Polarization-based Quantum Key Distribution Without Shared Reference Frame

By Jean Christian Boileau

Collaborators:
Daniel Gottesman
Raymond Laflamme
Martin Laforest
Casey Myers
David Poulin
Rob Spekkens

IQC Institute for Quantum Computing

Outline:

- Give new polarization-based QKD protocols based on decoherence-free subspace to overcome the problem of birefringence in optical fiber.
- Relate this to the problem of doing QKD without shared spatial reference frame or synchronized clocks.

Birefringence and Collective Noise

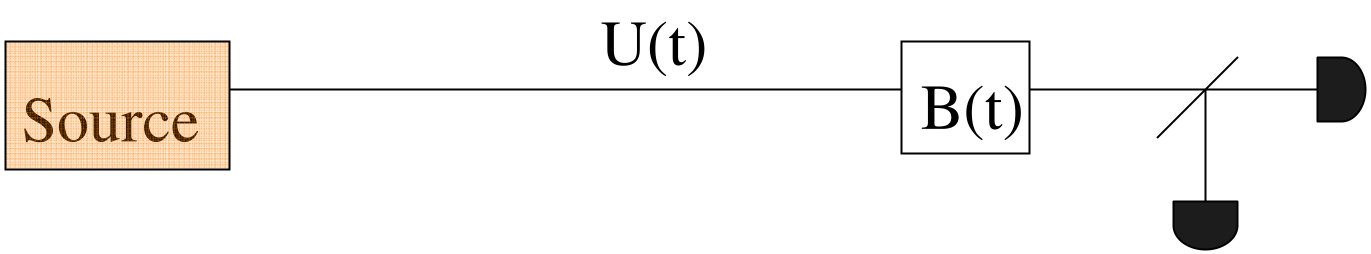
- The fiber acts like a random unitary transformation U(t) on the polarization states.
- The same transformation is applied to each photon if they are sent through the fiber at approximately the same time and if they have similar wavelength.
- Collective noise on *n* photons: $U^{\otimes n}$

Past Implementation of Polarization-Based QKD

- Encode in polarization space and periodic calibration of the reference frame

Franson and Jacobs,Electron. Lett. **31** 232-234 (1995).

