Toward feasible long-distance quantum communications systems

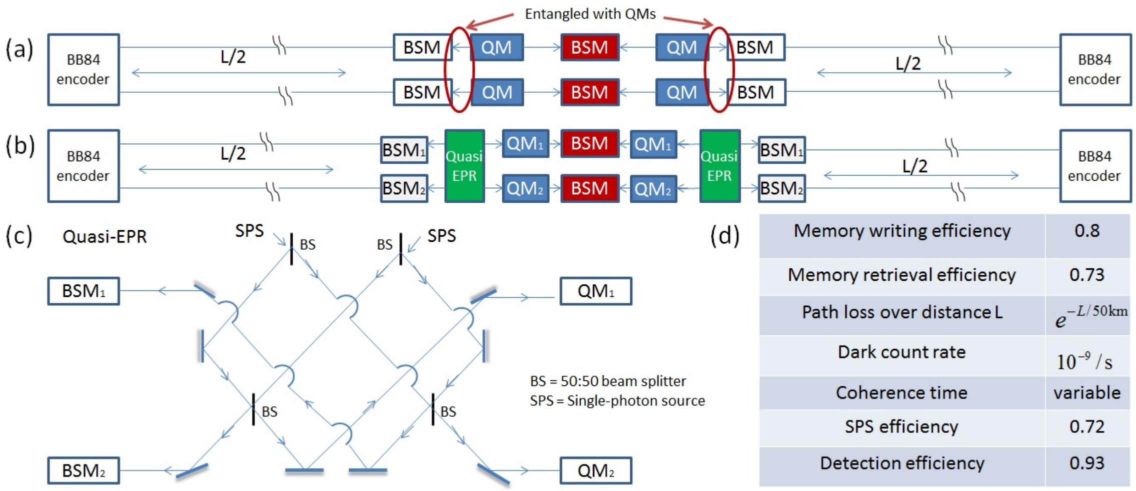
Nicoló Lo Piparo,[1] Mohsen Razavi,[1] and William J. Munro[2]

[1]School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK.
[2]NTT Basic Research Laboratories, NTT Corporation, Atsugi, Japan.

Memory-assisted measurement-device-independent quantum key distribution (MA-MDI-QKD) aims to improve the rate-versus-distance behavior of QKD systems by using the existing technologies [1]. While quantum repeater systems, as the ultimate solution to long-distance quantum communications, are still too challenging to be implemented, MA-MDI-QKD presents a feasible middle step toward the realization of long-distance QKD. Here, we summarize the progress with MA-MDI-QKD and propose two new MA-MDI-QKD schemes, where one relies on single-photon sources (SPSs) and ensemble-based memories, and the other uses nitrogen-vacancy (NV) centers in diamond embedded into cavities. We calculate the secret key rates for both schemes and compare them with conventional no-memory schemes. We show that, by using the state-of-the-art devices, we can potentially beat existing QKD schemes in reach and rate.

