Practical single-fibre network-oriented Quantum Key Distribution from a compact source of entangled photons in presence of White Rabbit time synchronisation

K.P. Schatz, B. Amies-King, S. Albosh, R. Kumar, and M. Lucamarini

School of Physics, Engineering & Technology and York Centre for Quantum Technologies, Institute for Safe Autonomy, University of York, York YO10 5FT, UK

ABSTRACT

We demonstrate the feasibility of a network-oriented Quantum Key Distribution (QKD) from affordable components, in the presence of White Rabbit time synchronisation on the same optical fibre. This allows for an optimal usage of resources, where optical networks are tailored for fast and accurate time distribution and lighter QKD systems exploit the network timing for synchronising the operations between distant users.

Keywords: Entanglement, Single Photons, Heralded Single Photon, Entangled Single-Photon Source, Quantum Communications, Quantum Key Distribution, White Rabbit, Optical Networks, Time Synchronisation

1. INTRODUCTION

Quantum communications technology, and QKD in particular, is headed for real-life applications, leveraging the existing optical infrastructure to create the foundations of the future quantum internet.[1] This requires not only compatibility of quantum and classical hardware, but can go as far as to demand coexistence of quantum and classical signals within the same fibre.[2–6]

One of the most fundamental features of any network, which is likely to be inherited unchanged by the future internet, is the synchronisation of the operations between its nodes. The central aspect of time distribution for the management of the information in an extended network has been caught by the researchers at CERN, who in 2011 introduced White Rabbit (WR) as a form of fast and precise time synchronisation over optical fibres.[7] Intriguingly, CERN is also the place where the World Wide Web was initially proposed.[8]

WR is an optical clock distribution scheme that achieves sub-nanosecond precision over tens of kilometres in optical fibre, with a jitter of the order of picoseconds. Remarkably, this is achieved with off-the-shelf plug-and-play inexpensive devices, which adds to the practicality of our proposal. Therefore, WR well matches the requirements in speed, precision, propagation medium and distance of modern QKD systems, which feature gigahertz clock rates over tens of kilometres in optical fibres.[9–12] Current QKD modules include sub-systems, sub-routines and often a separate optical channel to transmit the time information between the users, thus requiring additional hardware and software that increase complexity and cost of the modules. In the foreseeable future, optical networks will offer precise time distribution as a service. QKD suppliers could therefore leverage the network's timing capability to simplify their systems, reducing their cost but also the risk of quantum hacking based on manipulating the time information.[13,14]

In this perspective, prior work has shown the synchronisation of QKD systems by means of WR.[15] However, the demonstration was limited to using separate fibres for QKD and WR signals, thus leaving the question of their coexistence on the same fibre open. WR signals are launched with power in the region of $0.1 - 1$ mW, hence they can be considered 'classical'. These signals cause Rayleigh and Raman scattering which, in turn, introduce noise to the quantum transmission and affect the overall performance of QKD.

In this paper, we demonstrate the distribution of single photons suitable for QKD over kilometer-long optical fibres in the presence of the classical bidirectional WR communication, which takes place over the same fibre that carries the QKD photons. The demonstration is practical as it only includes affordable components. It

Correspondence to: K.P.S. (karolina.schatz@york.ac.uk), M.L. (marco.lucamarini@york.ac.uk)

uses a novel portable and ready-to-use source of entangled photons[16] as well as off-the-shelf wavelength division multiplexing (WDM) components, filters and detectors. The clock distribution is performed using the WR protocol and achieves sub-nanosecond precision. It will allow distant users to post-select correlated detection events in a real-life QKD implementation. The large bandwidth of the emitted photons and the network-oriented versatility of the WDMs are ideally suited to a network implementation with multiple users.

We measure the visibility in polarisation of the distributed photons and show that it remains suitable for QKD in the presence of WR signals. The measurements take place in a network configuration that mirrors existing optical networks in order to ease future deployment in the field. Our results show that the commercial source of entangled photons can coexist with the classical signals distributed in an optical WR network, with a minimal demand on customisation of the network's WDM and WR components.

