Quantum Technologies : objectives, prospects and challenges

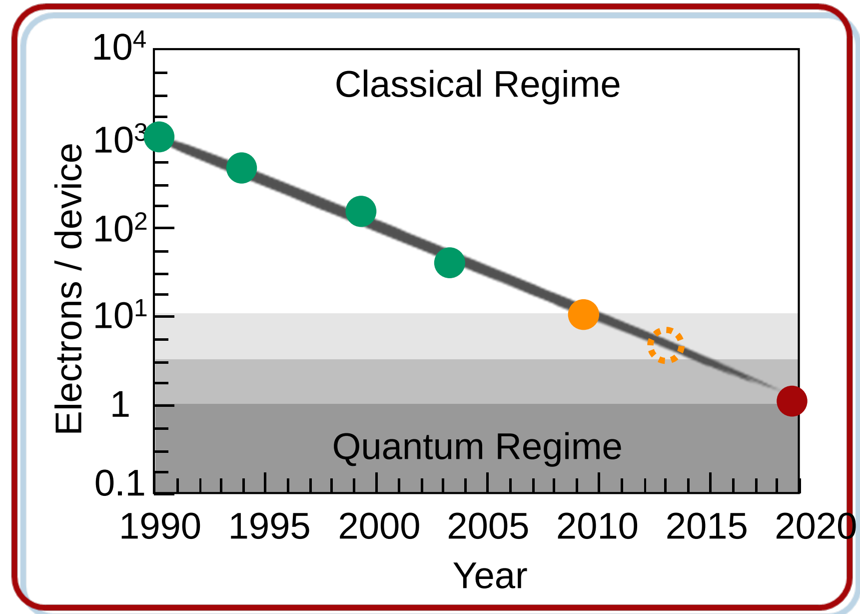
Elisabeth Giacobino
Ecole Normale Supérieure,
Université Pierre et Marie Curie,
Centre National de la Recherche Scientifique,
Paris, France

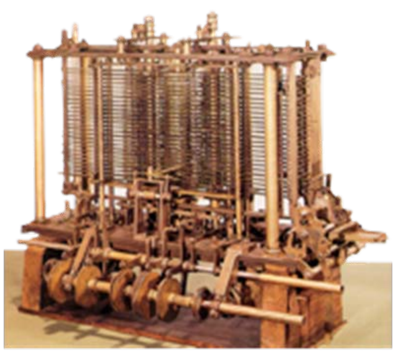
Member of ISTAG
(Information Society Technology Advisory Group)

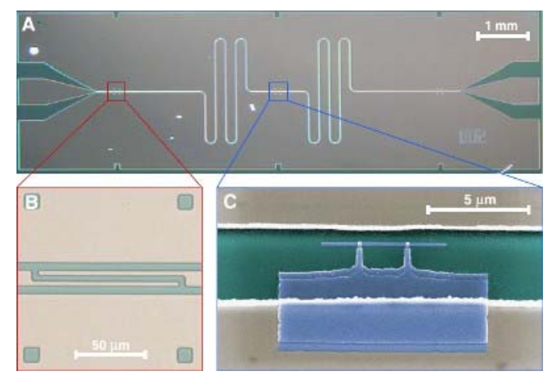
Rainer Blatt
Vladimir Buzek
Tommaso Calarco
Elisabeth Giacobino
Philippe Grangier
Peter Zoller

the future
IS quantum

- Moore's law: the number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years
  - Driving force of technological and social change in the late 20th and early 21st centuries
- Eventually the quantum wall will be hit
  - Not a question of if rather of when
  - Push back the hitting time (more Moore) and/or change completely the technology (more than Moore)



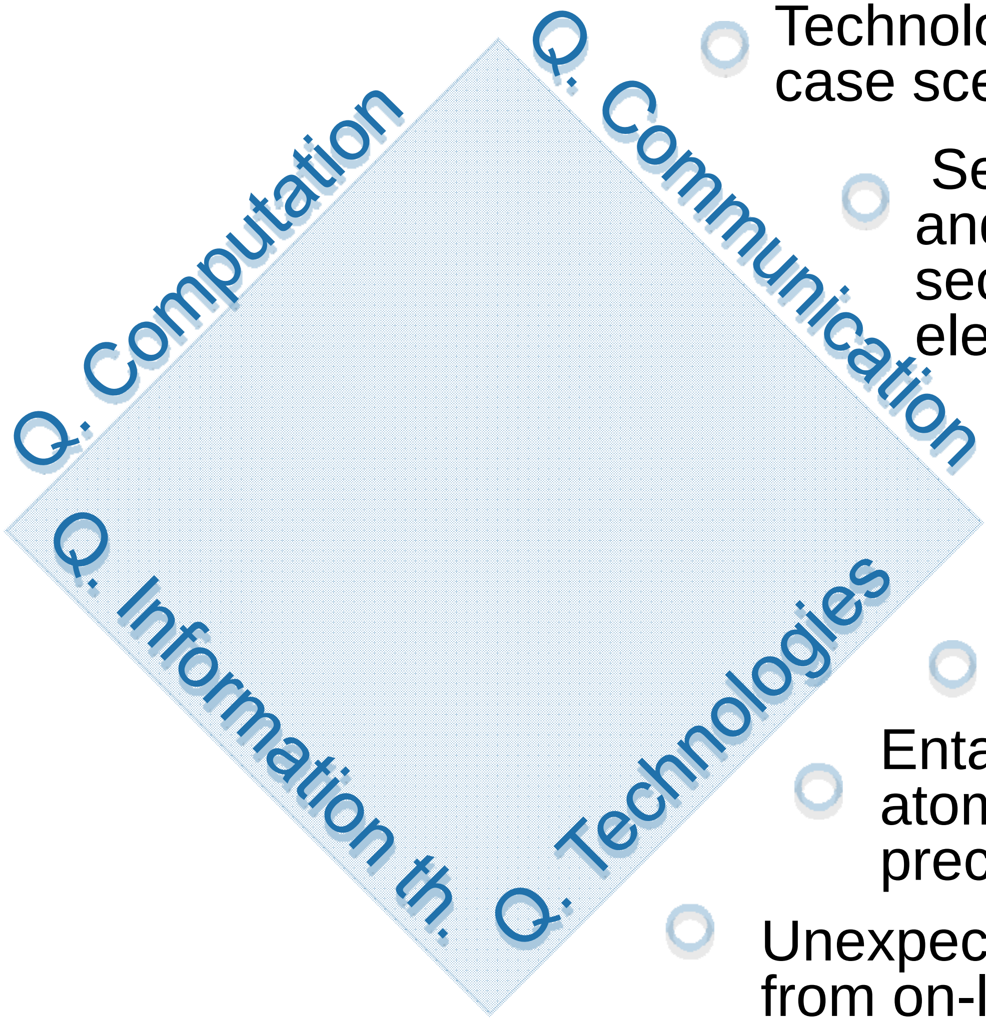




"quantum information is a radical departure in information technology, more fundamentally different from current technology than the digital computer is from the abacus".

W. D. Phillips, 1997 Nobel laureate
member of the AQUTE Integrating Project

QIPC areas

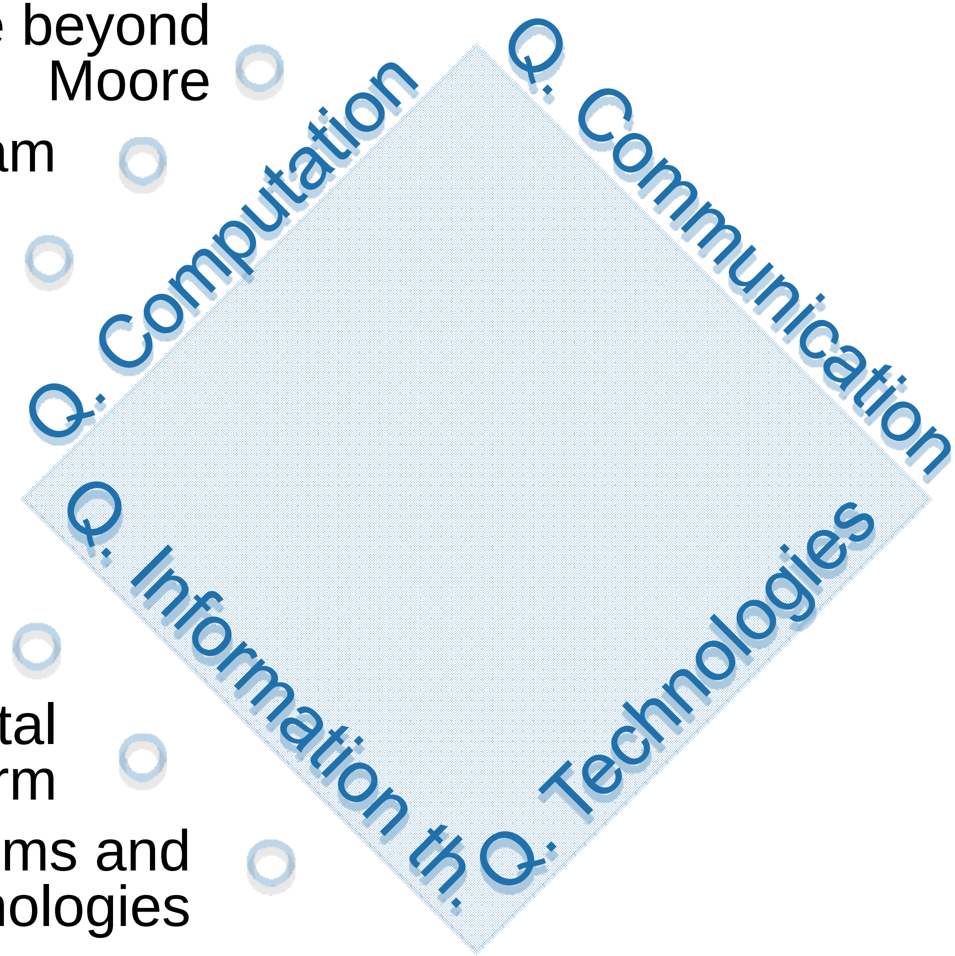


- Technology ready to be deployed in real case scenarios
- Several SMEs use quantum techniques and quantum cryptography. It was used to secure the results of a Swiss federal elections in 2007
- Standardization process started

- Technologies enabled by harnessing entanglement
- Entanglement allows for much better atomic clocks and therefore more precision in GPS
- Unexpected markets : QRNG customers are from on-line gambling and lotteries

QIPC areas

- One of the most promising route beyond Moore
- Still upstream
- but few qubits special purpose processors (quantum simulators) are on sight
- Major driver for the development of the field (e.g., BB84, Shor)
- Guide and support for experimental platform
- Inspiration for new protocols pardigms and technologies



timeline for
quantum computation

t=0

t=10

t=20

1981. First idea: Feynman quantum simulator

-14 y

1995. Shor’s algorithm; Cirac-Zoller gate
Start of quantum computation

5 y

2000. Diverse approaches
(Trapped ions, neutral atoms, cavity QED, semiconductor, superconducting, linear optics, impurity spins, single molecular cluster, NMR,...)

7 y

Too early to pick up the winning implementation technology
(still true, see e.g., hybrid techs)

2002. 2-qubit gates

11 y

2006. Quantum byte (trapped ions)

13 y

2008. Error correction threshold reached

18 y

2013. Few qubit quantum processors
Quantum simulators

>25 y

>2020. General purpose quantum processors

timeline for
quantum communications

t=0

t=10

t=20

QKD
point-to-point < 400Km

- 1984. First idea BB84
- 1991. Ekert PRL; start of quantum information
- 1992. First experiment
- 1993. Diverse approaches
- 1995. Out of lab
- 2001. id Quantique start-up
- 2008. Autonomous operations
- 2012. Mbps @ 50Km

400 km

Q REPEATERS
network and > 400Km

- 1998. First idea: Briegel et al
- 2005. Diverse approaches (REI, NV, Atoms, Gases)
- 2007. First experiment (Atom gas and ions
  Multi-mode memory idea
- 2013. First functional quantum repeater link
- 2020. Out of lab

> 1000 km

QIPC scientific challenges

Source:
Quantum Information Processing and Communication: Strategic Report on current status, vision and goals for research in Europe
Version 1.7, April 2010

Quantum Computation

short term (~5y)

- Devices realizing quantum algorithms with up to 10 qubits
- Fault tolerant computing and error correction on small scale systems
- Distributed quantum algorithm
- Different classes of entangled states up to 10 qubits
- Quantum simulation of a system that cannot be simulated classically

long term (~10y)

- Large dimension quantum memory
- Quantum algorithm with up to 50 qubits
- Quantum simulation of a key problem in science
- Quantum algorithm with fault tolerant error correction

Quantum Commmunication

short term (~5y)

- Build a quantum repeater with two nodes
- Interface photons with matter
- Secure quantum key distribution network

long term (~10y)

- Satellite quantum communication
- 1000 km quantum cryptography
- Multi-node quantum networks
- Realization of new quantum protocols

QIPC
scientific challenges

Source:
Quantum Information Processing and Communication: Strategic Report on current status, vision and goals for research in Europe
Version 1.7, April 2010

short term (~5y) / long term (~10y)

Quantum Technologies

- Develop entanglement based technologies, e.g.,
  - Clocks
  - Metrology
- Develop entanglement enhanced technologies, e.g.,
  - Sensors
  - Imaging, photonics
- Entanglement enabling quantum control
- Entanglement system engineering

- Quantum simulator as a scientific tool
- Bootstrap the quantum technologies market

Quantum Information Theory

- Develop
  - Computation paradigms and algorithms
  - Communication protocols
  - Quantum specific techniques (e.g., quantum control and feedback methods)
- Guide and support experimental developments, covering the widest possible range of physical systems and technologies.

Roadmap Quantum information processing and communication
http://qurope.eu

quantum computation

- New components and devices that will be elements in the long term in high-performance computing facilities

It will provide

- Quantum processors
- Quantum simulators
- Hybrid technologies

quantum communication

- New components and devices that will be elements in the long term in high-performance computing facilities

  It will provide

  - Global scale quantum communication (security, privacy)
  - Quantum internet
  - Wiring of quantum processors

quantum technologies

- New technologies ready for a market where the quantum limits will define the performance of industrial applications

  It will provide

  - Global scale quantum communication (security, privacy)
  - Disruptive photonics devices (e.g.,single photon detectors, quantum repeaters)
  - Metrology, sensors, imaging
  - Quantum simulators

quantum information theory

- Guide and support experimental developments, covering all range of physical systems and technologies

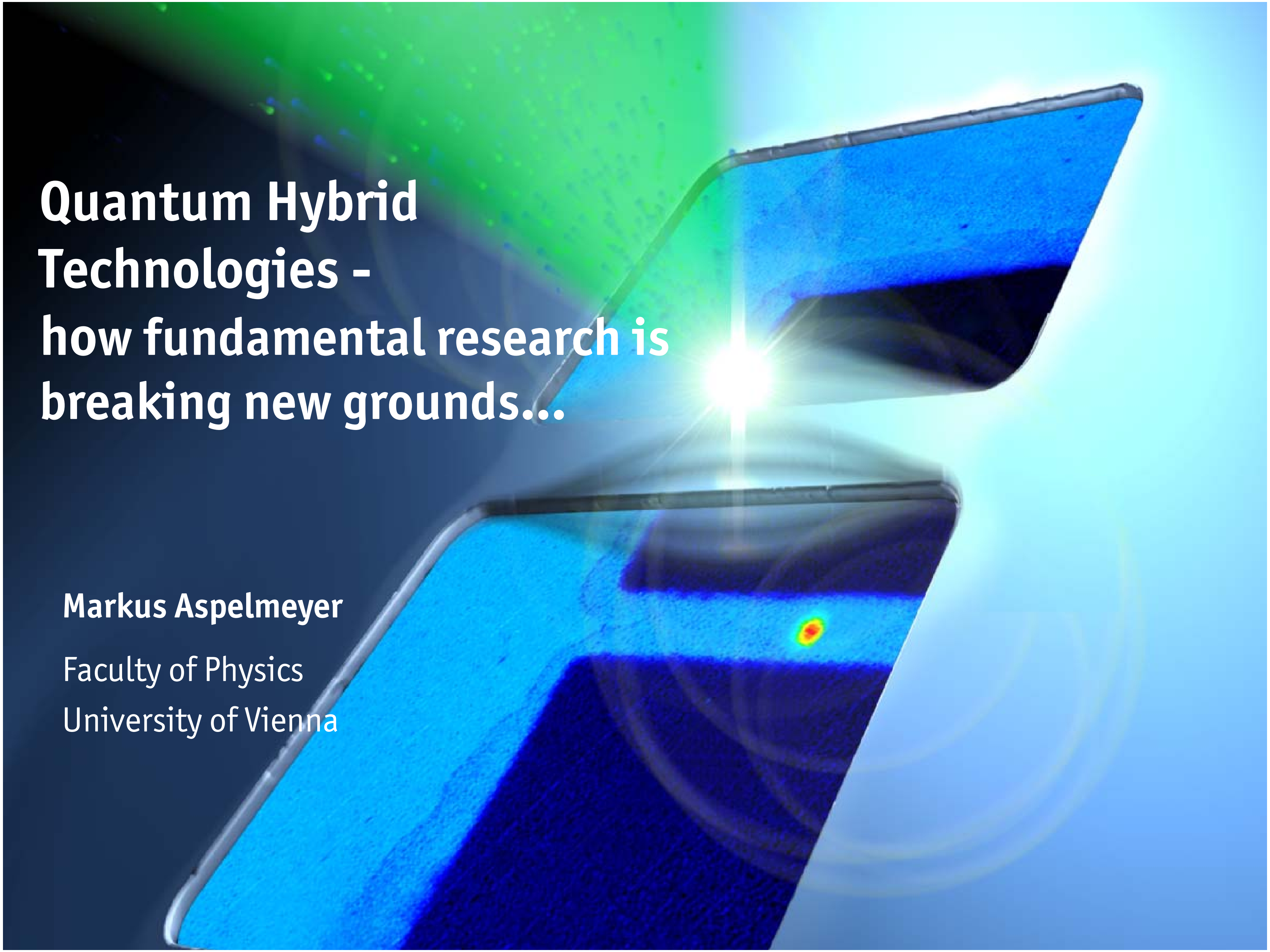
  Il will provide

  - Computational paradigms, algorithms and optimized techniques
  - Communication protocols
  - Inspiration for new technologies

Conclusion

“**Quantum Information Technologies hold the promise of revolutionizing computing and communication**. FET invested early in these mind boggling technologies and rallied a group of Member States to match its efforts. Thank to this support, Europe now produces half of the scientific knowledge worldwide in this area and leads the commercial exploitation of this technology in the area of network security. What was considered fiction less than a decade ago, has become a reality today.”

V. Reading, Commissioner DG-INFSO
opening address of the FET “Science Beyond Fiction” conference (Prague, 2009)



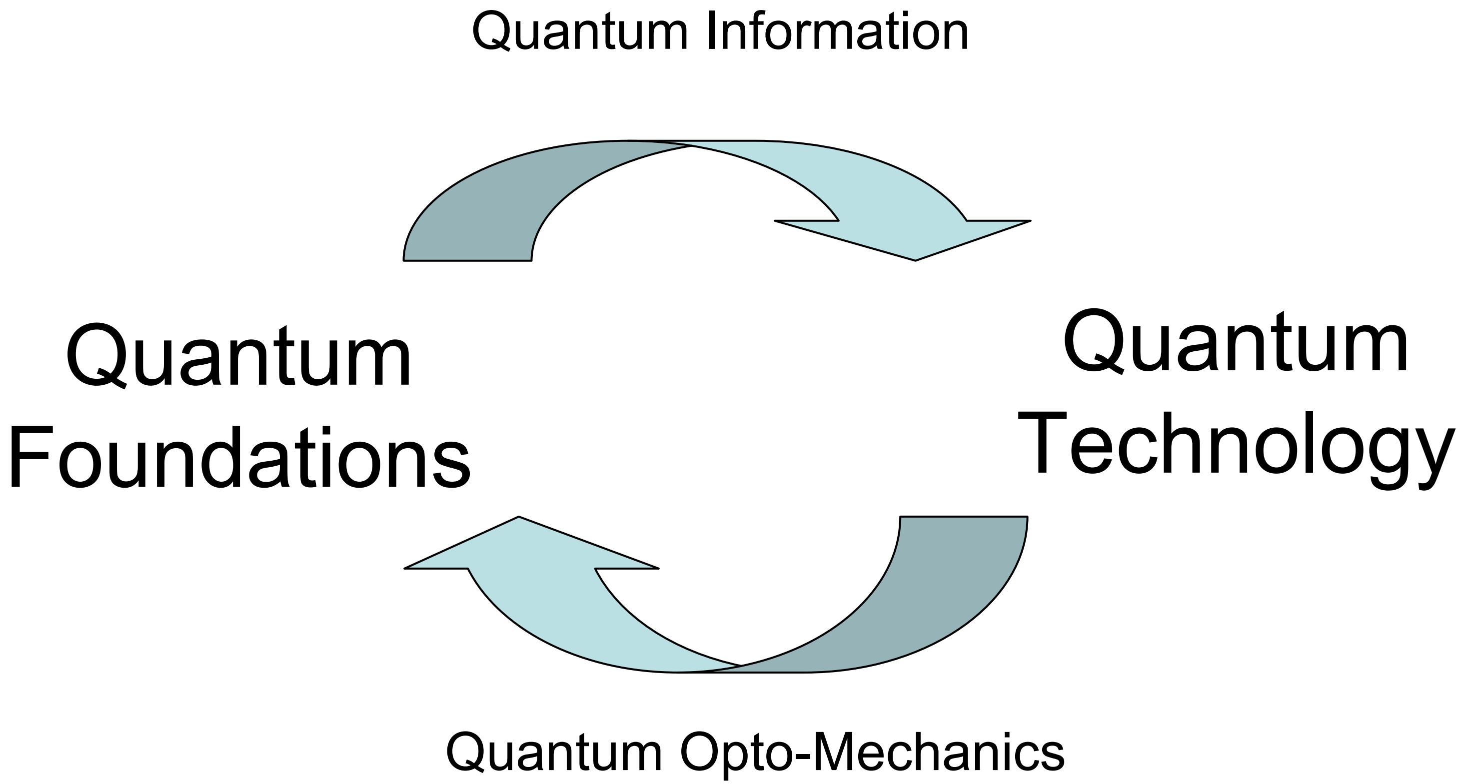
Quantum Hybrid Technologies - how fundamental research is breaking new grounds...

