Quantum information:

from the optics laboratory to the “real” world

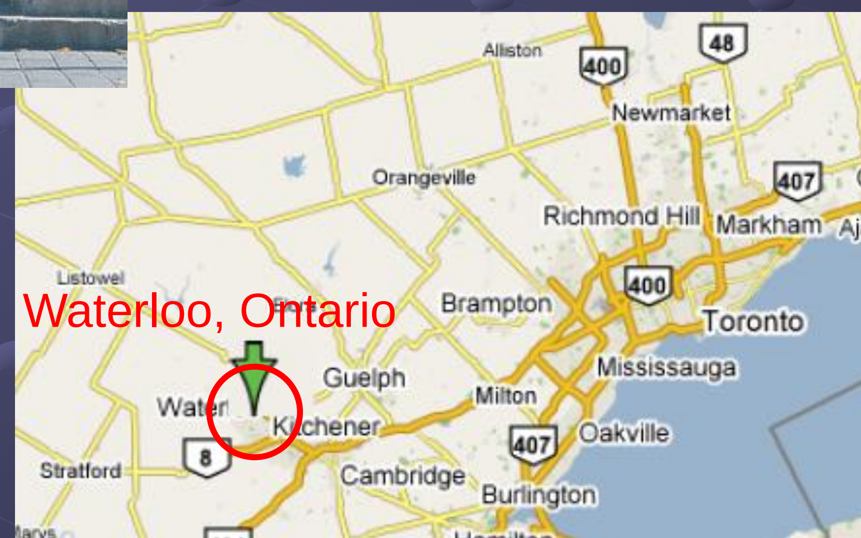
Kevin Resch
IQC, Dept. of Physics
University of Waterloo

University of Waterloo

IQC Institute for Quantum Computing

Institute for Quantum Computing

- Founded 2001 at University of Waterloo



- 14 faculty
- 6 post-docs
- ~50 students

Always looking for more!

http://www.iqc.ca/

Optical Quantum Information
Talk Outline

Nonlinear Optics

- Measurement-induced nonlinearity
- Interference-enhanced nonlinearity

Quantum Information

Quantum Computation

- One-way quantum computation
- Linear optics entangling gates

Quantum Communication

- Free-space entanglement distribution
- Entanglement Purification

Quantum Metrology

- Classical analogues of quantum interference

Quantum Foundations

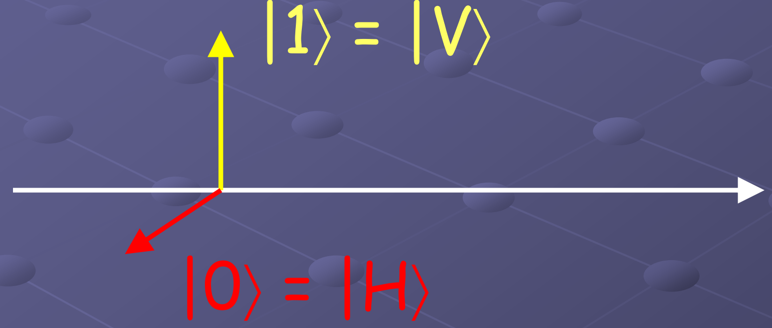
- Tomography
- Weak measurement
- Multipartite entanglement
- Nonlocality tests

Quantum information

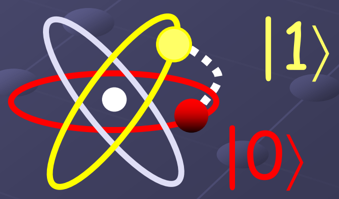
Quantum bits can be 0 or 1 but also superpositions

bit: 0 or 1

qubit: $\alpha|0\rangle + \beta|1\rangle$



Photon Polarization



Atomic Levels

Familiar quantum features

- Uncertainty principle

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

Position

Momentum

W. Heisenberg

- No-cloning theorem

$$|\psi\rangle|0\rangle \xrightarrow{NOPE} |\psi\rangle|\psi\rangle$$

Wootters

Zurek

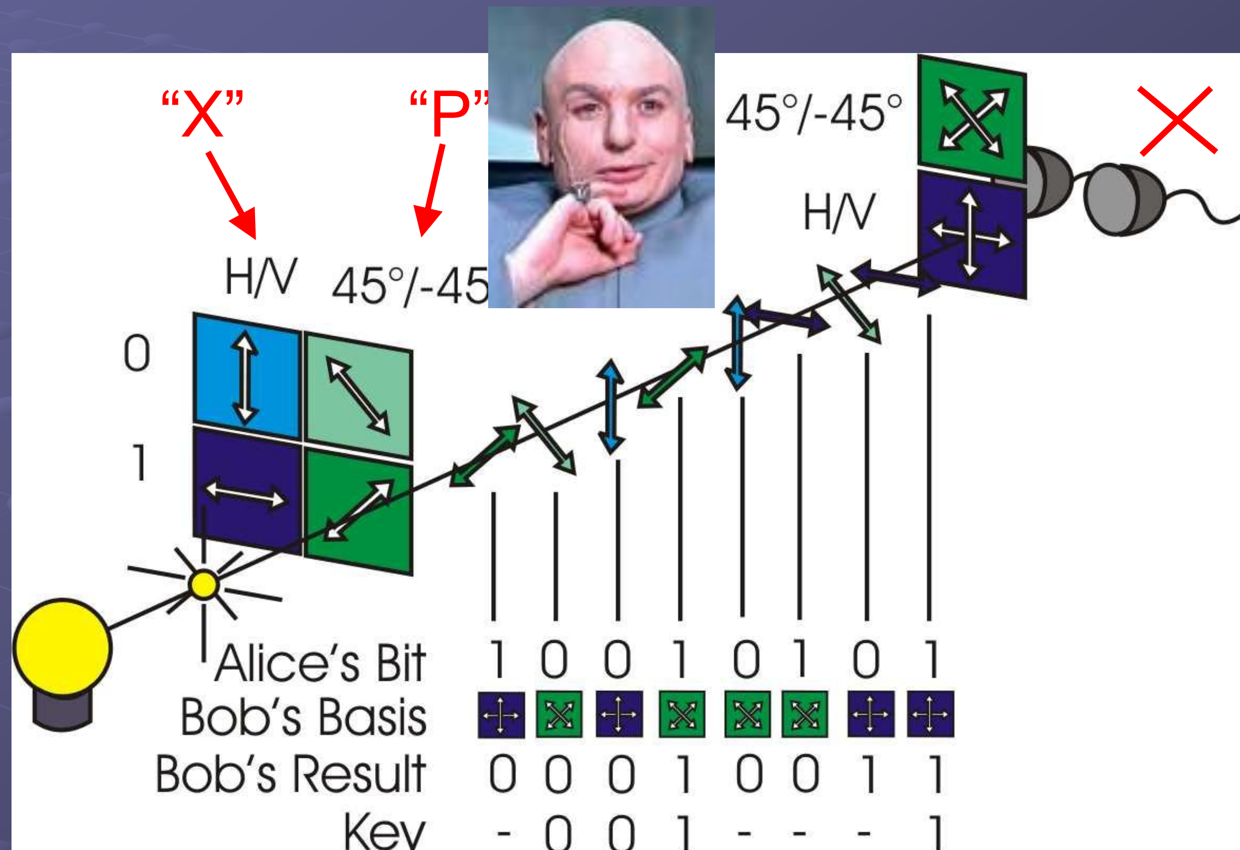
Dieks

…leads to ultimate cryptosystem

Attempting proper measurements to learn about the state but cannot do so without disturbance (HUP)

Eavesdropper: either strategy will lead to errors in the detected signal

[illegible] eavesdroppers make identical copies of unknown state and make measurements on them (no-cloning)



C. Bennett, G. Brassard 1984

…leads to ultimate cryptosystem

Attempting either strategy will lead to errors in the detected signal

Single photons are sent in one of two noncommuting basis states

An eavesdropper must make measurements to learn about the state, but cannot do so without disturbance (HUP)

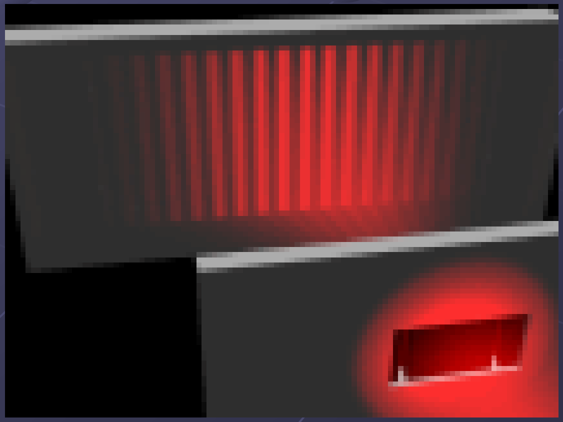
Nor can the eavesdropper make identical copies of the state and make measurements on them (no-cloning)

More quantum features

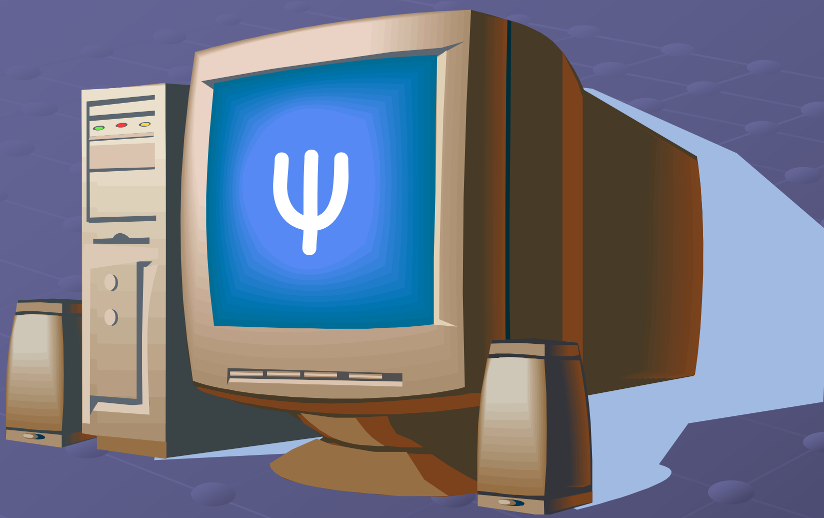
- Superposition
  - A quantum system can be in many states at the same time

$$\left|\Psi\right\rangle = \frac{1}{\sqrt{N}}\left(\left|\psi\right\rangle_1 + \left|\psi\right\rangle_2 + \left|\psi\right\rangle_3 + \ldots\right)$$

- Interference



…more powerful computers



Quantum computer takes a superposition of all possible input state to a superposition of all possible output states

Measurement results are random, except that interference (+clever algorithms) can reduce wrong answers

Feynman

Deutsch

Entanglement

- An entangled state
- A product state (not entangled)

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

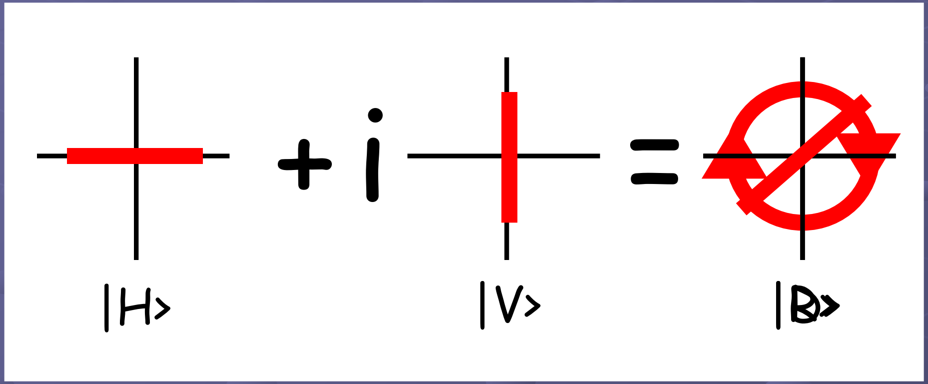
$$= |00\rangle + |11\rangle$$

"Bell state"

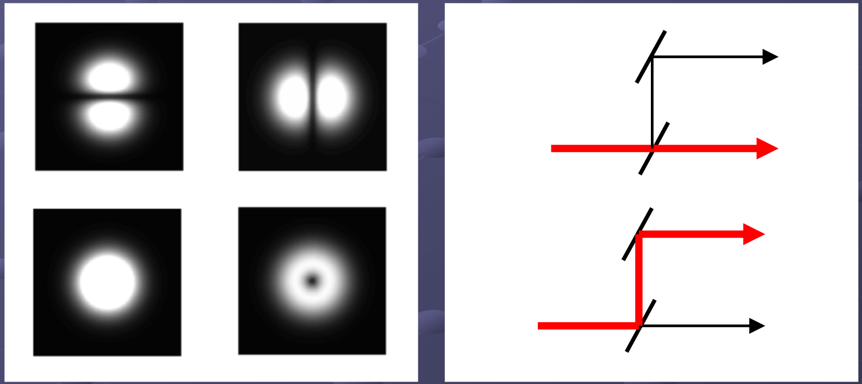
- Foundation for most quantum information protocols

