Experimental device-independent quantum key distribution between distant users

Charles Lim (✉ charles.lim@nus.edu.sg)

National University of Singapore <https://orcid.org/0000-0002-2332-4126>

Wei Zhang

LMU München

Tim Leent

LMU München

Kai Redeker

LMU München

Robert Garthoff

LMU München

Rene Schwonnek

National University of Singapore

Florian Fertig

LMU München

Sebastian Eppelt

LMU München

Valerio Scarani

National University of Singapore

Harald Weinfurter

LMU München

Wenjamin Rosenfeld

LMU München

Physical Sciences - Article

Keywords: secure key, Rubidium 87 atoms, DIQKD

Posted Date: October 21st, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-960507/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Version of Record: A version of this preprint was published at Nature on July 27th, 2022. See the published version at <https://doi.org/10.1038/s41586-022-04891-y>.

Experimental device-independent quantum key distribution between distant users

Wei Zhang,^{1,2,*} Tim van Leent,^{1,2,*} Kai Redeker,^{1,2,*} Robert Garthoff,^{1,2,*}
René Schwonnek,^{3,4} Florian Fertig,^{1,2} Sebastian Eppelt,^{1,2} Wenjamin Rosenfeld,^{1,2}
Valerio Scarani,^{5,6} Charles C.-W. Lim,^{3,5,†} and Harald Weinfurter^{1,2,7,‡}

¹*Fakultät für Physik, Ludwig-Maximilians-Universität, München, Germany*

²*Munich Center for Quantum Science and Technology (MCQST), München, Germany*

³*Department of Electrical & Computer Engineering, National University of Singapore, Singapore*

⁴*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Germany*

⁵*Centre for Quantum Technologies, National University of Singapore, Singapore*

⁶*Department of Physics, National University of Singapore, Singapore*

⁷*Max-Planck Institut für Quantenoptik, Garching, Germany*

(Dated: October 19, 2021)

Device-independent quantum key distribution (DIQKD) is the art of using untrusted devices to establish secret keys over an untrusted channel [1–8]. So far, the real-world implementation of DIQKD remains a major challenge, as it requires a loophole-free Bell test with very high quality entanglement and detection efficiency across two remote locations to ensure secure key exchange. Here, we demonstrate for the first time the distribution of a secure key—based on asymptotic security estimates—in a fully device-independent way between two users separated by 400 metres. The experiment is based on heralded entanglement between two independently trapped single Rubidium 87 atoms. The implementation of a robust DIQKD protocol indicates an expected secret key rate of $r = 0.07$ per entanglement generation event. Furthermore, we analyse the experiment’s capability to distribute a secret key with finite-size security against collective attacks.

Quantum key distribution (QKD) [9, 10] uses the unique features of quantum mechanics to exchange provably-secure secret keys over an untrusted network. The technology is now well established in a wide variety of network settings [11–20] and commercial QKD systems are available. QKD protocols are designed to detect eavesdropping attacks on the quantum channel based on fundamental quantum effects like the no-cloning theorem and the uncertainty principle. In order to invoke these effects, most QKD protocols require that the underlying quantum devices are well characterised and are accurately described by the mathematical models used in the security analysis. The users of such protocols must trust not only the honesty of the QKD vendors, but also the specifications provided by them. This may be critical: indeed, it has been known for at least a decade that some QKD devices can be readily hacked from the out-

side by exploiting physical features that had not been deemed relevant in a first analysis [21].

To overcome the above issues, a promising solution is to use device-independent QKD (DIQKD)—an entanglement-based method which allows the users to exchange secret keys with uncharacterised (or untrustworthy) quantum devices. First introduced by Mayers and Yao [1], DIQKD [2–8] ensures the proper and secure functioning of the underlying QKD devices via a loophole-free Bell test [22, 23]. More specifically, the users only need to analyse their input-output measurement statistics to put an upper bound on the amount of information leaked to an eavesdropper, hence eliminating the requirement to characterise the devices. DIQKD at the same time automatically provides security against implementation flaws and especially any form of misalignment. It only requires a few very basic assumptions to be fulfilled.

