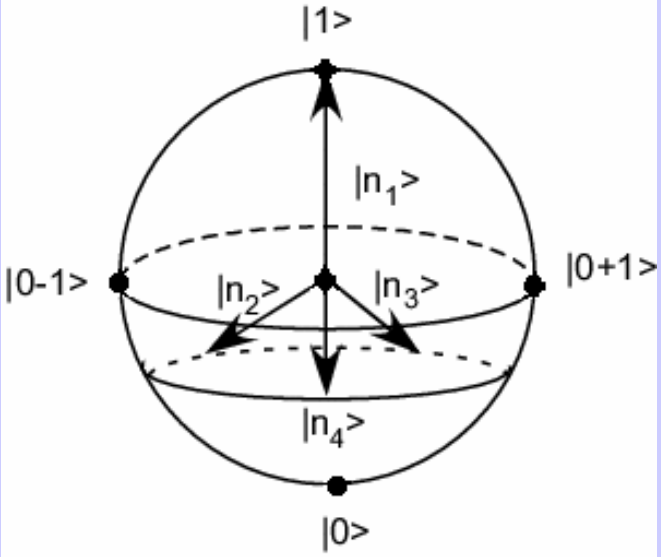
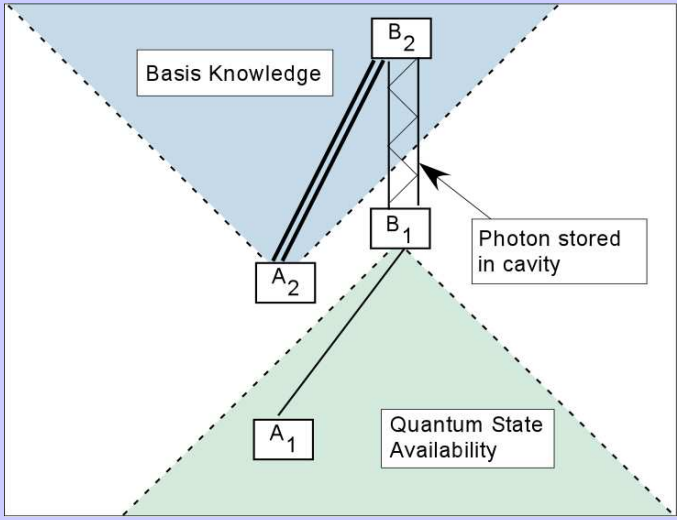
Quantum Communication via Entanglement:

Quantum Orienteering &

Relativistic Quantum Cryptography

Paul Kwiat





Outline

1. Quantum “Orienteering”
2. “Relativistic” Quantum Cryptography

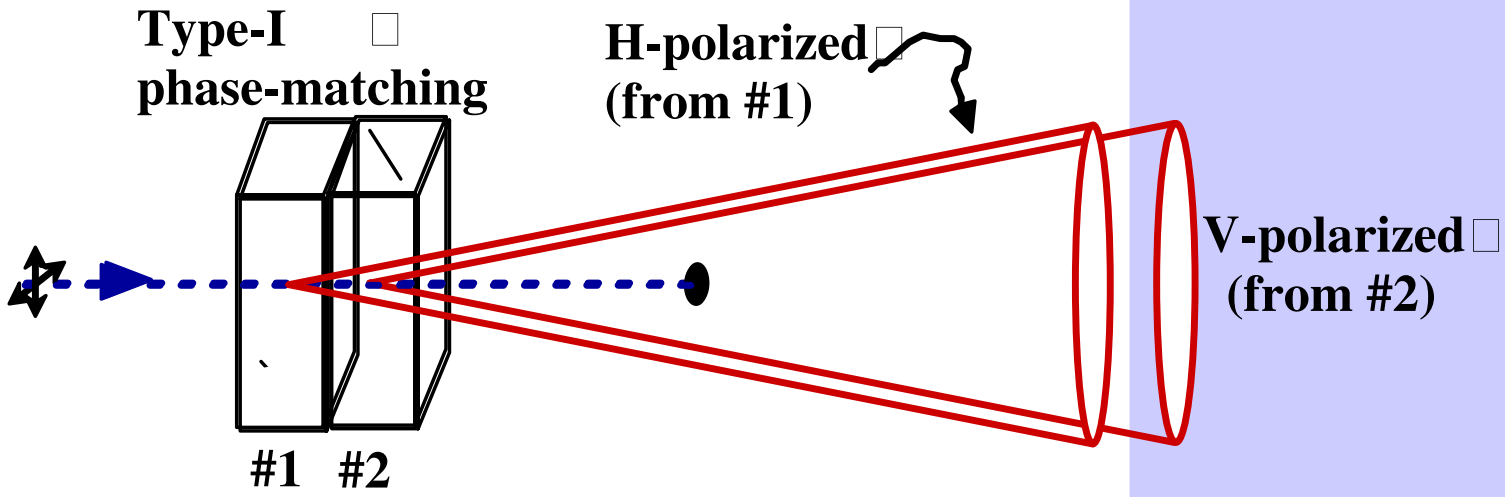
PGK Group

Graduate Students: Joe Altepeter, Julio Barreirro, Onur Hosten, Evan Jeffrey, Nicholas Peters, Radhika Rangarajan, Aaron VanDevender, Joseph Yasi

Undergraduates: Kyle Arnold, Gleb Akselrod, Rachel Hillmer, Kevin Uskali

Associated Theory Post-Doc: Tzu-Cheih Wei

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:

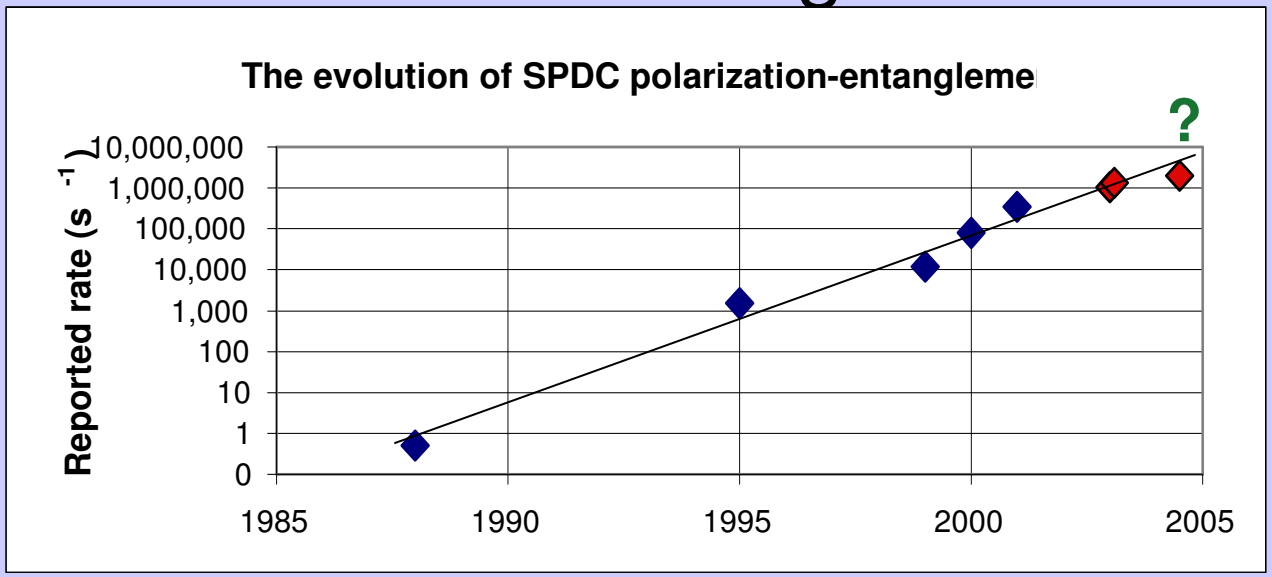
à **Nonmax. entangled states**

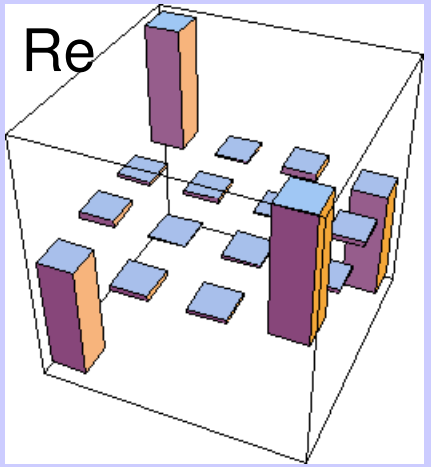
Add decoherence to arms

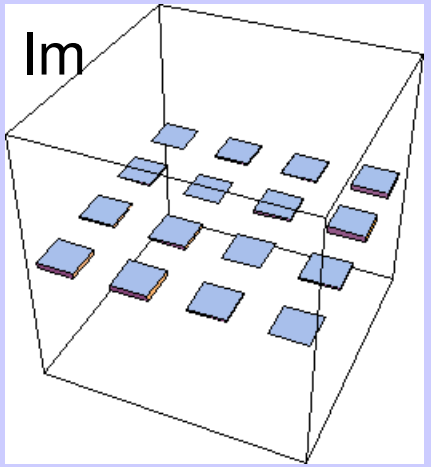
à **(Partially) mixed states**

Moore's law for entanglement

$\Phi^{(-)} \sim |HH\rangle - |VV\rangle$







We have observed polarization-entangled pairs @ 2,000,000 s^{-1}, with F ~98%!

