Quantum Communication

Serge Massar
Université Libre de Bruxelles

Plan

- Why Quantum Communication?
- Prepare and Measure schemes
  - QKD
- Using Entanglement
- Teleportation
- Communication Complexity
- And now what?

Talk: Theoretical Concepts & Illustrative Experiments

Quantum Communication

Why?

How?

Quantum Communication

Why?

- Quantum Crypto
  - Q. Key Distribution
  - Other protocols
    - Coin Tossing, etc…
- Communication Complexity
- Foundations of Physics

How?

Quantum Communication

Why?

- Quantum Crypto
  - Q. Key Distribution
  - Other protocols
    - Coin Tossing, etc…
- Communication Complexity
- Foundations of Physics

How?

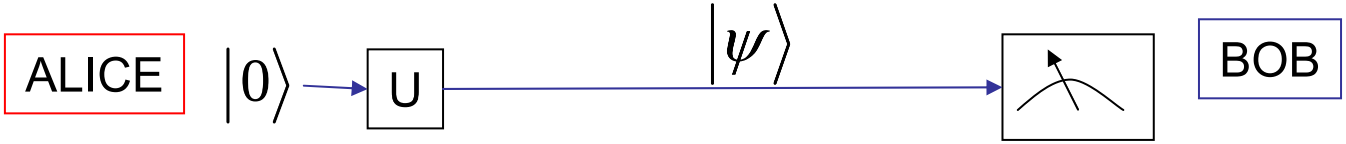
Photons

$$\vec{E}\left(\vec{x},t\right) = A\vec{u}\cos\left[\omega t - \vec{k}.\vec{x} - \varphi\right]$$

- $\vec{u}$ Polarization
- ω, t Frequency/Energy
- $\vec{k}, \vec{x}$ Momentum/Position
- A, φ Amplitude/Phase

- Wavelength
  - Visible: Free Space
  - Near IR: fiber optics $\lambda \simeq 1.5\mu m$

- Protocols in which a single qubit is
  - Prepared
  - Sent
  - Measured



- Quantum Key Distribution

Quantum Key Distribution

Alice Eve Bob

- Alice and Bob want to share a secret key

$r_1 r_2 r_3 \ldots r_N \in \{0,1\}$ $r_1 r_2 r_3 \ldots r_N$

Quantum Key Distribution

Alice Eve Bob

- Alice and Bob want to share a secret key

$r_1 r_2 r_3 \ldots r_N \in \{0,1\}$ $r_1 r_2 r_3 \ldots r_N$

- Eve should not learn the key
- If Eve tries to learn the key, she is detected

Quantum Key Distribution

Alice | Eve | Bob

- Alice and Bob want to share a secret key

$r_1 r_2 r_3 \ldots r_N \in \{0,1\}$ $\qquad$ $r_1 r_2 r_3 \ldots r_N$

- Eve should not learn the key
- If Eve tries to learn the key, she is detected

Use quantum communication
& uncertainty principle / no cloning theorem

QKD

- If Alice prepares:

two orthogonal states

$$|0\rangle \pm e^{i\varphi}|1\rangle$$

Send to Bob →

- If Bob measures:

in basis

$$|0\rangle \pm e^{i\varphi}|1\rangle$$

- Then Bob learns which state was prepared by Alice

QKD

- If Alice prepares:

two orthogonal states

$$|0\rangle \pm e^{i\varphi} |1\rangle$$

Send to Bob →

- If Bob measures:

in basis

$$|0\rangle \pm e^{i\varphi} |1\rangle$$

- Then Bob learns which state was prepared by Alice

!!!But Eve can also learn the state by Measuring in same basis!!!

QKD: Trick

- Alice randomly prepares

bit=0,1 $|0\rangle \pm |1\rangle$

bit=0,1 $|0\rangle \pm i|1\rangle$

Send to Bob →

- Bob randomly measures in

$|0\rangle \pm |1\rangle$ 0° basis

$|0\rangle \pm i|1\rangle$ 90° basis

Now Eve is stymied.
In which basis to measure?
!!If she learns information, she disturbs the state!!

QKD: Trick

- Alice randomly prepares

bit=0,1 $|0\rangle \pm |1\rangle$

bit=0,1 $|0\rangle \pm i|1\rangle$

Send to Bob

- Bob randomly measures in

$|0\rangle \pm |1\rangle$ 0° basis

$|0\rangle \pm i|1\rangle$ 90° basis

Now Eve is stymied.
In which basis to measure?
!!If she learns information, she disturbs the state!!

Alice and Bob can obtain a secret key by revealing publicly at a later stage the basis used. If the basis are the same, the prepared and measured state constitute the secret key.

QKD: Example

Emission φ	0°	90°	180°	90°	0°	270°	180°	0°	90°
Bit Sent	0	0	1	0	0	1	1	0	0
Mst Basis	90°	90°	0°	90°	0°	0°	0°	90°	0°
Mst Result	1	0	1	0	0	1	1	1	0
Key	X	0	1	0	0	X	1	X	X

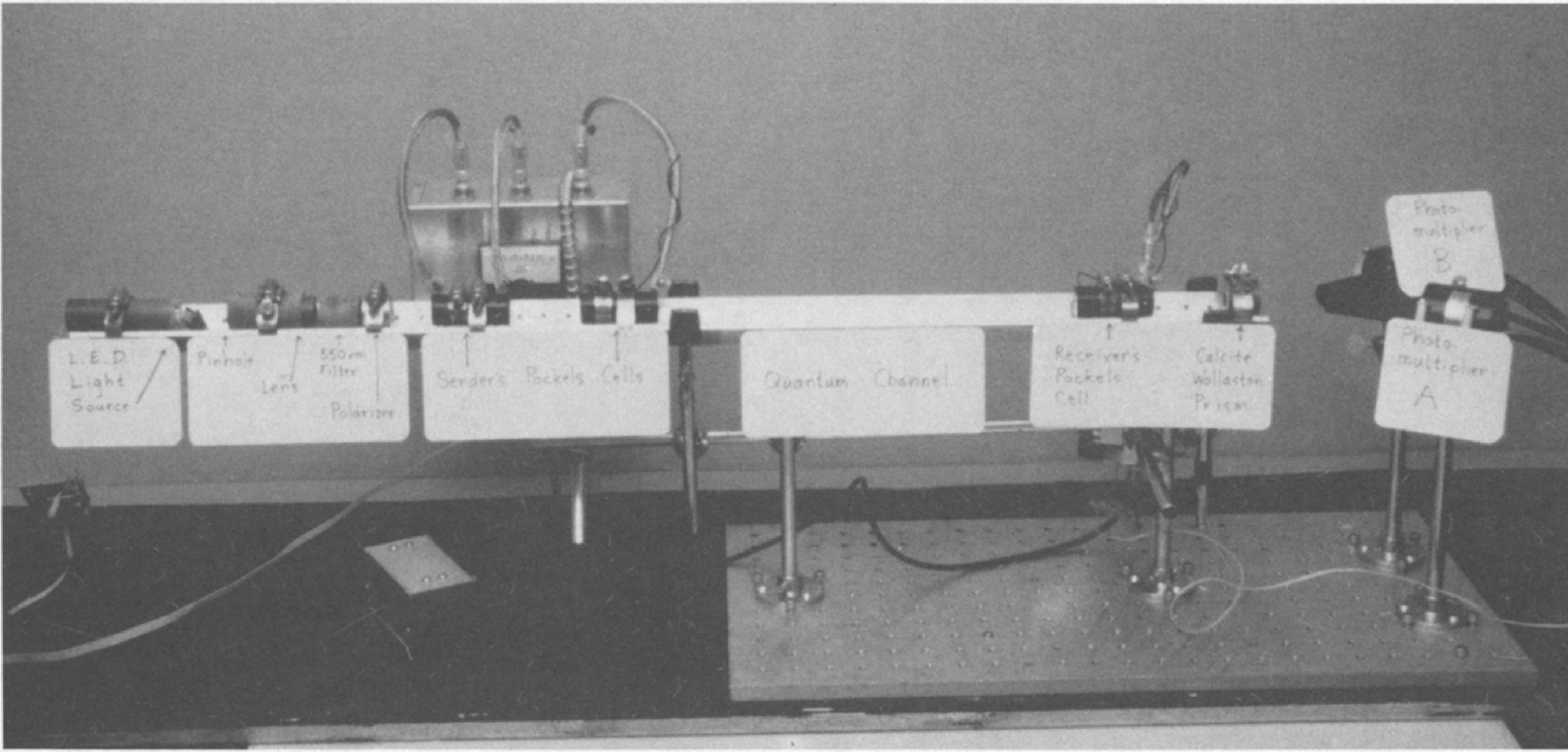
- QKD needs single photon states

- In practice: Attenuated coherent states

  « The poor man's single photon source »

