Metropolitan free-space quantum networks

Andréj Kržič\textsuperscript{1,2,*}, Sakshi Sharma\textsuperscript{1,2}, Christopher Spiess\textsuperscript{1,2}, Uday Chandrashekara\textsuperscript{1,2}, Sebastian Töpfer\textsuperscript{1}, Gregor Sauer\textsuperscript{1,2}, Luis Javier González-Martín del Campo\textsuperscript{1,2}, Teresa Kopf\textsuperscript{1}, Stefan Petzcharmig\textsuperscript{3}, Thomas Grafenauer\textsuperscript{1}, Roland Luger\textsuperscript{3}, Bernhard Ömer\textsuperscript{3}, Christoph Pacher\textsuperscript{3}, René Berlich\textsuperscript{1}, Thomas Peschel\textsuperscript{1}, Christoph Damm\textsuperscript{1}, Stefan Risse\textsuperscript{1}, Matthias Goy\textsuperscript{1}, Daniel Rieländer\textsuperscript{1}, Andreas Tünnermann\textsuperscript{1,4,5}, Fabian Steinlechner\textsuperscript{1,5,*}

\textsuperscript{1} Fraunhofer Institute for Applied Optics and Precision Engineering, Albert-Einstein-Str. 7, 07745 Jena, Germany
\textsuperscript{2} Friedrich Schiller University Jena, Faculty of Physics and Astronomy, Max-Wien-Platz 1, 07743 Jena, Germany
\textsuperscript{3} AIT Austrian Institute of Technology, Giefinggasse 4, 1210 Vienna, Austria
\textsuperscript{4} Institute of Applied Physics, Friedrich Schiller University Jena, Albert-Einstein-Str. 15, 07745 Jena, Germany
\textsuperscript{5} Abbe Center of Photonics, Friedrich Schiller University Jena, Albert-Einstein-Str. 6, 07745 Jena, Germany

Quantum communication has seen rapid progress towards practical large-scale networks, with quantum key distribution (QKD) spearheading this development. Breakthroughs in satellite-based QKD promise to bridge large intercity distances between nodes. Advances in optical fibre networks, on the other hand, have shown that fibre-based systems are well suited for metropolitan scales. However, in many scenarios, suitable fibre infrastructure may not be in place. Here, we make the case for an entanglement-based free-space quantum network as a practical and efficient alternative for metropolitan applications. To support this prospect, we developed a deployable free-space QKD system and demonstrated its use in two realistic scenarios: between 300 m separated offices and over a 1.7 km link with a temporary container atop another building. We achieved secure key rates of up to 6 kbps, with over 2.5 kbps in full daylight, and estimate kbps rates are achievable even for 10-km distances. These results indicate that round the clock network accessibility as well as full coverage of a city is within reach with the present technology. We anticipate that our work will establish free-space networks as a viable solution for metropolitan scales and an indispensable complementary building block in the future global quantum internet.

Introduction

The core functionality of a quantum communication network is to transmit quantum information – qubits – between two or more parties. Many revolutionizing applications of quantum networks have already been identified and a roadmap towards full-blown quantum internet has been proposed [1]. While there are still many uncertainties as to the technological platforms that will ultimately make up the quantum internet, one thing is clear: it will be a heterogeneous network of various special purpose sub-networks that employ different types of links and interconnects.

Quantum key distribution (QKD) networks have so far been the driving force for this development [2]. Although certainly not the only networks of interest, they have been paving the way also for other distributed quantum information processing schemes. For this reason, QKD has often been used to benchmark the level of technological maturity of quantum networks in general. Currently, connecting many users distributed over large distances requires trusted nodes [3], which comes with the price of losing any possibility of end-to-end security. Unlocking the full quantum advantage in global-scale networks is therefore an ongoing challenge. A substantial proportion of current research is focused on extending the reach of individual quantum links, either through satellites [4–7] or fibre-based quantum repeaters [8–10].

Over shorter, metropolitan-scale distances, where end-to-end quantum state transmission is more easily achieved, the research focus is on a different set of challenges. One of the primary concerns is the question of scalability, i.e., how to increase the number of users in a network [11–14]. Another line of research aims to make metropolitan quantum network technology more accessible, flexible, and deployable [15–18]. An important challenge is also to interconnect networks based on different physical platforms [19]. However, all this progress is made almost exclusively with optical fibre links.

\[\text{Andrej.Kržic}@iof.fraunhofer.de\]
\[\text{Fabian.Steinlechner}@iof.fraunhofer.de\]
In some metropolitan application scenarios, end-to-end fibre links are not feasible. A possible alternative are terrestrial free-space links. These are still far behind the technological maturity of their fibre counterparts. The free space sector did not benefit from an extensive legacy of classical telecom technologies nearly as much as the fibre sector. It faces additional challenges, such as non-trivial link alignment, atmospheric turbulence, and daylight noise [20]. Nevertheless, a number of notable terrestrial free-space QKD experiments has been done [21–26].

Most of the free-space experiments so far aimed at advancing technology towards satellite applications, leaving their potential for metropolitan use largely unaddressed. In the following, we show that quantum entanglement is particularly well-suited to metropolitan-scale networks. Among the plethora of prepare-and-measure implementations, however, only a handful of groups have performed entanglement-based QKD in free space. Secure key rates in the order of hundreds of bits per second (bps) have been achieved over kilometre distances at night [27, 28], and in broad daylight, only a single successful demonstration over 350 m has been reported [29]. It has therefore been widely argued that the entanglement-based approach lacks the technological maturity and applicability of alternative approaches.

Here, we propose a metropolitan free-space quantum network architecture that can be deployed to secure communication at summits, conferences, and other events, or complement an existing network infrastructure whenever end-to-end fibre connections are not available. The architecture is built around a central entanglement server that streams entangled photons to users on the network. We developed the key building blocks of this architecture, including: a portable high-visibility entangled photon pair source, deployable and efficient free-space terminals that are specifically designed for metropolitan applications, compact and passive quantum state analysis and detection with dedicated filtering for daytime operation, and complete post-processing for live generation of ready-to-use encryption keys.

