Optical Quantum Information Processing

P. Kwiat

An inaccurate history
An incomplete progress report
An unbiased vision...not

Anti-Outline

• Continuous-variable systems
• Atom-photon systems (cf. Kimble)
• Hybrid systems (cf. Lukin)
• Quantum imaging, or not
• ...

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

How **do** you prove it?

The Beamsplitter...

Photon only detected in one output.
- use $g^{(2)} = 0$ to test sources...

Equally likely to be transmitted or reflected -- cannot tell which:
- quantum random number generator (patented)
Photon, but just 1:

- Single emitter
  - atom/ion (Kimble) [hard to collect]
  - quantum dot (“designer atom”)
    [BUT no two exactly alike...]

- Pair sources (SPDC, 4-wave mixing)
  - detection of signal photon --> “heralds” presence of idler photon in well-defined mode
Resources for **Photonic** Quantum Information Processing

Spontaneous Parametric Downconversion

Well-behaved spatial modes

High-quality OTS components ⇒ >99.9% fidelity 'gates'

Conditional 1-photon per mode

NOT "on-demand" (multiplexed sources help)
Resources for Photonic Quantum Information Processing

**Detectors:**

- What we want
  - high efficiency (at $\lambda$), low noise
  - fast (ideally at 100-fs scale)
  - photon-number resolving
- What we have now*
  - APDs, VLPCs, TES, SSPDs
  - $\eta \sim 85$-95% (visible to 1550 nm)
  - 1 MHz - 1 GHz
  - can resolve up to $\sim$10 photons

*But NOT all at once!
Resources for Photonic Quantum Information Processing

Superconducting bolometric detectors
- system efficiency (at 1550 nm) ~95% (pushing toward 99%)
- near-perfect photon-number resolution
- slow-ish (0.1 - 1 µs)

(Polarization-) Entangled Source:

Type-I phase-matching → H-polarized (from #1)

|ψ⟩ = \frac{1}{\sqrt{2}}(|H⟩_1|H⟩_2 + e^{iφ}|V⟩_1|V⟩_2)

Maximally entangled state

Tune pump polarization: → Nonmax. entangled, mixed states
Stable, simple → Used to test QM in various undergrad labs
New ultra-bright versions, narrow bandwidth, …

Not on-demand, unwanted entanglement in other DOFs

PRL 75, 4337 (1995)
Fiber-Based Sources (4-wave mixing) @ NIST, Northwestern, …

- Pairs created in fiber i.e., naturally single-mode
- Low-loss
- Exploits existing telecom infrastructure
- 1550 nm or 1310 nm
- Require cryogenic cooling

LOQC Gates


Degenerate Entanglement

Moore’s law for entanglement

Polarization-entangled pairs @ 2,000,000 s⁻¹, with F ~98%, T > 96%  

Next main limitation: detector saturation

Bell-Ineq. Tests

\[ S_{LHV} \leq 2 \quad |S_{\text{expt}}| = 2.7260 \pm 0.0008 \]

(216\sigma in 0.8 s)

Optimized \[ |S_{\text{QM, max}}| = 2\sqrt{2} = 2.828 \]

Bell test: \[ |S_{\text{expt}}| = 2.826 \pm 0.005 \quad 165\sigma \]

Now: Various tests with 2-5 photons (GHZ), with different DOFs, “qudits”, etc.  
More to come…
Entanglement distribution (and QKD) over 144-km link between La Palma and Tenerife (QIPS)

Now heading into space...

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.
Entanglement Advantages for QKD

• 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!)

• “Monogamy of entanglement”: Any leakage of info to other DOF ⇒ increased bit error rate (BER)

Challenges: Source brightness/robustness to compete, e.g., with Decoy-state QKD. Fast quantum repeaters for long distance key distribution.

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:

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...

E.g. Alice measures photons C and A to be in a singlet state. Since C and A are orthogonal, and A and B are orthogonal, C and A must be identical!
Two-Photon Interference

*Traditional Hong-Ou-Mandel: interfere two photons (from same source):*

*Photons must be indistinguishable (& not entangled to other photons)!*

**Coincidence Probability**

$$\left| \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \frac{i}{\sqrt{2}} \right|^2 = 0$$
Experimental Teleportation
Bouwmeester et al., Nature 390, 575 (1997)

Quantum Teleportation of a Composite System

Experimental results of teleporting an entanglement

What are the limits? How large (complex) of a system?
How far? How fast? Teleport complex “process”?
Entanglement Swapping

What if the unknown state is already entangled to a 4th particle?

