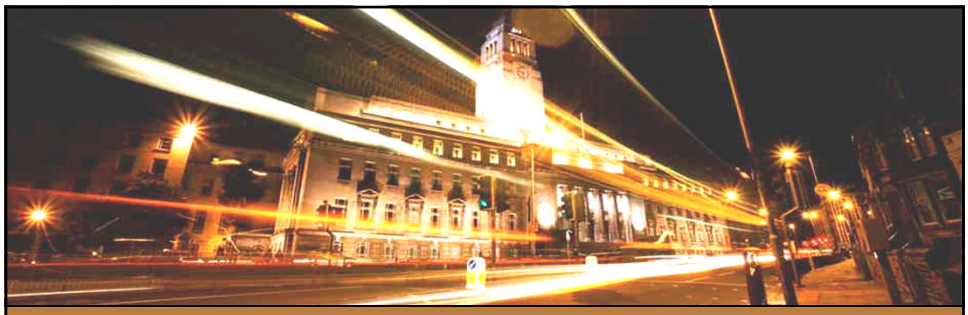


5 September 2014

Reaching beyond existing QKD links: how to take advantage of *imperfect* quantum memories

Nicoló Lo Piparo[1], Christiana Panayi[1], Mohsen Razavi[1], Xiongfeng Ma[2], and Norbert Lütkenhaus[3]

[1]School of Electronic and Electrical Engineering, University of Leeds
[2]Institute for Interdisciplinary Information Sciences, Tsinghua University
[3]Institute for Quantum Computing, University of Waterloo

Quantum Memories Wanted!

Quantum Memories in Action!

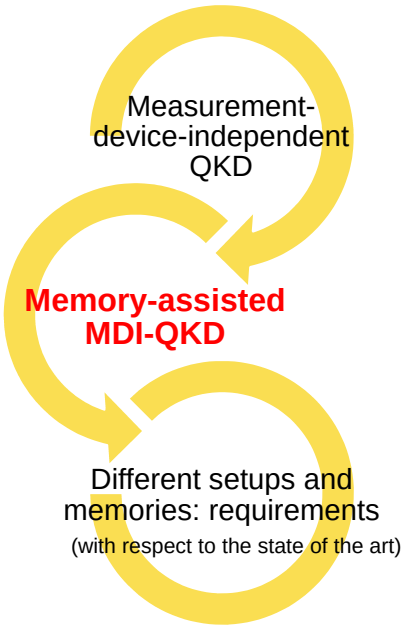
But, do we have such a memory?

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



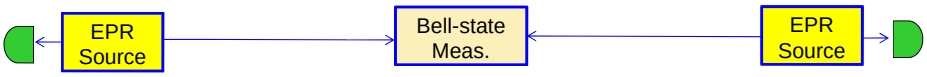
Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol

Measurement-Device-Independent QKD (MDI-QKD)

- EPR Protocol

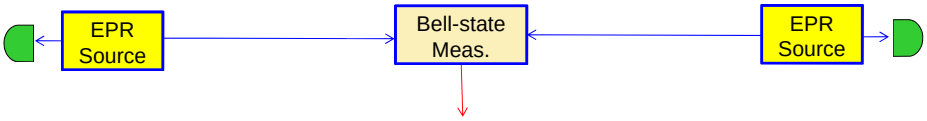
- Entanglement Swapping Protocol



Measurement-Device-Independent QKD (MDI-QKD)

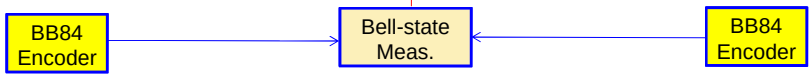
- EPR Protocol

- Entanglement Swapping Protocol



- Reverse EPR protocol

Untrusted → Meas-Device Independent

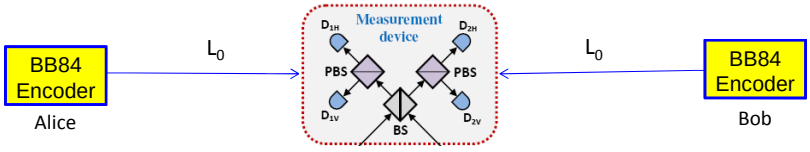


[Biham, Huttner & Mor, PRA **54,** 2651 (1996)]

