Article

A device-independent quantum key distribution system for distant users

https://doi.org/10.1038/s41586-022-04891-y

Received: 8 October 2021

Accepted: 20 May 2022

Published online: 27 July 2022

Open access

Check for updates

Wei Zhang[1,2,9], Tim van Leent[1,2,9], Kai Redeker[1,2,9], Robert Garthoff[1,2,9], René Schwonnek[3,4], Florian Fertig[1,2], Sebastian Eppelt[1,2], Wenjamin Rosenfeld[1,2], Valerio Scarani[5,6], Charles C.-W. Lim[4,5,8] ✉ & Harald Weinfurter[1,2,7] ✉

Device-independent quantum key distribution (DIQKD) enables the generation of secret keys over an untrusted channel using uncharacterized and potentially untrusted devices[1–9]. The proper and secure functioning of the devices can be certified by a statistical test using a Bell inequality[10–12]. This test originates from the foundations of quantum physics and also ensures robustness against implementation loopholes[13], thereby leaving only the integrity of the users' locations to be guaranteed by other means. The realization of DIQKD, however, is extremely challenging—mainly because it is difficult to establish high-quality entangled states between two remote locations with high detection efficiency. Here we present an experimental system that enables for DIQKD between two distant users. The experiment is based on the generation and analysis of event-ready entanglement between two independently trapped single rubidium atoms located in buildings 400 metre apart[14]. By achieving an entanglement fidelity of $\mathcal{F} \geq 0.892(23)$ and implementing a DIQKD protocol with random key basis[15], we observe a significant violation of a Bell inequality of $S = 2.578(75)$—above the classical limit of 2—and a quantum bit error rate of only 0.078(9). For the protocol, this results in a secret key rate of 0.07 bits per entanglement generation event in the asymptotic limit, and thus demonstrates the system's capability to generate secret keys. Our results of secure key exchange with potentially untrusted devices pave the way to the ultimate form of quantum secure communications in future quantum networks.

Secure communication over public channels requires the users to share a common secret key. Today, this crucial task faces major challenges from quantum-based attacks and implementation vulnerabilities. A promising solution is to use quantum key distribution (QKD), which uses the laws of quantum physics to assess eavesdropping attempts on the public channel[16,17]. However, in its standard form, QKD is prone to implementation side channels, like all modern information systems[13,18]. In particular, the security of QKD is also based on the mathematical models of the devices, so it is absolutely essential that the quantum devices are behaving as specified during the protocol execution.

Device-independent QKD[1–9] (DIQKD) is an advanced form of QKD. First proposed by Mayers and Yao[1], it warrants the proper and secure functioning of the underlying devices by a Bell test[11], in which the users only need to analyse their input–output measurement data to establish an upper limit on the amount of information that an eavesdropper could have gained during the protocol. Importantly, this verification step eliminates the need to characterize the quantum devices and hence DIQKD is naturally robust against implementation flaws.

To implement DIQKD, a system is required that distributes high-quality entangled states with high detection efficiency between two remote locations. More specifically, the system needs to achieve both high Bell violation and low quantum bit error rate (QBER) to generate secret keys. State-of-the-art systems can achieve high Bell violations between distant particles[14,19–21], but are not good enough to generate a secret key in the device-independent setting[22]. In a recent effort to relax the system requirements various improved designs of the original DIQKD protocol[2,3] were introduced, for example, on the basis of noisy preprocessing[23], randomized key settings[15] and random post-selection[24]. Simultaneously to this work, two proof-of-concept DIQKD experiments were performed: one demonstrated finite-key distribution over 2 m using trapped ions[25] and the other verified that a photonic implementation over up to 220 m of fibre is within reach[26].

Here, we report on an experimental system that enables DIQKD between two distant users. It combines experimental advances in a previous loophole-free Bell test experiment[14] with the DIQKD protocol proposed in ref. [15]. The quantum channel is formed by two single ^{87}Rb atoms, trapped and manipulated individually in buildings approximately 400 m line-of-sight apart. More specifically, entanglement between the two atoms is created through an event-ready entanglement swapping scheme, which is performed across a 700 m long optical fibre connecting the two buildings. Substantial improvements in the entanglement quality, entanglement generation rate and noise tolerance of