Next main limitation: detector saturation

Bell-Ineq. Tests

New source: $|S_{expt}| = 2.7260 \pm 0.0008$ **(216σ in 0.8 s)**

($S_{LHV} \leq 2$) $|S_{expt}| = 2.7392 \pm 0.00008$ **(2417σ in 2 min)**

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

Bell test: $|S_{expt}| = 2.826 \pm 0.005$ **165σ**

(Total counting time = 10 s)

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

Classical Orienteering

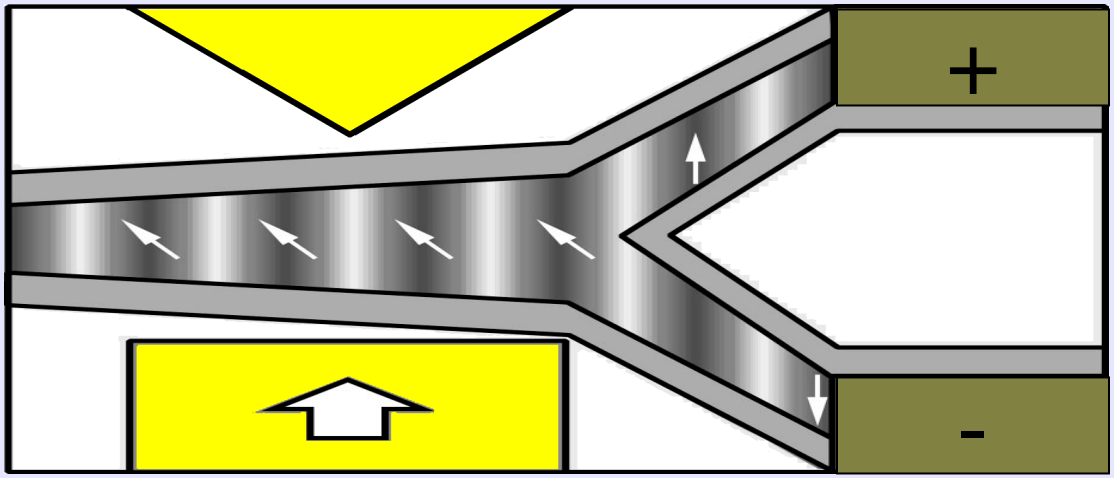
Directions can be transmitted classically by sending a spinning object.

The indicated direction can be measured to arbitrary precision.

Quantum Orienteering

- Instead of gyroscopes, send individual spin-1/2 particles.
- Assume a particle is sent in direction $\hat{n}$.
- There is a finite amount of information that can be extracted, depending on Bob's measurement.

Orienteering with a single spin



Measure in the z-basis

Guess “up” or “down” based on outcome

$\Rightarrow F_{1\ spin} = 2/3$ (1/2 without measurement)

Extendable to multiple state copies*:

For two spins, measure, e.g., z and x $\Rightarrow F_{LOCC} = 73.6\%$

*Massar, PRA **62**, 040101 (2000)

Orienteering with 2 identical spins

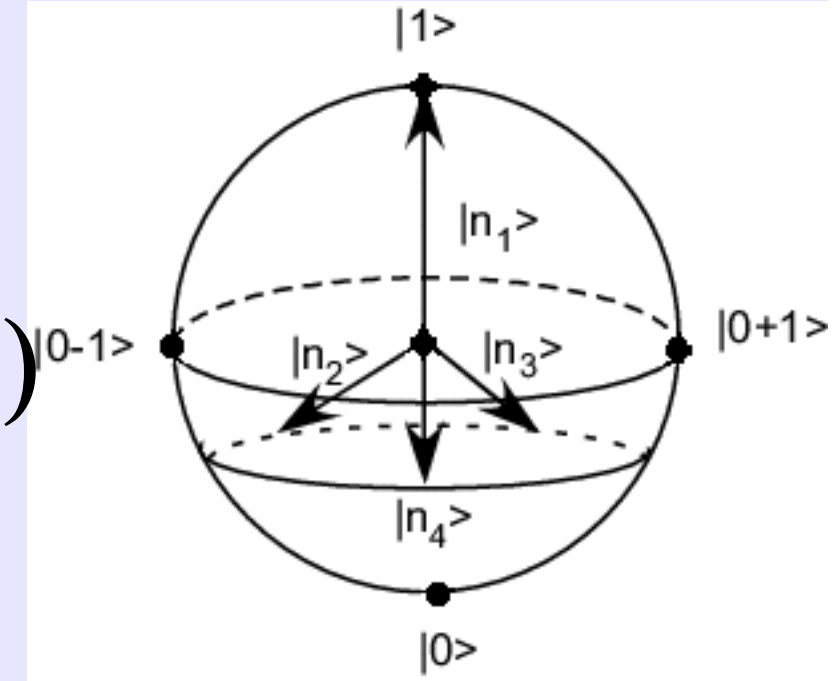
For 2 or more spins, *local* measurements are <u>not</u> optimal.

If Alice sends two *identical* spins $|\hat{n},\hat{n}\rangle$ the best measurements* have eigenvectors:

$$|\psi_k\rangle = \frac{\sqrt{3}}{2}|\hat{n}_k,\hat{n}_k\rangle + \frac{1}{2}|\psi^{(-)}\rangle$$

$$|\psi^{(-)}\rangle \equiv \frac{1}{\sqrt{2}}\left(|\hat{n}_k,-\hat{n}_k\rangle - |-\hat{n}_k,\hat{n}_k\rangle\right)$$

$\Rightarrow$ F = 3/4



(For *N* qubits: $F = \frac{N+1}{N+2}$)

*Massar & Popescu, PRL **74**, 1259 (1995)

Optimal orienteering with 2 spins

Surprisingly, even this is not optimal*…

Alice should flip the second spin and transmit $|\hat{n}, -\hat{n}\rangle$

The optimal measurement states are then**:

$$|\psi_k\rangle = \frac{\sqrt{3}}{2}\frac{|\hat{n}_k, -\hat{n}_k\rangle + |-\hat{n}_k, \hat{n}_k\rangle}{\sqrt{2}} + \frac{1}{2}|\psi^{(-)}\rangle$$

$\Rightarrow$ F = 0.789

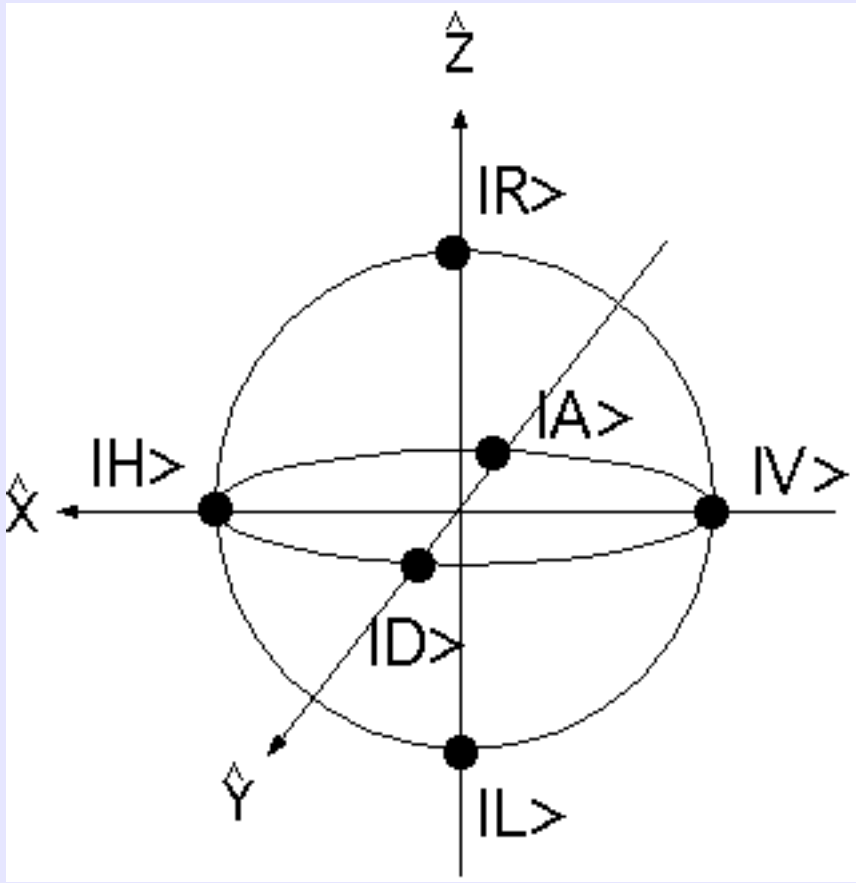
Why does it help to use anti-parallel spins? They reside in the full Hilbert space, i.e., singlet and triplet; the state $|\hat{n}, \hat{n}\rangle$ does not occupy the singlet sector of the space.

*Gisin & Popescu, PRL **83**, 432 (1999)

**Terry Rudolph, private comm.

Orienteering with photons

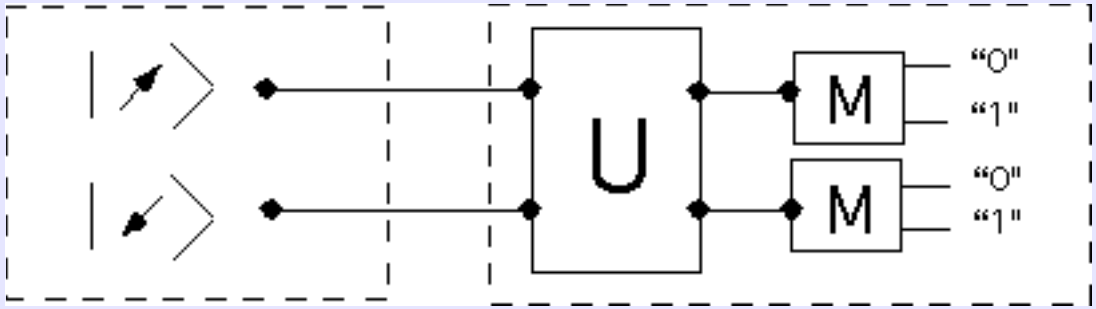
Photon polarization has no natural embedding in space. However, we can associate real-space directions with particular polarization states (directions on the Poincaré sphere).



Note: This requires using a shared reference frame.

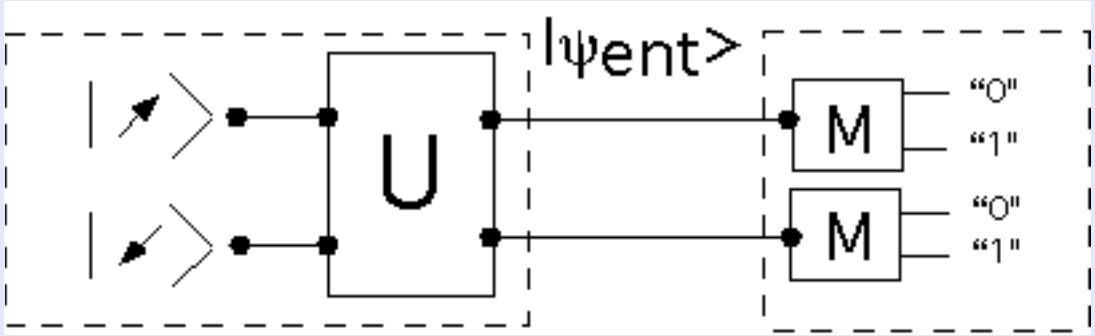
Also, we must be wary -- the operation of wave plates and polarizers are k-vector dependent.

