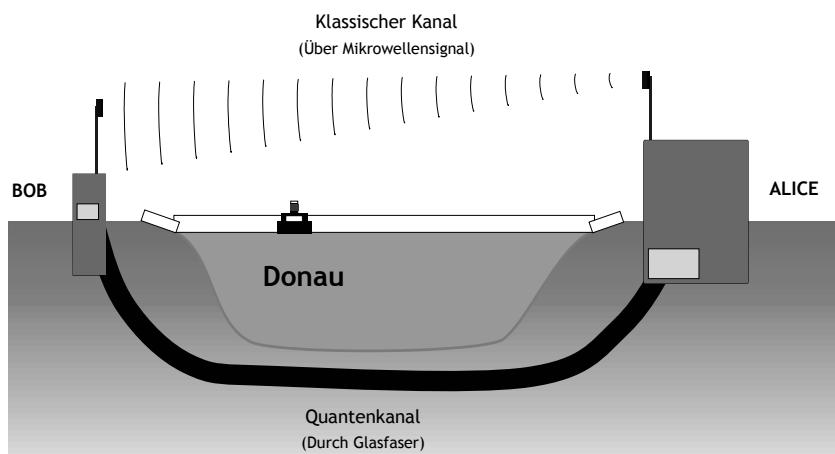
How it really works ;-)

$$|\Psi\rangle_{123} = |\Psi\rangle_1 \otimes |\Psi^-\rangle_{23}$$

$$\begin{aligned} |\Psi\rangle_{123} &= (\alpha|0\rangle_1 + \beta|1\rangle_1) \frac{1}{\sqrt{2}} (|0\rangle_2 |1\rangle_3 - |1\rangle_2 |0\rangle_3) \\ &= \frac{1}{\sqrt{2}} (\alpha \{|0\rangle_1 |0\rangle_2 |1\rangle_3 - |0\rangle_1 |1\rangle_2 |0\rangle_3\} + \beta \{|1\rangle_1 |0\rangle_2 |1\rangle_3 - |1\rangle_1 |1\rangle_2 |0\rangle_3\}) \\ &= \frac{1}{\sqrt{2}} (\alpha |1\rangle_3 - \beta |0\rangle_3) |\Phi^+\rangle_{12} - (\alpha |0\rangle_3 + \beta |1\rangle_3) |\Psi^-\rangle_{12} - (\alpha |0\rangle_3 - \beta |1\rangle_3) |\Psi^+\rangle_{12} \end{aligned}$$

 Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

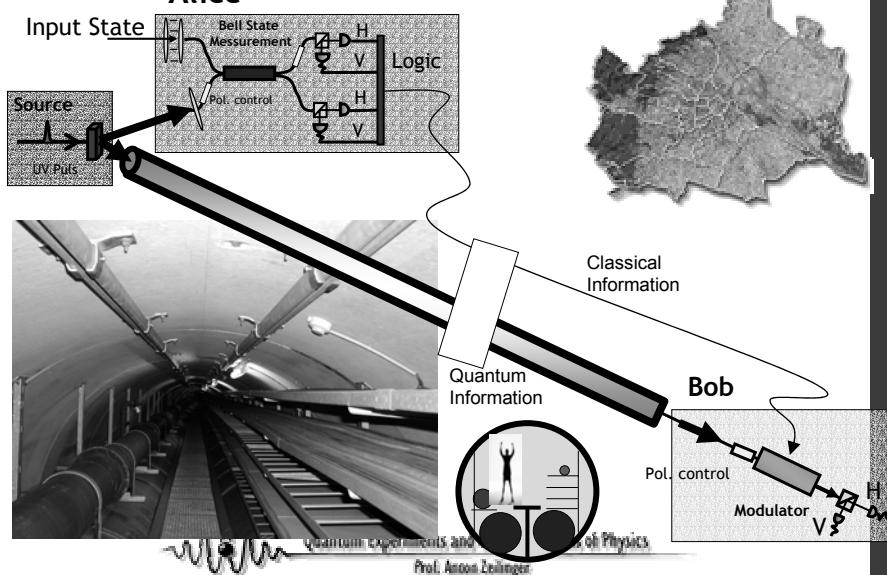
Long Distance Teleportation I



 Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Long Distance Teleportation II

Alice



Bells Telephone



Graham Bell



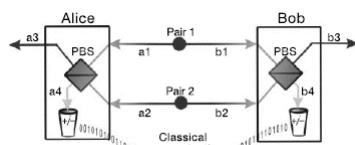
John Bell

- # Teleportation and Cloning would allow faster than light communication
- # Cloning is forbidden in QM
- # Theory remains consistent

