The Quantum Information Revolution:

~~101~~ Uses for Schrödinger's ~~Cat~~

4 Kitten-embryo

Paul Kwiat

DTO MURI NSF QCCM

Wednesday, 4 December, 2002, 09:02 GMT

Woolly writing creates new poetry

North East writer Valerie Laws has been given a grant of £2,000 to use sheep to create random poems, which also utilize the deepest workings of the universe.

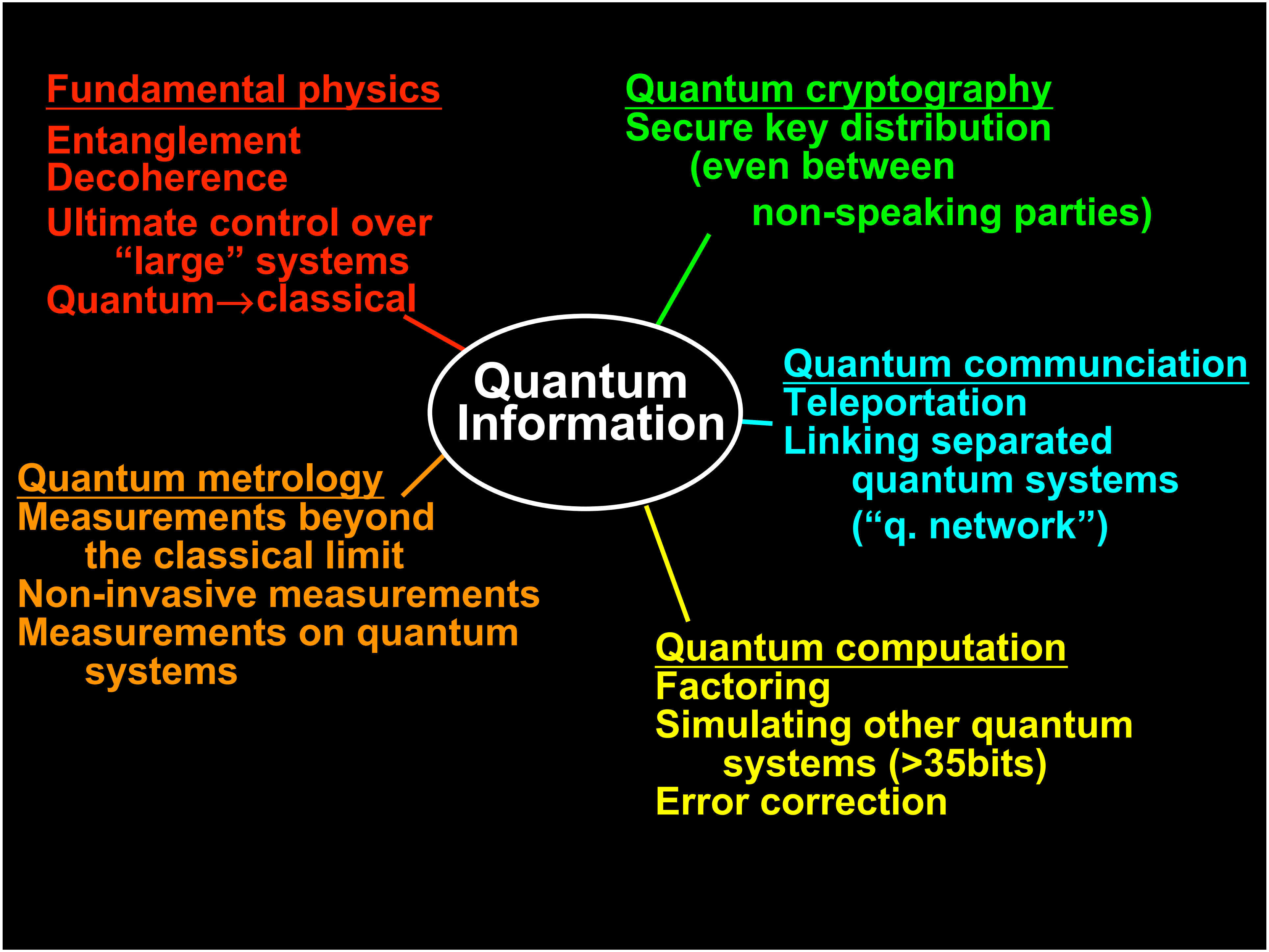
“Quantum mechanics is a branch of physics which a lot of people find hard to understand, as it seems to go against common sense. So *I decided to explore randomness and some of the principles of quantum mechanics, through poetry, using the medium of sheep.*”

PGK Group

Graduate Students: Joe Altepeter, Julio Barreirro, Onur Hosten, Evan Jeffrey, Nicholas Peters, Radhika Rangarajan, Aaron VanDevender, Kevin McCusker, Michael Wayne, Scott Jobling Associated Theory Post-Doc: Tzu-Cheih Wei
Undergraduates: Gleb Akselrod, Rachel Hillmer, Trent Graham, Kevin Uskali

Outline

-1. Quantum Information Overview
0. Entanglement 101
1. Two-crystal source, and Bell's inequalities
2. Quantum cryptography 101
3. Relativistic quantum cryptography
4. Hyper-entanglement
5. Quantum dense coding
6. ?Quantum cooking?


Fundamental physics
Entanglement
Decoherence
Ultimate control over "large" systems
Quantum→classical
Quantum cryptography
Secure key distribution (even between non-speaking parties)
Quantum Information
Quantum communciation
Teleportation
Linking separated quantum systems ("q. network")
Quantum metrology
Measurements beyond the classical limit
Non-invasive measurements
Measurements on quantum systems
Quantum computation
Factoring
Simulating other quantum systems (>35bits)
Error correction

Binary digit -- “bit”

0, 1

copyable

Quantum bit -- “qubit”

$|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}$

unclonable

Physical realization of qubits → any 2 level system

2-level atom: $|g\rangle, |e\rangle$ spin-1/2: $|\uparrow\rangle, |\downarrow\rangle$ polarization: $|H\rangle, |V\rangle$

All 2-level systems are created equal, but some are more equal than others!

Quantum communication → photons

Quantum storage → atomic vapors, spins

Scaleable circuits → ions, solid state systems

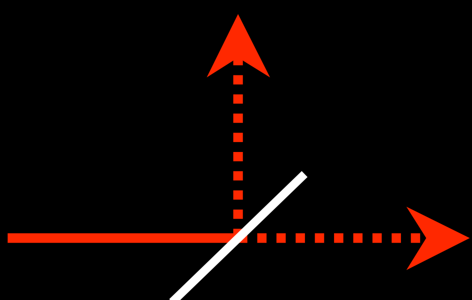
“Quantum” phenomena →

Superposition Interference Wave-particle duality Intrinsic randomness in measurement Entanglement

1905: Einstein proposed that light was really particles -- explained the photoelectric effect (for which he got the Nobel prize!)

Ironically, it was later realized the photoelectric effect does *not* prove that light is quantized (contrary to popular belief!) How <u>do</u> you prove it?

The Beamsplitter…



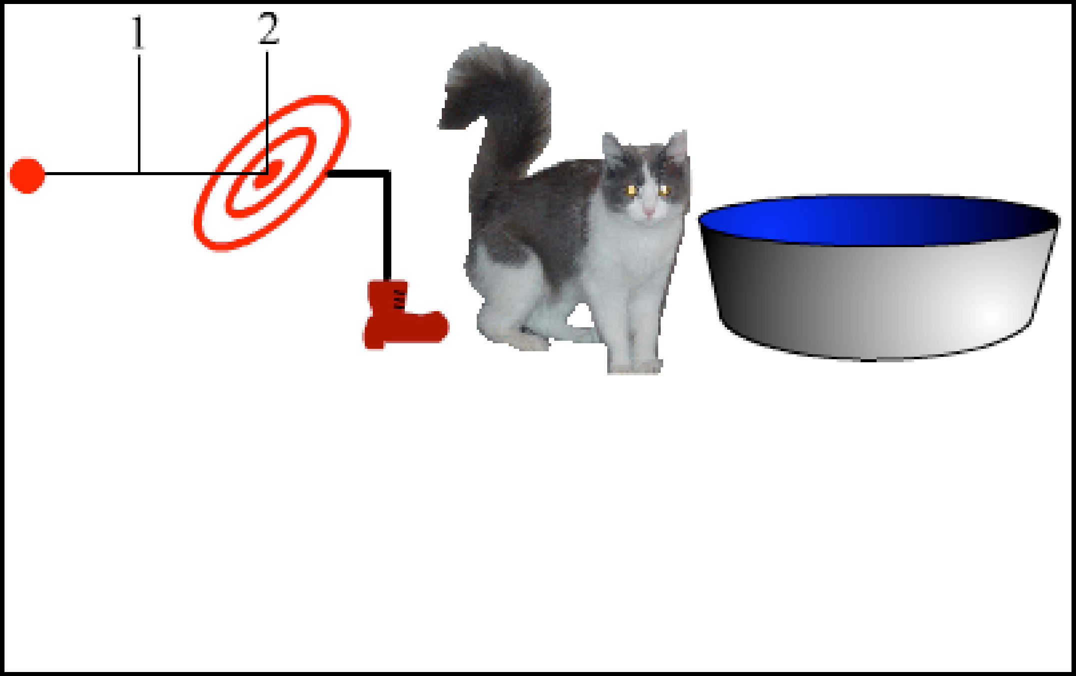
Photon only detected in one output.

Equally likely to be transmitted or reflected -- cannot tell which.

"God does not play dice with the universe."

Quantum Random Number Generator!

Creating a Schrödinger cat



After interacting with the photon, the cat-photon system becomes "entangled". The cat is not in a definite state (but not for long…)

We can't entangle anything so large as even a DNA molecule yet. But we *can* make entangled photons….

The *Two* Types of Quantum States

I. Factorizable states: Can be written as a *product*

Examples: $|H\rangle_1|H\rangle_2$, $|H\rangle_1 |H\rangle_2 + |H\rangle_1 |V\rangle_2 = |H\rangle_1 |45\rangle_2$

In a product state, each particle has its own definite properties.

II. Non-factorizable: can*not* be written as a product ⇒ Entanglement

Example ("Bell states"):

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

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

$|HV\rangle + |VH\rangle = |45,45\rangle - |-45,-45\rangle$

$|HV\rangle - |VH\rangle = |45,-45\rangle - |-45,45\rangle$

(Like the spin singlet: $|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle$)

In an entangled state, neither particle has definite properties alone.
⇒All the information is (nonlocally) stored in the *joint* properties.

Entanglement is
"***the*** **characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought"**

—E. Schrödinger

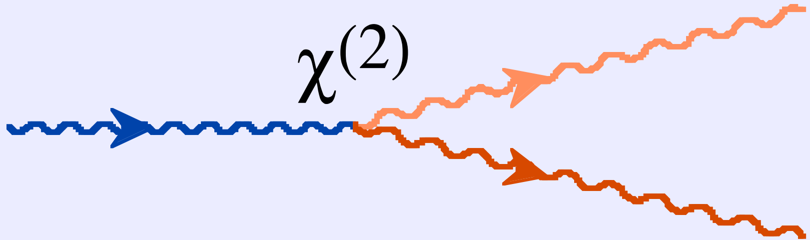
WHY are they important?

- Responsible for quantum measurements and decoherence
- Central to demonstrations of quantum nonlocality (e.g., Bell's inequalities, GHZ, Hardy, etc.)
- Quantum cryptography – separated particles' correlations allow sharing of secret random key
- Quantum dense coding – sending more than one bit of information in a single photon
- Quantum teleportation – transmit unknown quantum state via 2 classical bits + EPR pair
- Quantum computation – intermediate states are all complex entangled states

"It's fine to talk about these things, but here's a hammer and a wrench – can you *make* one?" –J. S. Bell

Spontaneous Parametric Downconversion

Burnham & Weinberg, PRL **25**, 84 (1970)



$\omega_p = \omega_s + \omega_i$ *

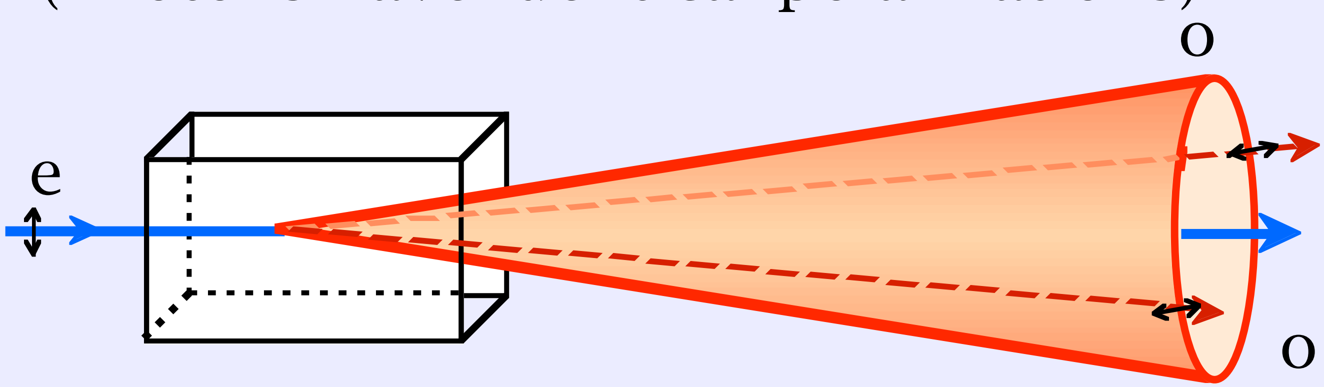
$\vec{\kappa}_p = \vec{\kappa}_s + \vec{\kappa}_i$ †

*Energy conservation → energy entanglement

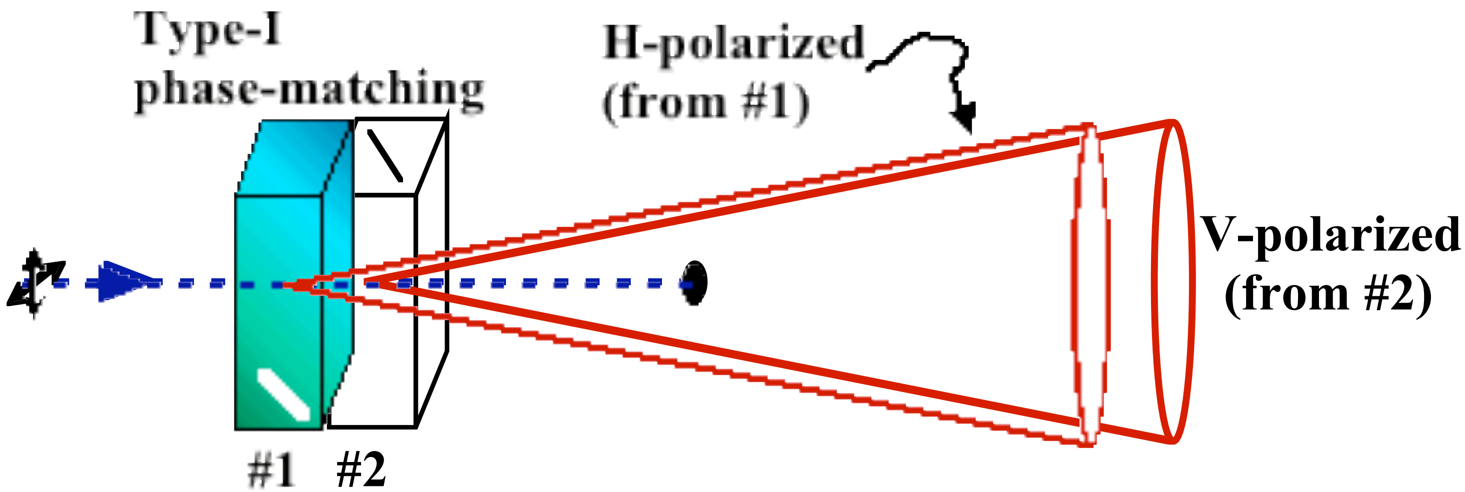
†Momentum conservation → momentum entanglement

Type-I Phase-matching

(Photons have identical polarizations)



Two-crystal Polarization-Entangled Source



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + e^{i\varphi}|V\rangle_1|V\rangle_2\right)$$

Maximally entangled state

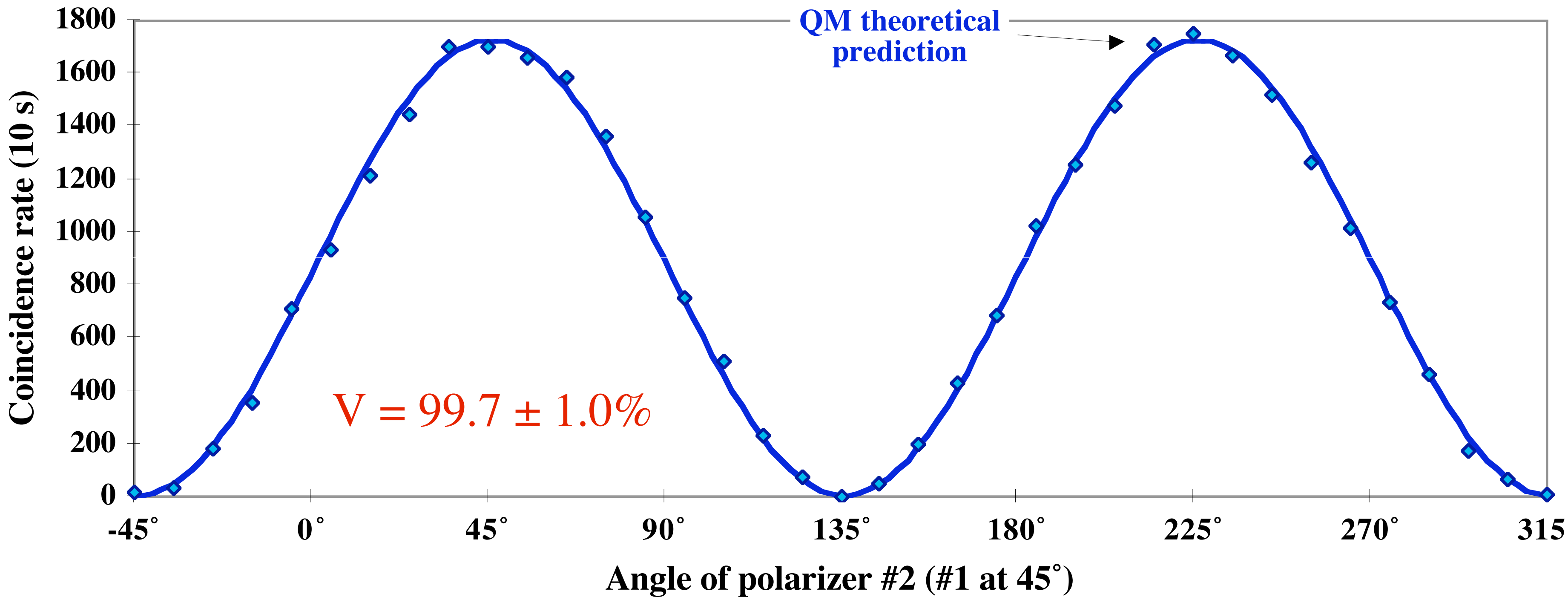
Tune pump polarization:

→ Nonmax. entangled states

Spatial-compensation: all pairs have same phase ϕ

Opt. Exp. **13**, 8951 (2005)

Proof of Quantum Correlations



$$|H\rangle|H\rangle + |V\rangle|V\rangle = |45\rangle|45\rangle + |-45\rangle|-45\rangle$$

- Near-perfect quantum behavior
- Ultrabright source

Test of Quantum Nonlocality

Einstein, Podolsky, Rosen (1935):
Correlations are due to some local element of reality ("local hidden variable" model)

Bell (1965): QM gives different statistical predictions than any local realistic model

Bell-inequality

$|S_{LHV}| \leq 2$

$|S| = 2.7260 \pm 0.0008$
216σ in 0.8 s

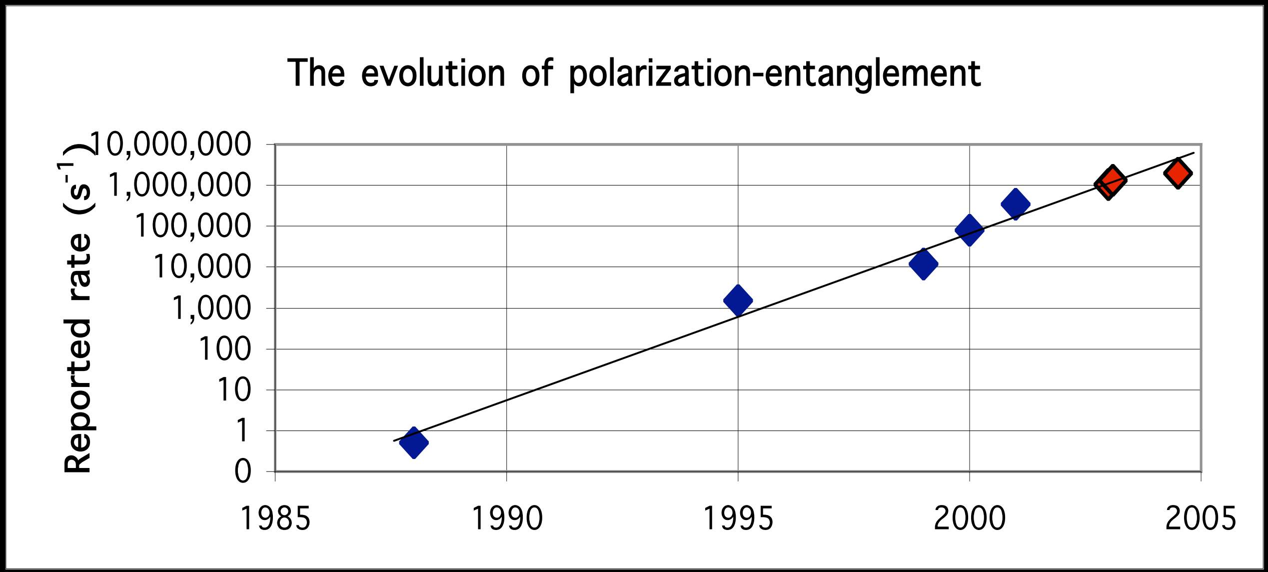
$|S| = 2.7392 \pm 0.00008$
2417σ in 2 min

Optimized Bell test:

$|S_{QM,\ max}| = 2\sqrt{2} = 2.828$

$|S_{expt}| = 2.826 \pm 0.005$ 165σ

Moore's law for entanglement

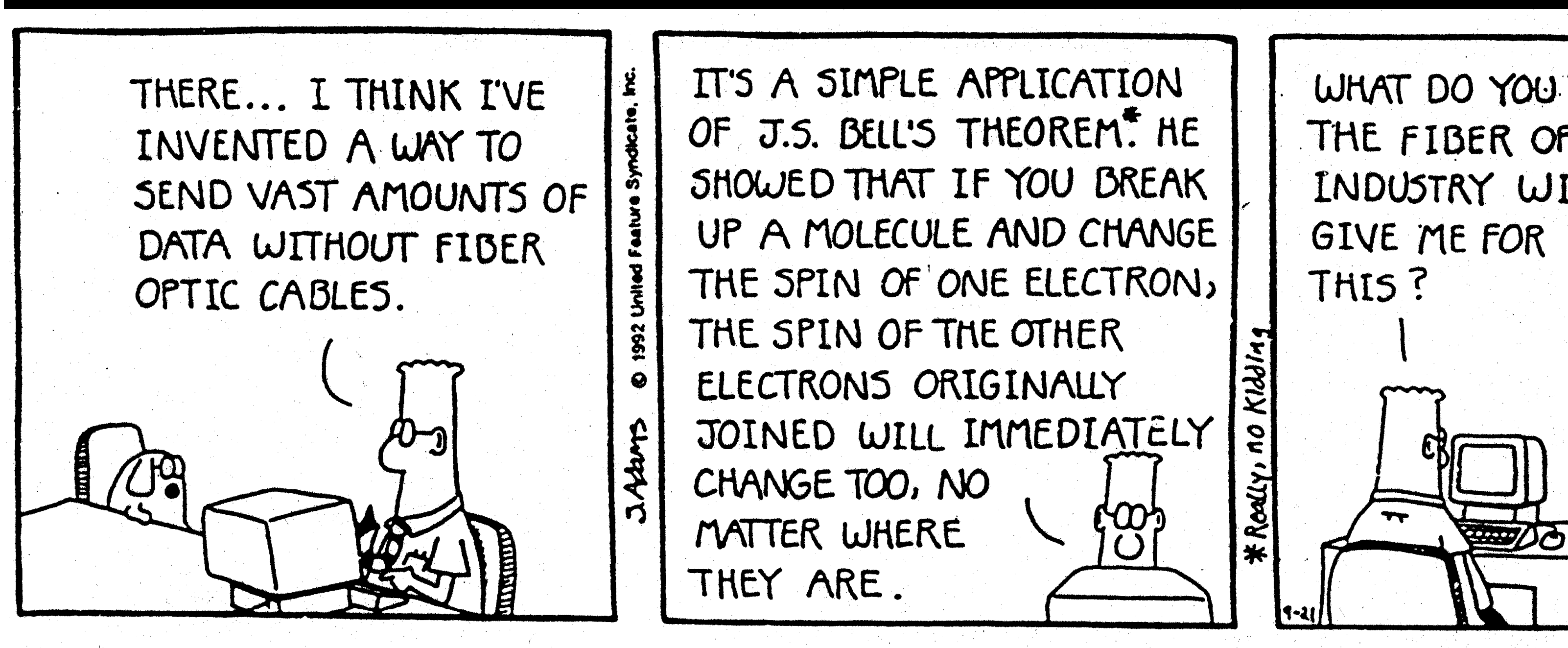


World record to date (July 21, 2004): 2,000,000 s^{-1} at Fidelity = 98%

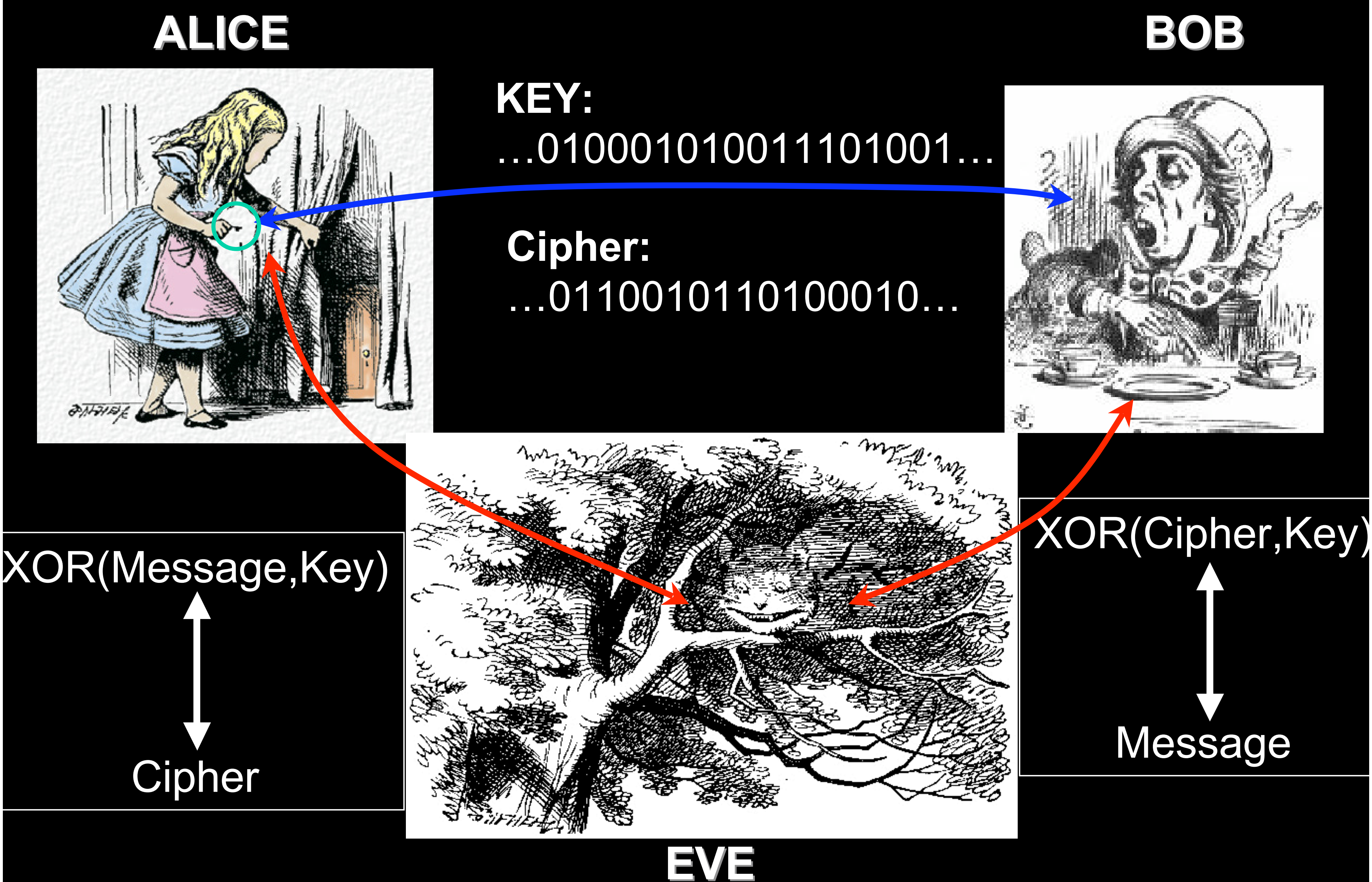
Currently limited by detector saturation.