For the ease of reference, let us list these basic requirements of DIQKD (see the Supplemental Material A for more details). The two DIQKD users, Alice and Bob, (i) should each hold a device that is able to receive an input and then respond with an unambiguous output, as illustrated in Fig. 1. The communication between these devices is assumed to be restricted, namely (ii) the users control when their respective devices communicate with each other [24]; and (iii) the devices do not send unauthorised classical information to an eavesdropper. Finally, as it is with any QKD protocol, it is required that (iv-a) quantum mechanics is correct, (iv-b) the users’ inputs are private and random, and (iv-c) the users are connected via an authenticated classical channel and the post-processing platform is trusted.

The experimental realisation of DIQKD is, however, a major challenge. The main difficulty is to devise a system that enables for a loophole-free Bell test while achieving both an high Bell violation and a low quantum bit error rate (QBER). Current state-of-the-art loophole-free Bell experiments [25–28] are able to achieve significant Bell violations, but the QBERs are still not good enough for DIQKD (e.g., see the survey provided by Ref. [29]). To lower these requirements, one approach is to devise DIQKD protocols which are more robust and efficient. Recently, this yielded two improved variants

* These authors contributed equally

† charles.lim@nus.edu.sg

‡ h.w@lmu.de

FIG. 1. **Schematic of the DIQKD connection.** Each of the two parties, Alice and Bob, holds one of the two QKD devices which are connected via 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 between the two parties is necessary for exchange of information during post-processing.

of the original DIQKD protocol—one based on noisy-preprocessing [30] and the other based on randomised key setting [31].

Here we present a proof-of-concept DIQKD experiment with distant users, demonstrating the protocol proposed in Ref. [31]. For this, we employ the upgraded version of an event-ready loophole-free Bell experiment [28]. There, the quantum channel for DIQKD is formed by two single ^{87}Rb atoms separated 400 metres line-of-sight where photons are exchanged over a 700 m long optical fibre connecting the two labs. The event-ready entanglement generation scheme runs in two stages for each measurement round: (1) an entangled spin-polarisation state between the atom and a spontaneously emitted photon is generated locally in each laboratory and (2) the photons are sent to a Bell-state measurement (BSM) setup for entanglement swapping. Hence, whenever the results of the BSM indicates that entanglement swapping is successful, entanglement between the spin states of the atoms is generated and announced. Significant improvements in the entanglement generation rate, coherence of atomic states, and entanglement swapping fidelity enabled the implementation of the protocol. Based on the measurement data obtained from the experiment, we find that a positive asymptotic secret key fraction (the ratio of achievable secret key length to the total number of heralded events) of 0.07 was achieved in a fully device independent configuration.

DIQKD PROTOCOL

The protocol considered here is similar to the standard protocol [3, 33], except that two measurement settings are used for key generation instead of one. Importantly, in doing so, the protocol can tolerate significantly more noise—the critical QBER is extended from 7.1% to 8.2% [31]. The protocol considers that Alice and Bob

each hold a device, which are connected via a quantum channel (Fig. 1). The protocol consists of N measurement rounds, whereby in each i th round both devices receive an input (X_i and Y_i) and respond with an output (A_i and B_i). More specifically, Alice’s device accepts four different values $X_i \in \{0, 1, 2, 3\}$, while Bob’s device has two inputs $Y_i \in \{0, 1\}$. The input for each round is provided by a trusted local source of randomness. Both devices output two possible values, $A \in \{\uparrow, \downarrow\}$ at Alice’s side and $B \in \{\uparrow, \downarrow\}$ at Bob’s side. Additionally, the input and output values are recorded and stored in a local secured storage.