[Lo, Curty & Qi, PRL **108,** 130503 (2012); Braunstein & Pirandola, PRL **108,** 130502 (2012)]

Measurement-Device-Independent QKD (MDI-QKD)

Untrusted



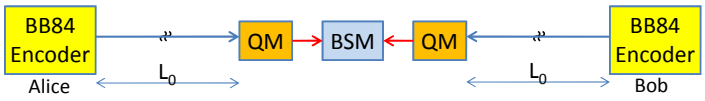
[Lo, Curty, & Qi, PRL **108,** 130503 (2012)]

- 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



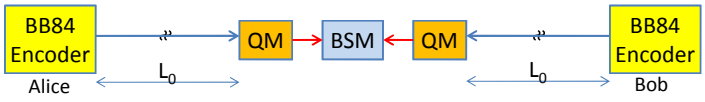
QM: Quantum Memory
BSM: Bell-state Measurement

[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

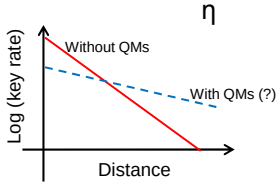


QM: Quantum Memory
BSM: Bell-state Measurement

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

- Expected benefit: better rate-vs-distance behaviour

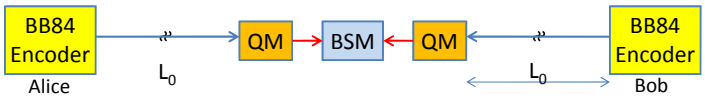
$$\text{Key rate} \propto \underbrace{\exp(-\alpha L_0)}_{\eta}$$



FACULTY OF ENGINEERING UNIVERSITY OF LEEDS

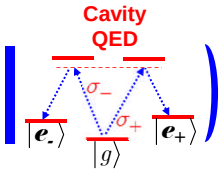
Memory-Assisted MDI-QKD

- 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?

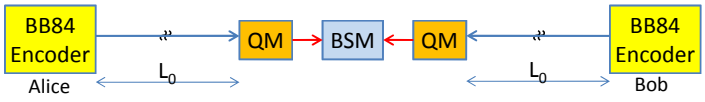


T_2 : *dephasing time constant in* $|e_+\rangle - |e_-\rangle$ *space*

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:



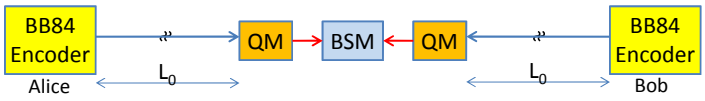
QM: Quantum Memory
BSM: Bell-state Measurement

- 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		

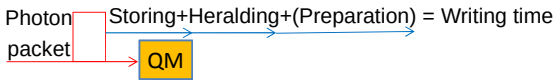
Writing time

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



QM: Quantum Memory
BSM: Bell-state Measurement

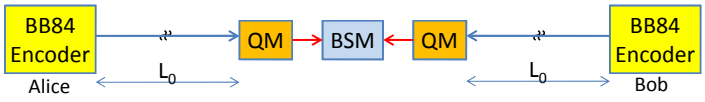
- Writing time: The time it takes for a single photon at the memory input to be stored into the QM, and we get to know about it



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

Memory-Assisted MDI-QKD

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



QM: Quantum Memory
BSM: Bell-state Measurement

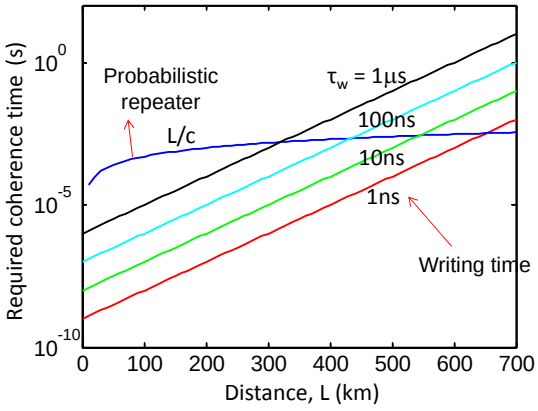
- What is the advantage over quantum repeaters? Simpler @ the user end &