We performed QKD in two realistic metropolitan scenarios. First, we distributed secret keys between two 300 m separated government offices, showcasing ad hoc quantum security. We then moved the system to a different location, where we realized a 1.7 km link. We achieved secure key rates of up to 6 kbps under various link conditions, with over 2.5 kbps in broad daylight. This is not only the first demonstration of kbps QKD over metropolitan free-space distances for an entanglement-based system, but also an improvement of its daylight capability by an order of magnitude in both secret key rate and link range. By extrapolating our experimental results with established models, we estimate kbps secure key rates to be achievable even for a 10-km link, showing that the present technology is suitable for distances spanning across entire cities.

**Entanglement-based quantum network**

In the proposed network architecture, an entangled photon source acts as a server that streams entanglement into a metropolitan-scale network consisting of free-space links (Fig. 1a). The natural choice for placing the entanglement server (ES) is a central high-rise building with a clear line of sight to the relevant urban areas. Each of the end users owns a quantum receiver subsystem (QRS), which typically incorporates quantum state analysis and detection, timing and synchronisation electronics, and post-processing software. Although the network has a star topology at the physical layer (Fig. 1b), recently proposed multiplexing strategies [11, 14, 18] can leverage the nonlocal correlations of entangled pairs to provide a fully connected mesh network at the quantum communication layer.

Employing quantum entanglement as the main network resource has several key advantages over the more established prepare-and-measure schemes. Entanglement offers additional layers of security via the prospect of device-independent protocols [30]. The ES can thus act as an untrusted relay node and lift the requirement for direct line of sight between the transceiver telescopes of any two users. Furthermore, the ES is all passive, meaning that the post-processing is delegated downstream to the users, which allows for standardization of ES, while the users can use an application-specific QRS. This gives a large degree of flexibility and even upgradeability, as more advanced schemes, protocols, and
post-processing methods become available over time. Moreover, entanglement quite naturally supports many other promising network schemes beyond QKD [20].

The network size and reach can be readily extended by introducing several ESs, all interconnected through a central trusted node and each distributing entanglement to end users in their own local areas (Fig. 1c). In a more distant future, the requirement for trusting the central node could eventually be lifted by introducing entanglement swapping [31], without changing the overall network topology (Fig. 1d). As indicated in Fig. 1a, the architecture is also not limited to free-space links – the ES can act as a convenient interface between a free-space and a fibre link segment, for example, to connect a metropolitan free-space network to the fibre backbone of a larger intercity network.

Fig. 1: Metropolitan entanglement-based free-space network. a, A standardized centrally located entanglement server (ES, black box) is streaming entangled photons into the network. Free-space channels are used to connect distant buildings and parts of a metropolitan area, while fibre connections may still be used in a complementary way, for example, to connect to offices within the central building. Each end user owns an application-specific quantum receiver subsystem (green boxes). b, The corresponding physical layer network topology. At the quantum communication layer, the network is a pairwise connected mesh, so that every end user can communicate with any other (not shown). c, A near-term extension possibility using several ESs and a central trusted node. d, Eventually, by introducing entanglement swapping, the trusted node could again be turned into an untrusted one, while the overall network topology would remain unchanged.

**Experimental demonstration**

We developed a deployable standalone QKD system specifically suited for metropolitan applications. It consists of all the key building blocks necessary to implement the present free-space quantum network and can be fully deployed at a new site in less than a day, without requiring prior infrastructure apart from access to electricity. The system is schematically shown in Fig. 2 and roughly corresponds to the Alice-Bob segment of the network in Fig. 1a. In our experiments, Alice was located next to the ES. Note that this is not required – the ES could also be at a different location and connected to Alice with a longer single-mode fibre or another free-space link. Our ES generates pairs of polarization-entangled photons at 810 nm (Methods), of which one is sent to Alice via a single-mode fibre, while the other one is sent to Bob using a free-space link. For fine alignment of the free-space link and beam stabilization, we use a 1064 nm beacon laser beam, which co-propagates along the signal photons from Alice to Bob. Analysis of the beacon beam at Bob provides a feedback signal for two fast steering mirrors, which in turn counteracts fluctuations and stabilize the free-space channel in the presence of atmospheric turbulence and mechanical system instabilities. The use of a closed-loop beam stabilization system enables long-term operation and also facilitates the use of a spatial filter with a small field of view at Bob, which is necessary for daylight operation of the system.
Both Alice and Bob own a quantum receiver subsystem (QRS), which we developed for performing QKD with the BBM92 protocol [32]. Each QRS incorporates a polarization analysis module, 4 single-photon avalanche detectors, time-tagging electronics, a rubidium clock, post-processing software, and a key management system (Methods). Bob's QRS further includes specially designed spectral and spatial filtering modules for daylight operation. Alice's QRS, on the other hand, does not require dedicated filtering of daylight noise, since it is not directly exposed to the free-space link. Bob's QRS is also equipped with a motorized polarization controller that allows for automated alignment of the polarization frame of reference with Alice.

To distill the final secure key, the post-processing software performs the following steps: synchronization of detection events between Alice and Bob, sifting (i.e. discarding pairs of detection events that did not happen using the same measurement basis), correction of transmission errors, privacy amplification, and delayed authentication (Methods). Post-processing requires Alice and Bob's QRS to exchange information via an information theoretically secure authentic classical channel. Information that could hypothetically be leaked to a potential eavesdropper via the classical channel is considered in the privacy amplification step, so that the security of the final key is not compromised.