Optical photons as qubits

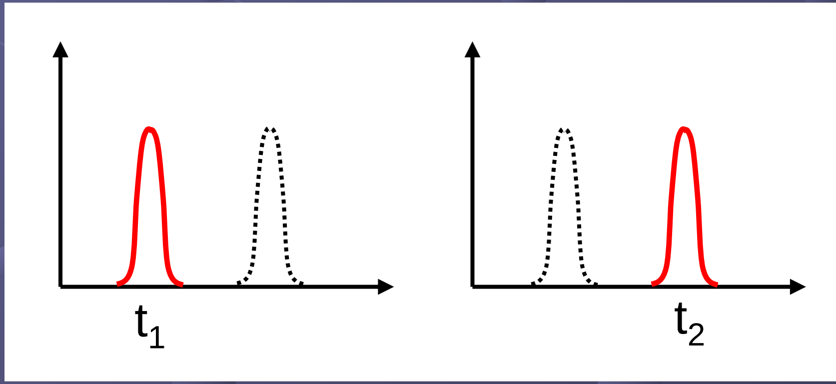
- Polarization



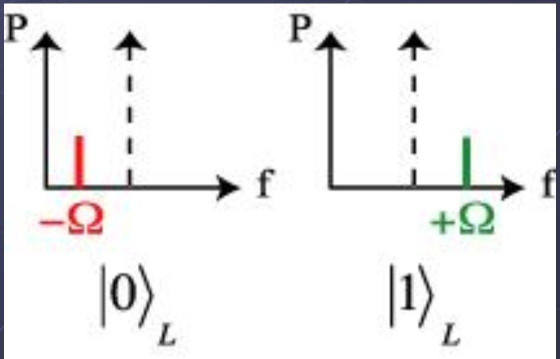
- Spatial modes



- Time-bin



- Freq. encoding



Optical photons as qubits

The Good

- Single-qubit operations
- Low decoherence
- High speed
- Perfect carriers of quantum information

The Bad

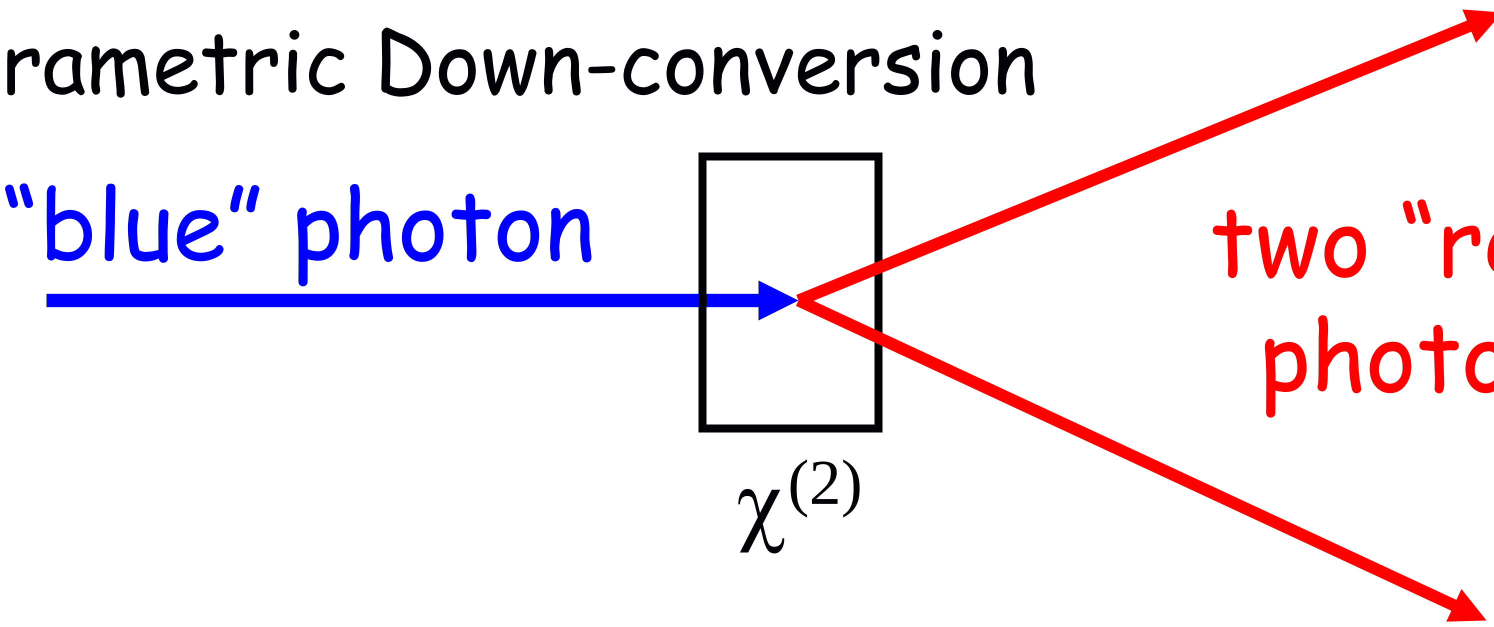
- Easy to lose a photon
- No natural interactions/weak nonlinearities means 2-qubit operations are hard

The Ugly

- Linear optics proposals for scalable quantum computing are extremely complicated (~50-1000s of ancillas/elements per CNOT)

Entangled Photon Source

Parametric Down-conversion



Phase matching:

$$\omega_{pump} = \omega_s + \omega_i$$

$$\vec{k}_{pump} = \vec{k}_s + \vec{k}_i$$

Type-II Down-conversion

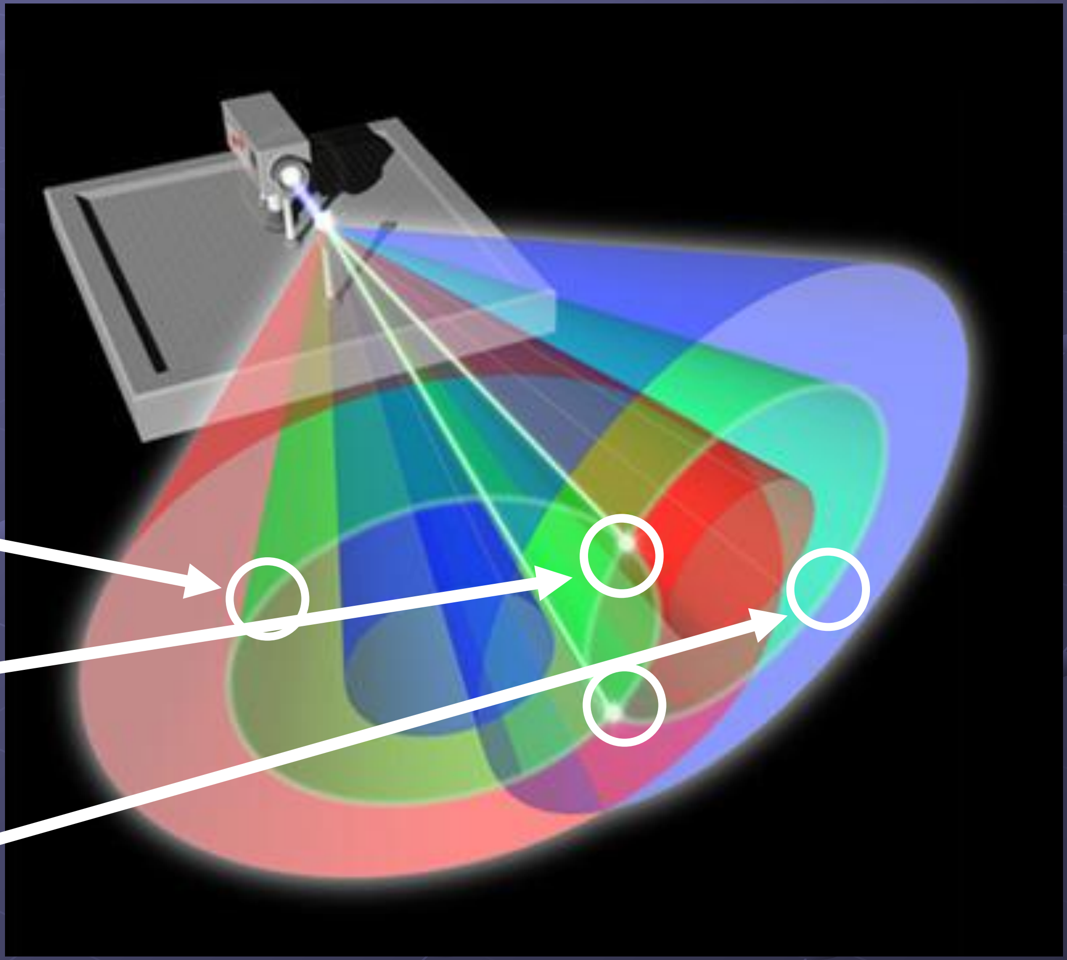
Entangled Pair

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1 |V\rangle_2 - |V\rangle_1 |H\rangle_2\right)$$

