# Reconfigurable network for quantum digital signatures mediated by measurement-device-independent quantum key distribution

G. L. Roberts,[1] M. Lucamarini,[1, *] Z. L. Yuan,[1] J. F. Dynes,[1] L. C. Comandar,[1]
A. W. Sharpe,[1] A. J. Shields,[1] M. Curty,[2] I. V. Puthoor,[3] and E. Andersson[3]

[1] *Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, United Kingdom*
[2] *EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[3] *SUPA, Institute of Photonics and Quantum Sciences,*
*Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

Quantum key distribution (QKD) aims to provide an unconditionally secure means of communication between distant parties. Its recent measurement-device-independent (MDI) version greatly enhances the security of the implementation, by removing Eve's ability to attack the detection unit. Here we introduce and experimentally realise a novel reconfigurable quantum network that connects three parties with only two optical links and allows switching between QKD and MDI-QKD in real time. This structure brings about an interesting security model, where the central node of the network can be either trusted or untrusted depending on its role in the communication protocol. The enriched functionality of the network is demonstrated by extracting the first quantum digital signature (QDS) rates mediated by MDI-QKD. In doing so, we adopt a novel treatment of the finite-size effect that greatly improves the QDS rate, especially in the case of a limited sample size.

In standard QKD protocols [1], two trusted parties, Alice and Bob, distill an encryption key by exchanging photonic qubits through a direct optical channel. Alice is configured as transmitter and Bob as receiver in this communication scheme. On the other hand, in MDI-QKD [2, 3], Alice and Bob are both transmitters and a third, generally untrusted, party (Charlie) acts as the receiver. However, Charlie is not doomed to remain forever untrusted. He can also act as a trusted party in a quantum communication protocol, as we show here.

The scheme in the top diagram of Fig. 1 represents a basic, newly proposed, reconfigurable network[1] that combines QKD and MDI-QKD in a single setup and makes it possible to switch between the two in real time. When QKD is enabled, Charlie is a trusted receiver who can distill encryption keys with Alice or Bob. On the contrary, when MDI-QKD is active, Charlie acts as an entirely untrusted node connecting Alice to Bob.

The way to switch between QKD and MDI-QKD is described in the caption of the top diagram in Fig. 1. It relies on two intensity modulators (IM) owned by Alice and Bob, which cut the optical links with Charlie by attenuating the intensity of the pulses directed to him. When this happens, only QKD is possible, as MDI-QKD requires that both Alice's and Bob's pulses interfere on Charlie's beam splitter. Because the users independently control their IMs, they do not actually know whether QKD or MDI-QKD is enabled in a given run, and they find it out only during the public discussion that follows the exchange of the quantum signals. One should note that the IMs are already present in the typical decoy-state [5, 6] layouts of QKD and MDI-QKD. Therefore it is not necessary to add extra components to realise the reconfigurable network.

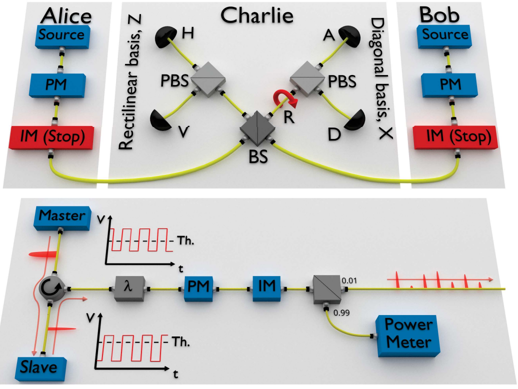

FIG. 1. *Top* – Fiber-based reconfigurable network. The key elements are coloured red. The rotator (R) in Charlie's station sets each detector to measure a different polarization state, H, horizontal, V, vertical, D, diagonal, and A, anti-diagonal. The intensity modulators (IMs) can be set to high attenuation, to nearly stop the light passing through them (Stop in the figure). This can enable Alice-Bob MDI-QKD, when no IM is set to Stop, or Alice-Charlie QKD, when Bob's IM is set to Stop, or Bob-Charlie QKD, when Alice's IM is set to Stop. At the same time, the IMs can be used to prepare decoy states [5, 6]. PM: polarization modulation; BS: beam splitter; PBS: polarizing beam splitter. *Bottom* – Transmitting module. The depicted optically-seeded light source is used by both Alice and Bob to transmit light pulses to Charlie. Master and slave lasers' driving signals are displayed alongside the equipment and are set differently for the two lasers. A power meter connected to the output beam splitter is used to set the intensity of the outgoing optical pulses to the correct level. The wavelength filter (λ) is for enhancing the indistinguishability of Alice's and Bob's photons.

The equipment used in the transmitting modules is described in the caption of the bottom diagram in Fig. 1. It includes our recently introduced optically-seeded laser source, to enhance the two-photon interference necessary

[1] For a free-space reconfigurable network see [4].