What's it good for…

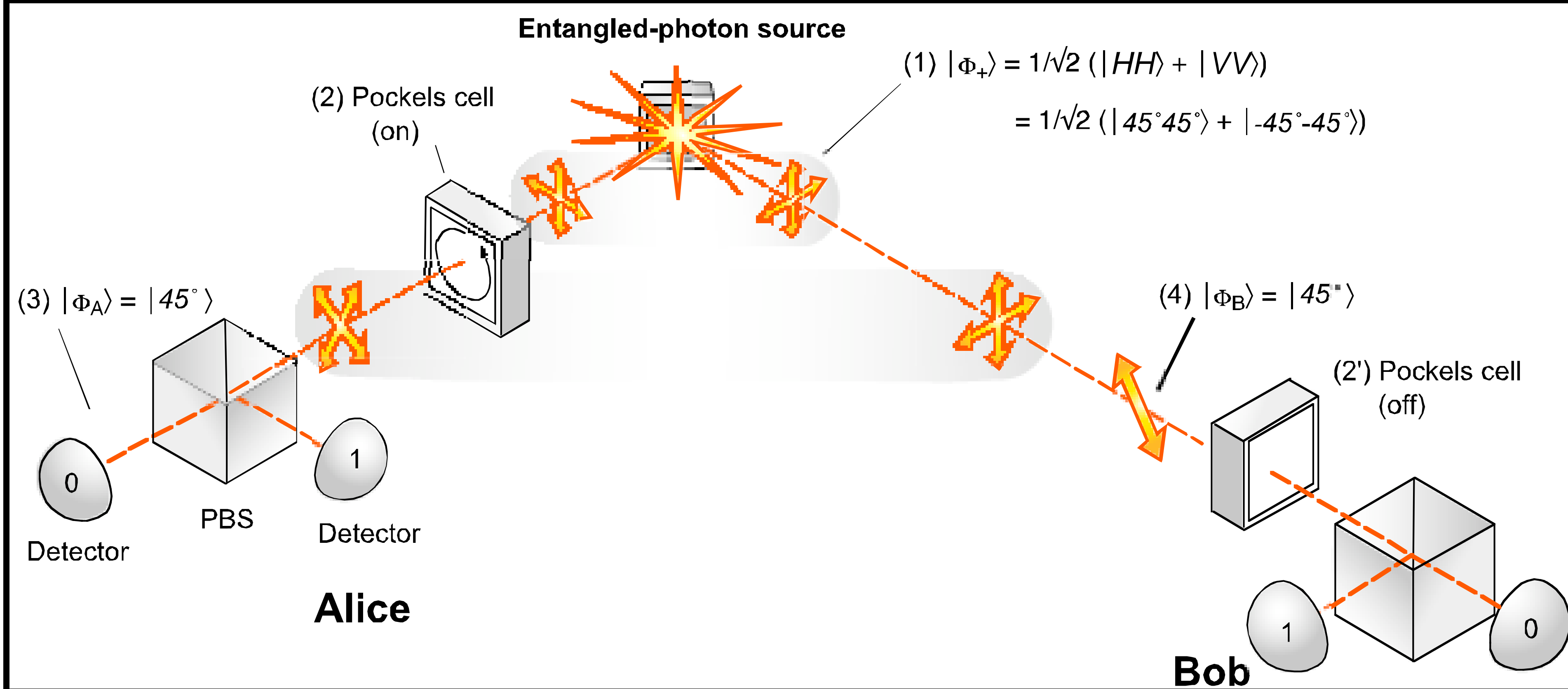
Quantum Cryptography



Quantum Cryptography

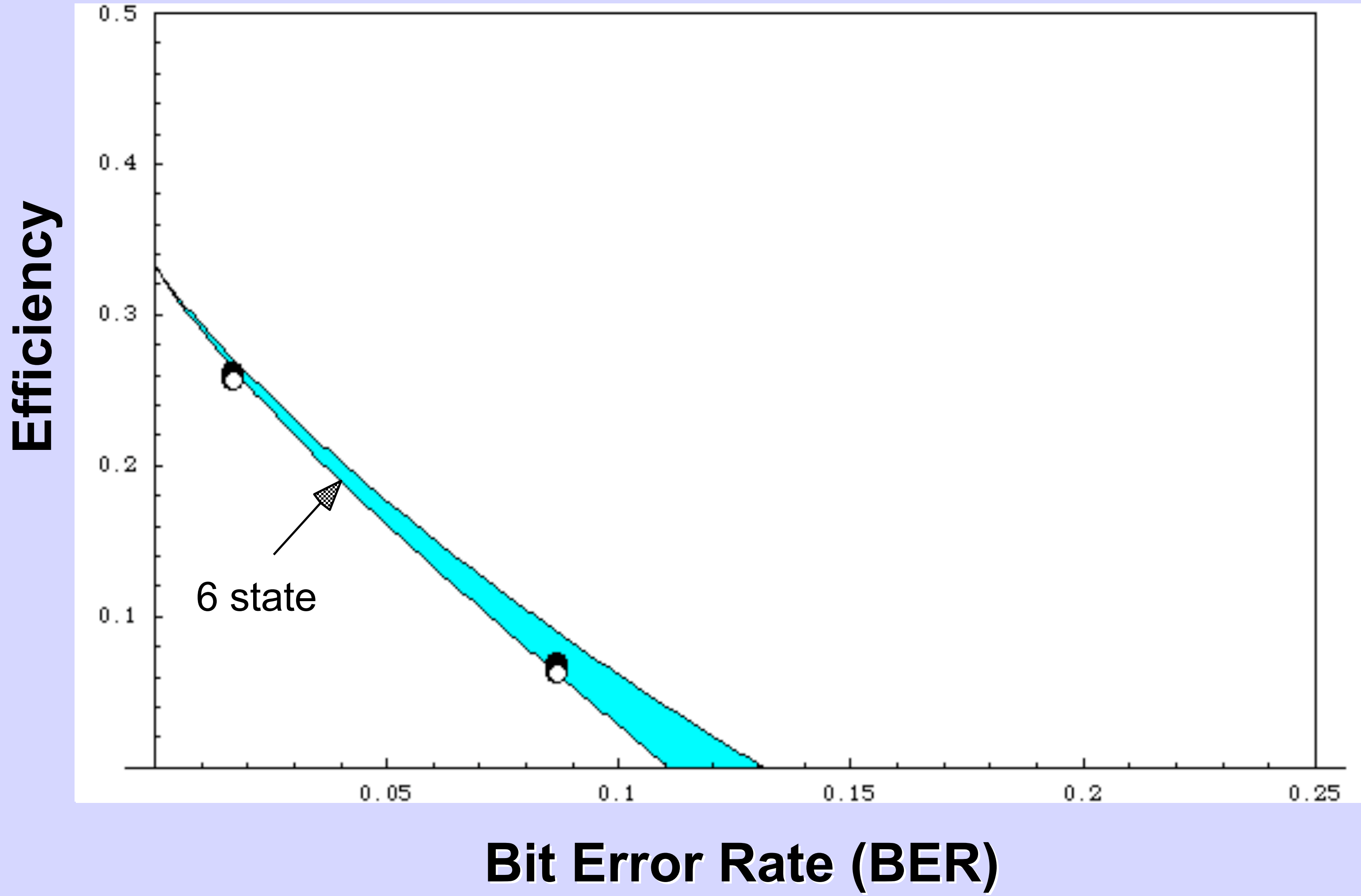


Entangled-Photon Quantum Cryptography

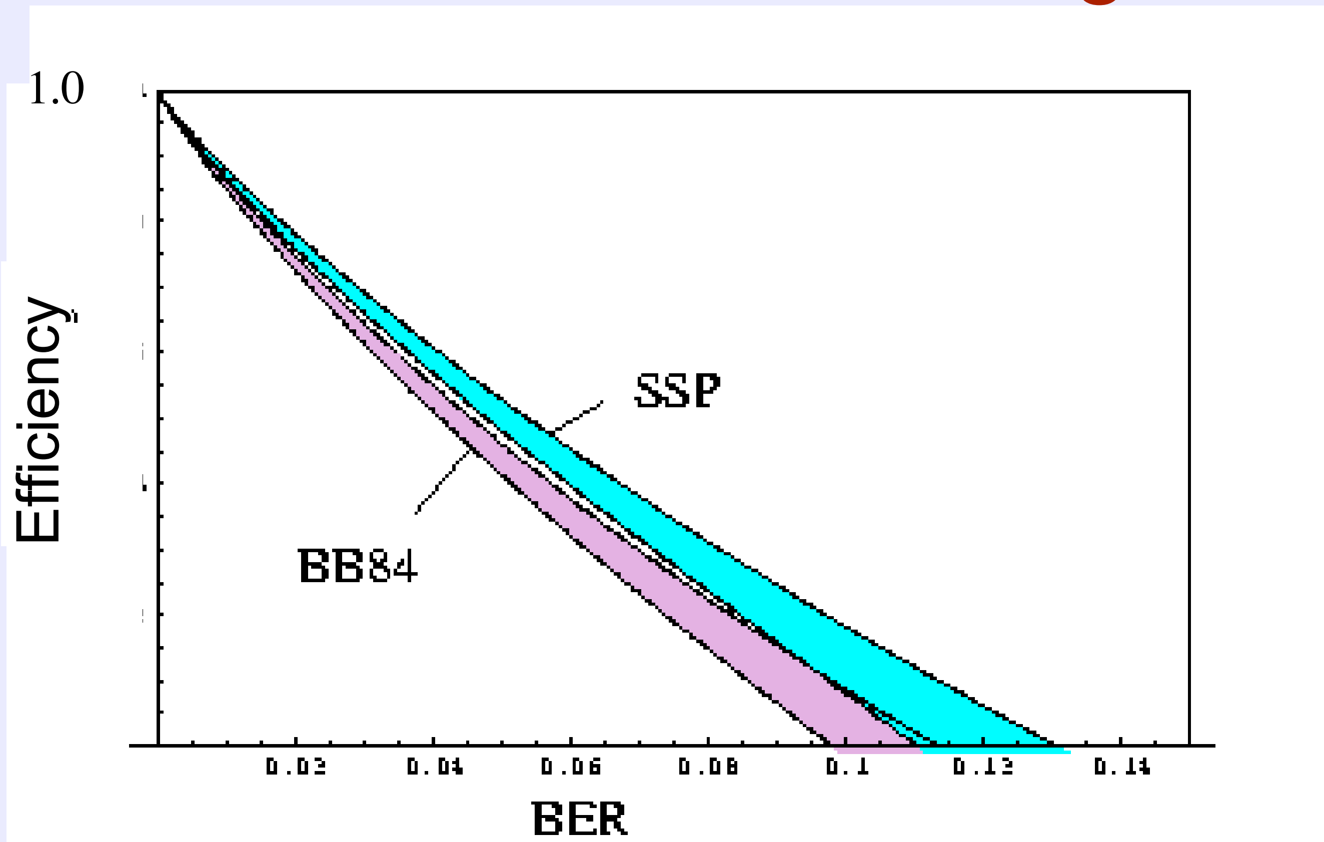


- Alice & Bob randomly measure polarization in the (HV) or the (45 -45) basis.
- Discuss via a "public channel" which bases they used, *but not the results*.
- Discard cases (50%) where they used different bases → uncorrelated results.
- Keep cases where they used the same basis → *perfectly correlated results!*
- Define H ≡ "0" ≡ 45, V ≡ "1" ≡ –45. **They now share a secret key.**

Bit yield, after Error Detection & Privacy Amplification



The Trouble with Sifting

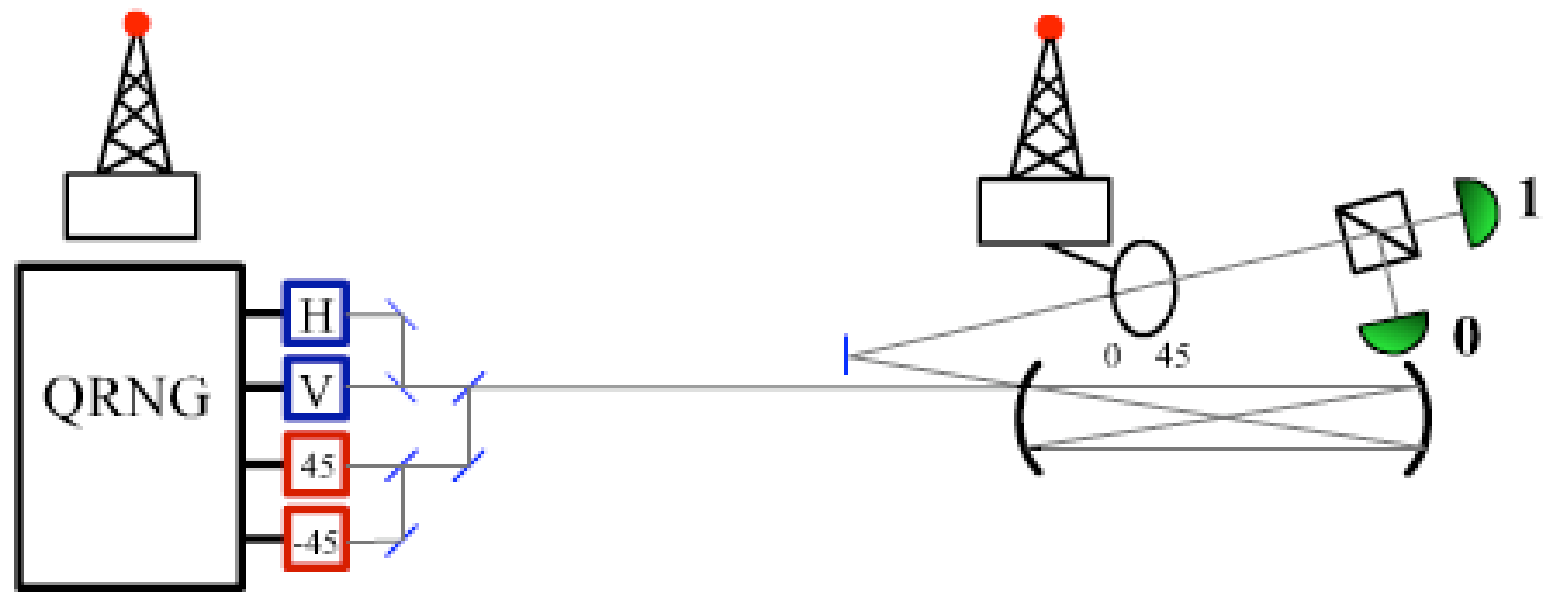


Eliminating the sifting ⇒ double efficiency of BB84
⇒ triple efficiency of SSP

- In principle, every photon contributes to key!
- SSP is always advantageous

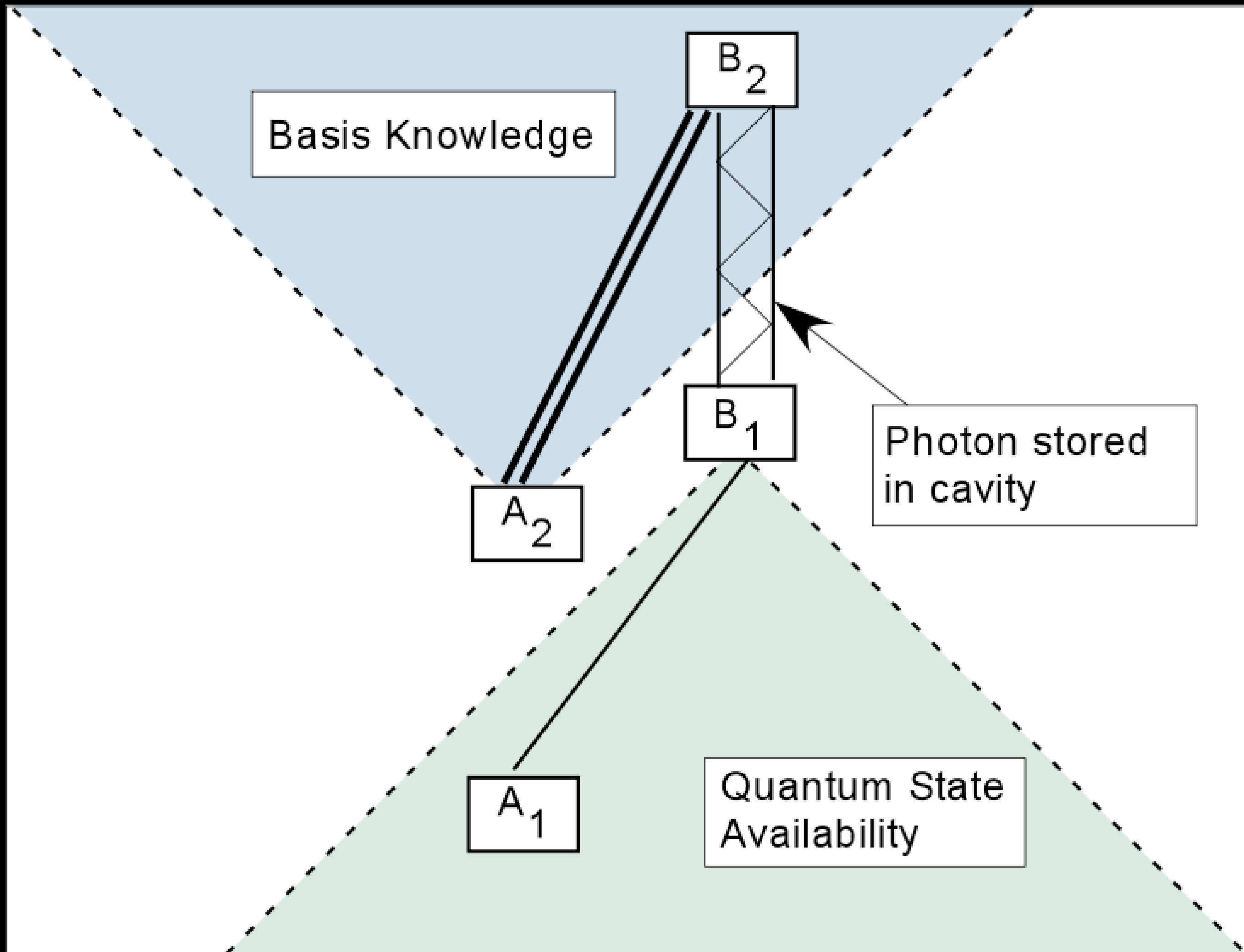
How can we eliminate sifting…

"Relativistic" Quantum Cryptography



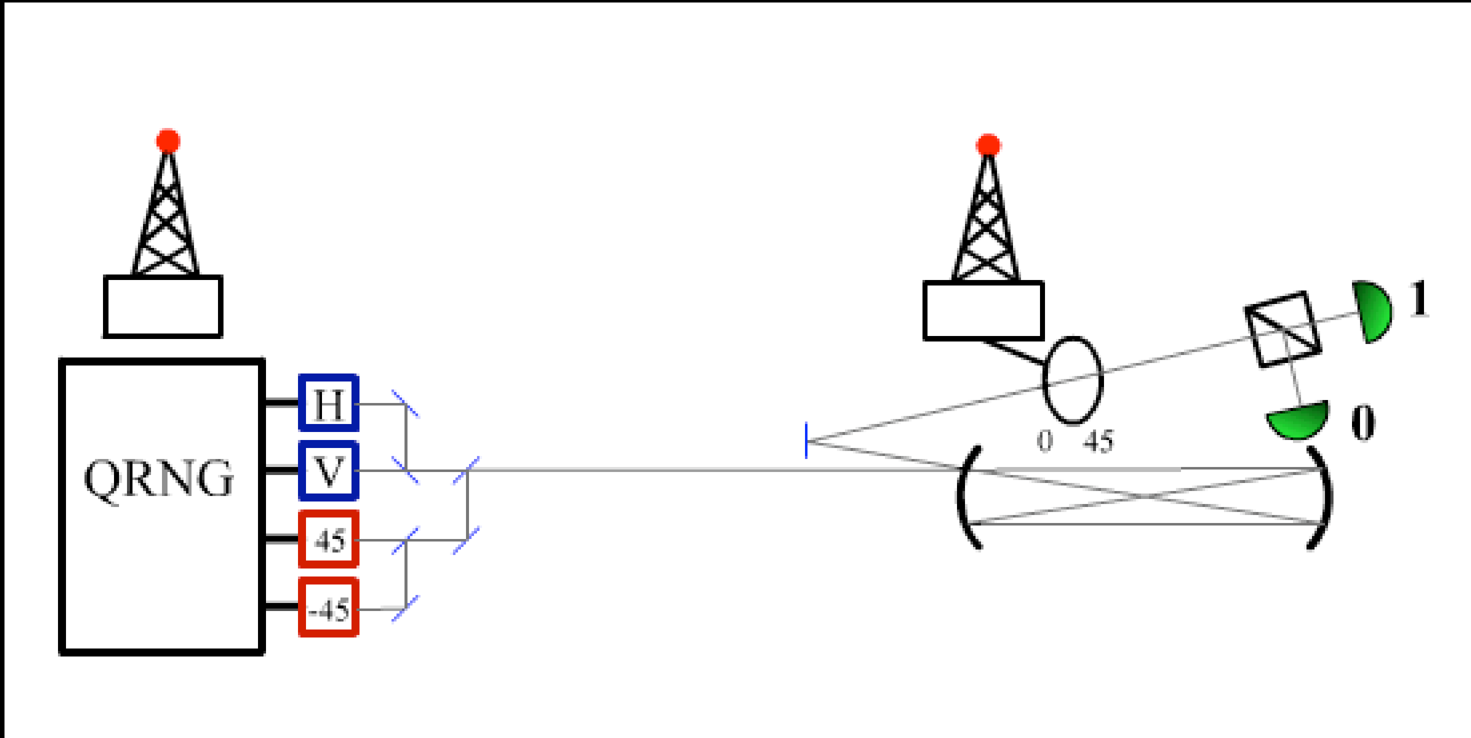
Bob stores each photon until Alice tells him which basis to use
→ net efficiency is increased to 100% (in principle)
→ same security as BB84 (Eve's ρ cannot depend on Bob)

QKD and Special Relativity



- These two light cones must not overlap
- A_2 may be before B_1 in some reference frames
- *Alice and Bob must know their space-time coordinates*