[1] Fakultät für Physik, Ludwig-Maximilians-Universität, München, Germany. [2] Munich Center for Quantum Science and Technology (MCQST), München, Germany. [3] Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Siegen, Germany. [4] Department of Electrical & Computer Engineering, National University of Singapore, Singapore, Singapore. [5] Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore. [6] Department of Physics, National University of Singapore, Singapore, Singapore. [7] Max-Planck Institut für Quantenoptik, Garching, Germany. [8] Present address: JPMorgan Chase, Singapore, Singapore. [9] These authors contributed equally: Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff. ✉e-mail: charles.lim@nus.edu.sg; h.w@lmu.de

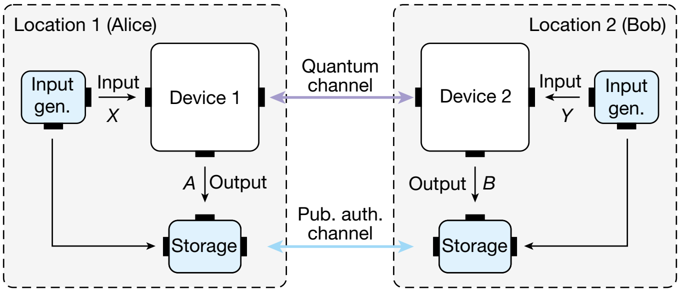

Fig. 1 | Schematic of a DIQKD scheme. Each of the two parties, Alice and Bob, holds QKD devices, which are connected by a quantum channel. The devices receive the inputs *X* and *Y*, and respond with outputs *A* and *B*, respectively. To run the protocol each party needs a trusted supply of inputs and a trusted local storage unit to store both output and inputs. Additionally, a trusted authenticated public channel (pub. auth. channel) between the two parties is necessary for exchange of information during post-processing. gen., generation.

the protocol enable the system to achieve a positive secret key rate (the ratio of achievable secret key length to the total number of heralded events) of 0.07 bits in a fully device-independent configuration.

DIQKD protocol

Let us first review the basic assumptions of DIQKD. The two users, Alice and Bob, should (1) each hold a device that is able to receive an input and then respond with an unambiguous output that can be used to generate a secure key (Fig. 1). The communication between their devices is limited to what is necessary to generate a secure key, namely, (2) the users control when their respective devices communicate with each other[27]; and (3) the devices do not send unauthorized classical information to an eavesdropper. Finally, as it is with any QKD protocol, it is required that (4-a) quantum mechanics is correct, (4-b) the users' inputs are private and random and (4-c) the users are connected by an authenticated classical channel and use trusted post-processing methods. For more details, we refer the interested reader to Supplementary Appendix A.

The DIQKD protocol considered here is similar to the original DIQKD protocol[2,3], except that two measurement settings are used for key generation instead of one. Importantly, in doing so, the protocol can tolerate more system noise—the critical QBER increases from 0.071 to 0.082 (ref. [15]). The protocol considers that Alice and Bob each hold a device, which are connected by a quantum channel (Fig. 1). In each *i*th of *N* measurement rounds, one of four different inputs $X_i \in \{0, 1, 2, 3\}$ is given to Alice's device, whereas Bob's device receives one of two possible values $Y_i \in \{0, 1\}$. The input for each round is provided by a trusted local source of randomness. Both devices output two possible values, $A_i \in \{\uparrow, \downarrow\}$ at Alice's side and $B_i \in \{\uparrow, \downarrow\}$ at Bob's side. The input and output values are recorded and stored in independent, local secured storage.

After *N* rounds classical post-processing starts, with Alice and Bob revealing their inputs for each round over an authenticated public channel. For the rounds with differing input settings, that is, $X_i \in \{2, 3\}$ together with $Y_i \in \{0, 1\}$, the outputs are shared over the public channel to compute the Clauser–Horne–Shimony–Holt (CHSH)[28] value using

$$S := E_{2,1} - E_{2,0} - E_{3,0} - E_{3,1}, \tag{1}$$

where the correlation functions are defined as $E_{X,Y} := p^{A=B}_{X,Y} - p^{A\neq B}_{X,Y}$. Probabilities of the form $p^{A,B}_{X,Y}$ are estimated by the ratio $N^{A,B}_{X,Y}/N_{X,Y}$ of the number of rounds with outcomes (A, B) for input combination (X, Y), to the total number of rounds with those inputs. Provided that the devices share a sufficiently entangled state, the Bell inequality can be violated, that is, $S > 2$.

