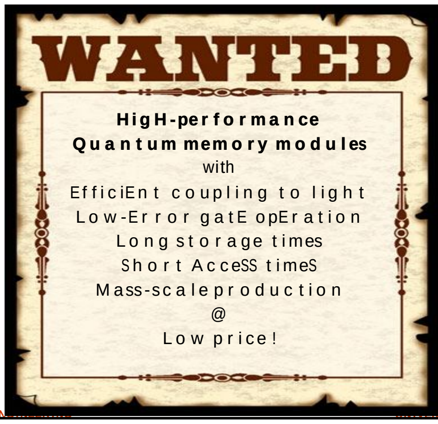
29 Dec 2016

Memory-Assisted Quantum Key Distribution

Mohsen Razavi

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

Quantum Memories Wanted!



Quantum Memories in Action!

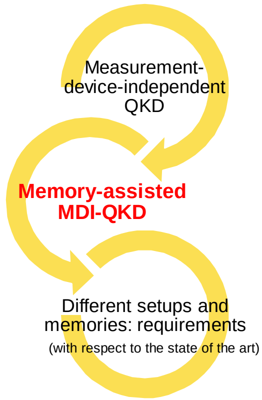
But, do we have such a memory?

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



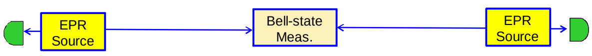
Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol

Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol

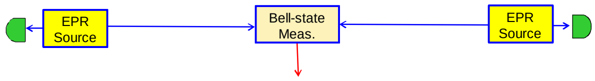
- Entanglement Swapping Protocol



Measurement-Device-Independent QKD (MDI-QKD)

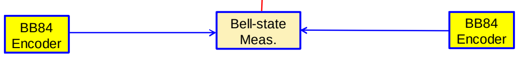
- EPR Protocol

- Entanglement Swapping Protocol



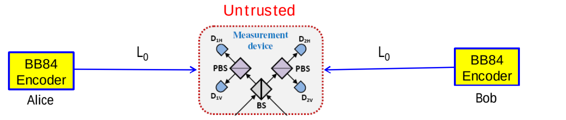
Untrusted → Meas-Device Independent

- Reverse EPR protocol



[Biham, Huttner & Mor, PRA **54,** 2651 (1996)]
[Lo, Curty & Qi, PRL **108,** 130503 (2012); Braunstein & Pirandola, PRL **108,** 130502 (2012)]

Measurement-Device-Independent QKD (MDI-QKD)



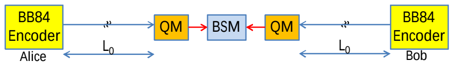
[Lo, Curty, & Qi, PRL **108,** 130503 (2012)]

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

$$\text{Key rate} \propto \underbrace{\exp(-\alpha L_0)}_{\eta} \times \exp(-\alpha L_0)$$

Memory-Assisted MDI-QKD

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



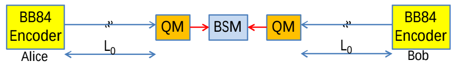
QM: Quantum Memory
BSM: Bell-state Measurement

[PRA **89**, 012301 (2014)]
[NJP **16**, 043005 (2014)]

- Memory-assisted protocol:
  - Send encoded photons toward memories
  - Attempt to store them into memories; whenever successful, stop and wait for the other side → a heralding mechanism needed
  - Do the BSM whenever both memories are loaded

Memory-Assisted MDI-QKD

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

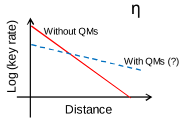


QM: Quantum Memory
BSM: Bell-state Measurement

[PRA **89**, 012301 (2014)]
[NJP **16**, 043005 (2014)]

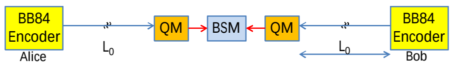
- Expected benefit: better rate-vs-distance behaviour

$$\text{Key rate} \propto \underbrace{\exp(-\alpha L_0)}_{\eta}$$



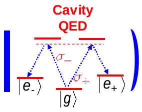
Memory-Assisted MDI-QKD

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



QM: Quantum Memory
BSM: Bell-state Measurement

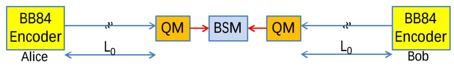
- But, how about memory errors? Wouldn't the memory decohere?