Conceptual considerations



- States are simple to create
- Measurements are difficult (U is a 2-qubit gate)

Because we have a shared reference frame, we can "move" the transformation*:

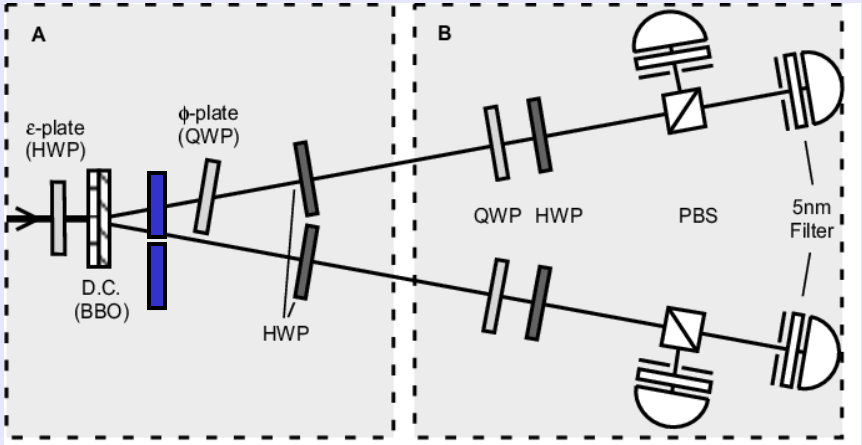


- Separable measurements are easy.
- Precise entangled state synthesis required.

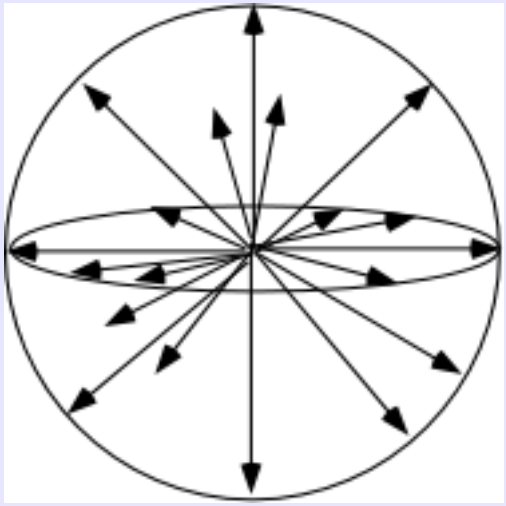
*T. Rudolph, private communication

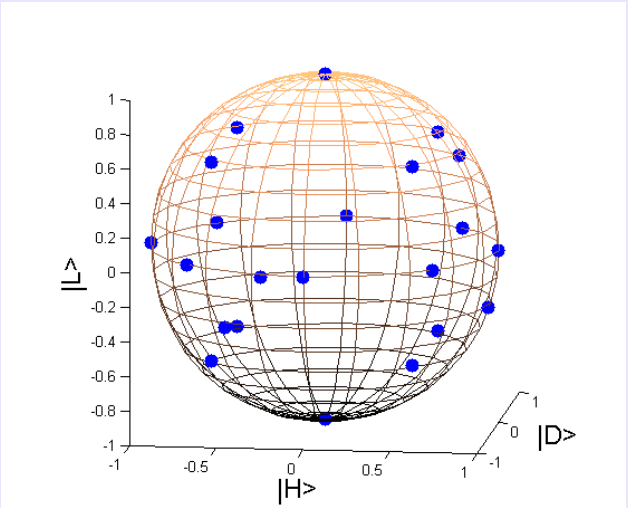
Experimental configuration

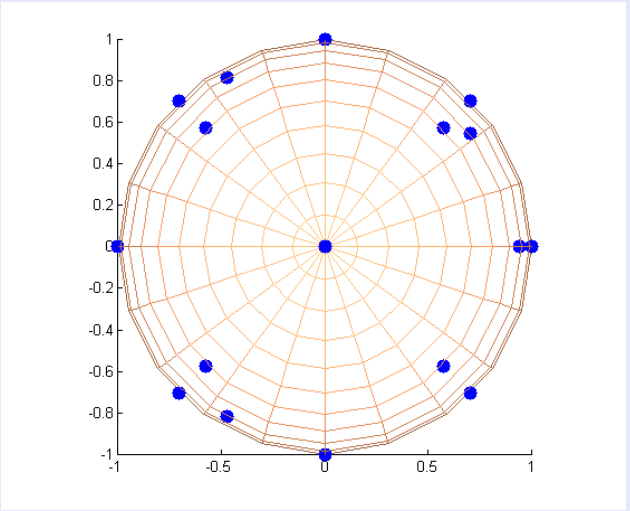
Alice can create a wide variety of entangled states; Bob can make arbitrary separable measurements.



Directions sent







All states had > 98% state fidelity with the target state

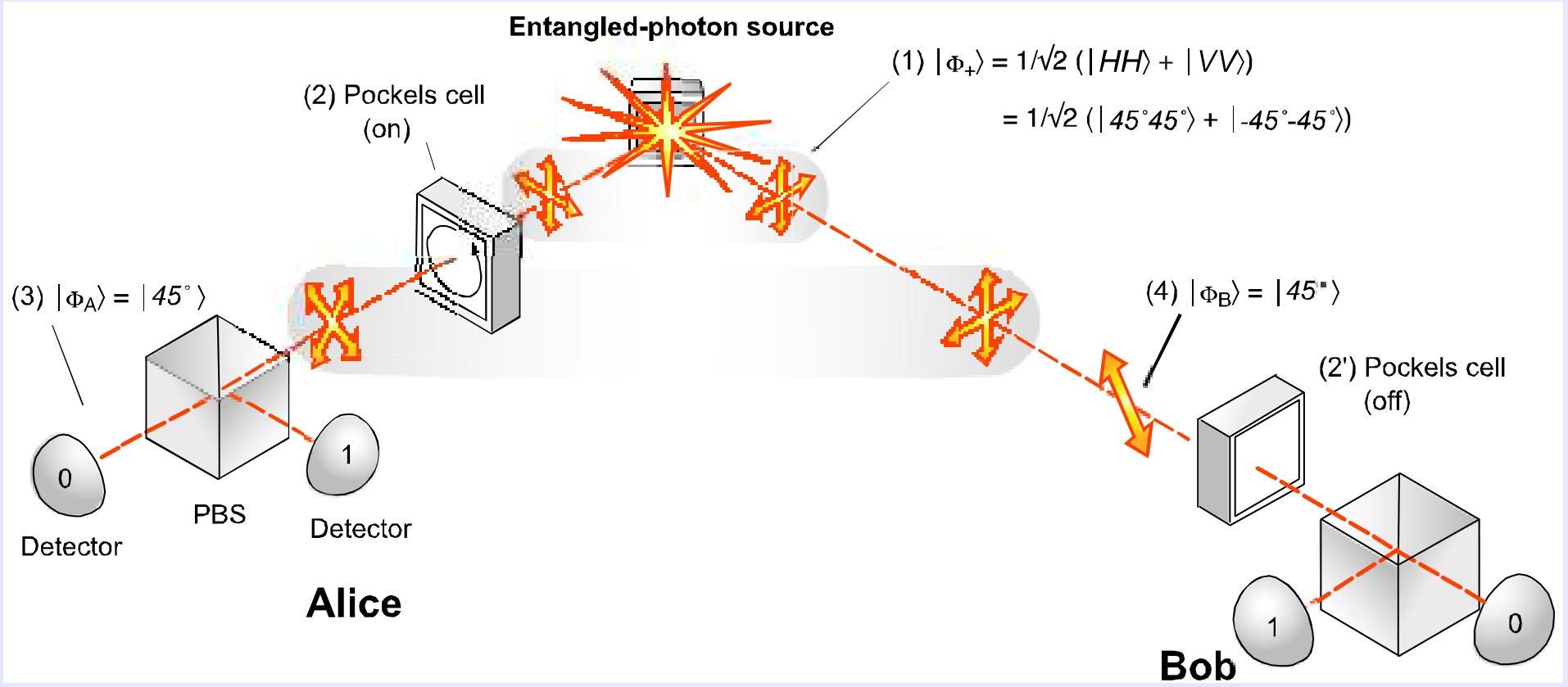
E. R. Jeffrey, J. B. Altepeter, M. Colci, and P. G. Kwiat, Phys. Rev. Lett. 96, 150503 (2006)

Summary of average fidelities

Direction set	Separable (Th/Exp)
all	73.6/73.2

• Because photon spin is not "pointing" in real space, Alice and Bob require a shared reference frame.