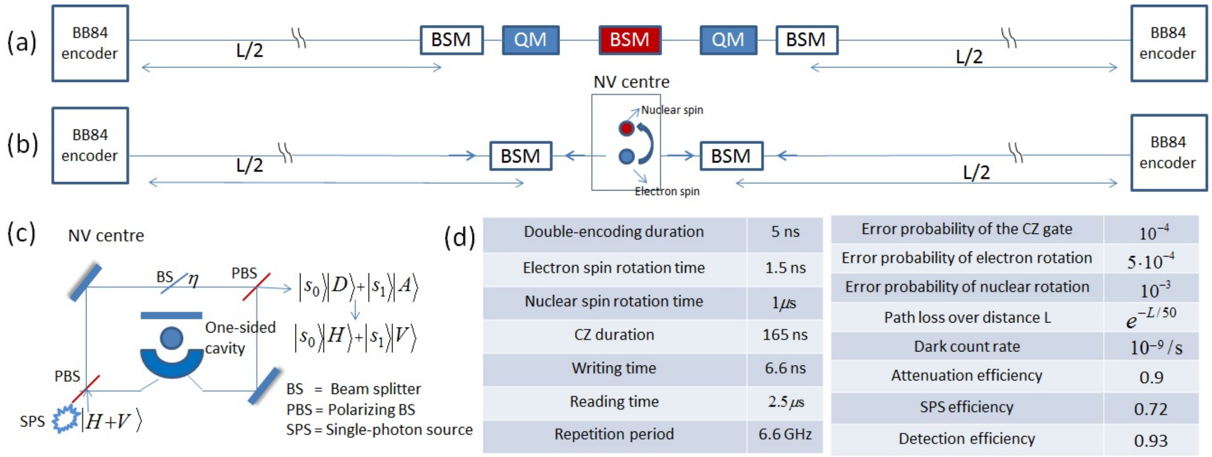
A typical MA-MDI-QKD scheme resembles a single-node quantum repeater setup with quantum memories (QMs) only in the middle site: see Fig. 1(a) for the phase-encoding scheme and Fig. 2(a) for the polarization-encoding scheme. In these schemes, both users encode a photon in one of the four BB84 states and send it to a middle station. The photons interact with other photons entangled with the QMs in the side Bell-state measurement (BSM) modules. A successful side BSM will ideally teleport the users' states into the corresponding QMs. Once all QMs are loaded with the relevant states, they are read out and a central BSM is performed on the retrieved photons, creating, thus, a correlated pair of bits between the users. The preliminary work in [1] shows that the QMs in use must meet certain criteria, such as having a high bandwidth-storage product and fast entangling times [1]. Both these conditions are met by ensemble-based QMs [2]. However, the conventional entangling procedure for such QMs will lead to multiple excitations, which have been shown to be detrimental for the performance of the system [3]. A remedy to this problem, proposed in [3], was to use a nearly ideal EPR source for creating the initial QM-photon entanglement. The ideal is that if we have an EPR source, which ideally generates only one pair of photons per trigger, and if we can store one of these photons efficiently into a QM, we do not need to worry about multiple excitation issues. The other benefit is that we only need to write into QMs if the corresponding side-BSM is successful. This further reduces the requirements on the access times to QMs.

In this paper, we propose two alternative solutions to the multiple-excitation problem. Our first solution implements the EPR idea, mentioned above, by using SPSs. The possible advantage is that it is easier to generate a good SPS rather than a good EPR source. Our second solution relies on using NV centers in diamond, rather than atomic ensembles, which, if embedded into cavities, would resemble trapped single atoms immune to multiple excitations. We have already studied an MDI-QKD system with NV centers [4]. Here, we enhance that structure and propose a setup that only requires one NV center unit. The key enabling idea is to use both electronic and nuclear spins in NV centers to store qubits. This way, considering the long coherence time of nuclear spins, the system would also be immune to decoherence issues.



Memory writing efficiency	0.8
Memory retrieval efficiency	0.73
Path loss over distance L	$e^{-L/50\text{km}}$
Dark count rate	10^{-9} /s
Coherence time	variable
SPS efficiency	0.72
Detection efficiency	0.93

Figure 1: (a) Phase-encoding MA-MDI-QKD scheme with indirectly heralding QMs. (b) The proposed scheme relying on quasi-EPR modules sketched in (c). (d) The nominal values of the parameters used.



Double-encoding duration	5 ns	Error probability of the CZ gate	10^{-4}
Electron spin rotation time	1.5 ns	Error probability of electron rotation	$5\cdot10^{-4}$
Nuclear spin rotation time	$1\mu s$	Error probability of nuclear rotation	10^{-3}
CZ duration	165 ns	Path loss over distance L	$e^{-L/50}$
Writing time	6.6 ns	Dark count rate	$10^{-9}/s$
Reading time	$2.5\mu s$	Attenuation efficiency	0.9
Repetition period	6.6 GHz	SPS efficiency	0.72
		Detection efficiency	0.93

Figure 2: (a) Polarization-encoding MA-MDI-QKD scheme with indirectly heralding QMs. (b) The proposed scheme with one NV center as the only QM relying on the double-encoding scheme sketched in (c). (d) The nominal values of the parameters used.

Figure 1(b) shows the dual-rail phase-encoded version of our proposed MA-MDI-QKD system that relies on SPSs. The entangling operation is done in the boxes labeled quasi-EPR, shown in Fig. 1(c). Here, two SPSs each generate ideally one photon that interfere at four 50:50 beam splitters. Due to the specific interaction pattern illustrated in Fig. 1(c), we can create an entangled photon pair plus some spurious terms. These spurious terms include four two-photon Fock states, each at every output of Fig. 1(c). Two of the output ports will be directed towards the BSM modules and the other two to the QMs, where the latter will be stored into the QMs.