Markus Aspelmeyer

Faculty of Physics

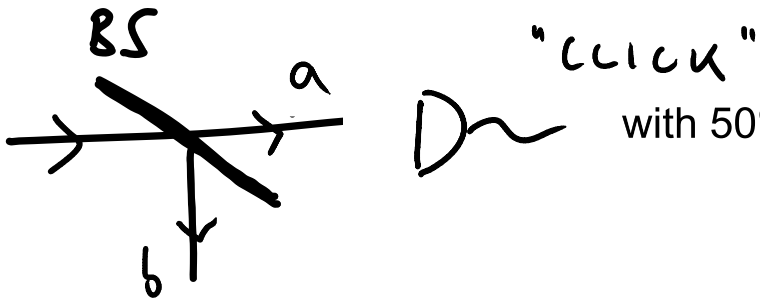
University of Vienna

Fundamental vs Applied Research: Give and Take...



Conceptual challenges of quantum theory: Randomness

Single-photon source



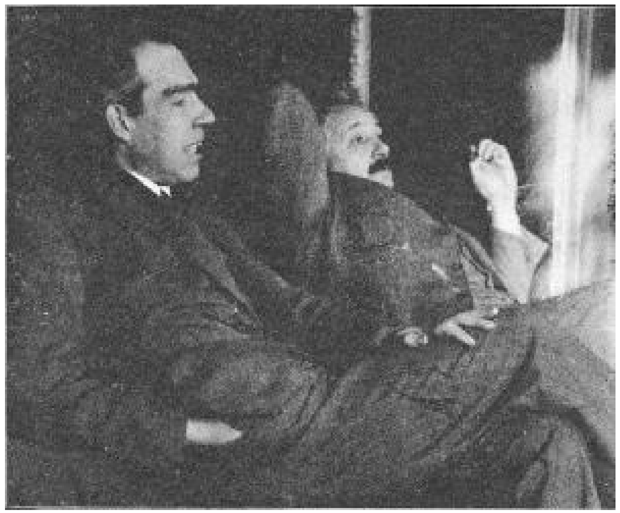
with 50% probability

→ **Objective randomness!**

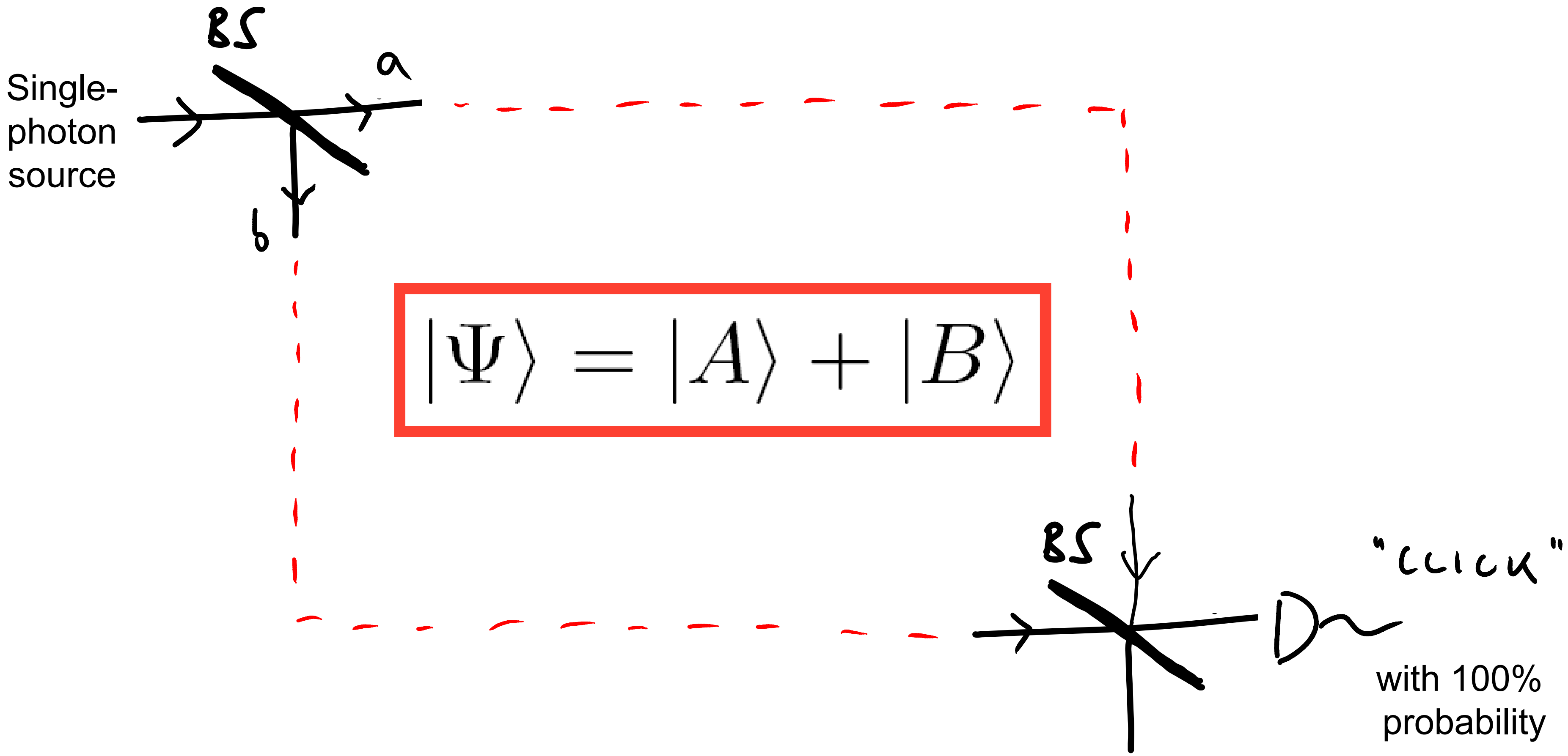
$$|\Psi\rangle = |A\rangle + |B\rangle$$

“The Weakness of the Theory lies ... in the Fact, that Time and Direction of the Elementary Process are left to „Chance“.”

A. Einstein, 1917 Z. Physik



Conceptual challenges of quantum theory: Which way?



WHICH WAY? A or B?

Quantum-Superposition:

how can we talk about *physical reality* in a consistent way?

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element correspo… to each element of reality. A suffici… reality of a physical qu… it with… c… d… o… th…

quantum mechanics is not complete or (2)… two quantities cannot have simult… …ion of the problem… …em …at …if …e …n

A… tinct… indep… conce… conce… object… we pic… In a… physica… tions: (… the desc… It is only…

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

PRINCETON, N. J., May 3.—Professor Albert Einstein will attack science's important theory of quantum mechanics, a theory of which he was a sort of grandfather. He concludes that while it is "correct" it is not "complete."

With two colleagues at the Institute for Advanced Study here, the noted scientist is about to report to the American Physical Society what is wrong with the theory of quan… …chanics, it has been learned … Service.

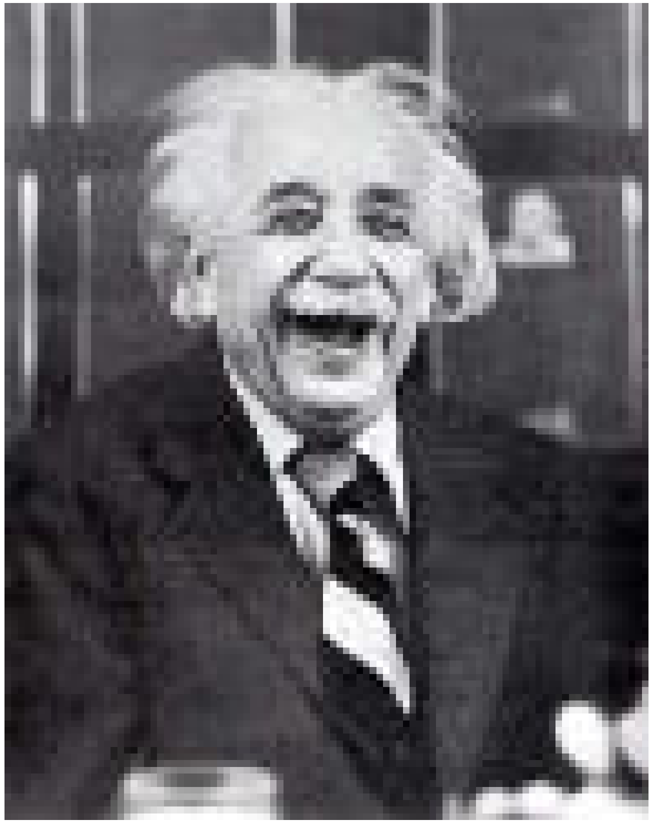
Verschränkung / Entanglement

$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right)$$

Erwin Schrödinger

- **non-separable** quantum states
- state describes **only joint correlations**
- no information on individual subsystems

Naturwissenschaften **23**, 807 (1935)



Entanglement in particular shows that a quantum mechanical description of physical reality is incomplete!

John Bell (1964)

That is correct. However, it **cannot be completed (in a reasonable way)**!

Bell's Theorem / GHZ Theorem

J. S. Bell, Physics 1, 1 (1964)
Greenberger, Horne, Zeilinger (1989)

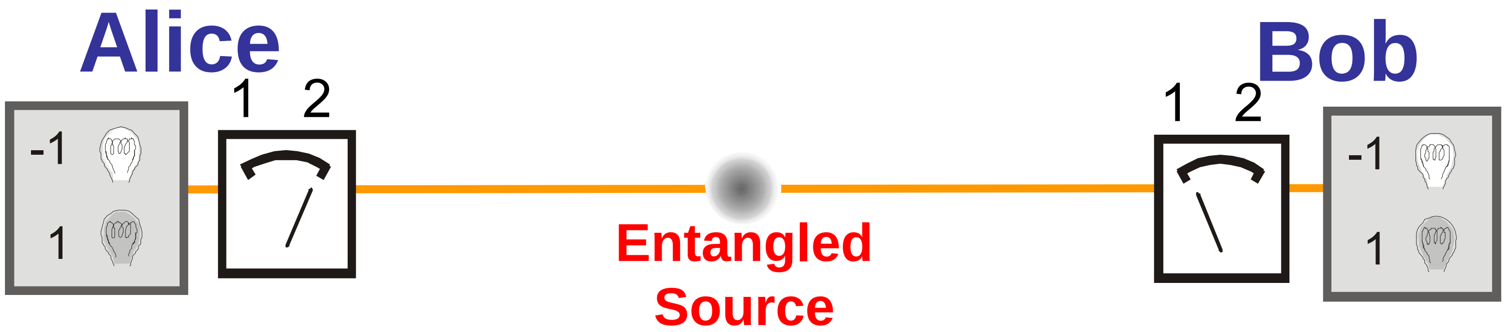
A) Predictions of quantum theory are correct

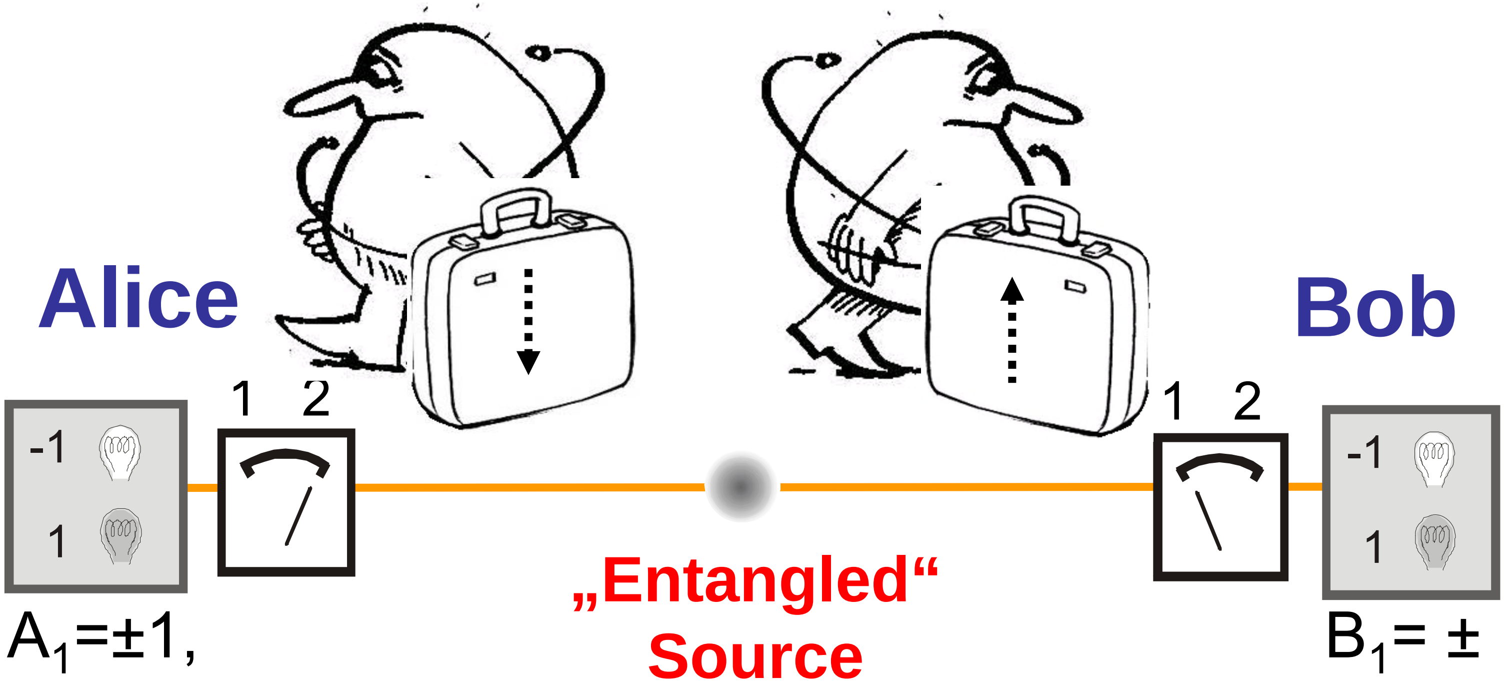
B) **Realism:** The outcome of *any* measurement depends on properties carried by the system prior to and independent of the measurement

C) **Locality:** The outcome of any meaurement is independent of actions in space-like separated regions.

Bell's theorem: granted A), either B) or C) or both fail

⟶ ***experimentally testable using entangled particles***





$A_1 = \pm 1$,
$A_2 = \pm 1$

$B_1 = \pm 1$,
$B_2 = \pm 1$

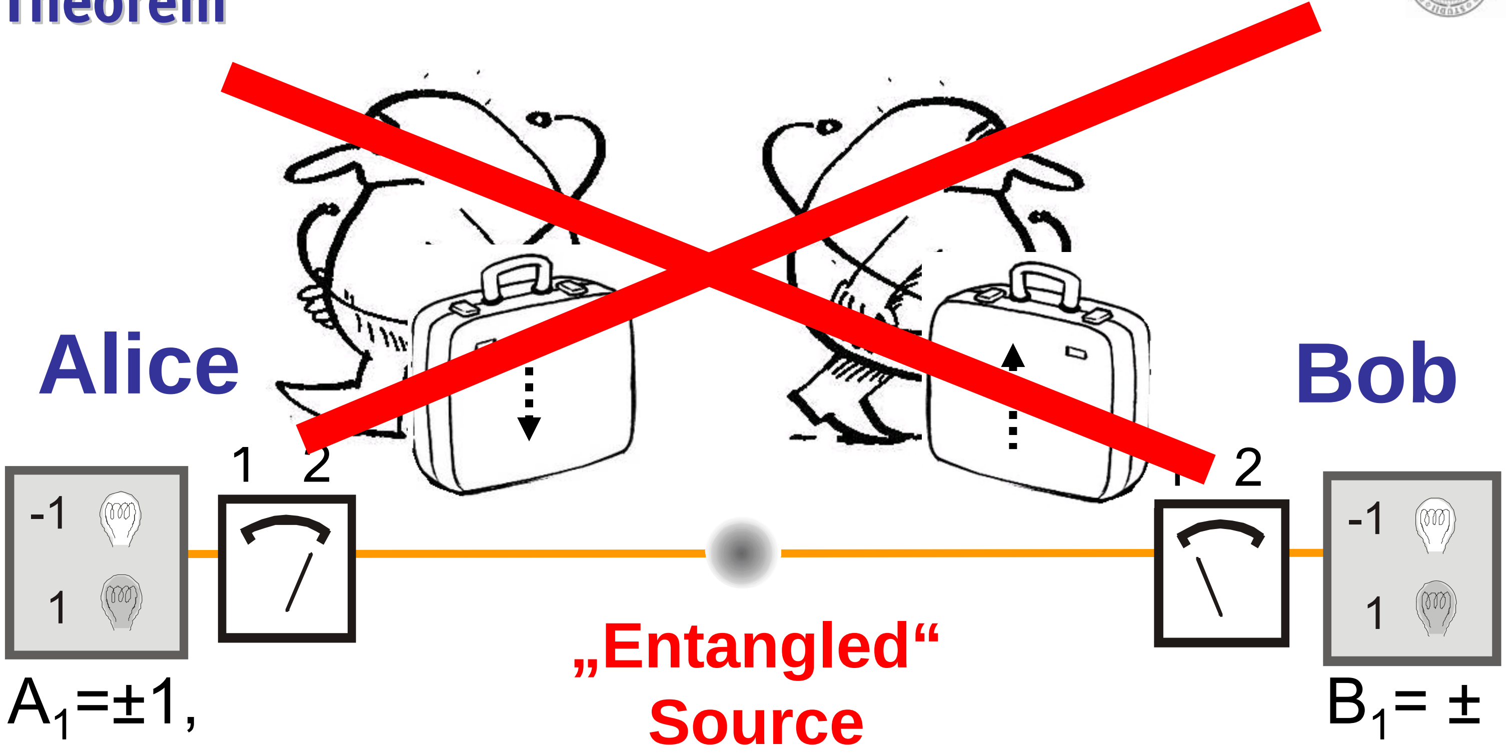
Correlation function: $E_{21} = p(A_2B_1=1) - p(A_2B_1=-1)$

