Quantum Communication:
QKD, teleportation into a solid-state quantum memory and Large entanglement

Nicolas Gisin, Hugo Zbinden, Mikael Afzelius, Rob Thew and Félix Bussières
GAP-Optique, University of Geneva

- Commercial QKD system
- Why QKD?
- Longer distances: networks based on trusted nodes
- Q memories for quantum repeaters and networks
- Large Entanglement
Years of continuous commercial operation

Installed multiplexed quantum channel for commercial users.

Used daily by some commercial
Why QKD?

How much of a problem for QKD is quantum computing, really??

Courtesy of Prof. Michele Mosca
How soon do we need to worry?

Depends on:
- How long do you need encryption to be secure? \((x \text{ years})\)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? \((y \text{ years})\)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance?) \((z \text{ years})\)

**Theorem 1:** If \(x + y > z\), then worry.

What do we do here??

Courtesy of Prof. Michele Mosca
Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

** Courtesy of Prof. Michele Mosca **
How far can one send a photon?

There is a hard wall around 400 km!

With the best optical fibers, perfect noise-free detectors and ideal 10 GHz single-photon sources, it would take centuries to send 1 qubit over 1000 km!
Long distance QKD: World records

150 km of installed fibers, Optics Express 17, 13326 (2009)

250 km in the lab.
NJP 11, 075003 (2009)
Proposals for quantum communication in space

Dual-downlink (ROM R&D 47 M€)

Using a motorized photo-lens-pod (existing) and a dedicated quantum detector as “camera”.

Astronaut: A. Kuipers

Single-uplink (ROM R&D 1 M€)

Simultaneous optical downlink: 1400 km separation.


T. Scheidl, E. Wille, and R. Ursin, New Journal of Physics, 15, 043008 (2013)

Rupert.Ursin@oeaw.ac.at - Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences
Network-centric Quantum Communications

Richard Hughes, Jane Nordholt and team
Los Alamos National Laboratory

application layer:
- confidentiality
- authenticity
- integrity
- non-repudiation
- between users who may have no direct QC

quantum key management (QKM) layer:
- classical protocols built from quantum primitives
- key establishment
- signatures
- certificates

quantum protocol layer:
- quantum identification (QID)
- quantum key distribution (QKD)
- quantum secret splitting (QSS)

quantum physical layer:
- novel BB84-type QC in fiber
- quantum multiple access (QMA)
- quantum random number gen.


R. J. Hughes et al., arXiv:1305.0305
Long Range QKD with trusted nodes

Battelle QKD Backbone
- Columbus OH to Washington DC Area
- > 770 km
- Deployment targeted in 2015

≈ 800 km

Battelle Main Campus

Battelle Aberdeen Office

Baltimore
The Security Onion

Environment
Physical Protection
Enclosure
Access Control
Chassis
Security Protocols
Intrusion Detection
Cryptographic Boundary

Courtesy Dr Don Hayford
Battelle
We still miss the capability to store entanglement: Developing quantum memories is a grand challenge!
Quantum memory

Goal: controlled and reversible mapping of a photonic quantum state onto a long lived atomic ensemble

Crystal doped with billions of

Photon in

Photon out at desired time in same Q state

Today’s efficiencies ≈ 20 %

Nature 456, 773, 2008
Controlling the Dephasing! Atomic Frequency Comb

\[ \sum_{j=1}^{N} e^{ikr_j} e^{-i\delta_j t} |g_1...e_j...g_N \rangle \]

\[ P_j = e^{-i\delta_j t} \]

\[ \Delta \text{ continuous } \Rightarrow \text{ Dephasing} \]

Absorption

\[ \text{Frequency} \]

Im\((P_j)\)

Re\((P_j)\)

\[ \text{Im}(|P_j|) \]

\[ \text{Re}(|P_j|) \]

GAP Quantique Geneva University
Atomic Frequency Comb (AFC) Quantum Memory

2 levels: preprogrammed delay (AFC echo)

3 levels: on-demand re-emission (spin wave storage)

$\sum_{j=1}^{N} e^{ikx_j} e^{i\delta_j t} |g_1 \cdots e_j \cdots g_N\rangle$

Periodic!

M. Afzelius et al. PRA 79, 052329 (2009)
AFC echo

(a)

Normalized intensity (arb. units)

Time (μs)

Optical detuning [MHz]

Optical depth

Input

Transmitted

Echo

Optical depth

Δ

d
γ
Multi-mode storage in Nd$^{3+}$:Y$_2$SiO$_5$

Mapping 64 input modes onto one crystal

$\langle n \rangle < 1$ per mode

64 time modes can be used to code 32 time-bin qubits!