In our second solution, we use a different type of QMs, which do not, in principle, suffer from multiple excitations: NV centers in diamond. This type of QMs has already been considered in [4] in the polarization-encoded MA-MDI-QKD scheme of Fig. 2(a). In [4], the authors show that, by embedding NV centers in cavities, it is possible to beat the no-memory systems. Despite these encouraging results, one limitation of using such memories derives from the low coherence time of the electron spin of the NV center, which reduces the security distance [4]. Here, we propose to use the nuclear spin of an NV center as a QM, as it has a much longer coherence time [5]. Our new protocol works as follows, see Fig. 2(b). In each round, Alice and Bob encode their photons and send them toward the middle site. The electron spin is then entangled with a single photon via the module shown in Fig. 2(c). The entangling procedure is made through the specific reflection properties of the cavity containing the NV center depending on its electron spin state, as described in [6]. Such entangled NV-photon states will, in one round, interact with the photon sent by Alice and, in the other round, with that of Bob. Once one of the side-BSMs is successful, the state of the corresponding user is ideally teleported to the electron spin. At this stage, the electron spin is transferred into the nuclear spin. Then, we initialize the electron spin again and continue with loading it with the photons from the other user. Once the electron spin is loaded for the second time, a deterministic BSM on the joint electron-nuclear spin state is performed [6].

The above protocol has several advantages over the two-QM module in Fig. 2(a) proposed in [4]. First, by using only one physical QM, the system offers a less complex setup than that with two QMs, which possibly makes its implementation easier. Secondly, in this new scheme, only the nuclear spin is used for storage, which is known to have a long coherence time. This makes our scheme extremely resilient to the decoherence effect. Finally, by using a deterministic, rather than probabilistic, BSM in the middle BSM, the success rate is further enhanced.

We have calculated the secret key rate of the setups of Fig. 1(b) and Fig. 2(b) by considering the main sources of errors in each setup. With regard to the setup of Fig. 1(b), the main source of error is due to the coherence time of the QM, T_1. In fact, the other source of error, due to the spurious terms generated in the setup of Fig. 1(c), do not strongly affect the overall performance of the system. That is due to the fact that when the two-photon Fock states generated by the quasi-EPR modules are directed towards the QMs, no photons will interact with the state sent by the users. Therefore, the side-BSM can be successful only through a dark count event. Similarly, when the two-photon Fock states are directed towards the side-BSM, a vacuum state will be loaded into the QMs, which would not result in a successful central-BSM, unless again because of the dark count. With a dark count rate as low as 10^{-9}/pulse, the corresponding errors will be low at short-to-moderate distances.

With regard to the setup of Fig. 2(b), we consider several practical issues. The first one is the timing of the protocol. In this scheme, in order to do the entangling operation in Fig. 2(c), we have to initialize the electron spin. This corresponds to the writing time parameter in Fig. 2(d), and it also determines the repetition rate of our protocol. Furthermore, the time that it takes to initialize the nuclear spin, to transfer the electron spin to the nuclear spin, and eventually the time that it takes to perform the final BSM must be accounted for in every successful loading. The latter time parameters would add up to about 2 μs, which slow down the protocol for short distances, but eventually become negligible at large