After N rounds the users stop the measurements and begin with classical post-processing. For this, Alice and Bob reveal their inputs for each round over an authenticated public channel. For the rounds with differing input settings, i.e., $X \in \{2, 3\}$ together with $Y \in \{0, 1\}$, the outputs are shared over the public channel to compute the Clauser-Horne-Shimony-Holt (CHSH) [34] value using

$$S := E_{2,1} - E_{2,0} - E_{3,0} - E_{3,1}, \quad (1)$$

where the correlation functions are defined as $E_{X,Y} := (N_{X,Y}^{A=B} - N_{X,Y}^{A \neq B})/N_{X,Y}$. Here, $N_{X,Y}$ is the number of rounds with input combination X, Y , while $N_{X,Y}^{A=B}$ ($N_{X,Y}^{A \neq B}$) is the number of rounds with identical (different) outcomes for input combination X, Y . Provided that the devices share a sufficiently entangled state, the Bell inequality can be violated, i.e., $S > 2$.

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 $Q_0 = N_{0,0}^{A \neq B}/N_{0,0}$ for $X_i = Y_i = 0$ and $Q_1 = N_{1,1}^{A \neq B}/N_{1,1}$ for $X_i = Y_i = 1$. Note that the key pairs are supposed to be anti-correlated due to the use of anti-correlated 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 [35]. 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 [36]. 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 depolarising quantum channel, positive key rates can be achieved when the expected CHSH value satisfies $S > 2.362$ (or equivalently, $Q < 0.082$ with $Q_0 = Q_1 = Q$) [31].

QUANTUM NETWORK LINK

A quantum network link (QNL) generates the entanglement between the two spatially separated laboratories in order to implement the DIQKD protocol. In our setup, entanglement is generated between two optically

FIG. 2. **Overview of the quantum network link for DIQKD.** **a**, Alice's equipment (Device 1 in Lab 1) is formed by a single atom trap and a Bell-state measurement (BSM) setup. Bob (Device 2 in Lab 2), uses a second single atom trap together with a 90:10 (T:R) beamsplitter (BS) and a single photon detector (SPD). Each trap setup contains of a high-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 beamsplitter (BS) heralds the entangled atom-atom state $|\Psi^+\rangle$, which is announced to both users via a "ready" signal. After receiving the ready signal, two quantum random number generators (QRNG) select the inputs to the devices determining the polarisation of a readout pulse in a state-selective ionization scheme. Whether or not the atom was ionized yields the binary output of the devices which can be determined by fluorescence collection since ionised atoms are lost from the trap. The in- 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 in- and outputs of the device via the quantum channel. **b**, Map showing the main campus of the LMU in Munich indicating the locations of the two laboratories. Map data were provided by Ref. [32].

trapped single ^{87}Rb atoms located in laboratories 400 m apart and connected via a 700 metre long optical fibre channel, see Fig. 2. The atoms act as quantum memories where 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 setup.

The two distant atoms are entangled using an entanglement swapping protocol [37]. The sequence starts by synchronously exciting a 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 polarisation of the respective spontaneously emitted single photon (Fig. 3a). This results in an entangled atom-photon state $|\Psi\rangle_{AP} = 1/\sqrt{2}(|\downarrow\rangle_x|V\rangle + |\uparrow\rangle_x|H\rangle)$ [38], where $|\uparrow\rangle_x := (|\uparrow\rangle_z + |\downarrow\rangle_z)/\sqrt{2}$ (resp. $|\downarrow\rangle_x := (|\uparrow\rangle_z - |\downarrow\rangle_z)/\sqrt{2}$), and $|H\rangle$ and $|V\rangle$ denote parallel and orthogonal linear polarisations with respect to the optical table, respectively. The two photons are then guided to a BSM setup employing two-photon interference. Projection of the photons onto a $|\Psi^+\rangle$ state heralds the creation of the maximally entangled atom-atom state

$$|\Psi^+\rangle_{AB} = \frac{|\uparrow\rangle_{z,A}|\downarrow\rangle_{z,B} + |\downarrow\rangle_{z,A}|\uparrow\rangle_{z,B}}{\sqrt{2}}, \quad (2)$$

where the orthogonal spin states $|\uparrow\rangle_z$ and $|\downarrow\rangle_z$ are defined as the computational basis states of the protocol. More specifically, given a successful projection, a ready