  - Gives good result only if the fiber is in a stable environment

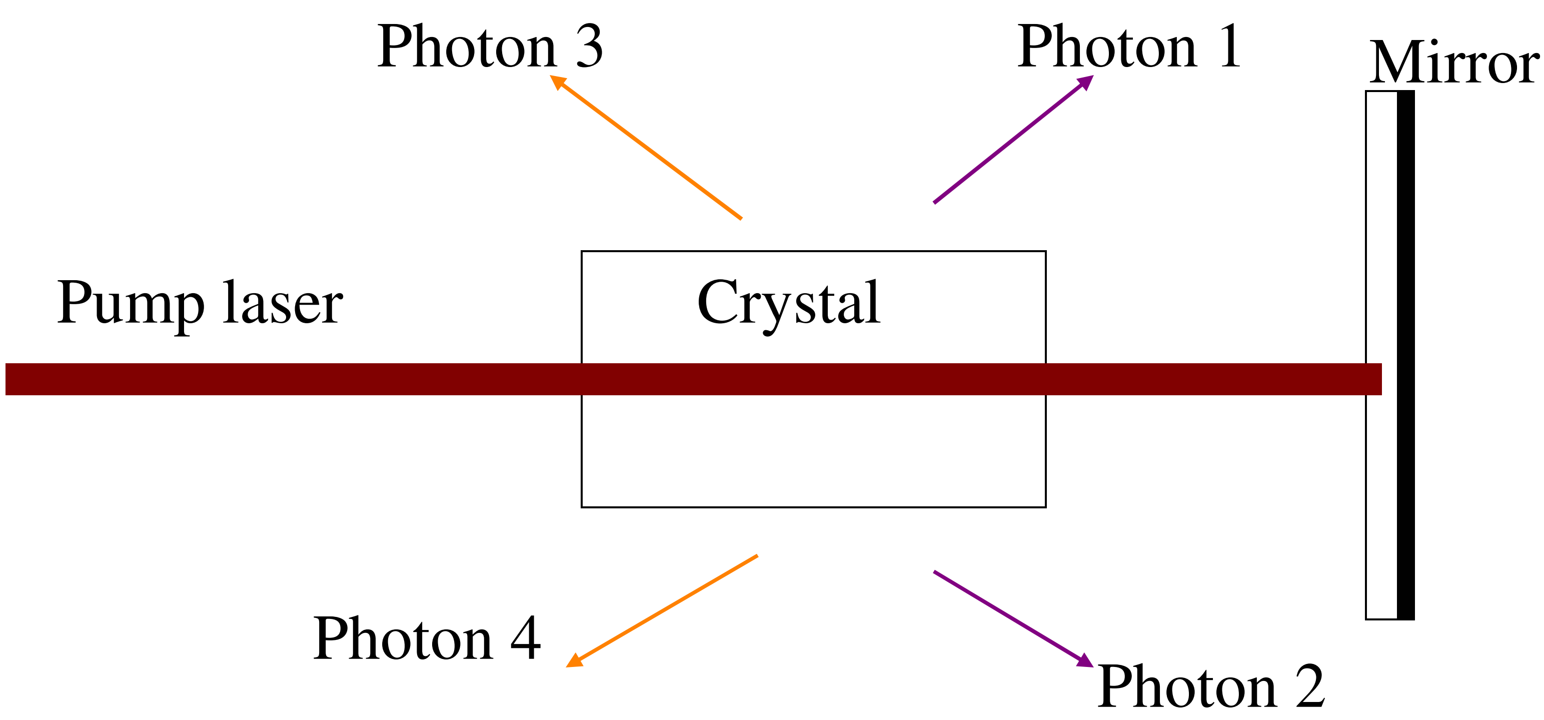


Decoherence-Free Subspace of the collective noise

# of Photons	DFS
1	None
2	$\|01\rangle - \|10\rangle$
3	None
4	$(\|01\rangle - \|10\rangle) \otimes (\|01\rangle - \|10\rangle)$ $2\|1100\rangle + 2\|0011\rangle - \|0101\rangle - \|1010\rangle - \|0110\rangle - \|1001\rangle$

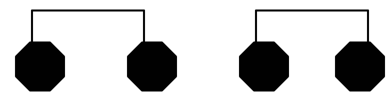
How to create $(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle)$

- Use parametric-down conversion with short pump pulse reflected on a mirror.

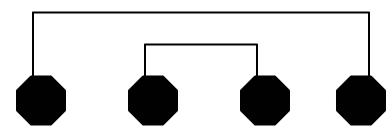


Four Photon Protocol

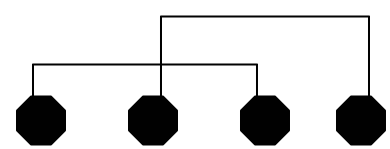
$$(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle) =$$



Swap photons 2 and 4:



Swap photons 2 and 3:



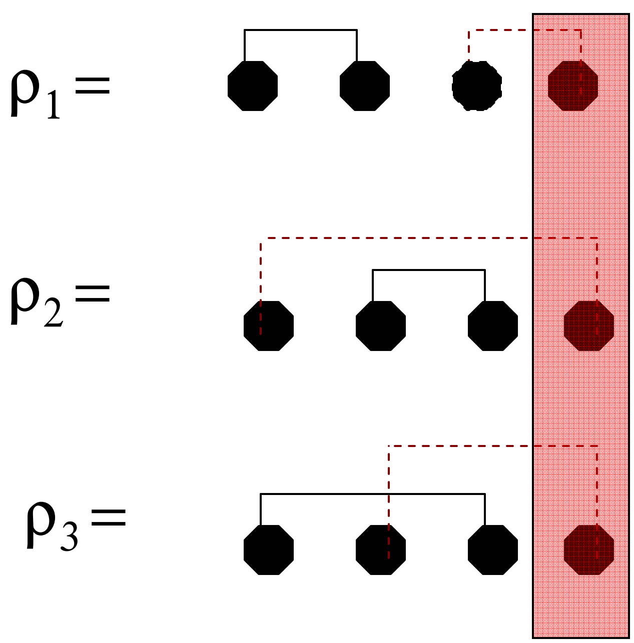
Four Photon Protocol

The three previous states can be written as

$$\begin{aligned} |\psi_1\rangle &= |a\rangle - |b\rangle \\ |\psi_2\rangle &= |b\rangle - |c\rangle \\ |\psi_3\rangle &= |c\rangle - |a\rangle \end{aligned} \qquad \text{where} \quad \begin{aligned} |a\rangle &= \tfrac{1}{2}(|0101\rangle + |1010\rangle) \\ |b\rangle &= \tfrac{1}{2}(|0110\rangle + |1001\rangle) \\ |c\rangle &= \tfrac{1}{2}(|0011\rangle + |1100\rangle) \end{aligned}$$