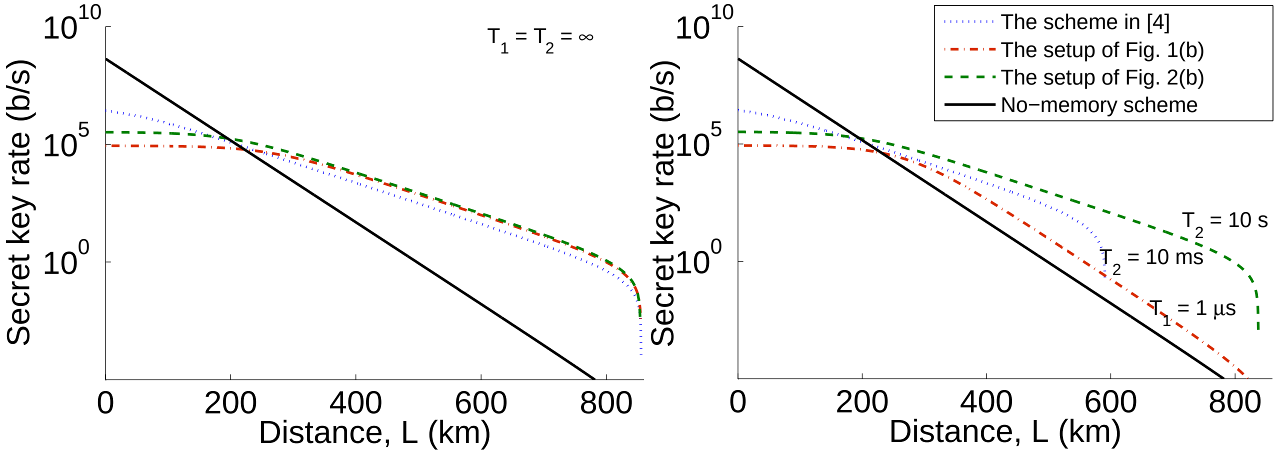


Figure 3: Key rate comparison of the system described in [4] with the systems in Fig. 1(b) and in Fig. 2(b) and with the no-memory MDI-QKD system [8] with (a) no decoherence and (b) for finite values of the coherence times T_1 and T_2.

distances. In our key rate analysis we have considered all these timing issues. The second issue is the errors that occur because of the decoherence of the nuclear spin, modeled by a depolarizing channel with time constant T_2. Moreover, we consider the errors associated to the operations needed to transfer the electron spin into the nuclear spin and to perform the deterministic BSM. In our key rate analysis, we account for the time needed for each operation as reported in [7], as well as for the errors in all required operations.

Figure 3(a) shows the comparison of secret key rates of the setups of Fig. 1(b) and Fig. 2(b) with the secret key rate of the protocol described in [4], all with an infinitely high coherence time, and with that of a conventional no-memory system [8]. All the MA-MDI-QKD schemes outperform the no-memory system for distances roughly above 200 km. The QM-assisted schemes differ in the initial rate values. This is mainly due to the difference in their writing times. In fact, the system with two NV centers has the lowest writing time equal to the initialization of the NV centers. This will correspond to a higher key rate for short distances. For higher distances all the QM-assisted systems show a similar behavior. Then, we have calculated the key rates of these schemes by considering a finite coherence time for each scheme, as shown in Fig. 3(b). In this case, the low coherence time of the electron spin of the NV center affects the security distance of the scheme proposed in [4], which is roughly 600 km at $T_2 = 10$ ms. A similar effect can be noticed for the setup of Fig. 1(b). In this case, Fig. 3(b) shows that this setup outperforms the no-memory system at a distance $L \sim 200$ km for a coherence time as low as to $T_1 = 1$ μs. However, after this point, the slope of the curve has almost the same value as that of a no-QM system. On the contrary, the key rate of the setup of Fig. 2(b) shows a much better rate versus distance behavior compared to the no-memory system, up to distances as high as 800 km. This is due to the high coherence time of the nuclear spin of the NV centers.

The required specifications for our proposed systems are mostly within reach of existing technologies. Ensemble-based memories have shown to have fast writing times, needed for high repetition rate, on the order of 300 ps, and coherence times on the order of 1 μs [9]. SPSs based on quantum dots in photonic nanowires also reach an efficiency of 0.72 [10] and are known to have very low two-photon components. For NV centers, nuclear coherence times of over a second has been reported in [5], while progress is being made toward cavity-enhanced NV centers. With such state-of-the-art devices, our scheme can lead to three orders of magnitude rate improvement at distances over 400 km, over existing no-memory QKD systems. This will provide us with a feasible approach to the next, memory-assisted, generation of QKD networks and sets an achievable intermediate milestone for long-distance QKD. This work was partly funded by the UK's EPSRC Grant EP/M013472/1.

References

[1] C Panayi, M. Razavi, X. Ma, and N. Lütkenhaus. *New. J. Phys.*, 16:043005, 2013.

[2] R. M. Camacho, P. K. Vudyasetu, and J. C. Howell. *Nat. Photon.*, 3:103–106, 2009.

[3] N. Lo Piparo and *et al. IEEE J. of Selected Topics in Quantum Electron.*, 21:6601010, May 2015.

[4] N. Lo Piparo, M. Razavi, and W. J. Munro. *arXiv:1603.03623*, 2016.

[5] P. C. Maurer and *et al. Science*, 336:1283, 2012.

[6] K. Nemoto and *et al. Phys. Rev. X*, 4:031022, 2014.

[7] M. S. Everitt, S. Devitt, W. J. Munro, and K. Nemoto. *Phys. Rev. A*, 89:052317, 2014.

[8] H.-K. Lo, M. Curty, and B. Qi. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[9] K. F. Reim and *et al. Phys. Rev. Lett.*, 107:053603, 2011.

[10] J. Caudon and *et al. Nat. Photon.*, 4:174–177, 2010.