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

For fast memories, milder requirements on coherence time

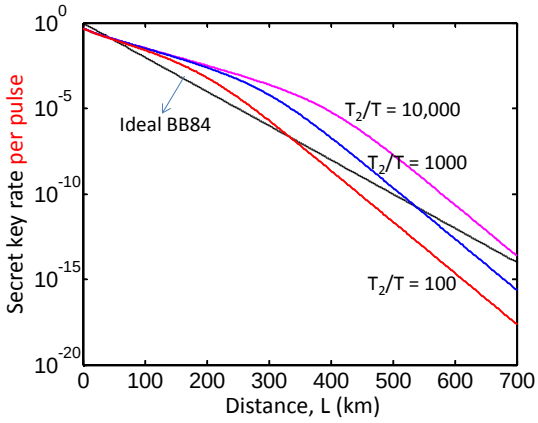
Memory-Assisted MDI-QKD

- Promise: milder requirements (than that of quantum repeaters) on the coherence time, if memories have short access times



Memory-Assisted MDI-QKD: SETUP-A Requirements

- If dephasing (T_2) was the only source of error:

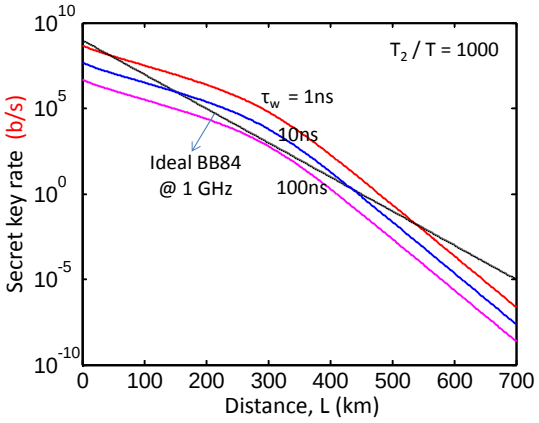


T = repetition period ≥ Writing time

- Conclusion: we need memories with large storage-bandwidth products

Memory-Assisted MDI-QKD: SETUP-A Requirements

- If dephasing (T_2) was the only source of error:

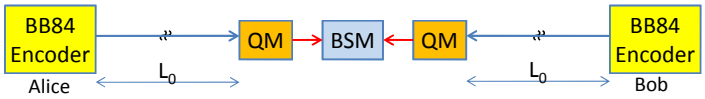


T = repetition period = Writing time

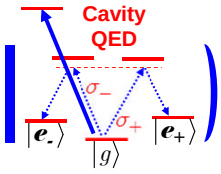
- Conclusion: again, we need short access times

Memory-Assisted MDI-QKD: Heralding Schemes

- In SETUP A, QMs need to be heralding:

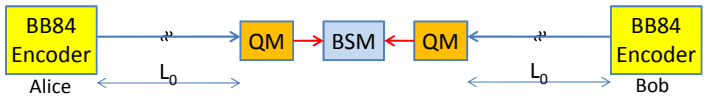


- Direct heralding is typically slow (~ms). Can we avoid it?

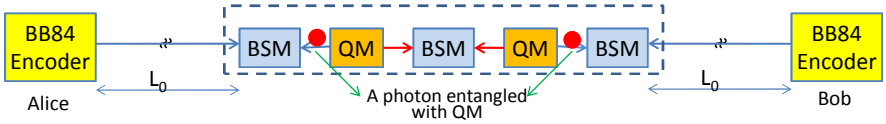


Memory-Assisted MDI-QKD: Heralding Schemes

- In SETUP A, QMs need to be heralding:



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

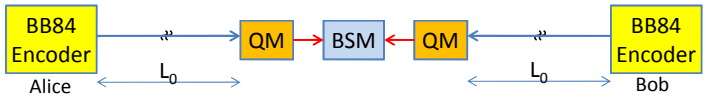


SETUP B:

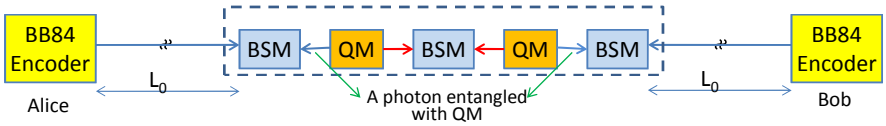
- Entangle a photon with the QM
- Use this photon to teleport the incoming state to the QM