H-Photon

Confused

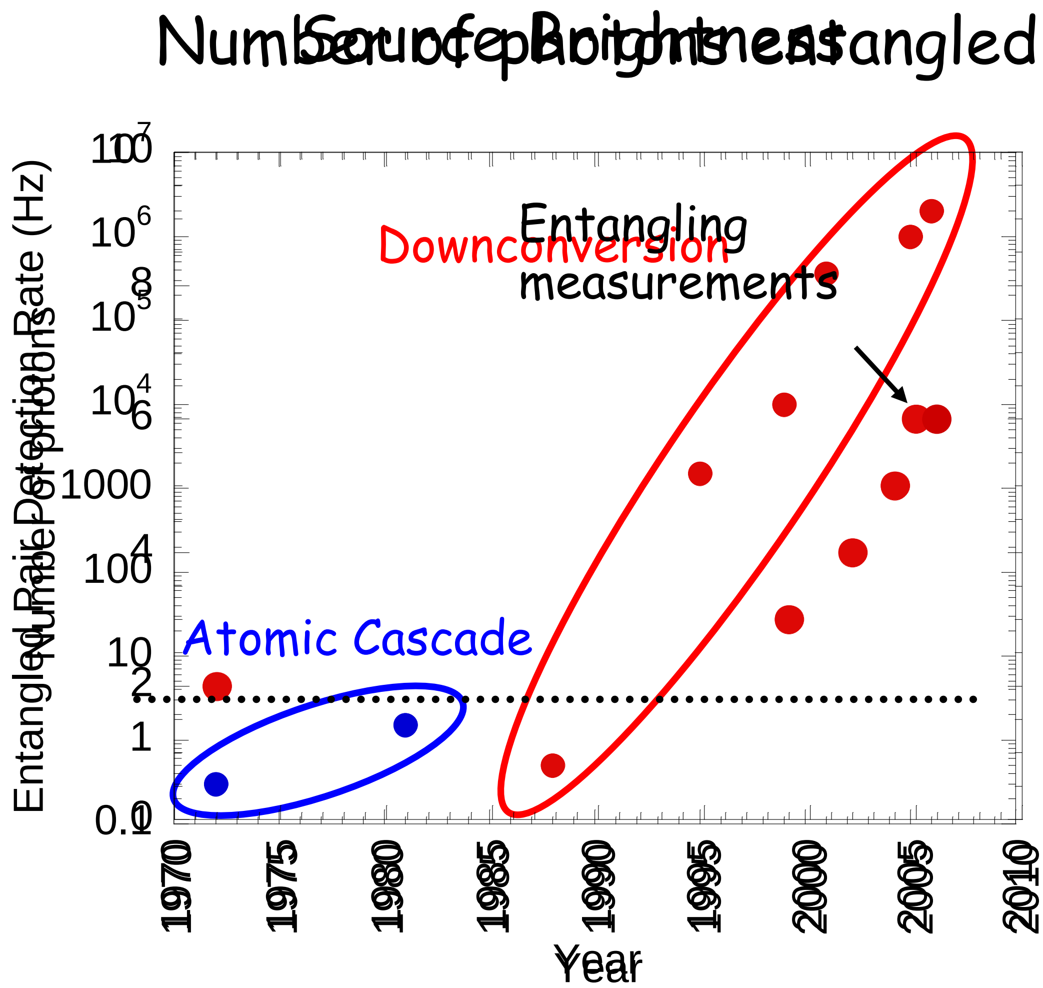
Correlated V-Photon

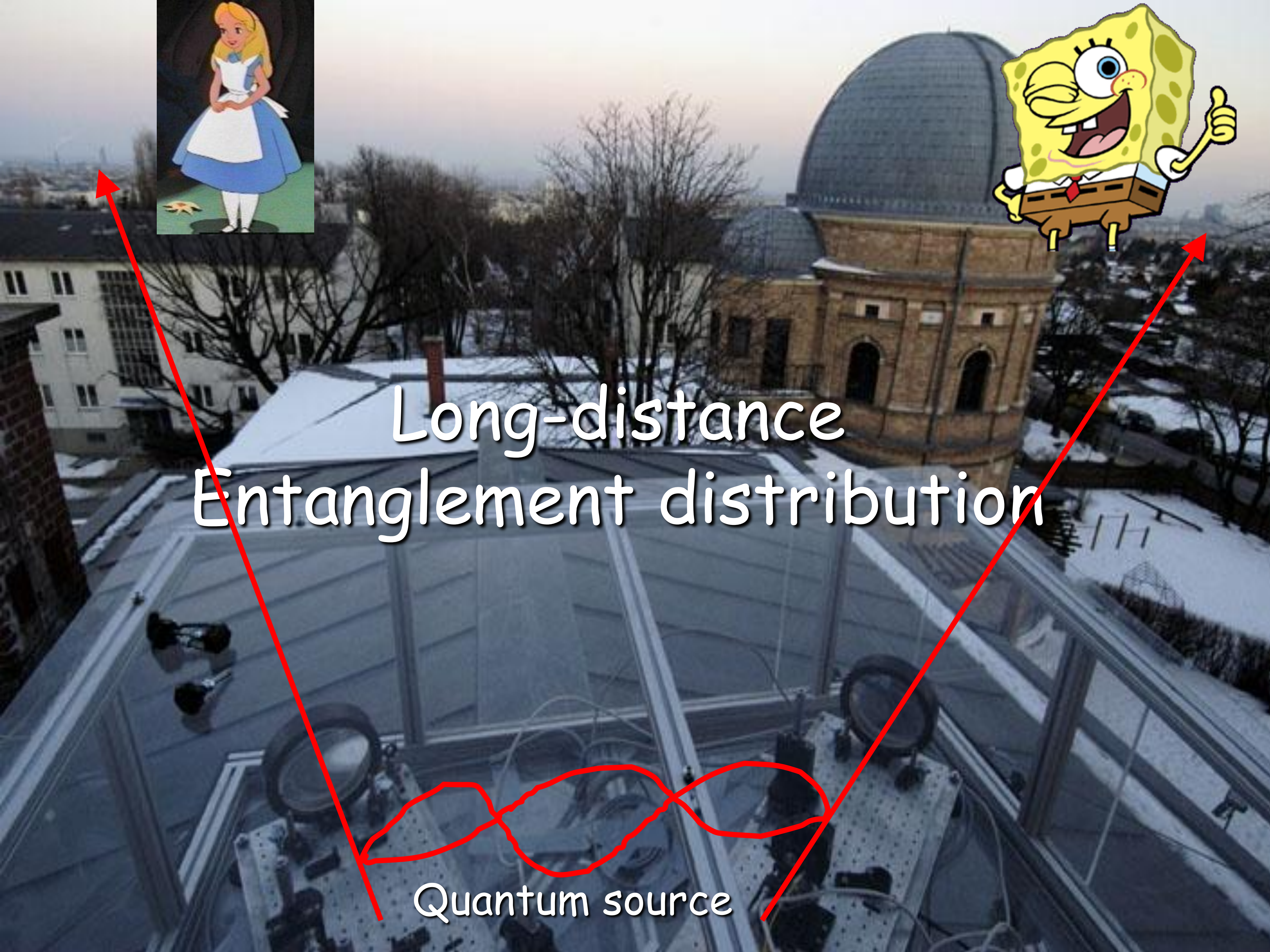


Recent source advancements

- High-power UV laser diodes (cheap, easy to use -> UG lab!)
- Efficient single-mode coupling (long-distance, low divergence, free-space)
- 4-, 5-, and 6-photon entanglement
  - Controllable entanglement – fundamental tests and quantum computing

State of the art




Long-distance
Entanglement distribution
Quantum source

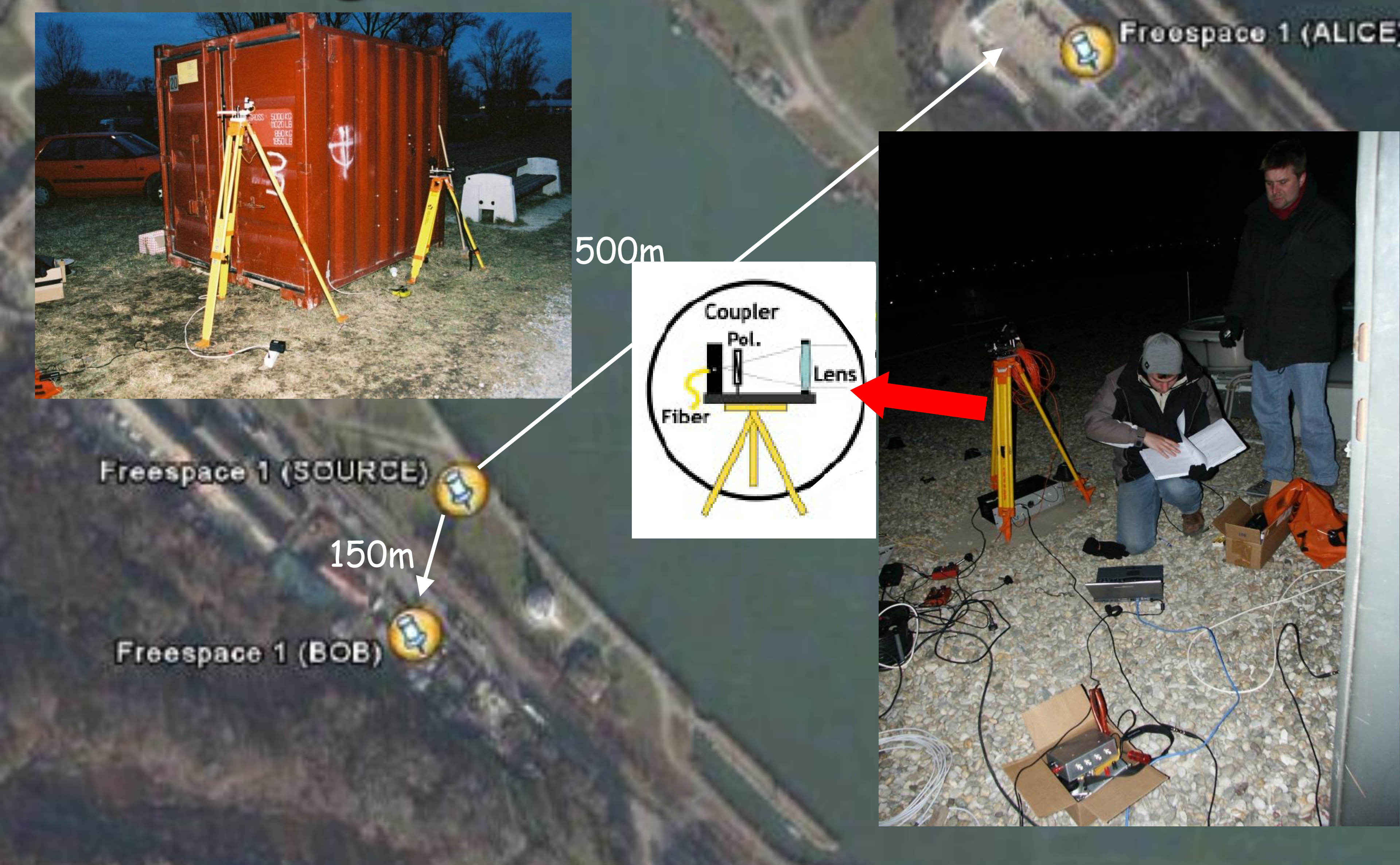
Zeilinger Group

Not Pictured here:
FS1&2: Michael Taraba
FS2: Bibiane Blauensteiner, Alessandro Fedrizzi, Christian Kurtsiefer, Tobias Schmitt-Manderbach, Henning Weier, Harald Weinfurter

Distributing Entanglement

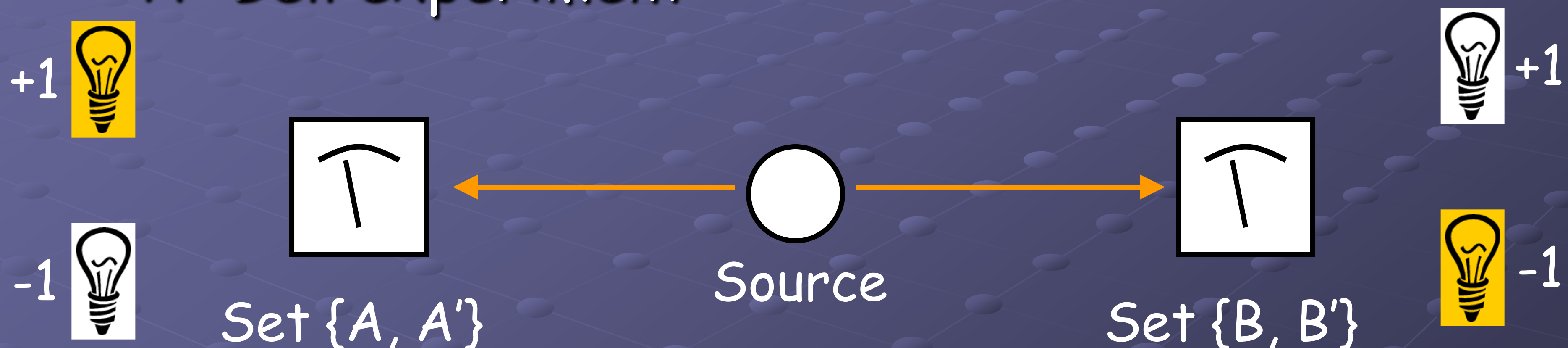
- Photons are the ideal carriers
- Practical quantum communication needs shared entanglement over long distances
- Challenges: High efficiency (no cloning) and high background rejection (single photons)

Entanglement takes to the air



Quantum correlations

- A “Bell experiment”



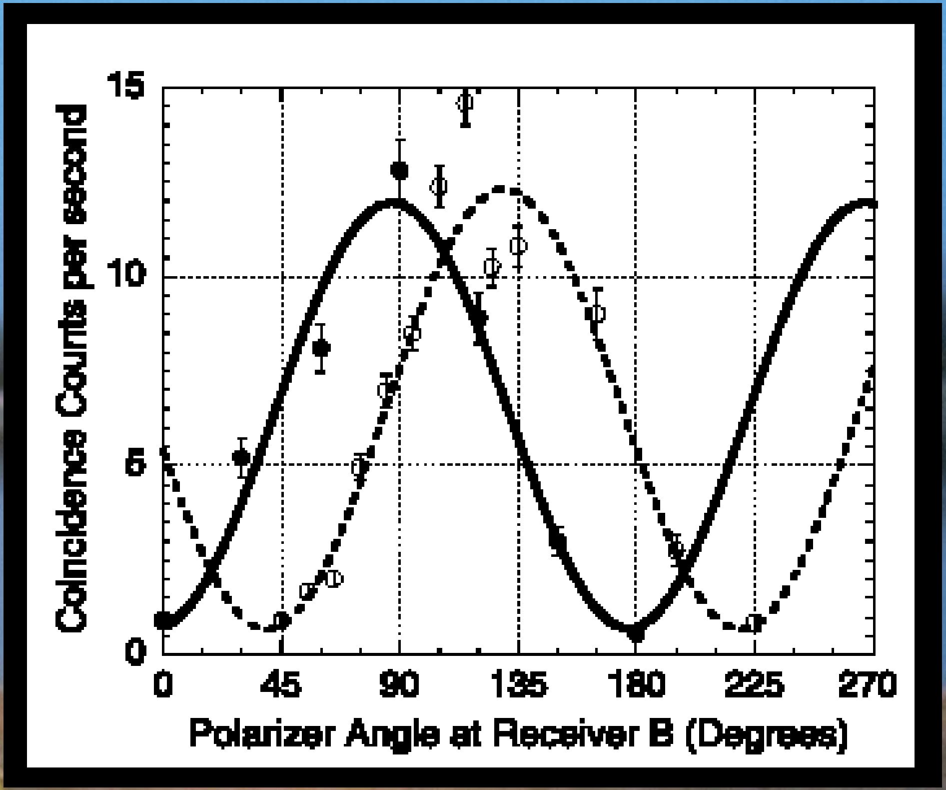
- ~~Local properties (ex. A=+1, A’=-1, B=+1, B’=+1)~~

  ~~$A(B+B')+A'(B-B') = \pm 2$~~
- CHSH-Bell inequality (req. 16 measurements)

  $S = |\langle AB+AB'+A'B-A'B' \rangle| \leq 2$
- QM allows $S = 2\sqrt{2} = 2.83$

Freespace 1 Results

- Measured S = 2.4 ± 0.1 (larger than 2 indicates entanglement)
- Two links 500m & 100m
- ~10 coincidences/s
- SMF-SMF coupling
- Time-stable channel