Entangled-Photon Quantum Cryptography



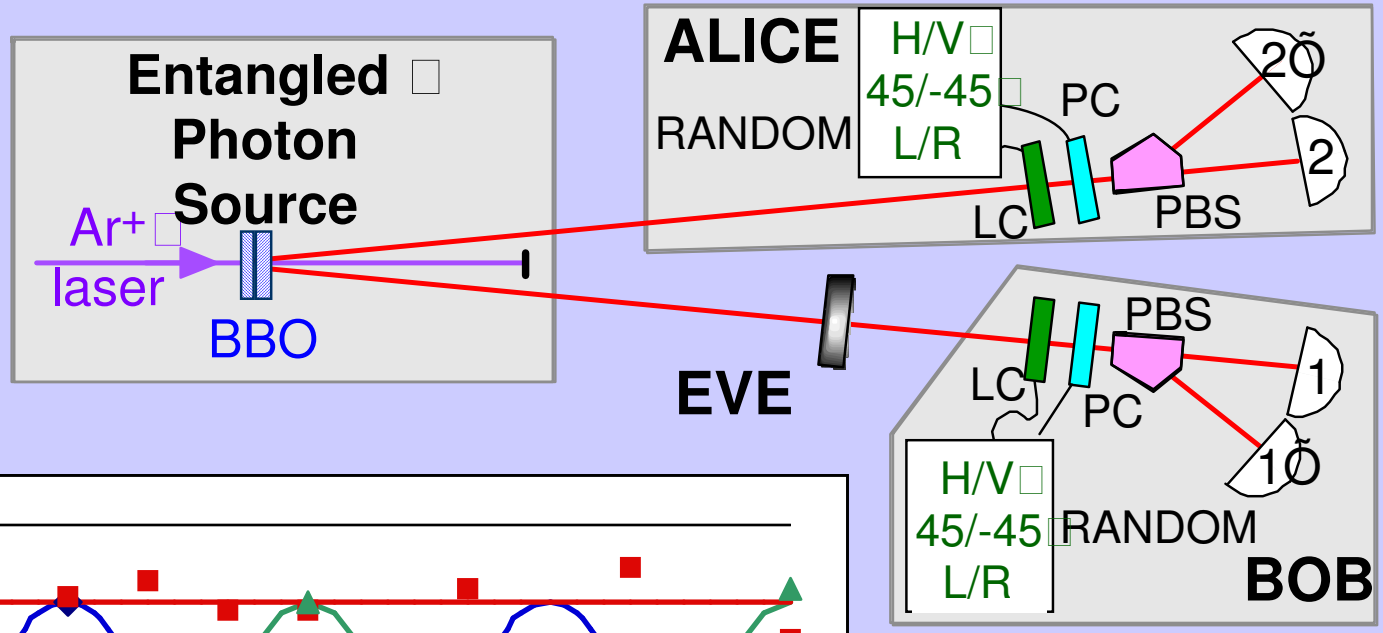
- Alice & Bob randomly measure polarization in the (HV) or the (45 45) basis.
- Discuss via a "public channel" which bases they used, *but not the results*.
- Discard cases (50%) where they used different bases à uncorrelated results.
- Keep cases where they used the same basis à *perfectly correlated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

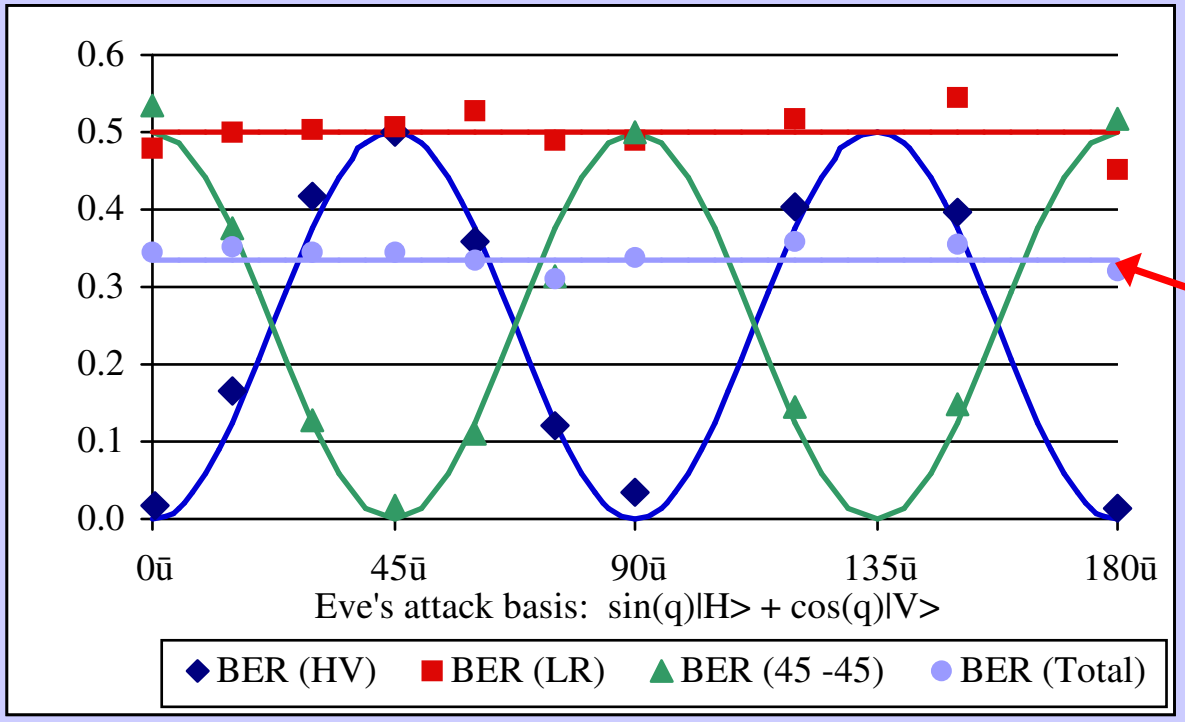
Advantages of Entanglement

- **In principle perfect correlations between Alice and Bob $\Rightarrow$ well, not really perfect…**
- **Automatic randomness of key**
- **Longer distances accessible (since Bob can know *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!)**