FIG. 3. **Schematics of the entanglement generation and atomic state readout schemes.** **a**, An entangled atom-photon state is generated by the spontaneous decay subsequent to excitation to the state $5^2P_{3/2}|F'=0, m_{F'}=0\rangle$. **b**, The qubit state is read-out via a state dependent ionisation scheme. First, a by polarisation controlled superposition of the qubit state is excited to the $5^2P_{1/2}$ level. Subsequently, the excited atom is ionised by a bright second laser pulse. If the atom decays to the state $5^2S_{1/2}|F=2\rangle$ before it is ionised, it is excited to the state $5^2P_{3/2}|F'=3\rangle$, which is ionised as well.

signal is sent to the trap setups and the atomic qubits are measured.

The two atomic qubits are independently analysed via state-selective ionisation (Fig. 3b) [39]. There, a particular state of the atomic qubit is ionised and leaves the trap depending on the polarisation $\chi = \cos(\gamma)V + e^{-i\phi}\sin(\gamma)H$ 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

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

The presence of the atom is then tested using fluorescence collection, which yields the final measurement outcome. On Alice's side, the single-photon detectors (SPDs) of the BSM detect the fluorescence of the atom, while on Bob's side an unbalanced beam splitter directs a small fraction of the fluorescence light onto a single SPD (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.

While the requirements for a DIQKD implementation are less stringent with the newly proposed protocols, significant improvements over existing loophole-free Bell experiments are still required. To that end, we enhance the entanglement generation rate, coherence of atomic states, and entanglement swapping fidelity of the loophole-free setup reported in Ref. [28] (see Methods).

DIQKD IMPLEMENTATION

The independent random inputs to the devices (requirement iv-b) are provided by independent quantum random number generators (QRNG) [28, 41] located in each laboratory. At Alice's side, two random bits are used to select the input, while at Bob's side only one random bit is used, leading to uniformly distributed input combination choices. Based on the generated entangled state (Eq. 2) and the atomic state measurement scheme (Eq. 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 and $Y \in \{0, 1\}$ translate to $\beta \in \{-22.5^\circ, 22.5^\circ\}$ for Bob's device, respectively. The capability for fast switching between various read-out settings is achieved by overlapping multiple read-out beams with different polarisation and individually controllable intensities [28]. The outputs $A, B \in \{\uparrow, \downarrow\}$ are derived from the fluorescence counts after the state-selective ionisation. Finally, the users' inputs and outcomes are stored in two independent, trusted secure storage (requirement iv-c).

Unauthorised incoming and outgoing communication of the laboratories can be mitigated with prudent steps (requirements ii and iii). Especially on Bob's side, extra measures are taken to prevent information leakage from the laboratory: a free-space shutter is used during the read-out process to prevent fluorescence light from leaking into the optical fibre (and into the outside environment) (see Fig. 2), and the trap is always emptied before reopening the shutter. Due to the approximate 5 ms reaction time of the shutter, a spectral filter 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 setup already serves as a natural filter [42].

RESULTS

The inputs and outputs of the devices were recorded for $N = 3342$ rounds over a measurement period of 75 hours. The resulting output (anti-)correlation probabilities for the eight different input combinations, i.e. $N_{X,Y}^{A=B}/N_{X,Y}$ and $N_{X,Y}^{A \neq B}/N_{X,Y}$, are shown in Fig. 4a.

It is instructive to first review the updated 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. 4a) with sinusoidal functions, the estimated visibility for input combinations $X = 2, 0, 3, 1$ and $Y = 0$ (resp. $X = 2, 0, 3, 1$ and $Y = 1$) is 0.869(25) (resp. 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 $\mathcal{F} \geq 0.892(19)$ [28].