Entanglement Purification

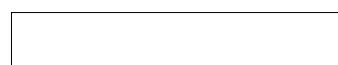


Fidelity 75% \rightarrow 98%
Pan et al. Nature 423 (2003) 417

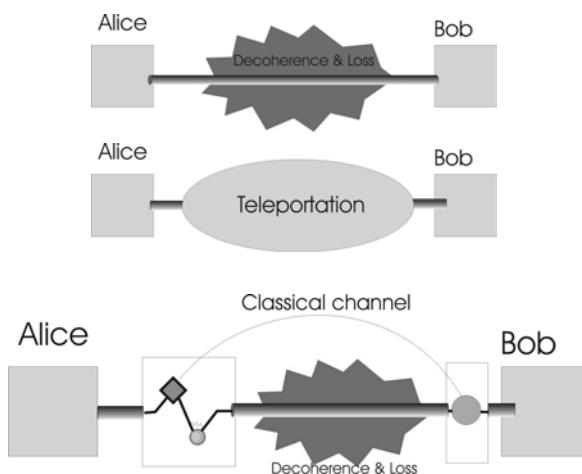


Classical Communication

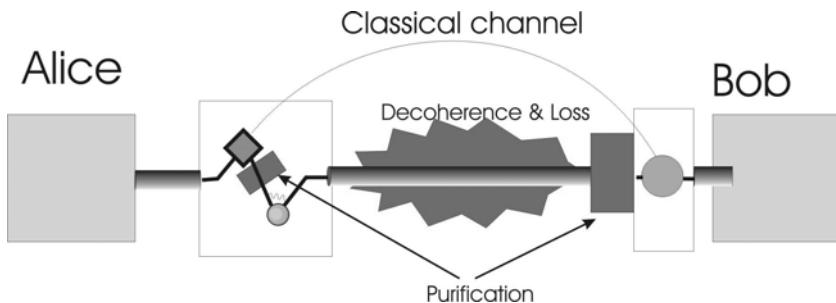
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)$$



The Quantum Repeater I

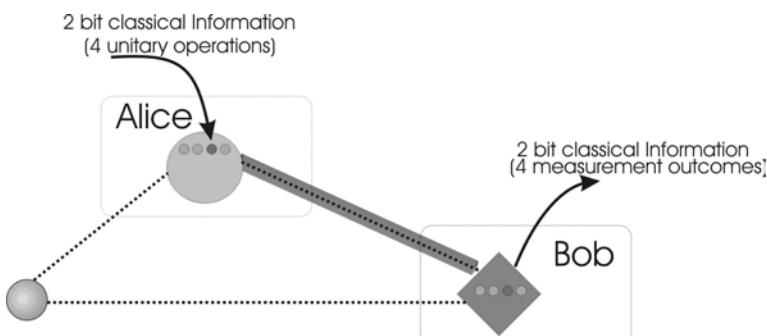


Quantum Repeater II



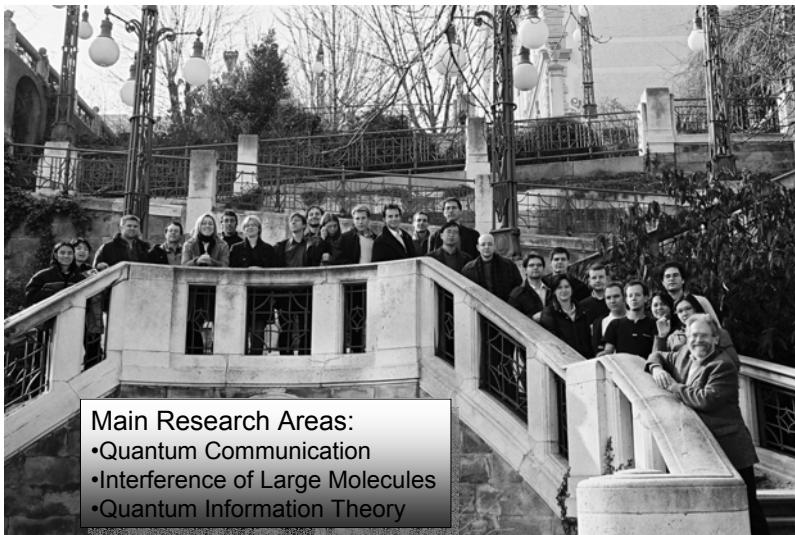
Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Dense Coding



Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

Our Group



Main Research Areas:

- Quantum Communication
- Interference of Large Molecules
- Quantum Information Theory



Quantum Experiments and the Foundations of Physics

Prof. Anton Zeilinger