The raw data are sifted so that only the outputs of measurement rounds with identical input settings are kept for further processing. The QBERs for both key settings are denoted by $Q_0 = N^{A=B}_{0,0}/N_{0,0}$ for $X_i = Y_i = 0$ and $Q_1 = N^{A=B}_{1,1}/N_{1,1}$ for $X_i = Y_i = 1$. Note that the key pairs are anticorrelated when using anticorrelated entangled states. Both the QBERs (Q_0, Q_1) and the CHSH value *S* are used to determine the amount of information about the sifted key that could have been obtained by an eavesdropper[29]. Next, by applying a technique known as leftover hashing, the eavesdroppers (quantum) information about the final key can be reduced to an arbitrary low level, defined by the security error of the protocol[30]. In this experiment, we focus on estimating the asymptotic security performance of the considered DIQKD protocol. For this purpose, we note that in the asymptotic limit and in case of a depolarizing quantum channel, positive key rates can be achieved when the expected CHSH value satisfies $S > 2.362$ (or equivalently, $Q < 0.082$ with $Q_0 = Q_1 = Q$)[15].

Quantum network link

A quantum network link (QNL) generates the entanglement to implement the DIQKD protocol. In our set-up, event-ready entanglement is generated between two optically trapped single ^{87}Rb atoms located in laboratories 400 m apart and connected by a 700 metre long optical fibre channel (Fig. 2). The atoms act as quantum memories in which a qubit is encoded in the Zeeman substates of the $5S_{1/2}|F = 1, m_F = \pm 1\rangle$ ground state, with $m_F = +1$ and $m_F = -1$ designated as computational basis states, $|\uparrow\rangle_z$ and $|\downarrow\rangle_z$, respectively, and where the quantization axis $\hat{z}$ is defined by the fluorescence collection set-up.

The two distant atoms are entangled using an entanglement swapping protocol[31]. The sequence starts by synchronously exciting the single atom in each trap to the state $5^2P_{3/2}|F' = 0, m_{F'} = 0\rangle$; when decaying to the ground state, each of the atomic qubits becomes entangled with the polarization of the respective spontaneously emitted single photon (Fig. 3a). The two photons are then guided to a Bell-state measurement (BSM) set-up using two-photon interference. Projection of the photons onto a $|\Psi^+\rangle$ state heralds the creation of the maximally entangled atom–atom state

$$|\Psi^+\rangle_{AB} = \frac{|\uparrow\rangle_{x,A}|\downarrow\rangle_{x,B} + |\downarrow\rangle_{x,A}|\uparrow\rangle_{x,B}}{\sqrt{2}}. \tag{2}$$

Given a successful projection, a 'ready' signal is sent to the trap set-ups, initiating the next measurement round for which, depending on input values X_i and Y_i, the two atomic qubits are independently analysed by state-selective ionization (Fig. 3b)[32]. There, a particular state of the atomic qubit is ionized and leaves the trap depending on the polarization $\zeta = \cos(\gamma)V + e^{-i\phi}\sin(\gamma)H$ of a read-out laser pulse ($\gamma = \alpha$ for Alice's and $\gamma = \beta$ for Bob's device). If the atom is still in the trap, it is thus projected onto the state

$$|D\rangle = \sin(\gamma)|\downarrow\rangle_x - e^{-i\phi}\cos(\gamma)|\uparrow\rangle_x = |\uparrow\rangle. \tag{3}$$

The presence of the atom is then tested using fluorescence collection at 780 nm, which yields the final measurement outcomes A_i and B_i, respectively. On Alice's side, the single-photon detectors of the BSM detect the fluorescence of the atom, whereas on Bob's side an unbalanced beam splitter directs a small fraction of the florescence light onto a single single-photon detector (Fig. 2). As the results are reported every time, the detection efficiencies of Alice's and Bob's measurements are effectively one. Any component loss or ionization inefficiency contributes to the noise in the quantum channel.

The requirements for DIQKD implementation are less stringent with the newly proposed protocols; however, substantial improvements over existing loophole-free Bell experiments were still required. To that end,