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle \approx \left(1 - \frac{|\alpha|^2}{2}\right)|0\rangle + \alpha|1\rangle + \ldots$$

First QKD Experiment



Propagation distance: 30cm
Key rate ≈ 1 bit/s

Journal of Cryptology 5, 3-28 (1992)

Quantum Cryptography Today

- Key distribution over 50km of optical fiber
- Secret key rate: 1Mbit/s
- Continuous operation for 36hours
- Technique used: time bins

A. R. Dixon *et al.*, *Applied Physics Letters*, **96**, 161102 (2010)

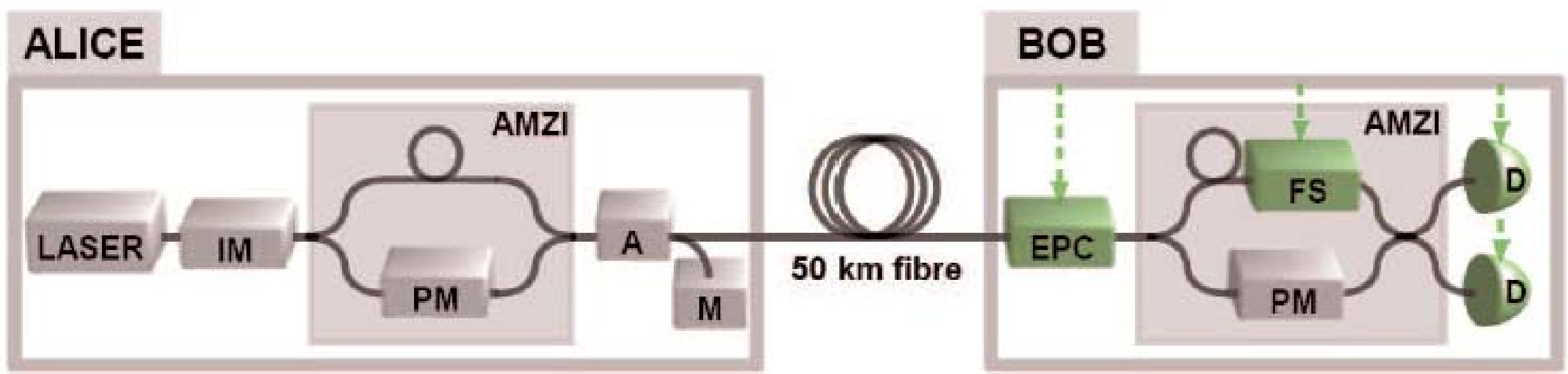
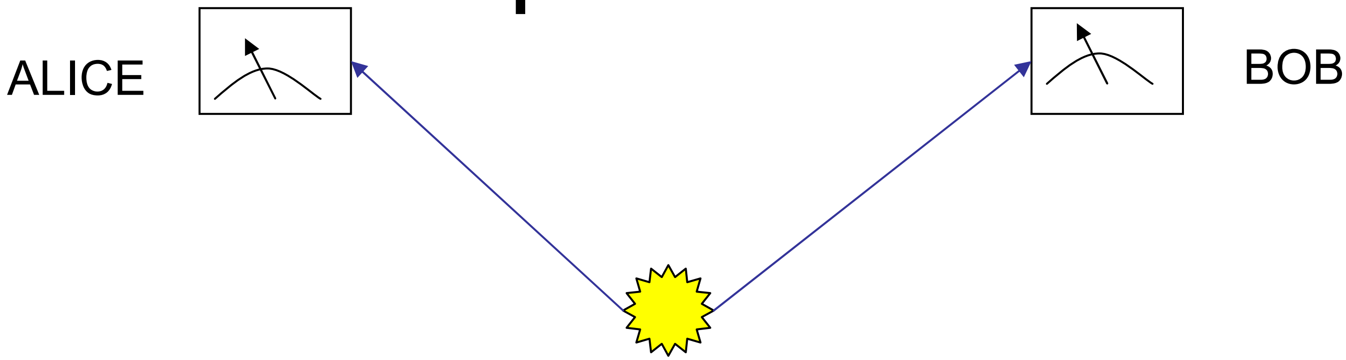


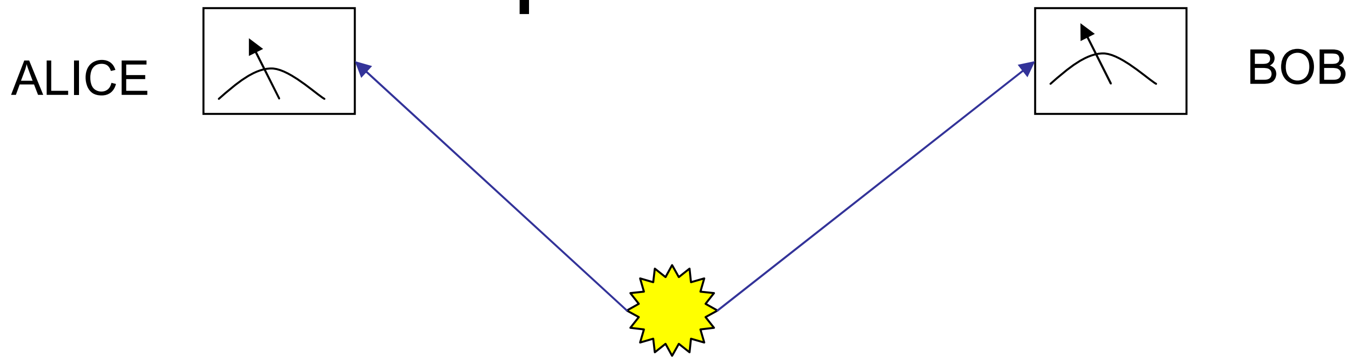
FIG. 1. Schematic of QKD system. IM denotes fiber intensity modulator, PM phase modulator, A attenuator, M optical power meter, EPC electrically-driven polarization controller, FS fiber stretcher, D InGaAs APD detectors. Components in green are feedback-controlled as part of the active stabilization system.