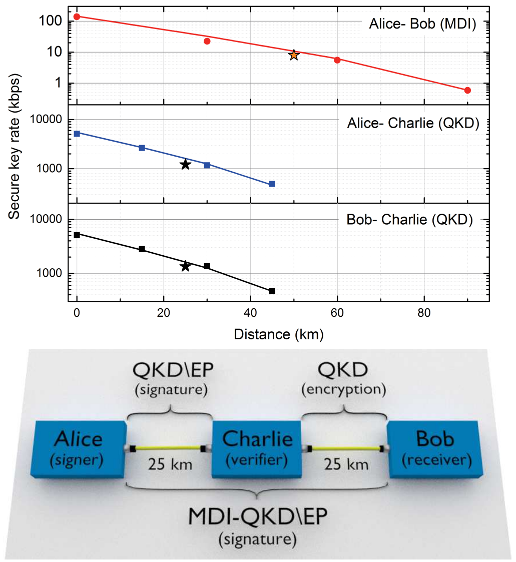

FIG. 2. *Top* – Secure key rates versus distance. MDI-QKD (top diagram) and QKD (centre and bottom diagrams) secure key rates for a Z(X) basis probability equal to 80%(20%) and a security parameter $\epsilon_{\rm sec} = 10^{-10}$ are shown as a function of distance. All the distances have been calculated assuming 0.2 dB/km attenuation on the channel, except for the data points indicated by stars, where a real fiber was used. The projected time to attain the shown key rates is 25 hours of which 3 minutes are spent on QKD and the rest on MDI-QKD. *Bottom* – MDI-QKD-mediated QDS. The signature is sent by Alice to Bob using an MDI-QKD setup, over an optical fiber with a total length of 50 km. The protocol is denoted "MDI-QKD\EP", where "\EP" stands for "*without error correction and privacy amplification*". QKD\EP is used to send a signature from Alice to Charlie, whereas full QKD is used to distribute keys between Bob and Charlie. The QKD links are implemented on two 25-km reels of single-mode fiber.

for MDI-QKD [7]. With this setup, we run an experiment to extract the typical key rates of the reconfigurable network. The results are shown in Fig. 2.

We used optical attenuators as the quantum channel, shown in the figure by circles (squares) for the MDI (QKD) link, and also performed the experiment over two 25 km reels of standard optical fibre, shown by stars. The solid lines give the theoretical simulations, which are in excellent agreement with the experimental results. The MDI-QKD key rates are between 134 kbps at an equivalent distance slightly above 0 km, and 606 bps for 90 km. QKD is faster, giving key rates from 5 Mbps at 0 km to around 0.5 Mbps at 45 km.

To show the enhanced functionality of the reconfigurable network, we employed it to demonstrate the first QDS rates [8] mediated by MDI-QKD[2]. QDS allow users to sign a document by quantum means and then transfer it to other users with information-theoretical security. Even in the simplest case, a QDS scheme involves at least three parties [10–12], as depicted in the bottom diagram of Fig. 2. Therefore, MDI-QKD alone or a pair of QKD systems would not suffice to implement it, whereas it becomes feasible in a network configuration.

The real fiber link was used to determine the QDS rates possible using this system. About 45 seconds and 72 ms were required, on average, to acquire enough signature material to sign one bit with the MDI-QKD protocol over 50 km of optical fiber and with the QKD protocol over 25 km of optical fiber, respectively. To increase the efficiency of the distillation, we have introduced an original treatment of the finite-size effect, where multiple signatures were distilled from the same block of data, thus alleviating the detrimental effect of statistical fluctuations. All details are presented in the supplementary section of the Technical Abstract [8].

The reconfigurable network used here to extract encryption key and signature rates features distinctive scalable advantages. For example, it allows $N$ parties to communicate through an untrusted central node using only $N-1$ optical links, as opposed to the $N(N-1)/2$ direct links required in a standard network. The achieved secure key and signature rates are comparable to or higher than those in the state of the art [13–15], which is especially notable when considering that they have been distilled in the finite-size scenario from a setup that includes an MDI-QKD link. Given the widespread use of encryption and signatures in today's society, we believe that this work constitutes an important step for the deployment of quantum communication networks.

[2] For a simultaneous submission of a related work, see [9].

* marco.lucamarini@crl.toshiba.co.uk

[1] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Comp. Syst. and Sign. Proc., Bangalore, India, pp. 175-179 (1984).
[2] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[3] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[4] B. Qi et al., 2015 IEEE Int. Conf. on Space Opt. Syst. and Appl. (ICSOS), New Orleans, LA, pp. 1-6 (2015).
[5] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[6] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[7] L. C. Comandar et al., Nat. Photon. **10**, 312 (2016).
[8] G. L. Roberts et al., eprint arXiv:1703.00493 (2017).
[9] H.-L. Yin et al., eprint arXiv:1703.01021 (2017).
[10] R. Amiri and E. Andersson, Entropy **17**, 5635 (2015).
[11] R. Amiri et al., Phys. Rev. A **93**, 032325 (2016).
[12] I. V. Puthoor et al., Phys. Rev. A **94**, 022328 (2016).
[13] P. J. Clarke et al., Nat. Commun. **3**, 1174 (2012).
[14] R. J. Collins et al., Phys. Rev. Lett. **113**, 040502 (2014).
[15] R. J. Collins et al., Opt. Lett. **41**, 4883 (2016).