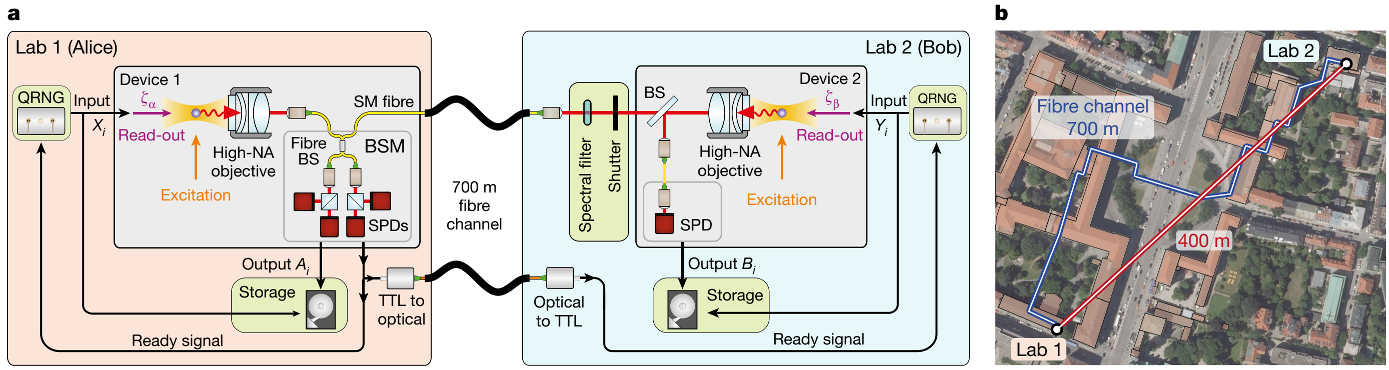

Fig. 2 | Overview of the DIQKD system. a, Alice's equipment (Device 1 in Lab 1) is formed by a single-atom trap and a BSM set-up. Bob (Device 2 in Lab 2) uses a second single-atom trap together with a 90:10 (T:R) beam splitter (BS) and a single-photon detector (SPD). Each trap set-up contains a high numerical aperture (NA) objective to optically trap a single atom and collect atomic fluorescence into a single-mode (SM) fibre. The atoms are entangled in an event-ready scheme by synchronously exciting them, after which the spontaneously emitted photons are collected by high-NA objectives and guided to the BSM. Here, a coincidental photon detection on two detectors in the same output arm of the fibre BS heralds the entangled atom–atom state $|\Psi^+\rangle$, which is announced to both users by a 'ready' signal. After receiving the ready signal, two quantum random number generators (QRNGs) select the inputs to the devices, determining the polarization of a read-out pulse in a state-selective ionization scheme. The binary output of the devices is determined from a fluorescence measurement of atom presence after the ionization attempt, as ionized atoms are lost from the trap. The inputs and outputs of each round are stored locally using a trusted storage. In Lab 2 a spectral filter and shutter are implemented to avoid leakage of the inputs and outputs of the device. **b**, Map showing the main campus of the LMU in Munich, indicating the locations of the two laboratories. Map data in **b** are from Bayerische Vermessungsverwaltung .

we enhanced the entanglement generation rate, coherence of atomic states and entanglement swapping fidelity (Methods).

DIQKD implementation

The independent random inputs to the devices (requirement (4-b)) are provided by independent quantum random number generators with a bias lower than 10^{-5} located in each laboratory[14,33]. At Alice's side, two random bits are used to select the input, whereas at Bob's side only one random bit is used, leading to uniformly distributed input combination choices. For the generated entangled state equation (2) and the atomic-state measurement scheme equation (3), the input values $X \in \{0, 1, 2, 3\}$ convert to measurement angles $\alpha \in \{-22.5^\circ, +22.5^\circ, -45^\circ, 0^\circ\}$ for Alice's device, whereas $Y \in \{0, 1\}$ translates to $\beta \in \{+22.5^\circ, -22.5^\circ\}$ for Bob's device. The capability for fast switching between various read-out settings is achieved by overlapping multiple read-out beams with different polarization and individually controllable intensities[14]. The outputs $A, B \in \{\uparrow, \downarrow\}$ are derived from the fluorescence counts after the state-selective ionization. Finally, the users' inputs and outcomes are stored in two independent, trusted secure storages (requirement 4-c).

Unauthorized incoming and outgoing communication of the laboratories can be prevented with prudent steps (requirements (2) and (3)). Especially on Bob's side, extra measures are taken to prevent information leakage from the laboratory: a free-space shutter is closed during the read-out process to keep the leakage of fluorescence light into the optical fibre and the outside environment to well below one photon per read-out event (Fig. 2), and the trap is always emptied before reopening the shutter. Owing to the approximate 5 ms reaction time of the shutter, a spectral filter (10^{-6} transmission at 795 nm) is deployed to block the read-out pulse after interacting with the atom and to prevent unintentional transmission of the read-out setting. For Alice's side, such countermeasures are not needed as the BSM set-up already serves as a natural blocker[34].

System measurements and performance

The inputs and outputs of the devices were recorded for $N = 3{,}342$ rounds over a measurement period of 75 h. The resulting output (anti) correlation probabilities for the eight different input combinations, that is, $N^{A=B}_{X,Y}/N_{X,Y}$ and $N^{A\neq B}_{X,Y}/N_{X,Y}$, are shown in Fig. 4.