Experiments with entangled photons



$$|\phi^{+}\rangle = \frac{1}{\sqrt{d}} \sum_{k} |k\rangle_{A} |k\rangle_{B}$$

Experiments with entangled photons

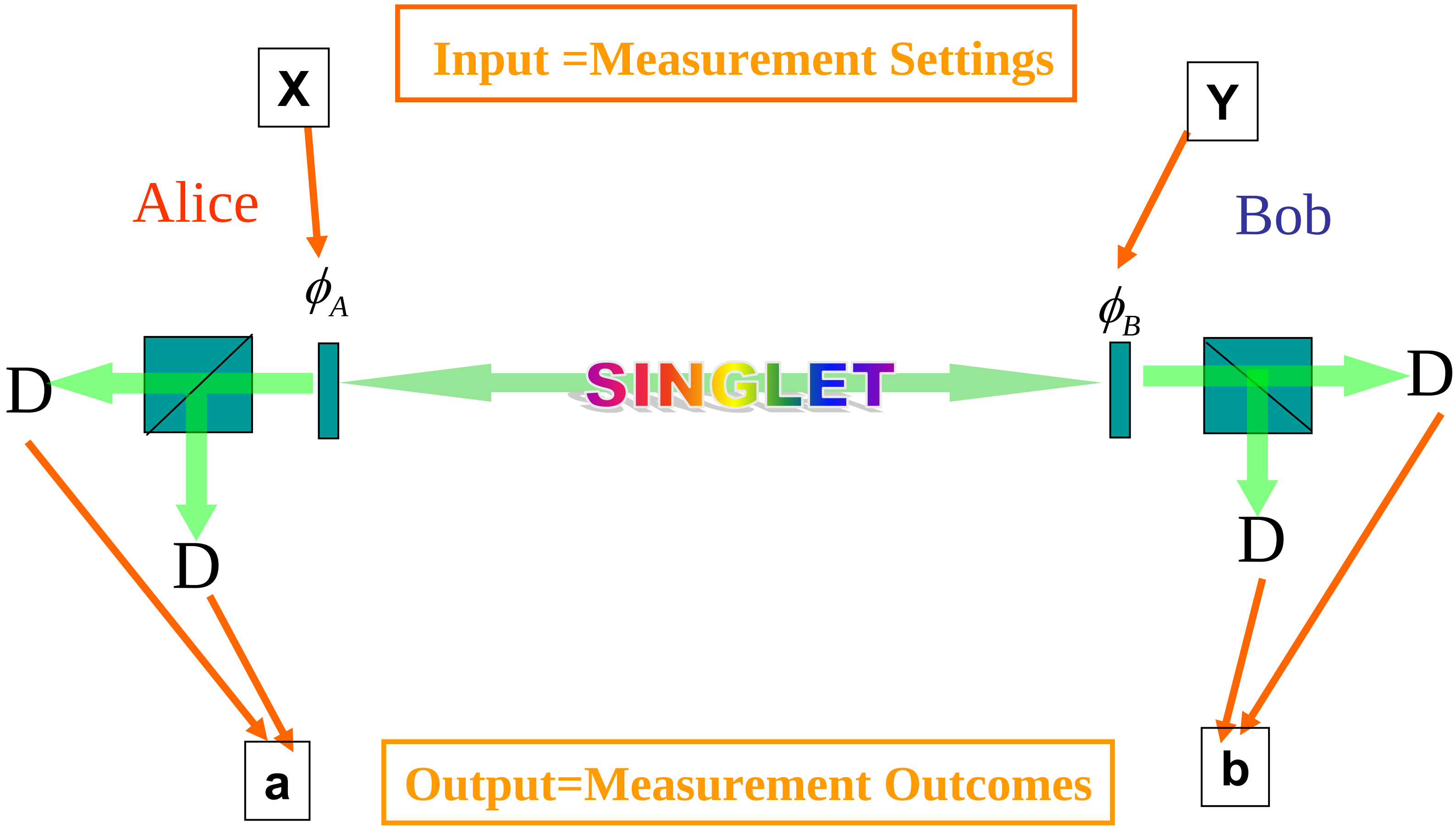


$$|\phi^{+}\rangle = \frac{1}{\sqrt{d}} \sum_{k} |k\rangle_{A} |k\rangle_{B}$$

Why?

- Q. Comm. Over longer distances:
  - Slightly further than prepare and measure schemes
  - First step towards quantum repeaters
- Fundamental test of Nature:
  - Quantum Non Locality
  - Device Independent Quantum Cryptography

Non Locality:
Aspect type experiment



P(ab|XY) = P(A outcome & B outcome | A mst setting & B mst setting)

Implications of Non Locality

Local Hidden Variable Model

$$P(ab \mid xy) = \int d\lambda P(\lambda) P(a \mid x\lambda) P(b \mid y\lambda)$$

If a lhv description is possible, P(ab|xy) satisfies all Bell inequalities

- *l*ocal deterministic description of measurements is possible

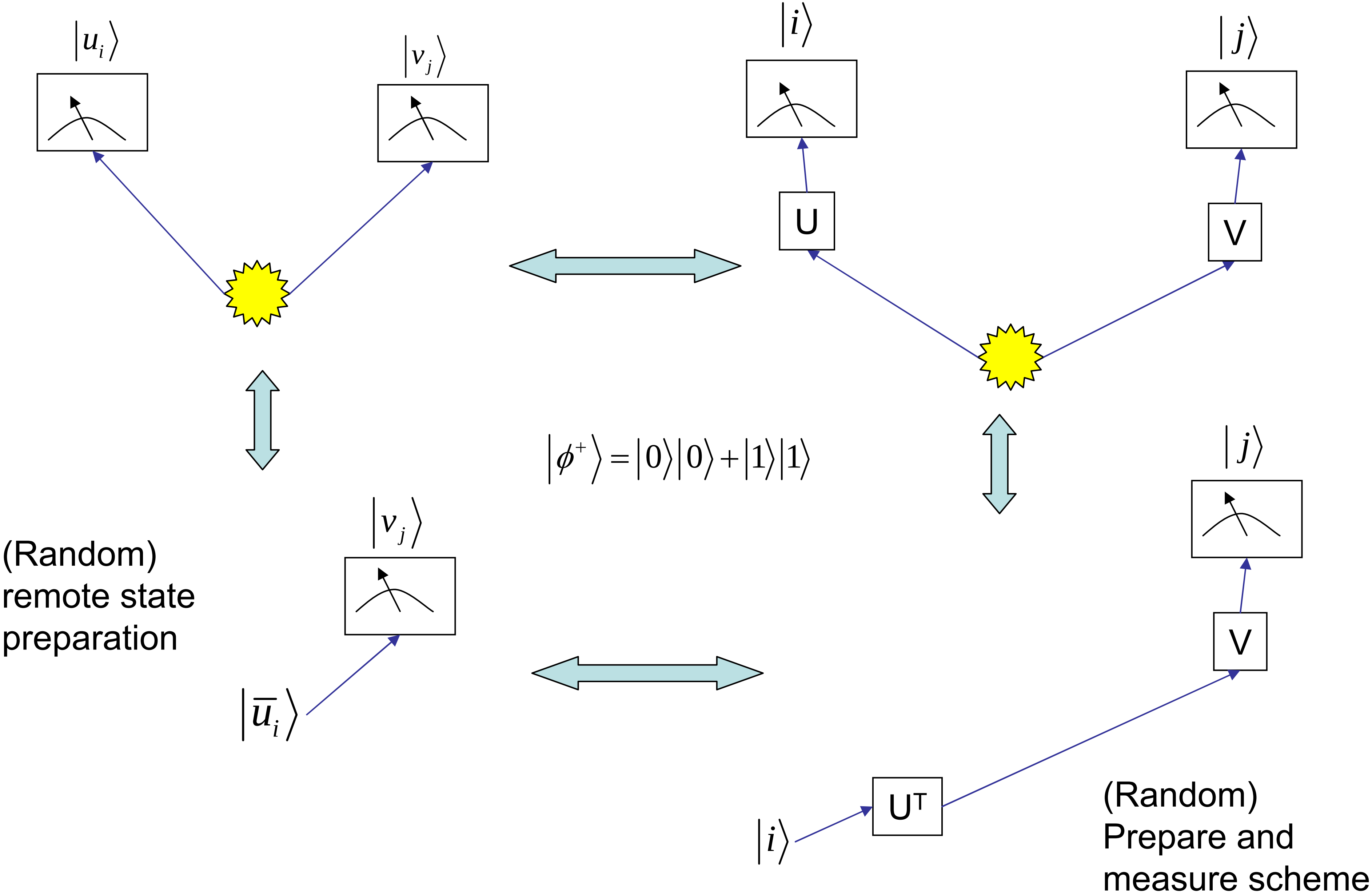
If lhv description is impossible: (Quantum) Non Locality