Using this system, we performed several QKD experiments in two different metropolitan settings. In the framework of QuNET Initiative [33], we first established an ad hoc QKD network between two 300 m separated government offices in Bonn, Germany. We achieved an average secure key rate of 6.5 kbps over 45 minutes around midnight from 8 to 9 July 2021. Furthermore, we demonstrated a stable daylight performance between 9:30 and 14:20 on a sunny day on 20 July 2021, with an average secure key rate of 3 kbps. In these experiments, we used an existing classical communication channel.

To showcase the system’s flexibility as well as its performance over longer distances, we then moved the system to Jena, Germany, where we established a link between the Fraunhofer IOF institute and a temporary container on top of a 1.7 km distant public service building. Here, we deployed commercial radio antennas to establish the classical channel. We conducted QKD experiments in February and March 2022 under various link conditions (Fig. 3). During nighttime, we achieved stable secure key rates (SKR) of about 6 kbps and a quantum bit error rate (QBER) of around 2%, which is the benchmark performance of our system (Fig. 3c). We achieved a similar performance throughout a cloudy day (Fig. 3a), demonstrating that when the link is not directly exposed to the sun, our filtering methods reduce daylight noise to a negligible level. However, in direct sunlight, both QBER and in turn SKR were
affected by high levels of noise. This dynamics can be clearly observed in Fig. 3b. During the perfectly sunny morning, QBER was steadily increasing and SKR steadily decreasing for the first couple of hours from 8:00 on, which is a consequence of the day getting brighter as it approaches noon. Right before noon, several clouds formed in the vicinity of the sun. During the upcoming hours, the clouds blocked the sun for extended periods of time, restoring the system performance almost to its benchmark values at times. Sporadically, a large amount of sunlight came through the clouds, causing sharp jumps in QBER and the corresponding drops of SKR. Nevertheless, SKR remained above 2.5 kbps even under the brightest conditions.

![Fig. 3: Demonstration of free-space quantum key distribution. The achieved secure key rates and quantum bit error rates are shown for experiments performed under various link conditions. The plotted values are 5-minute averages and the horizontal axis shows the local time of day. The background colour corresponds to the measured solar radiation. (solar radiation data: University of Applied Sciences Jena) a. Daytime performance on a cloudy day. b. Daytime performance in direct sunlight (morning) and in presence of varying partial cloud coverage (afternoon) c. Nighttime performance.](image)

**Discussion and conclusion**

We proposed an entanglement-based free-space quantum network architecture as a viable solution for metropolitan scales. With our fully deployable QKD system, which is particularly suitable for ad hoc implementation in scenarios where fibre connections are infeasible, we demonstrated all the main building blocks of such a network. We achieved up to 6 kbps secure key rates over two different links and under various link conditions, with over 2.5 kbps in full daylight, indicating that the system has a potential for 24/7 operation. To our knowledge, this is the first demonstration of kbps QKD over metropolitan free-space distances with an entanglement-based system. Moreover, it is an improvement of entanglement-based QKD daylight capability by an order of magnitude in both secret key rate and link range [29]. The results are also competitive with prepare-and-measure systems. With our large-aperture free-space terminals, we estimate kbps key rates are possible even over 10 km links (Methods). A full coverage of a city is therefore within reach with the present technology.

By implementing the free-space quantum channel at 810 nm, we break with ongoing trends of transferring to telecom C band wavelengths. Fibre-based network architectures typically strive to minimize the number of detectors [3, 34], which is due to the fact that single-photon detection at 1550 nm is a cost driver. This does not apply in our case, where transmitter and receiver systems are of similar cost and complexity. A non-degenerate entangled photon source [35], which emits photons at 1550 nm and 810 nm, could act as an elegant interface between fibre and free-space segments of a heterogeneous network.

There are many possible improvements to the present system on the horizon. Extending the two-user scenario to a fully connected multi-user network is straightforward with the latest multiplexing techniques [11, 14, 18]. Recent developments towards ultra-bright GHz rate entangled pair sources [36, 37] show that a single entanglement server could support many end users. Adaptive optics (AO) could
significantly improve daylight performance by reducing the effective focal spot size and thus giving the possibility for tighter spatial filtering [21, 24]. Furthermore, with efficient AO-enabled single-mode fibre coupling, hybrid free-space to fibre quantum links become possible. This would allow for physical separation of the end user from the receiver free-space terminal, introducing considerably more flexibility. Entanglement swapping [31] would not only increase the extent of the present network without the need for trusted nodes, but it would also enable integration into larger heterogeneous networks that employ fundamentally different forms of entanglement [19].

Another way forward is to exploit high-dimensional entanglement, which promises higher information capacity per photon, better security, and enhanced robustness to noise [38, 39]. Although the practicality of orbital angular momentum (OAM) modes remains questionable for long-distance free-space communication [40], the OAM-entanglement might still be well suited for metropolitan distances [41]. AO would further improve key rates by protecting spatial mode entanglement from the influence of atmospheric turbulence [42]. An entangled photon source can also generate hyperentanglement – simultaneous entanglement in different degrees of freedom – quite naturally [43], which could be used to make a single server compatible with a range of receiver types. A recent experiment demonstrates that extending entanglement into the time-bin degree of freedom could also significantly boost secure key rates [44].

Finally, the distribution of entanglement lies at the heart of many applications beyond QKD. Practical and efficient metropolitan entanglement distribution networks would therefore facilitate the development of entirely new applications at the intersection of distributed sensing and quantum information processing, such as quantum clock synchronisation [45], long baseline interferometry [46], and multi-partite quantum cryptography [47, 48].