It is instructive to first review the increased performance of the QNL independently of the DIQKD protocol. Here, the figure of merit is the fidelity of the observed entangled atom–atom state relative to a maximally entangled state. By fitting the data (Fig. 4) with sinusoidal functions, the estimated visibility for input combinations $X = 2, 0, 3, 1$ and $Y = 0$ (respectively $X = 2, 0, 3, 1$ and $Y = 1$) is 0.869(25) (respectively 0.888(45)). Then, averaging the found visibilities and taking into account that a third atomic ground-level spin state can be populated ($5^2S_{1/2}|F = 1, m_F = 0\rangle$), a lower bound on the fidelity is given by $\mathcal{F} \geq 0.892(23)$ (ref. [35]).

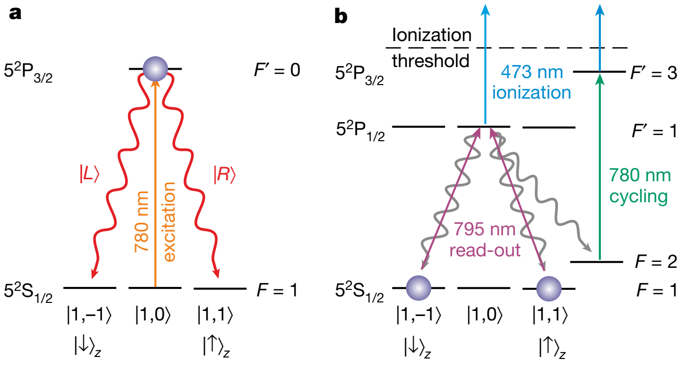

Fig. 3 | Schematics of the entanglement generation and atomic-state read-out schemes. a, An entangled atom–photon state is generated by the spontaneous emission of a photon subsequent to excitation of the atom. Decay from the state $5^2P_{3/2}|F' = 0, m_{F'} = 0\rangle$ results in an entangled atom–photon state $|\Psi\rangle_{AP} = 1/\sqrt{2}\,(|\downarrow\rangle_x|H\rangle + |\uparrow\rangle_x|V\rangle)$[41], where $|\uparrow\rangle_x := 1/\sqrt{2}\,(|\uparrow\rangle_z + |\downarrow\rangle_z)$ (respectively $|\downarrow\rangle_x := i/\sqrt{2}\,(|\uparrow\rangle_z - |\downarrow\rangle_z)$) and $|H\rangle$ and $|V\rangle$ denote parallel and orthogonal linear polarizations with respect to the optical table, respectively, with $|V\rangle := 1/\sqrt{2}\,(|L\rangle + |R\rangle)$ and $|H\rangle := i/\sqrt{2}\,(|L\rangle - |R\rangle)$. **b**, The atomic qubit state is read out by a state-dependent ionization scheme. First, a certain superposition of the qubit state is excited to the $5^2P_{1/2}$ level depending on a respective polarization of the so-called read-out laser light ($\lambda = 795$ nm). The excited atom is ionized by a bright second laser applied simultaneously at $\lambda = 473$ nm. If the atom decays to the state $5^2S_{1/2}|F = 2\rangle$ before it is ionized, it is excited to the state $5^2P_{3/2}|F' = 3\rangle$ with the third excitation laser at $\lambda = 780$ nm, which is ionized as well.