“Relativistic” Quantum Cryptography



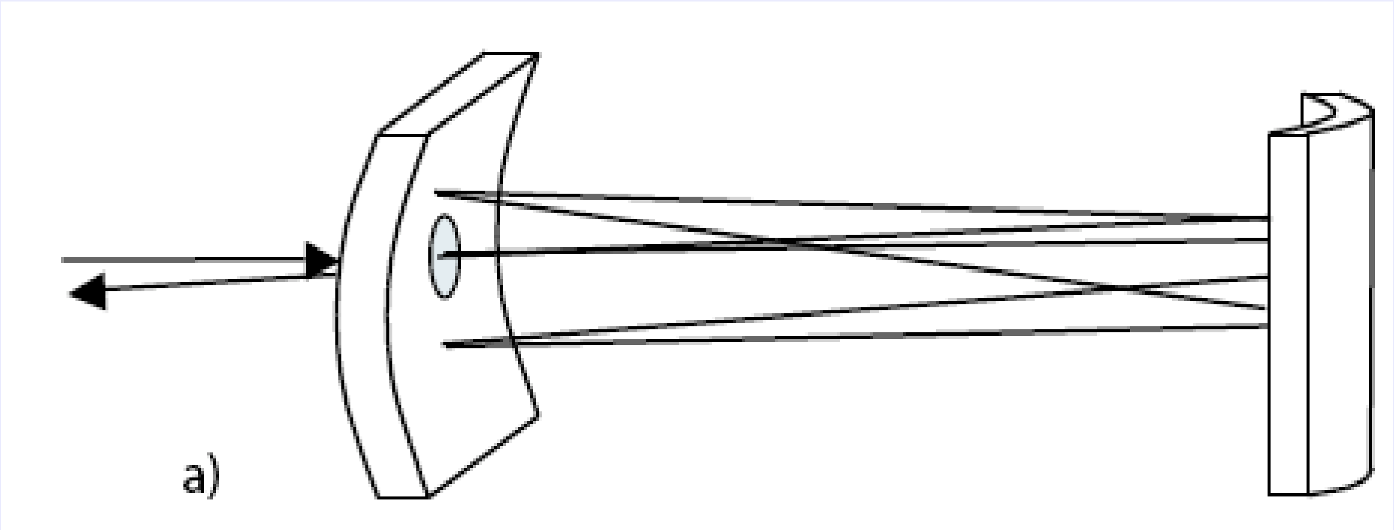
Special components

→ fast classical modulation system

→ **quantum memory**

Quantum Memory:low-loss optical delay line

Applications to quantum cryptography, quantum "repeaters", scalable quantum logic, novel quantum communication protocols



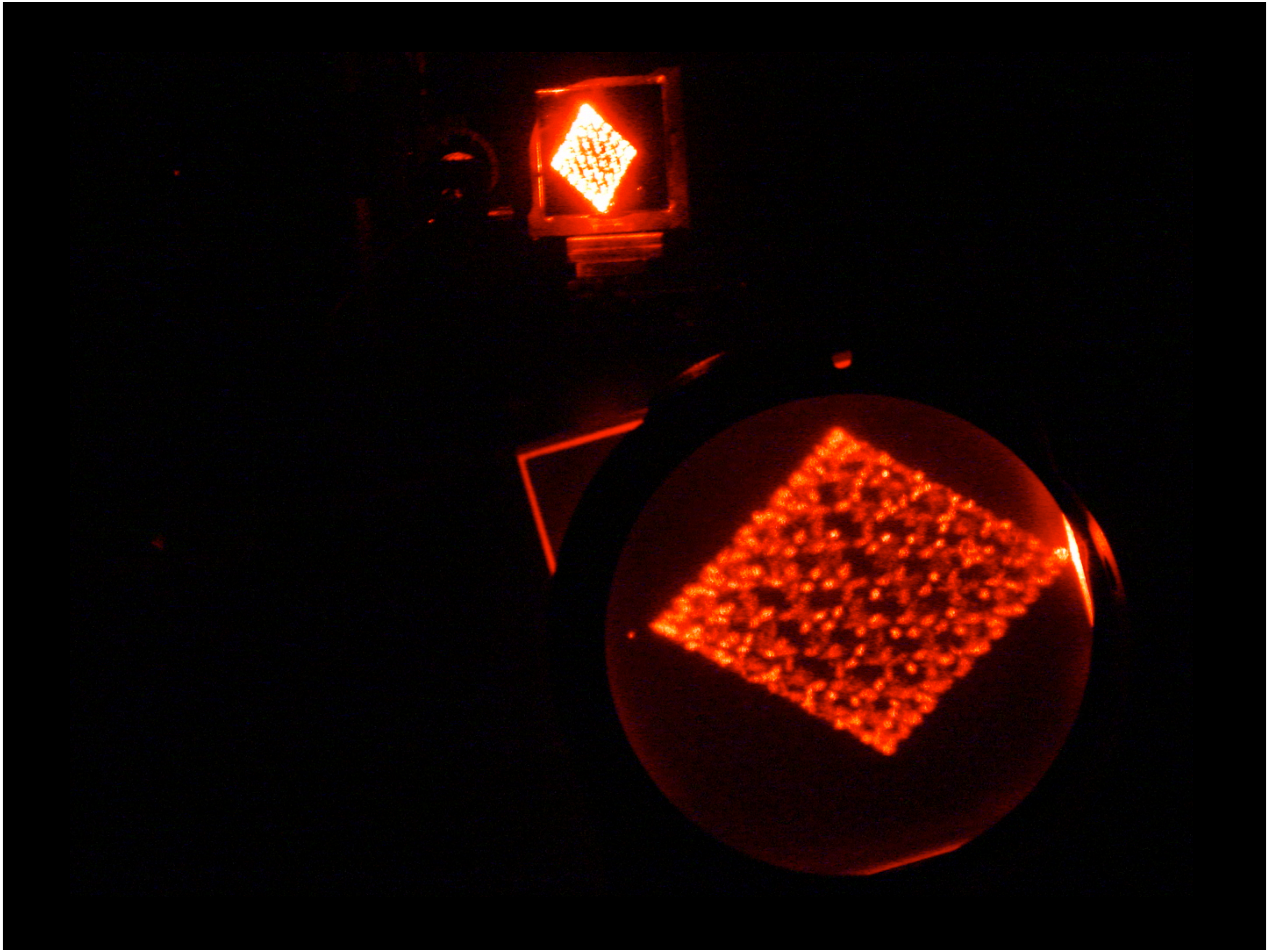
So far: 0.5 μs to 7.8 μs delay*;

T ~ 90-9% (→ R_{mirror}~ 99.83%)

Present experiment: 180 ns delay, T = 85%

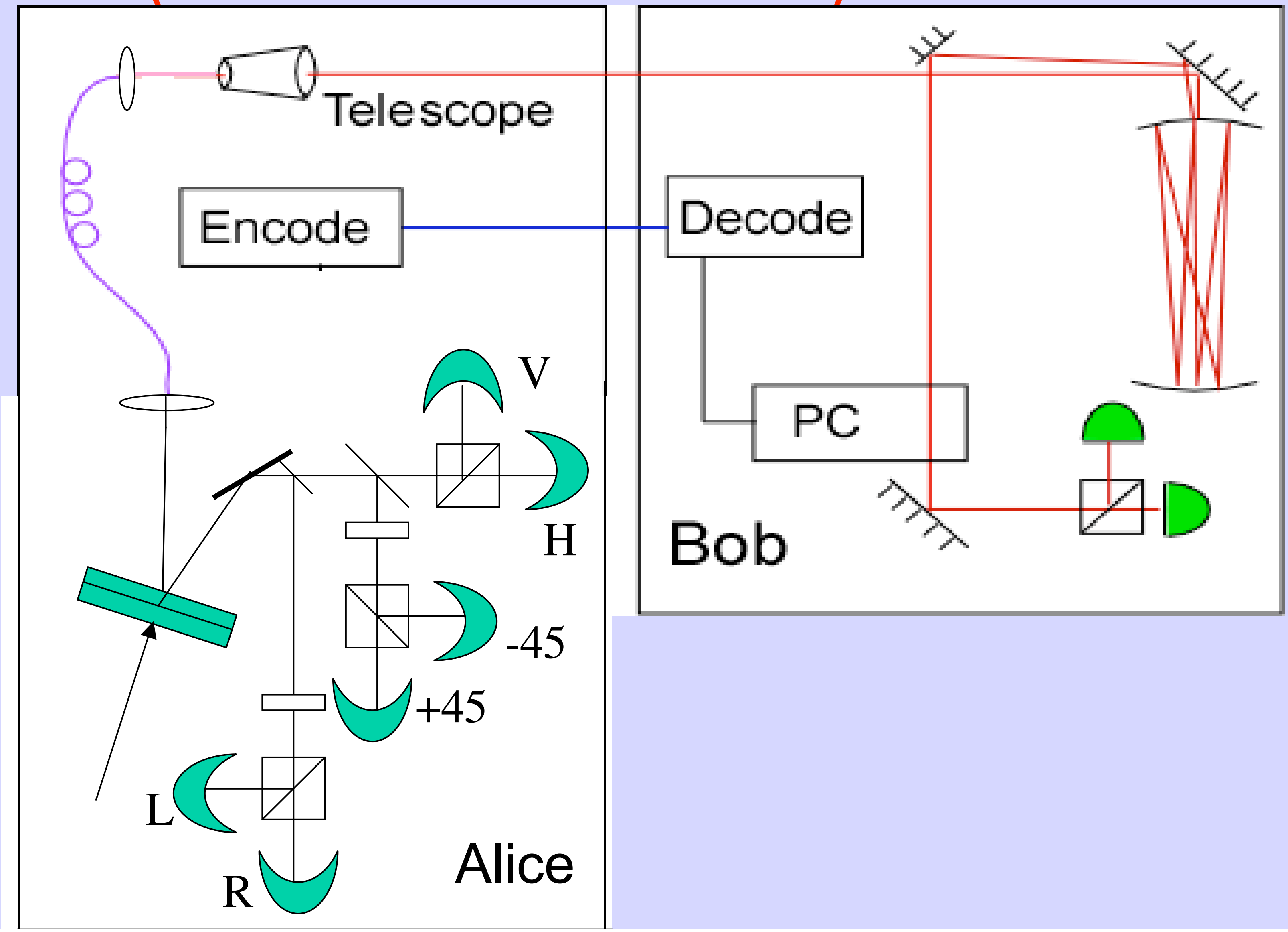
Possible: R_{mirror} = 99.99% → T = 98.5%; up to 10μs w. T >90%

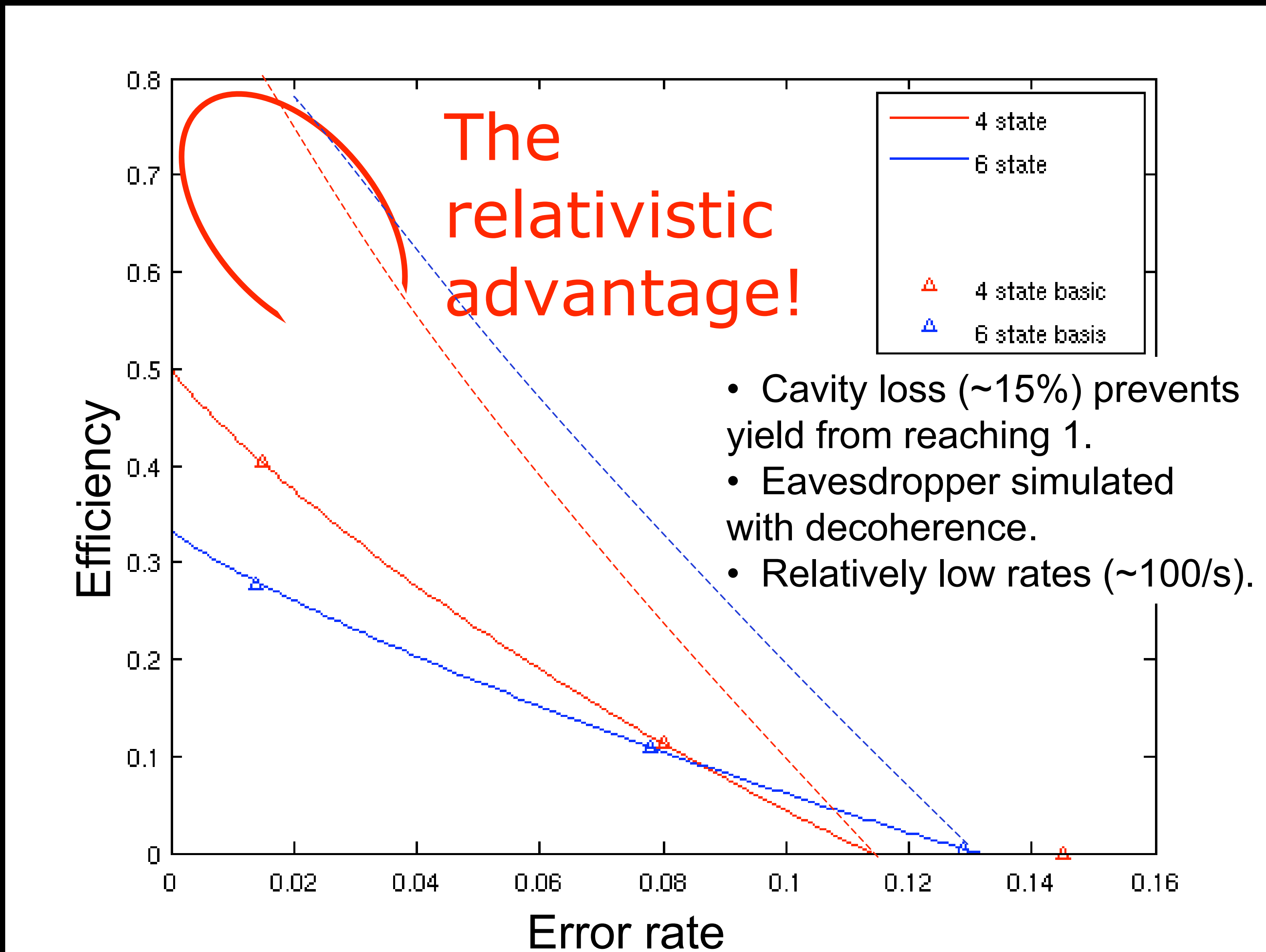
*Adjustment is performed by altering the separation and twist angle



Entangled-photon Relativistic Q. Cryptography

Non-degenerate polarization-entangled state (351 nm → 670 nm + 737 nm)





The relativistic advantage!
4 state
6 state
4 state basic
6 state basis
• Cavity loss (~15%) prevents yield from reaching 1.
• Eavesdropper simulated with decoherence.
• Relatively low rates (~100/s).
Efficiency
Error rate
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16

Photon Entanglements

- Polarization (spin)

  (Ou & Mandel, Shih & Alley, PGK et al., etc.)

- Linear momentum

  (Rarity & Tapster)

- Orbital angular momentum

  (Zeilinger et al.)

- Energy-Time

  (Franson et al., Howell et al.)

- Time-Bin

  (Gisin et al., Inoue et al.)

Hyper-Entanglement

PGK, JMO **44**, 2173 (1997)

- Photons simultaneously entangled in multiple DOFs:

$$\underbrace{(|H,H\rangle + |V,V\rangle)}_{polarization} \otimes \underbrace{(|rl\rangle + \alpha|gg\rangle + |lr\rangle)}_{spatial\ modes} \otimes \underbrace{\int_0^{E_p} dE A(E)|E\rangle_s|E_p - E\rangle_i}_{energy}$$

- Enlarged Hilbert space: $2 \otimes 2 \otimes m \otimes m \otimes n \otimes n$

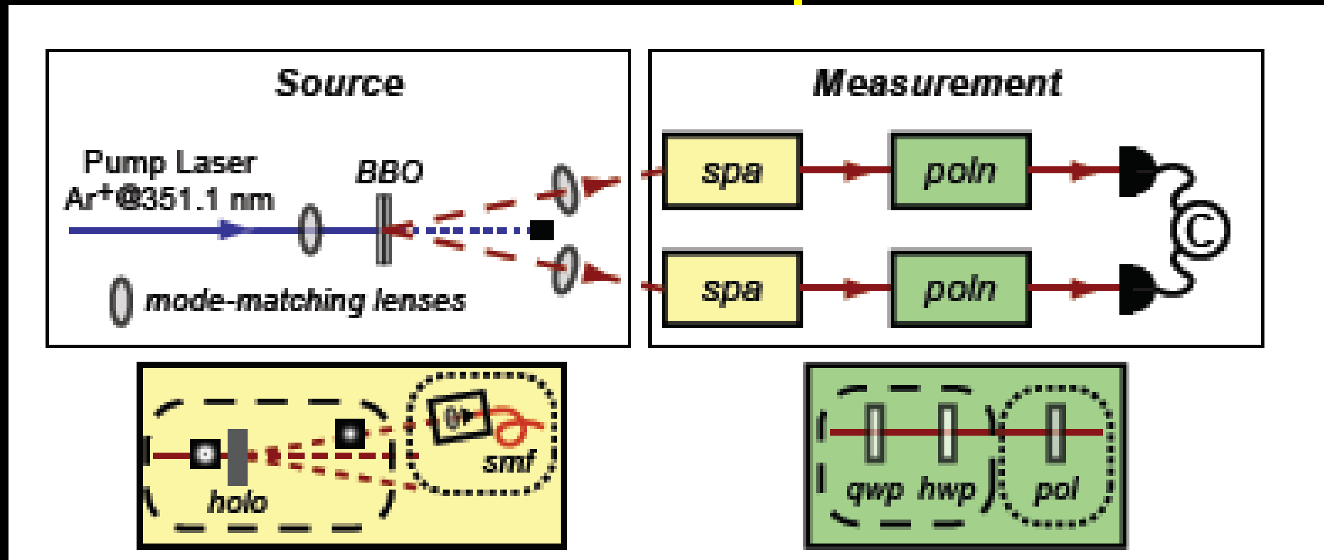
- Easy to perform quantum logic *between* DOFs

- New capabilities in quantum info. processing
  - remote preparation of entangled states
  - full Bell-state analysis
  - "super-duper" dense coding
  - quantum communication with higher alphabets
  - ???

Physics Illinois

THE UNIVERSITY OF QUEENSLAND

Hyper-Entanglement: Polarization and spatial mode

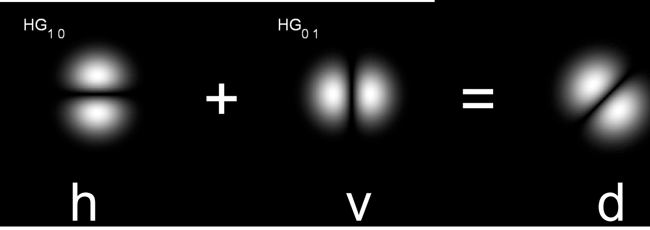


Hilbert space: $\{H, V\}^{\otimes 2} \otimes \{h, v\}^{\otimes 2}$ $\qquad 2 \otimes 2 \otimes 2 \otimes 2$

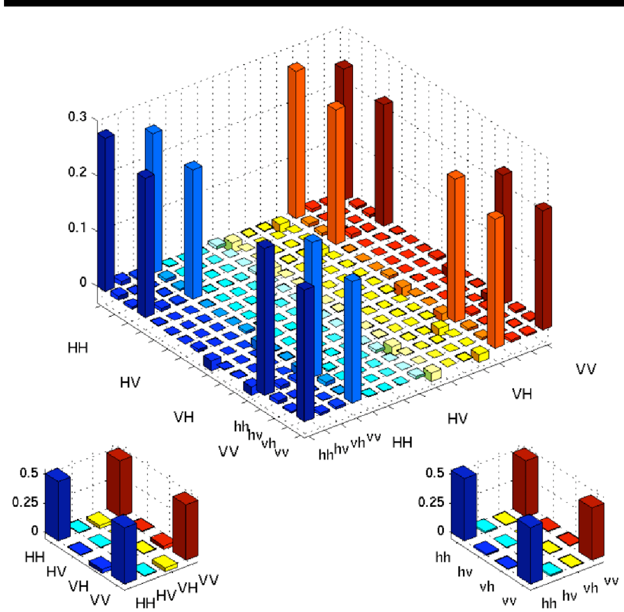
Bell states:

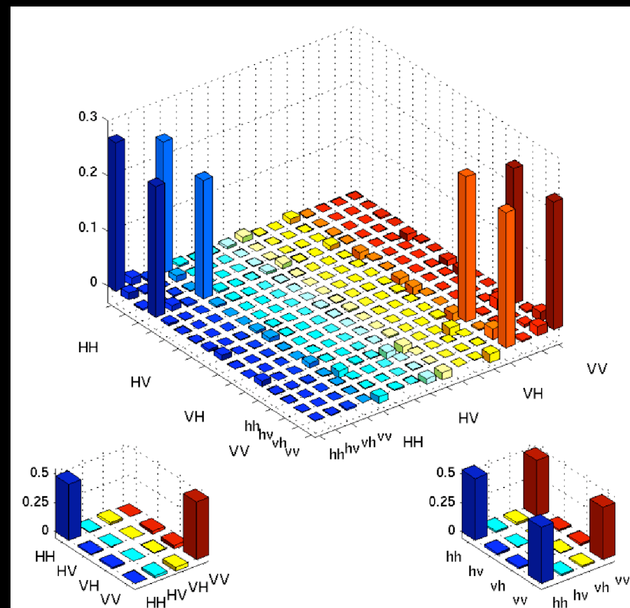
$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle) \qquad \phi^{\pm} = \frac{1}{\sqrt{2}}(|hh\rangle \pm |vv\rangle)$$

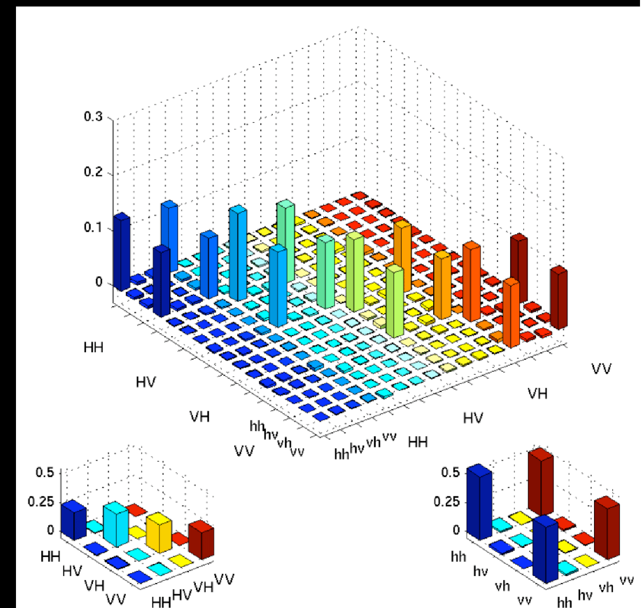
$$\Psi^{\pm} = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle) \qquad \psi^{\pm} = \frac{1}{\sqrt{2}}(|hv\rangle \pm |vh\rangle)$$



Controllable Hyper-entanglement







$$|\Phi^+\rangle \otimes |\phi^+\rangle$$

Maximally hyper-entangled state
F = 97%; T's > 94%

$$\{HH, VV\} \otimes |\phi^+\rangle\langle\phi^+|$$

Half-mixed/Maximally entangled state (classical & quantum)

$$\frac{1}{4} I \otimes |\phi^+\rangle\langle\phi^+|$$

Maximally mixed/ Maximally entangled state

J. T. Barreiro et al., PRL **95**, 260501 (2005)

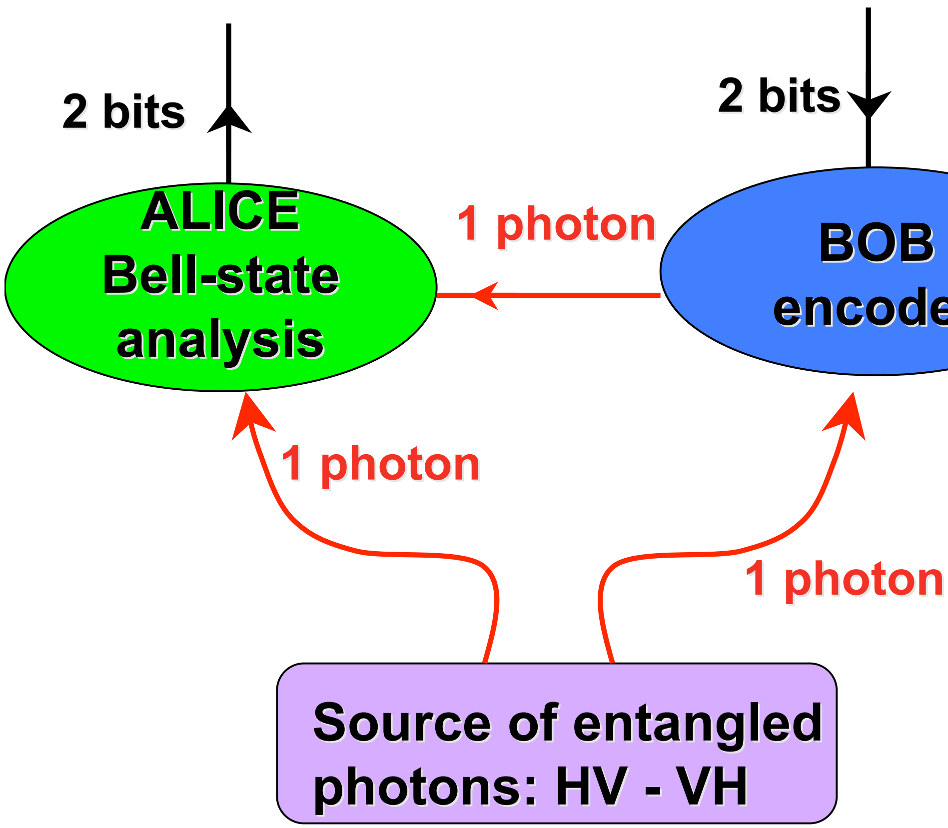
Physical Review Letters

VOLUME 69 16 NOVEMBER 1992 NUMBER 20

Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Stephen J. Wiesner



Bob's Transformation	Resulting State
I	HV - VH
H ↔ V	HH - VV
V → -V	HV + VH
H ↔ V, V→ -V	HH - VV

1 photon carries 2 bits of info:

Channel cap. = $\log_2 4$ = 2 bits/photon

Super-dense coding

Bob encodes 1 of 4 messages (2 bits) on a single photon.