**Acknowledgements**

We thank Robert Jende, Ralf Steinkopf, Mathias Rohde, Sandra Müller, and Stefan Schwinde for their work on the transceiver telescopes; Herbert Gross for help with the spatial filter design; Mirko Liedtke and Carl Zeiss Microscopy GmbH for providing a motorized aperture for the spatial filter; Nico Döll for work on the spatial filter module; Emma Brambila-Tamayo and Rana Sebak for help with the entangled photon source; Stadtwerke Jena for giving us access to their rooftop for our experiments; Daniel Heining for general experimental support; Rodrigo Gomez and Nina Leonhard for preliminary calculations; Aoife Brady and Claudia Reinlein for helpful discussions and support in the early stage planning; Markus Selnke and Julian Gritsch for administrative support; and Hanna Läkk for the network scheme figure graphics design. This research was conducted within the scope of the project QuNET, funded by the German Federal Ministry of Education and Research (BMBF) in the context of the federal government’s research framework in IT-security “Digital. Secure. Sovereign.” A.K. and C.S. are part of the Max Planck School of Photonics supported by the BMBF, the Max Planck Society, and the Fraunhofer Society. A.K. is co-sponsored by the European Space Agency (ESA) through the Networking Partnering Initiative (NPI) Contract No. 4000125842/18/NL/MH/mg (Project DIFFRACT).

**References**

[1] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” Science (New York, N.Y.), vol. 362, no. 6412, 2018, doi: 10.1126/science.aam9288.

[2] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, “Large scale quantum key distribution: challenges and solutions Invited,” Optics express, vol. 26, no. 18, pp. 24260–24273, 2018, doi: 10.1364/OE.26.024260.

[3] Y.-A. Chen et al., “An integrated space-to-ground quantum communication network over 4,600 kilometres,” Nature, vol. 589, no. 7841, pp. 214–219, 2021, doi: 10.1038/s41586-020-03093-8.

[4] S.-K. Liao et al., “Satellite-Relayed Intercontinental Quantum Network,” Physical review letters, vol. 120, no. 3, p. 30501, 2018, doi: 10.1103/PhysRevLett.120.030501.

[5] J. Yin et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” Nature, vol. 582, no. 7813, pp. 501–505, 2020, doi: 10.1038/s41586-020-2401-y.

[6] S.-K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature, vol. 549, no. 7670, pp. 43–47, 2017, doi: 10.1038/nature23655.
[7] J. Yin et al., “Satellite-to-Ground Entanglement-Based Quantum Key Distribution,” Physical review letters, vol. 119, no. 20, p. 200501, 2017, doi: 10.1103/PhysRevLett.119.200501.

[8] Z.-D. Li et al., “Experimental quantum repeater without quantum memory,” Nature Photon, vol. 13, no. 9, pp. 644–648, 2019, doi: 10.1038/s41566-019-0468-5.

[9] Y.-F. Pu et al., “Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments,” Nature Photon, vol. 15, no. 5, pp. 374–378, 2021, doi: 10.1038/s41566-021-00764-4.

[10] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, “Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution,” Physical review letters, vol. 126, no. 23, p. 230506, 2021, doi: 10.1103/PhysRevLett.126.230506.

[11] S. K. Joshi et al., “A trusted node-free eight-user metropolitan quantum communication network,” Science advances, vol. 6, no. 36, 2020, doi: 10.1126/sciadv.aba9599.

[12] J. F. Dybes et al., “Cambridge quantum network,” npj Quantum Inf, vol. 5, no. 1, p. 2728, 2019, doi: 10.1038/s41534-019-02211-4.

[13] T.-Y. Chen et al., “Implementation of a 46-node quantum metropolitan area network,” npj Quantum Inf, vol. 7, no. 1, p. 661, 2021, doi: 10.1038/s41534-021-00474-3.

[14] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübner, and R. Ursin, “An entanglement-based wavelength-multiplexed quantum communication network,” Nature, vol. 564, no. 7735, pp. 225–228, 2018, doi: 10.1038/s41586-018-0766-y.

[15] D. Bunandar et al., “Metropolitan Quantum Key Distribution with Silicon Photonics,” Phys. Rev. X, vol. 8, no. 2, 2018, doi: 10.1103/PhysRevX.8.021009.

[16] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, “Plug-and-play continuous-variable quantum key distribution for metropolitan networks,” Optics express, vol. 28, no. 10, pp. 14547–14559, 2020, doi: 10.1364/OE.391491.

[17] M. Alshowkan et al., “Reconfigurable Quantum Local Area Network Over Deployed Fiber,” PRX Quantum, vol. 2, no. 4, p. 503, 2021, doi: 10.1103/PRXQuantum.2.040304.

[18] F. Appas et al., “Flexible entanglement-distribution network with an AlGaAs chip for secure communications,” npj Quantum Inf, vol. 7, no. 1, p. 2021, doi: 10.1038/s41534-021-00454-7.

[19] G. Guccione et al., “Connecting heterogeneous quantum networks by hybrid entanglement swapping,” Science advances, vol. 6, no. 22, 2020, doi: 10.1126/sciadv.aba4508.

[20] J. S. Sidhu et al., “Advances in space quantum communications,” IET Quantum Communication, vol. 2, no. 4, pp. 182–217, 2021, doi: 10.1049/qt2.12015.

[21] M. T. Gruneisen et al., “Adaptive-Optics-Enabled Quantum Communication: A Technique for Daytime Space-To-Earth Links,” Phys. Rev. Applied, vol. 16, no. 1, p. 126111, 2021, doi: 10.1103/PhysRevApplied.16.014067.

[22] S. Ecker et al., “Strategies for achieving high key rates in satellite-based QKD,” npj Quantum Inf, vol. 7, no. 1, p. 163, 2021, doi: 10.1038/s41534-020-00335-5.

[23] Y. Cao et al., “Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution,” Physical review letters, vol. 125, no. 26, p. 260503, 2020, doi: 10.1103/PhysRevLett.125.260503.

[24] Y.-H. Gong et al., “Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror,” Optics express, vol. 26, no. 15, pp. 18897–18905, 2018, doi: 10.1364/OE.26.018997.

[25] S.-K. Liao et al., “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication,” Nature Photon, vol. 11, no. 8, pp. 509–513, 2017, doi: 10.1038/nphoton.2017.116.