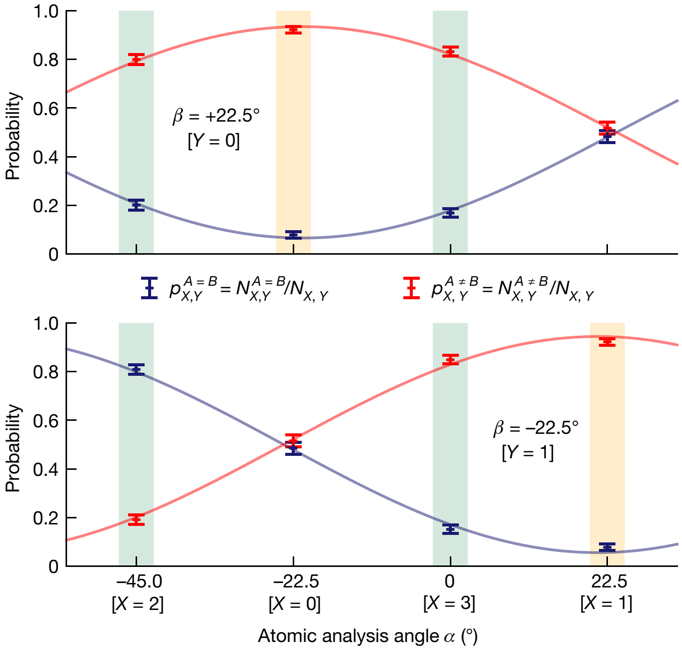

Fig. 4 | Atom–atom state correlations. The correlations $E_{X,Y}$ are obtained from the correlation (blue) and anticorrelation (red) probabilities of the device outputs for the eight input combinations. The data are fitted with sinusoidal functions estimating visibilities of 0.869(25) and 0.888(45). The settings for $X = 2$ or $X = 3$ (green background) contribute to the evaluation of the Bell parameter $S = 2.578(75)$, whereas the QBER $Q = 0.078(9)$ follows from settings with $X = Y$ (yellow background). The error bars indicate statistical errors of one standard deviation. $N = 3,342$.

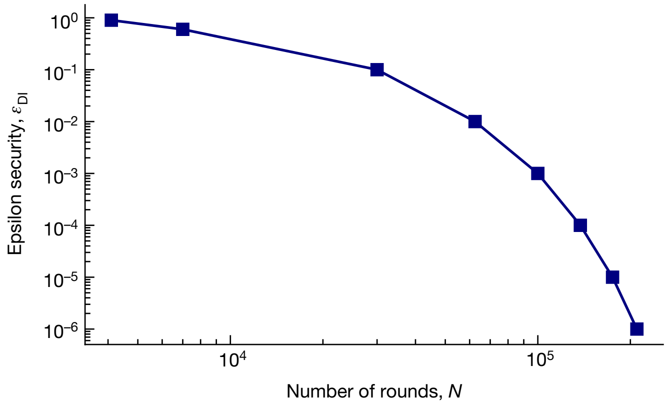

Fig. 5 | Finite-key simulation for the robust DIQKD protocol. Shown is the minimum number of rounds, that is, block length, required to distribute a finite key with a certain epsilon security, considering collective attacks and uniformly distributed measurement settings. The channel parameters S, Q_0 and Q_1 are set to the observed values in the experiment. A non-asymptotic security of $\varepsilon_{\rm DI} = 10^{-5}$ is considered to be realistic for cryptography applications.

The CHSH value is found to be $S = 2.578(75)$ using equation (1) with $E_{2,0} = -0.599(41)$, $E_{3,0} = -0.664(36)$, $E_{2,1} = 0.618(39)$ and $E_{3,1} = -0.697(35)$. The QBERs are given by the correlation data for $X = Y$, that is, $Q_0 = 0.0781(127)$ and $Q_1 = 0.0777(132)$, which gives an average error rate of $Q = 0.078(9)$. For the considered DIQKD protocol and the uniformly distributed measurement settings, the observed S value and QBER result in a secret key rate of 0.07 bits in the asymptotic limit, out of a maximum achievable value of 0.25—showing that the system is capable of performing DIQKD between two users 400 m apart. To quantify the confidence of this estimate, we assume that underlying input–output probability distributions are independent and identically distributed and use standard Bayesian methods to determine the uncertainties of the estimated parameters. We find that taking the worst-case estimates of S (2.4256), Q_1 (0.107) and Q_2 (0.107) using a common probability error of 3% still give a positive rate. We note that, thanks to the high-quality entanglement, also the original DIQKD protocol[2,3] achieves a positive key rate for the observed S and Q_0 (or Q_1), but only for a larger common probability error.

In addition, using state-of-the-art finite-key analysis[30] for the protocol, we find that for a typical security error value of $\varepsilon_{\rm DI} = 10^{-5}$ a secure key can be obtained with a minimum block length of 1.75×10^5, as shown in Fig. 5. Here, $\varepsilon_{\rm DI}$ is the security error of the protocol and can be seen as the probability that the protocol fails in its task, for example, that the final key pair is not secret[36]. In the simulation, we consider collective attacks, an error correction efficiency of 1.15 and uniformly distributed measurement settings for Alice and Bob.

Discussion and outlook

In this work, we present an experimental system that is capable of achieving positive asymptotic key rates between users separated by 400 m line-of-sight (700 m fibre length) in a fully device-independent setting. Although the current set-up outperforms existing loophole-free Bell set-ups, there are still several areas that require improvements for implementing DIQKD with finite-key security and longer reach.