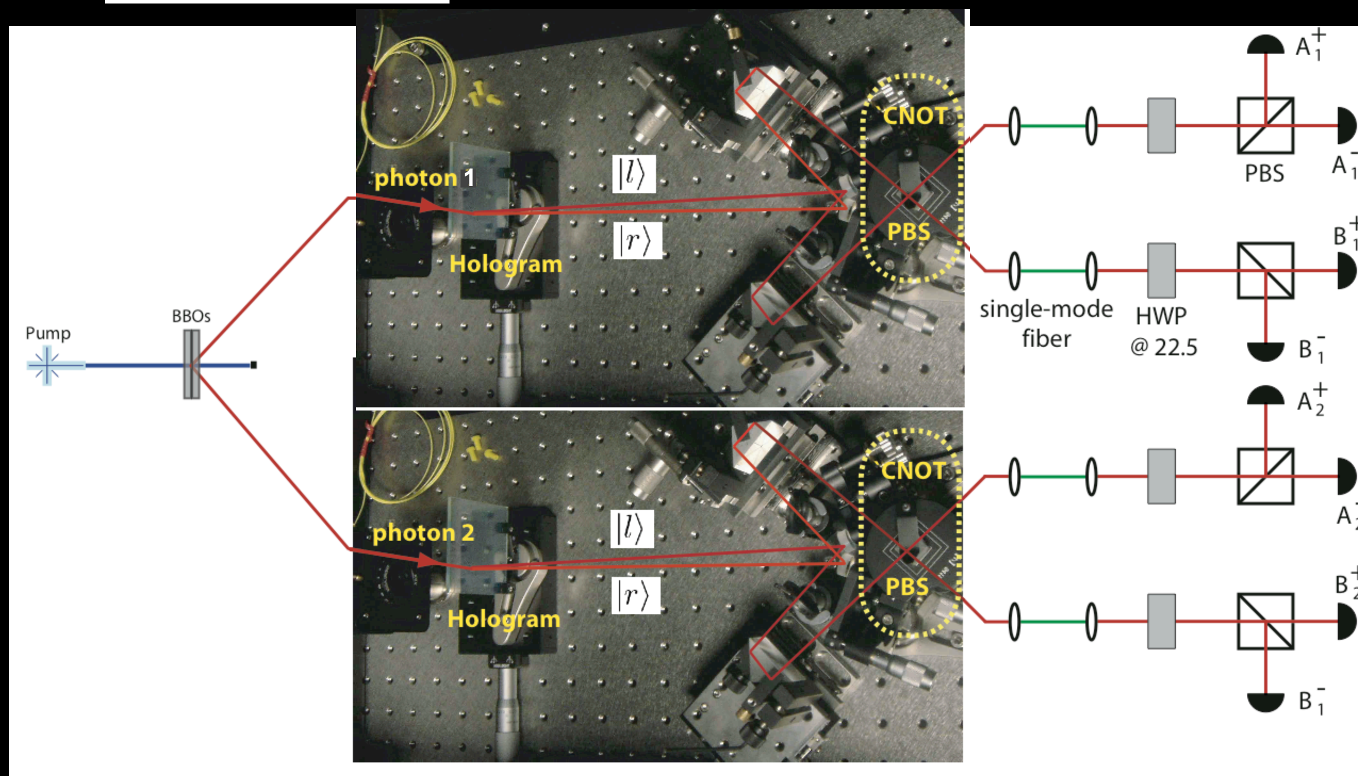
*Alice can decode **if** she can distinguish all the Bell states in a single measurement -- **"Bell state analysis"***

- Impossible with Linear Optics -- only 3 of 4 Bell states discriminated: Dense-coding capacity = $\log_2(3) = 1.58$
- Probabilistic: 4 out of 4, but <u>at most</u> 50% efficient
- **Hyper-entanglement enhanced** Bell-State analysis: 100% efficient, 4 out of 4

Kwiat & Weinfurter, PRA **58**, R2623 (1998)

Bell-state analysis

Polarization Bell states: $$\begin{pmatrix} \Phi^{\pm} \\ \Psi^{\pm} \end{pmatrix} \otimes \phi^{+}$$ Spatial mode Ancillary DOF



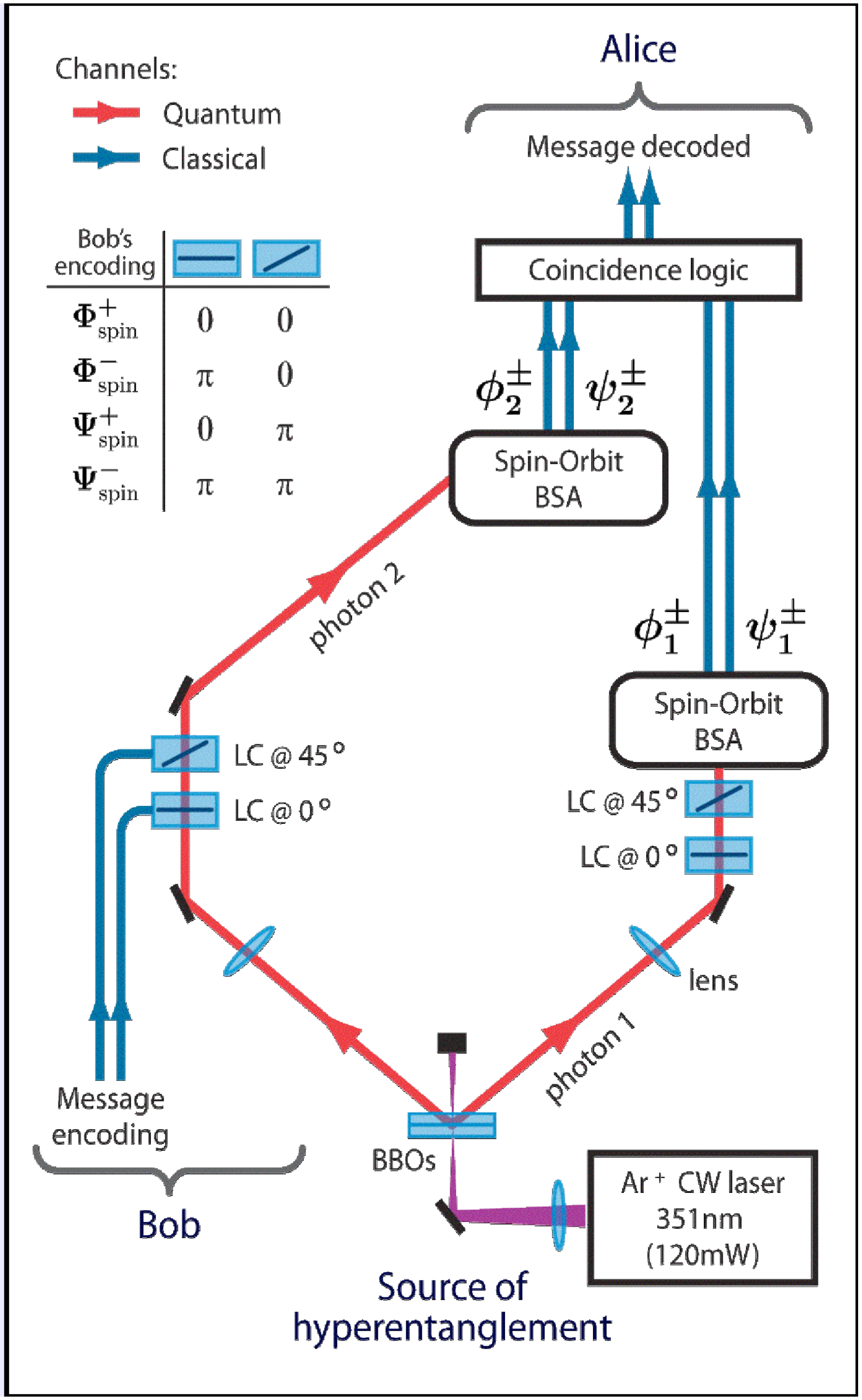
State	Detector signature			
$\lvert\Phi^{\pm}\rangle$	$A_1^+ A_2^{\pm}$	$B_1^+ B_2^{\pm}$	$A_1^- A_2^{\mp}$	$B_1^- B_2^{\mp}$
$\lvert\Psi^{\pm}\rangle$	$A_1^+ B_2^{\pm}$	$B_1^+ A_2^{\pm}$	$A_1^- B_2^{\mp}$	$B_1^- A_2^{\mp}$

Weinfurter et al., PRL 96, 190501 (2006)

Walborn et al., PRA 68, 042313 (2003)

Hyper-entanglement-assisted Superdense coding

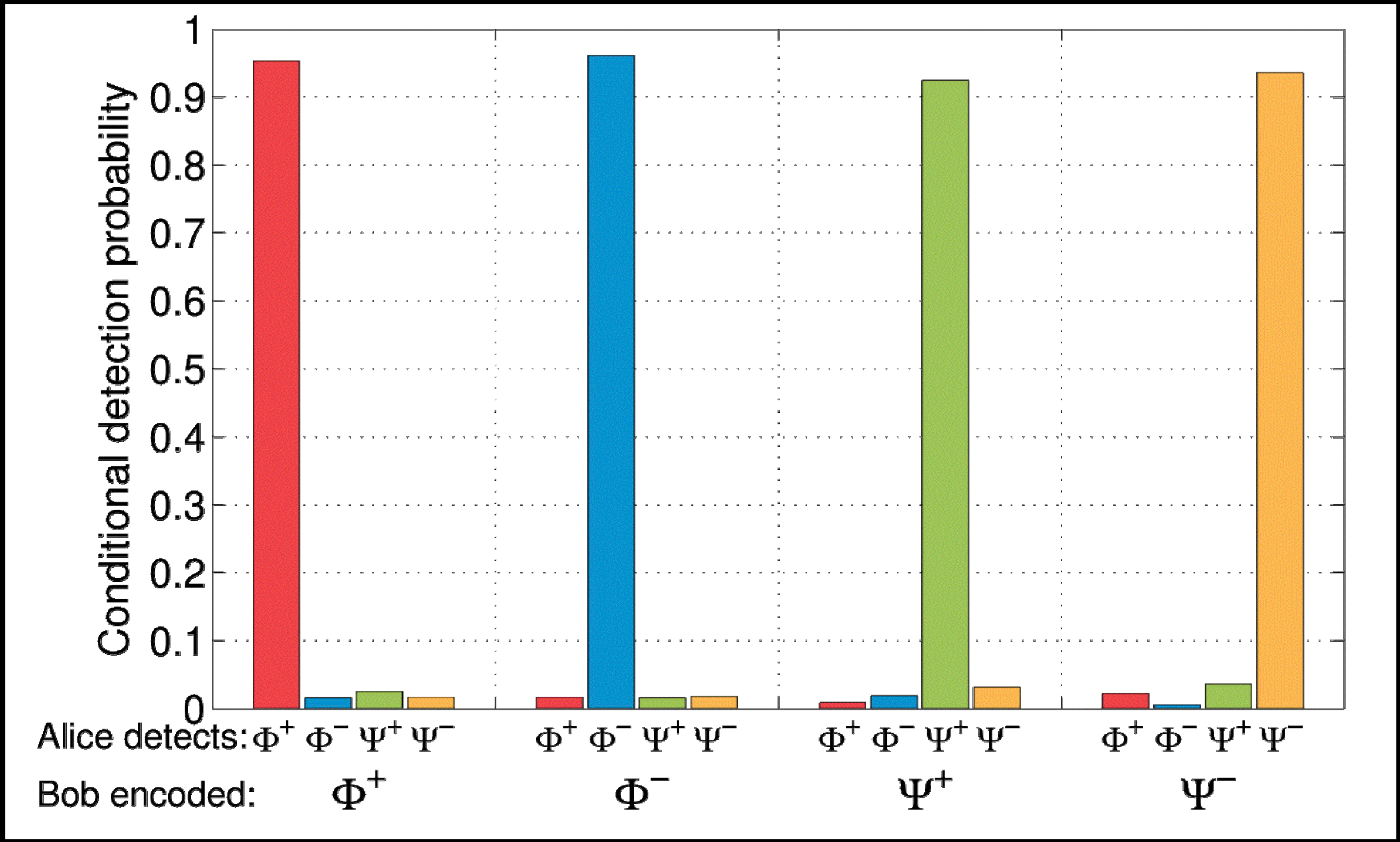
1. Alice and Bob share hyper-entangled photon pairs.
2. Bob encodes one of 4 messages: uses LCs to prepare one of 4 polarization Bell states.
3. Alice performs full BSA (via spin-orbit BSA *independently* on each photon*).



Φ^+_{spin}	0	0
Φ^-_{spin}	π	0
Ψ^+_{spin}	0	π
Ψ^-_{spin}	π	π

*Note: No storage needed.

Hyper-entanglement Enhanced Bell-state Analysis



Average success probability: 94%

Channel capacity = 1.606(6) > 1.58!

Summary

"Relativistic Quantum Cryptography"

- By allowing photon-storage, Bob can use the correct basis for every measurement ⇒ enhanced yield by 2 (4-state) or 3 (6-state)
- Yield enhancements of ~1.7 (4-state) and ~2.6 (6-state)
- First demo. of Überquantum advantage, i.e., QM + SR > QM

"Hyper-entanglement"-enhanced Quantum Dense Coding

- The photons are born entangled in multiple DOFs.
- Enhanced Bell-state analysis
  - –All four polarization Bell-states may be distinguished
  - –Thus far: Channel capacity for dense-coding: 1.606 bit/photon
- Super-duper dense-coding: 2.8 bits/photon
  (since 7/16 hyper-Bell states may be distinguished)

"The Mystery of the Quantum Cakes"

PGK & L. Hardy

AJP **68**, 33 (2000)

1. Sometimes (~9%), both cakes Rise early

2. If Lucy's cake Rises early, then Ricardo's tastes Good.

2' If Ricardo's cake Rises early, then Lucy's tastes Good.

3. If they both taste their cakes....

We expect that ≥9% of the time, both will taste Good.

3' Quantum mechanically...

Both *never* taste Good!

Quantum cakes: Mystery revealed!

$$|\psi\rangle = \frac{1}{2}|B\rangle_L|B\rangle_R - \sqrt{\frac{3}{8}}\left[|B\rangle_L|G\rangle_R + |G\rangle_L|B\rangle_R\right]$$

Experimentally:

G = Horizontal (0°), B = Vertical (90°)

R = -50.8°, NR = 39.2°

N(GG) ≥ N(RR) − N(RB) − N(BR)

or

N(GG) + N(RB) + N(BR) ≥ N(RR)

113 + 128 + 137 2422

(= 378)

“This isn’t right. This isn’t even wrong.”
– Wolfgang Pauli

“It was absolutely marvelous working for Pauli. You could ask him anything. There was no worry that he would think a particular question was stupid, since he thought all questions were stupid.”
– Victor Frederick Weisskopf

Ode to Entanglement

**Photons twins, at birth separated
And yet they remain so well correlated
Their colors, directions and spins synchopated
No wonder these states are so celebrated**

**If that one goes this way, this one goes that
If this one is thin, that one is fat
Like two random roulette wheels, yet somehow both “fixed”
To hit the same number though they’re never mixed**

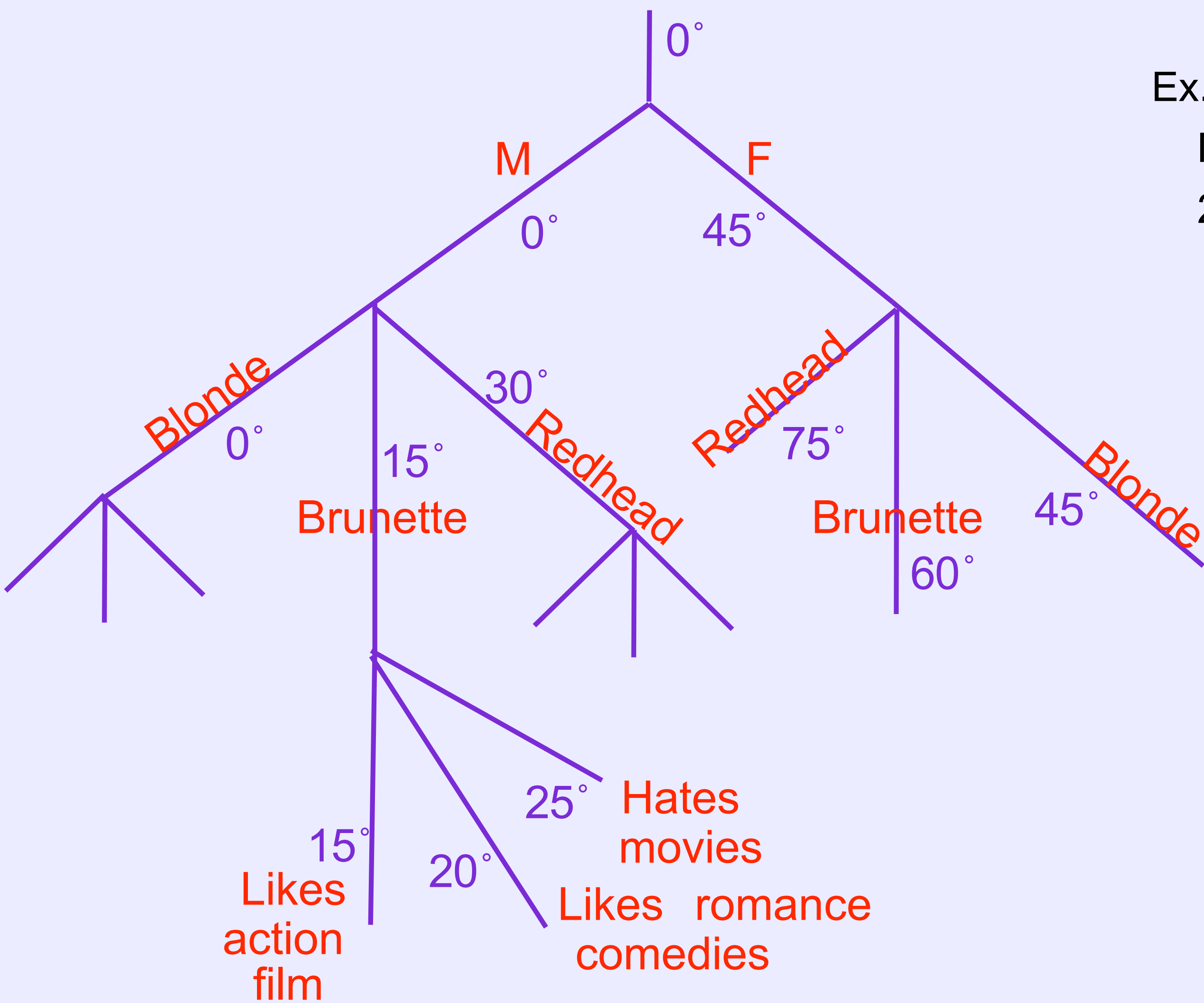
**They drove EPR to say “It’s incomplete”
They’ve got the Bell inequalities beat
When factoring primes they allow you to cheat
Who knows what new marvel is next at our feet**

**Just out of reach were problems that dangled
Current attempts to solve them seem wangled
Perhaps what’s required is something new-fangled
Enter the states called *hyper-entangled***

How much information is in a single photon?

The Quantum Dating Game:

Start with horizontally-polarized photon (0°)



Ex. Final polarization = 18.32405° --
M, brunette, likes action films,
27 years old, Gemini, ...

In principle we can encode an ***infinite*** amount of information in a single photon

But…
we can only read out a *single* bit

e.g., H or V
or 45° or -45°

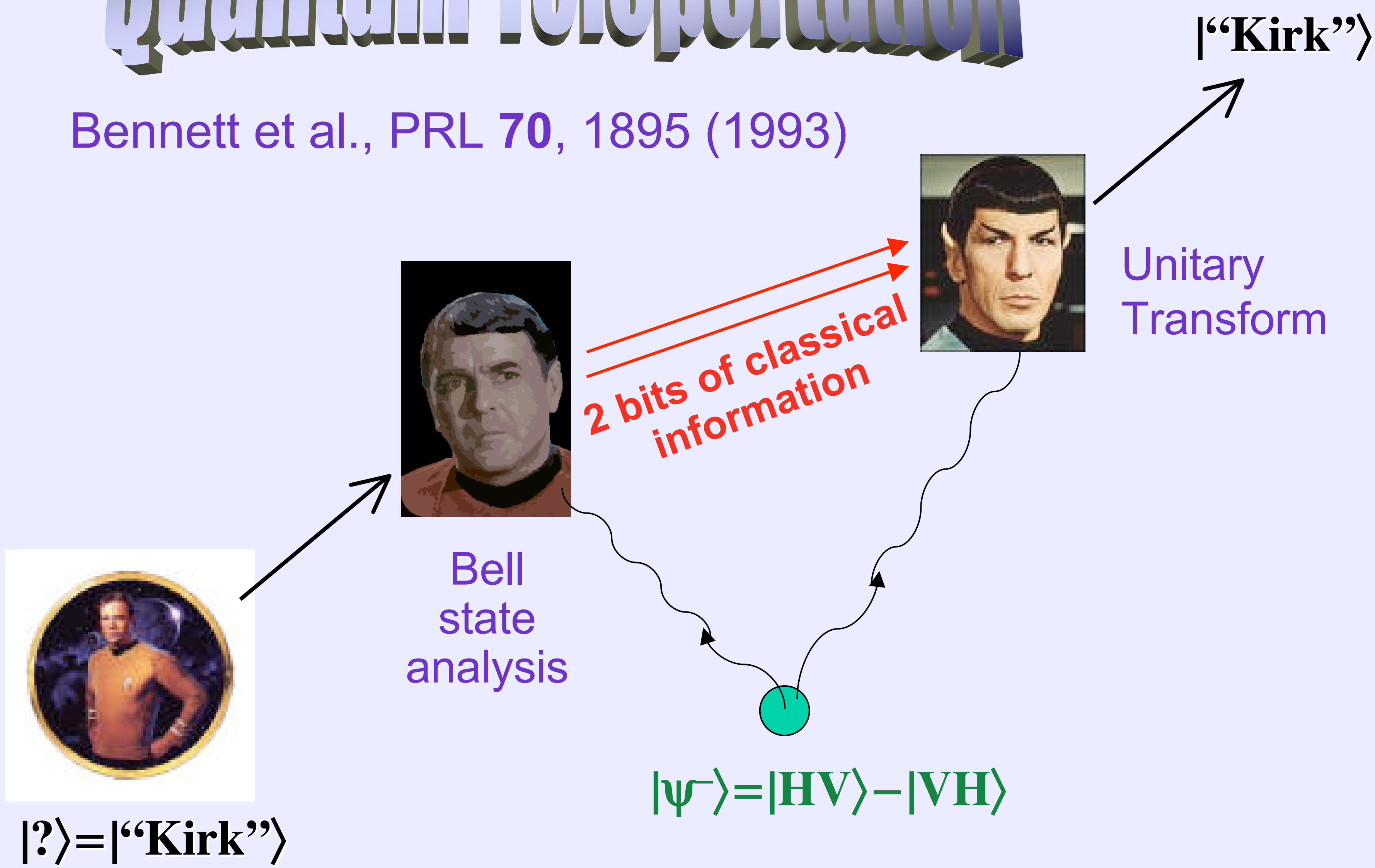
Quantum Teleportation

$|\text{"Kirk"}\rangle$

$|?\rangle = |\text{"Kirk"}\rangle$

Quantum Teleportation

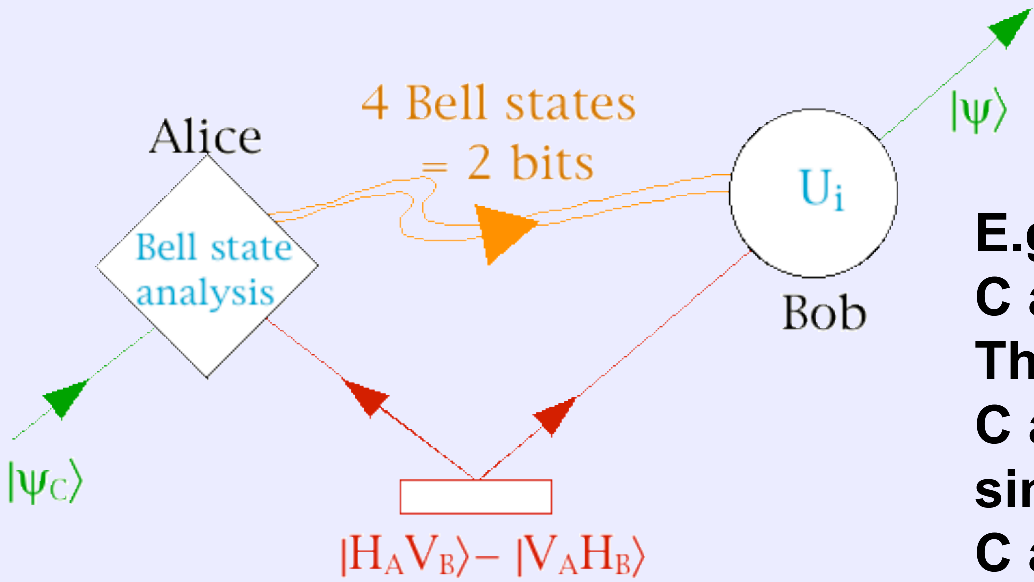
Bennett et al., PRL **70**, 1895 (1993)



Quantum Teleportation

The basic idea –> transfer the (infinite) amount of information in a qubit from Alice to Bob without sending the qubit itself.

Requires Alice and Bob to share entanglement:



E.g. Alice measures photons C and A to be in a singlet state. Then since C and A are perpendicular, and since A and B are perpendicular, C and A must be *identical*!

Remarks:

- **The original state is gone.**
- **Neither Alice nor Bob know what it was.**
- **Requires classical communication – no superluminal signaling.**
- **Bell state analysis is *hard*.**

Entangle (Oxford-English Dictionary)

To make tangled or mix up in such a manner that a separation cannot easily be made.

1699 BURNET 39 Art. i. (1700) 20

This is rather a flight of Metaphisicks that intangles one, than a plain and full conviction.

To involve in surroundings from which extrication is difficult.

1710 J. CLARKE, Rohault's Nat. Phil. (1729) I. 115

All these Particles of Matter must be broken where-ever they are intangled with those that join to them.

To involve (a person) in compromising relations with another.

1888 F. HUME Mad. Midas I. I

He became entangled with a lady whose looks were much better than her morals.