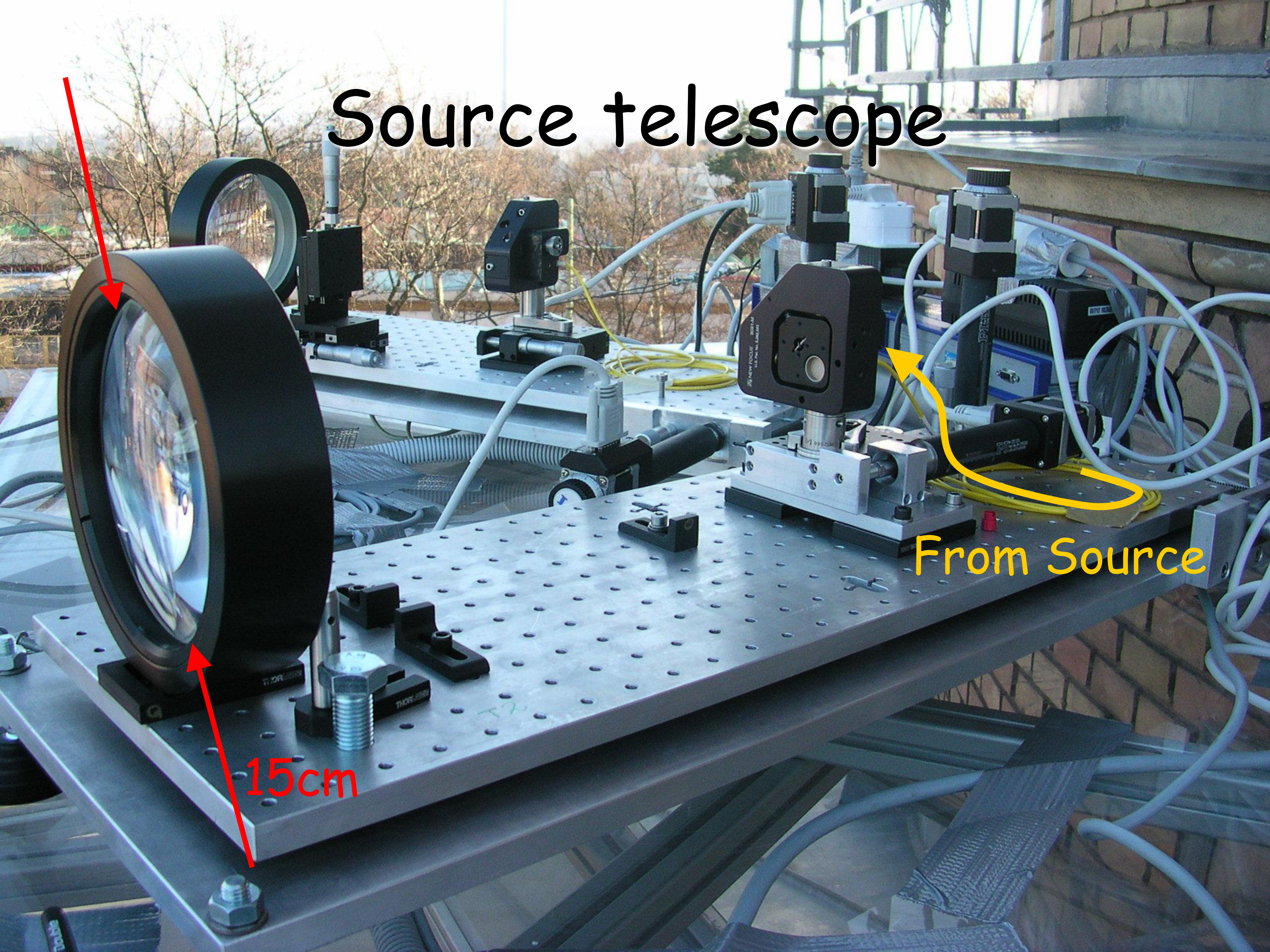


Polarization correlations

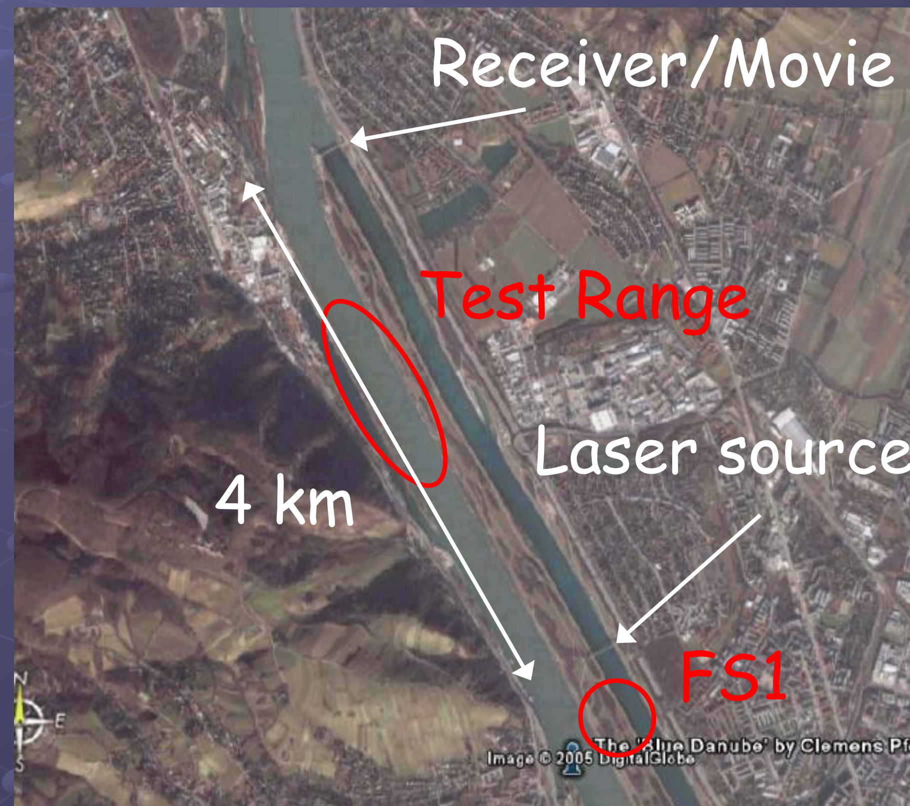
Science (2003)

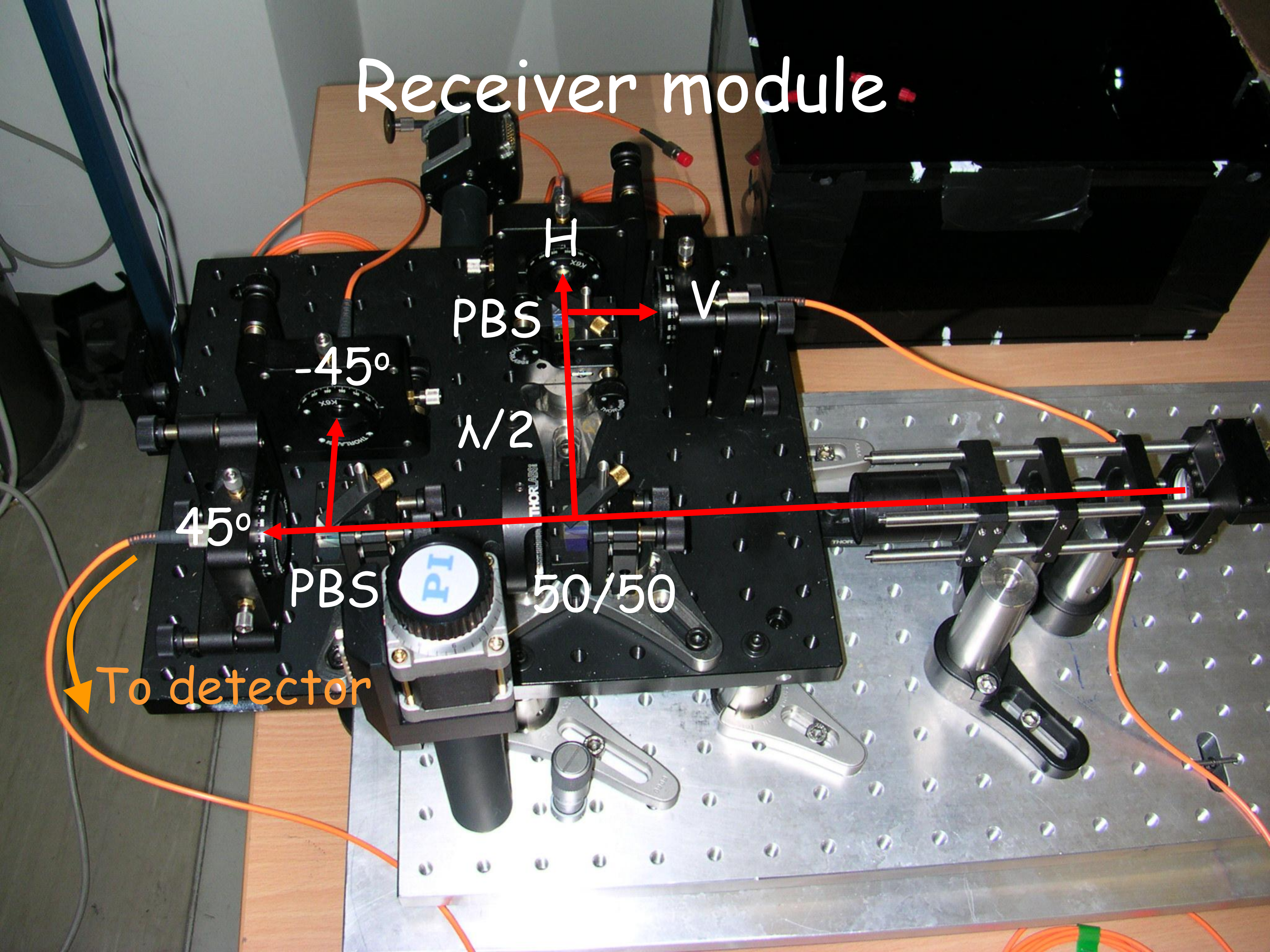
The next step

- 500m to 7.8km (the atmosphere straight up is 7.3km thick)
- No more cable
- Light passed over a city – likely real-world scenario