2. METHODS AND RESULTS

Fig. 1(a) shows the schematics of the network-oriented QKD in presence of WR time distribution, as well as the experimental setup used to measure the correlations in polarisation of the distributed photons. The source of quantum light is a compact entangled photon source (EPS) commercialised by OZ Optics. It exploits type-0 spontaneous parametric down conversion (SPDC) from a 25 mm periodically-poled lithium niobate (PPLN) crystal to generate the following maximally entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_S |H\rangle_I + |V\rangle_S |V\rangle_I\right) = \frac{1}{\sqrt{2}}\left(|HH\rangle + |VV\rangle\right) \tag{1}$$

$|H\rangle_j = |0\rangle_j$ and $|V\rangle_j = |1\rangle_j$ are the eigenvectors of the Pauli Z matrix and S and I denote the signal and idler photons respectively. Signal and idler photons are produced symmetrically over 1560 nm, with a total bandwidth of approximately 60 nm, and separated by an internal dichroic mirror at 1565 nm. The source's second order autocorrelation function, frequency bandwidth and exact two-qubit state were characterised prior to this experiment; the optical spectrum of the EPS' signal and idler photons is shown in Fig 1(b).

The signal photons travel through a set of optical add-drop modules in preparation for the inclusion of additional classical signals and additional channel length. An off-the-shelf dense wavelength division multiplexing (DWDM) module, spanning the 100 GHz ITU grid channels 35 - 42 (1548.51 nm - 1543.73 nm), is used to reproduce a network of multiple users, each receiving a different wavelength channel from the source.[17] On the idler side, an optical tunable filter (OTF) is used to select photons corresponding to a particular signal DWDM channel. This solution allows the user receiving the idler photons (server) to selectively address a different user receiving signal photons (client). It also increases the practicality of the setup, because the OTF can dynamically compensate for the imperfections of the EPS. As an example, if the degenerate wavelength of the EPS drifted in the static ITU grid defined by WDMs placed on both the idler and the signal arms, the pairs of entangled photons would be directed to different WDM channels, causing a dramatic reduction of the coincidence rates. On the other hand, when an OTF is placed on one of the two arms, it can follow the change in wavelength of the EPS through the fixed WDMs thus maintaining a high coincidence count rate for the users.

The photon polarisation is analysed in the Z ($\{|H\rangle, |V\rangle\}$) and X ($\{|D\rangle, |A\rangle\}$) bases, as required for the 4-state BB84 protocol.[18] Our setup achieves this via the polarisation analysers (PA in Fig. 1(a)), which consist of fibre and free-space polarisation components. Within the analysers, a fibre-optic manual polarisation controller is used to compensate for any change in the polarisation state that occurs between the SPDC crystal and the analysing unit. The analyser then couples the light from fibre to free-space and measurement basis selection is performed via an appropriate set of quarter and half waveplates and a polarising beam splitter and/or linear polariser. The signal and idler photons are detected using InGaAs SPADs: a free-running ID220 by IDQuantique and a gated PDM detector by Micro Photon Devices. The signal detection is gated using the idler counts registered by the free-running detector to improve noise reduction. A quTAG Qutools time-tagger is used to record the coincidence counts between the two SPADs. In the laboratory setting, the SPAD's performance can be significantly improved by using the idler photon as a trigger and gating the signal photon detection. For distant users however, this practice is not feasible. A precise clock has to be distributed alongside the quantum signal to allow alignment of independent SPAD gating and post-selection of correlated events. This clock will be distributed via the