- measurements results are random, must be secret
- detected by Bell inequality violation

Experiments with entangled particles

Equivalence with remote state preparation
Equivalence with prepare and measure

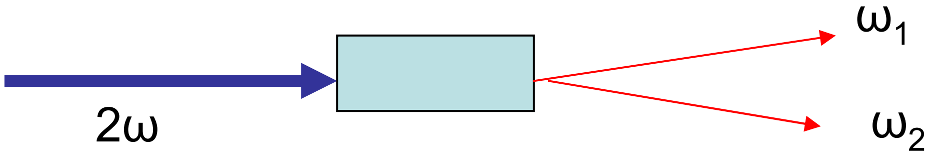
Equivalences between schemes



Entangled Photon source

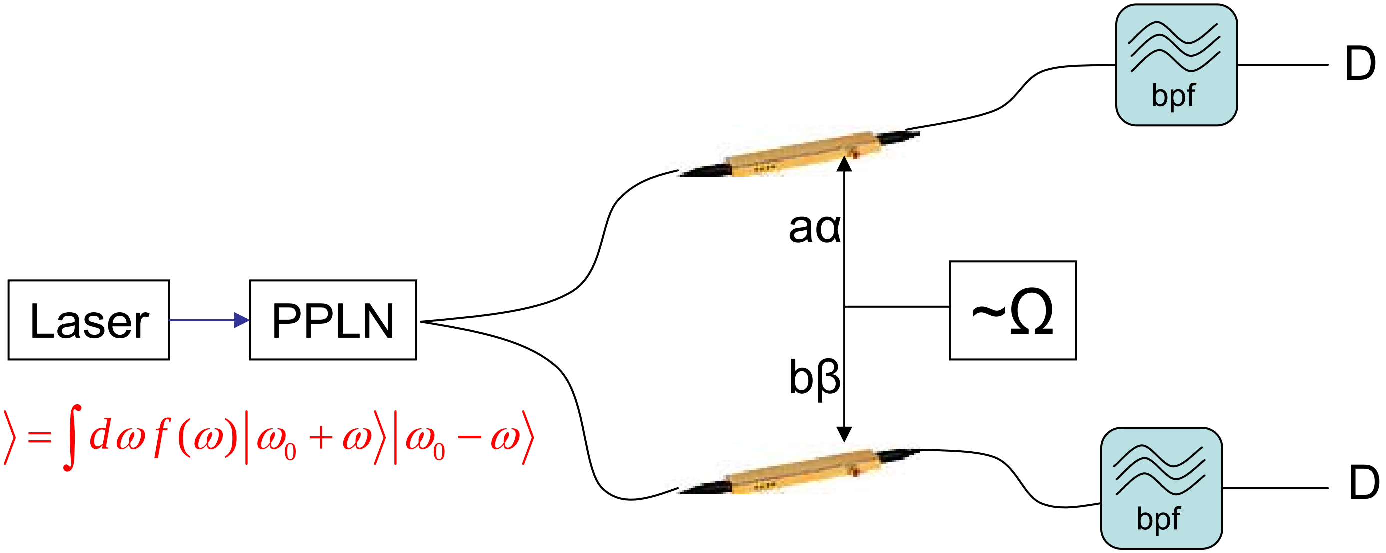
- Frequency Doubling

- Parametric Down Conversion

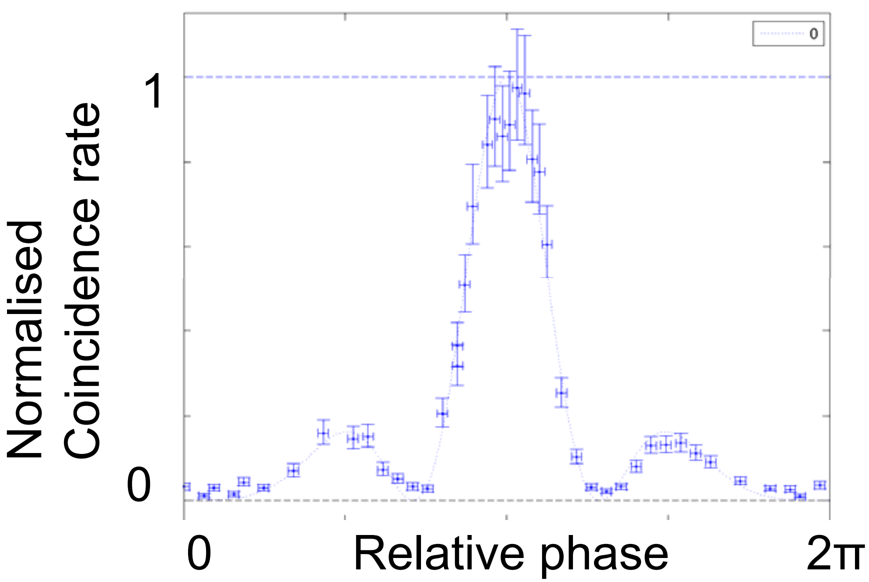


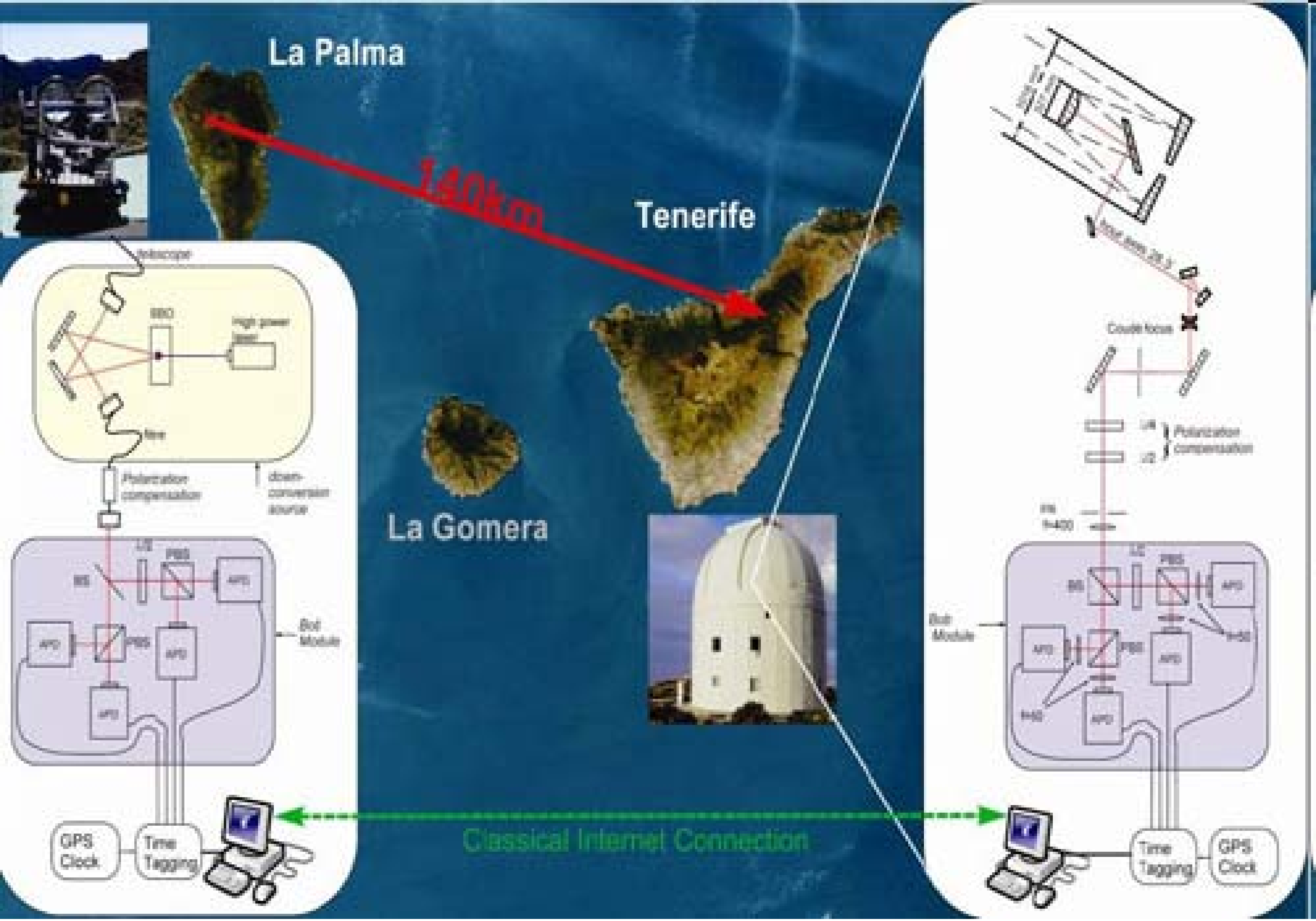
$\omega_1 + \omega_2 = 2\omega$: Energy Conservation
(approximate) Momentum Conservation (Phase Matching Condition)