Source telescope
From Source
15cm

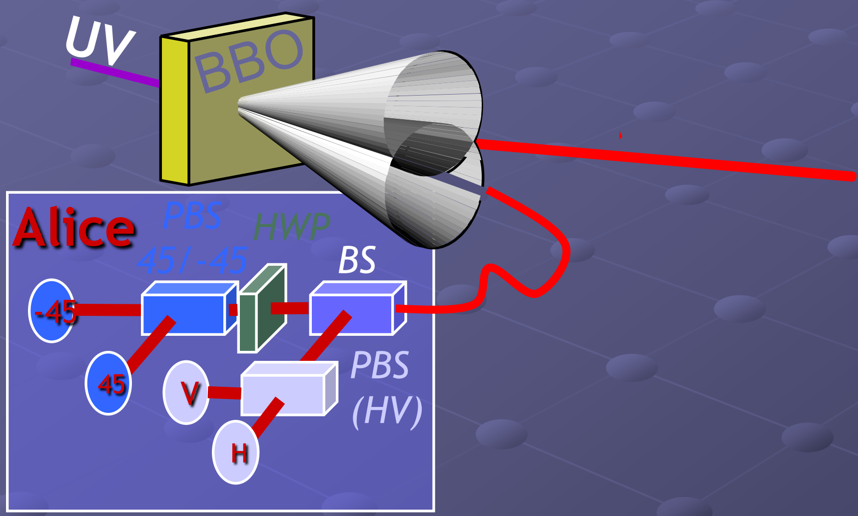
Atmospheric fluctuations




Receiver module
H
PBS
V
-45°
λ/2
45°
PBS
50/50
To detector

Practicalities

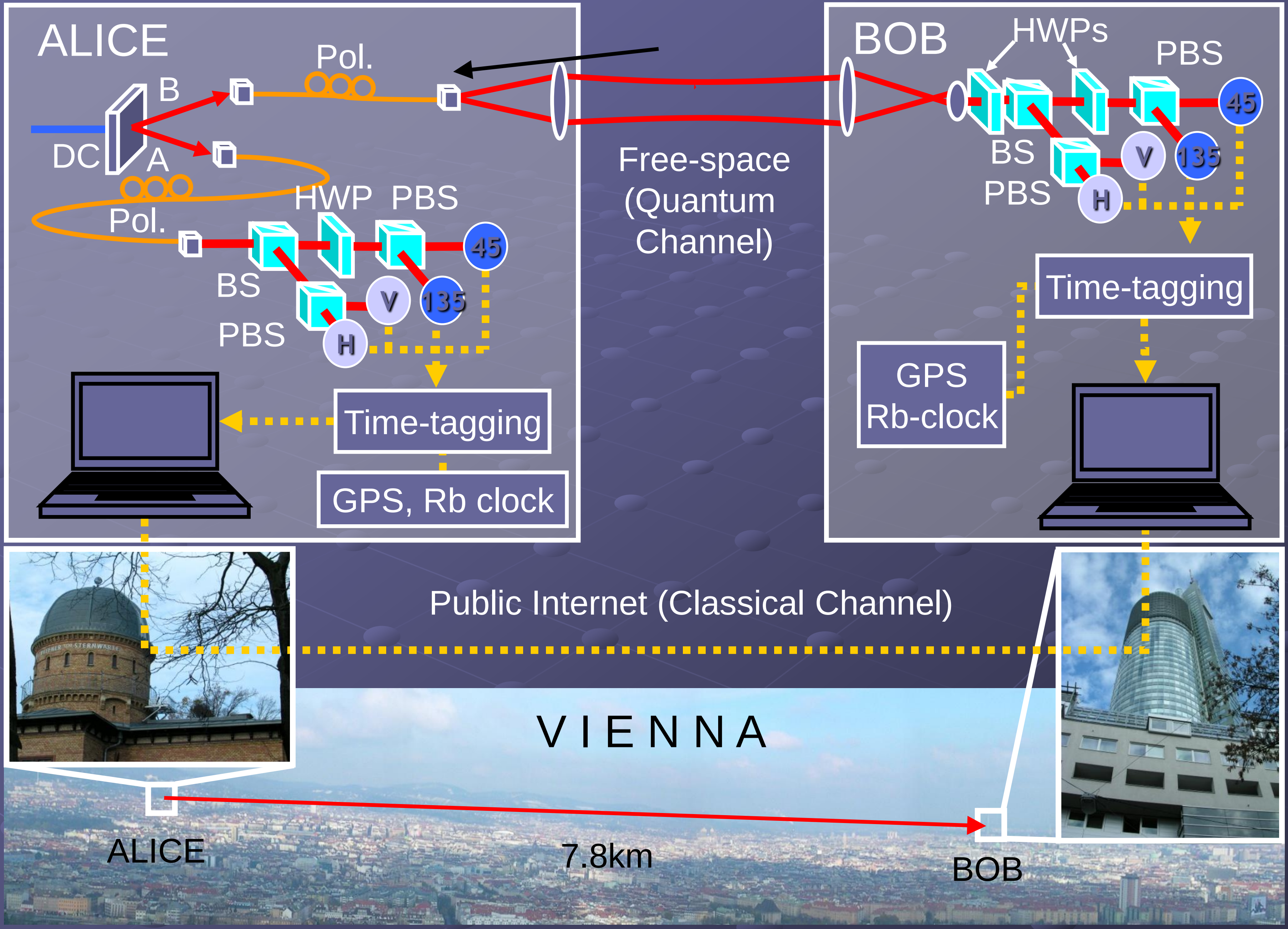
- Absence of good single-photon sources
- Can use quantum randomness to select state:



$$\left|HH\right\rangle + \left|VV\right\rangle$$
$$= \left|45,45\right\rangle + \left|-45,-45\right\rangle$$

- Triggered single photons, reduced "empty" pulses |0> and double photons |2>
- Laser frequency monitoring unnecessary

Entanglement takes to the air – again!


ALICE
Pol.
B
DC
A
Pol.
HWP
PBS
BS
PBS
45
V
135
H
Time-tagging
GPS, Rb clock
Free-space
(Quantum
Channel)
BOB
HWPs
PBS
BS
PBS
45
V
135
H
Time-tagging
GPS
Rb-clock
Public Internet (Classical Channel)
VIENNA
ALICE
7.8km
BOB


PI

Freespace 2 Results

Millenium Tower (Bob)

Kuffner Sternwarte (Alice)	22.5°	112.5°	67.5°	157.5°
0°	1469	5763	6500	1067
90°	4015	1305	1483	2959
45°	2171	9103	2633	6357
135°	5373	1701	6889	1090

$S = 2.27 \pm 0.019 > 2$

Quantum Correlations!

- Two links 7.8 km and 10^{-4}km
- 25 ccps found over time tags/internet
- Single-mode fibre to spatial-filter coupling
- 14-σ Bell violation, all 16 meas. taken simultaneously

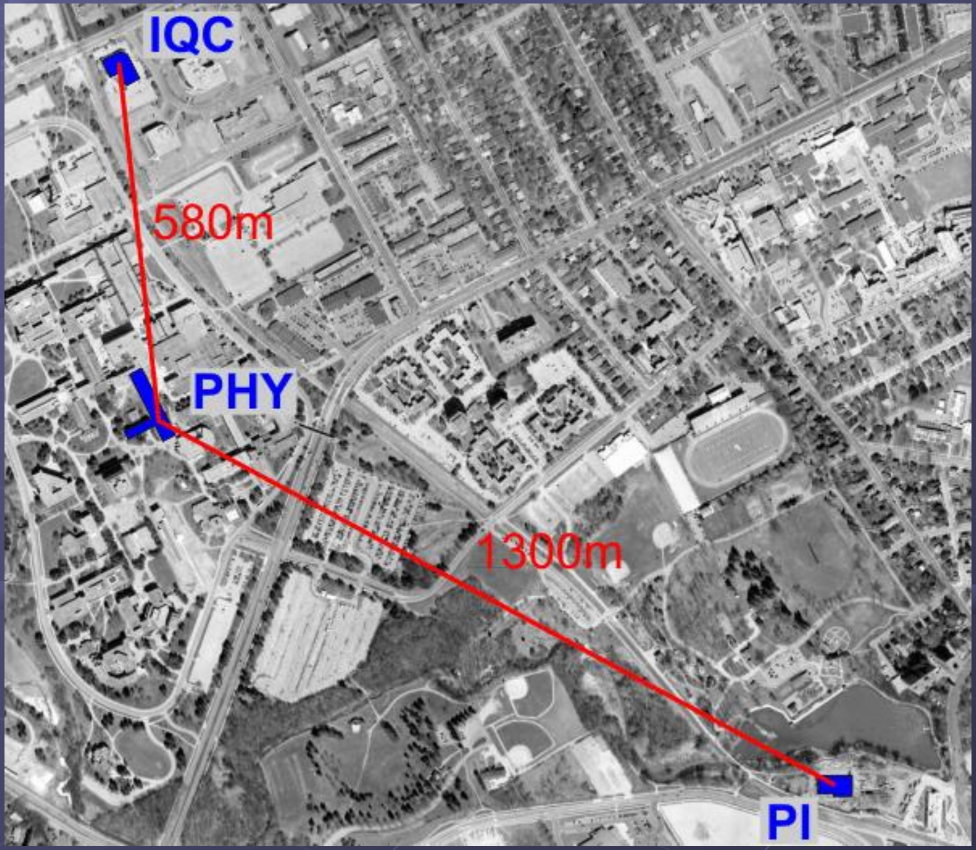
Optics Express (2005)

Remaining challenges

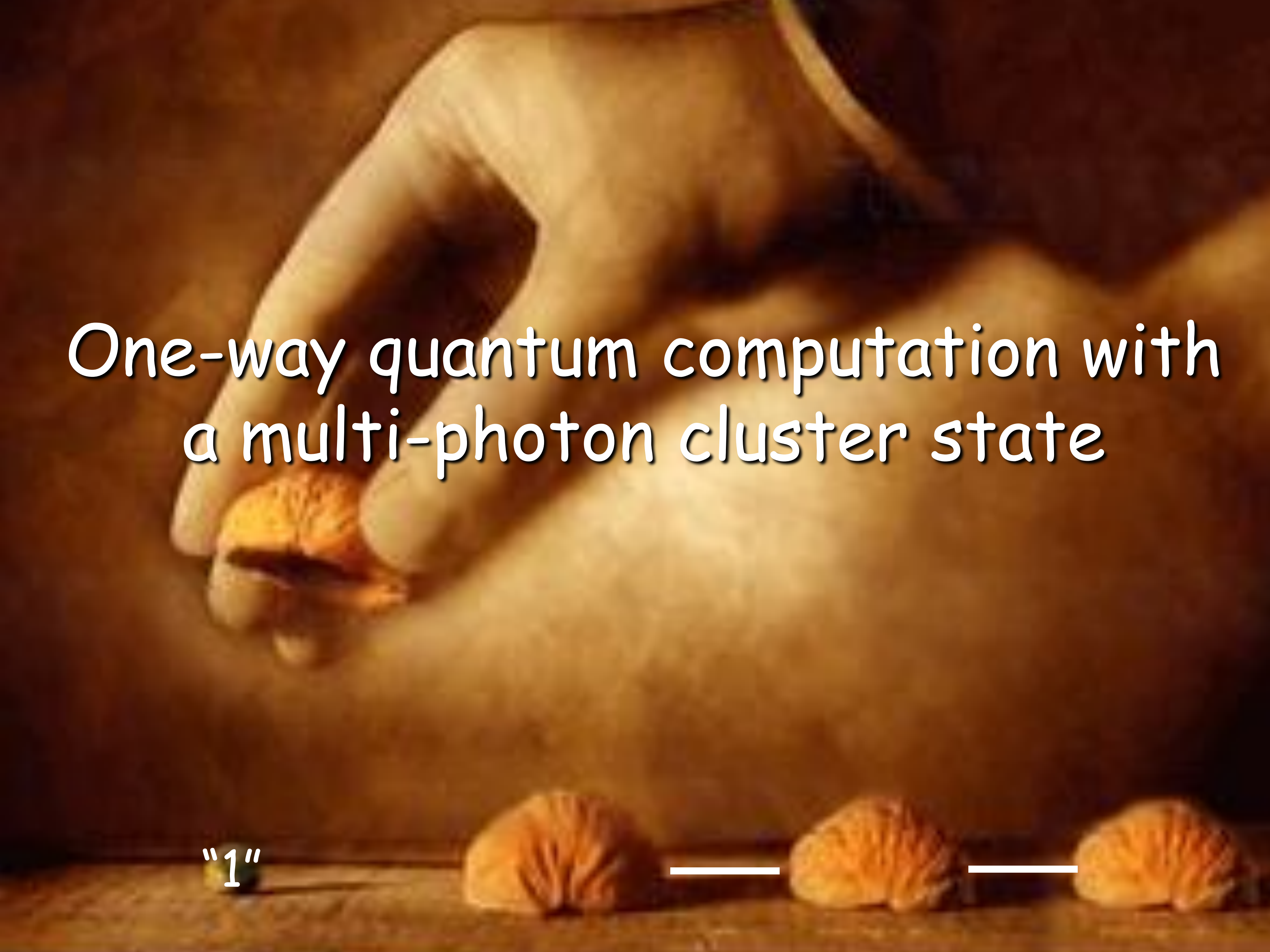
- Longer distances, Higher bit rates
- Active components to compensate atmosphere
- Long-distance quantum interference (repeaters)
- Full cryptography, different protocols
- Moving targets (satellites, airplanes)

IQC free-space experiment

- Gregor Weihs
- Raymond Laflamme
- Chris Erven

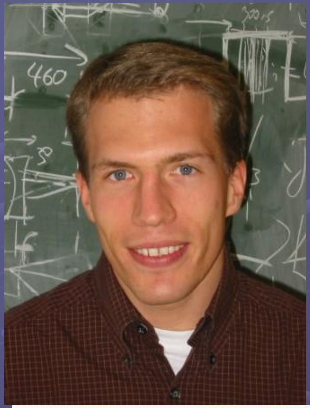
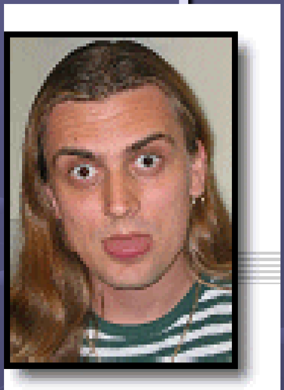


One-way quantum computation with a multi-photon cluster state



Photonic one-way quantum computation

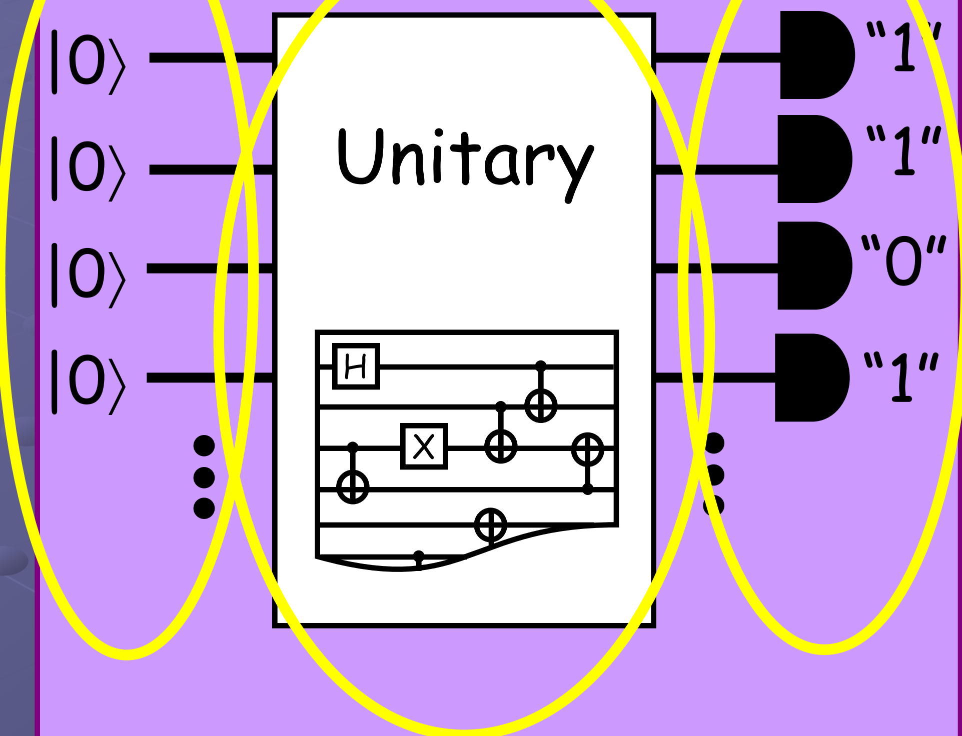
- Philip Walther (Vienna→Harvard)
- Terry Rudolph (Imperial)
- Emmanuel Schenck (Vienna→ENS)
- Vlatko Vedral (Leeds)
- Markus Aspelmeyer (Vienna)
- Harald Weinfurter (LMU, Munich)
- Anton Zeilinger (Vienna)