[26] M. Avesani et al., “Full daylight quantum-key distribution at 1550 nm enabled by integrated silicon photonics,” npj Quantum Inf, vol. 7, no. 1, p. 145, 2021, doi: 10.1038/s41534-021-00421-2.

[27] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, “Free-space quantum key distribution with entangled photons,” Appl. Phys. Lett., vol. 89, no. 10, p. 101122, 2006, doi: 10.1063/1.2348775.

[28] C. Erven et al., “Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere,” New J. Phys., vol. 14, no. 12, p. 123018, 2012, doi: 10.1088/1367-2630/14/12/123018.

[29] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, “Daylight operation of a free space, entanglement-based quantum key distribution system,” New J. Phys., vol. 11, no. 4, p. 45007, 2009, doi: 10.1088/1367-2630/11/4/045007.

[30] S. Pirandola et al., “Advances in quantum cryptography,” Adv. Opt. Photon., vol. 12, no. 4, p. 1012, 2020, doi: 10.1364/AOP.361502.

[31] T. Herbst et al., “Teleportation of entanglement over 143 km,” Proceedings of the National Academy of Sciences of the United States of America, vol. 112, no. 46, pp. 14202–14205, 2015, doi: 10.1073/pnas.1517007112.

[32] Bennett, Brassard, and Mermin, “Quantum cryptography without Bell’s theorem,” Physical review letters, vol. 68, no. 5, pp. 557–559, 1992, doi: 10.1103/PhysRevLett.68.557.

[33] Qunet Initiative. [Online]. Available: https://www.qunet-initiative.de/qunet-alpha-bonn/

[34] B. Fröhlich, J. F. Dybes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, “A quantum access network,” Nature, vol. 501, no. 7465, pp. 69–72, 2013, doi: 10.1038/nature12493.

[35] M. Hentschel, H. Hübner, A. Poppe, and A. Zeilinger, “Three-color Sagnac source of polarization-entangled photon pairs,” Optics express, vol. 17, no. 25, pp. 23153–23159, 2009, doi: 10.1364/OE.17.023153.
[36] A. Lohrmann, C. Perumangatt, A. Villar, and A. Ling, “Broadband pumped polarization entangled photon-pair source in a linear beam displacement interferometer,” *Appl. Phys. Lett.*, vol. 116, no. 2, p. 21101, 2020, doi: 10.1063/1.5124416.

[37] T. J. Steiner et al., “Ultrabright Entangled-Photon-Pair Generation from an AlGaAs-On-Insulator Microring Resonator,” *PRX Quantum*, vol. 2, no. 1, p. 1, 2021, doi: 10.1103/PRXQuantum.2.010337.

[38] A. Forbes and I. Nape, “Quantum mechanics with patterns of light: Progress in high dimensional and multidimensional entanglement with structured light,” *AVS Quantum Sci.*, vol. 1, no. 1, p. 11701, 2019, doi: 10.1116/1.5112027.

[39] M. Erhard, M. Krenn, and A. Zeilinger, “Advances in high-dimensional quantum entanglement,” *Nat Rev Phys*, vol. 2, no. 7, pp. 365–381, 2020, doi: 10.1038/s42254-020-0193-5.

[40] M. Krenn et al., “Twisted light transmission over 143 km,” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 113, no. 48, pp. 13648–13653, 2016, doi: 10.1073/pnas.1612023113.

[41] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, “Twisted photon entanglement through turbulent air across Vienna,” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 112, no. 46, pp. 14197–14201, 2015, doi: 10.1073/pnas.1517574112.

[42] G. Sorelli, N. Leonhard, V. N. Shatokhin, C. Reinlein, and A. Buchleitner, “Entanglement protection of high-dimensional states by adaptive optics,” *New J. Phys.*, vol. 21, no. 2, p. 23003, 2019, doi: 10.1088/1367-2630/ab006e.

[43] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, “Generation of hyperentangled photon pairs,” *Physical review letters*, vol. 95, no. 26, p. 260501, 2005, doi: 10.1103/PhysRevLett.95.260501.

[44] J. C. Chapman, C. C. W. Lim, and P. G. Kwiat, “Hyperentangled Time-bin and Polarization Quantum Key Distribution,” Aug. 2019. [Online]. Available: http://arxiv.org/pdf/1908.09018v4

[45] E. O. Ilo-Okeke, L. Tessler, J. P. Dowling, and T. Byrnes, “Remote quantum clock synchronization without synchronized clocks,” *npj Quantum Inf.*, vol. 4, no. 1, p. 281, 2018, doi: 10.1038/s41534-018-0090-2.

[46] D. Gottesman, T. Jennewein, and S. Croke, “Longer-baseline telescopes using quantum repeaters,” *Physical review letters*, vol. 109, no. 7, p. 70503, 2012, doi: 10.1103/PhysRevLett.109.070503.

[47] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, “Experimental quantum conference key agreement,” *Science advances*, vol. 7, no. 23, 2021, doi: 10.1126/sciadv.abe0395.

[48] C. Thalacker, F. Hahn, J. de Jong, A. Pappa, and S. Barz, “Anonymous and secret communication in quantum networks,” *New J. Phys.*, vol. 23, no. 8, p. 83026, 2021, doi: 10.1088/1367-2630/ac1808.
SUPPLEMENTARY INFORMATION

Free-space link

For the purpose of the present and future experiments, we developed two portable and highly versatile optical free-space terminals [49]. They have a symmetrical design, which means that in principle each terminal can act both as a transmitter and a receiver, with no dependence of signal channel efficiency on its directionality. Each terminal consists of a transceiver telescope, a beam stabilization subsystem, and a set of high and low pass filters to in-couple (or out-couple) a particular set of wavelengths into (or from) the common beam path. All these elements are integrated on an optical breadboard, which is mounted on a commercial motorized tripod mount with its own internal stabilization feedback loop.