Experimental Realization of Six-State QKD Protocol

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

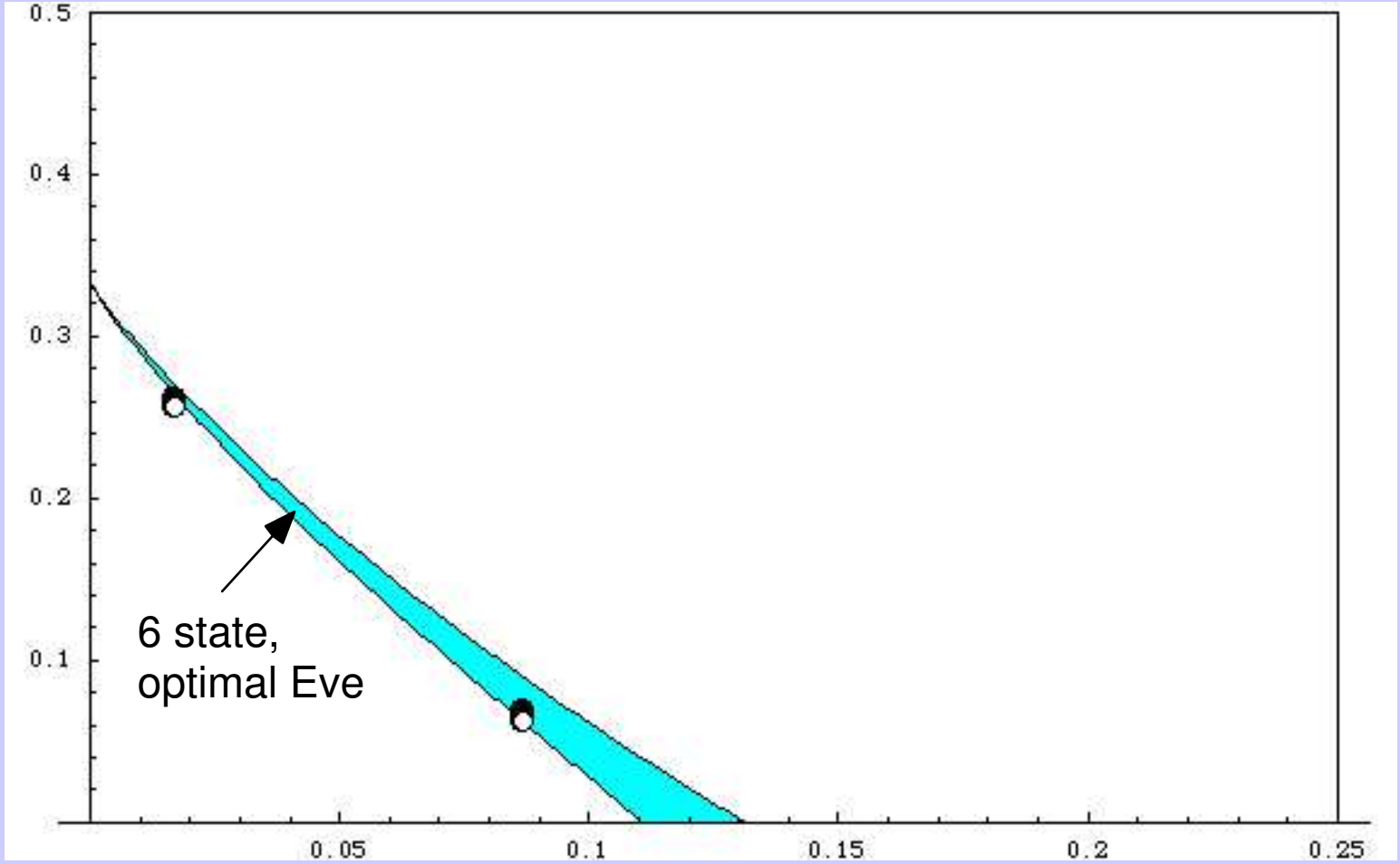




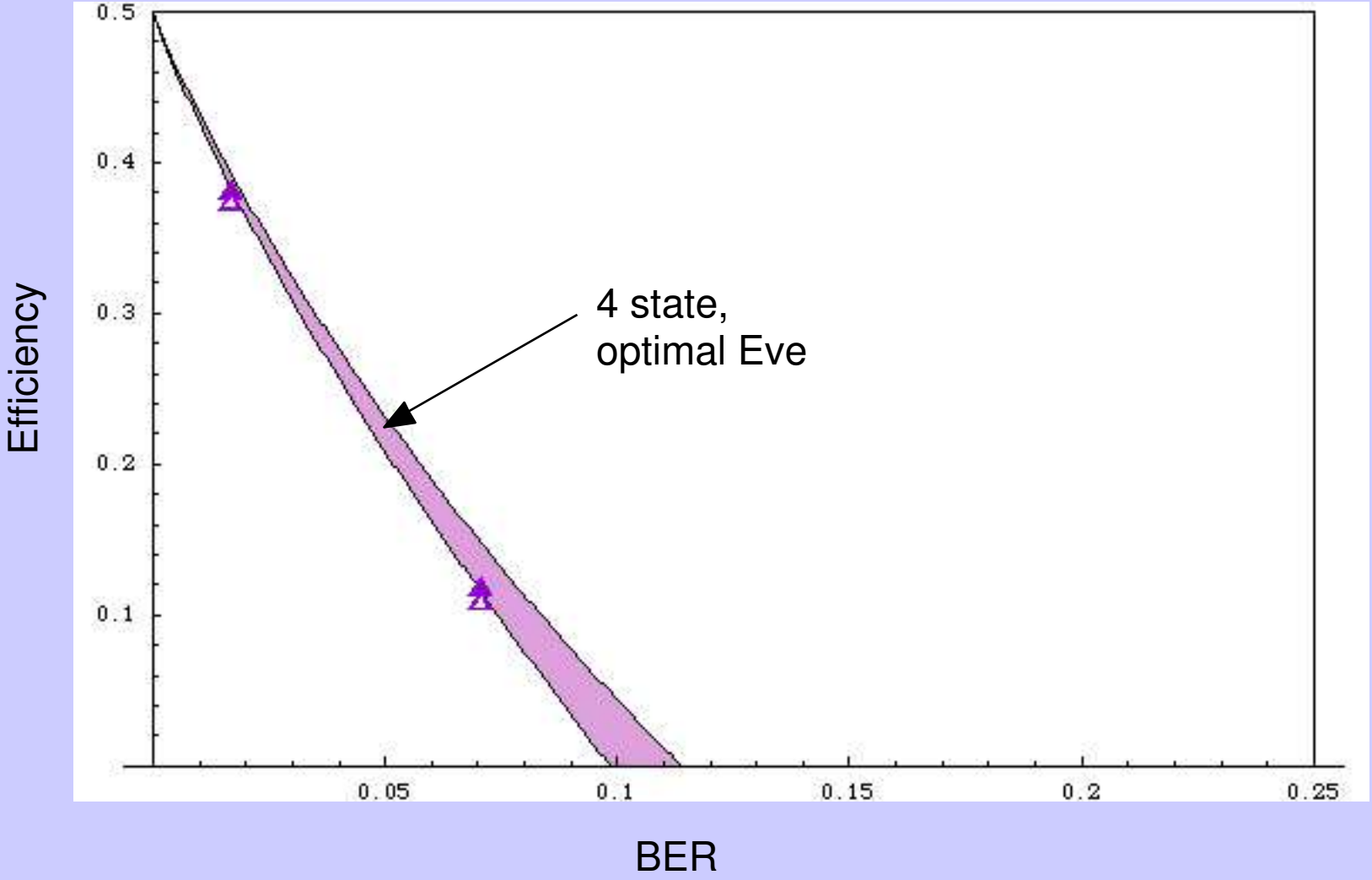
Total BER is 33%, independent of attack strategy

(c.f. to 25% BER in BB84 4-state protocol)

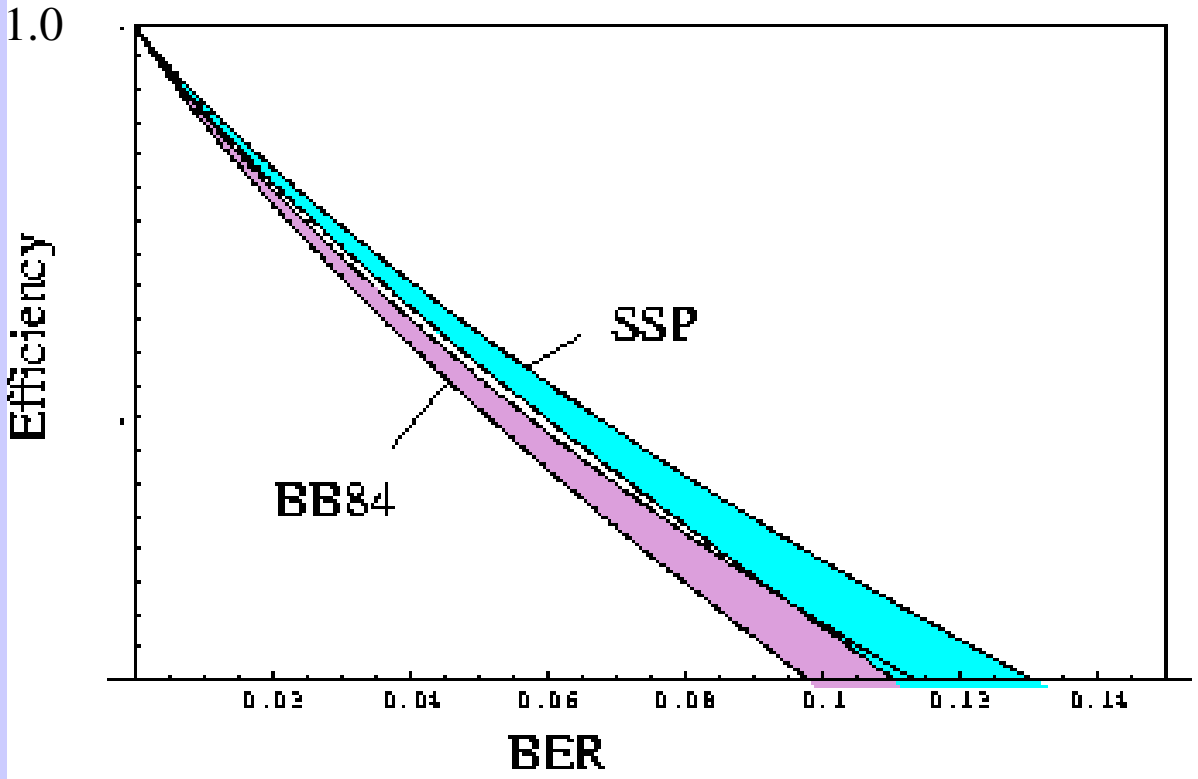
Bit yield, after Error Detection & Privacy Amplification



Bit yield, after Error Detection & Privacy Amplification



The Trouble with Sifting

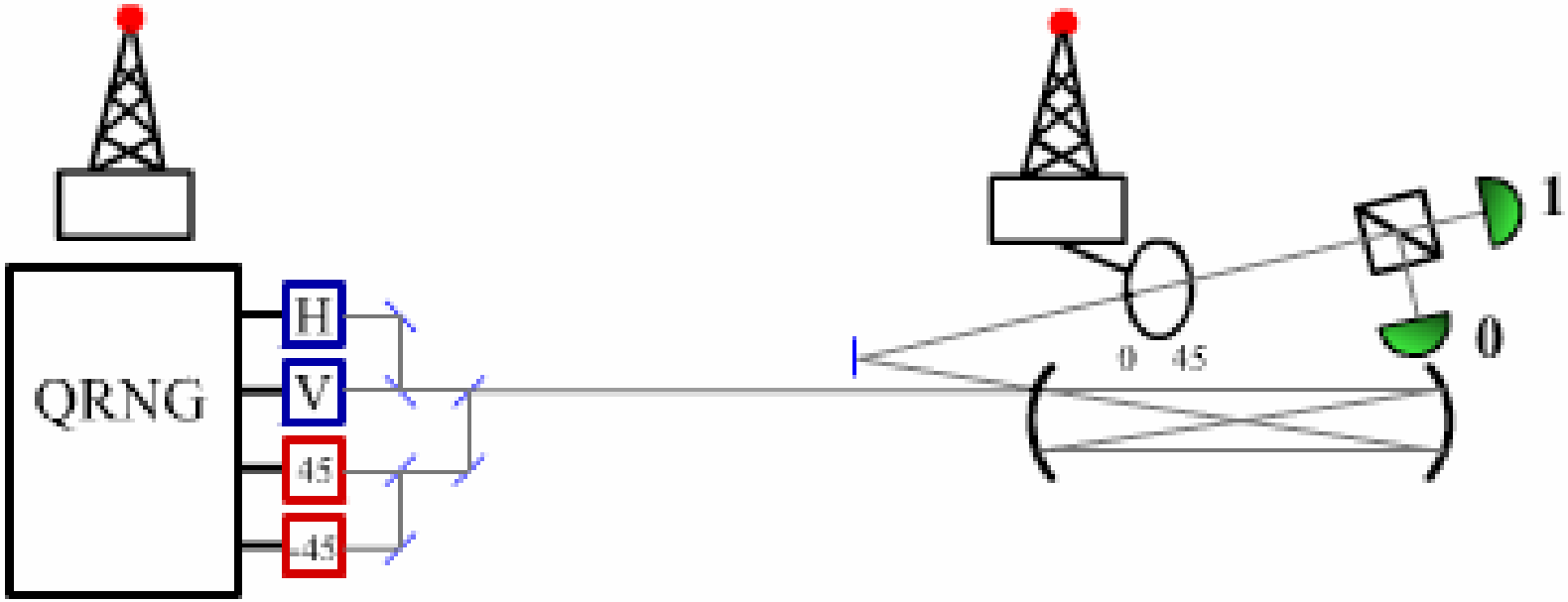


Eliminating the sifting $\Rightarrow$ double efficiency of BB84
$\Rightarrow$ triple efficiency of SSP