Now these are entangled, despite that they have never directly interacted!

Need to distribute entanglement over longer distances (repeaters):

If we have a quantum storage device we can wait until we have a pair from both sides.

Need ~100 pairs

Need ~20 pairs
Photon Entanglements

- Polarization (spin)  
  (Ou & Mandel, Shih & Alley, etc., etc.)

- Linear momentum  
  (Rarity & Tapster)

- Orbital angular momentum  
  (Zeilinger et al.)

- Time-Bin  
  (Gisin et al., Inoue et al.)

- Energy-Time  
  (Franson et al., Howell et al.)

- 3,4,5, high photon number  
  (many)
Hyper-Entanglement

- Photons simultaneously entangled in multiple DOFs:
  \[ (|H, H\rangle + |V, V\rangle) \otimes (|rl\rangle + \alpha|gg\rangle + |lr\rangle) \otimes \int_0^{E_p} dE A(E)|E\rangle_s |E_p - E\rangle_i \]
  - **polarization**
  - **spatial modes**
  - **energy**

- Enlarged Hilbert space: \( 2 \otimes 2 \otimes m \otimes m \otimes n \otimes n \)

- Easy to perform quantum logic *between* DOFs

- More efficient n-qubit transfer: \( T \) vs \( T^n \)

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

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)

✓ 1 entangled photon each to Bob and Alice  
✓ Bob applies one of 4 U’s $\Rightarrow$ 1 of 4 Bell states;  
  sends photon to Alice  
✓ Alice: BSA $\Rightarrow$ infer one of 4 messages

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

Full BSA analysis “impossible” with linear optics…
Hyperentanglement-enhanced Superdense Coding

Average success probability: 95%  
⇒ channel capacity: $1.630(6) > 1.58$  
(“limit” for linear optics superdense coding, i.e., without hyperentanglement)

What are the limits?  
How many bits/photon?  
Can the “hitchhiker” qubits be used, e.g., for error correction?

Why Optical Quantum Computing?

“Photons been very very very good to me”

• Very little/no decoherence -- photon’s don’t interact
• Excellent performance with off-the-shelf optics
• Very fast gates: single-qubit \( \sim 10 \text{ ps} - 5 \text{ ns} \)
  two-qubit \(<150 \text{ ns}\)

Why not Optical Quantum Computing?

• Photon’s don’t interact -- 2-qubit gates hard
• Linear approach: measurement-induced nonlinearity
• Nonlinear approach: Zeno and QND gates
Grover’s search algorithm with linear optics

Optical realization with single photons: A database of four elements

- Gates: Linear optical elements
- Nonscalable -- each new qubit doubles the required number of optical elements

Accuracy: ~97.5% (as of 2004)

Linear optical quantum computing


SINGLE PHOTONS

FAST FEEDFORWARD

SINGLE-PHOTON DETECTION

LARGE overhead requirements…\(>10^5\)/gate
A New Paradigm:
Measurement-based computation

• 2004 - Nielsen’s solution: combine KLM non-deterministic gate with cluster-state model of quantum computation

Raussendorf and Briegel, PRL 86, 5188 (2001)

Nielsen, PRL 93, 040503 (2004)
Photons are hard to hold, but with cluster states you can build as you go...
Graph states (clusters and parity-encoding techniques) have greatly reduced the required resources and the loss-tolerance threshold for LOQC:

- Resources (Bell states, operations, etc.) for a reliable entangling gate
- Acceptable loss for a scalable architecture
- Efficient LOQC possible if (source purity) x (detection effic.) > 2/3.

CNOT with >95% success (KLM)
Cluster-state architectures are remarkably immune to loss.
The tradeoffs between Resources and Loss-threshold
Realization of photon cluster states

- Direct creation via down-conversion
- Interferometric setup
- Simple polarizers

\[
\frac{1}{2} \left( |H\rangle_1 |H\rangle_2 |H\rangle_3 |H\rangle_4 + |H\rangle_1 |H\rangle_2 |V\rangle_3 |V\rangle_4 \\
+ |V\rangle_1 |V\rangle_2 |H\rangle_3 |H\rangle_4 - |V\rangle_1 |V\rangle_2 |V\rangle_3 |V\rangle_4 \right)
\]

Present status:

- 1-qubit gate fidelity: F >90%
- Few count rates: 10^{-1} 3-pair/s
- Thus far up to n = 6 (at very low rates)

Grover search algorithm

Need ‘on-demand’ sources, better detectors, and better wires...
Feed-Forward Implementation


Pockels Cells:
KD*P crystals ~ 6.3 kV
Over 99 % fidelity (500:1)

~1 ns possible
(w better detectors, integrated optics)

Feed-Forward Time < 150 ns !!