Frequency Entanglement



$$|\psi\rangle = \int d\omega\, f(\omega) |\omega_0 + \omega\rangle |\omega_0 - \omega\rangle$$

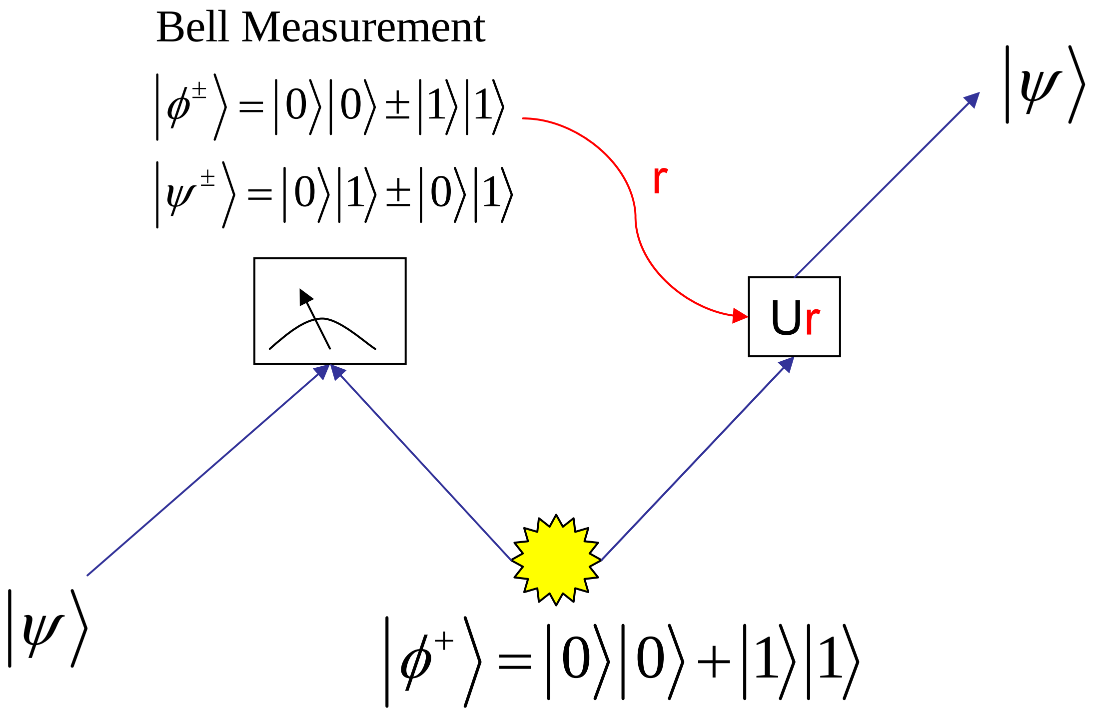




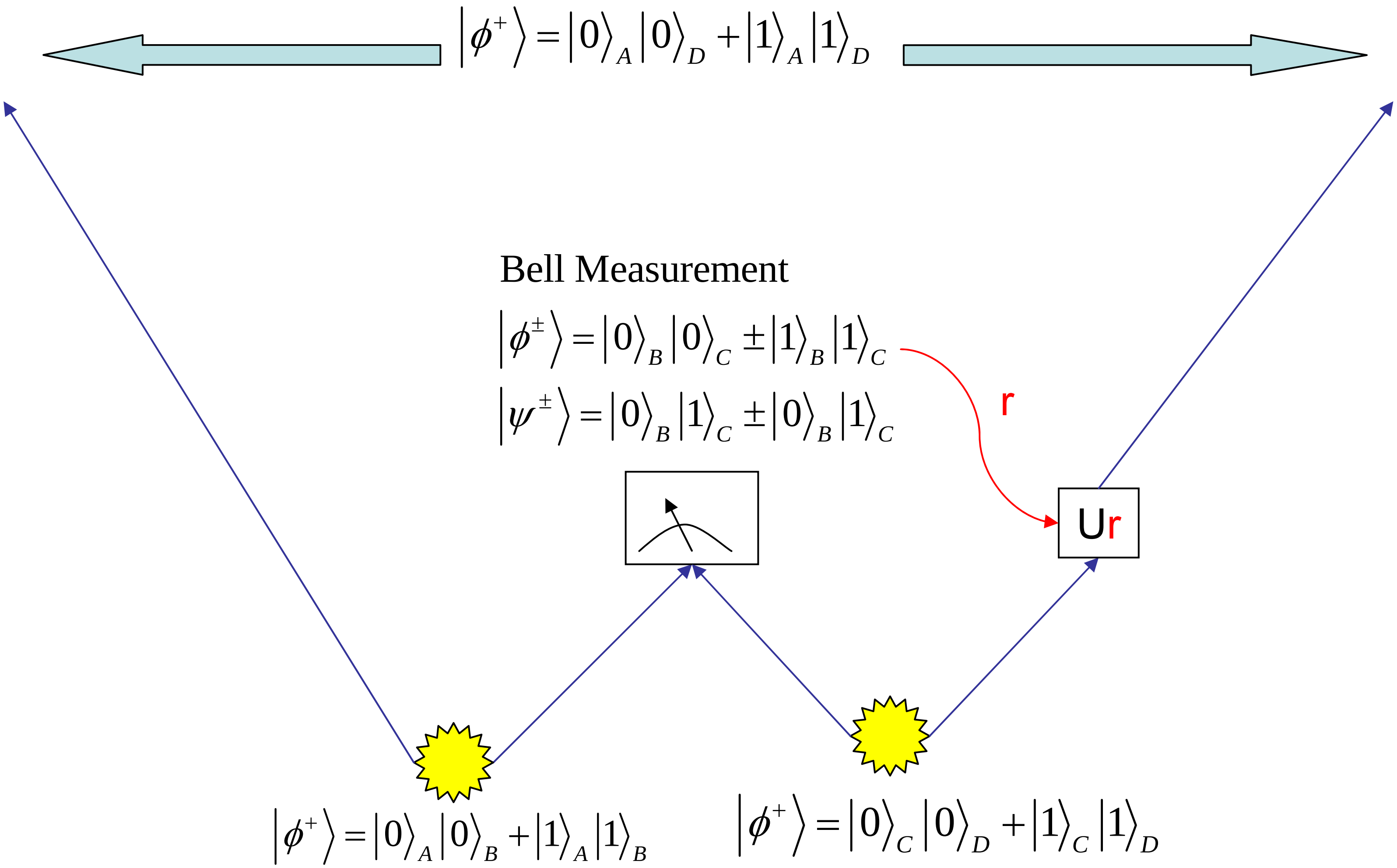
Nature Physics 3, 481 - 486 (2007)