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

How can we eliminate sifting…

“Relativistic” Quantum Cryptography

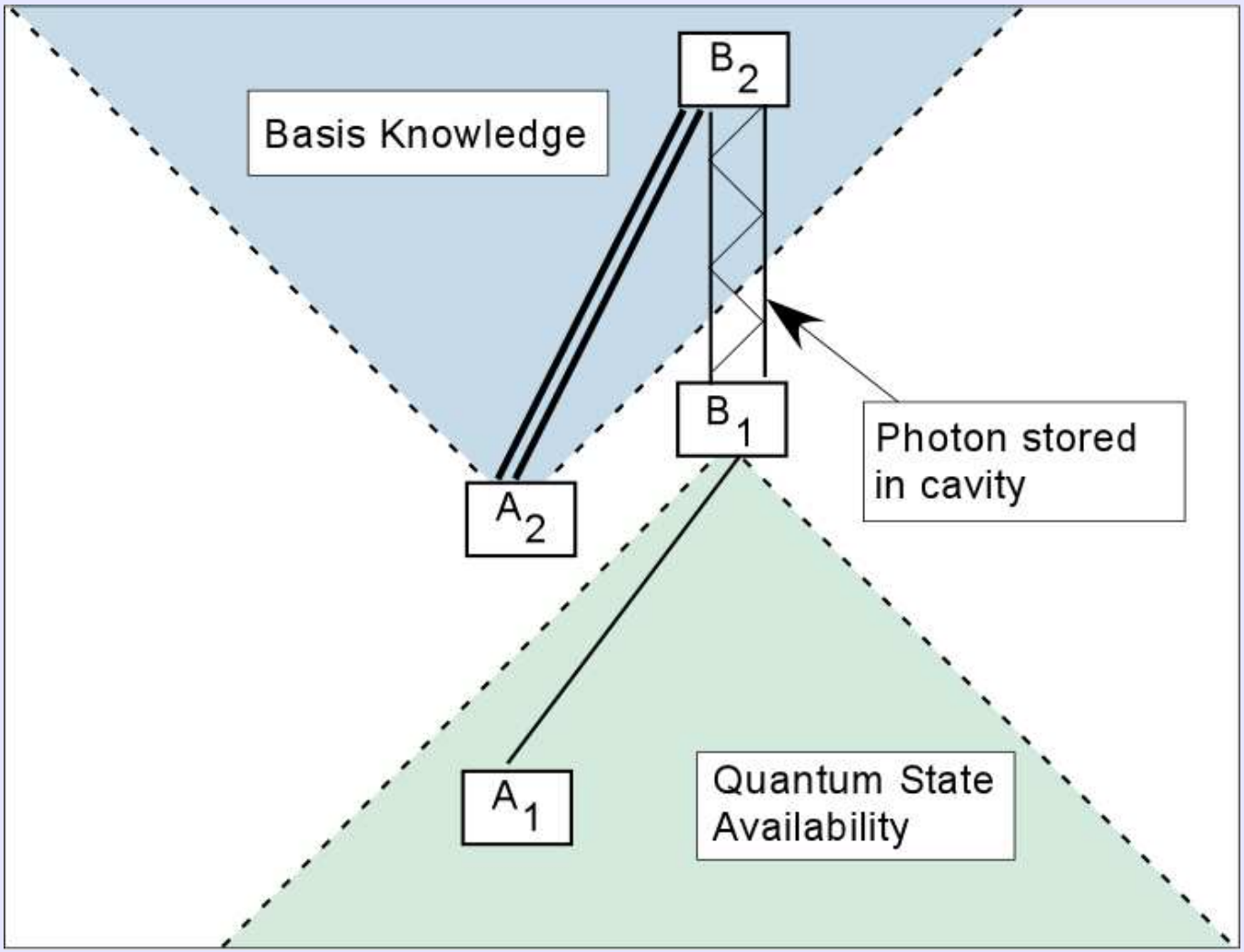


Bob stores each photon until Alice tells him which basis to use

à net efficiency is increased to 100% (in principle)

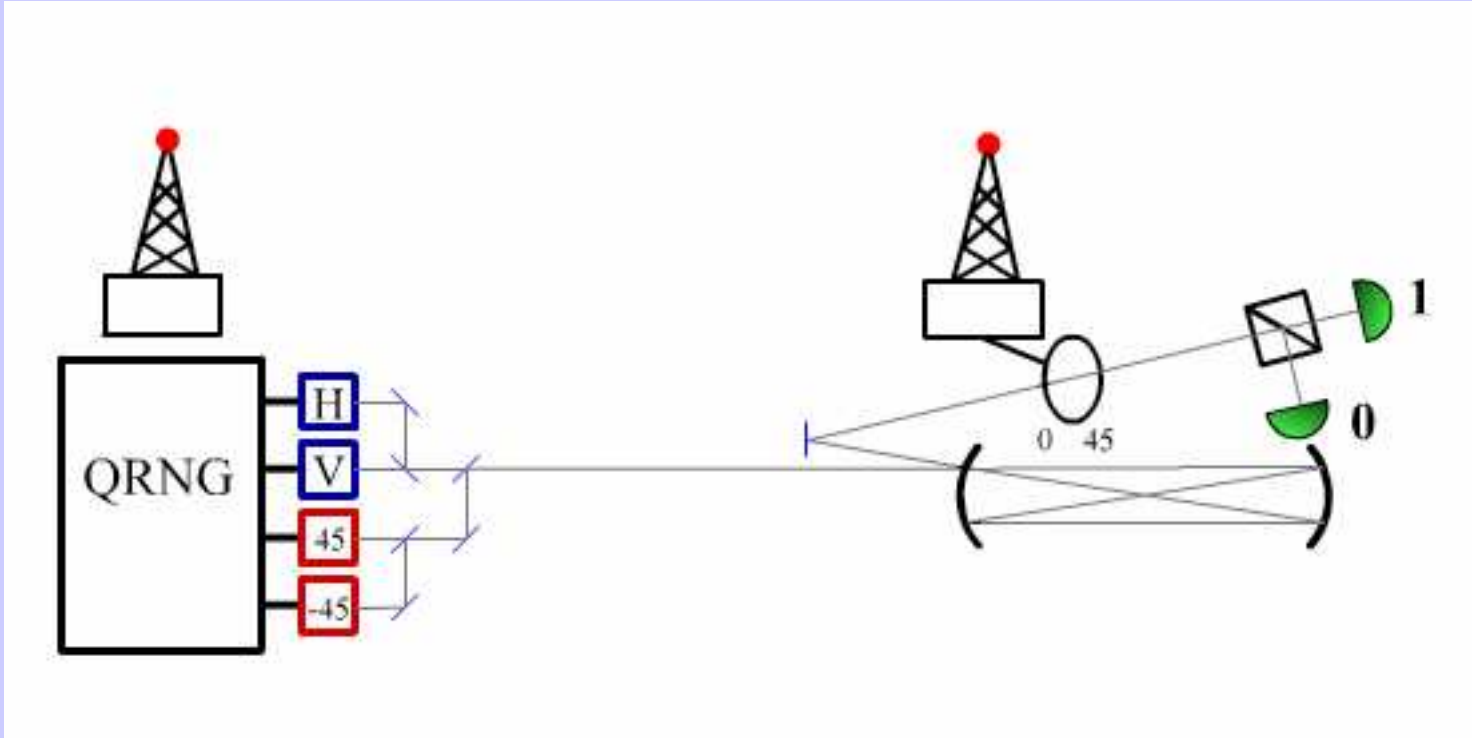
à same security as BB84 (Eve’s ρ cannot depend on Bob)

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

à fast classical modulation system

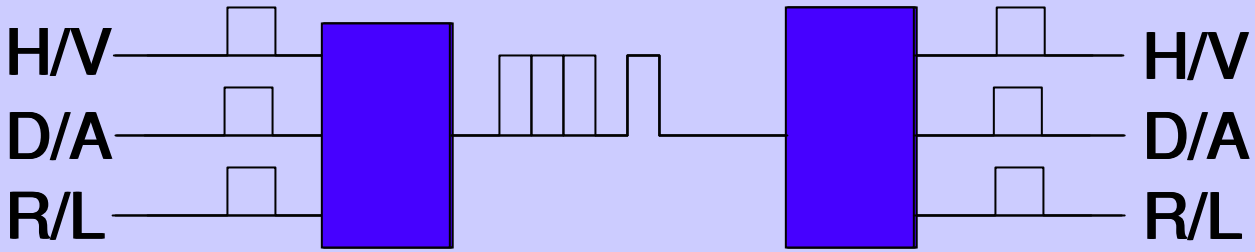
à quantum memory

à simpler 6-state analysis system

Modulation System

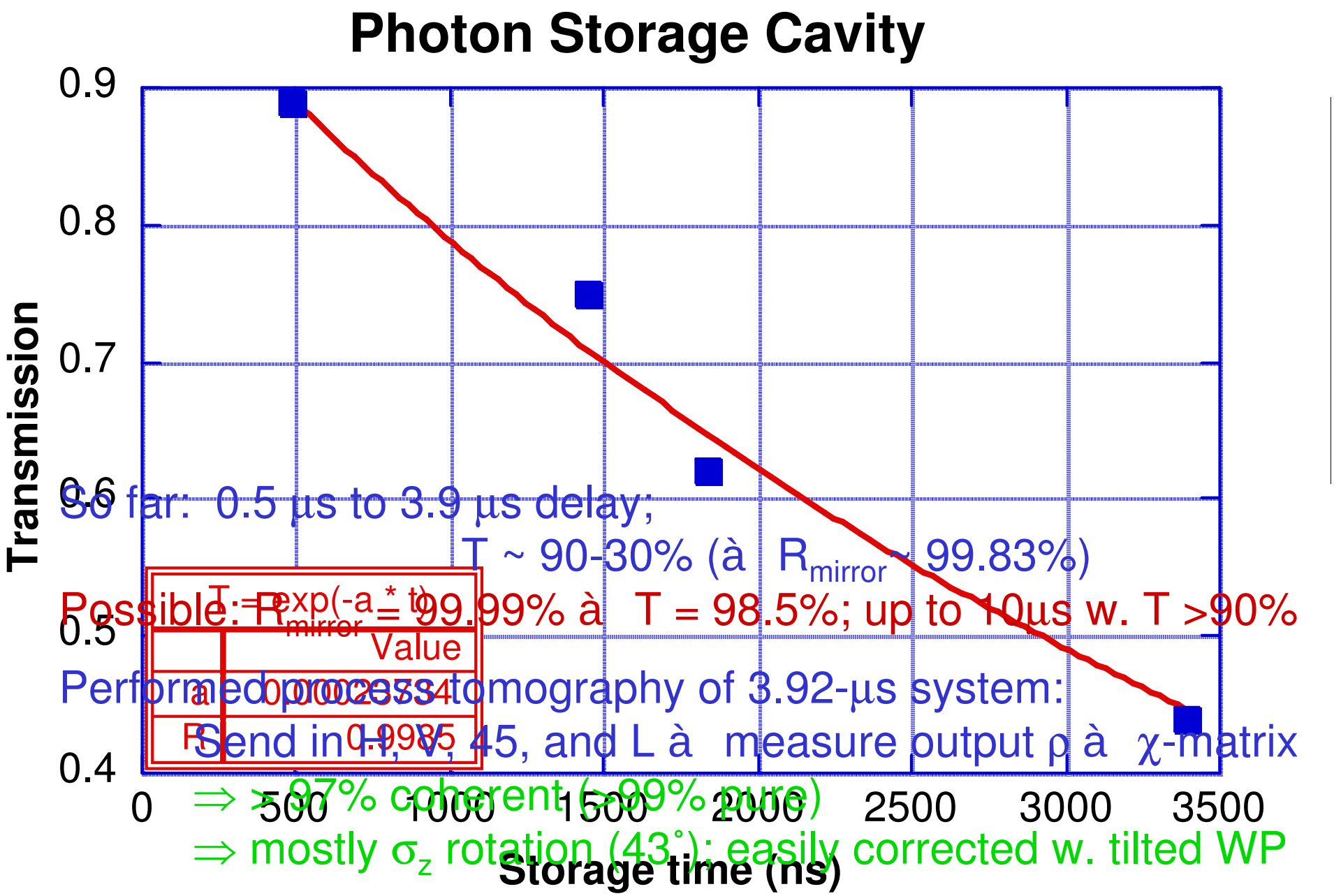
The classical basis information must be sent over a low-latency communication channel (since Bob can only store the photon for ~1 μs).