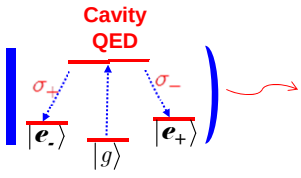
Memory-Assisted MDI-QKD: Heralding Schemes

- In SETUP A, QMs need to be heralding:

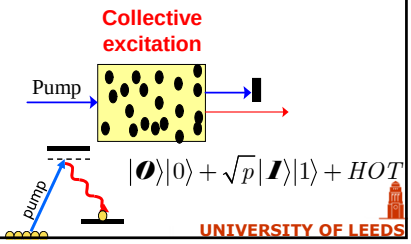


- Direct heralding is typically slow (~ms). Can we avoid it?





$$|e_-\rangle|\sigma_+\rangle + |e_+\rangle|\sigma_-\rangle$$

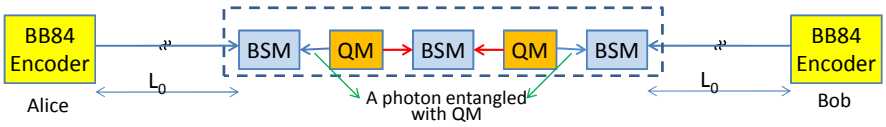


$$|0\rangle|0\rangle + \sqrt{p}|1\rangle|1\rangle + HOT$$

FACULTY OF ENGINEERING UNIVERSITY OF LEEDS

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*

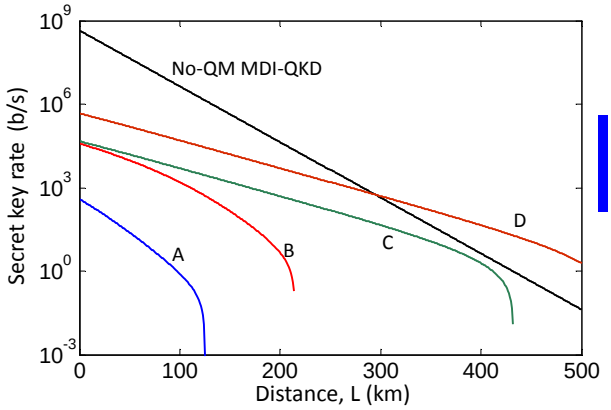


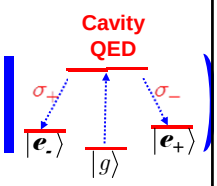
- We find the achievable key rate under the normal mode of operation, where there are no eavesdroppers. More details at

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

[arXiv:1407.8016]

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

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]

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

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

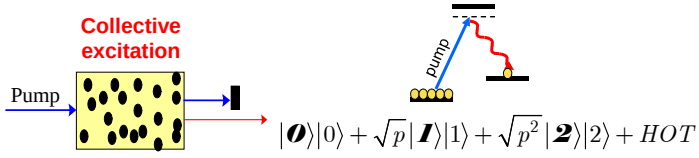
Erhan Saglamyurek, Neil Sinclair, Jeongwan Jin, Joshua A. Slater, Daniel Oblak, Félix Bussières, Mathew George, Raimund Ricken, Wolfgang Sohler & Wolfgang Tittel

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

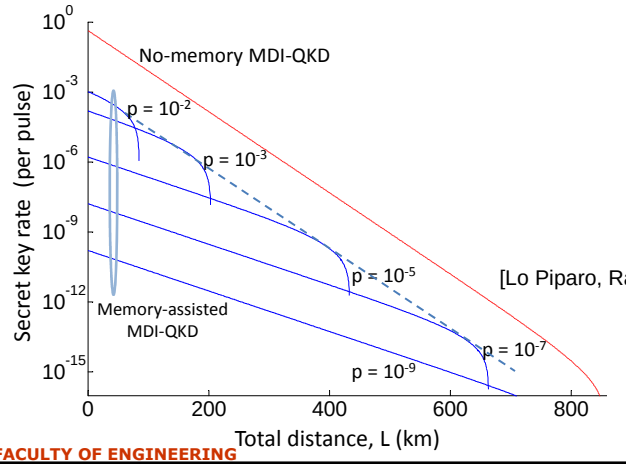
The reversible transfer of quantum states of light into and out of matter constitutes an important building block for future applications of quantum communication: it will allow the synchronization of quantum information[1], and the construction of quantum repeaters[2] and quantum networks[3]. Much effort 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