Entangle (Oxford-English Dictionary)

Mil. An extensive barrier -- formed of trees and branches, or an obstruction formed of stakes and barbed wire, arranged so as to impede an enemy's movements

1917 Shepherd 69

They've all died on the entanglements.

Hyper-Entanglement

PGK, JMO **44**, 2173 (1997)

- Photons simultaneously entangled in multiple DOFs:

$$\underbrace{(|H,H\rangle + |V,V\rangle)}_{polarization} \otimes \underbrace{(|rl\rangle + \alpha|gg\rangle + |lr\rangle)}_{spatial\ modes} \otimes \underbrace{\int_0^{E_p} dEA(E)|E\rangle_s|E_p - E\rangle_i}_{energy}$$

- Enlarged Hilbert space: $2 \otimes 2 \otimes m \otimes m \otimes n \otimes n$
- Easy to perform quantum logic *between* DOFs

  Cerf, Adami, PGK, PRA **57**,R1477 (1998)

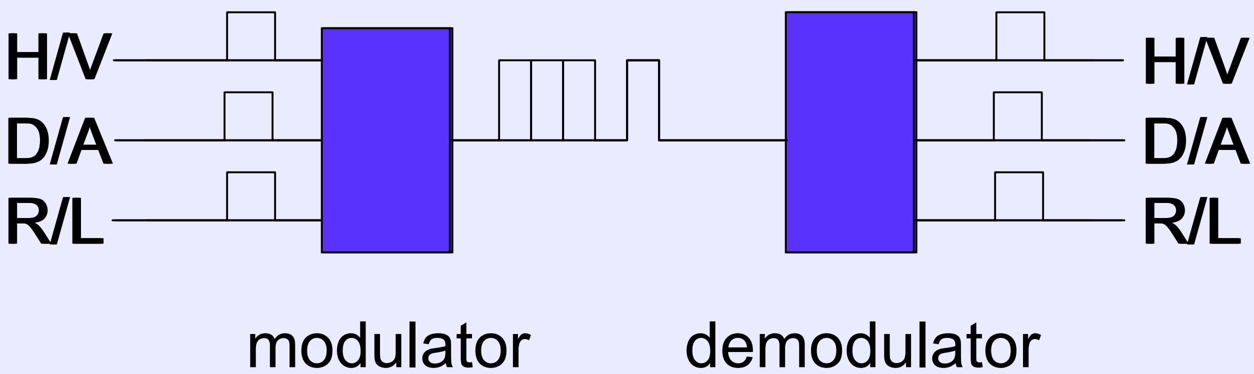
  Fiorentino & Wong, PRL **93**, 070502 (2004)

- New capabilities in quantum info. processing
  - remote preparation of entangled states
  - full Bell-state analysis
  - “super-duper” dense coding
  - quantum communication with higher alphabets
  - ???

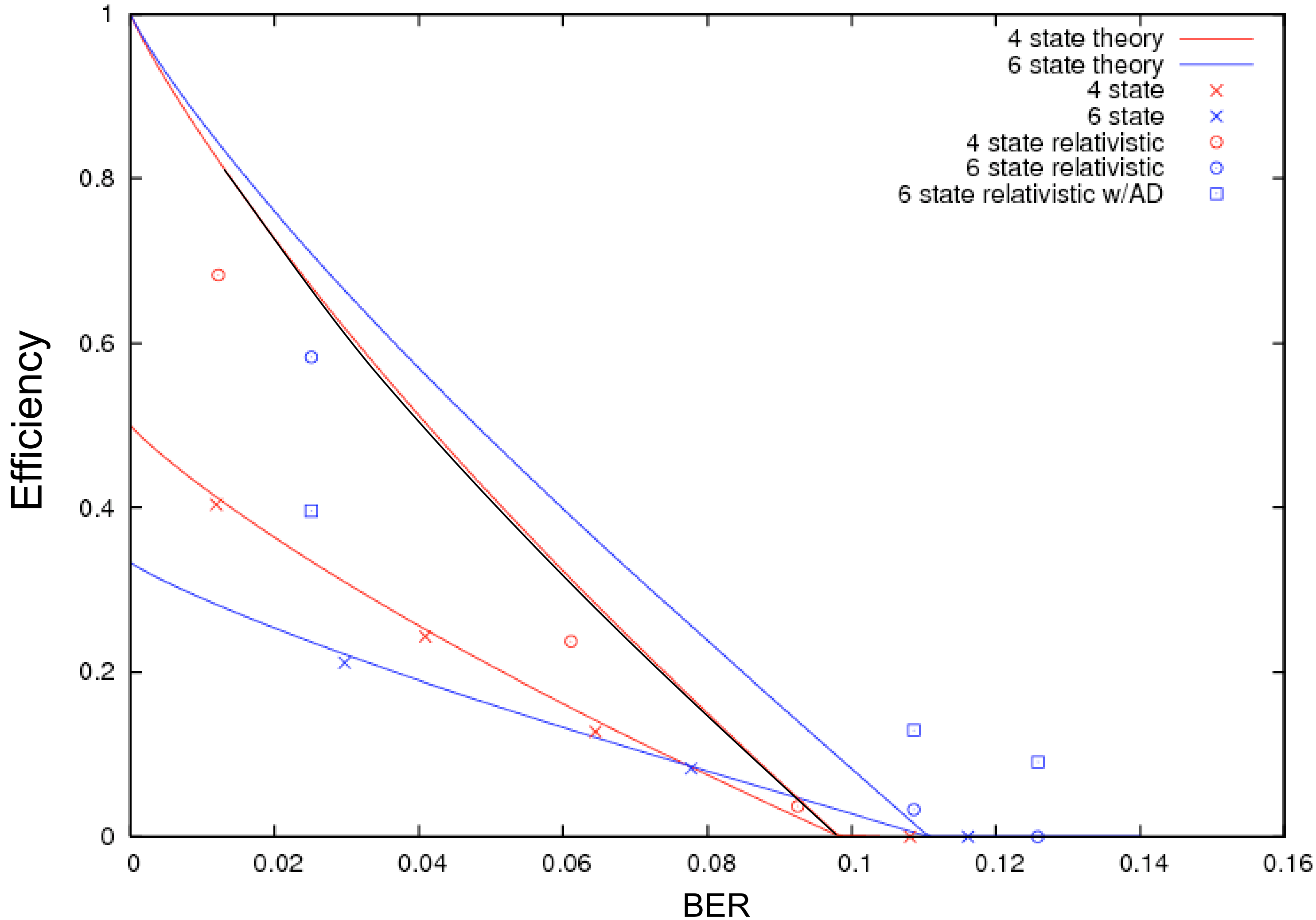
Modulation System

The classical basis information must be sent over a low-latency communication channel (since Bob can only store the photon for ~1 μs).

We implement a finite state machine using fast programmable logic (CPLD) to drive a diode laser:

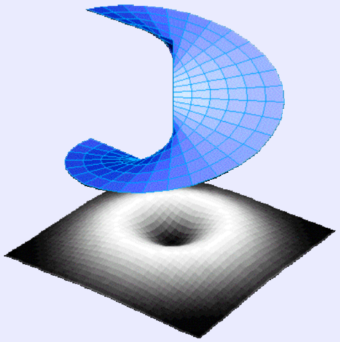


Total latency < 145 ns

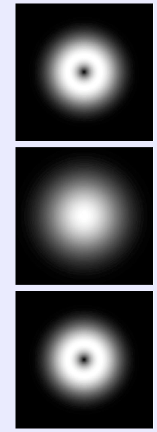


- Cavity loss (~15%) prevents yield from reaching 1.
- Eavesdropper simulated with decoherence.
- Relatively low rates (~100/s).

“Orbital” Angular Momentum of Photons



- Donut modes- Laguerre-Gaussian
- Phase SINGULARITY
- Quantized in multiples of $\hbar$



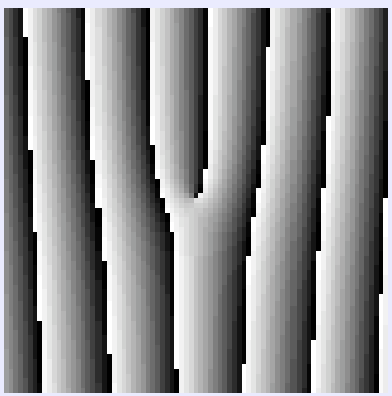
$|-1\rangle = L$

$|0\rangle = G$

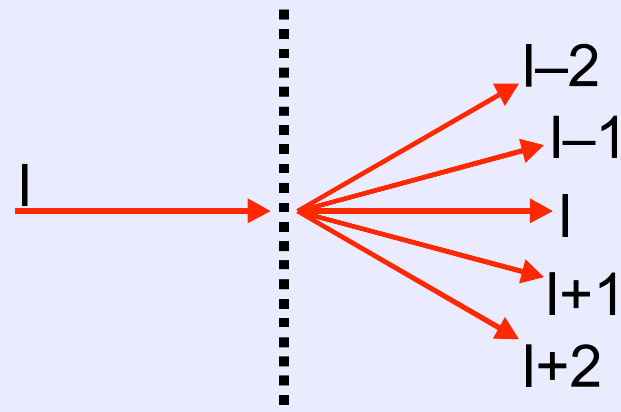
$|1\rangle = R$

Qutrits!

Holographic Detection



Diffraction at a dislocation changes the donut mode angular momentum



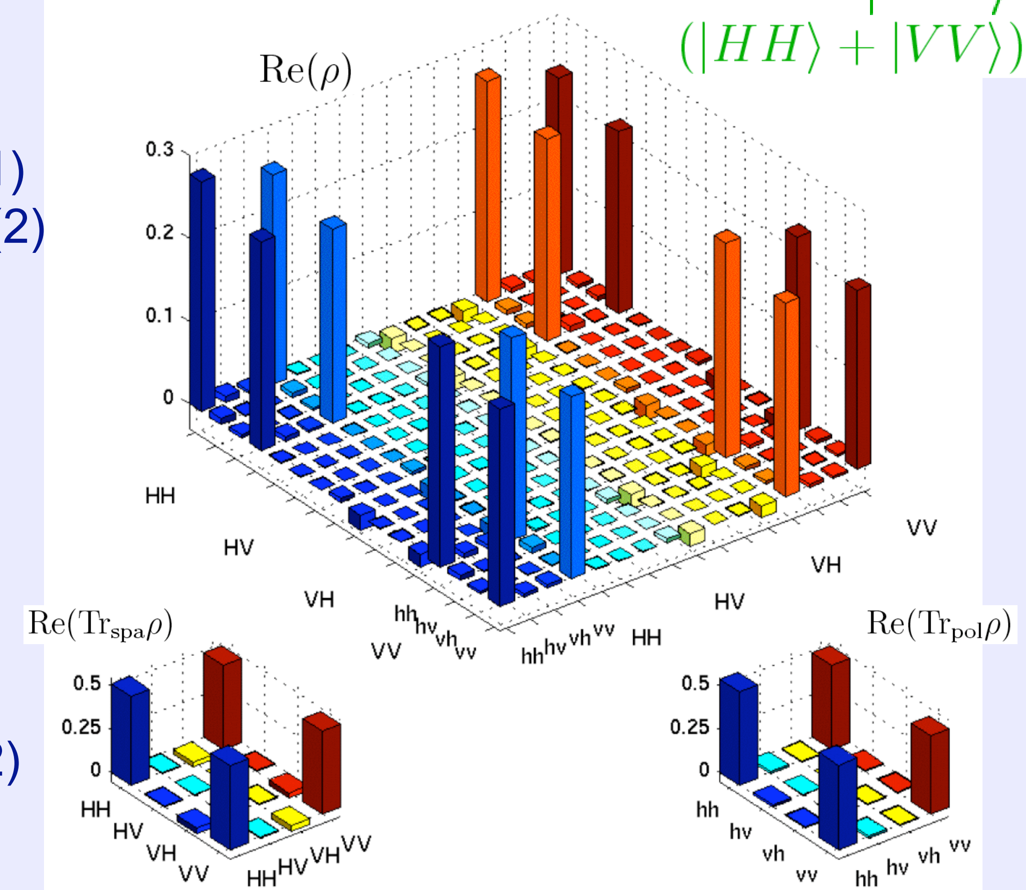
- Couple into single-mode fiber -- only accepts Gaussian mode; all others too big and cannot propagate inside fiber
- Together with the hologram we can detect other spatial modes

High-quality hyper-entangled state

Maximally hyper-entangled state: $|\Phi^+\rangle \otimes |\phi^+\rangle$

$(|HH\rangle + |VV\rangle)\otimes(|hh\rangle + |vv\rangle))$

F=0.974(1)
S_L=0.039(2)



T=0.945(2)
S_L=0.035(2)

T=0.943(2)
S_L=0.033(2)

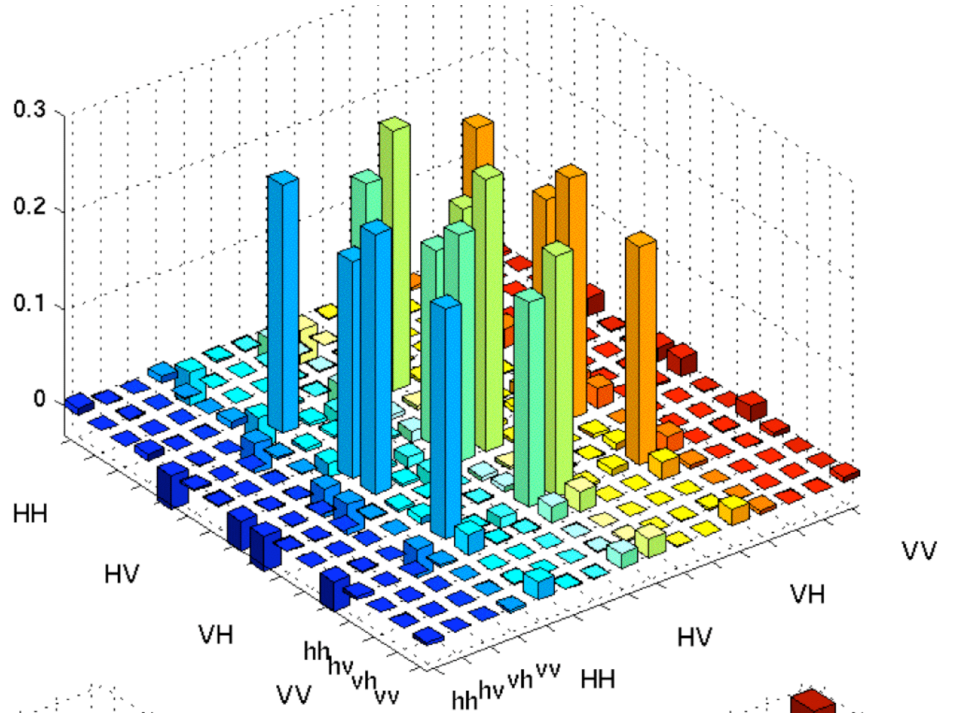
J. T. Barreiro et al., PRL **95**, 260501 (2005)

A different Bell-state combination…

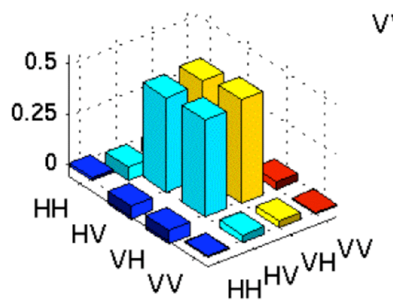
Maximally hyper-entangled state $|\Psi^{+}\rangle \otimes |\phi^{+}\rangle$

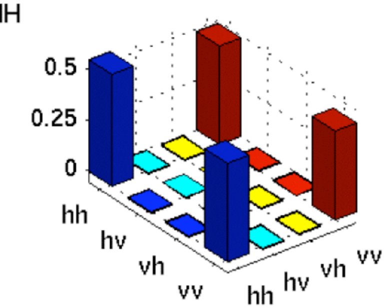
$$|\Psi^{+}\rangle_{pol} \otimes |\phi^{+}\rangle_{spa} \sim (|HV\rangle + |VH\rangle) \otimes (|hh\rangle + |vv\rangle)$$

F=0.98
S_L=0.05



T=0.93
S_L=0.05





T=0.94
S_L=0.03

PHYSICAL REVIEW LETTERS

VOLUME 69 | 16 NOVEMBER 1992 | NUMBER 20

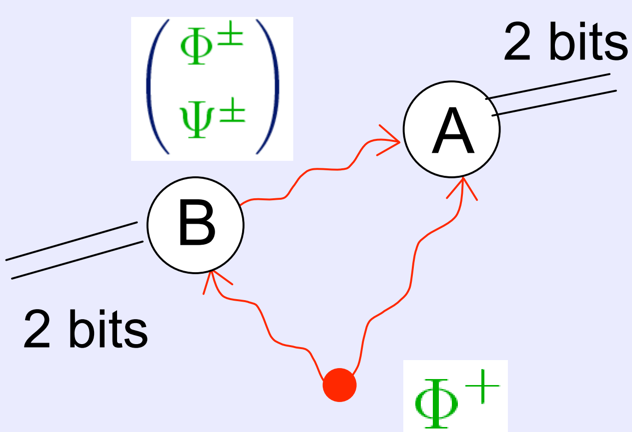
Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Stephen J. Wiesner
74 Parkman Street, Brookline, Massachusetts 02146

(Received 16 June 1992)

Quantum "Superdents Coating"



1 entangled photon each to Bob and Alice

Bob applies one of 4 U's →

one of the 4 Bell states; sends photon to Alice

Alice: BSA → infer one of 4 messages

Channel cap. = $\log_2 4$ = 2 bits/photon_from_Bob

Bell-state analysis

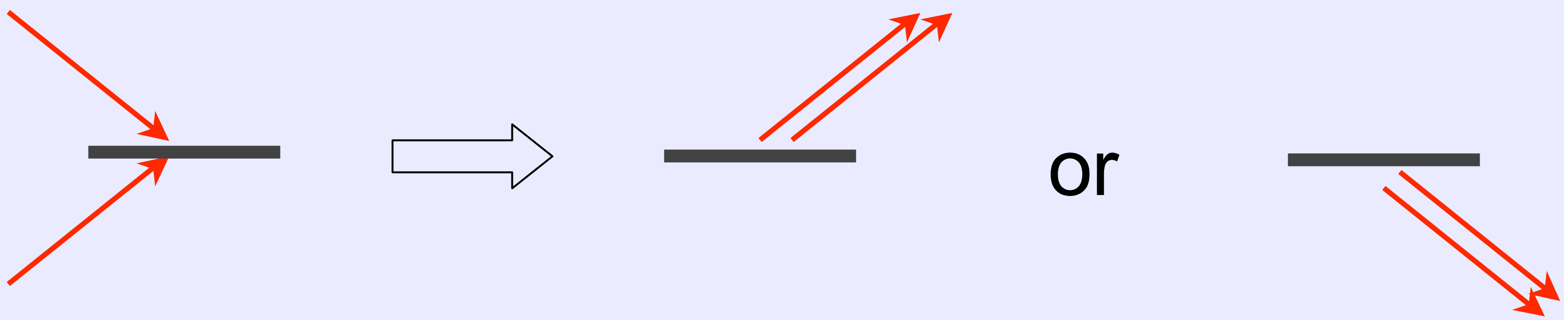
Discriminate every Bell state in a single measurement

Necessary for dense-coding, quantum teleportation, etc.

- Photon-Photon interactions (e.g., upconversion)
  - –in principle 100%; in practice 10^{-9} [Kim et al. PRL **86**, 1370 (2001)]
- Impossible with LOCC -- only 2 Bell states discriminated
  - –Vaidman & Noran, PRA **59**, 116 (1999)
  - –Lutkenhaus et al., PRA **59**, 3295 (1999)
- Probabilistic: 4 out of 4, but <u>at most</u> 50% efficient
  - –Calsamiglia & Lutkenhaus, Appl. Phys. **B72**, 67 (1999)
- **Hyper-entanglement assisted** BSA (100% efficient, 4 of 4)
  - –PGK & Weinfurter, PRA **58**, R2623 (1998)

Why BSA is hard…

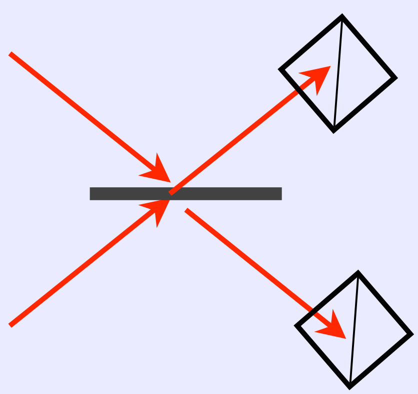
Usual HOM inteference:



Identically polarized photons go off the same way

HH + VV, HH - VV,   HV +VH   (DD - AA)

HV - VH (photons go off different ways)

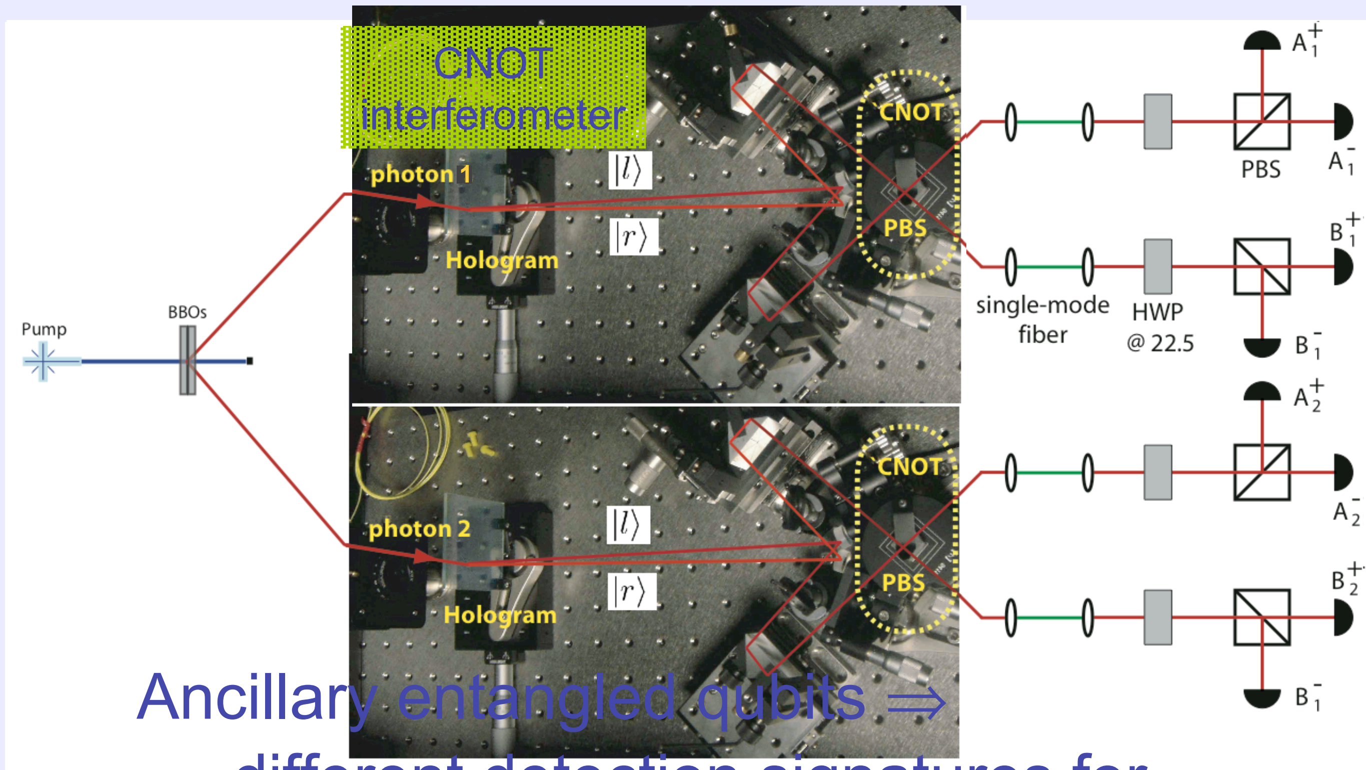


(HV +VH) behaves differently from (HH ± VV)

No way to distinguish HH + VV   and HH - VV

Hyper-entanglement Assisted Bell-state analysis

Polarization Bell states: $\begin{pmatrix} \Phi^{\pm} \\ \Psi^{\pm} \end{pmatrix} \otimes \phi^{+}$ Spatial mode Ancillary DOF



Ancillary entangled qubits ⇒ different detection signatures for all four polarization Bell states

State	Detector signature			
$\|\Phi^{\pm}\rangle$	$A_1^+ A_2^\pm$	$B_1^+ B_2^\pm$	$A_1^- A_2^\mp$	$B_1^- B_2^\mp$
$\|\Psi^{\pm}\rangle$	$A_1^+ B_2^\pm$	$B_1^+ A_2^\pm$	$A_1^- B_2^\mp$	$B_1^- A_2^\mp$

PGK & Weinfurter, PRA **58**, R2623 (1998)

Walborn et al., PRA **68**, 042313 (2003)

Schuck et al., PRL **96**, 190501 (2006)

Barbieri et al., PRA **75**, 042317 (2007)

Why hyper-entanglement helps…

Bob prepares one of 4 “hyper”-Bell states:

$$\Phi^{\pm}_{\rm spin} \otimes \Psi^{+}_{\rm orbit}$$
$$\Psi^{\pm}_{\rm spin} \otimes \Psi^{+}_{\rm orbit}$$

E.g.,

$$\frac{1}{2}(|HH\rangle + |VV\rangle) \otimes (|\circlearrowleft\circlearrowright\rangle + |\circlearrowright\circlearrowleft\rangle)$$

Rewrite in terms of *single-photon* entanglements:

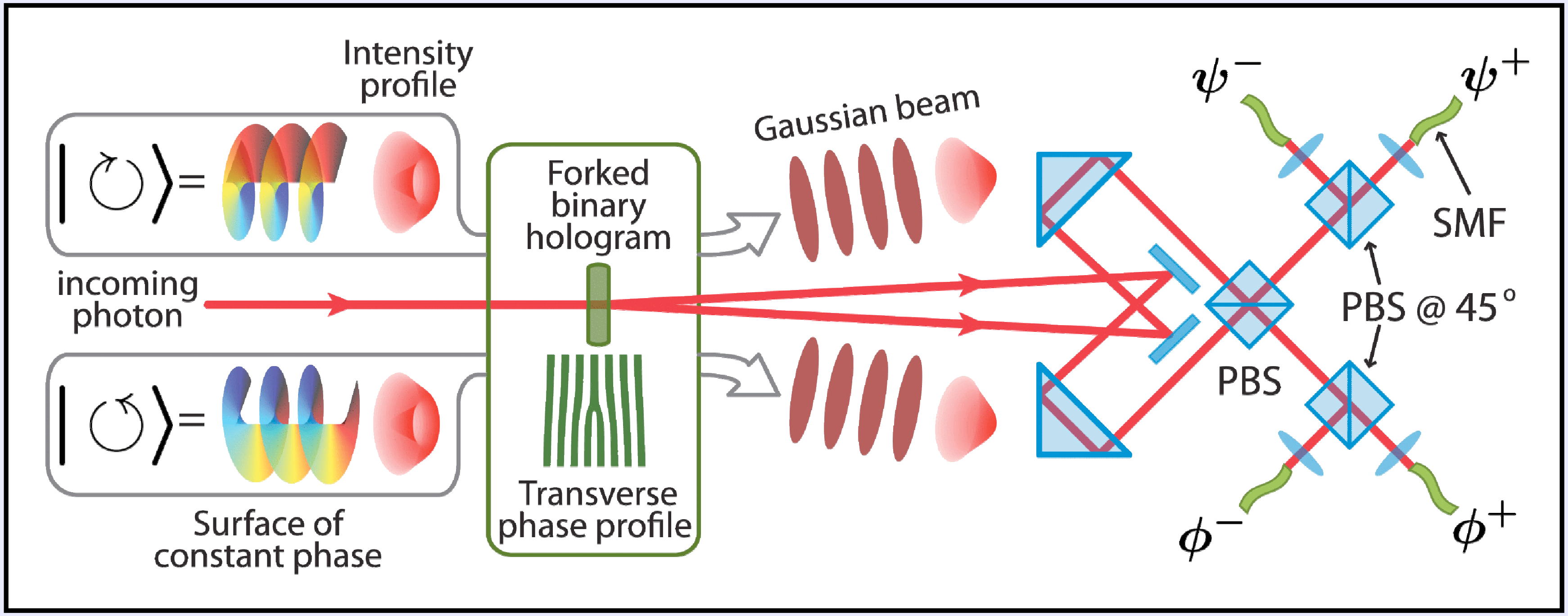
$$\Phi^{\pm}_{\rm spin} \otimes \Psi^{+}_{\rm orbit} = \frac{1}{4}(\ \phi_1^{+} \otimes \psi_2^{\mp} + \phi_1^{-} \otimes \psi_2^{\pm} + \psi_1^{+} \otimes \phi_2^{\pm} + \psi_1^{-} \otimes \phi_2^{\mp})$$
$$\Psi^{\pm}_{\rm spin} \otimes \Psi^{+}_{\rm orbit} = \frac{1}{4}(\ \phi_1^{+} \otimes \phi_2^{\mp} + \phi_1^{-} \otimes \phi_2^{\pm} + \psi_1^{+} \otimes \psi_2^{\pm} + \psi_1^{-} \otimes \psi_2^{\mp})$$

where

$$\phi^{\pm} \equiv \frac{1}{\sqrt{2}}(|H\circlearrowleft\rangle \pm |V\circlearrowright\rangle)$$
$$\psi^{\pm} \equiv \frac{1}{\sqrt{2}}(|H\circlearrowright\rangle \pm |V\circlearrowleft\rangle)$$

Alice only needs to distinguish $\phi^{\pm}$, $\psi^{\pm}$…

Spin-Orbit CNOT Gate

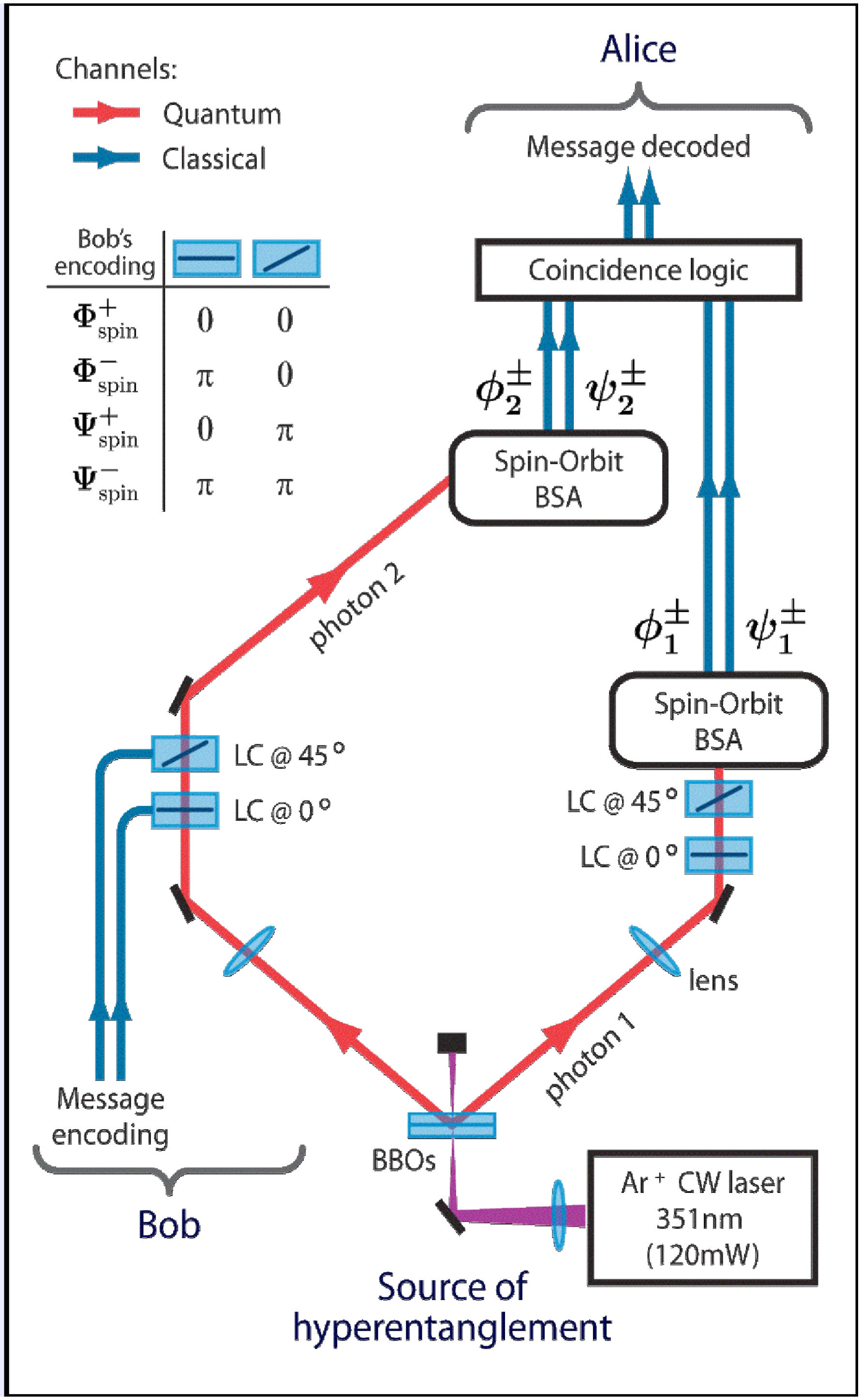


$$\phi^{\pm} \equiv \frac{1}{\sqrt{2}}\left(|H \circlearrowleft\rangle \pm |V \circlearrowright\rangle\right)$$

$$\psi^{\pm} \equiv \frac{1}{\sqrt{2}}\left(|H \circlearrowright\rangle \pm |V \circlearrowleft\rangle\right)$$

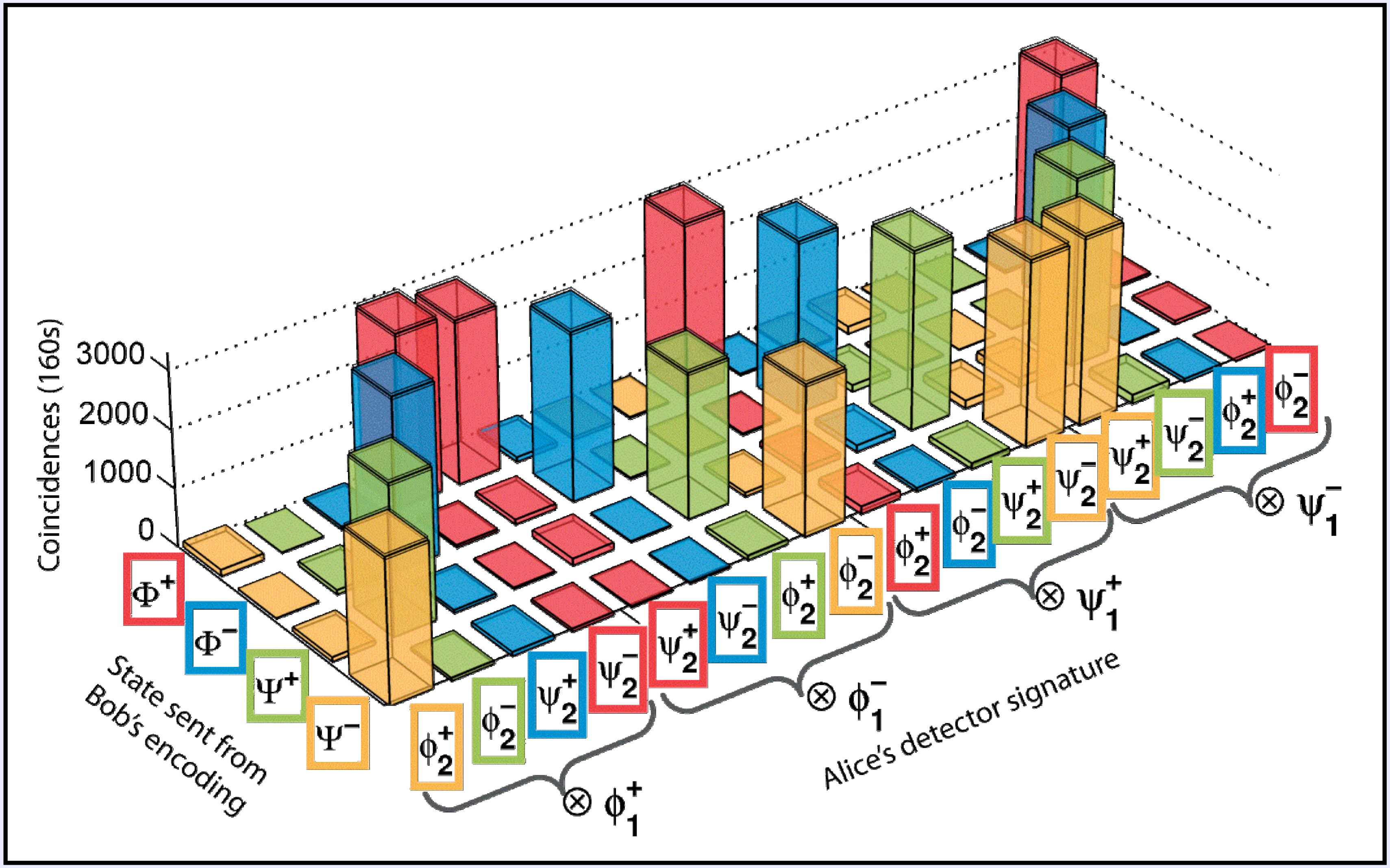
Hyper-entanglement-assisted Superdense coding

1. Alice and Bob share hyper-entangled photon pairs.
2. Bob encodes one of 4 messages: uses LCs to prepare one of 4 polarization Bell states.
3. Alice performs full BSA (via spin-orbit BSA *independently* on each photon*).



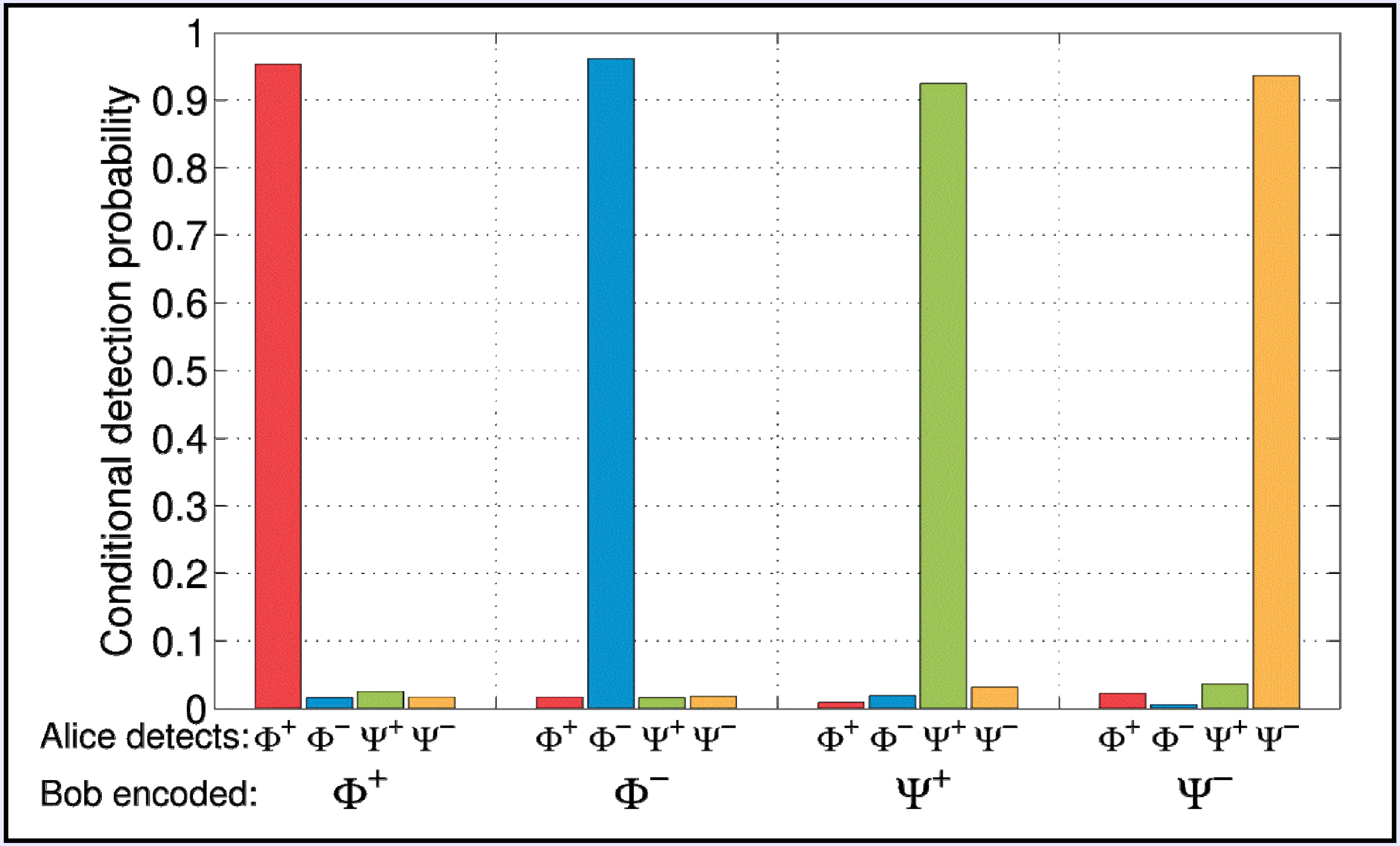
*Note: No storage needed.

Superdense-coding Results



Combine to get probabilities…

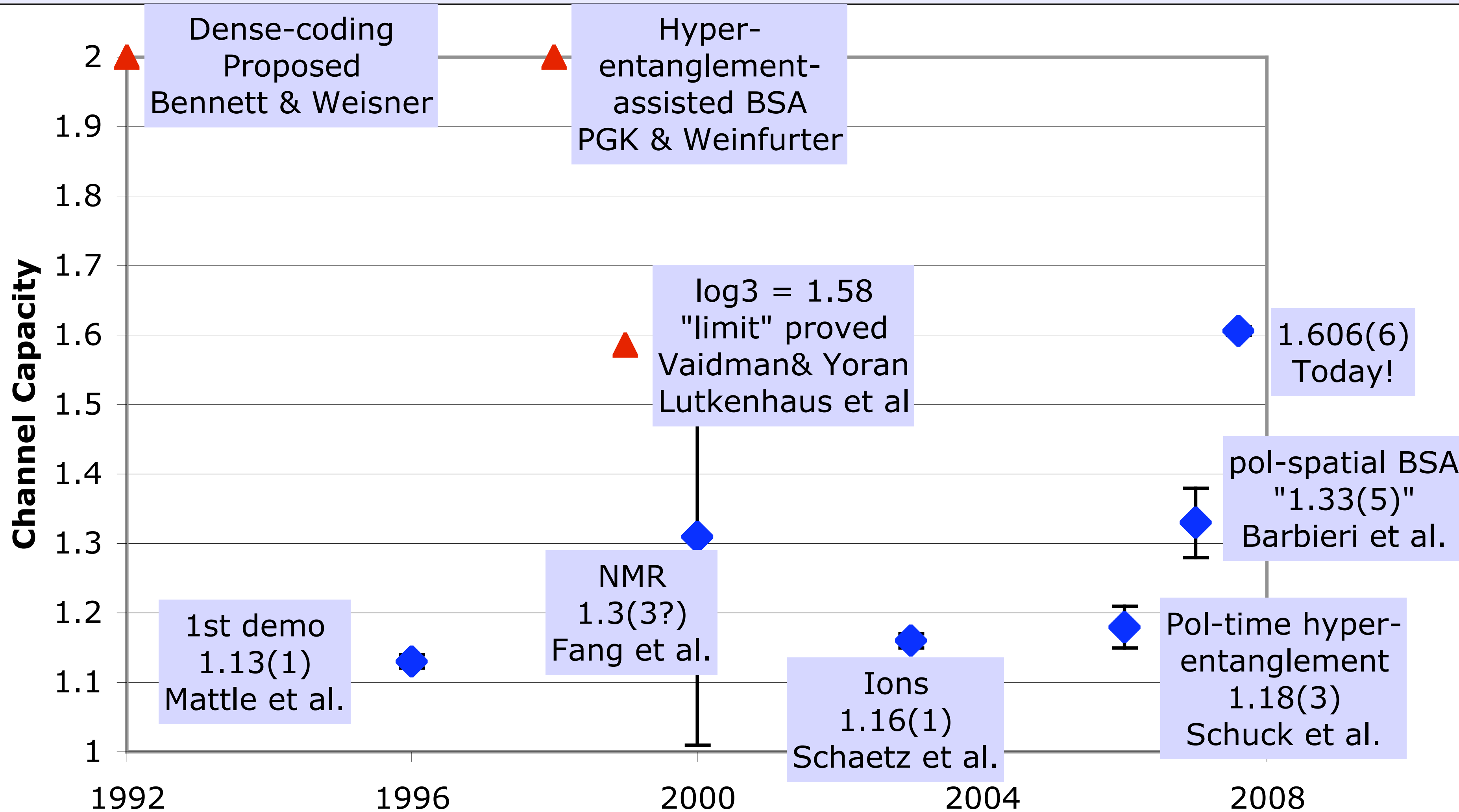
Superdense-coding Results, cont.



Average success probability: 94%

But what's the channel capacity??

Dense-Coding Timeline



Measured CC: 1.606(6) > 1.58 (“limit” for linear optics superdense coding, i.e., without hyperentanglement)

Superdense-Coding Error Budget

Effect	Reduction to C.C.
Imperfect state*	
T_{pol} = 95(2)%, S_{pol} = 3(1)%	–0.12(3)
T_{OAM} = 91(4)%, S_{OAM} = 6(2)%	–0.20(5)
PBS crosstalk	
T_V = 1.0(1)%, R_H = 0.5(1)%	–0.11(1)
Accidental coincidences	
0.02 s^{-1}	–0.01
	–0.36(5) ⇒ CC_{thy} = 1.64(5)
	CC_{exp} = 1.606(6)

* Measured via complete state tomography

Hyper-Bell state analysis

Use polarization

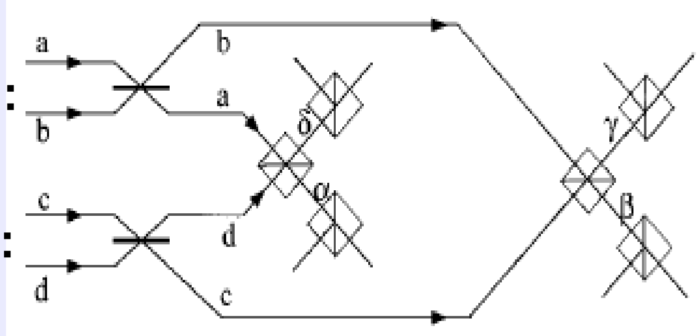
$$\Phi^{\pm} \equiv (H_1 H_2 \pm V_1 V_2), \quad \Psi^{\pm} \equiv (H_1 V_2 \pm V_1 H_2)$$

and momentum:

$$\phi^{\pm} \equiv (a_1 b_2 \pm c_1 d_2), \quad \psi^{\pm} \equiv (a_1 d_2 \pm c_1 b_2)$$

1:

2:



➔16 Bell states ➔ How to distinguish?

State	Detector signature
$\Phi^+ \otimes \phi^+$, $\Phi^- \otimes \phi^-$, $\Psi^+ \otimes \psi^-$, $\Psi^- \otimes \psi^+$	$\alpha_{45}\alpha_{45}$, $\alpha_{\overline{45}}\alpha_{\overline{45}}$, $\beta_{45}\beta_{45}$, $\beta_{\overline{45}}\beta_{\overline{45}}$, $\delta_{45}\delta_{45}$, $\delta_{\overline{45}}\delta_{\overline{45}}$, $\gamma_{45}\gamma_{45}$, $\gamma_{\overline{45}}\gamma_{\overline{45}}$
$\Phi^- \otimes \phi^+$, $\Phi^+ \otimes \phi^-$	$\alpha_{45}\alpha_{\overline{45}}$, $\beta_{45}\beta_{\overline{45}}$, $\delta_{45}\delta_{\overline{45}}$, $\gamma_{45}\gamma_{\overline{45}}$
$\Psi^+ \otimes \phi^+$, $\Phi^+ \otimes \psi^-$	$\alpha_{45}\delta_{45}$, $\alpha_{\overline{45}}\delta_{\overline{45}}$, $\beta_{45}\gamma_{45}$, $\beta_{\overline{45}}\gamma_{\overline{45}}$
$\Psi^- \otimes \phi^+$, $\Phi^+ \otimes \psi^+$	$\alpha_{45}\gamma_{45}$, $\alpha_{\overline{45}}\gamma_{\overline{45}}$, $\beta_{45}\delta_{45}$, $\beta_{\overline{45}}\delta_{\overline{45}}$
$\Psi^+ \otimes \phi^-$, $\Phi^- \otimes \psi^-$	$\alpha_{45}\delta_{\overline{45}}$, $\alpha_{\overline{45}}\delta_{45}$, $\beta_{45}\gamma_{\overline{45}}$, $\beta_{\overline{45}}\gamma_{45}$
$\Psi^- \otimes \phi^-$, $\Phi^- \otimes \psi^+$	$\alpha_{45}\gamma_{\overline{45}}$, $\alpha_{\overline{45}}\gamma_{45}$, $\beta_{45}\delta_{\overline{45}}$, $\beta_{\overline{45}}\delta_{45}$
$\Psi^- \otimes \psi^-$, $\Psi^+ \otimes \psi^+$	$\alpha_{45}\beta_{45}$, $\alpha_{\overline{45}}\beta_{\overline{45}}$, $\delta_{45}\gamma_{45}$, $\delta_{\overline{45}}\gamma_{\overline{45}}$

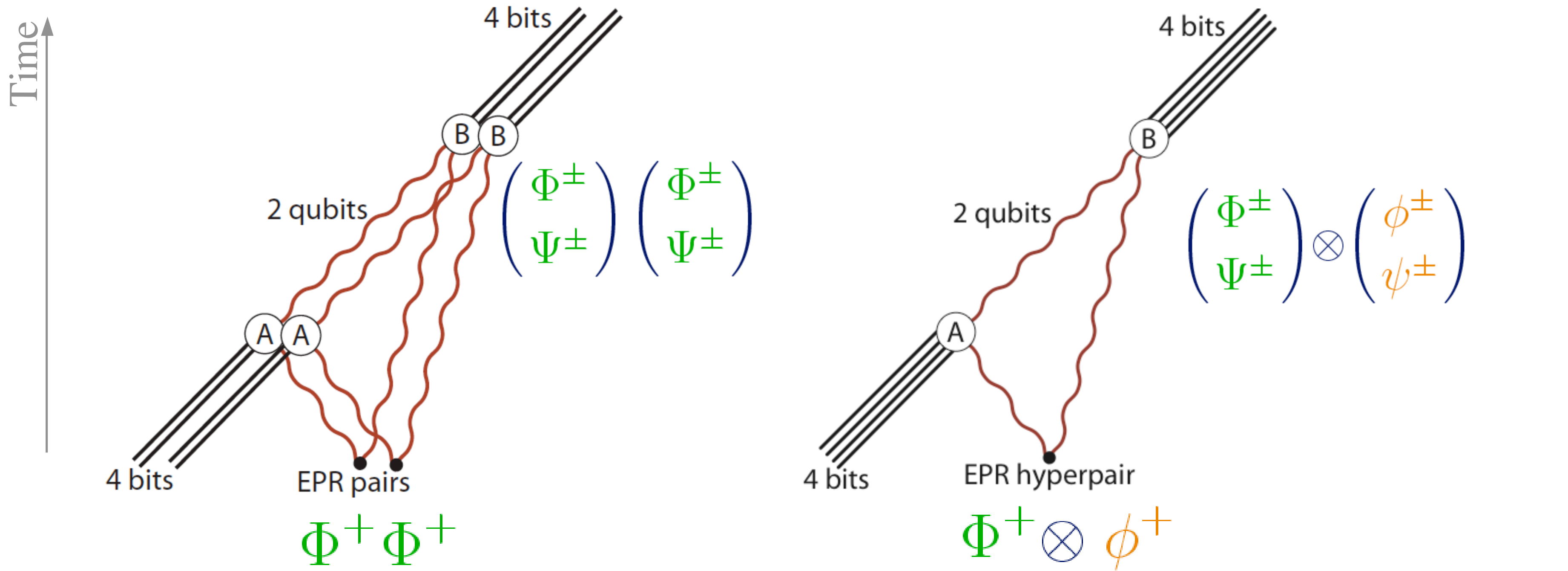
7 groups distinguishable; is it optimal?