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



Clock rate = 80 MHz

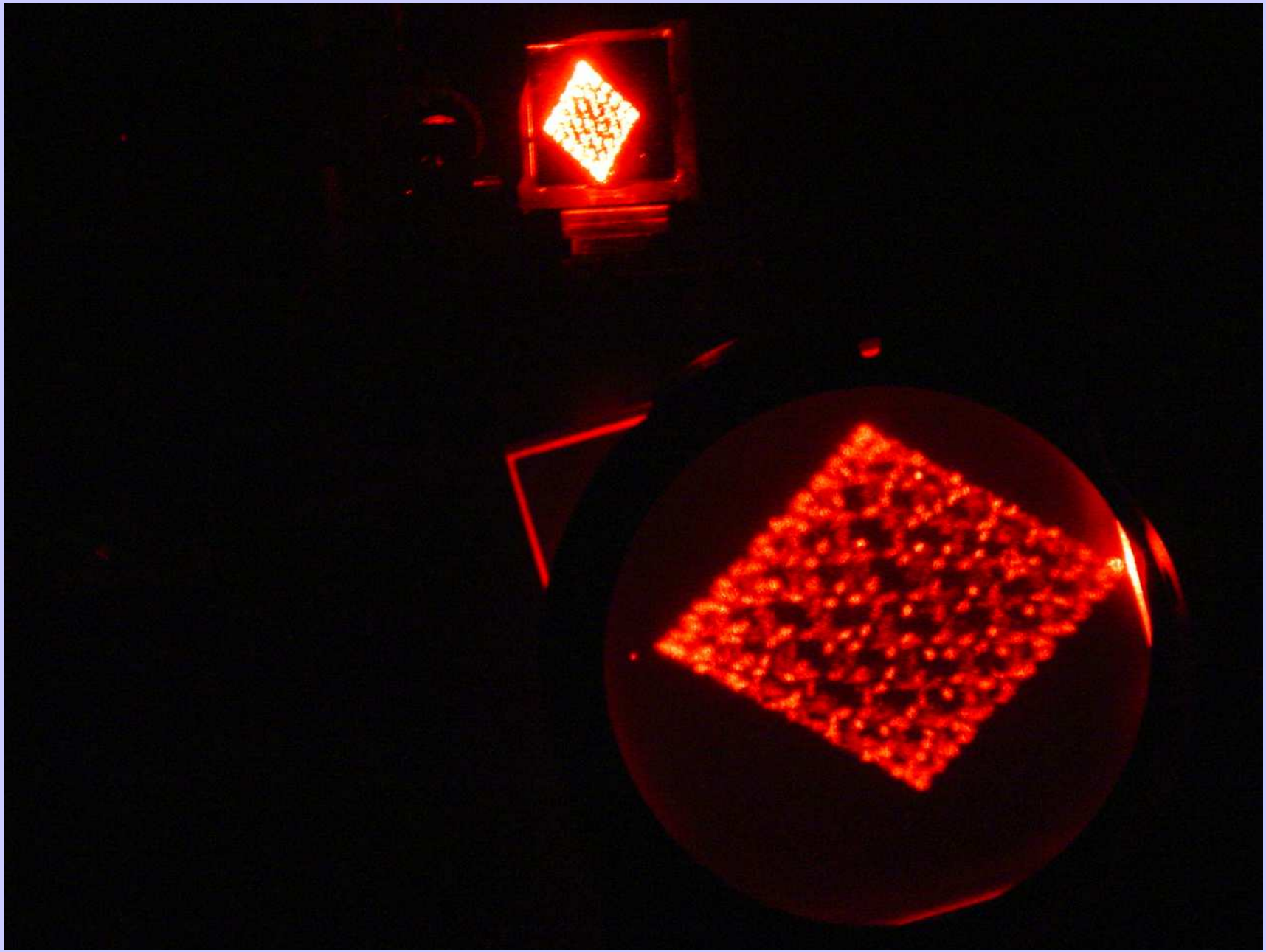
Total latency < 120 ns



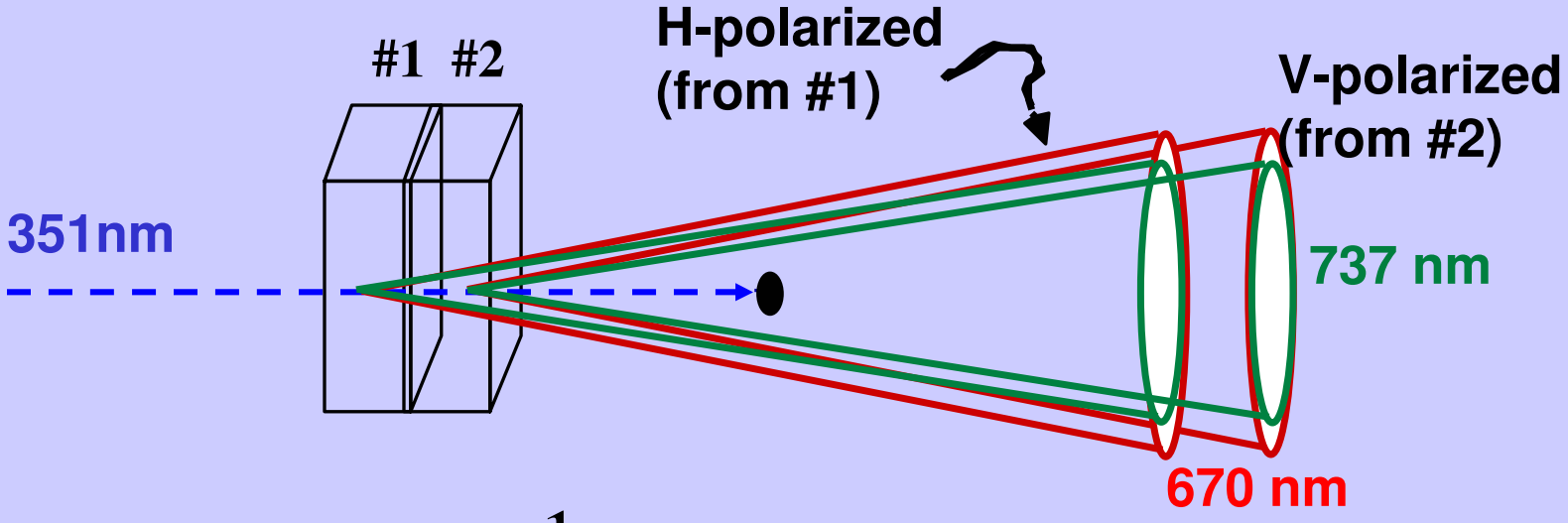
So far: 0.5 μs to 3.9 μs delay;
T ~ 90-30% (à R_{mirror} ~ 99.83%)

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

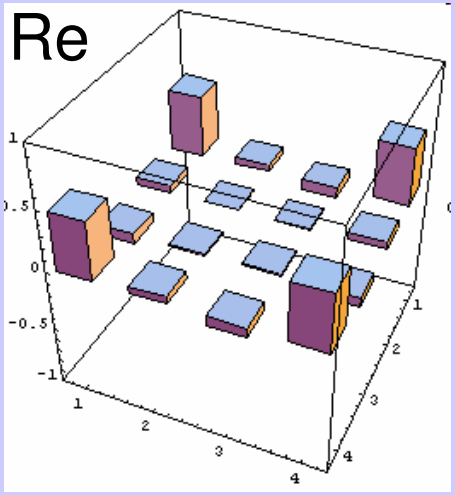
Performed process tomography of 3.92-μs system:
Send in H, V, 45, and L à measure output ρ à χ-matrix
⇒ >97% coherent (>99% pure)
⇒ mostly σ_z rotation (43°); easily corrected w. tilted WP

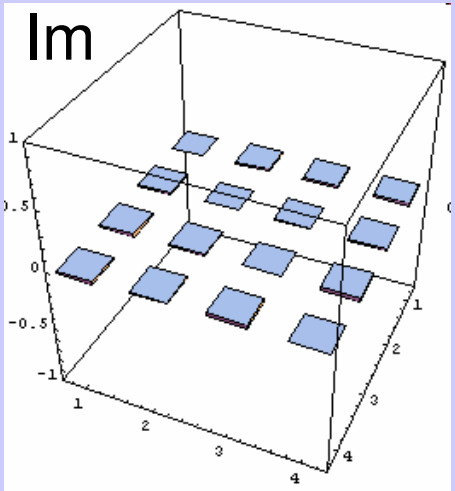


Non-degenerate Polarization-entanglement



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





$F_{\text{with HH+VV}} = 0.968$

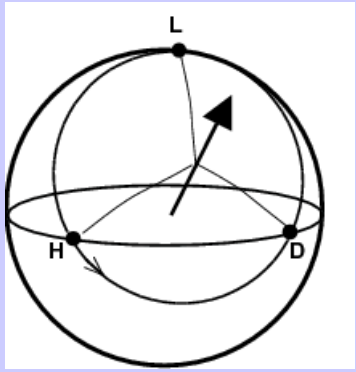
Linear entropy = 0.027

Tangle = 0.957

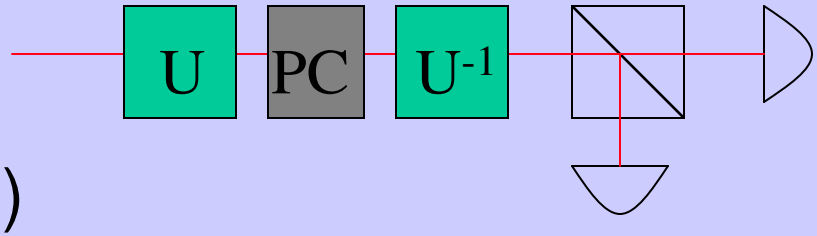
Six-State Polarization Analysis

- Measuring in three bases typically requires two electro-optic devices
- We desire a “Minimum parts-count analyzer”