The CHSH value is found to be $S = 2.578(75)$ using Eq. (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 $X = Y$, i.e., $Q_0 = 0.0781(127)$ and $Q_1 = 0.0777(132)$, which gives an average error rate of $Q = 0.0779(91)$. For the considered DIQKD protocol, the observed S value and QBER suggest that the DIQKD setup is capable of achieving a secret key rate of 0.07 in the asymptotic limit (Fig. 4b). To get a sense of how reliable this estimate is, 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% give positive rates. These results indicate a proof-of-concept realisation of DIQKD on a quantum network link connecting two users 400 m apart. We also note that the original DIQKD protocol [3, 33] results in positive key rates for the observed S and Q_0 (or Q_1), however, no positive rate is found using the above worst-case estimates.

Using state-of-the-art finite-key analysis for the protocol, we find that $\epsilon_{\text{DI}} = 10^{-5}$ security can be obtained with a minimal block length of 1.75×10^5 [36], as illustrated in Fig. 5. Here, ϵ_{DI} is the security error of the protocol, which quantifies how close the actual output of the protocol is to the ideal output (see Ref. [36]). In the simulation, we consider collective attacks, an error correction efficiency of 1.15, and uniformly distributed measurement settings for Alice and Bob.

FIG. 4. **Observed atom-atom state correlations and the expected secret key rate.** **a**, The (anti-)correlation probabilities of the device outputs for the eight input combinations, resulting in $S = 2.578(75)$ and $Q = 0.0779(91)$. The data is fitted with sinusoidal functions estimating visibilities of $0.869(25)$ and $0.888(45)$. The settings with the green (yellow) background contribute to the evaluation of the S (Q). **b**, Expected secret key rate for varying CHSH S-value and QBER for the robust DIQKD protocol [31]. The presented work (1) shows an expected secret key rate of 0.07 and lies well inside the positive region. For comparison, the results of [28] (2) and [25, 40] (3), which to the best of our knowledge are the only experiments that fulfill the requirements for DIQKD with significant distance between the two users. Note that (2) does not reach the positive key regime due to the high QBER. The error bars indicate statistical errors of one standard deviation.

FIG. 5. **Finite-key simulation for the robust DIQKD protocol.** Shown is the minimum number of rounds 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 $\epsilon_{DI} = 10^{-5}$ is considered to be realistic for cryptography applications.

DISCUSSION AND OUTLOOK

In this work, we presented a proof-of-concept DIQKD experiment by demonstrating a QNL that could achieve positive secret key rates between users separated by 400 metres line-of-sight (700 metres fibre length) in a fully device-independent setting. While the current setup im-

proves upon existing loophole-free Bell setups, there are still several areas that require enhancements before a DIQKD experiment with finite-key security and longer reach can be achieved.

For one, a significantly higher event rate is required to obtain finite-key security within a practical time-frame; based on the current setup and over the current distance, one would need months of measurement time to achieve finite-key security. The event rate critically depends on the entanglement generation efficiency and the repetition rate. To increase the former, several improvements are possible, e.g., improving the BSM setup fidelity to include the $|\Psi^-\rangle$ state projection would increase the entanglement generation rate by a factor of 2 (see Supplemental Material IV). However, the latter has an intrinsic limitation for event-ready schemes, such as the DIQKD scheme presented here: a repetition of the entanglement generation process is only possible after waiting for a feedback signal from the BSM. Therefore, the repetition rate is limited by the communication times between the two devices and the BSM. Consequently, there is a trade-off between the event rate and distance and one would have to prioritise distance over finite-key security (or vice versa). To address this issue for the current setup, it is possible to scale up the number of atom traps using multi-dimensional arrays [43–45], which combined with time multiplexing techniques [46] could increase the event rate by several orders of magnitude.

Another direction to improve is 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, one can convert the entangled single photons to the low-loss telecom band via polarisation-preserving quantum frequency conversion [39, 47]. Preliminary study of recent results indicates that distances up to 100 km are within reach.