35 coincidences / s

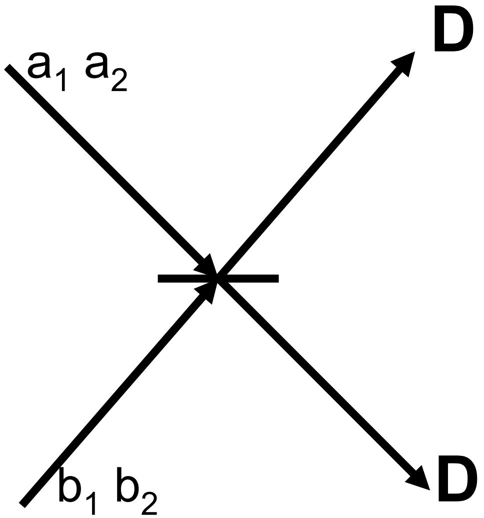
Quantum Teleportation



Entanglement Swapping



Bell State Measurement with Photons



$$|\psi\rangle = \left(\alpha a_1^\dagger b_1^\dagger + \beta a_2^\dagger b_1^\dagger + \gamma a_1^\dagger b_2^\dagger + \delta a_2^\dagger b_2^\dagger\right)|0\rangle$$

Two photons

Two modes in beam a

Two modes in beam b

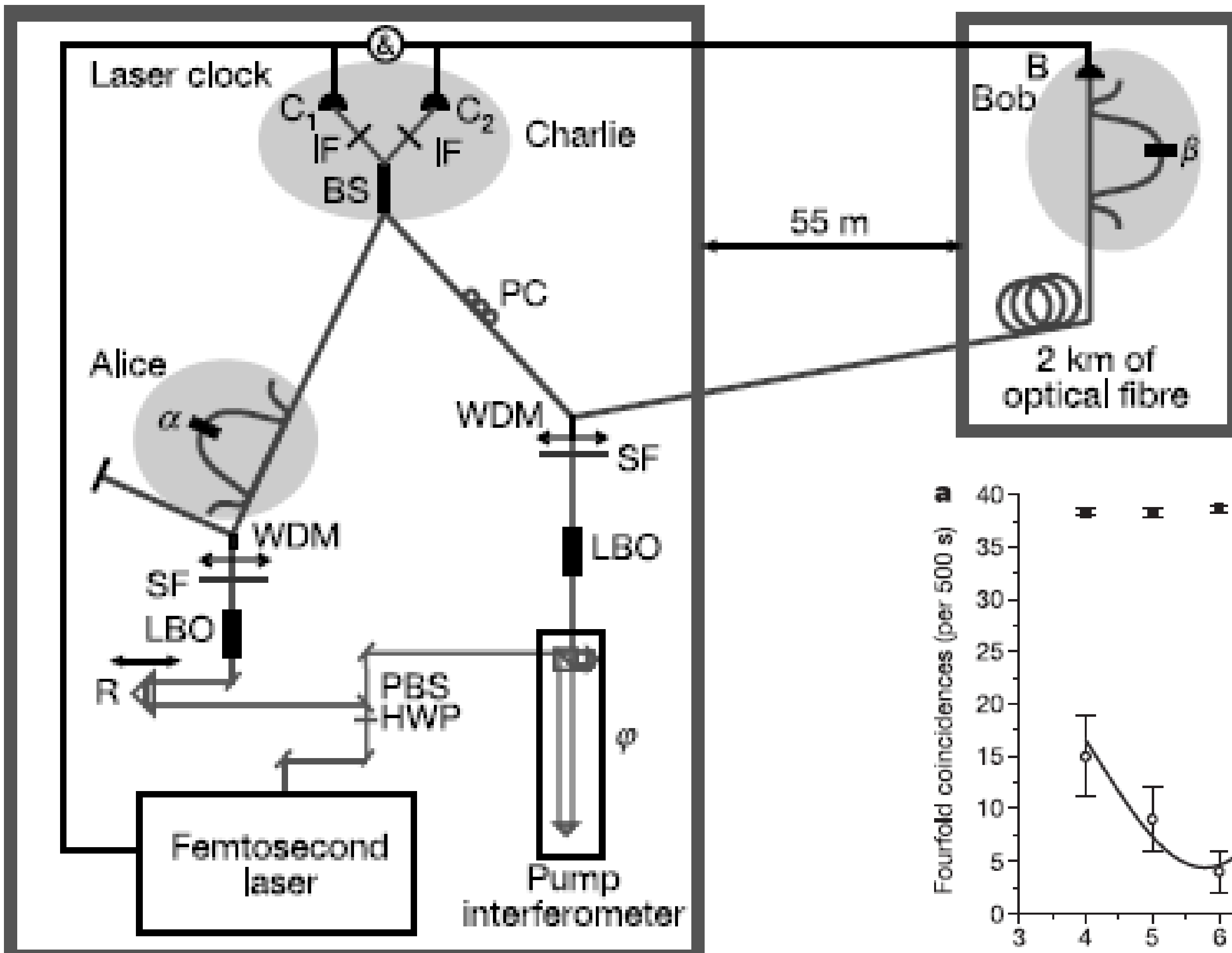
Coincident detection in both detectors implies that initial state was

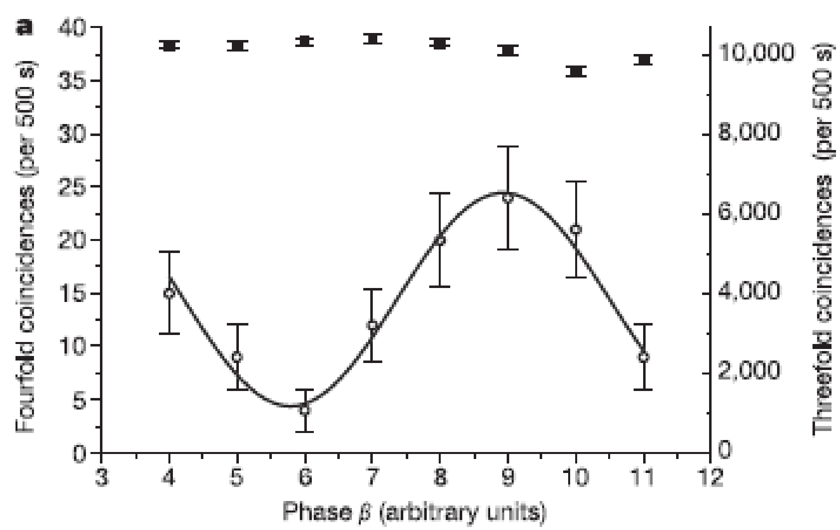
$$|\psi\rangle = \left(\frac{1}{\sqrt{2}} a_1^\dagger b_2^\dagger - \frac{1}{\sqrt{2}} a_2^\dagger b_1^\dagger\right)|0\rangle$$

With probability 1/4 one measures a Bell sta

Experimental Quantum Teleportation.
Telecomunication Wavelengths
distance 55m, passing through a spool of 2km optical fiber

Nature **421**, 509-513 (2003)





Quantum Communication with atoms and photons.