Local Realism: $E_{11} + E_{12} + E_{21} - E_{22} \leq 2$

Quantum Mechanics: $2\sqrt{2}$

Bell 1964, CHSH 1969, Bell 1971, CH 1974, GHZ 1989

Bell's Theorem



$A_1 = \pm 1$, $A_2 = \pm 1$

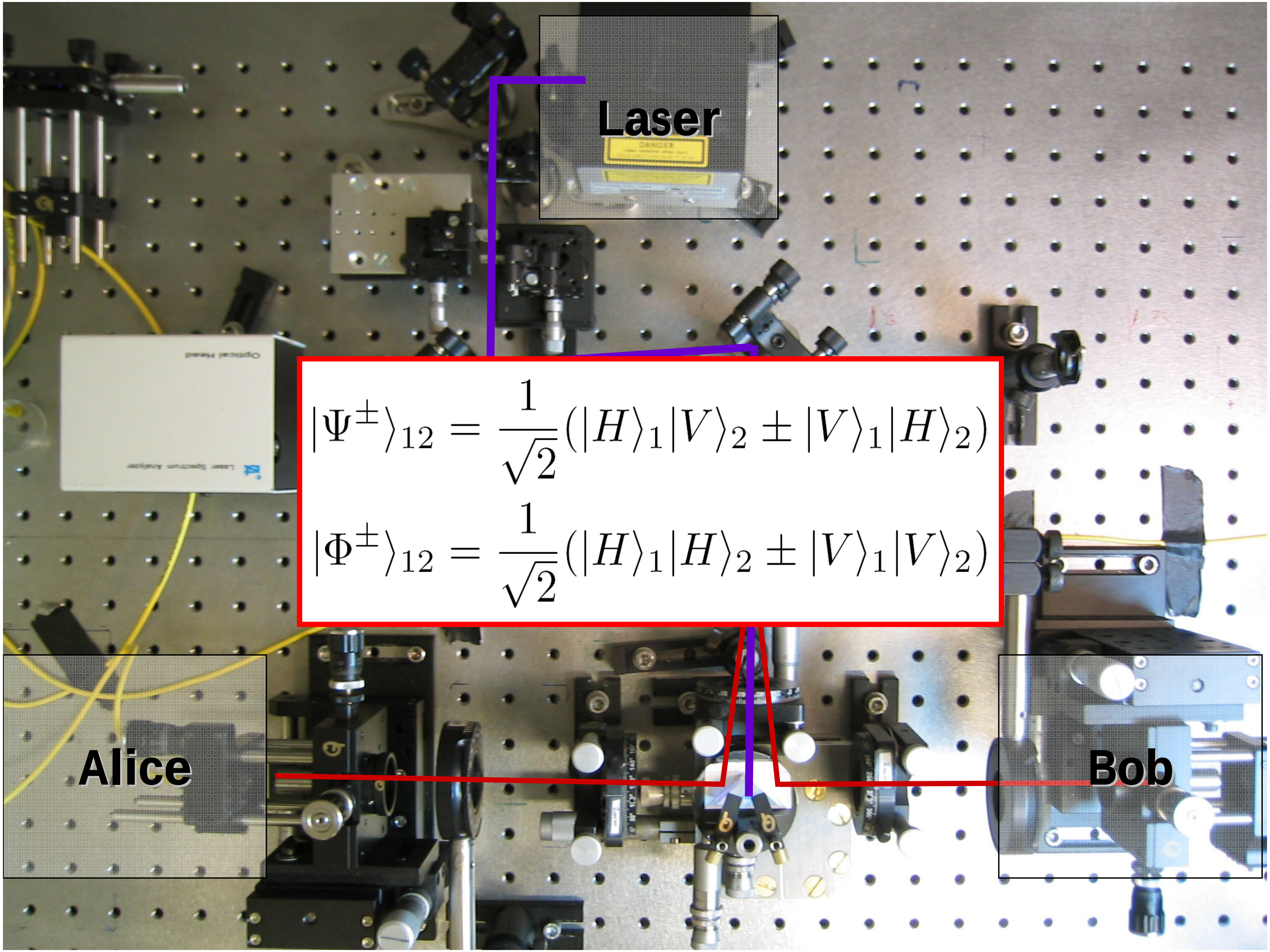
$B_1 = \pm 1$, $B_2 = \pm 1$

Correlation function: $E_{21} = p(A_2 B_1 = 1) - p(A_2 B_1 = -1)$

Local Realism: $E_{11} + E_{12} + E_{21} - E_{22} \leq 2$

Quantum Mechanics: $2\sqrt{2}$

Bell 1964, CHSH 1969, Bell 1971, CH 1974, GHZ 1989



$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2)$$

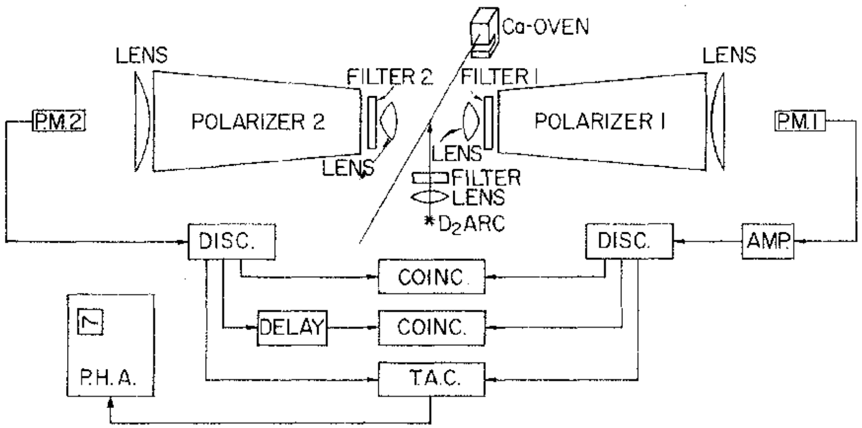
Bell Experiments

Experimental Test of Local Hidden-Variable Theories*

Stuart J. Freedman and John F. Clauser
Department of Physics and Lawrence Berkeley Laboratory, University of California, Berkeley, California 94720

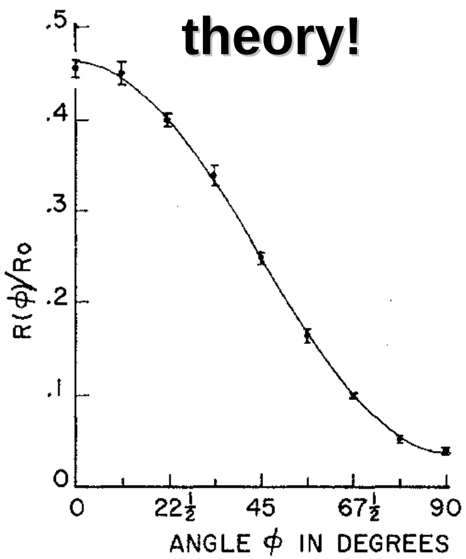
(Received 4 February 1972)

We have measured the linear polarization correlation of the photons emitted in an atomic cascade of calcium. It has been shown by a generalization of Bell's inequality that the existence of local hidden variables imposes restrictions on this correlation in conflict with the predictions of quantum mechanics. Our data, in agreement with quantum mechanics, violate these restrictions to high statistical accuracy, thus providing strong evidence against local hidden-variable theories.



PRL **28**, 938 (1972)

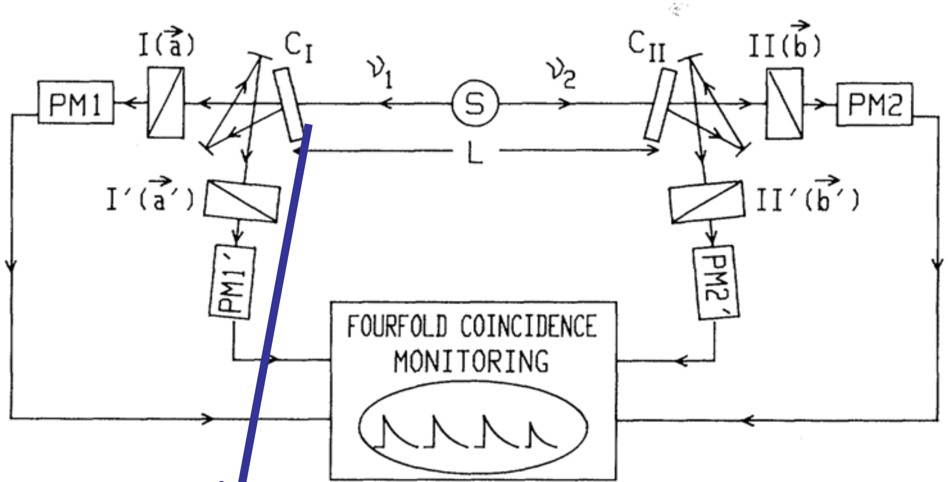
No deviation from quantum theory!



Experimental loopholes? (locality! Static settings)

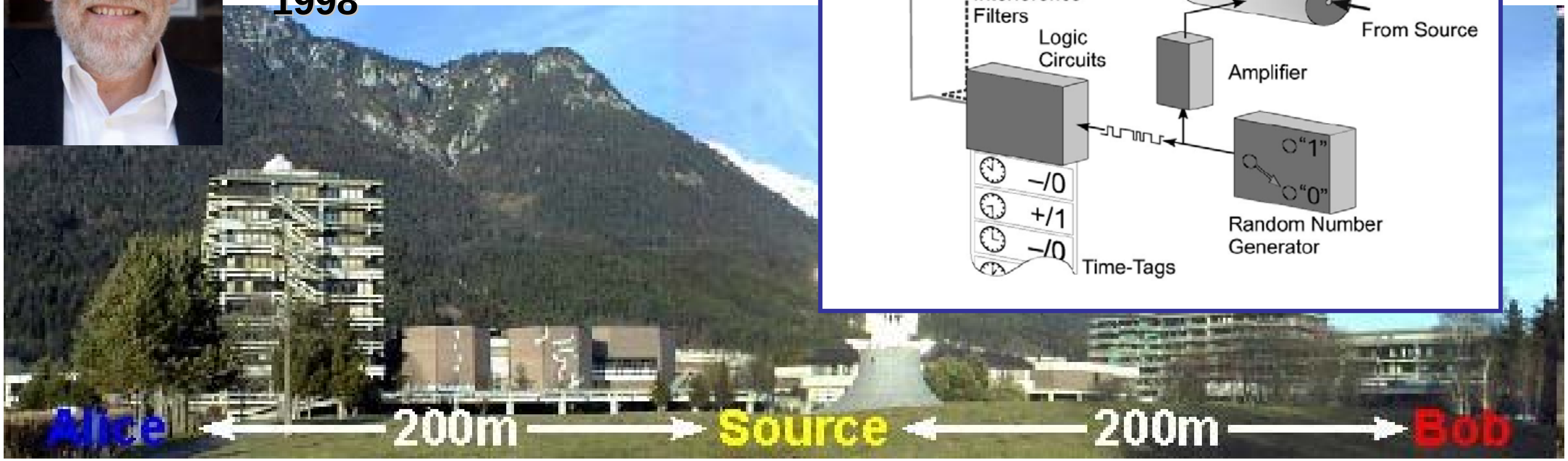
Bell Experiments under locality condition

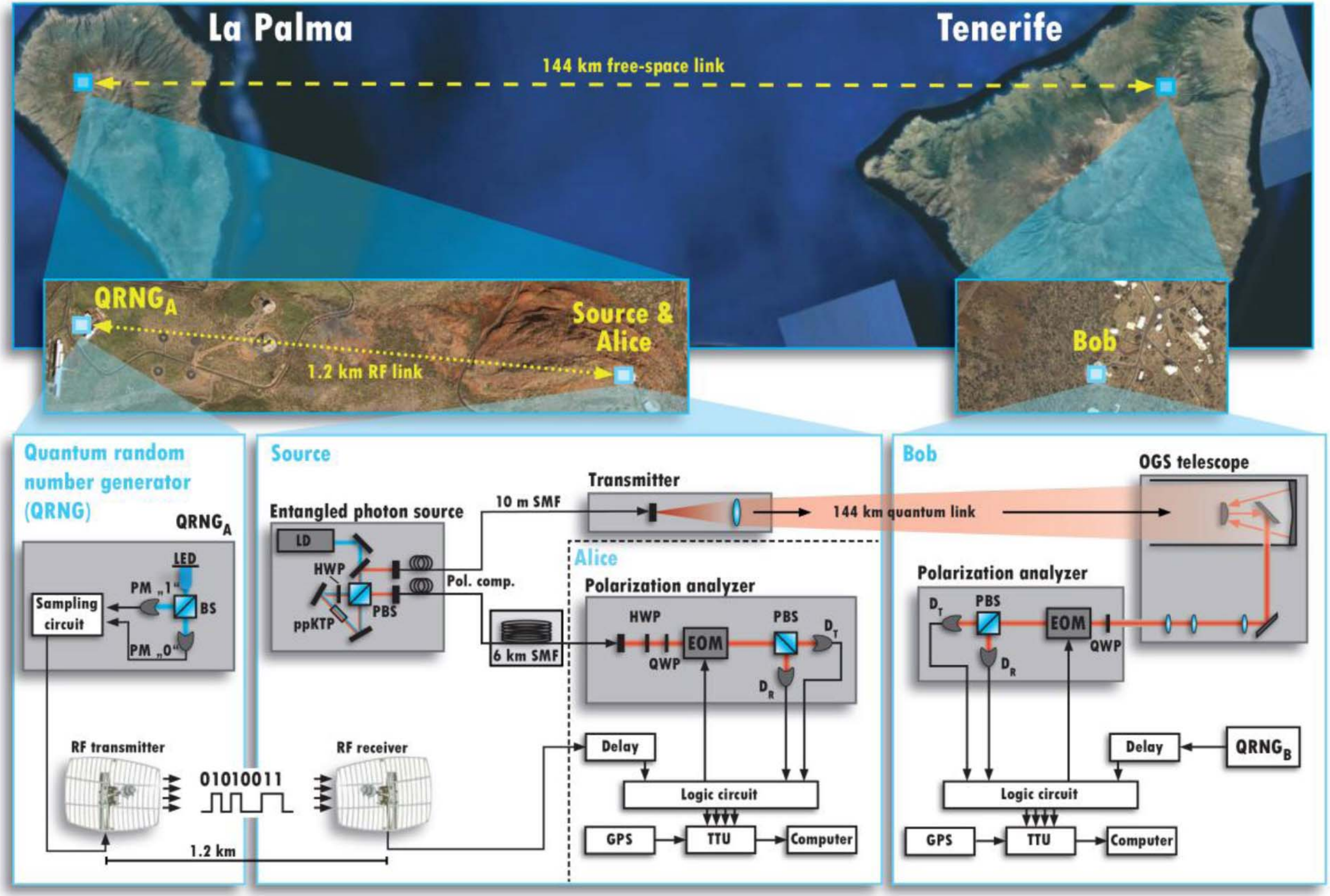
Random setting of measurement direction:
„spooky action“ or non-realism?



Aspect et al. 1984

Zeilinger et al. 1998





Entanglement over 144 km, Ursin, Weinfurter, Zeilinger et al., Nature Physics (2007)

Bell test over 144 km, Scheidl, Zeilinger et al. (2008)

What is left?

Local realistic theories are **inconsistent**

with predictions of quantum theory

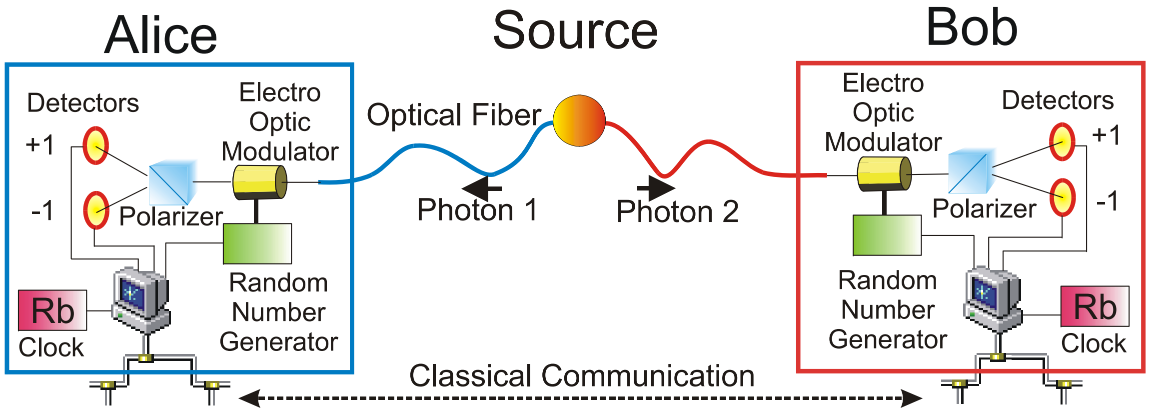
with experimental observation

Which assumption is wrong?

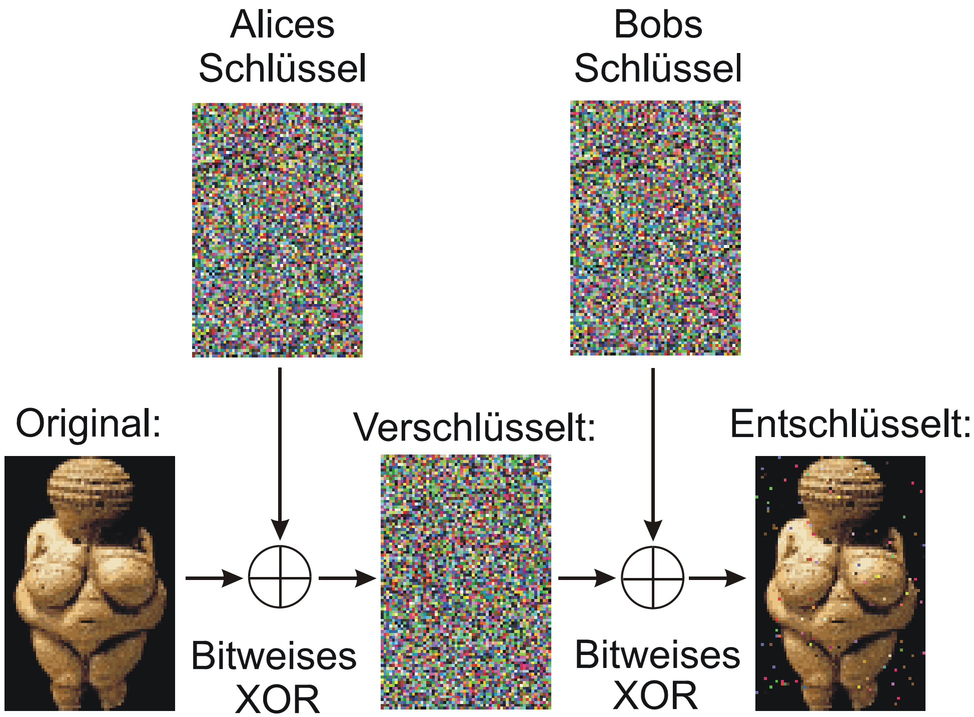
- **Locality**?
- **Realism**?
- Locality **and** realism?
- …other pre-assumptions? (Aristotelean logic?)

Quantum Cryptography

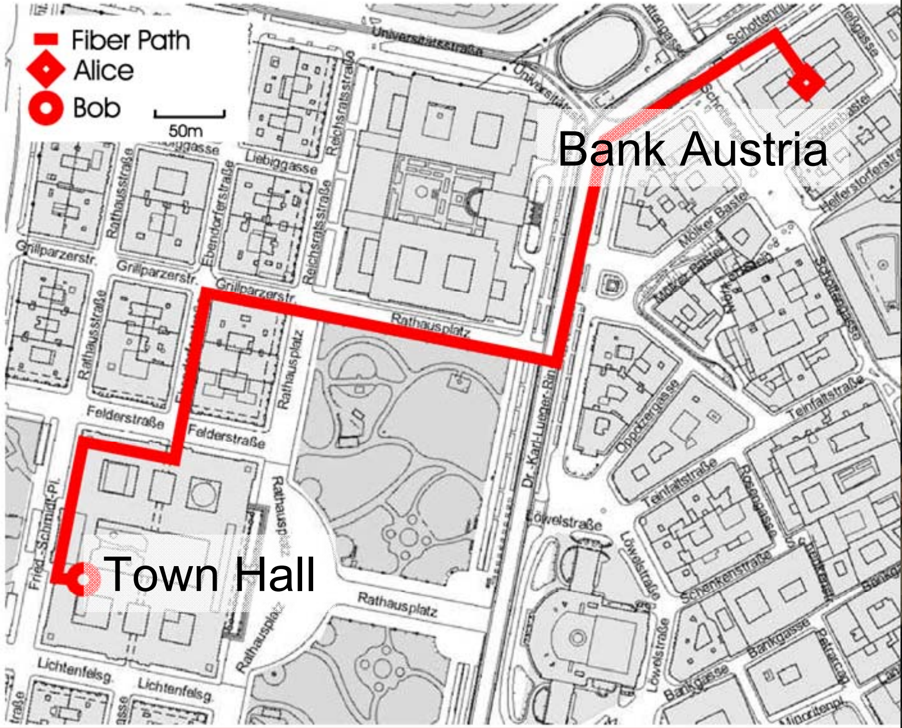
Entanglement creates shared random sequence (=key)

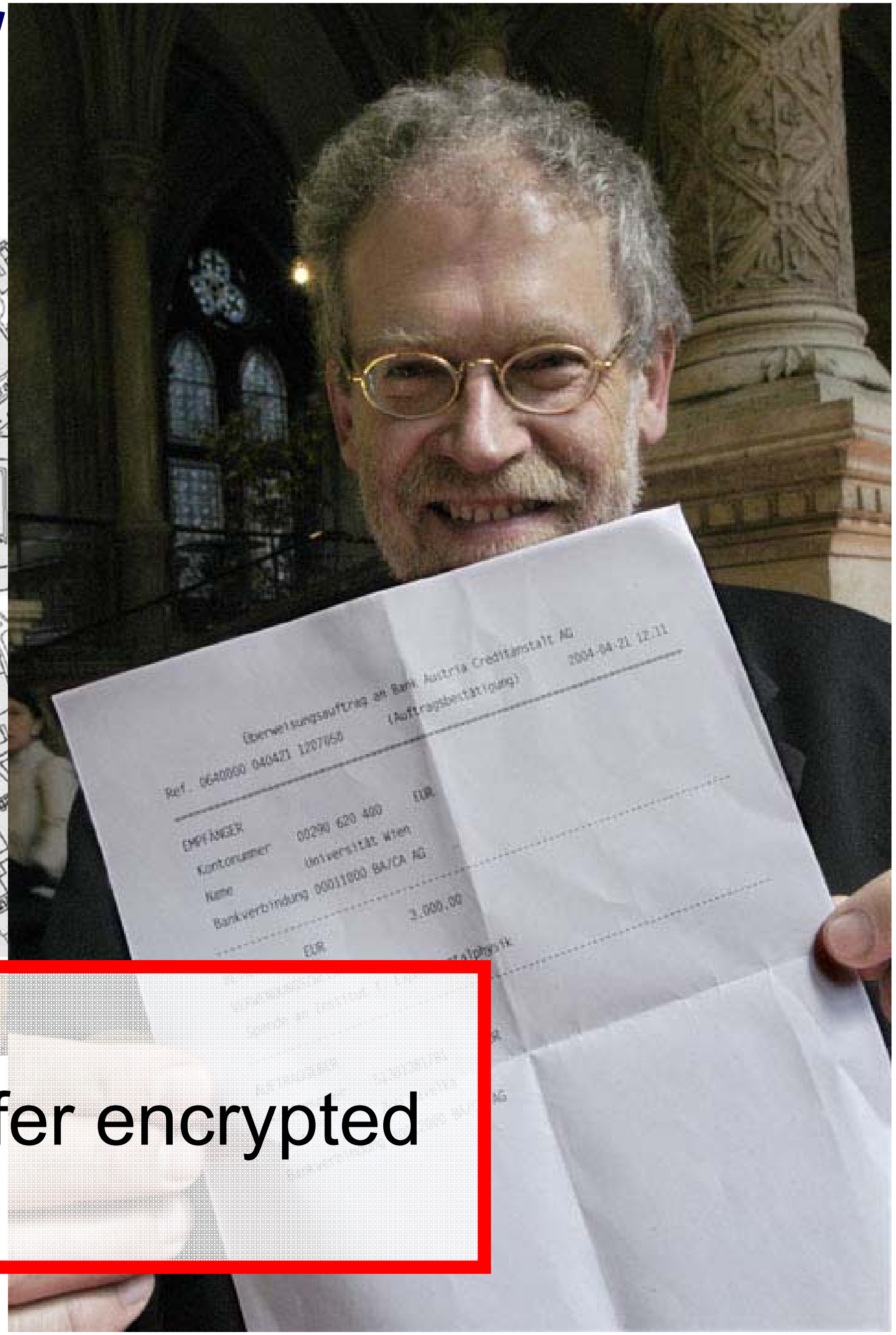


Security guaranteed e.g. by Bell inequality



Quantum Cryptography





Vienna, 21. April 2004:
Worldwide first bank transfer encrypted via quantum cryptography