FACULTY OF ENGINEERING UNIVERSITY OF LEEDS

MDI-QKD with Atomic Ensembles in SETUP B



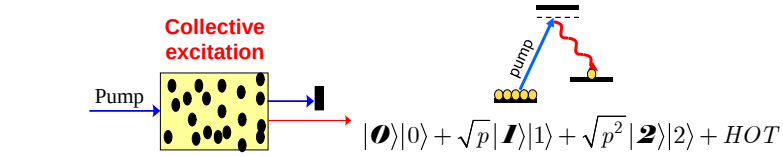
$$|\boldsymbol{0}\rangle|0\rangle + \sqrt{p}\,|\boldsymbol{1}\rangle|1\rangle + \sqrt{p^2}\,|\boldsymbol{2}\rangle|2\rangle + HOT$$

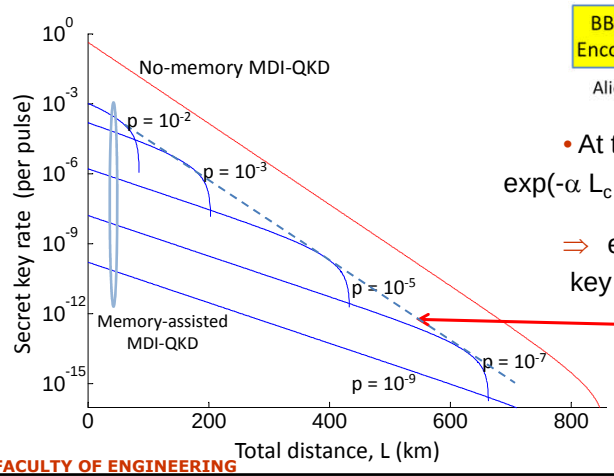


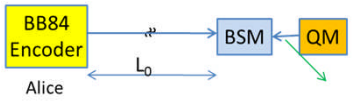
[Lo Piparo, Razavi & Panayi, arXiv:1407.8016]

FACULTY OF ENGINEERING UNIVERSITY OF LEEDS

MDI-QKD with Atomic Ensembles





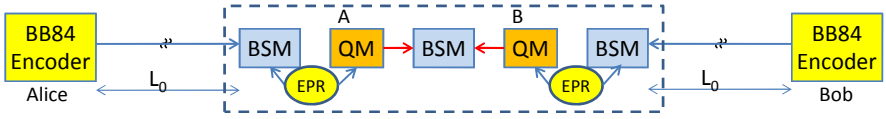


• At the cut-off distance L_c:
$\exp(-\alpha L_c/2) \times p$ is comparable to p^2

$\Rightarrow$ $\exp(-\alpha L_c/2) \propto p \Rightarrow$
key rate $\propto \exp(-\alpha L_c/2)\, p$
$\propto \exp(-\alpha L_c)$

Memory-Assisted MDI-QKD: SETUP C

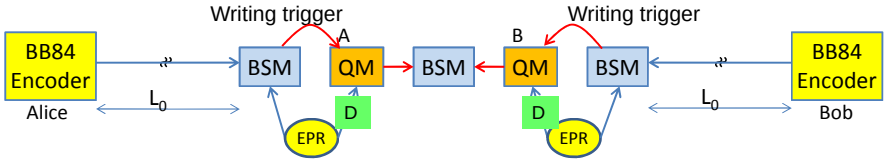
- An alternative (indirectly) heralding scheme: SETUP C



- 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 ($\rightarrow$ 1GHz)

Memory-Assisted MDI-QKD: SETUP C (modified)

- An alternative (indirectly) heralding scheme



- One great possibility: delayed writing!