"Hyperentangled Bell-state analysis", T.-C. Wei, J. Barreiro, P. Kwiat, quant-ph/0703117, to appear PRA (2007)

Check all *12870* partitions into 8 groups $\rightarrow$ none work.

Conclusion: **7 *is* the optimal with linear optics and projective measurements** (POVMs under consideration)

"Super-duper" dense-coding



- Standard dense-coding: In principle encodes 2 bits; LOCC limits to $\log_2(3)$ ~ 1.58 bits.
- *Hyper-entanglement-enhanced super-duper dense-coding encodes $\log_2(7)$ ~ 2.81 bits.*
- One *could* just use 2 pairs → distinguish 3x3 states ⇒ 3.2 bits BUT actual efficiency $\propto \eta^4$!

Conclusion: Hyper-entanglement is superior if $\eta < \sqrt{7/9}$ = 88%

Advanced Quantum Comm. Protocols

"Hyper-entanglement"

- The photons are born entangled in multiple DOFs.

- Demonstrate Remote Entangled State Preparation (F ~ 90%)

- Enhanced Bell-state analysis
  - –All four polarization Bell-states may be distinguished
  - –7/16 hyper-Bell states may be distinguished

- Super dense-coding: Achieved 1.606 bits/photon
  - –Exceeds the standard linear optics limit of 1.58.
  - –First experiment to show hyper-entanglement advantage.
  - –±1 OAM modes "extremely resilient to distortion" (Padgett et al.)

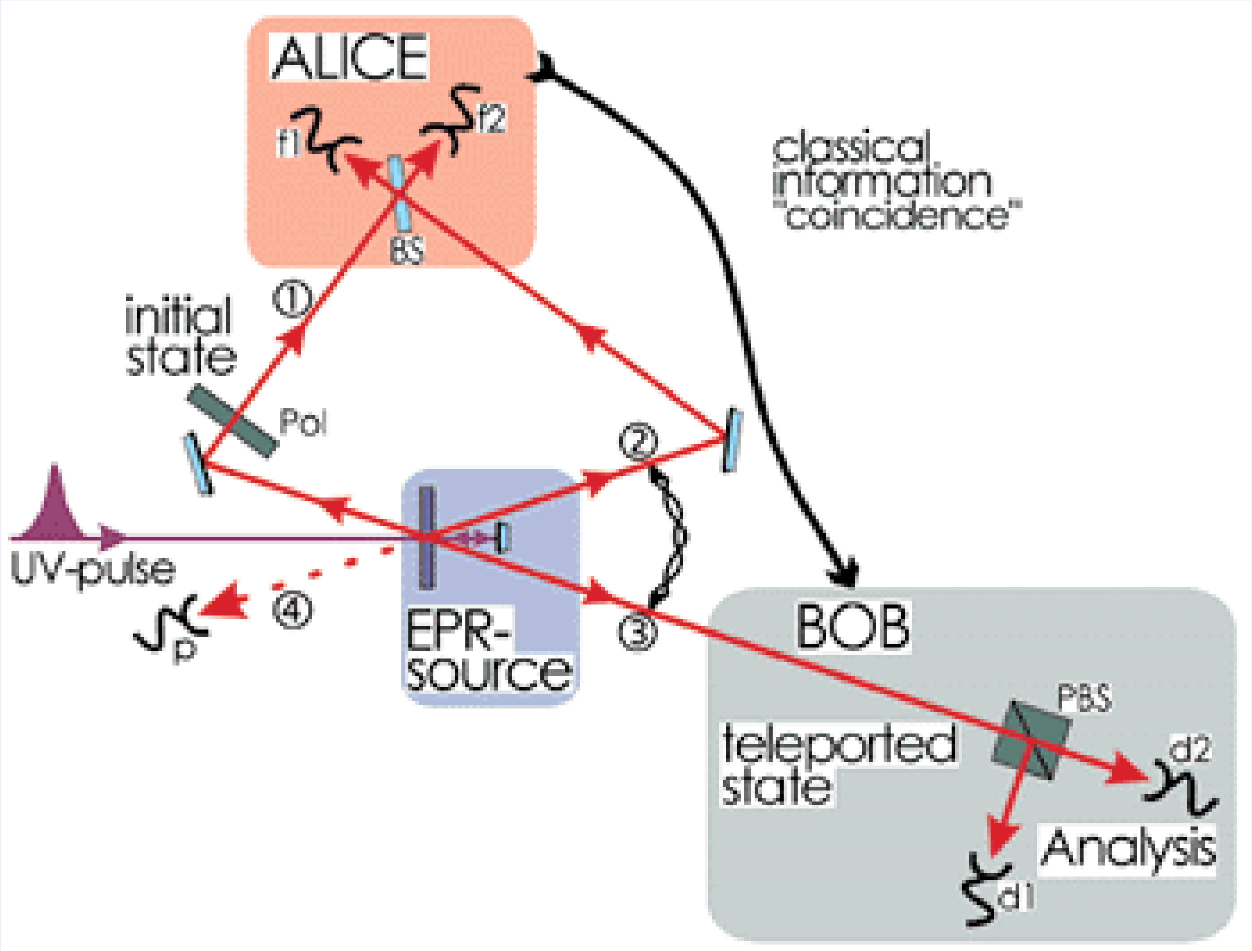
- Super-duper dense-coding: 2.8 bits/photon possible
  - –Better than multiple-pair encoding if $\eta < 88\%$
- Thank you!

Outlook for Photonic Quantum Information

- Quantum Communication:
  - –Robust, efficient sources of entanglement for provable security
  - –Q. cryptography over longer distances (q. repeaters, satellite?!)
- Quantum Computation:
  - –Scalable implementations require robust engineered sources and custom nano-optics.
  - –Implement simple algorithms; quantum simulation
- Quantum Metrology:
  - –High resolution, non-invasive measurements – microscopy
  - –More precise control – lithography
- Fundamental:
  - –Discover/create novel quantum states
  - –Develop intuition for the quintessential quantum features
  - –Quantum cooking…

Experimental Teleportation

Bouwmeester et al., Nature **390**, 575 (1997)



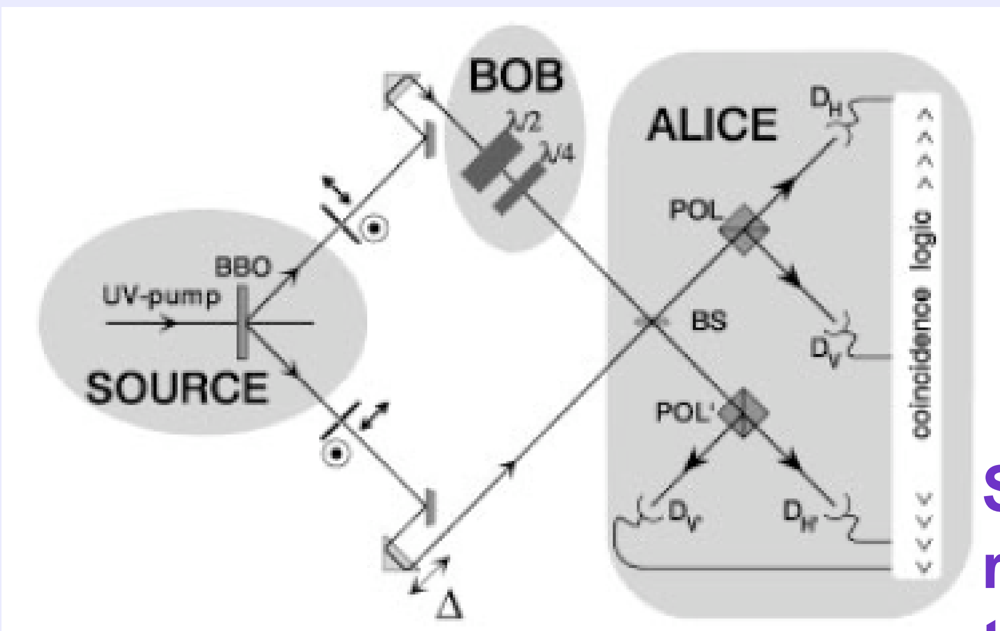
Now demonstrated teleportation of entanglement, other degrees of freedom, continuous variables, energy states of ions, 2-qubits …

VOLUME 76, NUMBER 25 PHYSICAL REVIEW LETTERS 17 JUNE 1996

Dense Coding in Experimental Quantum Communication

Klaus Mattle,[1] Harald Weinfurter,[1] Paul G. Kwiat,[1,2] and Anton Zeilinger[1]
[1]*Institut für Experimentalphysik, Universität Innsbruck, A-6020 Innsbruck, Austria*
[2]*Los Alamos National Laboratory, P-23, MS-H803, Los Alamos, New Mexico 87545*
(Received 22 November 1995)

Classically, sending more than one bit of information requires manipulation of more than one two-state particle. We demonstrate experimentally that one can transmit one of three messages, i.e., 1 "trit" ≈ 1.58 bit, by manipulating only one of two entangled particles. The increased channel capacity is proven by transmitting ASCII characters in five trits instead of the usual 8 bits. [S0031-9007(96)00478-4]



Bob's setting λ/2	Bob's setting λ/4	State sent
0°	0°	$\|\Psi^+\rangle$
0°	90°	$\|\Psi^-\rangle$
45°	0°	$\|\Phi^+\rangle$
45°	90°	$\|\Phi^-\rangle$

Signal-to-noise ratio further reduced channel capacity to only 1.13 bits/photon

Entangle (Oxford-English Dictionary)

To render (a subject, etc.) complicated or intricate; to involve in mental difficulties, perplex, bewilder.

1677 Govt. Venice 269
Your Scholars..rather intangle and perplex Councils than clear them.

1836 J. GILBERT Chr. Atonem. viii. (1852) 239
Thus entanglements arise not easy to be unravelled.

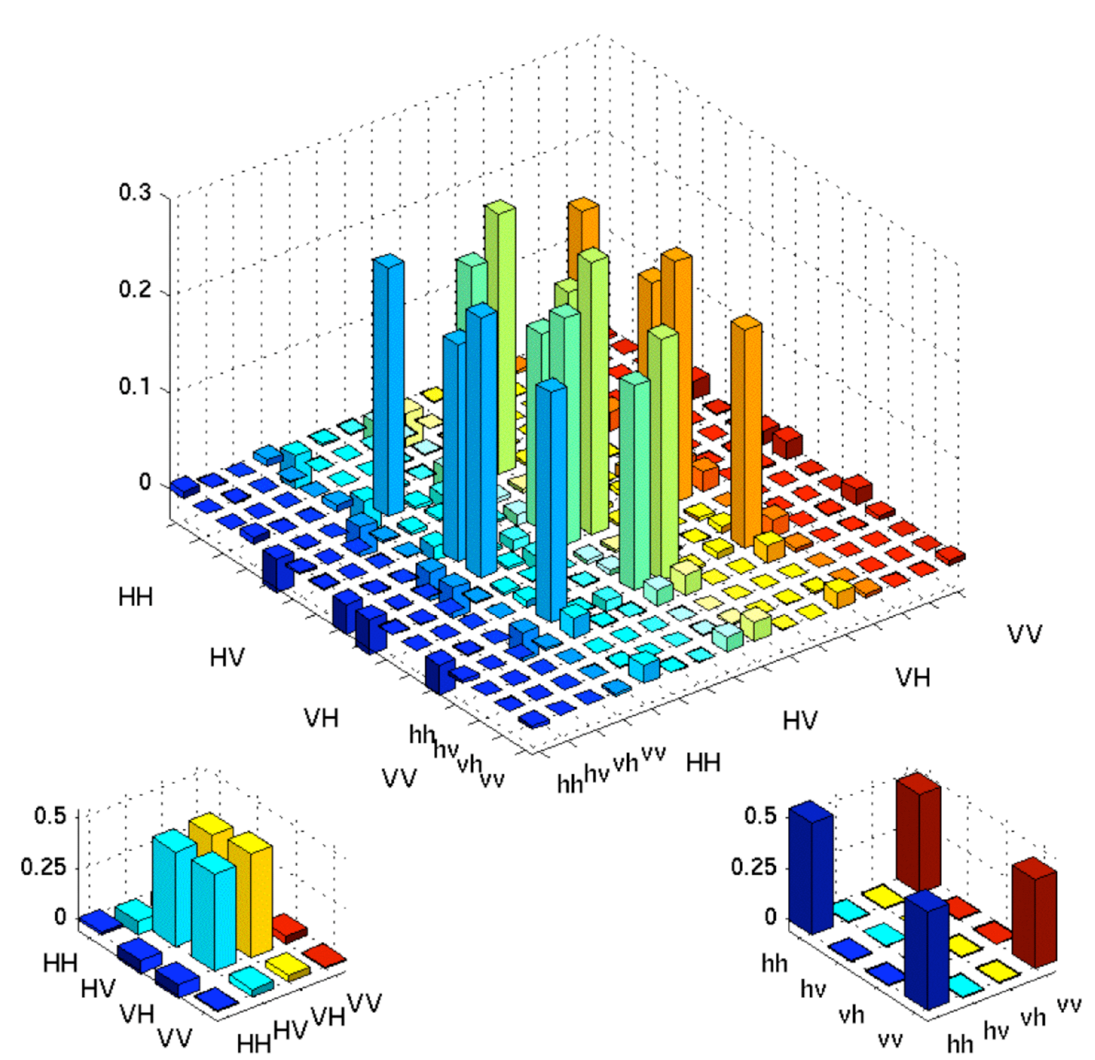
1875 JOWETT Plato (ed. 2) IV. 267
These are a few of the entanglements which impede the natural course of human thought.

Another Bell-state

$$|\Psi^+\rangle \otimes |\phi^+\rangle$$

F=0.98
S_L=0.05

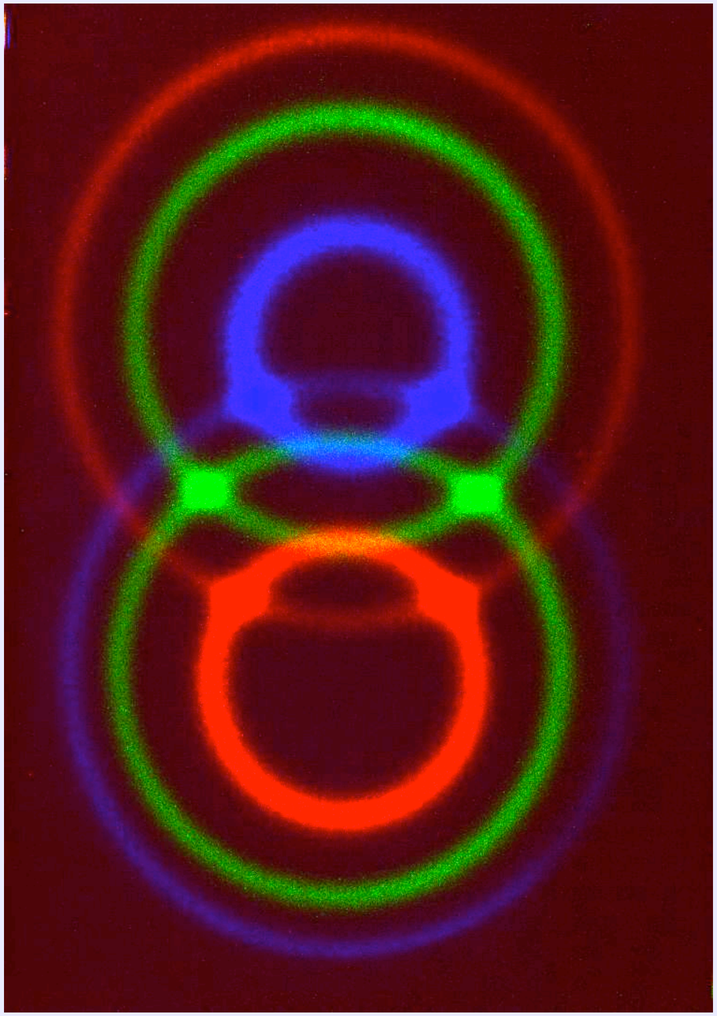
T=0.93
S_L=0.05



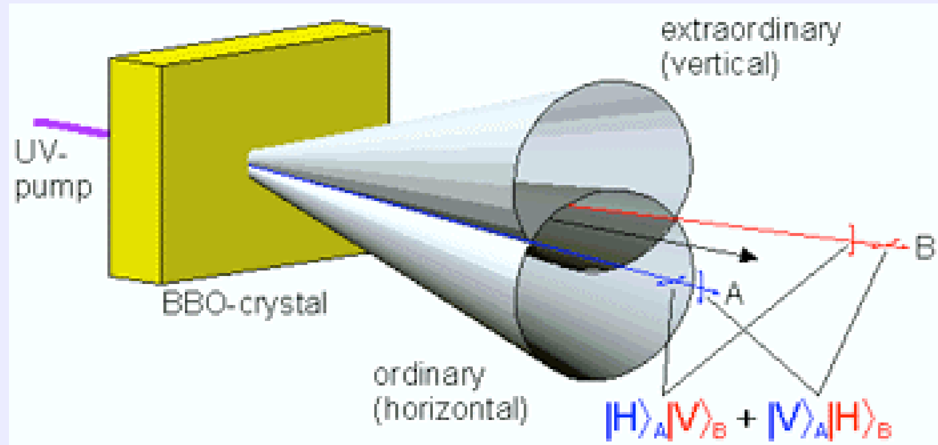
T=0.94
S_L=0.03

J. T. Barreiro et al., PRL **95**, 260501 (2005)

First polarization-entangled downconversion source



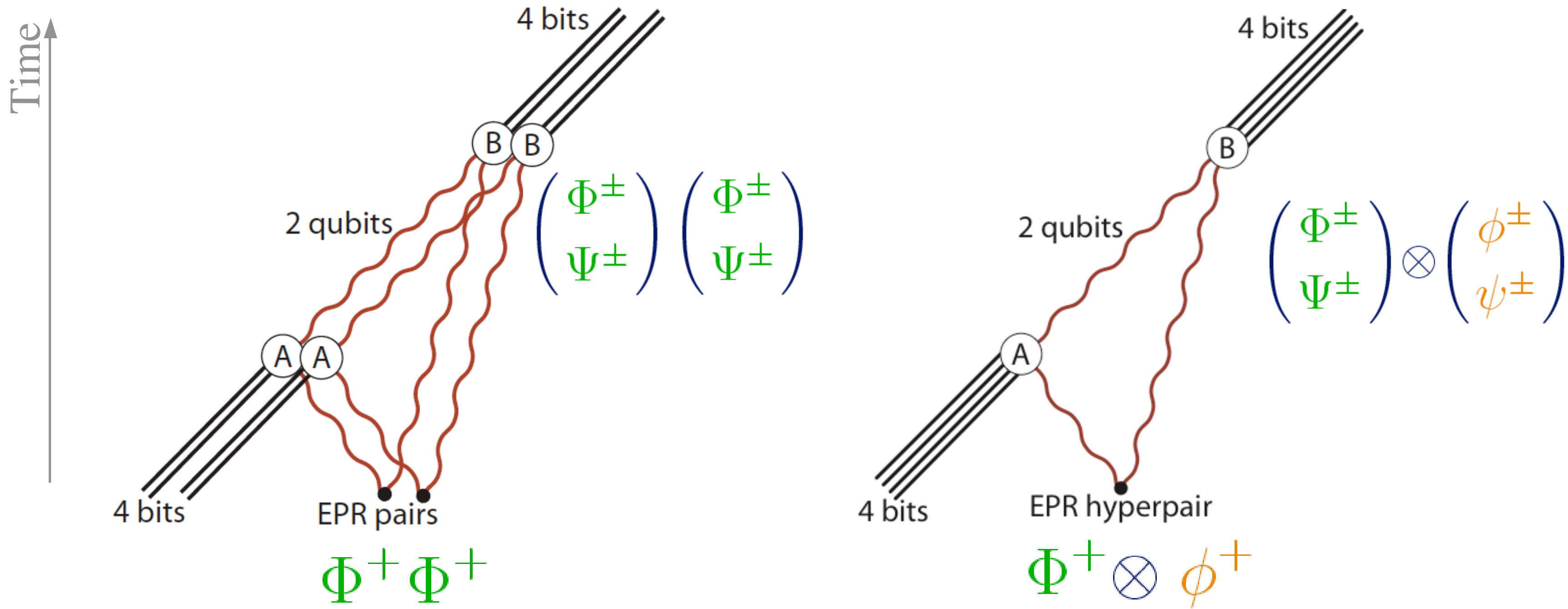
PRL **75**, 4337 (1995)



- Super dense-coding
- Teleportation
- Quantum cryptography
- 3 qubit GHZ correlations
- Entanglement swapping
- 4-6 qubit q. computing

•
•
•

"Super-duper" dense-coding
(a.k.a. state discrimination)



- Standard dense-coding: In principle encodes 2 bits; LOCC limits to $\log_2(3) \sim 1.6$ bits.
- *Hyper-entanglement-enhanced super-duper dense-coding encodes* $\log_2(7) \sim 2.81$ *bits.*
- One *could* just use 2 pairs $\rightarrow$ distinguish 3x3 states $\Rightarrow$ 3.2 bits

  BUT actual efficiency $\propto \eta^4$!

Conclusion: Hyperentanglement is superior if $\eta < \sqrt{7/9} = 88\%$

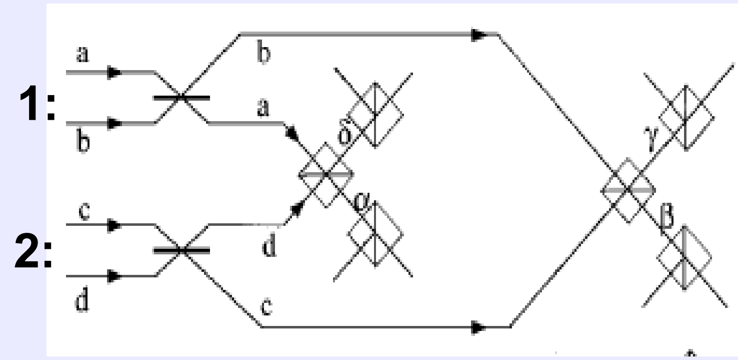
Hyper-Bell state analysis

Use polarization

$$\Phi^{\pm} \equiv (H_1 H_2 \pm V_1 V_2), \quad \Psi^{\pm} \equiv (H_1 V_2 \pm V_1 H_2)$$

and momentum:

$$\phi^{\pm} \equiv (a_1 b_2 \pm c_1 d_2), \quad \psi^{\pm} \equiv (a_1 d_2 \pm c_1 b_2)$$



➔16 Bell states ➔ 7 groups under current scheme

State	Detector signature
$\Phi^+ \otimes \phi^+$, $\Phi^- \otimes \phi^-$, $\Psi^+ \otimes \psi^-$, $\Psi^- \otimes \psi^+$	$\alpha_{45}\alpha_{45}$, $\alpha_{\overline{45}}\alpha_{\overline{45}}$, $\beta_{45}\beta_{45}$, $\beta_{\overline{45}}\beta_{\overline{45}}$, $\delta_{45}\delta_{45}$, $\delta_{\overline{45}}\delta_{\overline{45}}$, $\gamma_{45}\gamma_{45}$, $\gamma_{\overline{45}}\gamma_{\overline{45}}$
$\Phi^- \otimes \phi^+$, $\Phi^+ \otimes \phi^-$	$\alpha_{45}\alpha_{\overline{45}}$, $\beta_{45}\beta_{\overline{45}}$, $\delta_{45}\delta_{\overline{45}}$, $\gamma_{45}\gamma_{\overline{45}}$
$\Psi^+ \otimes \phi^+$, $\Phi^+ \otimes \psi^-$	$\alpha_{45}\delta_{45}$, $\alpha_{\overline{45}}\delta_{\overline{45}}$, $\beta_{45}\gamma_{45}$, $\beta_{\overline{45}}\gamma_{\overline{45}}$
$\Psi^- \otimes \phi^+$, $\Phi^+ \otimes \psi^+$	$\alpha_{45}\gamma_{45}$, $\alpha_{\overline{45}}\gamma_{\overline{45}}$, $\beta_{45}\delta_{45}$, $\beta_{\overline{45}}\delta_{\overline{45}}$
$\Psi^+ \otimes \phi^-$, $\Phi^- \otimes \psi^-$	$\alpha_{45}\delta_{\overline{45}}$, $\alpha_{\overline{45}}\delta_{45}$, $\beta_{45}\gamma_{\overline{45}}$, $\beta_{\overline{45}}\gamma_{45}$
$\Psi^- \otimes \phi^-$, $\Phi^- \otimes \psi^+$	$\alpha_{45}\gamma_{\overline{45}}$, $\alpha_{\overline{45}}\gamma_{45}$, $\beta_{45}\delta_{\overline{45}}$, $\beta_{\overline{45}}\delta_{45}$
$\Psi^- \otimes \psi^-$, $\Psi^+ \otimes \psi^+$	$\alpha_{45}\beta_{45}$, $\alpha_{\overline{45}}\beta_{\overline{45}}$, $\delta_{45}\gamma_{45}$, $\delta_{\overline{45}}\gamma_{\overline{45}}$

Check all *12870* partitions into 8 groups $\rightarrow$ none work.

Conclusion: **7 *is* the optimal with linear optics and projective measurements** (POVMs under consideration)

Bell-state analysis

Discriminate every Bell state in a single measurement

Necessary for dense-coding, quantum teleportation, etc.