T_2 : dephasing time constant in $|e_+\rangle - |e_-\rangle$ space
T_1 : amplitude decay time from $|e_+\rangle$ or $|e_-\rangle$ to $|g\rangle$

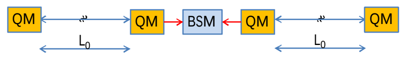
Memory-Assisted MDI-QKD

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



QM: Quantum Memory
BSM: Bell-state Measurement

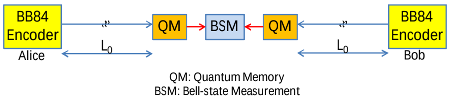
- What is the advantage over quantum repeaters? Simpler @ the user end &



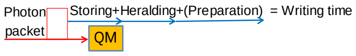
	attempt period	Coherence time
Qu. repeater	L_0 /c	$\propto L_0$ /c
MA MDI-QKD		

Writing time

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



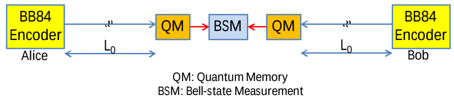
- Writing time: The time it takes for a single photon at the memory input to be stored into the QM, and we get to know about it



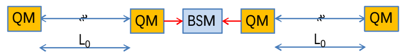
- For SETUP A, the repetition period >= writing time

Memory-Assisted MDI-QKD

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



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

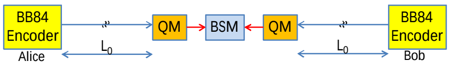


	attempt period	Coherence time
Qu. repeater	L_0 /c	$\propto L_0$ /c
MA MDI-QKD	Writing time	$\propto$ Writing time

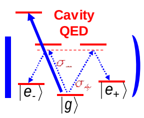
For fast memories, milder requirements on coherence time

Memory-Assisted MDI-QKD: Heralding Schemes

- In SETUP A, QMs need to be heralding:

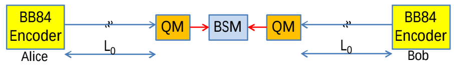


- Direct heralding is typically slow (~ms). Can we avoid it?

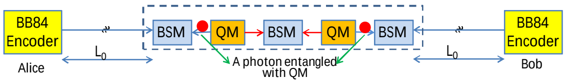


Memory-Assisted MDI-QKD: Heralding Schemes

- In SETUP A, QMs need to be heralding:



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



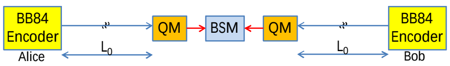
SETUP B:

- Entangle a photon with the QM

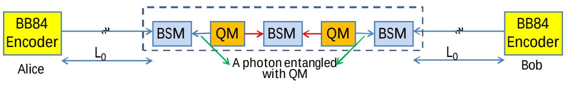
- Use this photon to teleport the incoming state to the QM

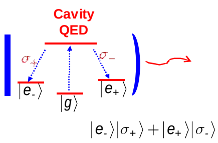
Memory-Assisted MDI-QKD: Heralding Schemes

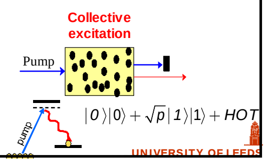
- In SETUP A, QMs need to be heralding:



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

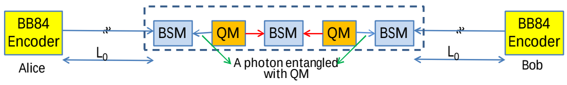






Memory-Assisted MDI-QKD: Key Rate Analysis

- 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*



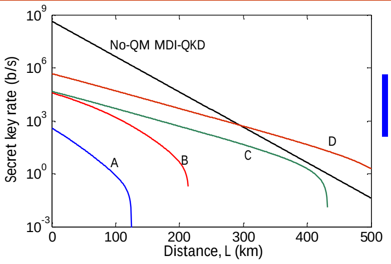
- We find the achievable key rate under the normal mode of operation, where there are no eavesdroppers. More details at

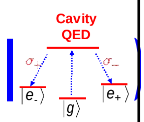
[NJP **16**, 043005 (2014)]