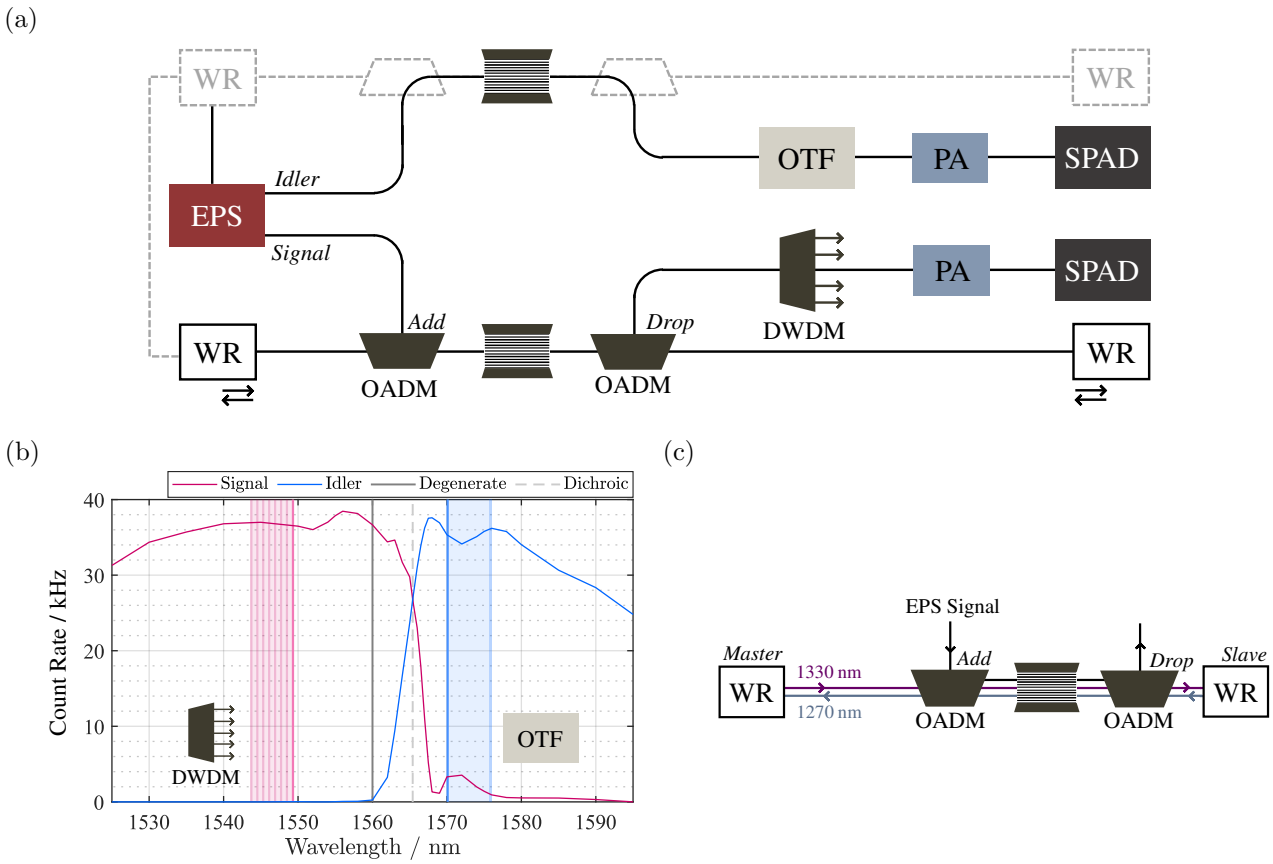
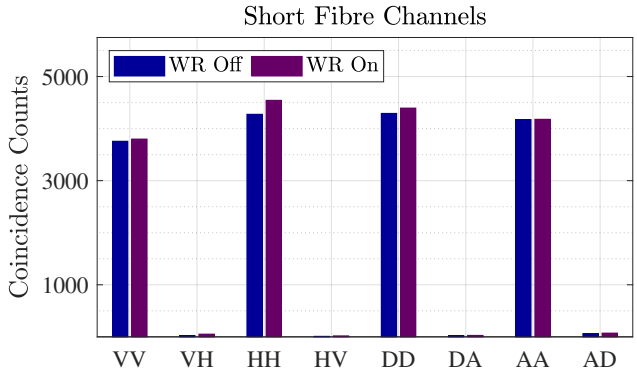