In summary, our results represent a major step towards the goal of ultimate secure communication based solely on quantum physics. Importantly, they indicate that state-of-the-art quantum network links are capable of harnessing the ultimate quantum advantage for secure communications. Even if it is still a long way to go; when the future quantum repeater based quantum networks provide the key resource, i.e., shared entanglement, DIQKD—as realized in this proof-of-concept experiment—will become the standard for secure key exchange.

Note added in proof. While completing the manuscript, we became aware of two similar proof-of-concept DIQKD experiment [48, 49].

ACKNOWLEDGEMENTS

We thank Ignatius William Primaatmaja, Ernest Y.-Z. Tan, and Koon Tong Goh for useful inputs and discussions. W.Z., T.L., K.R., R.G., F.F., S.E., 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 (Contracts No. 16KIS0127, 16KIS0123, 16KIS0864, and 16KIS0880), 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.

METHODS

Entanglement generation rate

Custom-design 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 pulse pair. Together with a duty cycle of approximately 1/2 and a repetition rate of the entanglement generation tries of 52 kHz resulting in an event rate

of $1/82 \text{ s}^{-1}$. 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. For DIQKD protocols, this results in a trade-off between the maximum separation of the users and the achieved secret key rate, see Outlook.

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 allows a high fidelity state measurement only when the atom has completed a full transverse oscillation in the trap [50]. Here, the better optical components of the new collection setup, which is also used to focus the trapping laser, enable a more symmetric trapping potential. In combination with lowering the atom temperatures and applying a magnetic bias field this extends the coherence time to approximately $330 \mu\text{s}$. 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) with an atomic readout delay of $26 \mu\text{s}$ and $17 \mu\text{s}$ in Alice's and Bob's setups, respectively. We refer the interested reader to Supplemental Material B for more details.

BSM fidelity

The quality of the entangled atom-atom state is further improved by optimising the two photon interference of the BSM through a rigorous analysis of the atom-photon entanglement generation process. Here, the multi-level 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 multi-photon events reduce the fidelity of the BSM result. To overcome this, only photons which are emitted after the end of the prior excitation pulse are accepted in the BSM. This reduces the entanglement generation rate by a factor of 4 (resulting in the entanglement generation rate mentioned before), but significantly increases the fidelity of the generated state; see Supplemental Material C for more details.

Data availability The datasets generated during 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.

Competing interests The authors declare no competing interests.