SECOQC

Development of a Global Network for Secure Communication based on Quantum Cryptography
www.secoqc.net

42 European partners from University and Industry

Quantum Cryprography in Vienna's glass fibre network

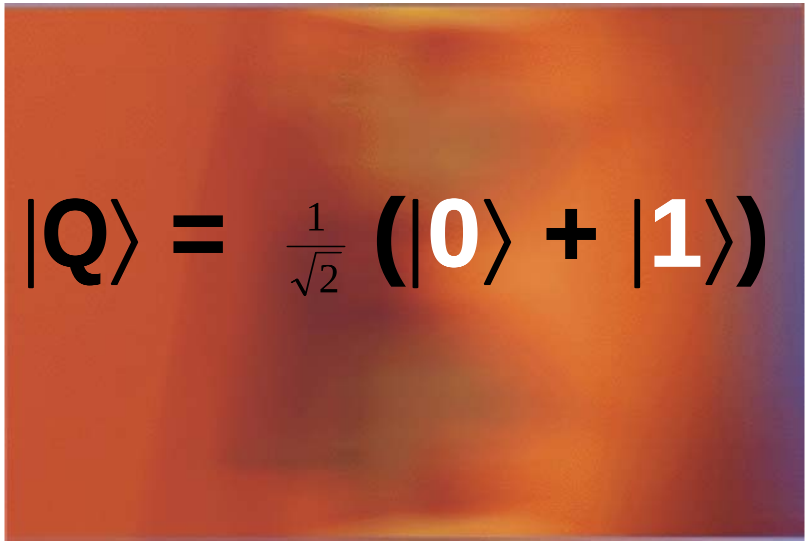
Quantum Information

Bit

„0“ or „1“

|computer> = 00000000
|computer> = 00000001
|computer> = 00000010

Qubit



„0“ and „1“

|Q-computer> = 00000000 + 00000001 + 00000010 + …

…

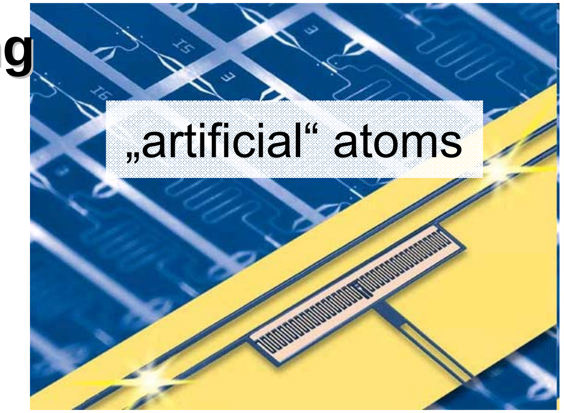
QUANTUM-HYBRID-TECHNOLOGIES:

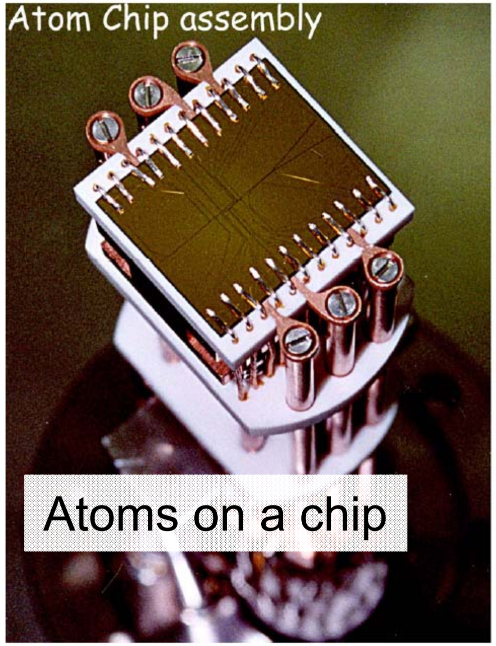
Quantum information processing

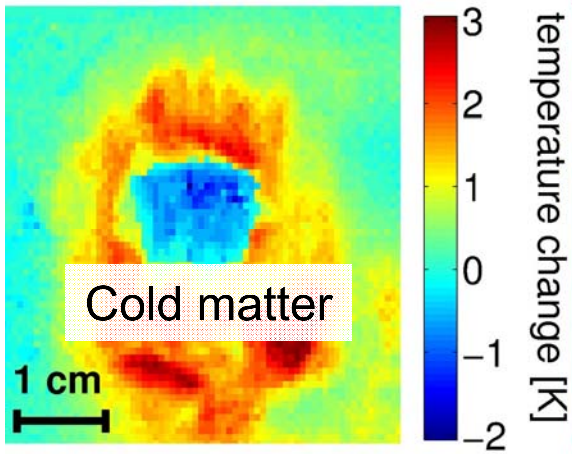
Quantum metrology

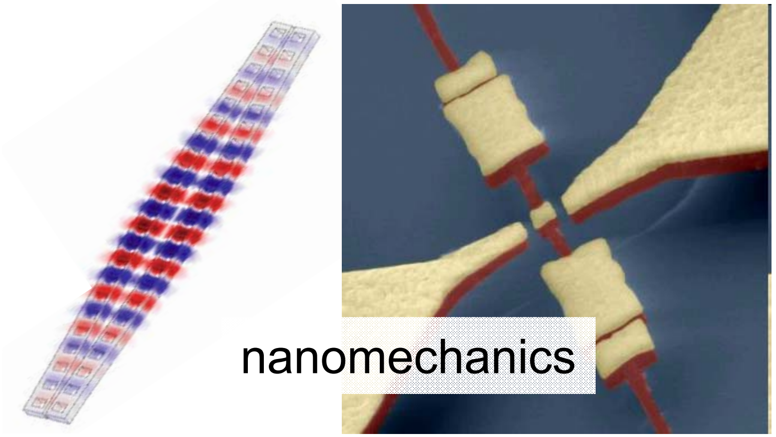
Quantum simulation

…









The zoology of quantum systems

- Photons
- Atoms/Ions
- neutrons, electrons
- Atomic gases, ultracold atoms
- Quantum dots
- Superconducting electronic circuits
- Spins in solid states
- Micro- and nanomechanical resonators
- …

Solid state!

Quantum entanglement: a key resource

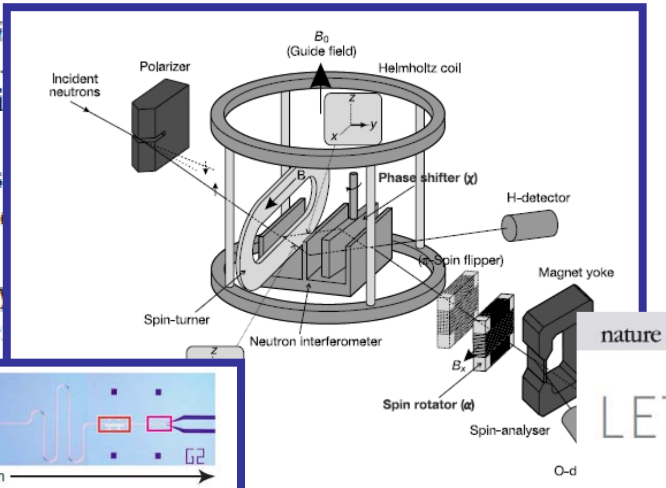
universität wien

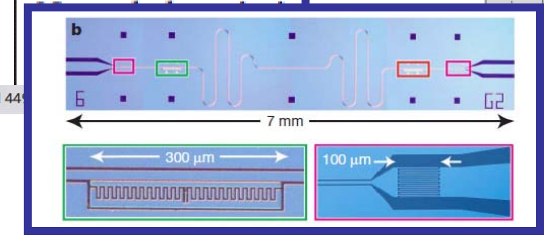
Violation of a Bell-like inequality in single-neutron interferometry

Yuji Hasegawa[1], Rudolf Loidl[1,2], Gerald Badurek[1], Matthias Baron[1,2] & Helmut Rauch[1]

[1] *Atominstitut der Österreichischen Universitäten, Stadionallee 2, A-1020 Wien, Austria*
[2] *Institute Laue Langevi*

Non-local correlati been extensively Podolsky and Ros Many proposals an theories and the reported[3–7]; usuall recently an expe





LETTE

Coupling superconducting qubits via a cavity bus

J. Majer[1*], J. M. Chow[1*], J. M. Gambetta[1], Jens Koch[1], B. R. Johnson[1], J. A. Schreier[1], L. Frunzio[1], D. I. Schu
A. A. Houck[1], A. Wallraff[1†], A. Blais[1†], M. H. Devoret[1], S. M. Girvin[1] & R. J. Schoelkopf[1]

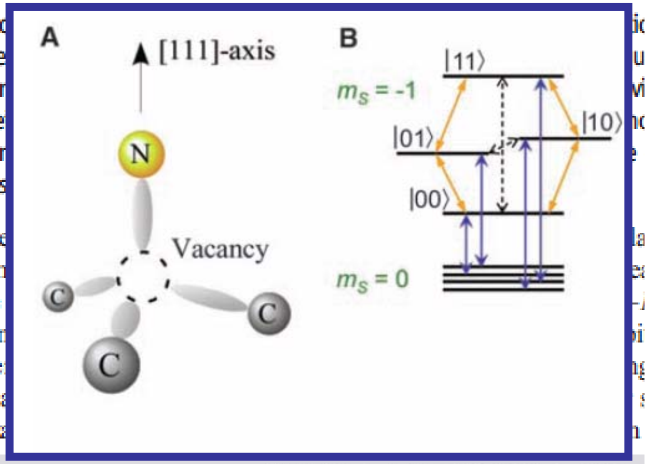
Superconducting circuits are promising candidates for constructing quantum bits (qubits) in a quantum computer; single-qubit operations are now routine[1,2], and several examples[3–9] of two-qubit interactions and gates have been demonstrated. These experi- charge and phase qubits, and inductive coupling for flu Therefore, these coupling mechanisms have been restricted interactions and couple only nearest-neighbour qubits. In th... we present a coupling that is realized with a cavity that is a distributed

REPORTS

Multipartite Entanglement Among Single Spins in Diamond

P. Neumann,[1*] N. Mizuochi,[2*] F. Rempp,[1] P. Hemmer,[3] H. Watanabe,[4] S. Yamasak
V. Jacques,[1] T. Gaebel,[1] F. Jelezko,[1] J. Wrachtrup[1]†

Robust entanglement at ro quantum technology. We de in a small quantum register spins are controlled via the center. Quantum correlatio room temperature, which is



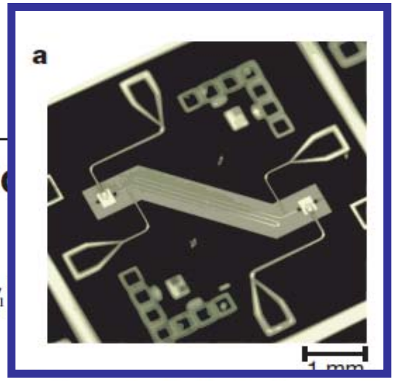
Schrödinger coined the to mean a peculiar n action in which the more physical objects car when separated. Since the retrieval of entanglement a have become of fundament

nature Vol 461|24 September 2009|doi:10.1038/nature08363

LETTERS

Violation of Bell's inequality in Josephson phase qubits

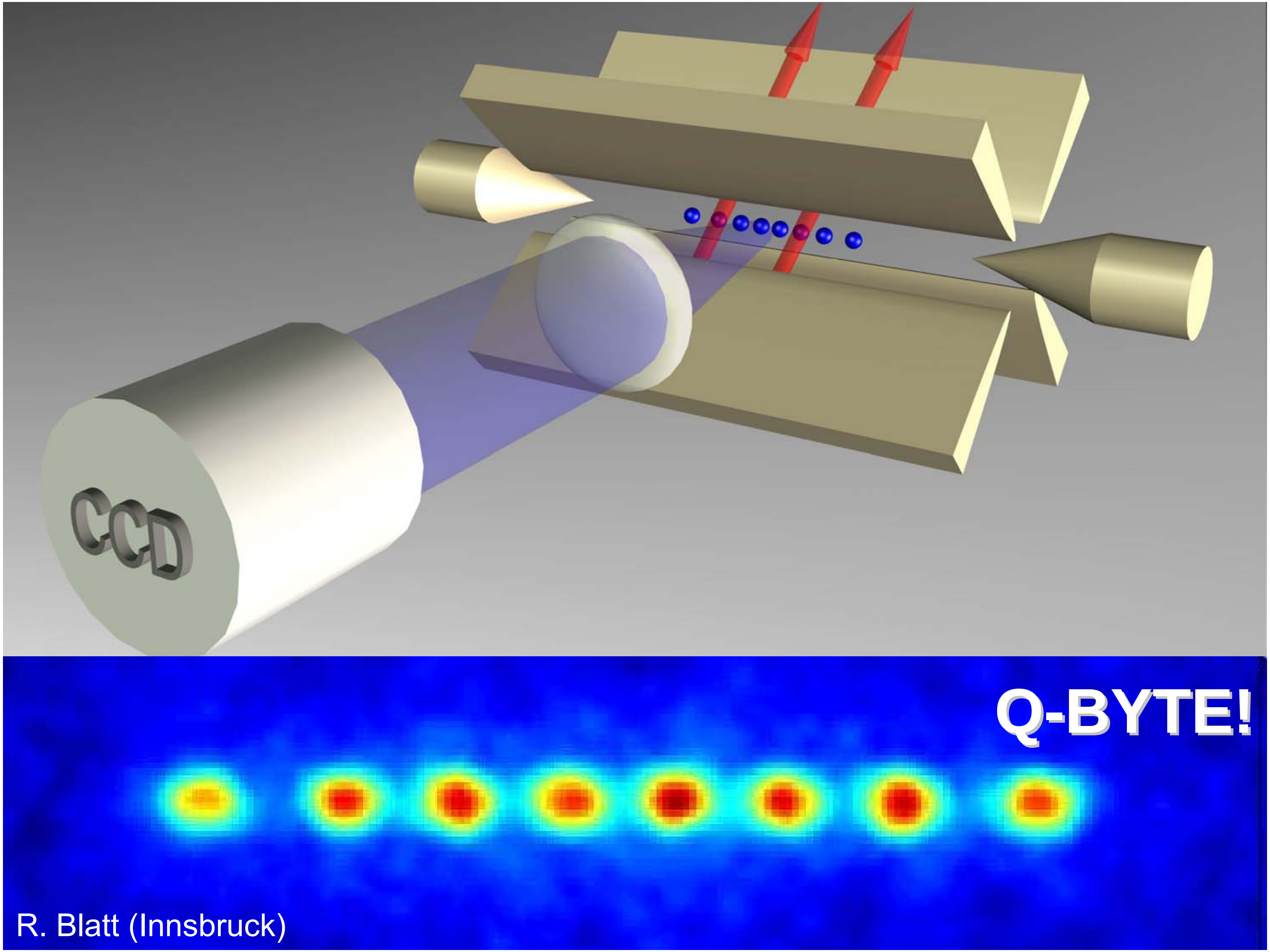
Markus Ansmann[1], H. Wang[1], Radoslaw C. Bialczak[1], Max Hofheinz[1],
D. Sank[1], M. Weides[1], J. Wenner[1], A. N. Cleland[1] & John M. Martinis[1]



The measurement process plays an awkward role in quantum mechanics, because measurement forces a system to 'choose' between possible outcomes in a fundamentally unpredictable manner. Therefore, hidden classical processes have been considered as possibly predetermining measurement outcomes while preserving their statistical distributions. However, a quantitative

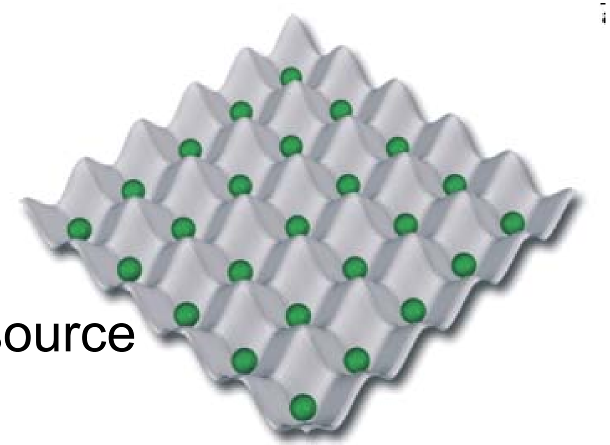
$$S = E(a, b) + E(a', b) - E(a, b') + E(a', b') \quad (2)$$

Classical (predetermined) outcomes result in a Bell signal $|S| \leq 2$, whereas quantum mechanics permits a larger signal $|S| \leq 2\sqrt{2} = 2.828$, for the appropriate measurement axes. Completely random outcomes result in $S = 0$. An experiment returns a Bell violation if $|S| > 2$, and

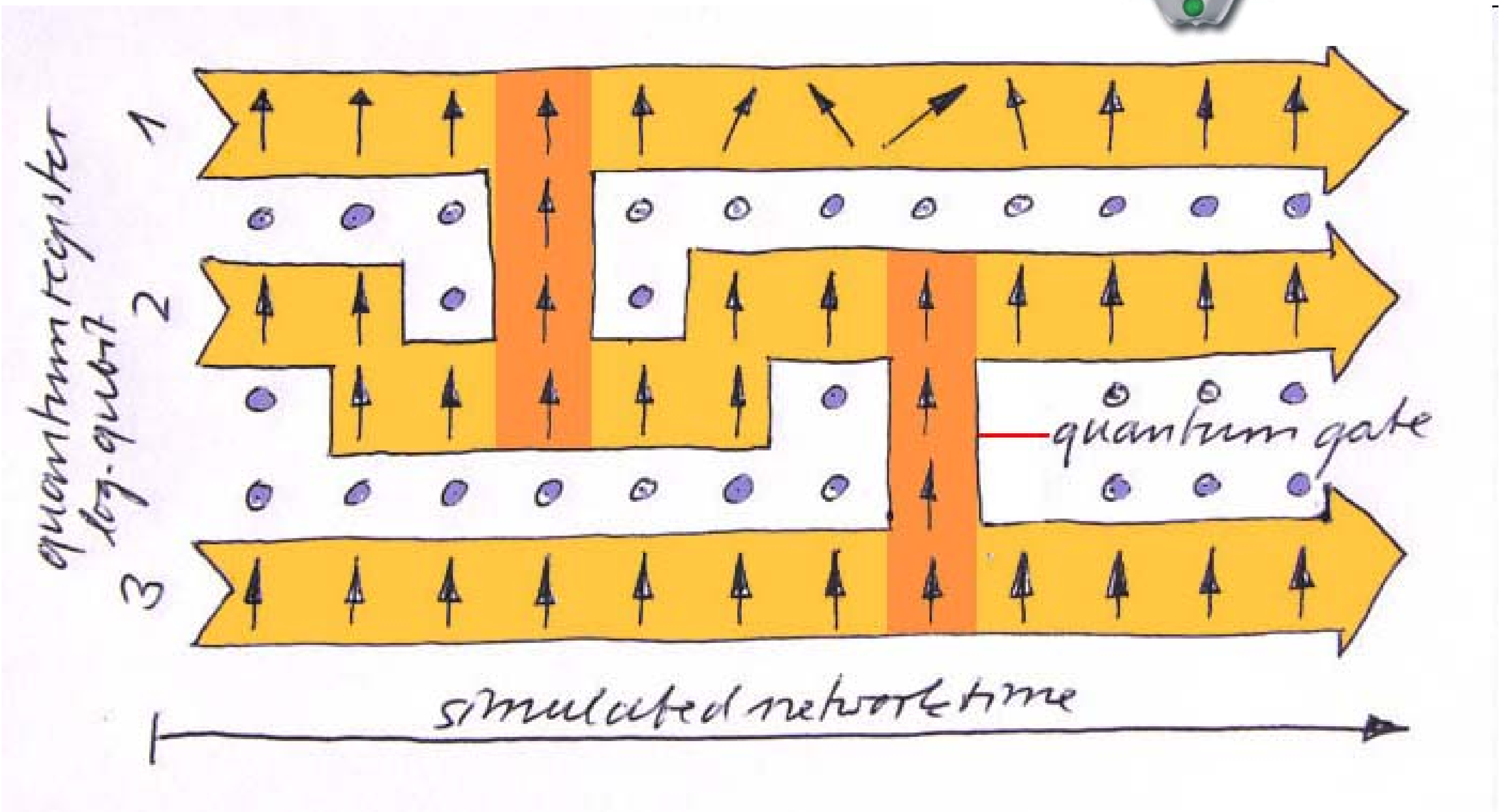

CCD
Q-BYTE!
R. Blatt (Innsbruck)