Figure 1. **Schematics of the network-oriented entanglement-based QKD multiplexed with WR time distribution.** (a) Setup for the distribution of WR time and polarisation-entangled photons. The entangled photon source (EPS) launches signal and idler photons through single-mode fibres (SMFs), optical add-drop multiplexers (OADM), spools of SMFs, a dense wavelength division multiplexer (DWDM) on one arm and an optical tunable filter (OTF) on the other arm, polarisation analysers (PAs) and a pair of single photon avalanche diodes (SPADs). The length of the fibre spool in each arm is a few meters and 1 km for the first and second experiment reported in this work, respectively. On the bottom arm, the light launched by the WR modules passes through the OADMs and is used to establish a common clock at the channel's end points. A similar scheme is drawn on the top arm, with the dashed lines and components not present in the experiments but indicative of the complete network structure. (b) Spectrum of the EPS signal and idler photons, measured using a SPAD placed after the OTF. The centre of the EPS spectrum (degenerate wavelength 1560 nm, $\sim$ Ch21 of the 100 GHz ITU grid) is shown, which is offset from the crossing wavelength of the signal and idler photons due to the fact that the dichroic mirror within the source is centred at $\sim$1565 nm. The channels of the DWDM and the corresponding wavelength range generated by the OTF are also highlighted, where the darker lines centred at 1549.32 nm and 1570.09 nm indicate the centre wavelengths used in this work. (c) Detailed schematic of the WR setup used. The transceiver modules emit light at 1330 nm and 1270 nm, co- and counter-propagating with the EPS signal photons respectively.

WR devices. We demonstrate multiplexing of the quantum signal into a WR communication line to show the compatibility of WR with QKD and entanglement distribution.

Two experiments are performed using single mode fibre channels (Thorlabs SMF-28-1000) in the signal and idler branches, with lengths of a few meters in the first experiment and 1 km in the second. For each configuration, the polarisation measurements are performed when the WR modules are ON and OFF, to provide a direct measure of the impact of the WR signals on the quality of the distributed quantum states. The WR modules incorporate standard off-the-shelf small form-factor pluggable (SFP) transceivers, operating at 1270 nm and 1330 nm with output powers of 0.562 mW and 0.793 mW respectively, suited to networking 10 km long optical channels. During each experiment, the WR clocks are monitored separately to ensure that they are

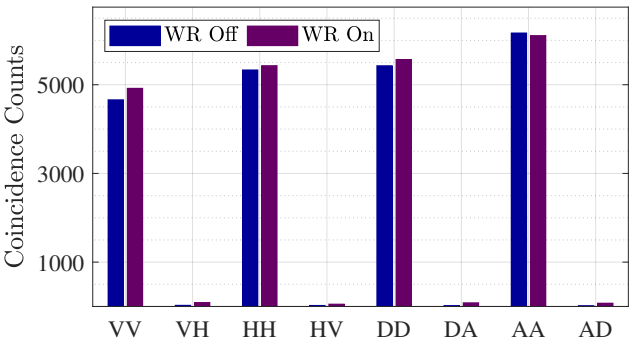
(a)



(b)

Visibility / %		
States	WR Off	WR On
$\|VV\rangle$ & $\|VH\rangle$	98.78	97.30
$\|HH\rangle$ & $\|HV\rangle$	99.53	99.17
$\|DD\rangle$ & $\|DA\rangle$	98.89	98.73
$\|AA\rangle$ & $\|AD\rangle$	97.07	96.61

(c)



(d)

Visibility / %		
States	WR Off	WR On
$\|VV\rangle$ & $\|VH\rangle$	98.89	96.45
$\|HH\rangle$ & $\|HV\rangle$	99.14	98.10
$\|DD\rangle$ & $\|DA\rangle$	99.27	97.06
$\|AA\rangle$ & $\|AD\rangle$	99.42	97.61

Figure 2. (a) Coincidence counts registered over 2 minutes between the two SPADs when the polarisation analysers are set to measure the orthogonal linear states for the idler and signal photons. The single mode fibre channels are a few meters long and measurements are taken when the WR signals are ON and OFF. The settings of the polarisation analysers are detailed on the x-axis where, for example, VH indicates when the system is measuring for occurrences of $|V\rangle_I |H\rangle_S$. (b) The visibility of the coincidence counts between the pairs of linear orthogonal states, calculated from the data shown in (a). Figures (c) and (d) are the same as (a) and (b) but extending the length of the single mode fibre to 1 km.

synchronised throughout.