Try rotating about the {1,1,1} axis on Poincaré sphere



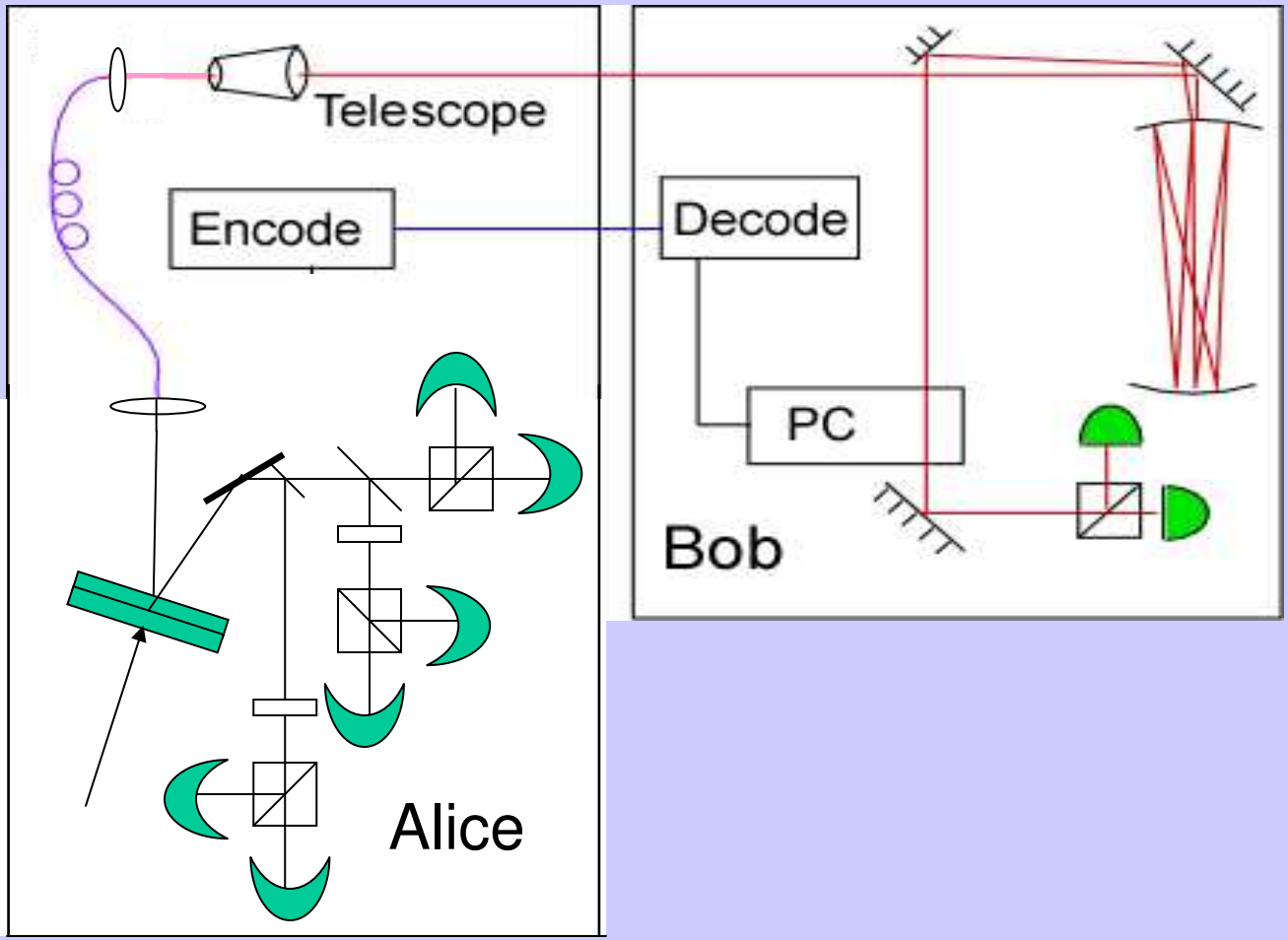
Use fixed waveplates plus one Pockels cell (with *three* voltages: 0, ±V)



In fact, because of polarization entanglement, Alice can set the bases by which measurements *she* uses (c.f., Remote State Preparation)

Incorporate *entangled* photon source

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

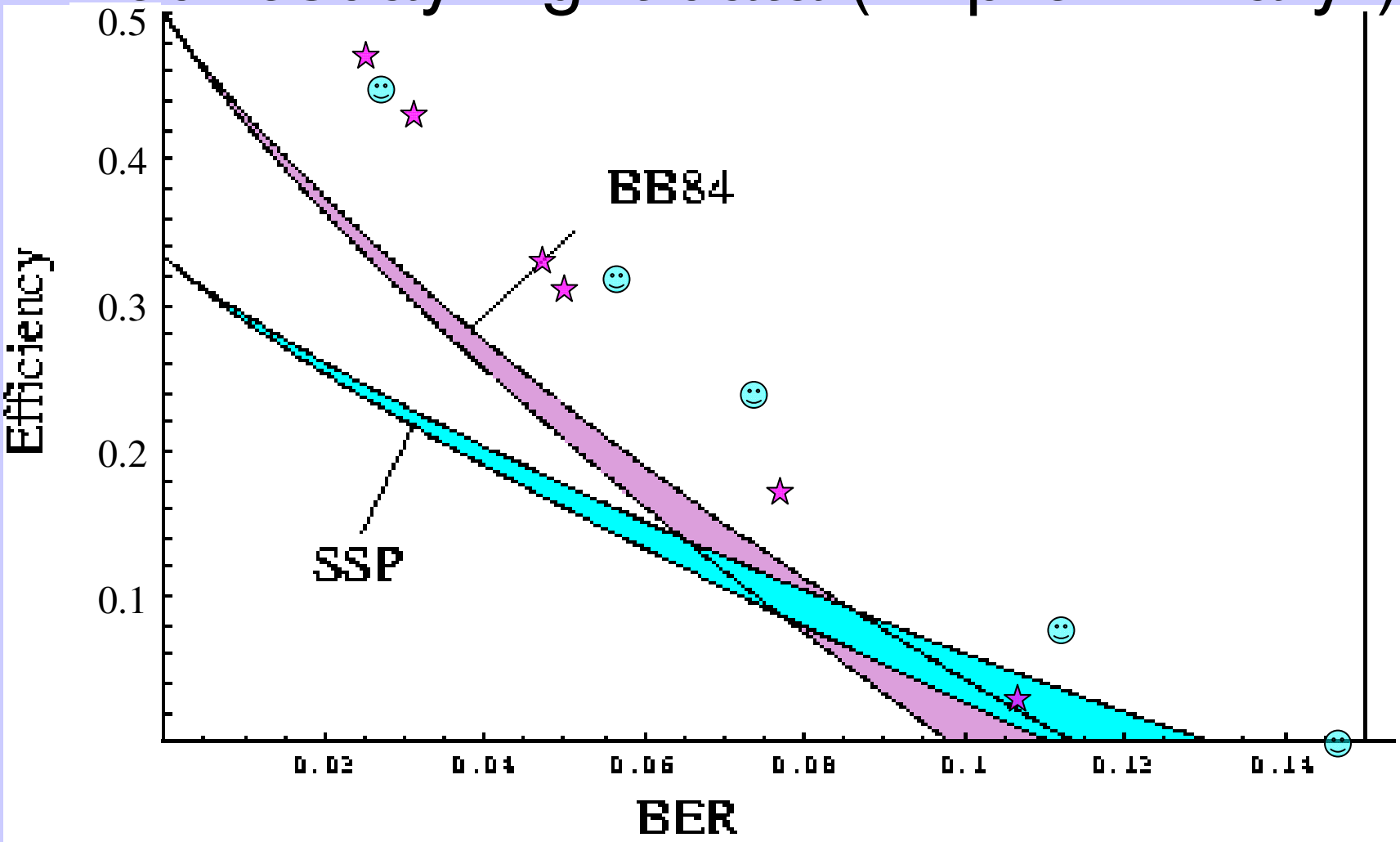


BB84, 30 mW pump power
94 sifted bits/second
2.5% error rate
→ 65.5 secret bits/second

BB84, 90 mW pump power
214 bits/second
3.1% error rate
→ 136 secret bits/second
→ yield enhancement = 1.3

SSP, 90 mW pump power
371 bits/second
2.7% error rate
→ 251 bits/second
→ yield enhancement = 2.1

Wednesday night data (= “preliminary”)



- Cavity loss (~33%) prevents yield from exceeding 1/2.
- Rate is …non-optimal (~50-100/s).
- Six-state protocol now advantageous if BER > ~4%.

Relativistic QKD: Summary

- By allowing photon-storage, Bob can use the correct basis for every measurement ⇒ enhanced yield by 2 (BB84) or 3 (6-state)
- Security constraint = "why it's relativistic"
  - –non-overlapping light cones of Bob's receipt of photon and Alice's classical basis transmission
  - –Alice and Bob must know their relative space-time coordinates!
- New technologies
  - –Twisted cylindrical-mirror cavity (450ns with T = 67%) [CLEAN mirrors!]
  - –Low latency classical modulation sender/receiver (CPLD logic, < 120 ns).
  - –3-basis analysis with single Pockel cell (three voltages: 0, ±V).
- Non-degenerate polarization-entangled source
  - –Preliminary yield enhancements of ~1.3 (BB84) and ~2.1 (SSP)
  - –Mirror cleaning may/should improve this (up to 1.6 [BB84] and 2.6 [SSP])
- First demo. of Überquantum advantage, i.e., QM + SR > QM
  - –Next steps: rates,stability,eavesdropping…