„One-Way“ Quantum Computer

(Raussendorff & Briegel 1998;
exp: Walther, Zeilinger 2005)



Multi-particle Entanglement as a universal resource



Mechanical Quantum Hybrids for QIPC

universität wien

Quantum information: mechanical quantum bus*

mechanical modes ↔ photons, charge, magnetic flux, atoms

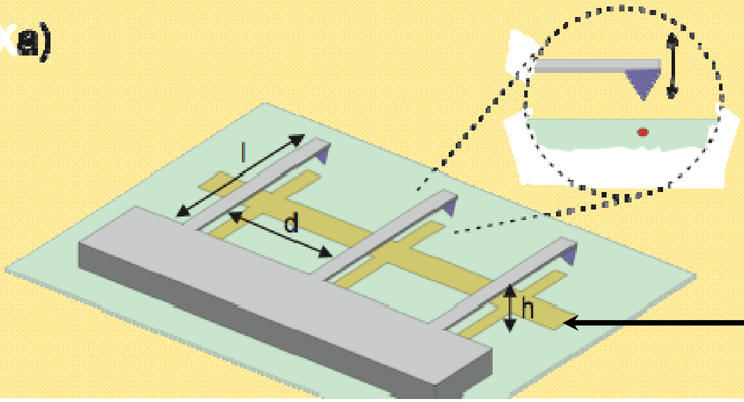
* Requires strong coupling regime;
see e.g. Gröblacher et al., Nature 2009

Long-range spin-spin interactions mediated by electrically coupled nano-resonator arrays

quant-ph 0908.0316 (2009)

Peter Rabl[1], Frank Koppens[2], Jack G. E. Harris[3], Peter Zoller[4], and Mikhail D. Lukin[1,2]

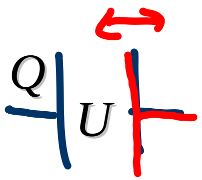
a)

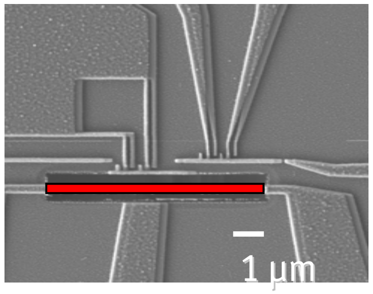


- cantilever with magnetic tip
- NV centers as qubits (+ microwave)
- capacitive coupling of cantilevers: phonon bus

Mechanics coupled to quantum systems

charge





force

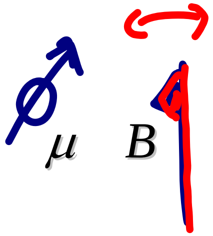
$$F = \frac{Q \cdot U}{d}$$

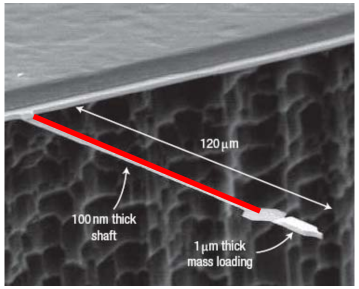
examples

single electron (SSET)

single electron (Cooper-Pair Box) < 50 aN

spin



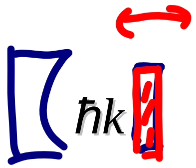


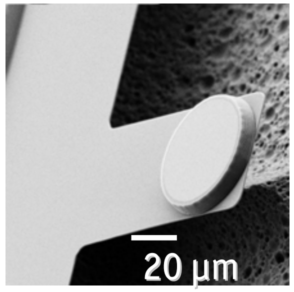
$$F = \mu \cdot \nabla B$$

single atom / electron spin < 10^2 aN

single nuclear spin < 0.05 aN

photon momentum

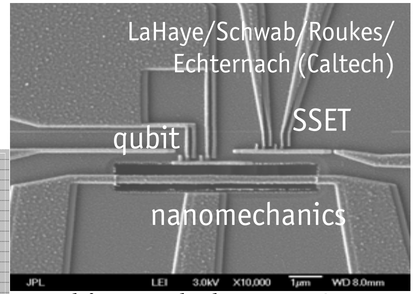




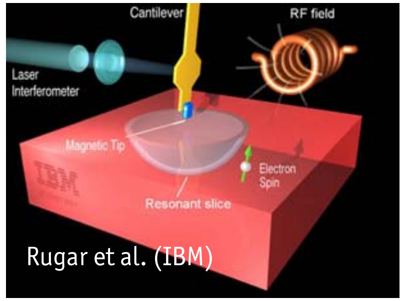
$$F = \frac{2\hbar k}{t_{cav}}$$

single photon (optical cavity) ~ 10^3 aN

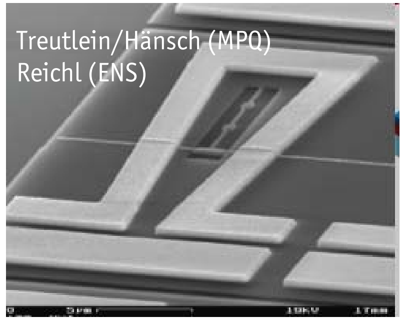
single photon (MW cavity) ~ 10^{-3} aN



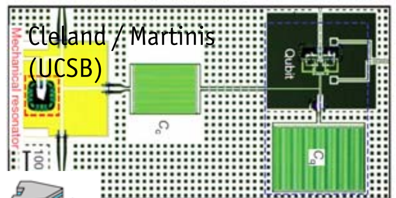
qubit coupled to NEMS

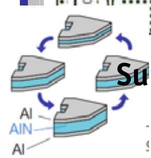


single electron spin - MOMS



BEC coupled to MEMS





Superconducting phase qubit and MEMS

Mechanical Systems IN the quantum regime

universität wien

doi:10.1038/nature08967 nature

ARTICLES

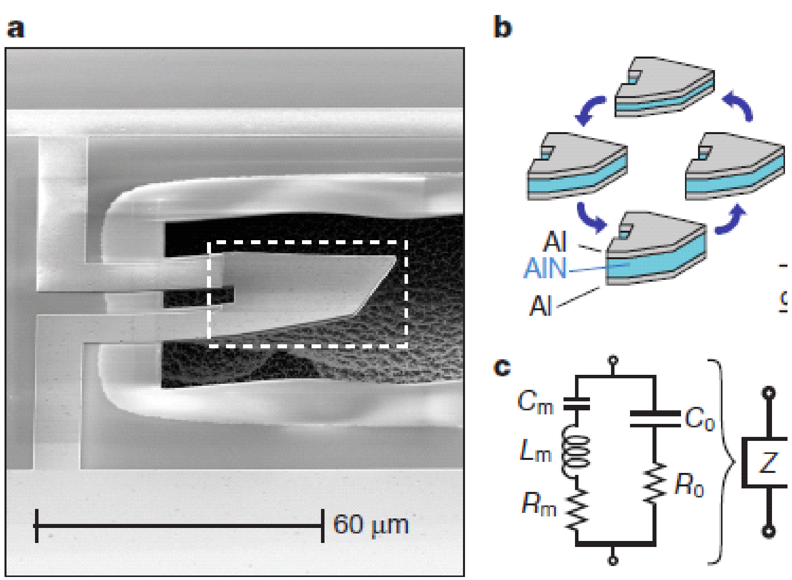
Quantum ground state and single-phonon control of a mechanical resonator

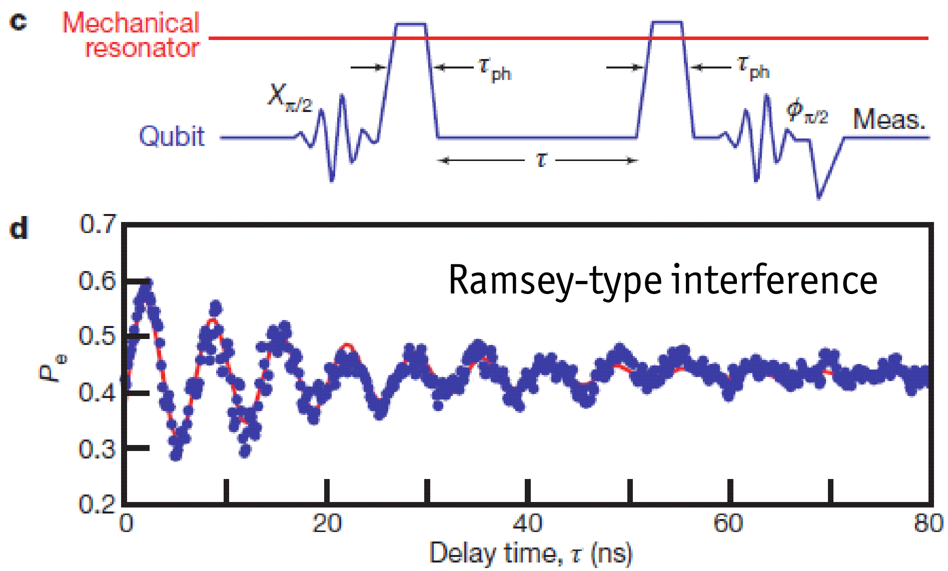
A. D. O'Connell[1], M. Hofheinz[1], M. Ansmann[1], Radoslaw C. Bialczak[1], M. Lenander[1], Erik Lucero[1], M. Neeley[1], D. Sank[1], H. Wang[1], M. Weides[1], J. Wenner[1], John M. Martinis[1] & A. N. Cleland[1]

Quantum mechanics provides a highly accurate description of a wide variety of physical systems. However, a demonstration that quantum mechanics applies equally to macroscopic mechanical systems has been a long-standing challenge, hindered

6 GHz piezo vibration → n ~ 0.07 @ 20 mK

Cleland/Martinis groups (UCSB); April 2010



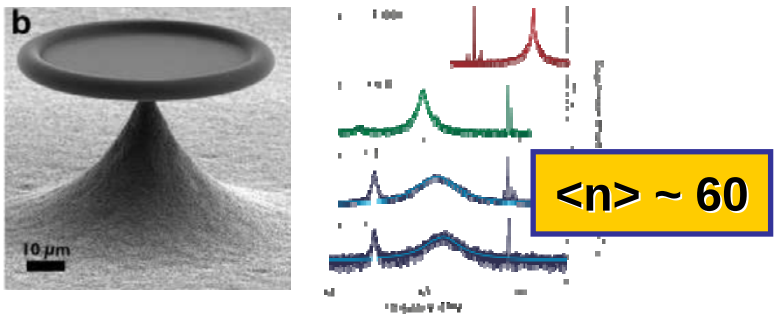


Mechanical systems CLOSE TO the quantum regime

Micromechanics close to the quantum ground state

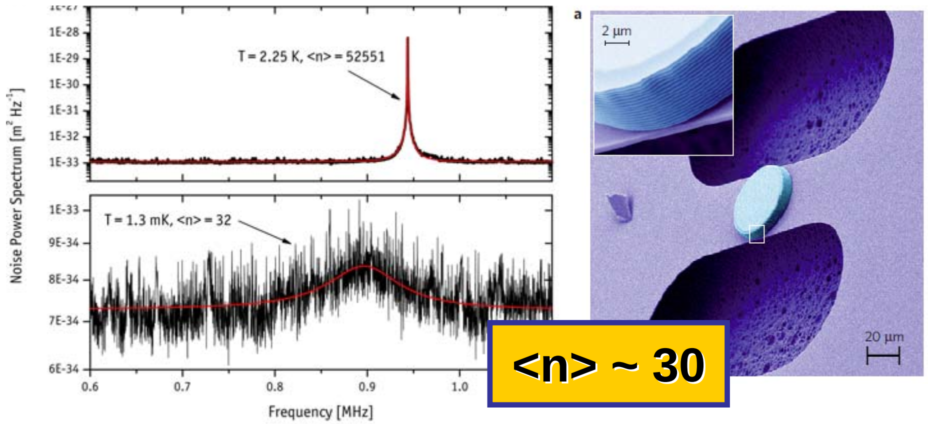
→ Laser cooling by optical photons

Schliesser et al., ***Nature Physics* 5**, 509 (2009)



Munich (Kippenberg group):
- Microtoroidal mechanics
- Sensing close to the uncertainty limit

Gröblacher et al., ***Nature Physics* 5**, 485 (2009)

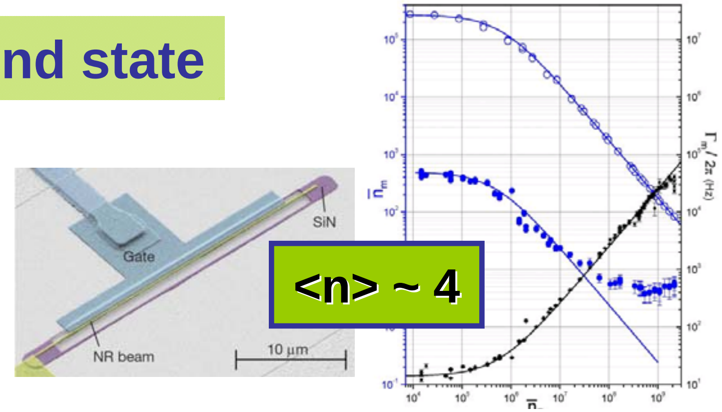


Vienna (Aspelmeyer group):
- Ultracold micromechanics with Bragg mirror pads
- Laser cooling in a cryogenic cavity

Nanomechanics close to the quantum ground state

→ Laser cooling by microwave photons

Caltech (Schwab group):
- Nanomechanical resonator inside a superconducting microwave cavity
- precooling in dilution cryostat



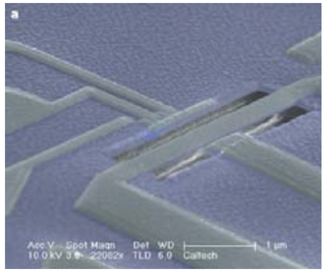
Rocheleau et al., ***Nature* 463**, 72 (2010)

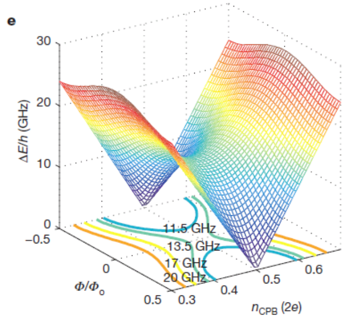
Mechanical coupling to quantum systems

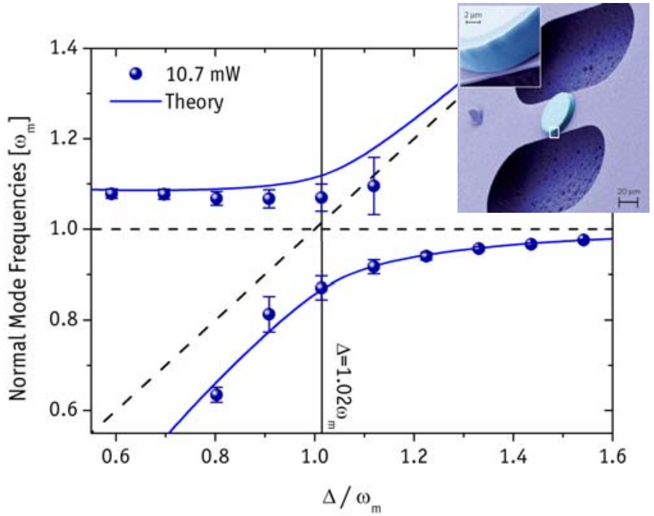
LaHaye et al., ***Nature* 459**, 960 (2009)

Nanomechanical measurements of a superconducting qubit

M. D. LaHaye[1], J. Suh[1], P. M. Echternach[3], K. C. Schwab[2] & M. L. Roukes[1]







Strong mechanical coupling

Gröblacher et al., ***Nature* 460**, 724 (2009)

Observation of strong coupling between a micromechanical resonator and an optical cavity field

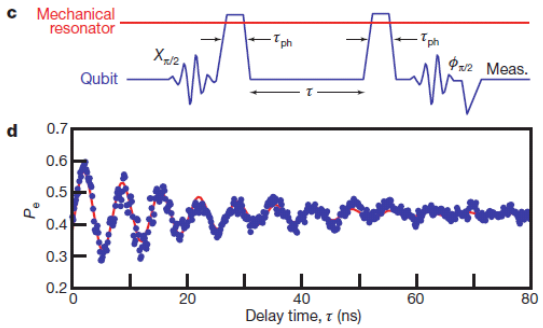
Simon Gröblacher[1,2], Klemens Hammerer[3,4], Michael R. Vanner[1,2] & Markus Aspelmeyer[1]

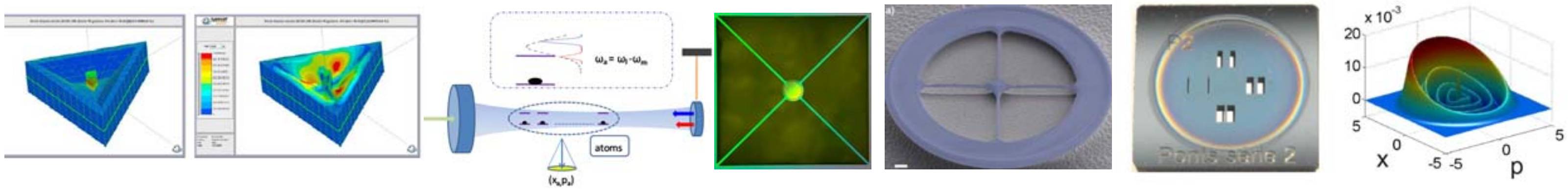
Strong mechanical coupling to quantum systems

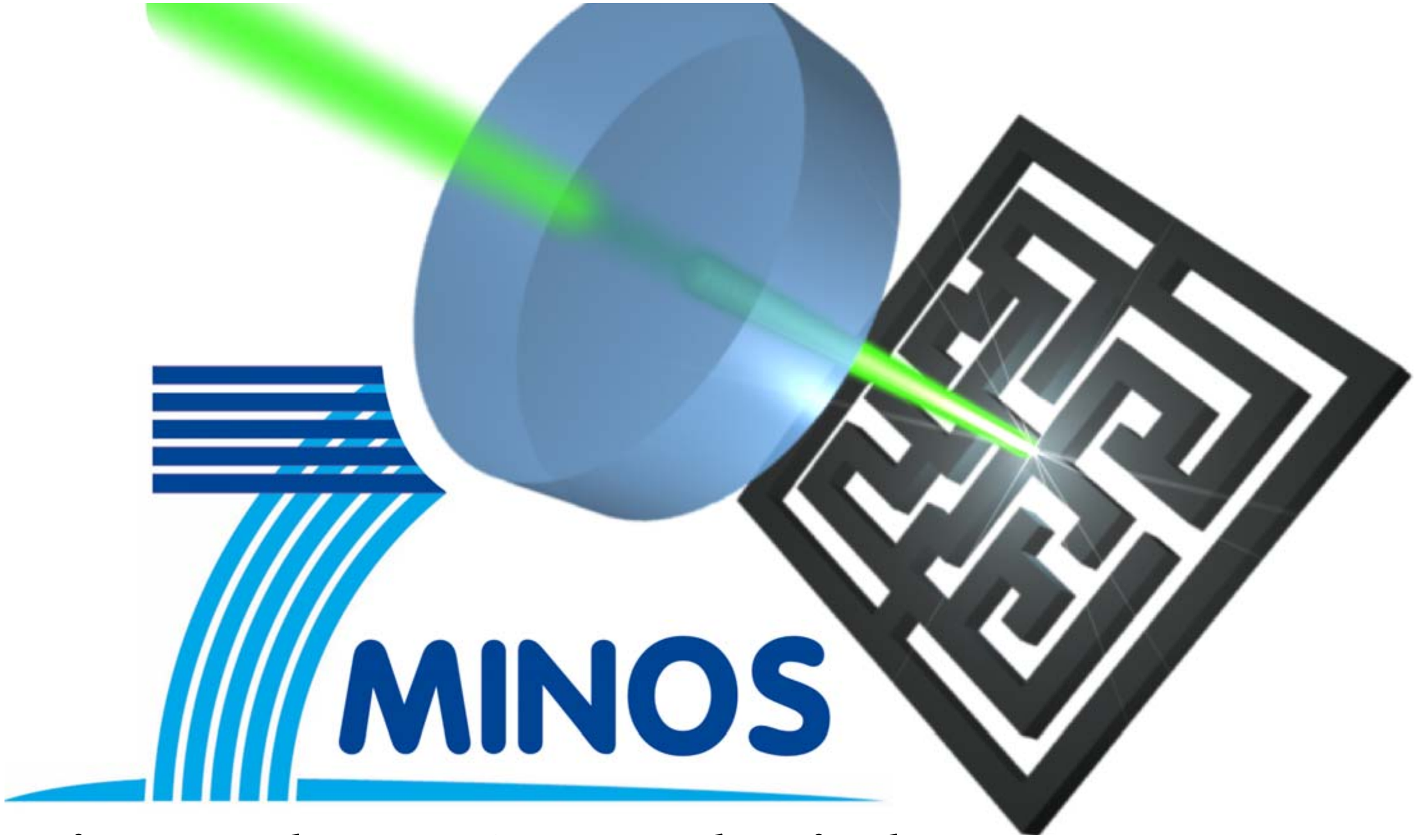
O'Connell et al., ***Nature***, advance online publication