[arXiv:1407.8016; IEEE JSTQE (2015)]

[arXiv:1603.03623]

MDI-QKD with Single Atoms in SETUP B





Curve A:
coherence time, T_2 = 100 μs
Reading time = 1 μs; Writing time = 21 μs
Entangling efficiency = 0.4
Retrieval efficiency at no decay = 1

Curve B:
→ 1 μs

Curve C:
T_2 = 1s

Curve D:
T_2 = 1s
0.1 μs

Improvements needed

All curves: QE = 0.93; Dark count = 1/s; Repetition rate for no-QM: 1 GHz
Parameters taken from [Nature **484**, 195 (2012)]

How About Ensemble-Based Memories?

Towards high-speed optical quantum memories

[Nat. Photon. **4,** 218 (2010)]

K. F. Reim[1], J. Nunn[1], V. O. Lorenz[1,2], B. J. Sussman[1,3], K. C. Lee[1], N. K. Langford[1], D. Jaksch[1] & I. A. Walmsley[1]

Quantum memories, capable of controllably storing and releasing a photon, are a crucial component for quantum computers[1] and quantum communications[2]. To date, quantum memories[3, 4, 5, 6] have operated with bandwidths that limit data rates to megahertz. Here we report the coherent storage and retrieval of sub-nanosecond low-intensity light pulses with spectral bandwidths exceeding 1 GHz in caesium vapour. The novel memory interaction takes place through a far off-resonant

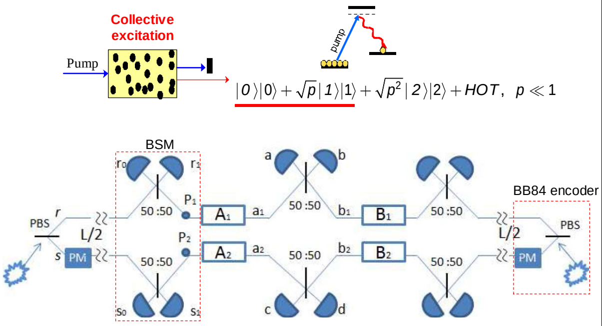
Broadband waveguide quantum memory for entangled photons

[Nature **469**, 512 (2010)]

Erhan Saglamyurek, Neil Sinclair, Jeongwan Jin, Joshua A. Slater, Daniel Oblak, Félix Bussières, Mathew George, Raimund Ricken, Wolfgang Sohler & Wolfgang Tittel

The reversible transfer of quantum states of light into and out of matter constitutes an important building block for future applications of quantum communication: it will allow the synchronization of quantum information[1], and the construction of quantum repeaters[2] and quantum networks[3]. Much effort has been devoted to the development of such quantum memories[1], the key property of which is the preservation of entanglement during storage. Here we report the reversible transfer of photon–photon entanglement into entanglement between a photon and a collective atomic excitation in a solid-state device. Towards this end, we employ a thulium-doped lithium niobate waveguide in conjunction with a photon-echo quantum memory protocol[4], and increase the spectral acceptance from the current maximum[5] of 100 megahertz to 5 gigahertz. We

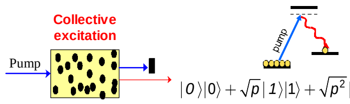
MDI-QKD with Atomic Ensembles in SETUP B



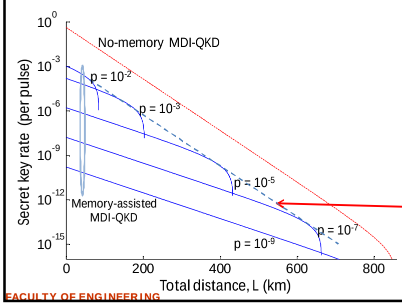
$$|0\rangle|0\rangle + \sqrt{p}\,|1\rangle|1\rangle + \sqrt{p^2}\,|2\rangle|2\rangle + HOT, \quad p \ll 1$$

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

MDI-QKD with Atomic Ensembles



$$|0\rangle|0\rangle + \sqrt{p}\,|1\rangle|1\rangle + \sqrt{p^2}\,|2\rangle|2\rangle + HOT$$



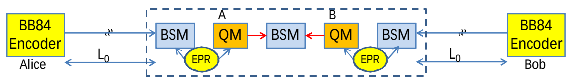
[IEEE JSTQE (2015)]

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

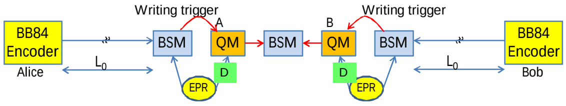
- An alternative (indirectly) heralding scheme: SETUP C



- Not fully heralding, but with efficient writing schemes, is almost there.
- We cannot use EPR sources based on parametric down-conversion (the same multi-photon statistics as atomic ensembles)
- 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!