For one, a higher event rate is required to obtain finite-key security within a practical time. The event rate critically depends on the entanglement generation efficiency and the repetition rate. To increase the former, several improvements are possible, for example, improving the BSM set-up fidelity to include the $|\Psi^-\rangle$ state projection would increase the entanglement generation rate by a factor of 2. Furthermore, it is possible to scale up the number of atom traps using multidimensional arrays[37–39], which, combined with time multiplexing techniques[40], could increase the event rate by several orders of magnitude (Supplementary Appendix H).

Another direction is to improve the reach of the QNL. Here, a limiting factor is attenuation loss of the 780 nm photons in long optical fibres, which is already 50% for a 700 m long link. To overcome losses in longer fibre links, a promising solution is to convert the entangled single photons to the low-loss telecom band by polarization-preserving quantum frequency conversion[32]. Recent results demonstrate extension of the QNL to 33 km fibre length[35] and show that high-quality entanglement over distances up to 100 km is achievable.

In summary, our results represent a major step towards the goal of ultimate secure communication based solely on the laws of physics. They indicate that state-of-the-art quantum links are capable of generating secret keys. Moreover, they show that future quantum networks distributing entanglement between their nodes can harness this quantum advantage, making DIQKD the standard for secure communications.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41586-022-04891-y.

1. Mayers, D. and Yao, A. Quantum cryptography with imperfect apparatus. In *Proc. 39th Annual Symposium on Foundations of Computer Science* 503–509 (IEEE, 1998).
2. Acn, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
3. Pironio, S. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
4. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).

5. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456–460 (2013).
6. Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X* **3**, 031006 (2013).
7. Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
8. Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM* **63**, 1–63 (2016).
9. Arnon-Friedman, R. et al. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **9**, 459 (2018).
10. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fizik.* **1**, 195–200 (1965).
11. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
12. Scarani, V. *Bell Nonlocality* (Oxford Univ. Press, 2019).
13. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
14. Rosenfeld, W. et al. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017).
15. Schwonnek, R. et al. Device-independent quantum key distribution with random key basis. *Nat. Commun.* **12**, 2880 (2021).
16. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
17. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661663 (1991).
18. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
19. Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3kilometres. *Nature* **526**, 682–686 (2015).
20. Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
21. Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
22. Murta, G. et al. Towards a realization of device-independent quantum key distribution. *Quantum Sci. Technol.* **4**, 035011 (2019).
23. Ho, M. et al. Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 230502 (2020).
24. Xu, F., Zhang, Y.-Z., Zhang, Q. & Pan, J.-W. Device-independent quantum key distribution with random postselection. *Phys. Rev. Lett.* **128**, 110506 (2022).
25. Nadlinger, D. P. et al. Experimental quantum key distribution certified by Bell's theorem. *Nature* https://doi.org/10.1038/s41586-022-04941-5 (2002).
26. Liu, W.-Z. et al. Photonic verification of device-independent quantum key distribution against collective attacks. Preprint at https://arxiv.org/abs/2110.01480 (2021).
27. Arnon-Friedman, R., Renner, R. & Vidick, T. Simple and tight device-independent security proofs. *SIAM J. Comput.* **48**, 181–225 (2019).
28. Clauser, J. F. et al. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880884 (1969).
29. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **6**, 1–127 (2008).
30. Tan, E. Y. Z. et al. Improved DIQKD protocols with finite-size analysis. Preprint at https://arxiv.org/abs/2012.08714 (2020).
31. Hofmann, J. et al. Heralded entanglement between widely separated atoms. *Science* **337**, 72–75 (2012).
32. van Leent, T. et al. Long-distance distribution of atom-photon entanglement at telecom wavelength. *Phys. Rev. Lett.* **124**, 010510 (2020).
33. Fürst, M. High speed optical quantum random number generation. *Opt. Express* **18**, 1302913037 (2010).
34. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
35. van Leent, T. et al. Entangling single atoms over 33 km telecom fibre. *Nature* https://doi.org/10.1038/s41586-022-04764-4 (2022).
36. Portmann, C. & Renner, R. Security in quantum cryptography. Preprint at https://arxiv.org/abs/2102.00021 (2021).
37. Endres, M. et al. Atom-by-atom assembly of defect-free one-dimensional cold atom arrays. *Science* **354**, 1024–1027 (2016).
38. Barredo, D., De Léséleuc, S., Lienhard, V., Lahaye, T. & Browaeys, A. An atom-by-atom assembler of defect-free arbitrary two-dimensional atomic arrays. *Science* **354**, 1021–1023 (2016).
39. Ohl de Mello, D. et al. Defect-free assembly of 2D clusters of more than 100 single-atom quantum systems. *Phys. Rev. Lett.* **122**, 203601 (2019).
40. Schupp, J. et al. Interface between trapped-ion qubits and traveling photons with close-to-optimal efficiency. *PRX Quantum* **2**, 020331 (2021).
41. Volz, J. et al. Observation of entanglement of a single photon with a trapped atom. *Phys. Rev. Lett.* **96**, 030404 (2006).
42. Rosenfeld, W. *Experiments with an Entangled System of a Single Atom and a Single Photon*. PhD thesis, Ludwig-Maximilians-Universität München (2008).

