Memory-Assisted Quantum Key Distribution

Mohsen Razavi
Institute of Microwaves and Photonics
School of Electronic and Electrical Engineering
University of Leeds

Quantum Memories Wanted!

High-performance quantum memory modules with:
- Efficient coupling to light
- Low-error gate operation
- Long storage times
- Short access times
- Mass-scale production
- Low price!

Quantum Memories in Action!

But, do we have such a memory?

How about existing (imperfect) memories? Can we use them in some useful way?

**Benchmark:** to beat an existing no-memory quantum system by adding quantum memory modules

Let’s find some examples!

Story line

Measurement-device-independent QKD
Memory-assisted MDI-QKD

Different setups and memories: requirements (with respect to the state of the art)

Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol

- Entanglement Swapping Protocol

Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol
Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol
- Entanglement Swapping Protocol
- Reverse EPR protocol

Memory-Assisted MDI-QKD

- Let's combine MDI-QKD with the repeater idea: SETUP A

- Expected benefit: better rate-vs-distance behaviour

Memory-Assisted MDI-QKD

- Let's combine MDI-QKD with the repeater idea:

- What is the advantage over quantum repeaters? Simpler @ the user end &

- But, how about memory errors? Wouldn't the memory decohere?

- Key rate \( \propto \exp(-\alpha L_0) \times \frac{\exp(-\alpha L_0)}{\eta} \)

- Resilient to detector attacks
- Suitable for access networks; End users only require the source/encoder
- BSM with linear optics and photodetectors

- BSM: Bell-state Measurement
**Writing time**

- Let’s combine MDI-QKD with the repeater idea:

  - **Writing time**: The time it takes for a single photon at the memory input to be stored into the QM, and we get to know about it

  - For SETUP A, the repetition period $\geq$ writing time

  - $\text{Writing time} = \text{Preparation} + \text{Storing} + \text{Heralding}$

**Memory-Assisted MDI-QKD**

- Let’s combine MDI-QKD with the repeater idea:

  - What is the advantage over quantum repeaters? Simpler @ the user end

  - $\text{Writing time} = \text{Writing time}$

**Memory-Assisted MDI-QKD: Heralding Schemes**

- In SETUP A, QMs need to be heralding:

  - Direct heralding is typically slow (~ms). Can we avoid it?

**Memory-Assisted MDI-QKD: Key Rate Analysis**

- Let’s see how our SETUP B performs in a realistic setup once we include various sources of nonideality including memory dephasing and decay, dark count and background noise, various inefficiencies (writing, reading, detectors, loss) and timing issues

- We find the achievable key rate under the normal mode of operation, where there are no eavesdroppers. More details at

  - [NJP 16, 043005 (2014)]
  - [arXiv:1407.8016; IEEE JSTQE (2015)]
  - [arXiv:1603.03623]
MDI-QKD with Single Atoms in SETUP B

- Curve A: T_2 = 100 µs
- Curve B: T_2 = 1 µs
- Curve C: T_2 = 1s
- Curve D: T_2 = 100 µs

Secret key rate (b/s)

- No-memory MDI-QKD
- Memory-assisted MDI-QKD

Parameters taken from [Nature 484, 195 (2012)]

MDI-QKD with Atomic Ensembles in SETUP B

- Bapt: Collective excitation
- |0⟩|0⟩ + √p|1⟩|1⟩ + √(1-p)|2⟩|2⟩ = HOT, p < 1

With prob p^2, we get two overall excitations in Alice/Bob’s memories → will cause error in the middle BSM

How About Ensemble-Based Memories?

Towards high-speed optical quantum memories


Quantum memories, capable of controllably storing and erasing a photon, are a crucial component for quantum computers and quantum communications. To date, quantum memories have operated with bandwidths that limit data rates to megahertz. Here we report the coherent storage and retrieval of sub-microwatt-level intensity-tuned photons with spectral bandwidth exceeding GHz, a crucial step toward the realization of a quantum internet.

Broadband waveguide quantum memory for entangled photons


What to do next?

- Our first attempt failed!
- Possible Solutions:
  - Change the entangling procedure
  - Find another suitable memory candidate
- Here we consider some of these options
- What can be done with a good EPR source?
- What can be done with a good single-photon source?
- How about NV centres in Diamond?