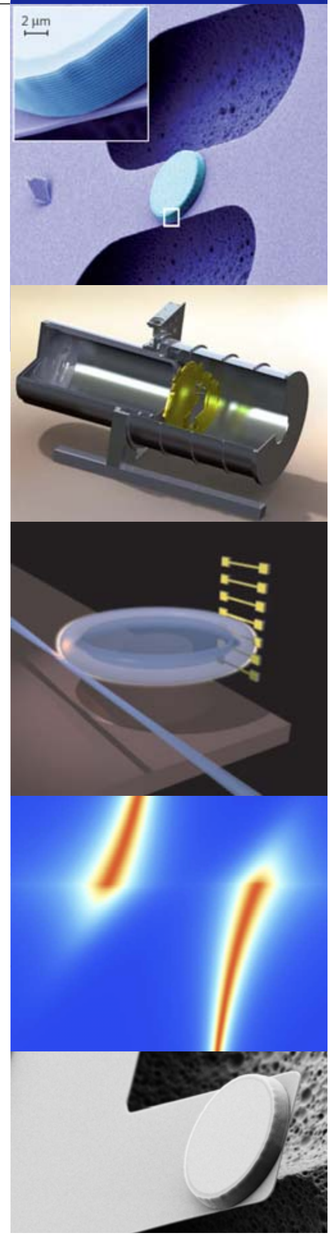
Quantum ground state and single-phonon control of a mechanical resonator

A. D. O'Connell[1], M. Hofheinz[1], M. Ansmann[1], Radoslaw C. Bialczak[1], M. Lenander[1], Erik Lucero[1], M. Neeley[1], D. Sank[1], H. Wang[1], M. Weides[1], J. Wenner[1], John M. Martinis[1] & A. N. Cleland[1]









Micro- and Nano-Optomechanical Systems for ICT and QIPC (MINOS)

an FP7 STREP Project of the FET-Open Initiative

10/2008 – 10/2011, 6 EU partners, 2.3M€
Worldwide first concerted effort, USA & Australia ramping up now

From quantum technology to quantum foundations

universität wien

articles

Experimental one-way quantum computing

P. Walther[1], K. J. Resch[1], T. Rudolph[2], E. Schenck[1*], H. Weinfurter[3,4], V. Vedral[1,5,6], M. Aspelmeyer[1] & A. Zeilinger[1,7]

[1]Institute of Experimental Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria
[2]QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, UK
[3]Department of Physics, Ludwig Maximilians University, D-80799 Munich, Germany
[4]Max Planck Institute for Quantum Optics, D-85741 Garching, Germany
[5]The Erwin Schrödinger Institute for Mathematical Physics, Boltzmanngasse 9, 1090 Vienna, Austria
[6]The School of Physics and Astronomy, University of Leeds, Leeds LS2 9JT, UK
[7]IQOQI, Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria
* Permanent address: Ecole normale supérieure, 45, rue d'Ulm, 75005 Paris, France

Standard quantum computation is based on sequences of unitary quantum logic gates that process qubits. The one-way quantum computer proposed by Raussendorf and Briegel is entirely different. It has changed our understanding of the requirements for quantum computation and more generally how we think about quantum physics. This new model requires qubits to be initialized in a highly entangled cluster state. From this point, the quantum computation proceeds by a sequence of single-qubit measurements

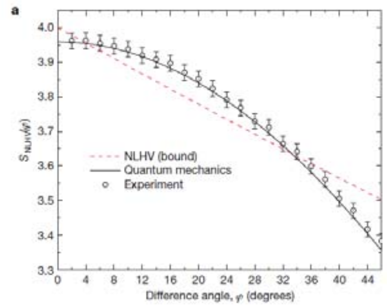
Vol 446 | 19 April 2007 | doi:10.1038/nature05677 nature

ARTICLES

An experimental test of non-local realism

Simon Gröblacher[1,2], Tomasz Paterek[3,4], Rainer Kaltenbaek[1], Časlav Brukner[1,2], Marek Żukowski[1,3], Markus Aspelmeyer[1,2] & Anton Zeilinger[1,2]

Most working scientists hold fast to the concept of 'realism'—a
independent of observation. But quantum physics has shattered
theorem, any theory that is based on the joint assumption of rea
affected by actions in space-like separated regions) is at varianc
entangled pairs of particles have amply confirmed these quantu
untenable. Maintaining realism as a fundamental concept would
that defy locality. Here we show by both theory and experiment
realistic theories is incompatible with experimentally observable
previously untested correlations between two entangled photon
proposed by Leggett for non-local realistic theories. Our result su
to be consistent with quantum experiments, unless certain intuit



nature Vol 443 | 21 September 2006 | doi:10.1038/natu

LETTERS

'Designer atoms' for quantum metrology

C. F. Roos[1,2], M. Chwalla[1], K. Kim[1], M. Riebe[1] & R. Blatt[1,2]

Entanglement is recognized as a key resource for quantum computation[1] and quantum cryptography[2]. For quantum metrology, the use of entangled states has been discussed[3–5] and demonstrated[6] as a means of improving the signal-to-noise ratio. In addition
efficient
scatterin
lation o
specific
an envi

and z, and where $\Theta(D, j)$ expresses the strength of the quadrupole moment in terms of a reduced matrix element[18].
Recently, quadrupole moments have been measured for $^{88}Sr^+$, $^{199}Hg^+$ and $^{171}Yb^+$ with a precision ranging from about 4% to 12%

nature Vol 463 | 7 January 2010 | doi:10.1038/nature08688

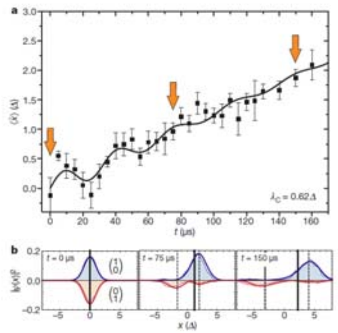
LETTERS

Quantum simulation of the Dirac equation

R. Gerritsma[1,2], G. Kirchmair[1,2], F. Zähringer[1,2], E. Solano[3,4], R. Blatt[1,2] & C. F. Roos[1,2]

The Dirac equation[1] successfully merges quantum mechanics with special relativity. It provides a natural description of the electron spin, predicts the existence of antimatter[2] and is able to reproduce accurately the spectrum of the hydrogen atom. The realm of the Dirac equation—relativistic quantum mechanics—is considered
ch as Klein's
ering motion
her predicted
nderstanding
serve in real

easily accessed e
over a wide ran
tivistic effects h
simulation of t
in solid-state ph
realized so far. A
Dirac equation[15]
Trapped ions
quantum simula
mental paramete

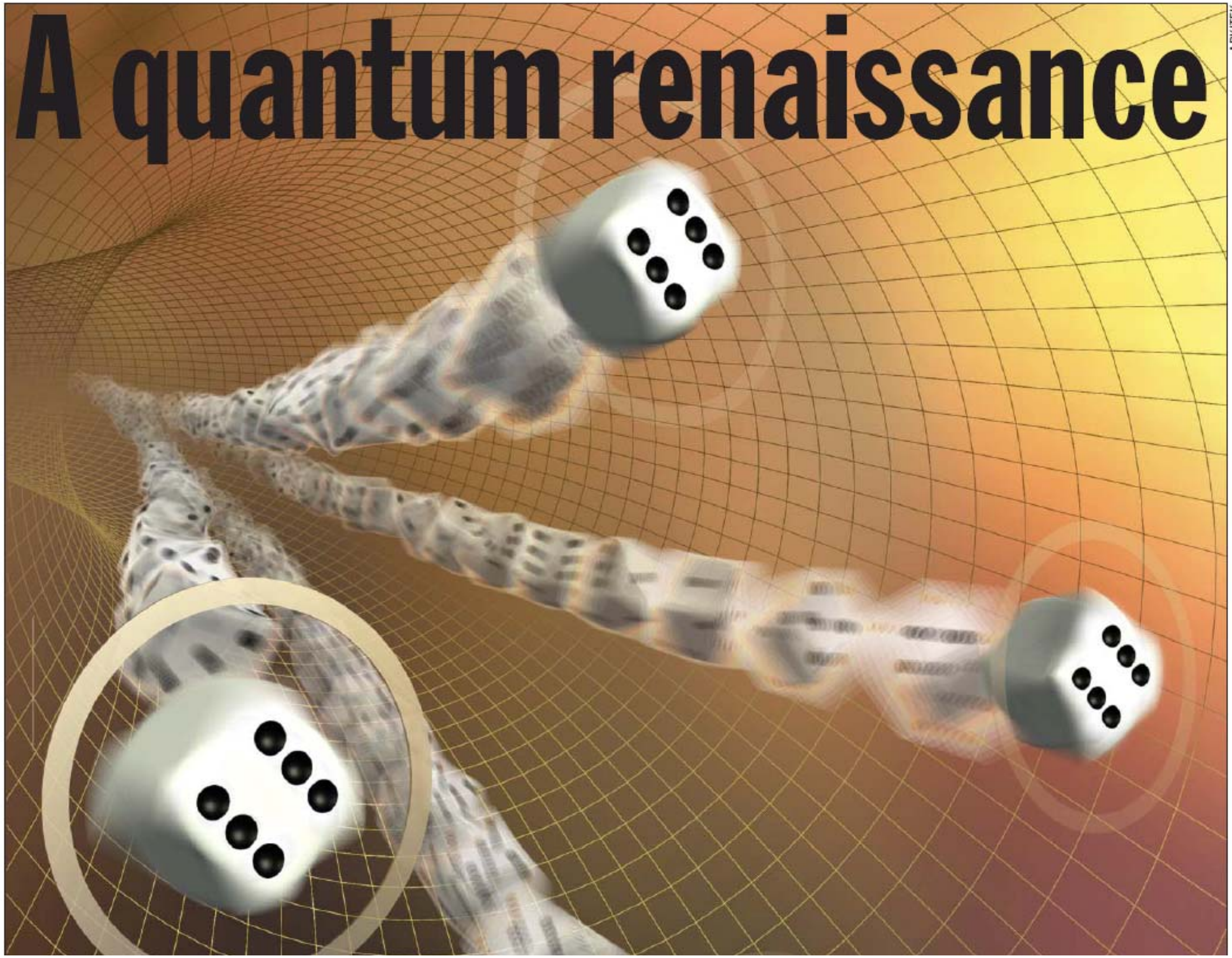


relativistic to non-relativistic dynamics. The high level of control of trapped-ion experimental parameters makes it possible to simulate textbook examples of relativistic quantum physics.

Aspelmeyer & Zeilinger

Physics World, July 2008

A quantum renaissance



Physicists can now routinely exploit the counterintuitive properties of quantum mechanics to transmit, encrypt and even process information. But as **Markus Aspelmeyer** and **Anton Zeilinger** describe, the technological advances of quantum information science are now enabling researchers to readdress fundamental puzzles raised by quantum theory

From quantum technology to quantum foundations

universität wien

Vol 444|2 November 2006|doi:10.1038/nature05273 nature

LETTERS

Self-cooling of a micromirror by radiation pressure

S. Gigan[1,2], H. R. Böhm[1,2], M. Paternostro[2]†, F. Blaser[2], G. Langer[3], J. B. Hertzberg[4,5], K. C. Schwab[4]†, D. Bäuerle[3]†, M. Aspelmeyer[1,2] & A. Zeilinger[1,2]

doi:10.1038/nature08967 nature

ARTICLES

Quantum ground state and single-phonon control of a mechanical resonator

A. D. O'Connell[1], M. Hofheinz[1], M. Ansmann[1], Radoslaw C. Bialczak[1], M. Lenander[1], Erik Lucero[1], M. Neeley[1], D. Sank[1], H. Wang[1], M. Weides[1], J. Wenner[1], John M. Martinis[1] & A. N. Cleland[1]

nature Vol 460|6 August 2009|doi:10.1038/na…

LETTERS

Observation of strong coupling between a micromechanical resonator and an optical cavity field

Simon Gröblacher[1,2], Klemens Hammerer[3,4], Michael R. Vanner[1,2] & Markus Aspelmeyer[1]

nature Vol 459|18 June 2009|doi:10.1038/nature08093

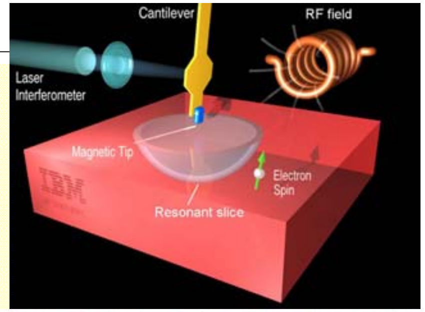
LETTERS

Nanomechanical measurements of a superconducting qubit

M. D. LaHaye[1], J. Suh[1], P. M. Echternach[3], K. C. Schwab[2] & M. L. Roukes[1]

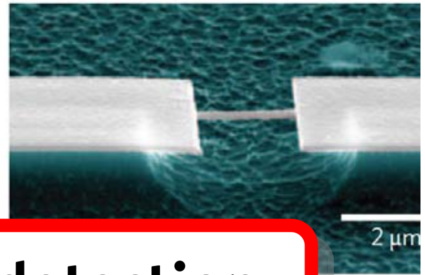
Mechanical quantum systems provide access to a **complete new parameter regime for experimental physics** (size, mass, sensitivity)

Mechanical (Quantum) Hybrids – for sensing



Today (existing technology)**:**

- **single electron-spin** detection via magnetic resonance
- **attometer-scale** displacement sensing (10^{-18} m)
- **zeptonewton-scale** force sensing (10^{-21} N)
- **yoctogram-scale** mass sensitivity (10^{-24} g)



Towards quantum limits of force- and displacement detection

Exploiting a new regime of (mechanical) sensing

→ **3D imaging of individual macromolecules** (Rugar, IBM)

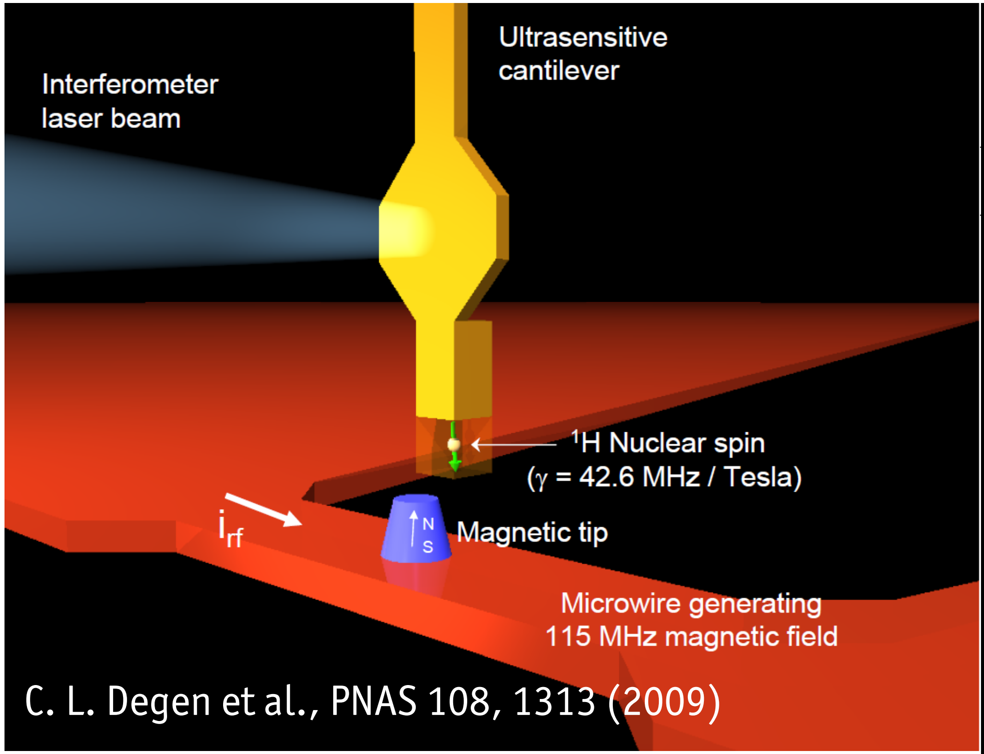
→ **Novel magnetometers based on spins in diamond** (Lukin, Harvard)

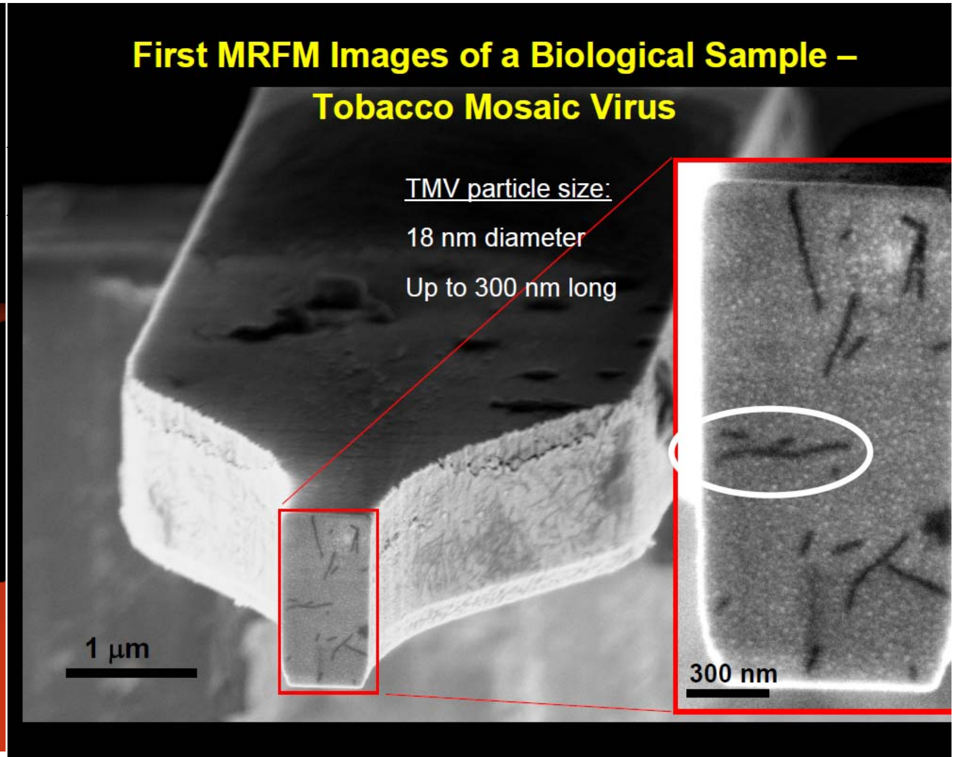
→ **Mechanical detection of Casimir forces** (Capasso, Harvard)

→ **Measuring Gravitation at small length scales** (Kapitulnik, Stanford)

→**Improving the sensitivity of gravitational wave detectors** (LIGO, GEO)

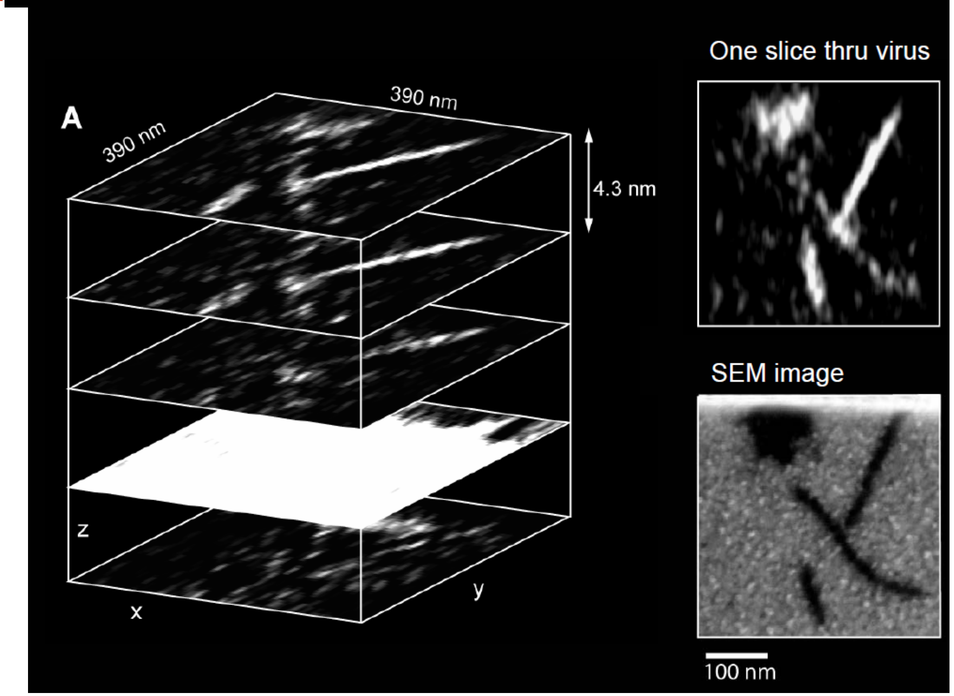
…





Example: 3D reconstruction of a Tobacco Mosaic Virus by magnetic resonance force microscopy (Rugar group, IBM)

→ 100 million times improvement in volume sensitivity compared to best conventional MRI