QC - Circuit vs. One-way model

Circuit Model

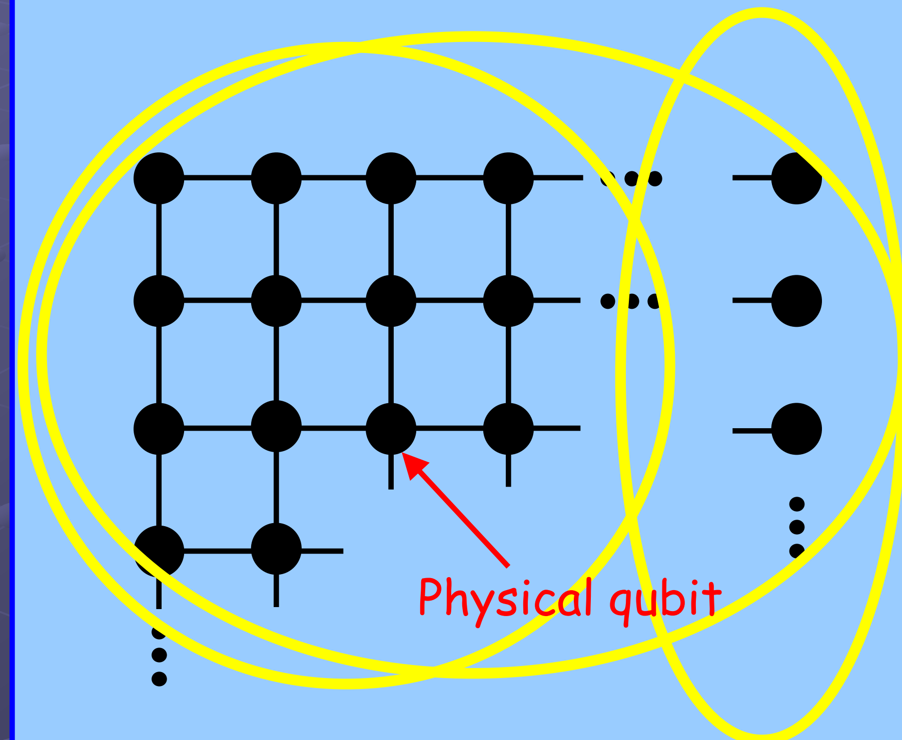


Initialization (all qubits |0⟩)

Algorithm (dynamics)

Readout (classical bits)

One-way model



Initialization (prepare a "cluster state")

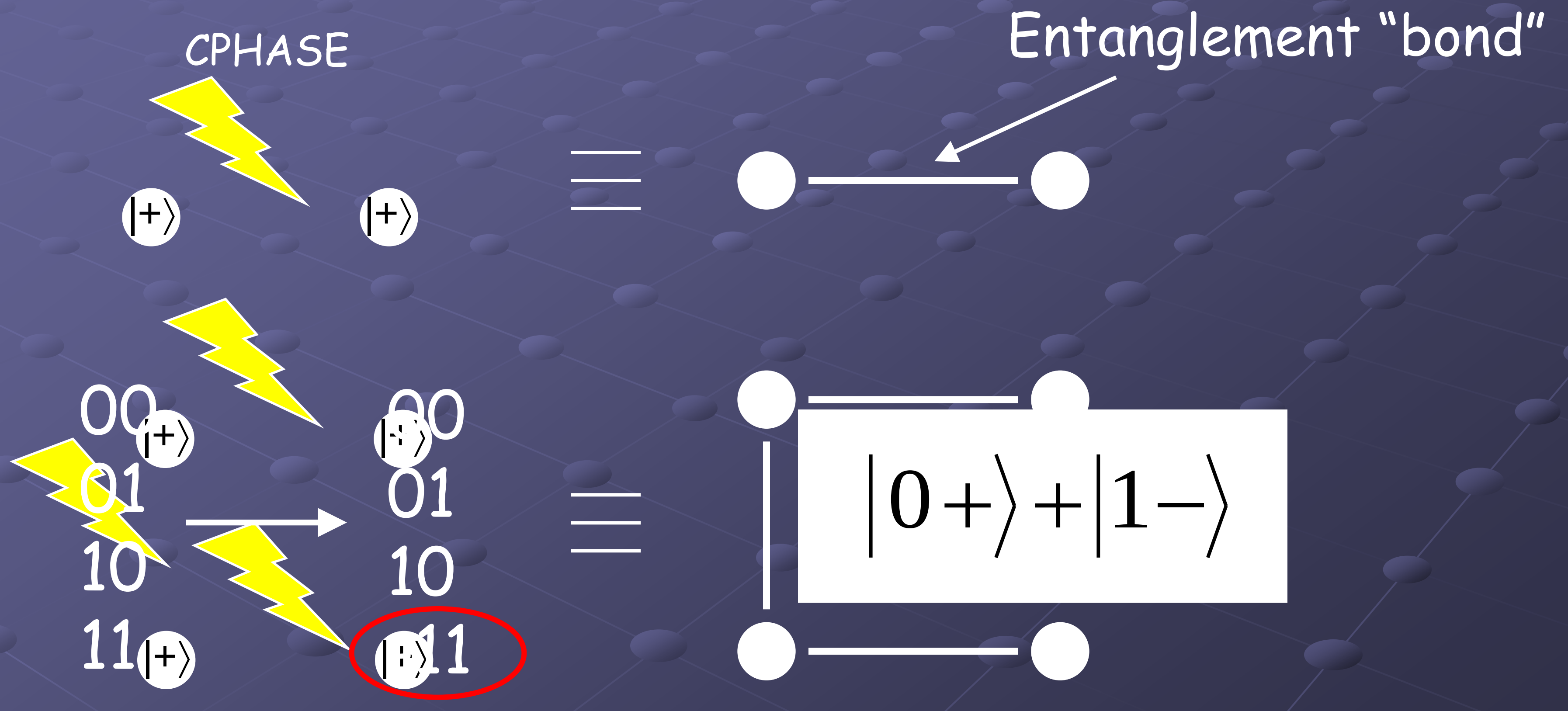
Algorithm (single-qubit measurements)

Readout (single-qubit measurements)

Raussendorff & Briegel, PRL 86, 5188 (2001)
Optics: Neilsen; Browne/Rudolph

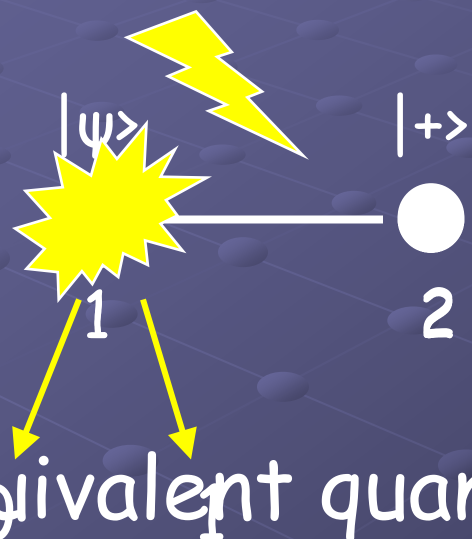
One-way quantum computing

- Cluster states can be represented by graphs



Processing encoded information

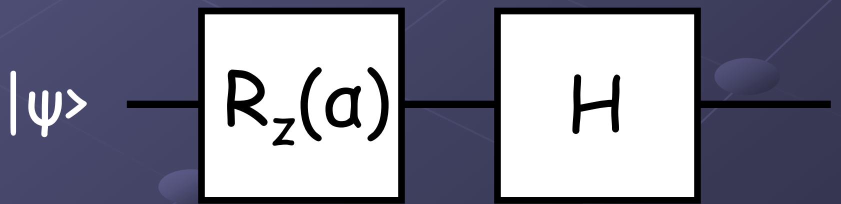
- How measurement can compute



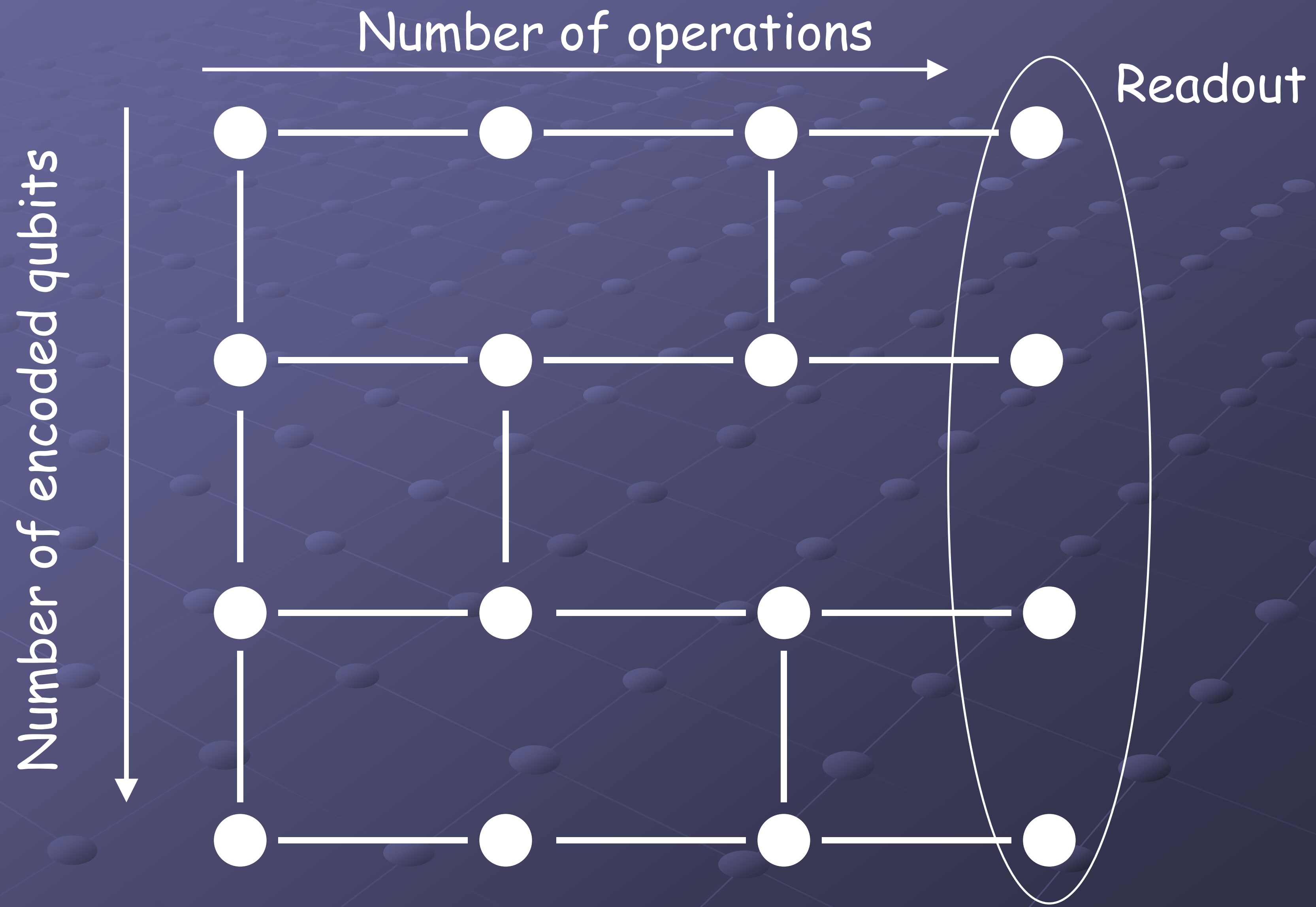
[illegible]