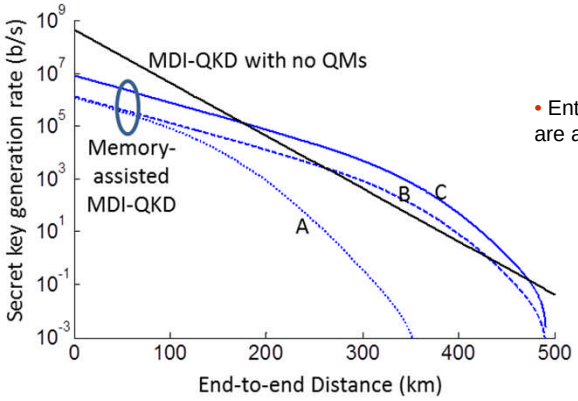
Only write to the memory if the side-BSM is successful
We need to delay one of the EPR photons for a short time

→ 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:
coherence time = 1.5 μs →
Writing/reading time = 300 ps
Entangling efficiency = 0.12
Retrieval efficiency at no decay = 30%

Curve B:
150 μs

Curve C:
150 μs
→
73%

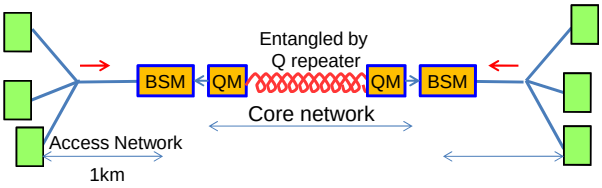
• available today!

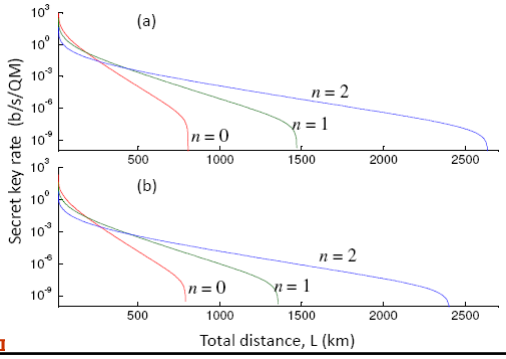
All curves: QE = 93%; Dark count = 1/s; Repetition rate: 1 GHz; writing eff = 1

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

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:

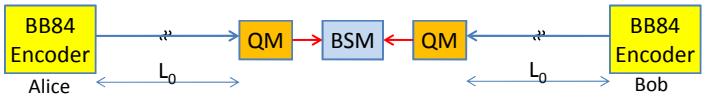




[Lo Piparo & Razavi, arXiv:1407.8025]

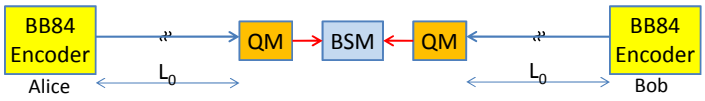
Summary

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

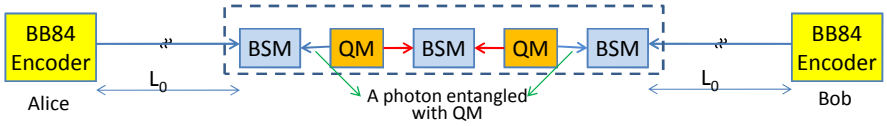


Summary

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

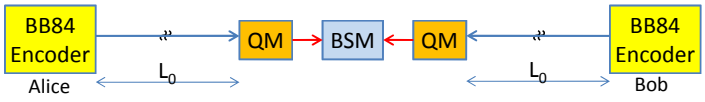


SETUP B: Relaxes the heralding requirement; cannot work with ensemble-based memories

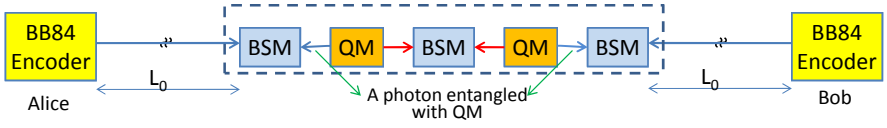


Summary

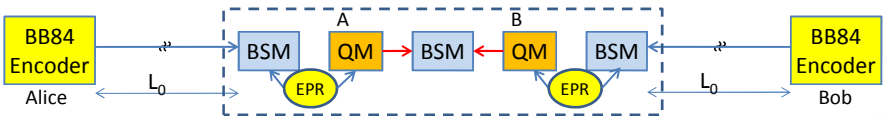
SETUP A: offers better rate-vs-distance behavior; requires heralding memories, with short access times and large storage-BW products



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 if good EPR sources are available



FACULTY OF ENGINEERING
UNIVERSITY OF LEEDS

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.

Thank You!