Entanglement of two Yb+ ions

- **Situated in 2 separate vacuum chambers separated by 1m**
- **1 event every 10 minutes**

Advantages:

- **Information can be stored**
- **Interfacable with quantum computer**
- **Detection loophole closed.**

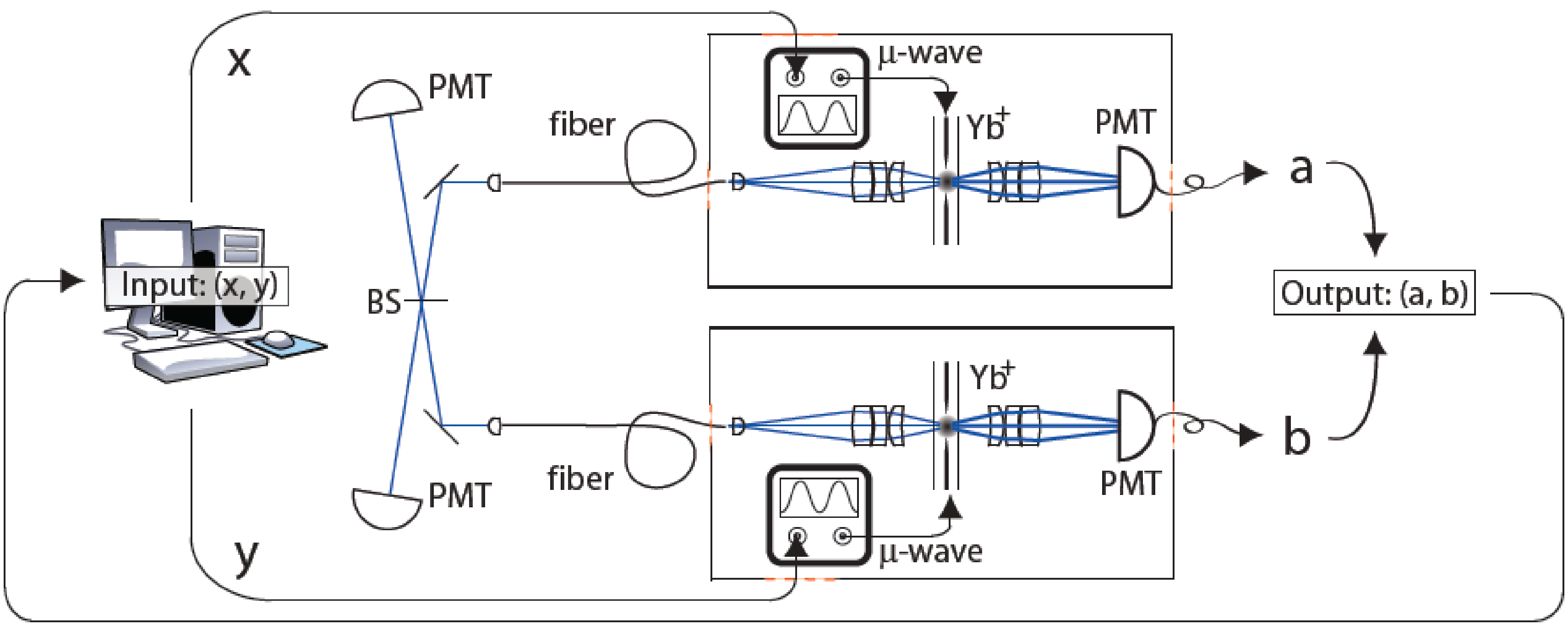
Quantum Communication with atoms and photons.

Entanglement of two Yb+ ions

- **Situated in 2 separate vacuum chambers separated by 1m**
- **1 event every 10 minutes**

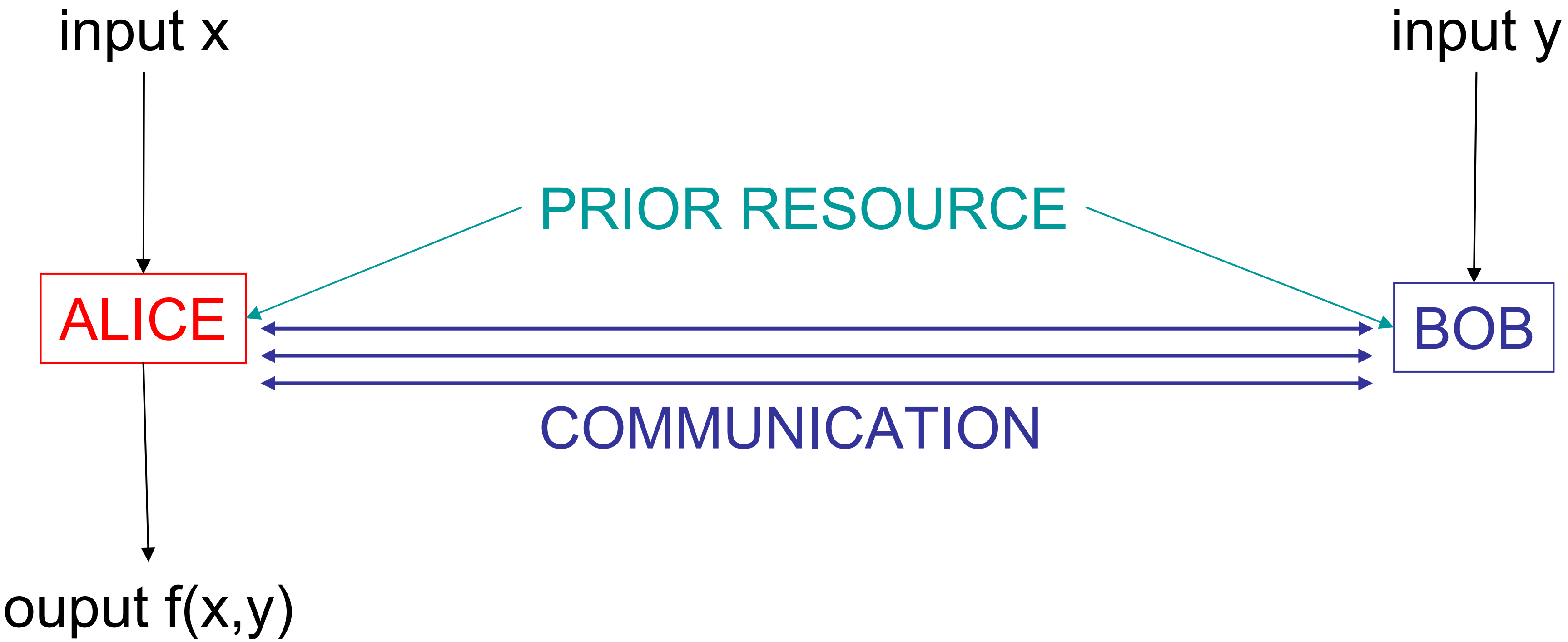
Advantages:

- **Information can be stored**
- **Interfacable with quantum computer**
- **Detection loophole closed.**