This is an example of Feed-forward

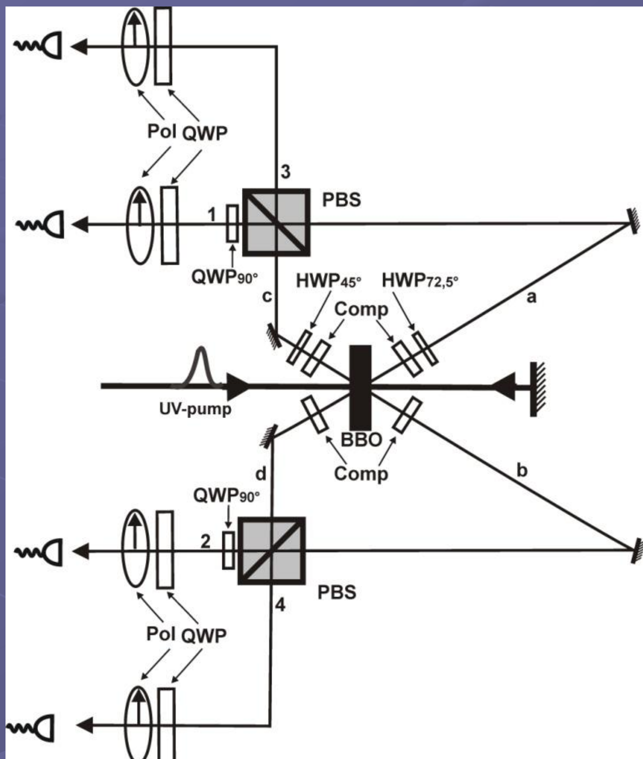
- Equivalent quantum circuit

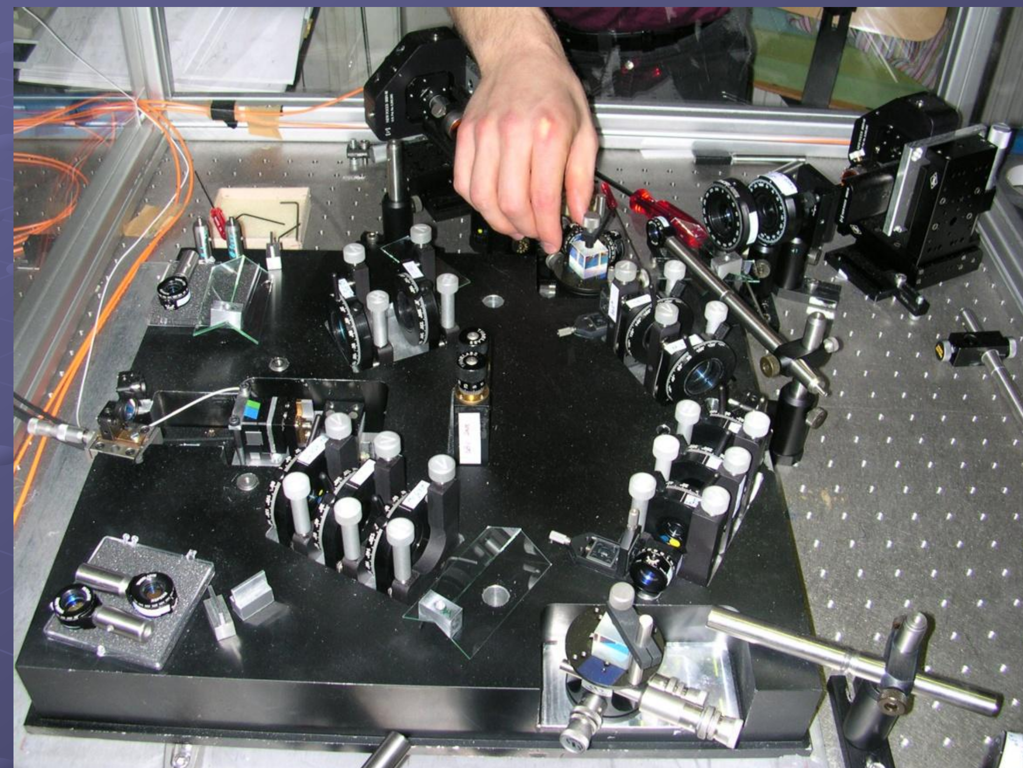


More general computations



Making cluster states

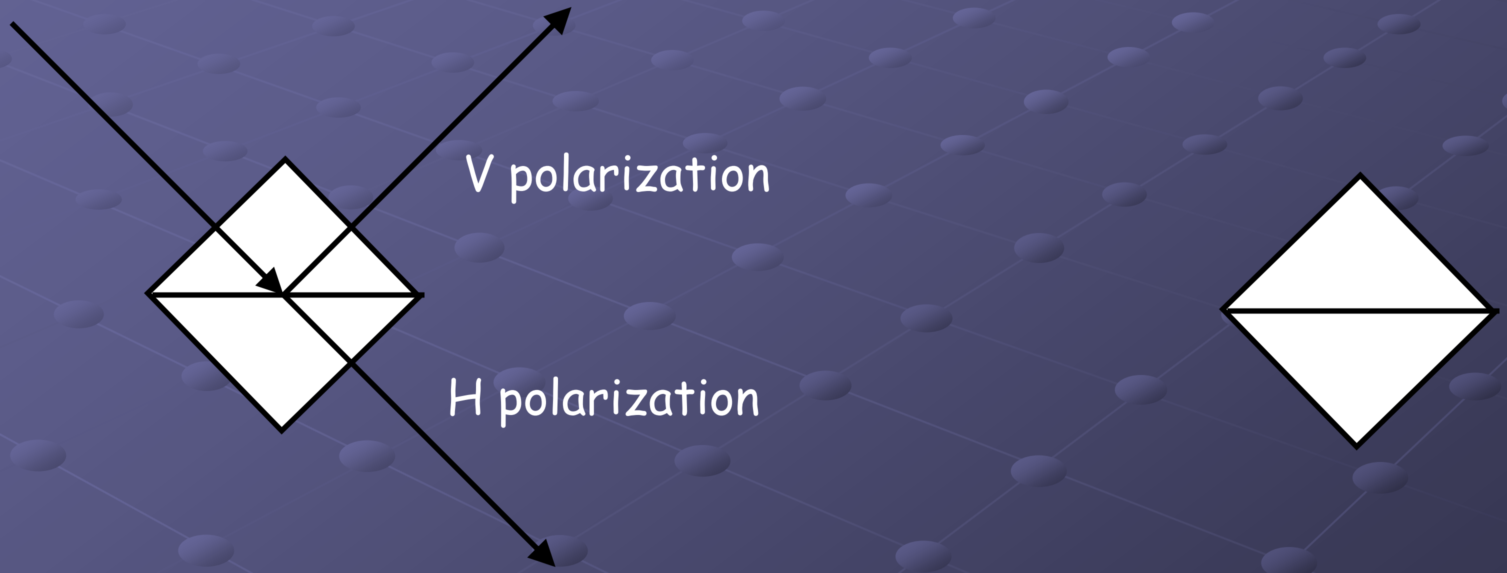




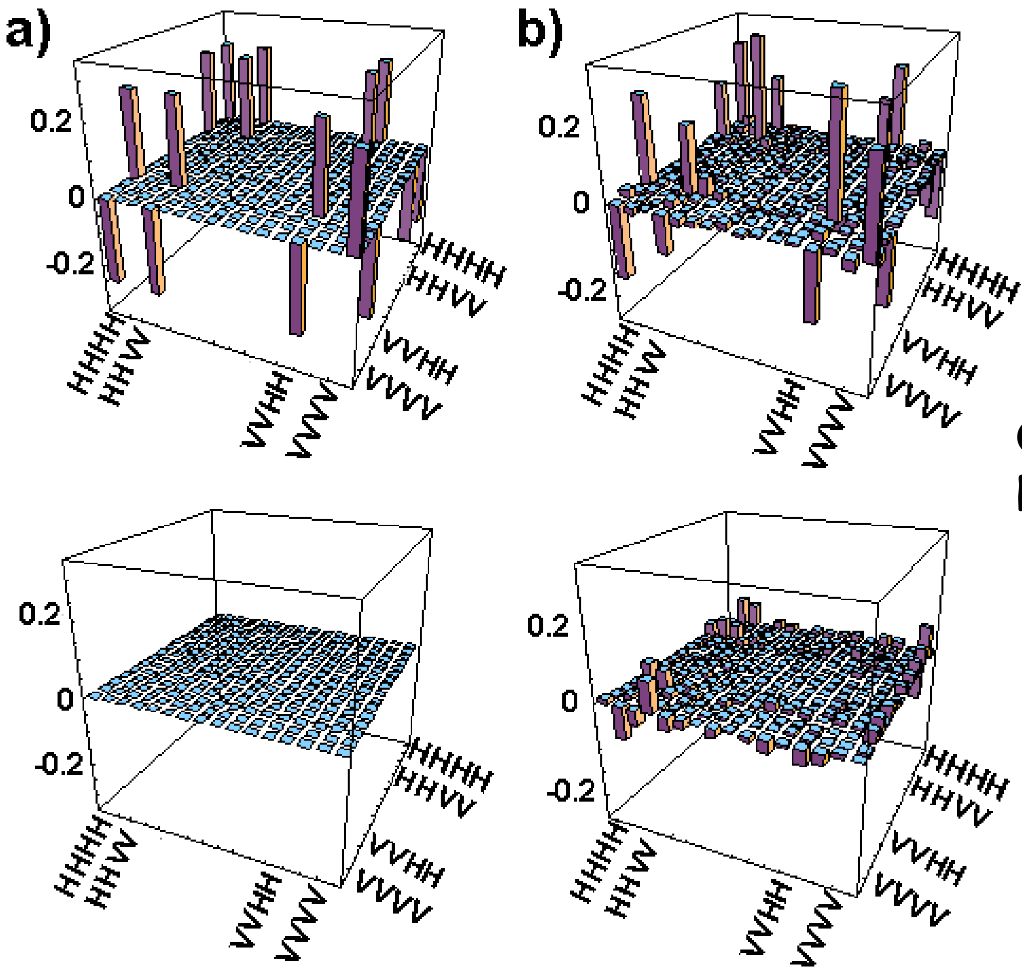
$$|\psi\rangle = |HHHH\rangle + |HHVV\rangle + |VVHH\rangle - |VVVV\rangle$$

Polarizing Beam-splitter

- Quantum "parity check"



The four-photon cluster



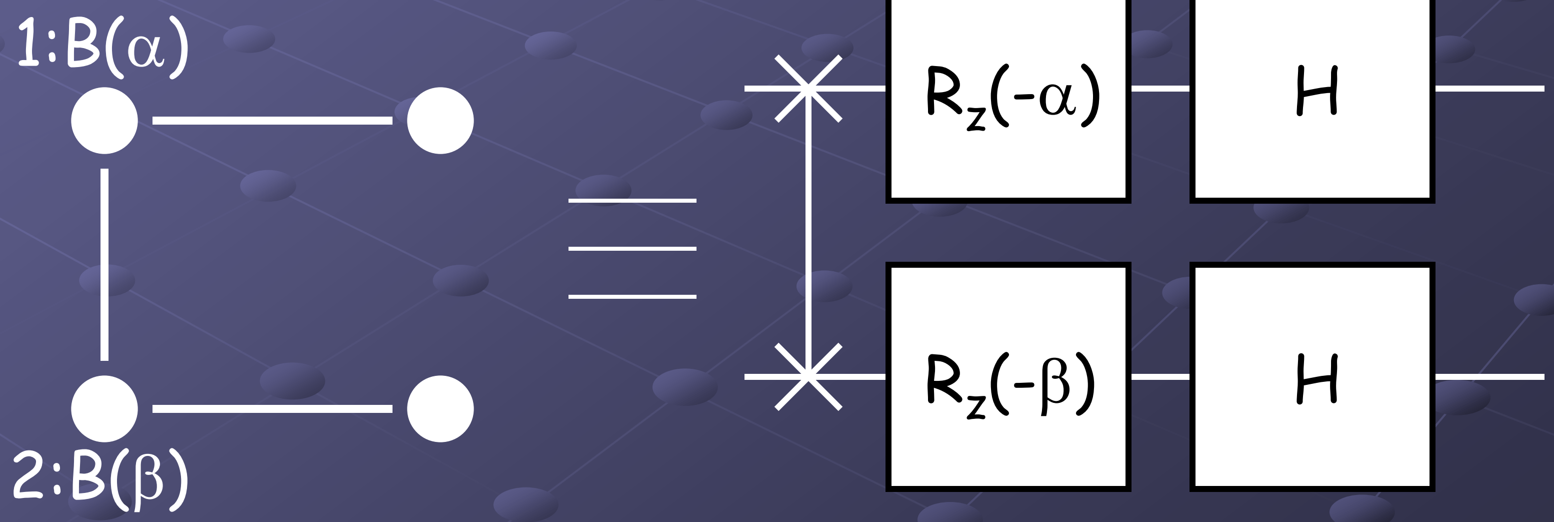
Quantum state tomography
Reconstructed density matrix