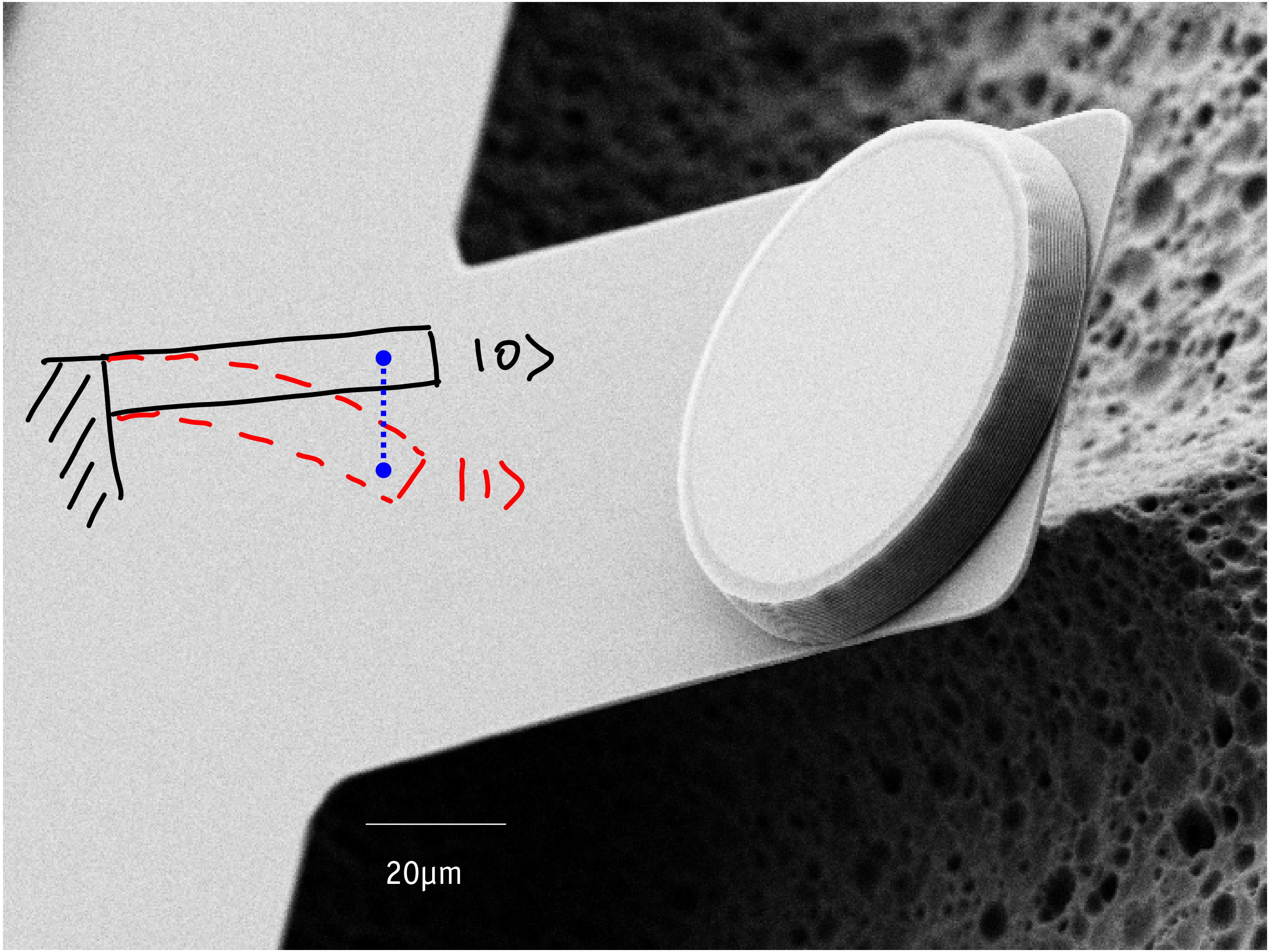
Schrödinger's Cat: The Measurement Problem

E. Schrödinger, Naturwissenschaften 23, 52 ff. (1935)

$|0\rangle_a + |1\rangle_a \rightarrow |0\rangle_a |$  $\rangle_{cat} + |1\rangle_a |$  $\rangle_{cat}$

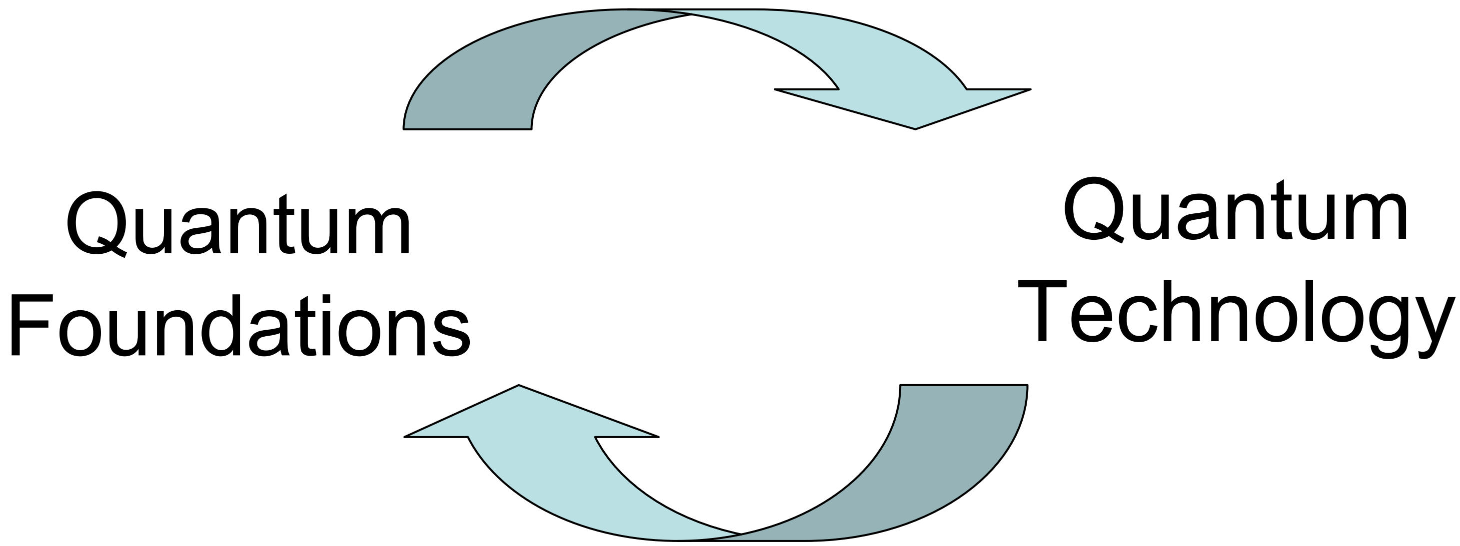
Schrödinger's Cat = Entanglement involving **macroscopically distinct states**

⟶ should be possible for **arbitrarily large systems**

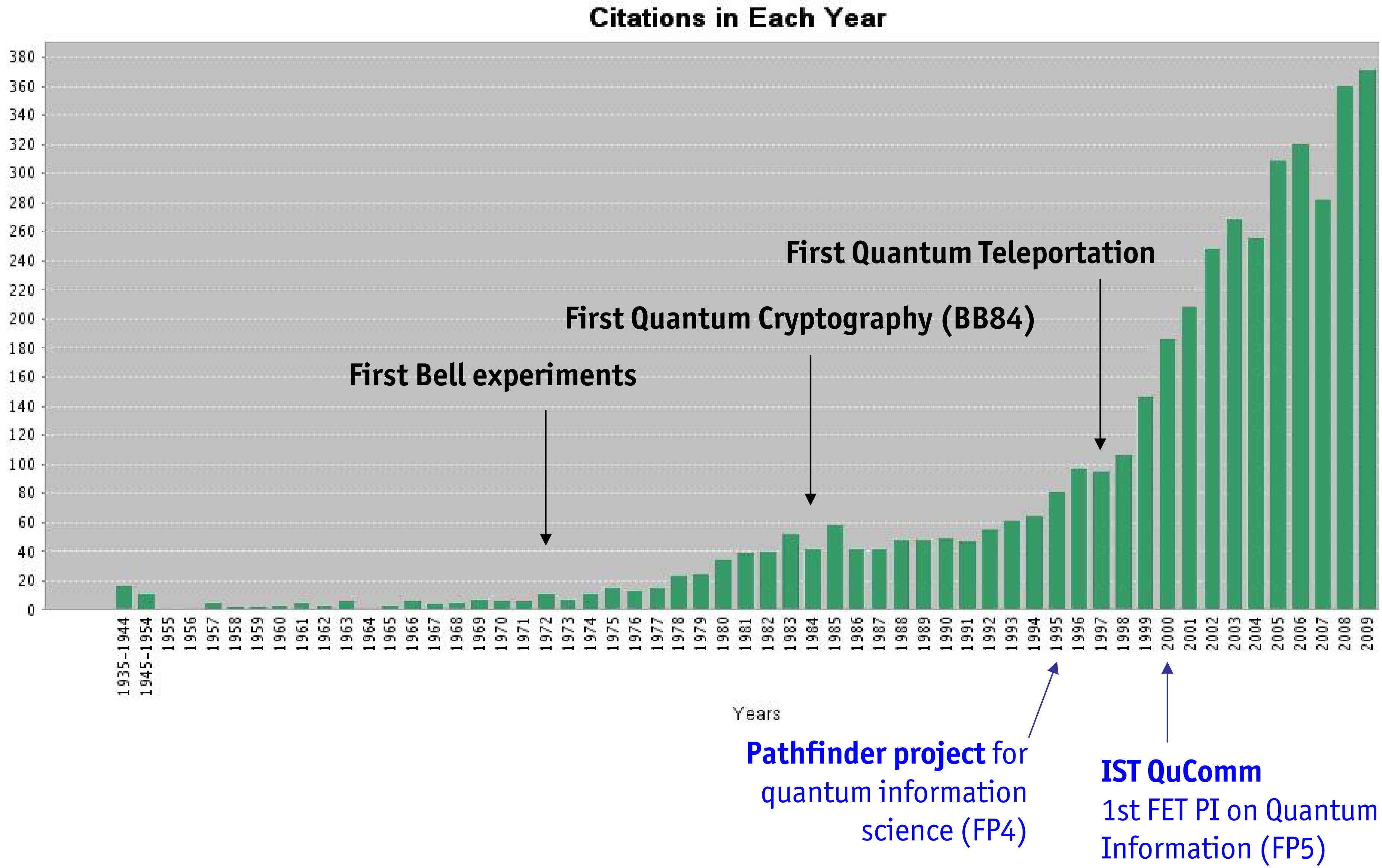


|0⟩
|1⟩
20μm

Fundamental vs Applied Research: Give and Take...



Fundamental vs Applied Research: Give and Take...



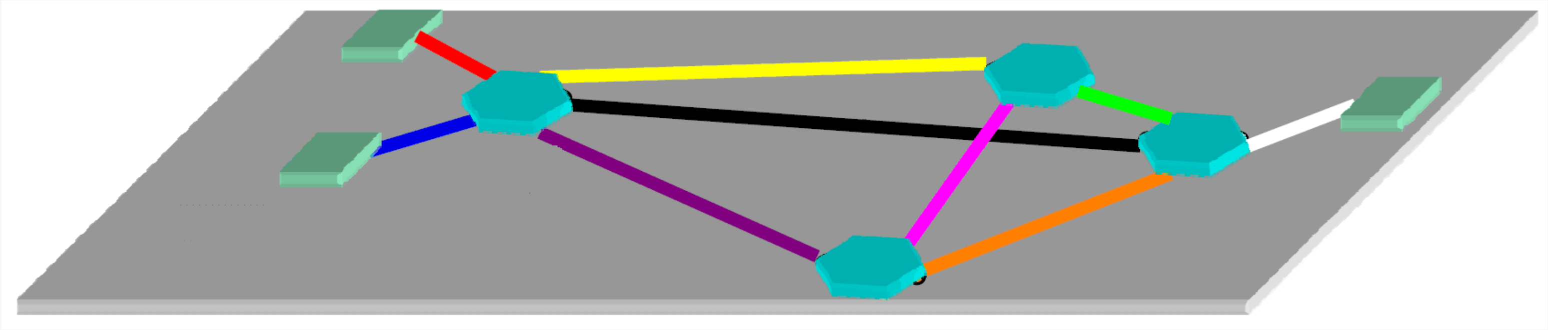
Take-Home Message

• **Quantum Foundations** has radically changed our view of information processing → QIPC

• **Quantum Information Technologies** have opened up a new frontier for fundamental research (also: QIT for solid state, field theory, etc.)

• New experiments on the foundations of quantum physics will eventually lead to new (quantum) technologies

Towards Quantum Communication Networks



Quantum Communication

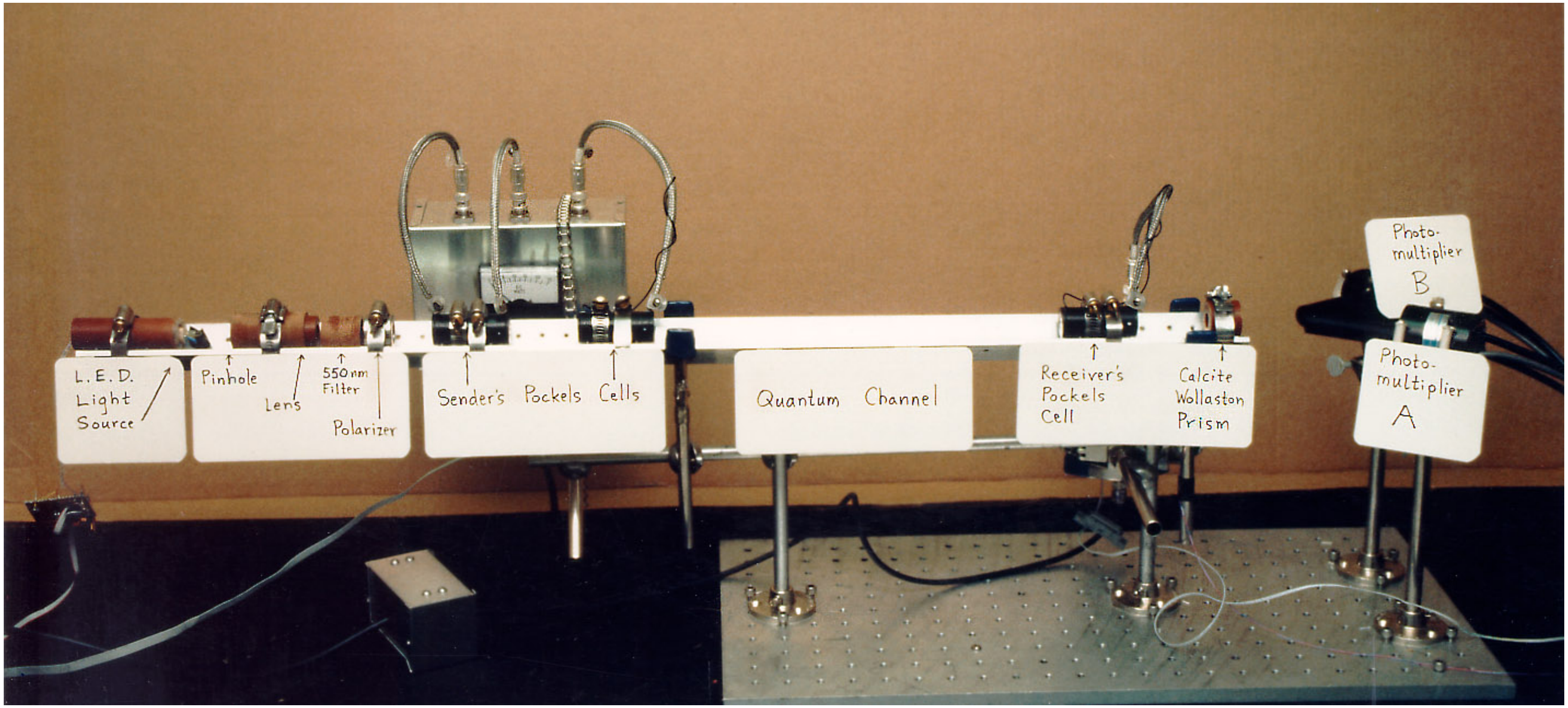
- applications
- today's networks
- future – quantum – networks

applications

- Quantum Key Distribution
  for secure communication
- cryptographic primitives:
  coin-tossing, secret-sharing, etc.
- communication complexity tasks, quantum games, quantum metrology
- quantum teleportation, entanglement swapping
  → distribute entanglement
- quantum internet → quantum-data links between quantum computation nodes

Quantum Key Distribution

- QKD enables quantifiable security



BB84: errors in key are measure for the information of a potential eavesdropper

commercial systems

id Quantique
A quantum leap for cryptography

- Id Quantique
  www.idquantique.com

- MagiQ

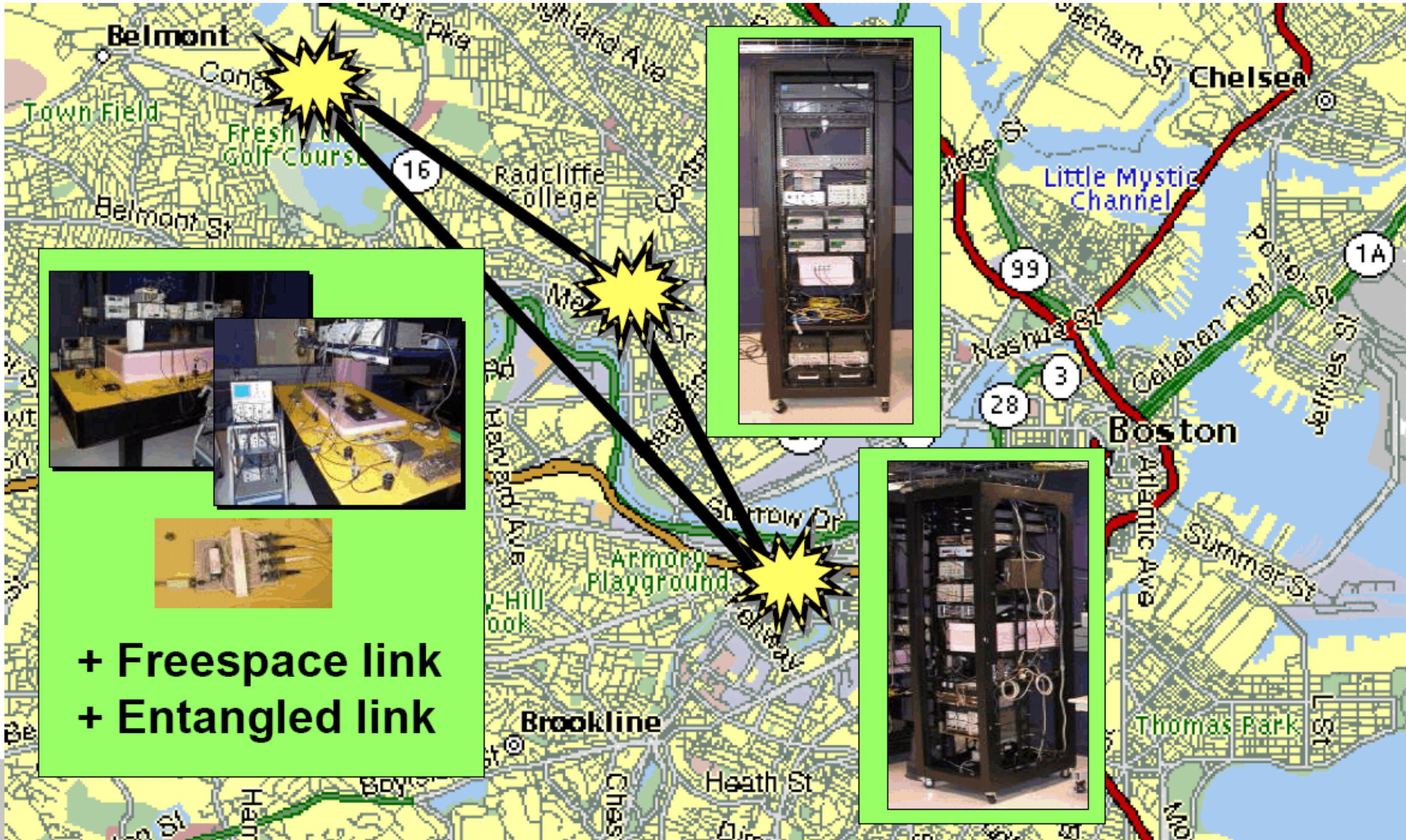
MagiQ™
Quantum Information Solutions for the Real World.