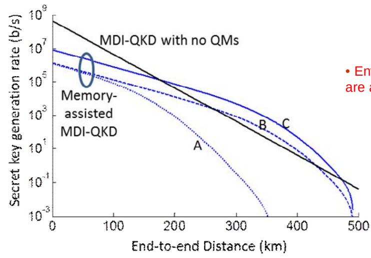
Only write to the memory if the side-BSM is successful
We need to delay one of the EPR photons for a short time

→ 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?



- Entangled states are assumed ideal

Curve A:	Curve B:	Curve C:
coherence time = 1.5 μs	150 μs	150 μs
Writing/reading time = 300 ps		
Entangling efficiency = 0.12		
Retrieval efficiency at no decay = 30%		73%

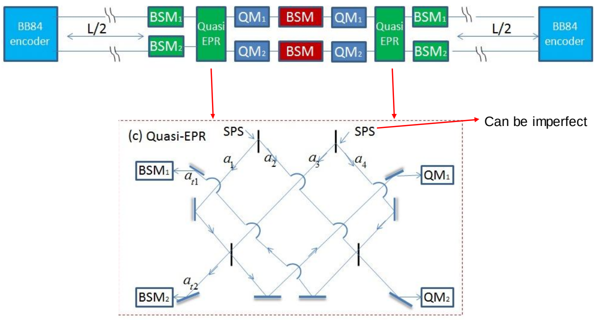
- available today!

All curves: QE = 93%; Dark count = 1/s; Repetition rate: 1 GHz; writing eff = 1

Parameters from [PRL **107,** 053603 (2011); Nature **466,** 217 (2010); Nat. Phys. **8,** 517 (2012)]

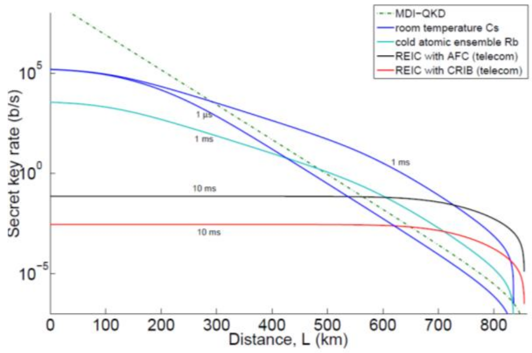
How about Using Single Photon Sources?

- SETUP D



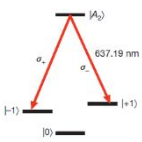
[presented at CLEO:2016]

Performance of Ensemble-Based Memories



MDI-QKD with NV Centers in Diamond

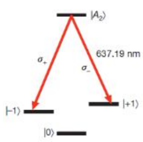
- To avoid multiple excitation effects, we can use single-atom like memories
- Negatively charged NV centres in diamond look like a plausible option
  - They can be entangled with photons
  - They are rather fast; 10 ns for writing
  - Long coherence times up to 0.6 s



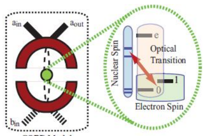
[Nature 466, 730 (2010)]

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

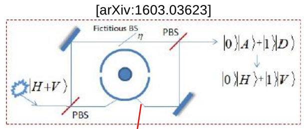


[Nature 466, 730 (2010)]



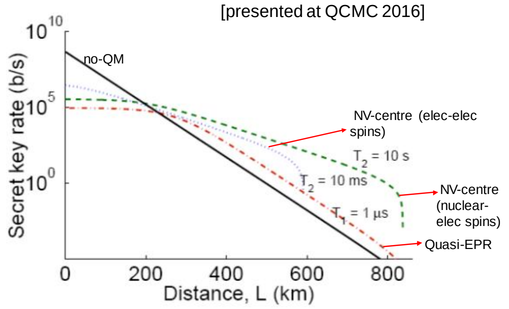
[PRX 4, 031022 (2014)]