Fidelity = 63%

Clusters to circuits

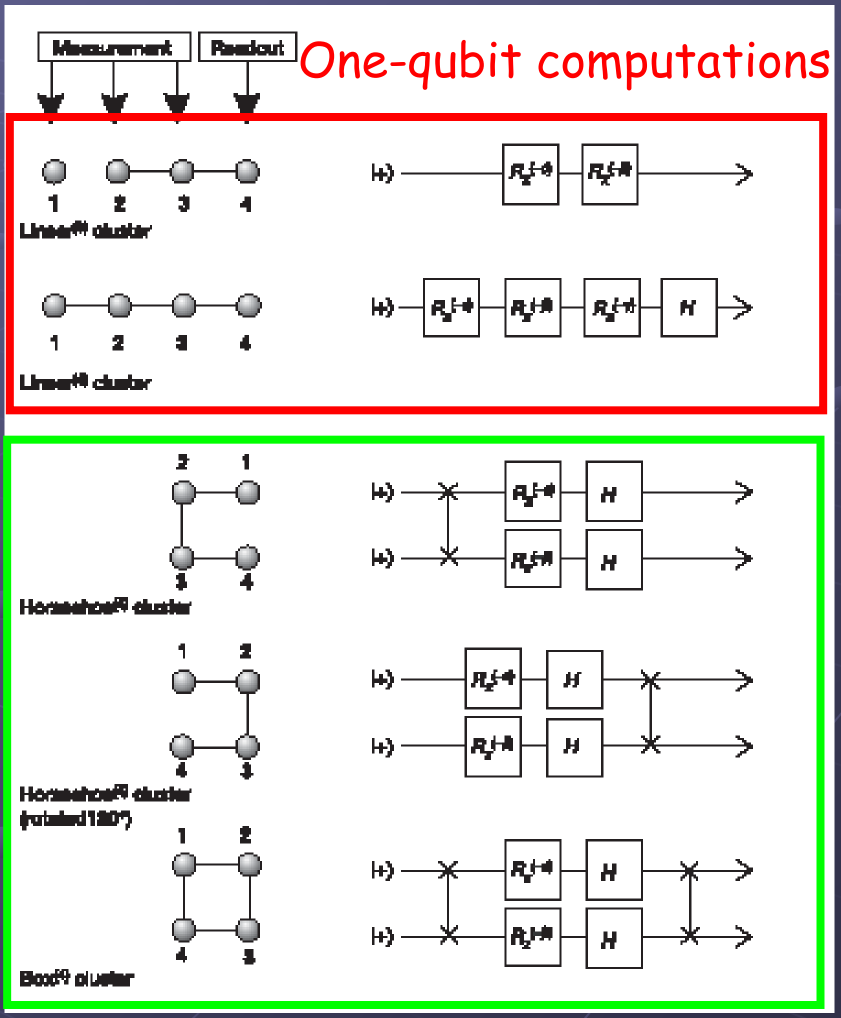
- Horizontal bond:

- Vertical bond:



Clusters to circuits

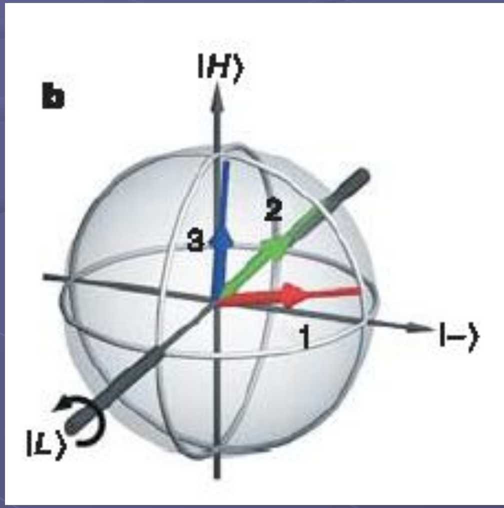
- Multiple circuits using a single cluster
- Different order of measurements



Two-qubit computations

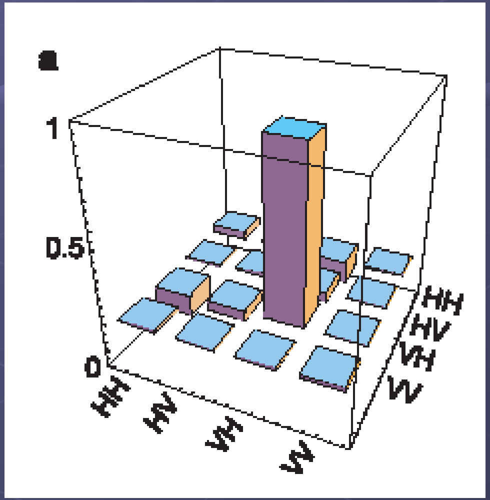
Single & two-qubit operation

Single-qubit rotations



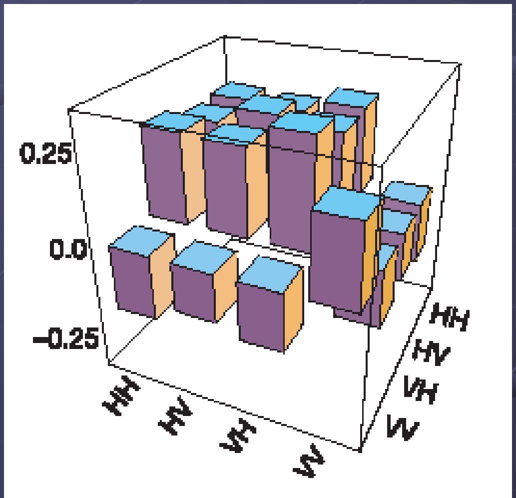
Fid ~ 83-86%

Two-qubit operations



Separable

Fid = 93%
Tangle = 0



Entangled

Fid = 84%
Tangle = 0.65

Grover's Algorithm

L.K. Grover, Phys. Rev. Lett. **79**, 325-328 (1997).

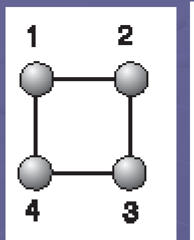
Conclusions and Future directions

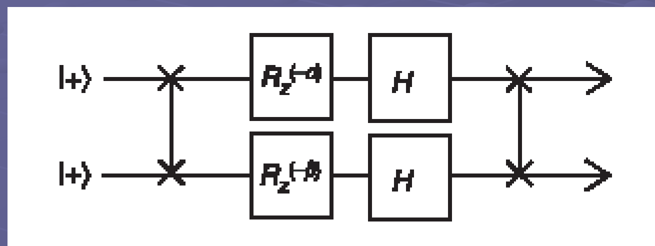
- First demonstration of one-way quantum computation using cluster states
- Experimental
  - Larger cluster states = more complex circuits
  - Feed-forward – two types – easy and hard
- Theoretical
  - Different geometries and measurements
  - Higher dimensions

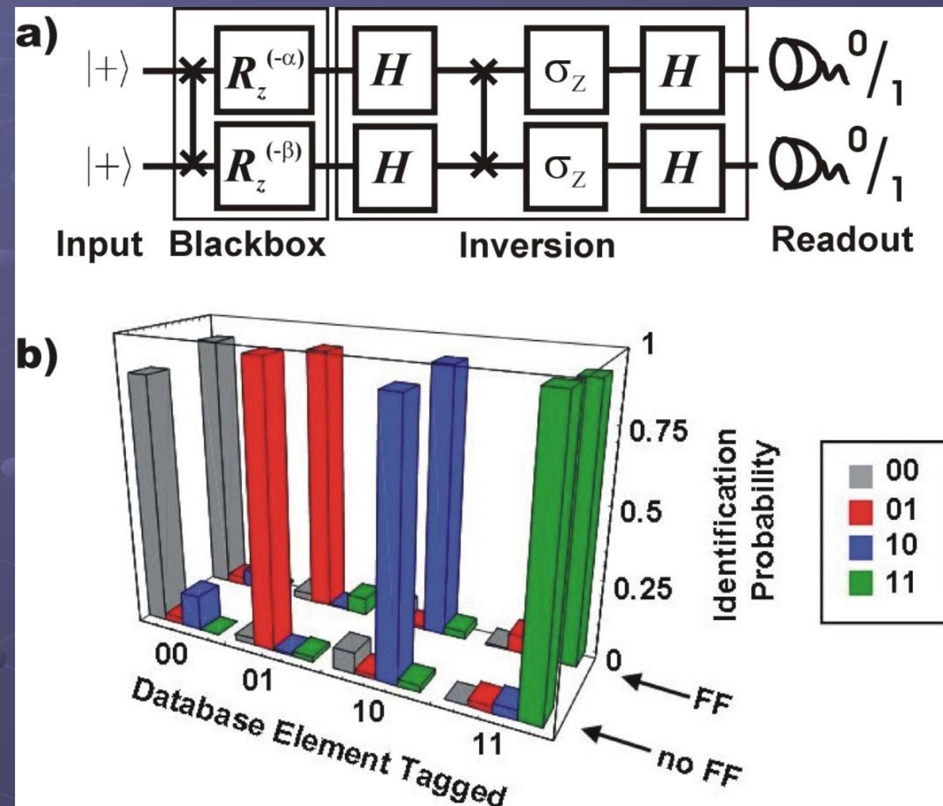
Summary

- "Real" world
  - First experiments demonstrating free-space entanglement distribution
- Ideal world
  - First demonstration of Cluster State Quantum Computing – including the first algorithm

Clusters/Grover's Algorithm



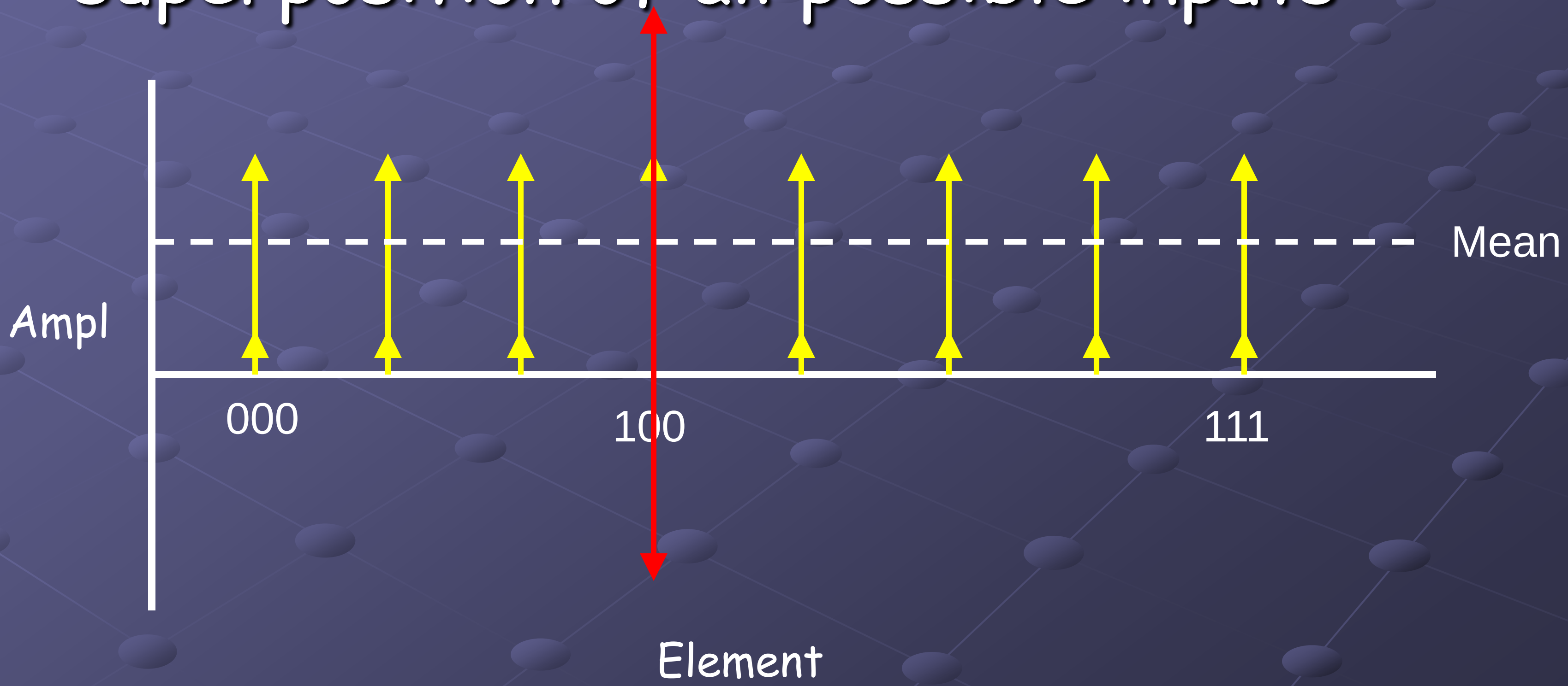




- 90% correct computational output
- First algorithm in the cluster model

Grover's algorithm

- Quantum parallelism
- GA initializes the qubits to equal superposition of all possible inputs



- Interference
- "Inversion about the mean" amplifies the correct element and reduces the others
- On a query to the black box (quantum database/phonebook), the sign of the amplitude of the special element is flipped

THANK YOU!

University of Waterloo

NSERC CRSNG

FWF Der Wissenschaftsfonds.

RAMBOQ

IQC Institute for Quantum Computing

Australian Government

Australian Research Council