The mirror-based design of transceiver telescopes allows for a high optical performance, i.e. low wavefront aberrations and a high optical throughput, over a wide range of wavelengths. In particular, the system supports several optical channels: two quantum signal channels at around 810 nm and 1550 nm, and two beacon channels (one for each direction) at 1064 nm and at 980 nm. Only the 810 nm signal and the 1064 nm beacon channels were used for the experiments presented here and are shown in Fig. 2. Additionally, the system supports an optical channel in the visible spectrum for the purpose of initial alignment of the terminals.

The transceiver telescopes are based on an afocal three-mirror anastigmat (TMA) design combined with an additional fourth mirror to reduce the size and improve the optical quality. The respective off-axis telescope layout renders the transceiver system with high signal throughput due to the absence of a central obscuration. Moreover, the shape of the individual telescope mirrors is optimized to provide diffraction limited performance even in case of considerable fluctuations of the beam angle and position due to atmospheric turbulence. Furthermore, the primary mirror’s large aperture of 200 mm prevents severe signal loss due to diffraction or atmospheric turbulences even over link distances of several kilometres. At 810 nm, for our transmitter beam waist of 40 mm and following the standard approach to model beam propagation through Kolmogorov turbulence [50], we estimate near-zero loss due to beam spreading (diffraction and turbulence induced spreading) over a 1.7 km link under medium turbulence with refractive index structure parameter $C_n^2 = 10^{-15} \text{m}^{2/3}$. For the same turbulence and a 10 km link, we estimate the average loss due to beam spreading to still be as low as 2.1 dB (Fig. 4).

Extending the free-space link to longer distances would introduce an additional loss factor of $\eta$ to Bob’s signal channel. Using the secure key rate model from [51], it is straightforward to show that in the limit of much larger received signal rates compared to noise rates, key rates would scale linearly with $\eta$. During our night experiment on 02 March 2022, we achieved a mean secure key rate of 5.6 kbps, while the estimated mean total count rate at Alice and Bob was 1.03 Mcps and 190 kcps, respectively. Mean total detected coincidence rate was 14.3 kcps, of which ~200 cps are estimated to be accidental. During

![Fig. 4: Estimated average link loss due to diffraction and turbulence induced beam spreading. The loss is shown for three different turbulence strengths characterized by refractive index structure parameter $C_n^2$.](image-url)

**Key rate estimation for a 10 km link**

Extending the free-space link to longer distances would introduce an additional loss factor of $\eta$ to Bob’s signal channel. Using the secure key rate model from [51], it is straightforward to show that in the limit of much larger received signal rates compared to noise rates, key rates would scale linearly with $\eta$. During our night experiment on 02 March 2022, we achieved a mean secure key rate of 5.6 kbps, while the estimated mean total count rate at Alice and Bob was 1.03 Mcps and 190 kcps, respectively. Mean total detected coincidence rate was 14.3 kcps, of which ~200 cps are estimated to be accidental.
this experiment, total noise count was less than 1 kcps per site (consisting mostly of dark counts). For a 10 km link, where we estimate $\eta = 10^{-2.1}$, we can therefore assume linear scaling of the key rate with $\eta$ and thus expect up to 3.4 kbps key rates to be achievable with our system.

**Entanglement server**

Our entanglement server (ES) consists of an entangled photon source, which generates bipartite polarization entanglement (Fig. 5). It is based on type-2 spontaneous parametric down conversion (SPDC) in a periodically poled potassium titanyl phosphate (ppKTP) crystal, employing an intrinsically phase-stable Sagnac configuration [52]. Pumping the crystal with a 405 nm laser generates an entangled pair state at 810 nm, which is of the form

$$|\Psi\rangle \propto |H_s\rangle|V_i\rangle + \beta e^{|\varphi|}|V_s\rangle|H_i\rangle,$$

where $H$ and $V$ are horizontal and vertical polarization states, and subscripts $s$ and $i$ stand for signal and idler paths. Coefficients $\beta$ and $\varphi$ are adjusted by manipulating the polarization of the pump to achieve a maximally entangled Bell state that we use for QKD.

![Entangled photon source.](image)

Fig. 5: Entangled photon source. A polarization-maintaining fibre (PMF) coupled pump laser (PL) generates a 405 nm beam (blue path), which is collimated with lens L1. The pump beam then passes a quarter- and a half-wave plate (QWP and HWP, respectively), which are used to adjust its polarization. Lens L2 focuses the pump beam at the non-linear crystal (NLC) located in the Sagnac loop. A dual-wavelength polarization beam-splitter (PBS) splits the pump beam into two counter-propagating beams. An additional HWP that rotates polarization by 90° is also required inside the loop to ensure proper operation. Thus pumped type-2 nonlinear crystal (ppKTP) emits down-converted photon pairs at 810 nm (red path) in both directions of the loop, which interfere at the PBS, finally generating entangled signal and idler photon pairs. To separate the signal photons from the pump beam, a dichroic mirror (DM) is used. Lenses L3 collect the entangled photons and subsequent band-pass filters (BPFs) spectrally filters them, before they are finally coupled into separate SMFs by the means of lenses L4.

Our ES can generate up to 1 million polarization entangled photon pairs per second with a spectral bandwidth of 0.4 nm and visibilities of up to 99.5% and 97.4% were measured for horizontal-vertical and diagonal-antidiagonal basis, respectively, in the low pump power limit. The source was built on an optical breadboard and housed in a wheeled 19-inch rack.