For a BB84-type QKD protocol using distributed entangled photons, also known as BBM92,[19] the polarisation measurements on the signal and idler photons should result in 100% correlated measurements when measured in the same basis and show only statistical correlation when different measurement bases are chosen. The results of the polarisation measurements are shown in Figs. 2(a) and 2(c), for the short and the 1 km fibre channels respectively. The visibility between the maximum and minimum coincidence counts for each orthogonal pair of linear polarisation states is calculated, where the maximum and minimum number of coincidences occur when the signal and idler photon states match and differ respectively. The visibility values for each of the polarisation state pairs are shown in Figs. 2(b) and 2(d) for the two setup configurations. In all scenarios, the presence of the WR signals only slightly impacts the visibility of the entangled states, with the largest decrease in visibility amounting to 2.44%. Due to imperfect polarisation optimisation, there is some discrepancy in the visibility between the short and 1 km fibre channels when the WR signals are disabled. However, the visibility obtained in these cases is within the tolerance due to experimental imperfections and is always larger than 96% in the Z and X bases, which would correspond to a Quantum Bit Error Rate (QBER) smaller than 2%. This clearly shows that QKD and entanglement distribution can co-exist with WR time distribution.

To further assess the quality of the distributed signals, an additional set of measurements was taken for the 1 km channel configuration, with polarisation measurements made for all combinations of the linear states. The

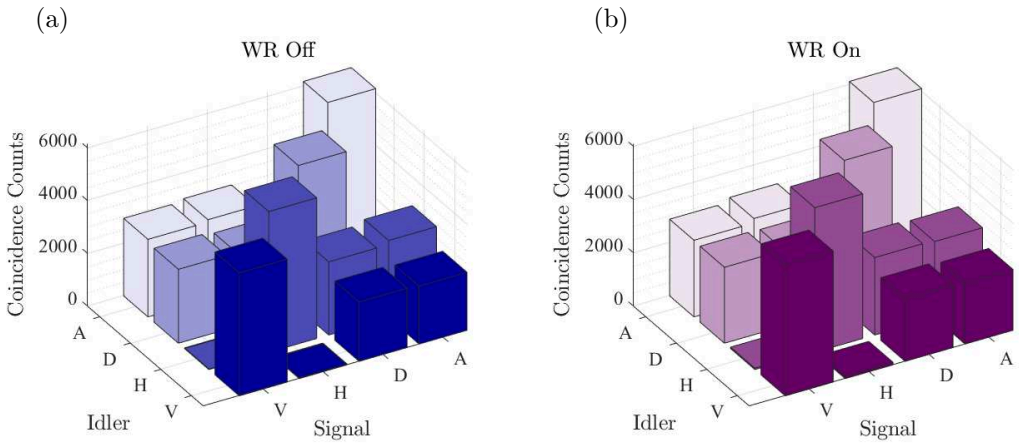


Figure 3. Coincidence counts registered over 2 minutes between the two SPADs for signal and idler photons, for the two 1 km channels with WR OFF (a) and ON (b). The four states needed for QKD generate the correct proportion of coincidence counts, even in the presence of the classical WR signals.

results are shown in Figs. 3(a) and 3(b) for WR signals OFF and ON respectively. Simultaneous measurements taken in mismatched bases were confirmed to result in correlations of approximately 50%, as expected for the Z and X measurement bases.

3. CONCLUSION

We have demonstrated the distribution of entangled single photon polarisation states with high visibility over optical fibres up to 1 km. The capability for quantum key distribution is achieved and maintained in coexistence with the classical optical signals needed for White Rabbit time synchronisation, with only a small increase of the quantum bit error rate when the time synchronisation is enabled.

Future work will include the full exploitation of the WR synchronisation with an active gating of the detectors placed in remote locations, as well as the implementation of various types of QKD and entanglement distribution protocols[20–25] over a more extended network, covering tens of kilometres of fibre.

ACKNOWLEDGMENTS

We acknowledge useful discussions with Rolf Horn in relation to the entangled photon source. Funding has been provided through the partnership resource scheme of the EPSRC Quantum Communications Hub grant (EP/T001011/1).

REFERENCES

[1] Wehner, S., Elkouss, D., and Hanson, R., "Quantum internet: A vision for the road ahead," *Science* **362**(6412) (2018).

[2] Chapuran, T. E., Toliver, P., Peters, N. A., Jackel, J., Goodman, M. S., Runser, R. J., McNown, S. R., Dallmann, N., Hughes, R. J., McCabe, K. P., Nordholt, J. E., Peterson, C. G., Tyagi, K. T., Mercer, L., and Dardy, H., "Optical networking for quantum key distribution and quantum communications," *New J. Phys.* **11**, 105001 (Oct. 2009).