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Methods

Increased entanglement generation rate

Custom-designed high-numerical aperture objectives are installed in each trap to increase the single-photon collection efficiency by a factor greater than 2.5. This ultimately leads to an atom–atom entanglement generation efficiency of 0.49×10^{-6} following an excitation attempt. Together with a duty cycle of approximately ½ and a repetition rate of the entanglement generation tries of 52 kHz, this results in an event rate of $1/82\ \mathrm{s}^{-1}$. Note that for event-ready entanglement generation schemes the repetition rate of the experiment is limited by the communication times between the two devices and the BSM[35]. For DIQKD protocols, this results in a trade-off between the maximum separation of the users and the achieved secret key rate.

Atomic coherence time

The coherence and stability of the atomic qubit states are limited by the fluctuations of local magnetic fields and position-dependent vector light shifts, which are introduced by the tight focus of the optical dipole traps. The latter is especially crucial as it enables a high-fidelity state measurement only when the atom has completed a full transverse oscillation in the trap[42]. Here, the better optical components of the new collection set-up, which is also used to focus the trapping laser, improve the spatial symmetry of the trapping potential and thereby enable a better cancellation of dephasing effects. In combination with lowering the atom temperatures and applying a magnetic bias field, this extends the coherence time to approximately 330 μs. This results in a lower bound on the atom–photon entanglement fidelity of 0.952(7) and 0.941(7) (relative to a maximally entangled state) for Alice's and Bob's set-ups, respectively. We refer the interested reader to Supplementary Appendix B for more details.

BSM fidelity

The quality of the entangled atom–atom state is further improved by optimizing the two-photon interference of the BSM on the basis of a rigorous analysis of the atom–photon entanglement generation process. Here, the multilevel structure of ^{87}Rb, the finite duration of the excitation pulse and experimental imperfections lead to the possibility of two-photon emission from one atom. Crucially, these multiphoton events reduce the fidelity of the BSM result. To overcome this, only photons that are emitted after the end of the previous excitation pulse are accepted in the BSM. This time filtering reduces the entanglement generation rate by a factor of 4 (resulting in the entanglement generation rate mentioned before), but greatly increases the fidelity of the generated state (see Supplementary Appendix C for more details).

Data availability

The datasets generated and/or analysed during the experiment are available from the corresponding authors on reasonable request.

Code availability

The code supporting the plots within this paper is available from the corresponding authors upon reasonable request.

Acknowledgements We thank I. W. Primaatmaja, E. Y.-Z. Tan and K. T. Goh for useful inputs and discussions. W.Z., T.v.L., K.R., R.G., F.F., S.E., W.R. and H.W. acknowledge funding by the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung (BMBF)) within the project Q.Link.X (16KIS0880), QR.X (16KISQ002) the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy (EXC-2111–390814868) and the Alexander von Humboldt foundation. C.C.-W.L. and R.S. are funded by the National Research Foundation, Singapore, under its NRF Fellowship programme (NRFF11-2019-0001) and NRF Quantum Engineering Programme 1.0 (QEP-P2). V.S. and C.C.-W.L. acknowledge support from the National Research Foundation and the Ministry of Education, Singapore, under the Research Centres of Excellence programme.

Author contributions C.C.-W.L. proposed the project and collaboration. W.Z., T.v.L., R.G., K.R., R.S., W.R., C.C.-W.L. and H.W. designed the experiment. W.Z., T.v.L. and R.G. performed the experiments, together with F.F. and S.E. T.v.L. analysed the data. R.S. and C.C.-W.L. performed the key rate simulations. T.v.L., K.R., C.C.-W.L., V.S. and H.W. wrote the manuscript based on input from all other authors.

Competing interests The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41586-022-04891-y.
Correspondence and requests for materials should be addressed to Charles C.-W. Lim or Harald Weinfurter.
Peer review information *Nature* thanks Lynden Shalm and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.
Reprints and permissions information is available at http://www.nature.com/reprints.