**Quantum receiver subsystem**

We developed two complete quantum receiver subsystems, one for Alice and one for Bob (QRS-A and QRS-B, respectively), for performing QKD based on the BBM92 protocol [32]. QRS-B is schematically shown in Fig. 6. Signal photons that come from the server via a free-space link are analysed in Bob’s polarization analysis module (PAM-B). Here, polarization is projected into one of two mutually unbiased bases, chosen at random for each photon, which is realized with a 50:50 beam-splitter (BS). Photons that are transmitted by the BS are projected into the horizontal-vertical basis by the means of a polarization-beam-splitter (PBS). In the reflection arm of the BS, the additional half-wave plate rotates polarization of the photons by 45°, which in turn makes the subsequent PBS project them into the
diagonal-antidiagonal basis. All the four outputs are finally coupled into multi-mode fibres using commercial fibre couplers and guided to the detectors. For detection, we use commercial single-photon avalanche diodes (SPADs) with detection efficiency of > 60%, dark count rate of < 500 counts/s, and timing resolution of 350 ps. Each SPAD click is given a precise arrival time by a rubidium clock driven time-tagging unit. Time-tags from both sides are synchronised and processed by a dedicated post-processing software, which finally generates secure encryption keys.

Fig. 6: Quantum receiver subsystem at Bob. a, The incoming free-space photons get sorted into 4 fibre channels according to their polarization state in the polarization analysis module (PAM-B) and detected with a single-photon avalanche detector (SPAD). Each SPAD click is given a precise arrival time by a rubidium clock (CLK) driven time-tagging (TT) unit. The post-processing software (PPS) processes the raw time-tags and generates secure encryption keys, which are fed to a key management system (KMS). From there, keys are pulled upon request for encryption (EC) of the classical communication channel between Alice and Bob. b, In PAM-B, a polarization controller (PC), consisting of a stack of waveplates, aligns Bob’s polarization frame of reference with that of Alice. Excess noise is removed with a spatial filter (SF) and a stack of interference filters (IF). A 50:50 beam-splitter (BS) realizes a random choice of the measurement basis. Transmitted photons are measured in the horizontal-vertical (HV) basis by the means of a polarization-beam-splitter (PBS), while reflected photons are measured in the diagonal-antidiagonal (DA) basis by the means of a half-wave plate and a PBS. All the four outputs are finally coupled into multi-mode fibres (MMFs) using fibre couplers (FCs).

Noise suppression turns out to be of critical importance when detecting signal in the single-photon regime. There are two most relevant sources of background noise that pollute our quantum channel. First, the dichroic mirror that separates beacon and quantum channels is not perfect, which results in a leakage of large numbers of beacon photons into PAM-B. The second source of noise, which becomes particularly critical in day time, is due to reflections and atmospheric scattering of sunlight within the intrinsic field-of-view of the receiver telescope. To reduce the noise, we employ filtering in all three degrees of freedom: spectral, spatial, and temporal. Spectral filtering is realized with a stack of commercial interference filters, resulting in a 3 nm wide pass-band (FWHM) around the signal wavelength of 810 nm. The spatial filter consists of a lens-based telescope with a tiny aperture in its focal plane [53, 54]. The aperture size is carefully chosen so that it transmits the majority of the incoming signal, while blocking a considerable portion of the noise. Temporal filtering, on the other hand, comes with coincidence-based detection, where only photon pairs that are detected within a time window of 1 ns at Alice and Bob – after the travel time difference due to different path lengths is taken into account – constitute the relevant signal in such an entanglement-based QKD scheme.

Finally, we need to ensure matching of polarization frames of reference at Alice and Bob. While each optical component along the path can in principle introduce some polarization transformation, by far the largest is due to the optical fibres that guide the photons from the ES. For this reason, PAM-B incorporates a polarization controller that consists of a stack of half- and quarter-wave plates in motorized rotation mounts. By rotating the wave plates, we can realize a transformation that inverts the
net transformation of the optical elements and fibres. To find the inverse transform in practice, we insert a polarizer into the entangled photon source to send a well-defined reference polarization to PAM-B and then use the polarization controller to maximize the signal in the corresponding detection channel. This polarization basis calibration only needs to be performed once before initiating the QKD, therefore active polarization control is not required.

QRS-A is almost identical to QRS-B – the only difference is in its PAM, which is a much more compact and simplified version of Bob’s. This is because QRS-A detects photons that are coming from the server via a single-mode fibre and is therefore not exposed to the free-space link environment and related challenges. The complete QRS-A was housed in a wheeled 19-inch rack, while PAM-B was mounted directly onto the receiver free-space terminal and the rest of the QRS-B was housed in a rack.

Sky brightness

To quantify sky brightness during our experiments, solar radiation data was extracted from the publically available database of the University of Applied Sciences Jena [55]. The measurements were performed with a pyranometer, which measures total incident solar radiation over the whole hemisphere in the spectral band between 300 nm and 2.8 μm. The pyranometer was located approximately 1.2 km from Alice and approximately 2.6 km from Bob. Although not measured exactly where our experiments took place, and despite being measured over a much broader spectral range compared to our QKD spectral filter bandwidth, it still offers a reasonable metric for quantifying sky brightness at the link. This is evident from the corellation between QBER and solar radiation during our daylight experiment on 24 February 2022, when the amount of cloud cover was dynamically changing throughout the day (Fig. 7e). Photos of the link during our daylight experiments, as seen looking from Bob towards Alice, are shown in Fig. 7a-d.

![Fig. 7: Sky brightness during daylight QKD experiments. a-d, View from Bob towards Alice (marked with the arrow) at different times, showing various daylight conditions during our experiments. e, Quantum bit error rate of our system and solar radiation measured at a weather station during one of our daylight experiments. (solar radiation data: University of Applied Sciences Jena)](image)

Post-processing and final key generation

The QKD post-processing software reads the raw key directly from the time-tagger units and executes a synchronization procedure. The final key is then reconciled in the following steps: delayed authentication initialization, sifting, error estimation, information reconciliation, correction confirmation, privacy amplification, and delayed authentication verification. Eventually, the final key is sent to a key buffer and is ready to be requested via an ETSI-004 based interface [56].
The first step of post-processing is to read data from the time-taggers. Alice and Bob exchange lists of time-tags and conduct time-bin synchronization in two steps. First, pre-synchronization is performed using a progressive cross-correlation-based $O(n \log n)$ algorithm to establish an initial clock offset over a wide range of multiple seconds. Once a coarse offset is found, fine synchronization works on a configurable smaller block size that depends on the number of detections (down to a minimum of $2^{10}$ detections). Fine synchronization is based on a discrete histogram-based linear-time algorithm. Events that coincide are passed to the next post-processing stage.