→Toshiba

- smart-quantum

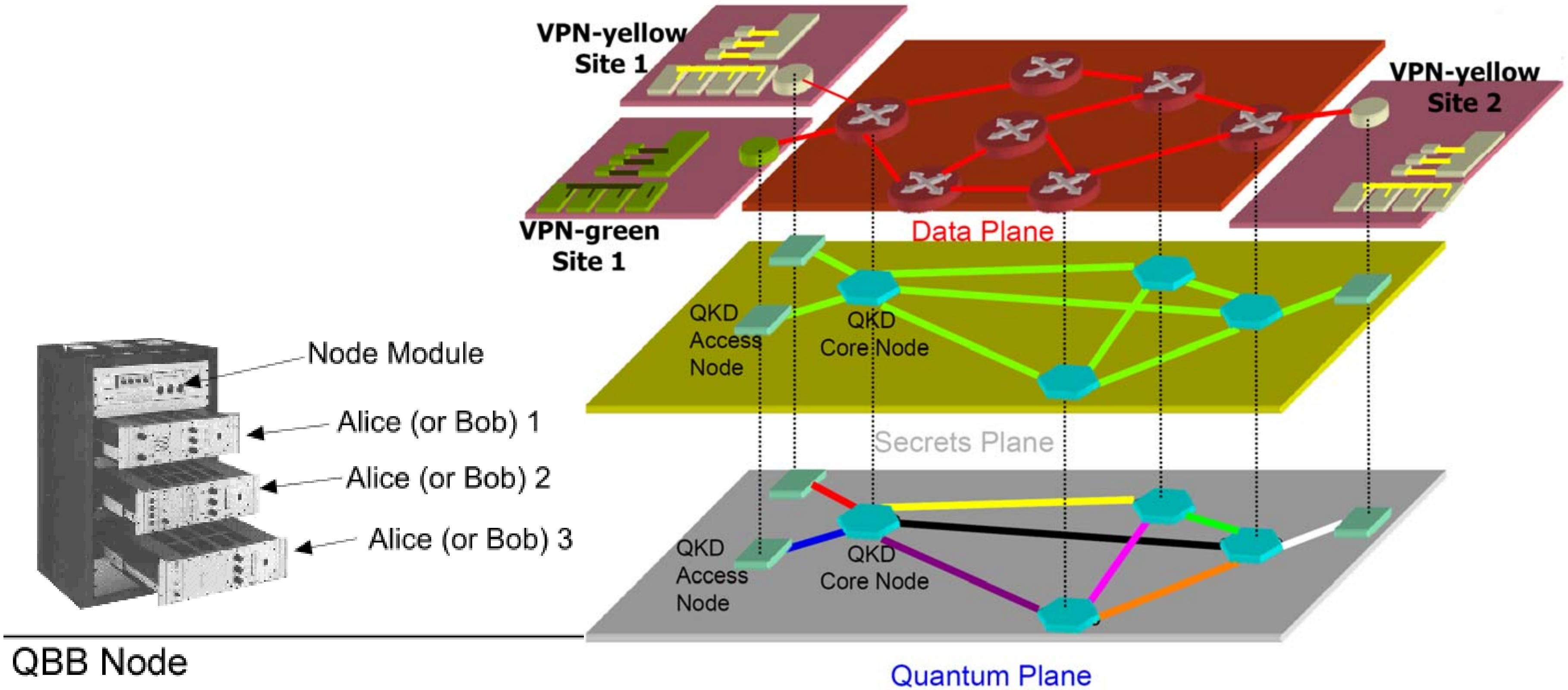
QKD in networks

- trusted repeater schemes
- DARPA network
  - Boston area; BBN, Harvard, Boston University; 2005



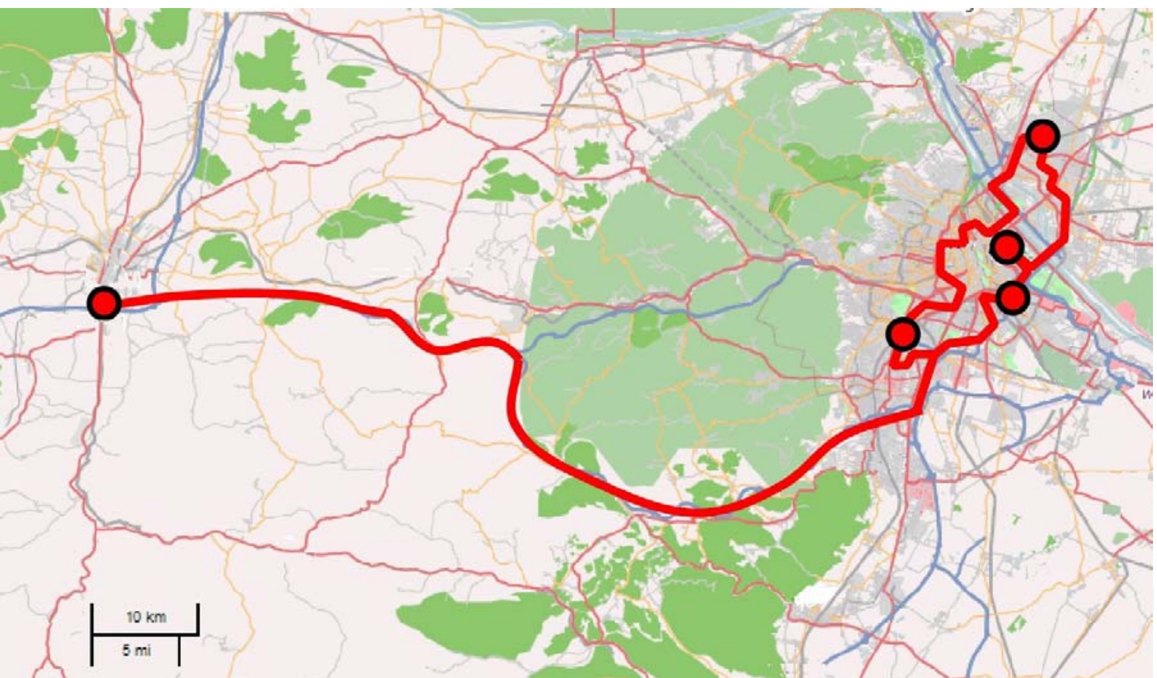
SECOQC network

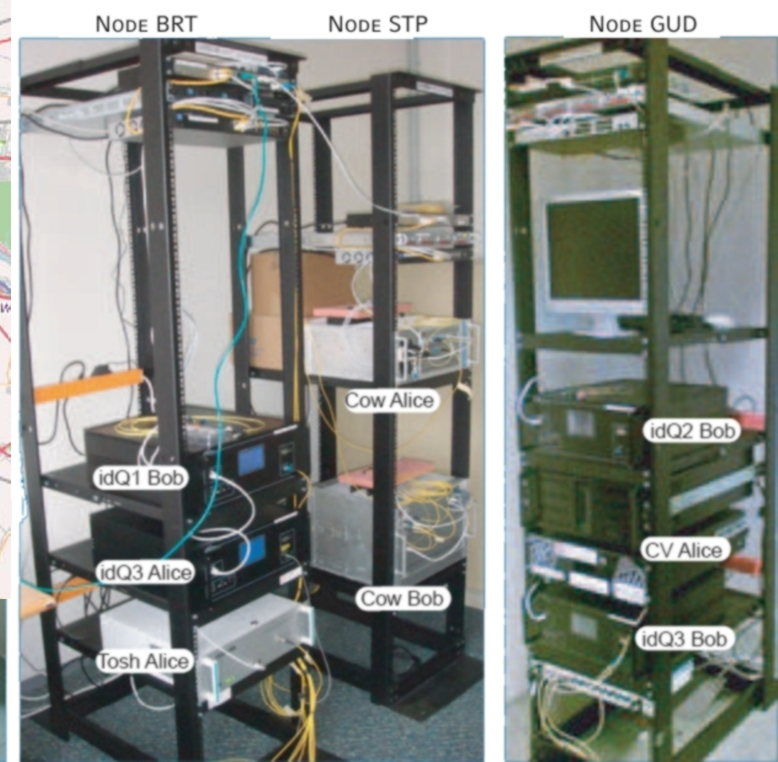
- seamless integration into multi-layer communication structure



SECOQC network

- highly integrated systems (19")
- operated in standard telecom infrastructure + daylight free-space link; continuously for 1 month





SECOQC network

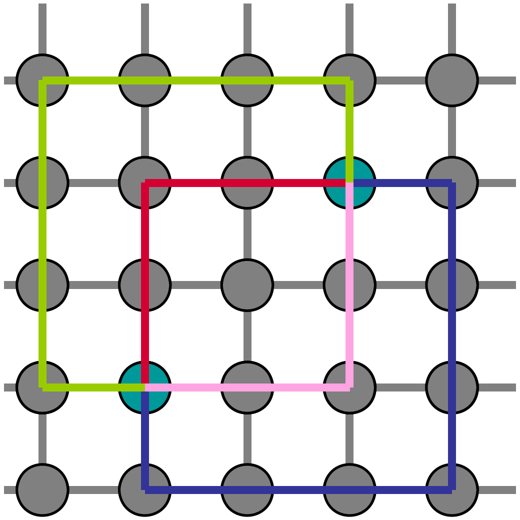
- seamless integration into multi-layer communication structure

– Increase distance and secret rate capacity

–Less initial secret has to be distributed: full covering joint tree is sufficient [*O(n) instead of O(n²)*] OR
Links running out of authentication key can recover

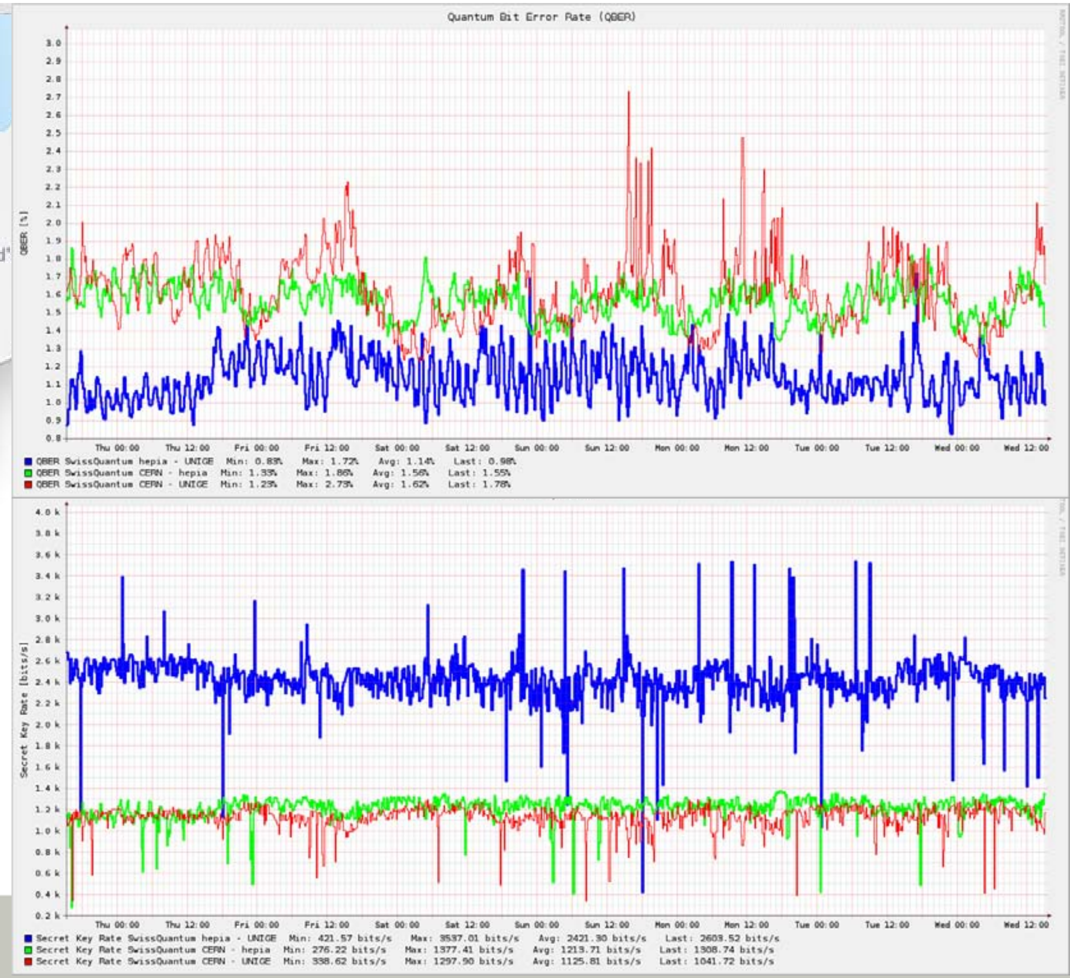
–Key is a network-wide asset and can be optimally redistributed

–Combining disjoint paths can ensure **information-theoretic security for a bounded adversary** (secret sharing)



swiss quantum

- secure links for Geneva election system (since 2007)
- 3 node network, continuous operation since 07/2009



- Univ. Geneva
  Univ. of Appl. Science
  CERN, id Quantique

http://www.swissquantum.com/

current projects

- in Durban, during World-Cup 2010
  University of KwaZulu Natal, id Quantique

- Tokyo QKD Network Oct. 2010
  JGN2plus, NICT, NEC, Mitsubishi Electric, NTT , Toshiba, id Quantique

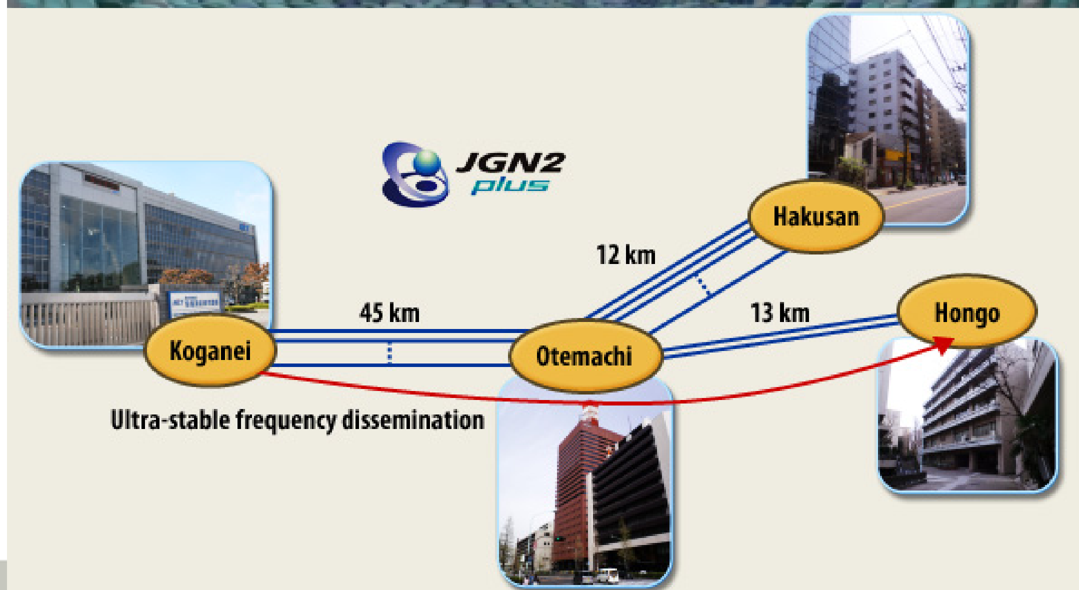
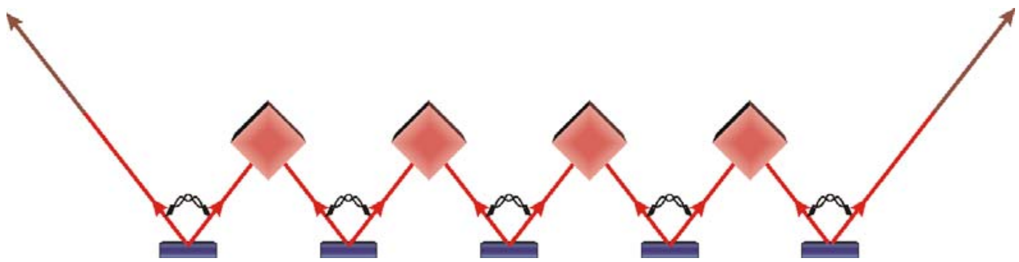


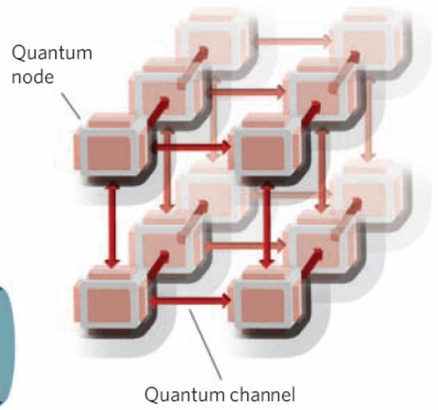
Fig. 1 Network Topology of the Tokyo QKD Network

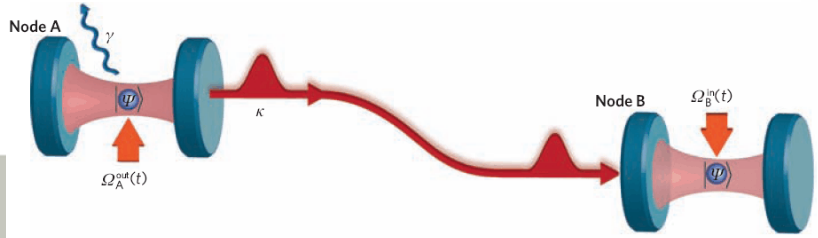
future networks

- long distance communication enabled by quantum repeater

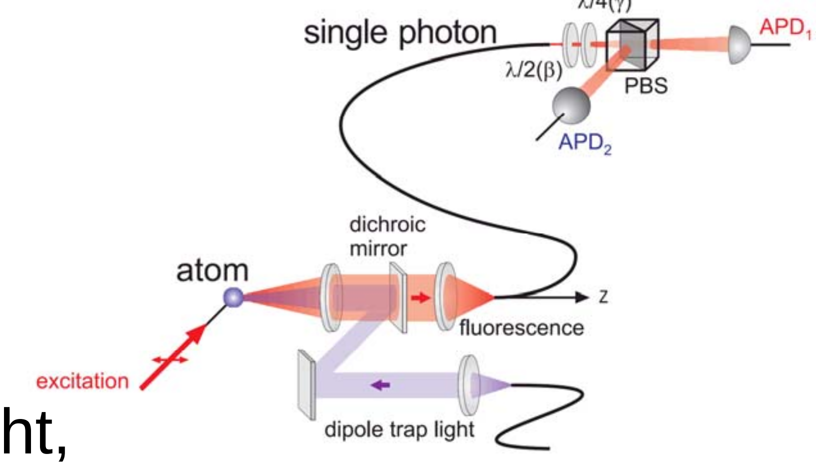


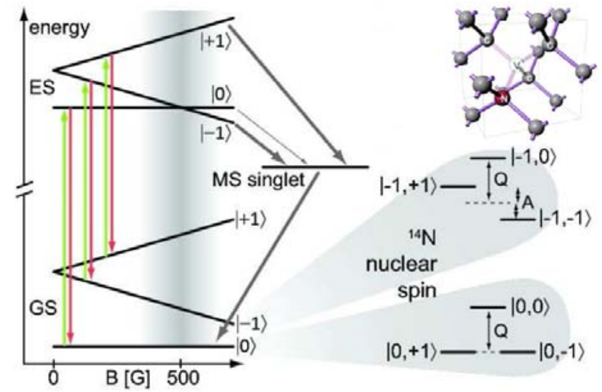
- sources of entangled qubits are conected via repeater nodes performing error correction and storage.
- quantum internet

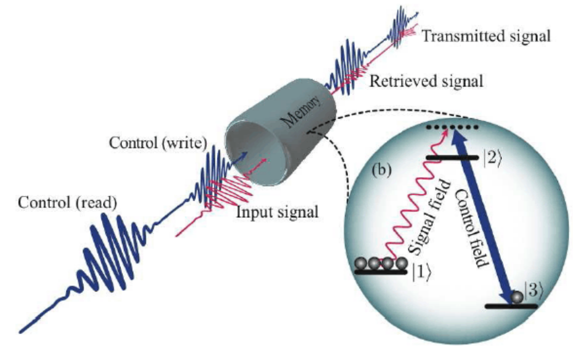




components



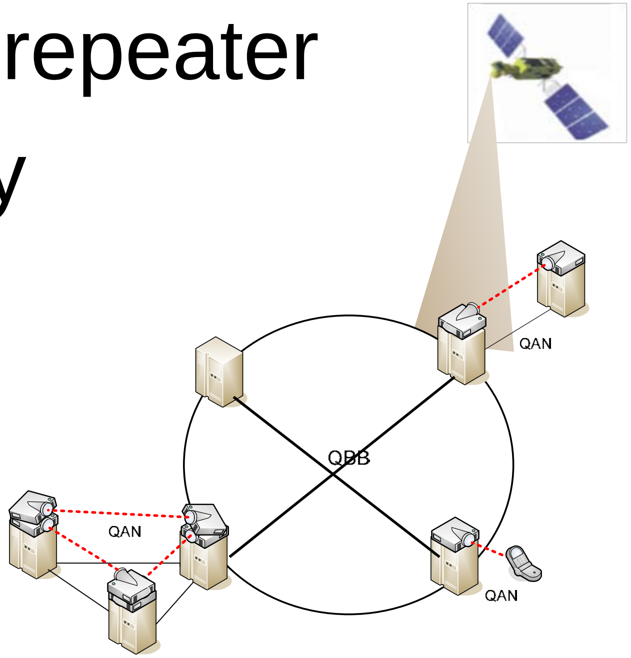




- sources of entanglement
  - photon pairs, cv-states of light,
  - atom-photon states,
  - quantum logic elements
- quantum memory
  - atoms, atomic clouds,
  - rare earth doped glass fiber,
  - solid state e^- and nuclear spin states
- quantum interfaces
  - light-matter interface,
  - hybrid systems....
- small scale quantum logics
  - Rydberg coupling, collisions, ion trap, SC-circuits....

where to go

- high rate, long distance QKD
- components for quantum repeater
- analysis of device security
(in real world scenarios)
- networking structures



- basis for:
world wide secure communication
quantum internet, quantum simulators...