Fibers to detector 15ns
Detector-Delay 35ns
EOM-Delay 65ns
Logics-Delay 7.5ns
Misc. cables 20ns


Silica-on-silicon Quantum Photonics

Quantum interference

V = 0.995 ± 0.007

S' = 0.990 ± 0.0

CNOT chip
Harnessing higher dimensions to reduce LOQC resources

• Even small quantum algorithms require large numbers of \textit{cu} and Toffoli gates
  - controlled-U gates: phase estimation, quantum chemistry...
  - Toffoli gates: Shor’s, error correction, fault tolerance...

• What if your architecture only has 2-qubit gates?
  - e.g., build Toffoli with 6 CNOT’s

• Works by coherently isolating some quantum information from gate actions

<table>
<thead>
<tr>
<th>chained gates</th>
<th>new scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>no. photons</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>1/2073</td>
<td>1/4096</td>
</tr>
</tbody>
</table>

| probability of success |            |
|                        | 1/72       |
| 1/32                   |            |

<table>
<thead>
<tr>
<th>min. photons</th>
<th>max. prob.</th>
<th>min. photons</th>
<th>max. prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1/32</td>
<td>6</td>
<td>1/72</td>
</tr>
</tbody>
</table>

What are the limits, e.g., when going for fault-tolerance...?
How to brew Really BIG Cluster-states: Percolation

Fusion success probability = 1/2, above percolation threshold. ⇒ get large piece of connected cluster state with high probability

From the percolated cluster it is easy to compute measurement patterns to produce any desired cluster circuit:

- Every photon undergoes only one Type-I gate and one single-qubit measurement
- Removes requirement for photon rerouting (only requires feedforward to classical measurement settings)
- Initial resources can be as small as 4-photon cluster states
Scalable quantum computing in the optical frequency comb


**Classical frequency comb**

The eigenmodes of a cavity form a naturally scaled ensemble of classically coherent modes

Physical graph
(frequency- & polarization-labeled)

Super-Resolution \textit{á la NOON}

\[ |N :: 0\rangle_{a,b} = \frac{1}{\sqrt{2}} (|N, 0\rangle_{a,b} + |0, N\rangle_{a,b}) \]

\[ \lambda / N \]

N=1 (classical)

N=5 (NOON)
Super-Sensitivity

\[ \Delta \varphi = \frac{\Delta \hat{P}}{|d\langle \hat{P} \rangle / d\varphi|} \]

\[ dP_N / d\varphi \]

\[ N=1 \text{ (classical)} \]
\[ N=5 \text{ (N00N)} \]

For Many Sensor Applications — LIGO, Gyro, etc., — We Don't CARE Which Fringe We're On!

The Question for Us is IF any Given Fringe Moves, With What Resolution Can We Tell This?!

How do we efficiently create these exotic states? What else are they good for?
Quantum (or not) Phase Metrology

1990
2-photon
Rarity, (1990)
Ou, et al. (1990)
Shih, Alley (1990)
...

6-photon
Super-Resolution
Resch, ... , White
PRL (2007)
Queensland

2004
3, 4-photon
Super-resolution
Mitchell, ... , Steinberg
Nature (13 May)
Toronto

2007
4-photon
Super-sensitivity &
Super-resolution
Walther, ... , Zeilinger
Nature (13 May)
Vienna

Nagata, ... , Takeuchi,
Science (04 May)
Hokkaido & Bristol
Weak-Value-Enhanced Deflection-Detection

This is a classical enhancement, discovered by studying QM weak measurements. So what!

What are the limits when combined, e.g., with squeezed input light, or N00N states, or…?
Photons

Quantum Physics

Quantum Communication

Quantum Metrology

Quantum Computing
Quantum Battle
Space of Tomorrow

What good is Quantum Information for Video Games??