Memory-Assisted MDI-QKD: SETUP C

- An alternative (indirectly) heralding scheme: SETUP C
- Not fully heralding, but with efficient writing schemes, is almost there.
- Not fully heralding, but with efficient writing schemes, is almost there.
- Not fully heralding, but with efficient writing schemes, is almost there.
- Not fully heralding, but with efficient writing schemes, is almost there.

- EPR sources based on quantum dots, however, have potentially lower double-pair emission rates (g(2) < 0.004, [Nat. Photon. 8, 224 (2014)]) as compared to their single-pair generation rate (0.1 - 0.9); high repetition rates (~ 1GHz)
Memory-Assisted MDI-QKD: SETUP C (modified)

- An alternative (indirectly) heralding scheme
- One great possibility: delayed writing!
  Only write to the memory if the side-BSM is successful
  We need to delay one of the EPR photons for a short time
  - Overhead time for cooling/preparing the QMs is almost irrelevant
  - Clock rate independent of the writing time
- Qdot-based EPR sources may need more time to mature, but that's no longer a memory problem! 😊

How would it perform?

- Curve A: coherence time = 1.5 µs
  Writing/reading time = 300 ps
  Entangling efficiency = 0.12
  Retrieval efficiency at no decay = 30%
  - Entangled states are assumed ideal

- Curve B: 150 µs
  - Available today!

- Curve C: 73%


How about Using Single Photon Sources?

- SETUP D
  [presented at CLEO:2016]
  Can be imperfect

Performance of Ensemble-Based Memories

MDI-QKD with NV Centers in Diamond

- To avoid multiple excitation effects, we can use single-atom like memories
- Negatively charged NV centres in diamond look like a plausible option
  - They can be entangled with photons
  - They are rather fast; 10 ns for writing
  - Long coherence times up to 0.6 s

MDI-QKD with NV Centers in Diamond

- To avoid multiple excitation effects, we can use single-atom like memories
- Negatively charged NV centres in diamond look like a plausible option
  - They can be entangled with photons
  - They are rather fast; 10 ns for writing
  - Long coherence times up to 0.6 s
  - Cavity-enhanced NV centres

[arXiv:1603.03623]
[PRX 4, 031022 (2014)]
Key Rate Comparison

[presented at QCMC 2016]

- Up to three orders of magnitude over a single no-QM system

Scalability: Long-distance Trust-free QKD

- Memory-assisted MDI-QKD is not scalable like quantum repeaters
- Eventually, one should think of MDI-QKD + Repeater setups:

Summary

SETUP A: offers better rate-vs-distance behavior; requires heralding memories, with short access times and large storage-BW products

SETUP B: Relaxes the heralding requirement; cannot work with ensemble-based memories

SETUP C: Further relaxes constraints on the writing time; can work with ensemble-based memories; can use practical SPS
**Summary**

**Take-home Message:**

Even with imperfect quantum memories of about today’s technology, we can devise memory-assisted QKD systems that outperform their no-memory counterparts. That is the first step toward building long-distance QKD systems.

---

**PhD Positions in Europe!**

QCALL is a European Innovative Training Network (ITN) that offers 15 extremely well-funded PhD positions on various topics related to quantum communications:
- 3 years of funded PhD research with annual salary > €43k and research budget > €60k per student
- Dedicated schools on QKD and quantum networks + complementary-skill training + extensive placement programmes
- Eligibility: meeting mobility criterion + being an early-stage researcher
- PhD start date: Early 2017 – Oct 2017
- Deadline for application: 15 Jan 2017

http://www.qcall-itn.eu

**Partners:**
- ID Quantique: 1 project on quantum hacking; contact: P. Brussieres
- Telecom ParisTech: 1 project on hybrid CV QKD; R. Alleaume
- Toshiba Research Europe Ltd: 2 projects on MDI QKD and integration; R. Alleaume
- University of Queensland: 2 projects on repeaters and multiparticle entanglement; D. Bruss
- University of Geneva: 2 projects on QKD and quantum memories; H. Zbinden
- University of Leeds: 2 projects on MDI-QKD and repeaters; M. Razavi (Coordination)
- University of Padova: 2 projects on satellite QKD and QRNGs; P. Villoresi
- University of Pierre and Marie Curie: 1 project on beyond-QKD protocols; E. Diamanti
- University of Vigo: 2 projects on security of QKD and beyond-QKD protocols; J. M. G. PRs
- Plus collaborative partners at BBN, Heriot-Watt, Inria, ICC, Madrid, Max Planck & NTT

---

**Thank You**