- The states $|a\rangle, |b\rangle$ and $|c\rangle$ are mutually orthogonal.
- $\langle\psi_j|\psi_i\rangle = \frac{1}{2}$ for $i \neq j$.

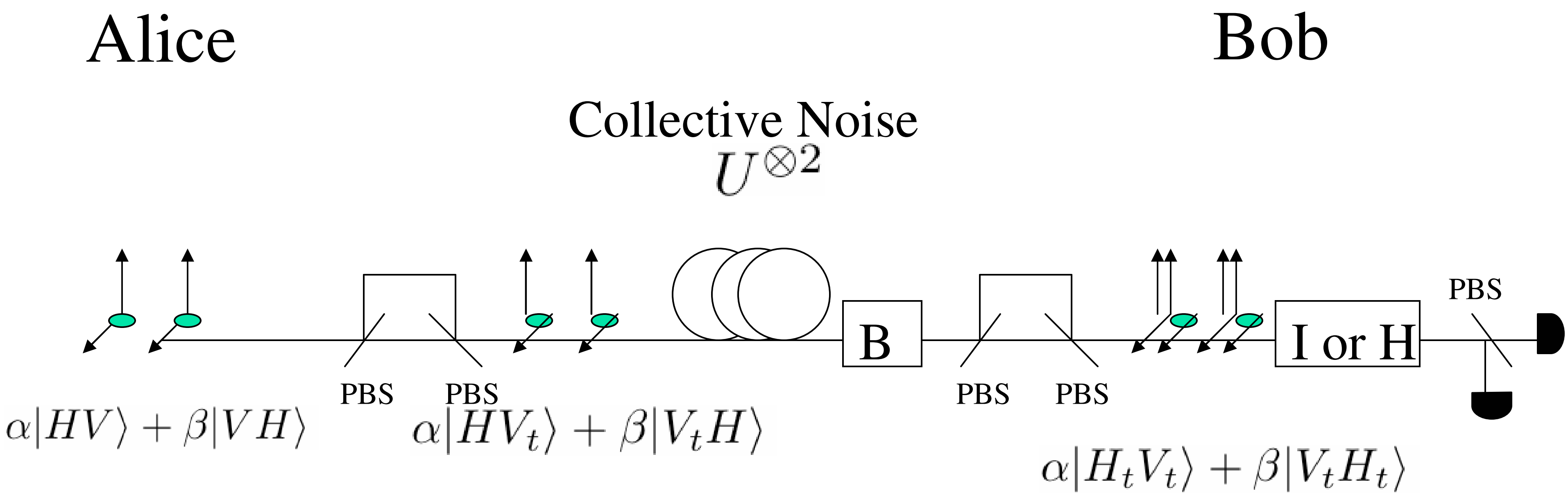
Three Photon Protocol



Two Photon Protocol

- Recently Walton et. Al. (*PRL*, **91** 087901 2003.) proposed a new protocol robust against phase instability in the interferometers that use photon pairs entangled in time.
- Can we improve their scheme using polarization?

Two Photon Protocol



with a probability that depends on $U^{\otimes 2}$.

Conclusion: I showed….

- a three state protocol quantum key distribution without any shared reference frame and
- a two photon protocol that does not need synchronized clock and that is robust again interferometer’s instability and birefringence.

Collaborators:

- Three and four Photon Protocol
  - Daniel Gottesman
  - Raymond Laflamme
  - David Poulin
  - Rob Spekkens
- PRL **91** 017901 (2004)
- Special thanks to Gilles Brassard

- Two Photon Protocol
  - Raymond Laflamme
  - Martin Laforest
  - Casey Myers
- quant-ph/0406118
- Special thanks to Joseph Emerson