- Impossible with Linear Optics -- only 3 of 4 Bell states discriminated: Dense-coding capacity = $\log_2(3) = 1.58$
- Probabilistic: 4 out of 4, but <u>at most</u> 50% efficient
- Photon-Photon interactions (e.g., upconversion)
  - –in principle 100%
  - –in practice 10^{-9}
- **Hyper-entanglement enhanced** Bell-State analysis: 100% efficient, 4 out of 4

Kwiat & Weinfurter, PRA **58**, R2623 (1998)

“Super-duper” Dense-Coding (LOCC)

	1 Degree of Freedom (polarization H/V or spatial modes h/v, etc)		2 Degrees of Freedom (H/V and h/v)
# of pairs / Det efficiency	One (η^2)	Two (η^4)	One (η^2)
Unbiased/uniform source	2 / 4	4 / 16	0 / 16
Biased source & photon-# detector	3	9	7
Biased source & NO photon-# detector	2	4	6

Conclusion: Hyperentanglement is superior if $\eta < \sqrt{7/9} = 88\%$

Hyper-Entanglement

PGK, JMO **44**, 2173 (1997)

- Photons simultaneously entangled in multiple DOFs:

$$\underbrace{(|H,H\rangle + |V,V\rangle)}_{polarization} \otimes \underbrace{(|rl\rangle + \alpha|gg\rangle + |lr\rangle)}_{spatial\ modes} \otimes \underbrace{\int_0^{E_p} dE A(E)|E\rangle_s|E_p - E\rangle_i}_{energy}$$

- Enlarged Hilbert space: $2 \otimes 2 \otimes m \otimes m \otimes n \otimes n$

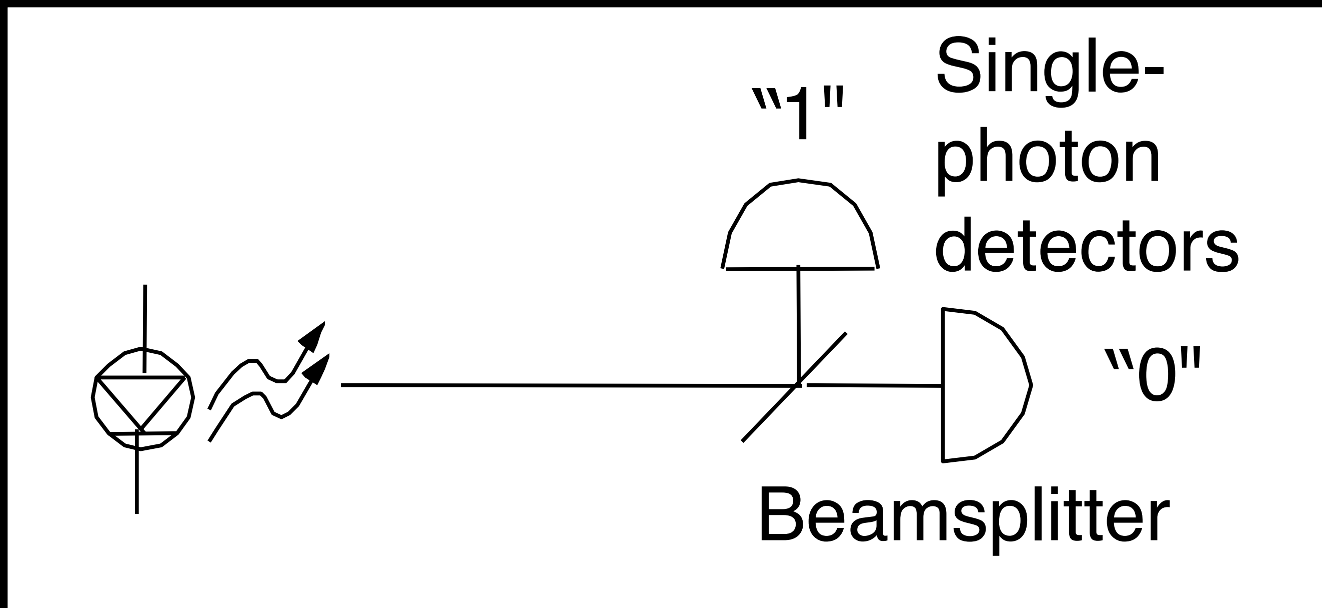
- Easy to perform quantum logic *between* DOFs

- New capabilities in quantum info. processing
  - remote preparation of entangled states
  - full Bell-state analysis
  - "super-duper" dense coding
  - quantum communication with higher alphabets
  - ???

Advantages of Entanglement

- **Automatic randomness of key**
- **Longer distances accessible (since Bob knows *when* to look for a photon) [But decoy states…]**
- **Established methods to verify security of key**
- **Source can be automatically verified (even if "sold" by Evesdropper!)**
- **Any leakage of info to other DOF**
  $\Rightarrow$ increased bit error rate (BER)

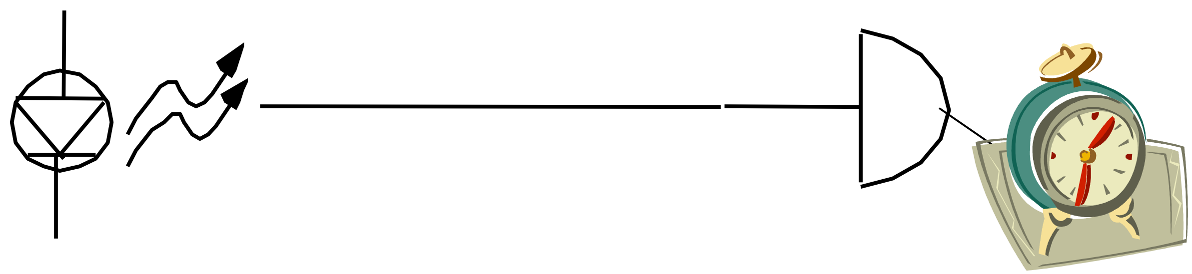
“Practical” Quantum Information: Random Number Generation



“Typical” optical random number generator:
Each photon detection gives a one or zero.
Limited by detector saturation rate (~MHz).

“Practical” Quantum Information: Random Number Generation

Time-based RNG



Measure precise time between detections.
1024 resolvable time bins ⇒10 bits/photon

Every detection gives ~10 random bits
(~8 bits after ‘whitening’)
Record to date: 20.4 Mbits/s
Data passes standard FIPS random number tests

Preliminaries: Dirac notation

$|H\rangle \equiv$ single photon polarized horizontally
$|V\rangle \equiv$ single photon polarized vertically

$|45\rangle \equiv$ single photon polarized at 45°
$|-45\rangle \equiv$ single photon polarized at -45°

Change of basis:

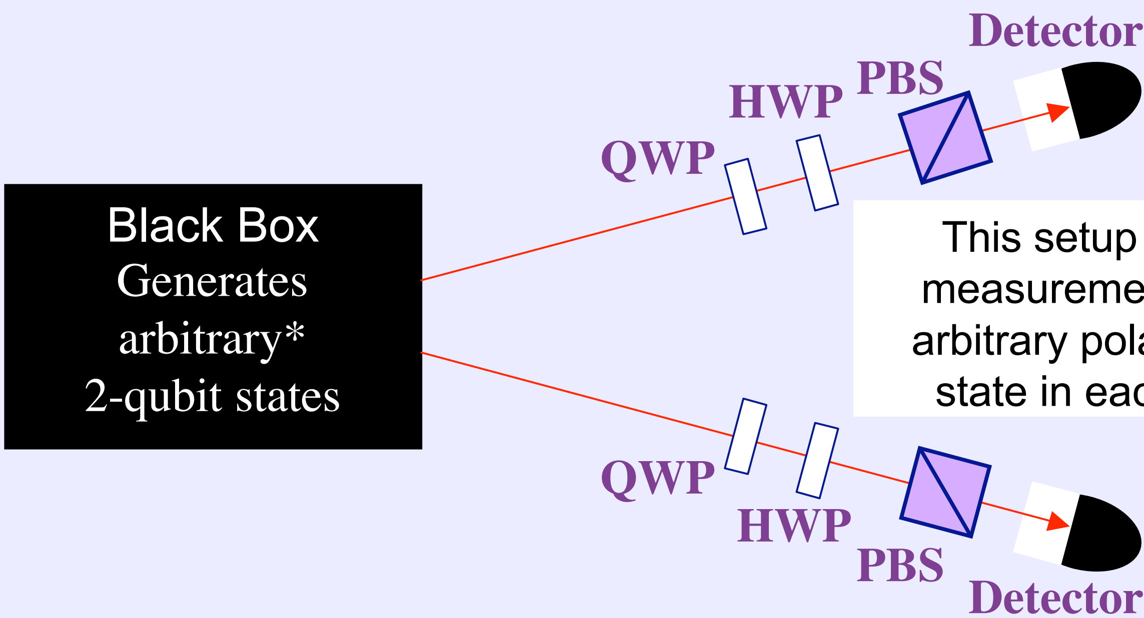
$$|45\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \qquad |-45\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} \qquad |H\rangle = \frac{|45\rangle + |-45\rangle}{\sqrt{2}} \qquad |V\rangle = \frac{|45\rangle - |-45\rangle}{\sqrt{2}}$$

Two photons:

$|H_1\rangle|H_2\rangle$ = a photon (traveling in direction #1)
and a photon (traveling in direction #2), both horizontally polarized

$|H_1\rangle\,|45_2\rangle$ = photon 2 is horizontally polarized, photon 2 is polarized at 45°

Quantum Tomography
of 2-Qubit Polarization States



This setup allows measurement of an arbitrary polarization state in each arm.

Any 2-qubit tomography requires 16 of these measurements.

Examples:

Arm 1	Arm 2
H	V
H	R
D	D

HH = 0.507
HV = 0.345
VH = 0.110

RD = 0.234
DH = 0.189

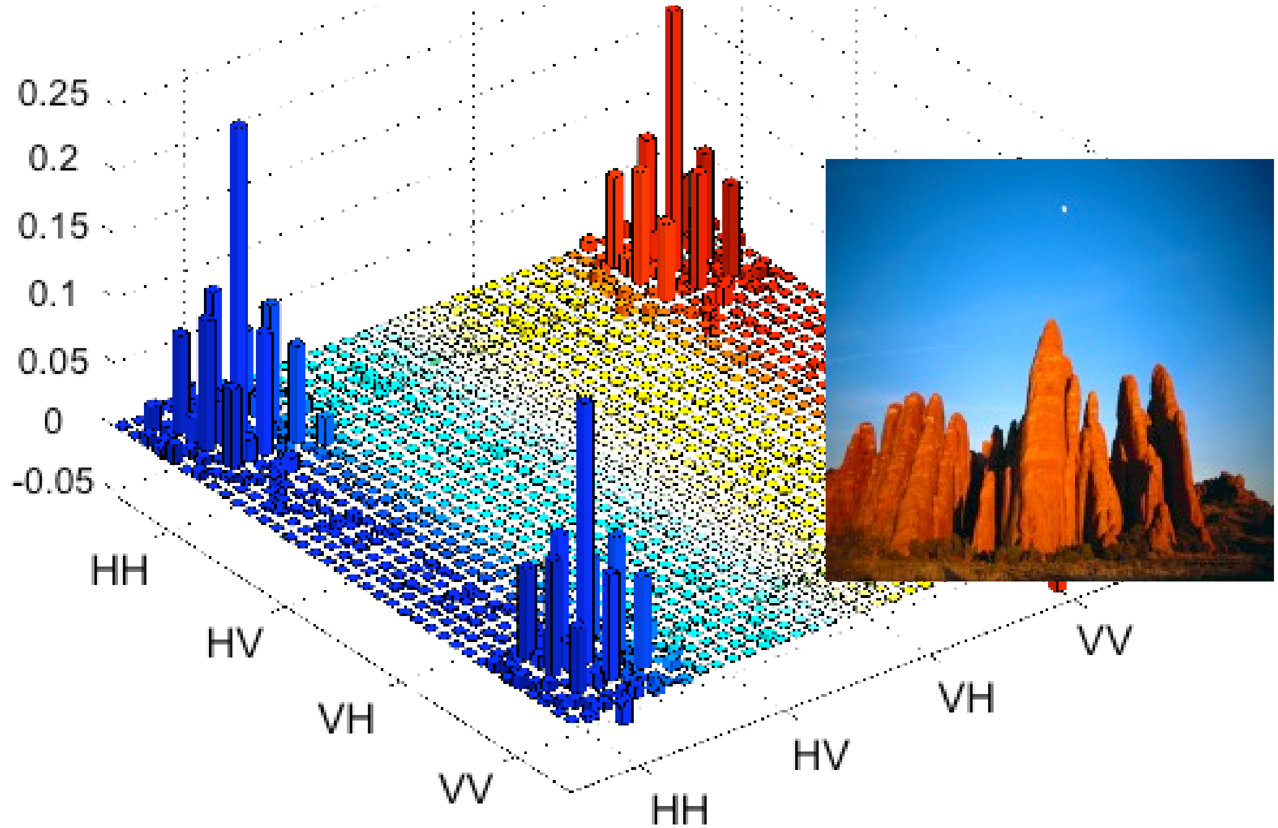
16 Precise Probabilities

→ **Maximum Likelihood Technique** → ρ **Precise Density Matrix**

- **Requires 16 measurements**
- **Gives most likely quantum state**

Qubit-qubit-qutrit-qutrit entanglement

$$|\psi\rangle \sim \left(\alpha|lr\rangle + \beta|gg\rangle + \alpha|lr\rangle\right) \otimes \left(|HH\rangle + |VV\rangle\right)$$



A 2⊗2⊗3⊗3 = 36 dim. Hilbert space!

"Space is big. Really REALLY **BIG**." HGTTG

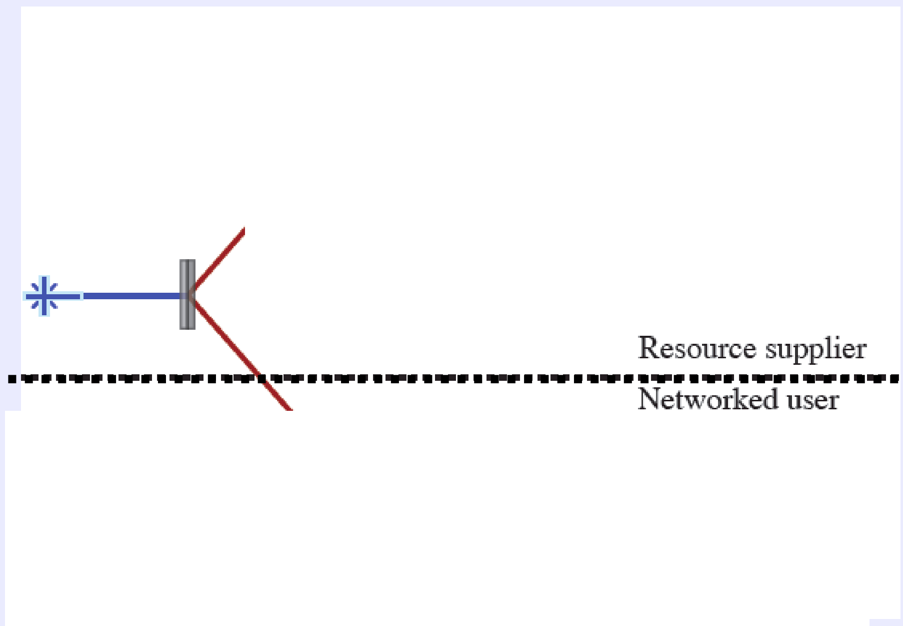
Application for Quantum Communication: **Remote State Preparation (RSP)**

C. H. Bennett et al., PRL **87**, 077902 (2001)

- Same resource requirements as teleportation ⇒ Alice and Bob share prior entanglement
- Alice makes a measurement ⇒ affects the state Bob receives
- Advantages over teleportation:
  - Potentially **simpler** because Alice knows what state she wants to send
  - Alice's preparation: Bell State Analysis **not** required
  - Bob's state retrieval: Only **one** bit of classical communication (vs. 2 bits)

Quantum Communication:
Remote *Entangled* State Preparation

Hyper-entangled resource: $(|H_{rp}H_t\rangle + |V_{rp}V_t\rangle) \otimes (|l_{rp}r_t\rangle + |r_{rp}l_t\rangle)$



Alice projects

$\cos\theta \, {}_t\langle Hr| + e^{-i\phi} \sin\theta \, {}_t\langle Vl|$

Bob gets

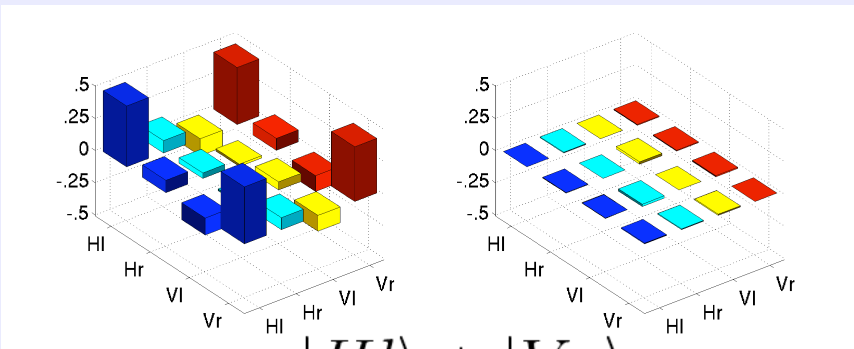
$\cos\theta |Hl\rangle_{rp} + e^{i\phi} \sin\theta |Vr\rangle_{rp}$

- Local entanglement between two degrees of freedom
- Single photon: 1 qubit in polarization and 1 qubit in orbital angular momentum

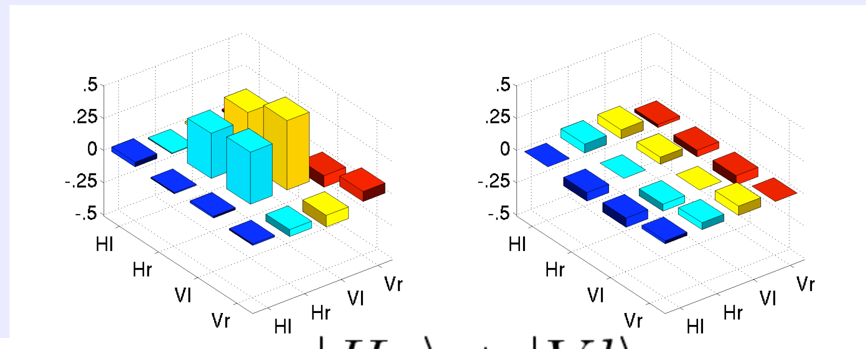
S. J. van Enk, PRA **72**, 064306 (2005)

Remote *Entangled* State Preparation:
Single-photon Bell States

Bob's state $\cos\theta|Hl\rangle_{rp} + e^{i\phi}\sin\theta|Vr\rangle_{rp}$



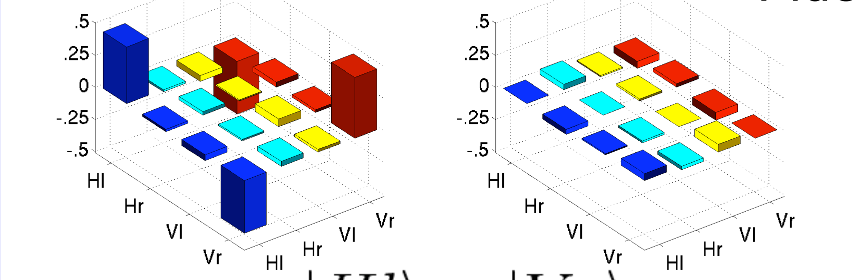
$|Hl\rangle + |Vr\rangle$



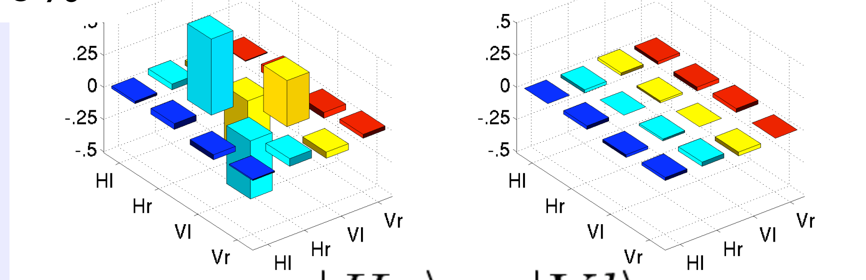
$|Hr\rangle + |Vl\rangle$

Tangle ~85%

Fidelity ~90%



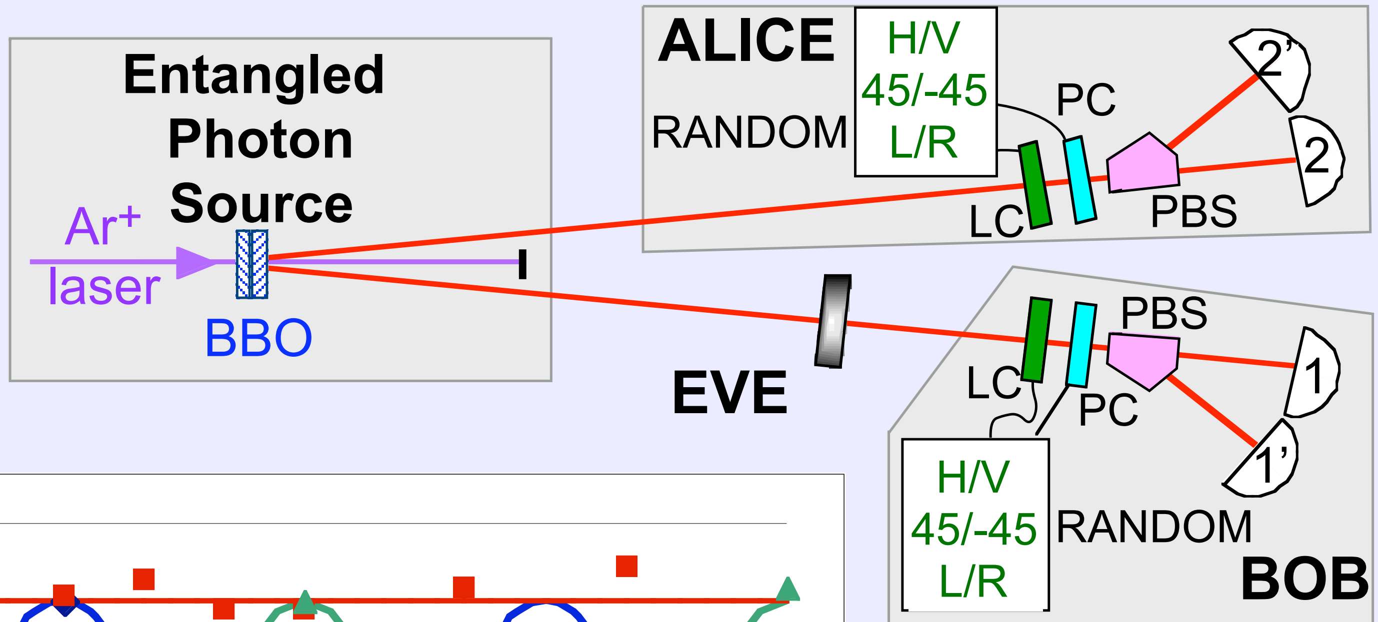
$|Hl\rangle - |Vr\rangle$

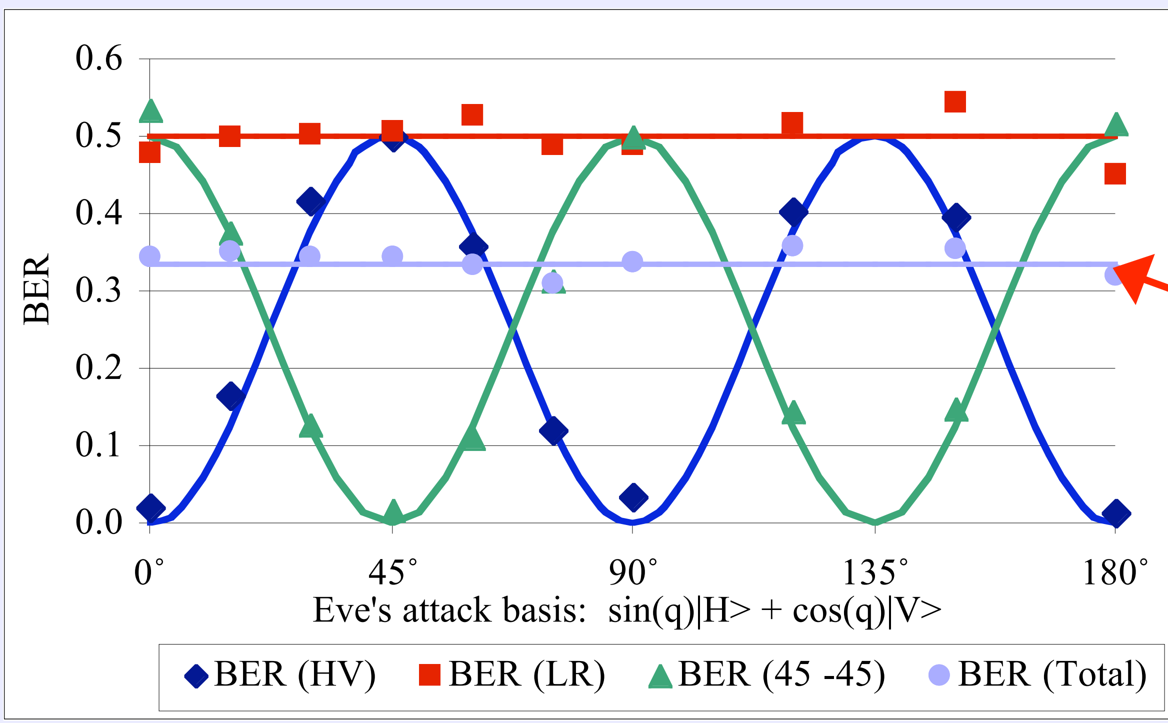


$|Hr\rangle - |Vl\rangle$

Experimental Realization of Six-State QKD Protocol

{D. Enzer et al., New Journal Physics **4**, 45.1 (2002)}





Total BER is 33%, independent of attack strategy

(c.f. 25% BER with 4-state protocol)