[3] Choi, I., Young, R. J., and Townsend, P. D., "Quantum information to the home," *New J. Phys.* **13**, 063039 (June 2011).

[4] Eraerds, P., Walenta, N., Legre, M., Gisin, N., and Zbinden, H., "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics* **12**(6), 063027 (2010).

[5] Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., and Shields, A. J., "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X* **2**, 041010 (Nov. 2012).

[6] Patel, K. A., Dynes, J. F., Lucamarini, M., Choi, I., Sharpe, A. W., Yuan, Z. L., Penty, R. V., and Shields, A. J., "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.* **104**, 051123 (Feb. 2014).

[7] Lipiński, M., Włostowski, T., Serrano, J., and Alvarez, P., "White rabbit: a ptp application for robust sub-nanosecond synchronization," in [*2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*], 25–30 (2011).

[8] Berners-Lee, T., "Information management: A proposal," (1990).

[9] Takesue, H., Diamanti, E., Langrock, C., Fejer, M. M., and Yamamoto, Y., "10-ghz clock differential phase shift quantum key distribution experiment," *Optics Express* **14**, 9522 (2006).

[10] Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W., and Shields, A. J., "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," *Opt. Express* **16**, 18790 (Oct. 2008).

[11] Lucamarini, M., Patel, K. A., Dynes, J. F., Fröhlich, B., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., and Shields, A. J., "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express* **21**, 24550 (Oct. 2013).

[12] Boaron, A., Korzh, B., Houlmann, R., Boso, G., Rusca, D., Gray, S., Li, M.-J., Nolan, D., Martin, A., and Zbinden, H., "Simple 2.5 ghz time-bin quantum key distribution," *Applied Physics Letters* **112**(17), 171108 (2018).

[13] Qi, B., Fung, C.-H. F., Lo, H.-K., and Ma, X., "Time-shift attack in practical quantum cryptosystems," *Quantum Info. Comput.* **7**, 73–82 (Jan. 2007).

[14] Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C., and Lo, H.-K., "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A* **78**, 042333 (Oct. 2008).

[15] Alshowkan, M., Evans, P. G., Williams, B. P., Rao, N. S. V., Marvinney, C. E., Pai, Y.-Y., Lawrie, B. J., Peters, N. A., and Lukens, J. M., "Advanced architectures for high-performance quantum networking," *J. Opt. Commun. Netw.* **14**, 493–499 (June 2022).

[16] Horn, R. and Jennewein, T., "Auto-balancing and robust interferometer designs for polarization entangled photon sources," *Opt. Express* **27**, 17369–17376 (June 2019).

[17] Wengerowsky, S., Joshi, S. K., Steinlechner, F., Hübel, H., and Ursin, R., "An entanglement-based wavelength-multiplexed quantum communication network," *Nature* **564**, 225–228 (Dec. 2018).

[18] Bennett, C. H. C. and Brassard, G., "Quantum cryptography: public key distribution and coin tossing," *Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing* **1**, 175–179 (1984).

[19] Bennett, C. H., Brassard, G., and Mermin, N. D., "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.* **68**, 557–559 (Feb. 1992).

[20] Lo, H.-K., Ma, X., and Chen, K., "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**, 230504 (June 2005).

[21] Lo, H.-K., Curty, M., and Qi, B., "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* **108**, 130503 (Mar. 2012).

[22] Braunstein, S. L. and Pirandola, S., "Side-channel-free quantum key distribution," *Phys. Rev. Lett.* **108**(13), 130502 (2012).

[23] Lucamarini, M., Vallone, G., Gianani, I., Mataloni, P., and Di Giuseppe, G., "Device-independent entanglement-based bennett 1992 protocol," *Phys. Rev. A* **86**, 032325 (Sept. 2012).

[24] Lucamarini, M., Yuan, Z. L., Dynes, J. F., and Shields, A. J., "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature* **557**, 400 (2018).

[25] Proietti, M., Ho, J., Grasselli, F., Barrow, P., Malik, M., and Fedrizzi, A., "Experimental quantum conference key agreement," *Science Advances* **7** (June 2021).