After pre-sifting, the delayed authentication according to [57] is initialized. To this end, the crypto context that is based on a polynomial hash is initialized with a pre-shared secret key $k$. From now on, every message $m$ that is exchanged between Alice and Bob is added to the authentication context $t$ by progressive hashing over the key

$$t' = (t + m) \ast k,$$

where $+$ and $\ast$ denote addition and multiplication in the finite field $\text{GF}(2^n)$ and $n$ denotes the size of the pre-shared secret key $k$ that can be configured to 32, 64, 96, 128, or 256 bit.

Next, the sifting stage compares the measurement bases of the detections and keeps only events that share the same basis. Afterwards, the error estimation stage discloses a configurable percentage of key data in order to estimate the quantum bit error rate (QBER) in the quantum channel. Information reconciliation is then performed according to the cascade protocol [58]. To ensure that the information reconciliation has been conducted successfully, the confirmation step compares a 96-bit hash of Alice and Bob’s key data. To this end, Alice and Bob perform a polynomial hash of the key data with a previously exchanged random number and exchange and compare the hash value. If Alice and Bob’s hash values are identical, in the next step, privacy amplification is done by universal Toeplitz hashing implemented using the number theoretic transform with a previously exchanged random seed. For experiments here, pseudo-random numbers have been used. However, our post-processing subsystem allows for a straightforward integration with a quantum random number source.

The final key length after privacy amplification is computed by estimating the amount of information an eavesdropper might get on the key by eavesdropping on the quantum channel and the post-processing communication [59, 60]. We compute the final key length as

$$N_{\text{fin}} = \max(N_{\text{in}} \tau(e) - N_{\text{dis}} - N_{\text{mar}}, 0),$$

with

$$\tau(e) = \begin{cases} 1 - (e \log_2(e) - (1 - e)\log_2(1 - e)), & \text{if } 0 < e \leq 0.5 \\ 1, & \text{if } e = 0 \\ 0, & \text{if } e > 0.5, \end{cases}$$

where $N_{\text{in}}$ is the input size, $N_{\text{dis}}$ is the number of bits disclosed in confirmation and correction, $N_{\text{mar}}$ is a configurable security margin (that includes finite-size corrections), and $e$ is the QBER.

After the privacy amplification has finished, the whole post-processing message exchange is authenticated with a message authentication code (MAC) using a (keyed) polynomial hash that is computed as described during pre-sifting initialization. The polynomial hash is one-time-padded (OTP) with a secure key to avoid data leakage. The keys needed to create the MACs are taken from an internal key-store of the post-processing software. The resulting authentication tags (one for incoming and one for outgoing communication) are exchanged and compared. In case of authentication success, the final key is pushed to the key management system (KMS) – a synchronized buffer where the key is stored. The KMS provides the keys via an ETSI004 based interface [56] featuring adapted ETSI004 use case 1 (one session, one client, one link).
References

[49] M. Goy et al., “High performance optical free-space links for quantum communications,” in *International Conference on Space Optics — ICSO 2020*, Online Only, France, Mar. 2021 - Apr. 2021, p. 18. [Online]. Available: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11852/2599163/High-performance-optical-free-space-links-for-quantum-communications/10.1117/12.2599163.full

[50] L. C. Andrews, *Field guide to atmospheric optics*. Bellingham, Washington, USA: SPIE Press, 2019.

[51] S. P. Neumann et al., “Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources,” *Phys. Rev. A*, vol. 104, no. 2, p. 226, 2021, doi: 10.1103/PhysRevA.104.022406.

[52] T. Kim, M. Fiorentino, and F. N. C. Wong, “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer,” *Phys. Rev. A*, vol. 73, no. 1, 2006, doi: 10.1103/PhysRevA.73.012316.

[53] M. T. Gruneisen, B. A. Sickmiller, M. B. Flanagan, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, “Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver,” *Opt. Eng.*, vol. 55, no. 2, p. 26104, 2016, doi: 10.1117/1.OE.55.2.026104.

[54] H. Ko et al., “Experimental filtering effect on the daylight operation of a free-space quantum key distribution,” *Scientific reports*, vol. 8, no. 1, p. 15315, 2018, doi: 10.1038/s41598-018-33699-y.

[55] Ernst-Abbe-Hochschule Jena, *Klimatologische Messstation*. [Online]. Available: http://wetter.mb.eah-jena.de/station/index.html

[56] *ETSI GS QKD 004 V2.1.1 (2020-08): Quantum Key Distribution (QKD); Application Interface*. [Online]. Available: https://standards.iteh.ai/catalog/standards/etsi/7568b28a-3cb2-450e-8c8a-cbbe01fe13d0/etsi-gs-qkd-004-v2-1-1-2020-08

[57] C. Pacher, G. Lechner, C. Portmann, O. Maurhart, and M. Peev, “Efficient QKD postprocessing algorithms,” 2nd Annual Conference on Quantum Cryptography (QCrypt), 2012.

[58] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, “Demystifying the Information Reconciliation Protocol Cascade,” *Quantum Information & Computation*, 2015. [Online]. Available: http://arxiv.org/pdf/1407.3257v2

[59] A. M. Abbas, A. Goneid, and S. El-Kassas, “Privacy Amplification in Quantum Cryptography BB84 using Combined Unursal2-True Random Hashing,” *International Journal of Information & Network Security (IJINS)*, vol. 3, no. 2, pp. 98-115, 2014.

[60] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, “Generalized Privacy Amplification,” *IEEE International Symposium on Information Theory*, p. 350, 1995.