I. Usmani et al., Nature Communications 1,12 (2010)
Entanglement-preserving quantum memory

$$|\Phi^+\rangle = |H\rangle_{1338} |H\rangle_{883} + |V\rangle_{1338} |V\rangle_{883}$$

Bandwidth: 680 MHz
Entanglement-preserving quantum memory

![Graph showing coincidences in 10 minutes](image)

- SPD1: $\nu = 93.7(53)\%$
- SPD2: $\nu = 97.7(94)\%$

![Graph showing $\lambda/2$ angle vs. SPD2](image)

- SPD1: $\nu = 87.0(40)\%$
- SPD2: $\nu = 99.7(39)\%$
Entanglement-preserving quantum memory

\[ |\Phi^+\rangle = |H\rangle_{138} |H\rangle_{883} + |V\rangle_{138} |V\rangle_{883} \]

Using Bell test as Entanglement Witness

\[
E(A_1, B_1) = 0.68 \pm 0.06 \\
E(A_1, B_2) = 0.51 \pm 0.06 \\
E(A_2, B_1) = 0.54 \pm 0.06 \\
E(A_2, B_2) = -0.79 \pm 0.08
\]

\[ S = 2.52 \pm 0.13 \]

S larger than local bound of 2 \(\rightarrow\) Device-Independent Entanglement!
Teleportation of a polarization qubit from a weak coherent state


sspd from NIST
Quantum teleportation of a telecom-wavelength photon to a solid-state quantum memory
Partial Bell State Measurement and post-selected fidelity

F. Bussières, Ch. Clausen et al., arXiv:1401.6958

**Tomographic reconstruction (short link)**

<table>
<thead>
<tr>
<th>State</th>
<th>Fidelity (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Analysis on a great circle of the Poincaré sphere
What do we need to do the full AFC memory scheme?

- **Input**
- **Absorption**
- **Control Pulses**
- **Output**
- **Signal Preparation**
- **Zeeman or hyperfine states**

The diagram shows the process involving states $|e\rangle$, $|g\rangle$, and $|s\rangle$, with control pulses and signals at different times.
**Some Basic $^{151}$Eu$^{3+}$:Y$_2$SiO$_5$ Spectroscopy**

- Excited state life time 2 ms
- Max. absorption coefficient 3-4 cm$^{-1}$
- Spin coherence time 15 ms for $^{151}$Eu (B=0)

*Inhomogeneous absorption spectrum (100 ppm $^{153}$Eu)*

$\Gamma \approx 700$ MHz
d = 1.3

$\frac{5}{2} \quad \frac{3}{2} \quad \frac{1}{2} \quad \frac{5}{2} \quad \frac{3}{2} \quad \frac{1}{2}$

580 nm

PRA 88, 02324 (2013)
Towards high SNR and long-lived Quantum Memory
Work in progress...

1. Higher two-level AFC efficiency Method 1

Frequency stable laser, optimized comb preparation

2. Higher two-level AFC efficiency Method 2

Cavity enhanced QM

Afzelius & Simon
PRA 82, 022310 (2010)

3. Longer two-level AFC storage time

4. Milliseconds spin-wave storage time

Spin-echo techniques

\[ \gamma_{\text{IS}} = 8.43 \pm 0.19 \text{ kHz} \]

\[ 1.51 \% \]

\[ 49\% \]

50 ms
3. Large Entanglement

Natalia Bruno, Anthony Martin, Pavel Sekatski, Nicolas Sangouard, Rob Thew and Nicolas Gisin

Group of Applied Physics
Geneva University, Switzerland
Do these entangled crystals count as macroscopic entanglement?

Nature Photonics 6, 234-7, 2012
What is macroscopic? What is quantum?

- Do these 2 crystals count as large entanglement? No!
- Billions of ions in a macroscopic object, but “only” one - delocalized - excitation
- Quantum = entanglement.

Nature Photonics 6, 234-7, 2012
Example: 1-photon entanglement

\[ |0,1\rangle + |1,0\rangle \]
Example: displaced $1-\nu$ entanglement

The components of this entangled state can easily be distinguished using classical detectors because $\Delta n_{D(\alpha|1)} \approx 3 \Delta n_{|\alpha\rangle}$

Pavel Sekatski, Nicolas Sangouard et al., PRA 86, 060301 (2012)
Distinguishability

\[ |0\rangle \otimes D(\alpha) |1\rangle^+ + |1\rangle \otimes |\alpha\rangle = |+\rangle \otimes \Psi_- + |-\rangle \otimes \Psi_+ \]

Where \( \Psi_\pm = D(\alpha) |1\rangle \pm |\alpha\rangle \)

For \( |\alpha|^2 >> \Delta \), \( P_{\text{guess}} \approx 74\% \)

For \( |\alpha|^2 >> \Delta \), \( P_{\text{guess}} \approx 89\% \)

Pavel Sekatski, Nicolas Sangouard et al., PRA 86, 060301 (2012)
Toward truly Large Entanglement

\[ \prod_j |\alpha_j\rangle \otimes D(\alpha)|1_j\rangle + D(\alpha)|1_j\rangle \otimes |\alpha_j\rangle \]

Inside the crystal, no longer a product state, But a complex sort of Dicke state with involved Phase relations.

billions of atoms
thousands of excitations
hundreds of e-bits
Experiment: demonstrate Large Size Entanglement

We measured the concurrence $C$ (a measure of entanglement):

$$C \geq V(p_{10} + p_{01}) - 2\sqrt{p_{00}p_{11}}$$
Conclusions

- Quantum cryptography exists since years, though only in niche markets.
- \( z > x+y \Rightarrow \text{Panic today!} \)
- Trusted nodes make a lot of sense.
- Quantum repeaters require teleportation and quantum memories.
- Decoy detectors are practical again “quantum hacking” on detectors
- Large entanglement is fascinating
  - Nature Physics 9, 545 (2013)
- Relativistic bit commitment:
  - PRL 111, 180504 (2013)