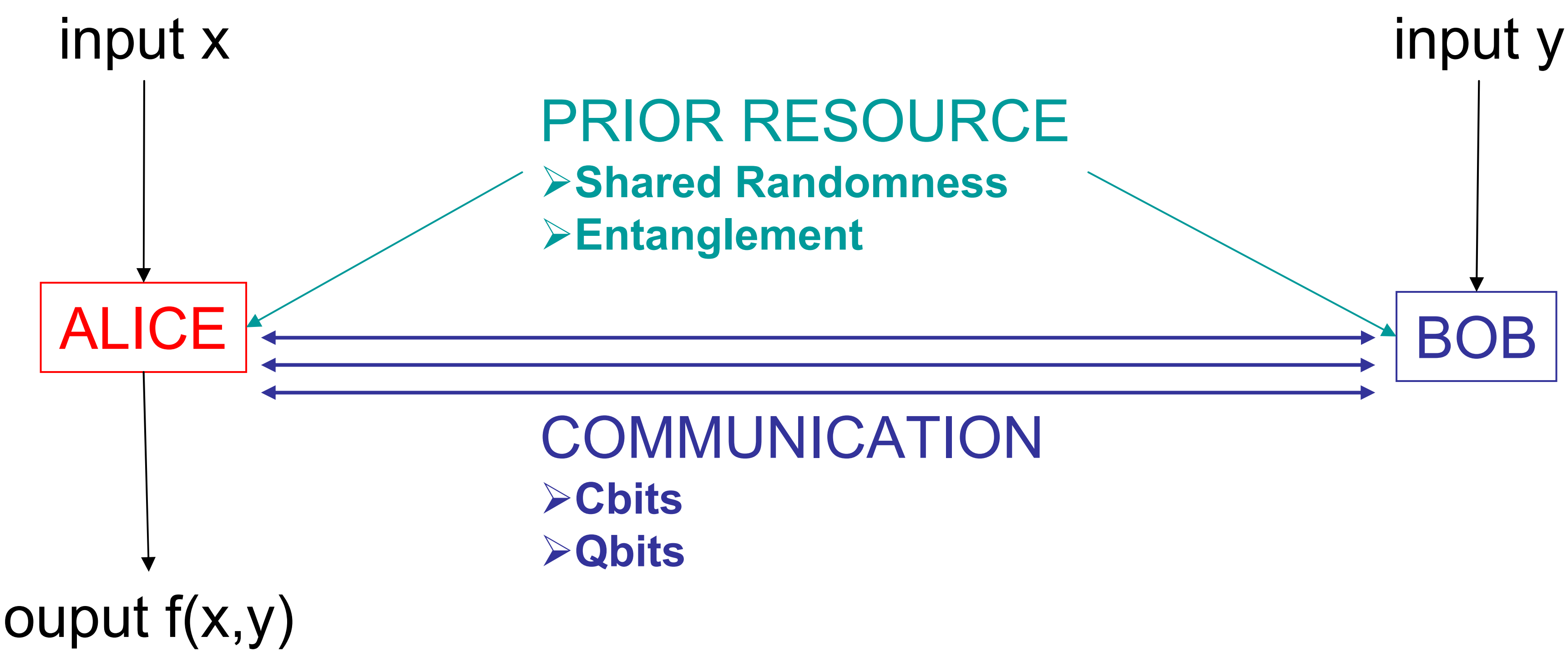
Nature **449**, 68-71 (2007)

Quantum Communication Complexity



TASK:Minimum Communication to provide the correct output

Quantum Communication Complexity



TASK:Minimum Communication to provide the correct output

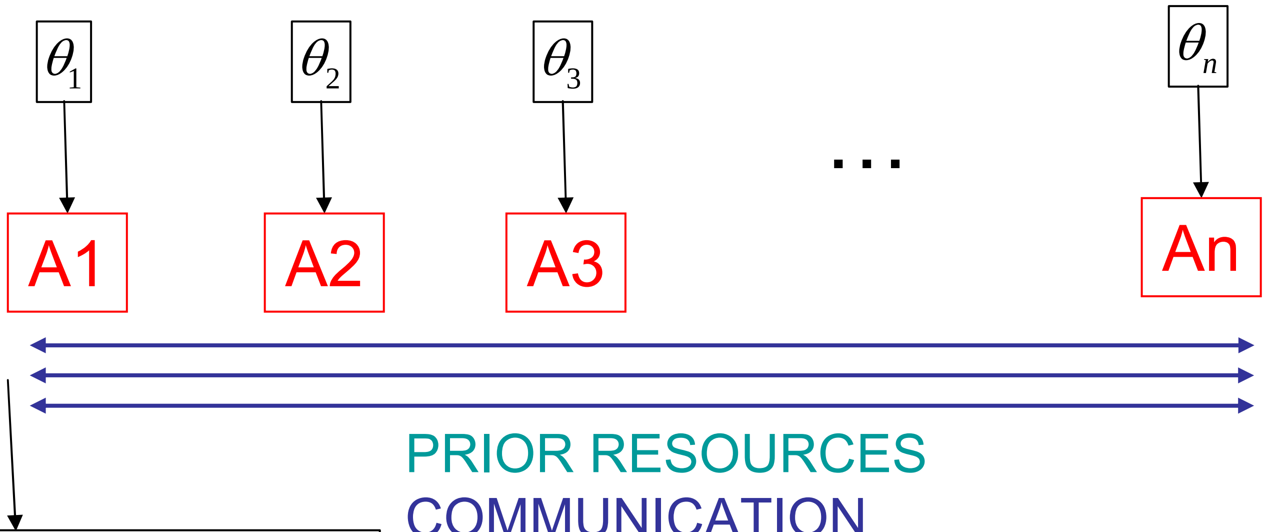
Example: Equality

Example: Equality

- No Error:
  - n cbits of communication required
- Small Error probability & shared randomness
  - Log(n) cbits of communication required
- Deutsch-Jozsa setting: either x=y or x differs from y in exactly n/2 positions
  - O(0.007n) cbits required
  - Log(n) qubits required
  - Log(n) ebits + Log(n) cbits

Example: Sum mod 2π

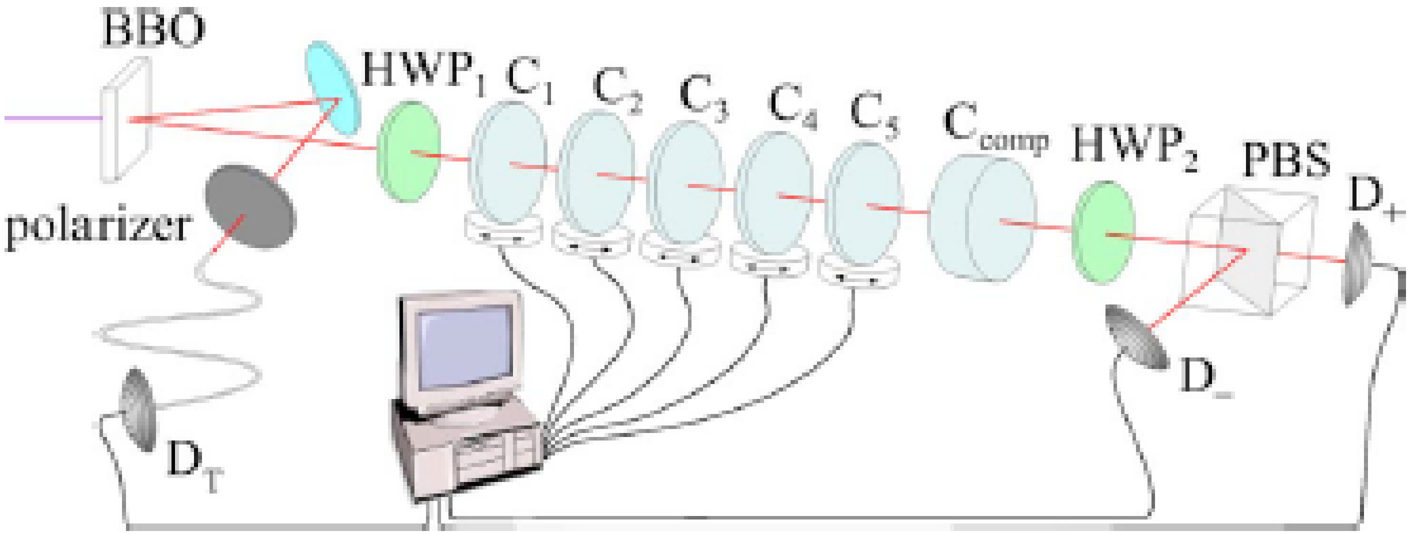
PROMISE $\sum_{i} \theta_i = 0 \text{ or } \pi \pmod{2\pi}$



Question: is $\sum_{i} \theta_i = 0 \text{ or } \pi \pmod{2\pi}$

- Bounded Error: requires O(n Log(n)) cbits
- n qubits
- 1GHZ state + n cbits

Experimental Realisation of Sum mod 2π



PRA **72**, 050305R 2005

Conclusion
The future of Quantum Communication

- Faster
  - Better detectors
- Further
  - Via satellite (?)
  - Repeaters
- Interfacing with stationary qubits
  - Quantum memories for light
  - Error Correction