[arXiv:1603.03623]



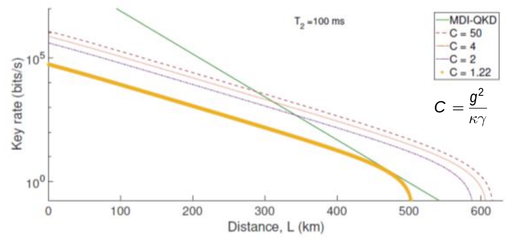
state dependent phase

Key Rate Comparison



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

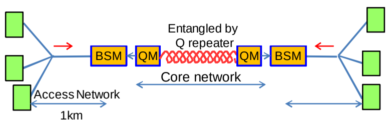
Moderate requirements on cavity coupling

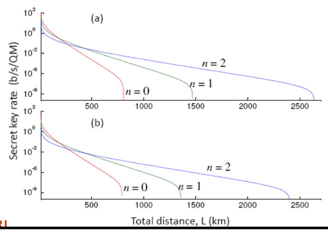


$$C = \frac{g^2}{\kappa\gamma}$$

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:

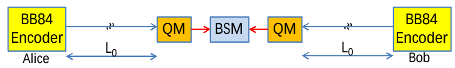




[Lo Piparo & Razavi, IEEE JSTQE 2015; arXiv:1407.8025]

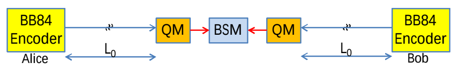
Summary

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

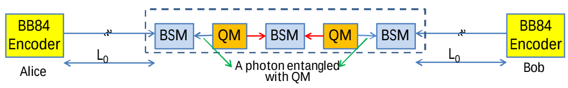


Summary

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

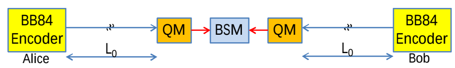


SETUP B: Relaxes the heralding requirement; cannot work with ensemble-based memories

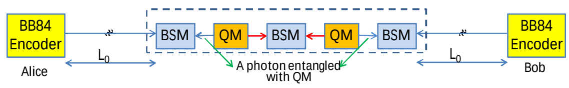


Summary

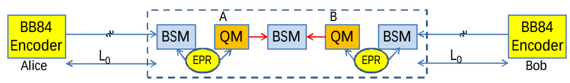
SETUP A: offers better rate-vs-distance behavior; requires heralding memories, with short access times and large storage-BW products



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

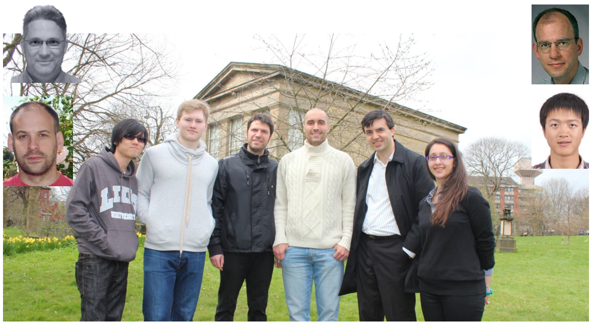
- 3 years of funded PhD research with annual salaries > €43k and research budget > €60k per student
- Dedicated schools on QKD and quantum networks + complementary-skill training + extensive internship/placement programmes
- Eligibility: meeting mobility criterion + being an early-stage researcher
- 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 *F Brussieres*
- **Telecom ParisTech:** 1 project on Hybrid CV QKD; *R Alleaume*
- **Toshiba Research Europe Ltd:** 2 projects on MDI-QKD and Integration; *A Shields*
- **University of Dusseldorf:** 2 projects on repeaters and multipartite 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* (**Coordinator**)
- **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; *M Curty*
- Plus collaborative partners at **BBN**, **Heriot-Watt**, **Inria**, **IQC**, **Madrid**, **Max Planck** & **NTT**

Thank You



SEVENTH FRAMEWORK PROGRAMME

QUANTUM COMMUNICATIONS HUB

PEOPLE