-
- [1] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus (IEEE, 1998) pp. 503–509.
- [2] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Physical Review Letters* **98**, 230501 (2007).
- [3] S. Pironio, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.* **11**, 045021 (2009).
- [4] J. Barrett, L. Hardy, and A. Kent, No signaling and quantum key distribution, *Phys. Rev. Lett.* **95**, 010503 (2005).
- [5] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, *Nature* **496**, 456 (2013).
- [6] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
- [7] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, *Journal of the ACM* **63**, 1 (2016).
- [8] R. Arnon-Friedman et al., Practical device-independent quantum cryptography via entropy accumulation, *Nat. Commun.* **9**, 459 (2018).
- [9] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 711 (2014).
- [10] A. K. Ekert, Quantum cryptography based on bell’s theorem, *Phys. Rev. Lett.* **67**, 661663 (1991).
- [11] C. Elliott and H. Yeh, *DARPA Quantum Network Testbed*, Final technical report (BBN Technologies, 2007).
- [12] M. Peev et al., The SECOQC quantum key distribution network in vienna, *New J. Phys.* **11**, 075001 (2009).
- [13] M. Sasaki, Field test of quantum key distribution in the Tokyo QKD Network, *Opt. Express* **19**, 1038710409 (2011).
- [14] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Large scale quantum key distribution: challenges and solutions, *Opt. Express* **26**, 24260 (2018).
- [15] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussieres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [16] T. Schmitt-Manderbach et al., Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, *Phys. Rev. Lett.* **98**, 010504 (2007).
- [17] R. Ursin et al., Entanglement-based quantum communication over 144 km, *Nat. Phys.* **3**, 481 (2007).
- [18] S. Nauerth et al., Air-to-ground quantum communication, *Nat. Photon.* **7**, 382 (2013).
- [19] S.-K. Liao et al., Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [20] S.-K. Liao et al., Satellite-Relayed Intercontinental Quantum Network, *Phys. Rev. Lett.* **120**, 030501 (2018).
- [21] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [22] J. S. Bell, On the Einstein Podolsky Rosen paradox, *PPF* **1**, 195 (1965).
- [23] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [24] R. Arnon-Friedman, R. Renner, and T. Vidick, Simple and tight device-independent security proofs, *SIAM Journal on Computing* **48**, 181 (2019).
- [25] B. Hensen et al., Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, *Nature* **526**, 682 (2015).
- [26] M. Giustina et al., Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons, *Phys. Rev. Lett.* **115**, 250401 (2015).
- [27] L. K. Shalm et al., Strong Loophole-Free Test of Local Realism, *Phys. Rev. Lett.* **115**, 250402 (2015).
- [28] W. Rosenfeld et al., Event-Ready Bell Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes, *Phys. Rev. Lett.* **119**, 010402 (2017).
- [29] G. Murta et al., Towards a realization of device-independent quantum key distribution, *Quantum Sci. and Technol.* **4**, 035011 (2019).
- [30] M. Ho, P. Sekatski, E.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution, *Physical Review Letters* **124**, 230502 (2020).
- [31] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y. Z. Tan, R. Wolf, V. Scarani, and C. C. W. Lim, Device-independent quantum key distribution with random key basis, *Nature Communications* **12**, 2880 (2021).
- [32] Bayerisches landesamt fuer digitalisierung, broadband und vermessung.
- [33] A. Acín et al., Device-Independent Security of Quantum Cryptography against Collective Attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [34] J. F. Clauser et al., Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880884 (1969).
- [35] R. Renner, Security of quantum key distribution, *International Journal of Quantum Information* **6**, 1 (2008).
- [36] E. Y. Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, and C. C. W. Lim, Improved diqkd protocols with finite-size analysis (2020), arXiv:2012.08714 [quant-ph].
- [37] J. Hofmann et al., Heralded Entanglement Between Widely Separated Atoms, *Science* **337**, 72 (2012).
- [38] J. Volz et al., Observation of Entanglement of a Single Photon with a Trapped Atom, *Phys. Rev. Lett.* **96**, 030404 (2006).
- [39] T. van Leent et al., Long-Distance Distribution of Atom-Photon Entanglement at Telecom Wavelength, *Phys. Rev. Lett.* **124**, 010510 (2020).
- [40] B. Hensen et al., Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis, *Scientific Reports* **6**, 30289 (2016).
- [41] M. Furst, High speed optical quantum random number generation, *Opt. Express* **18**, 1302913037 (2010).
- [42] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [43] M. Endres, H. Bernien, A. Keesling, H. Levine, E. R. Anschuetz, A. Krajenbrink, C. Senko, V. Vuletic, M. Greiner, and M. D. Lukin, Atom-by-atom assembly of defect-free one-dimensional cold atom arrays, *Science*

- 354**, 1024 (2016).
- [44] D. Barredo, S. De Léséleuc, V. Lienhard, T. Lahaye, and A. Browaeys, An atom-by-atom assembler of defect-free arbitrary two-dimensional atomic arrays, *Science* **354**, 1021 (2016).
 - [45] D. Ohl de Mello, D. Schäffner, J. Werkmann, T. Preuschoff, L. Kohfahl, M. Schlosser, and G. Birkel, Defect-free assembly of 2d clusters of more than 100 single-atom quantum systems, *Phys. Rev. Lett.* **122**, 203601 (2019).
 - [46] J. Schupp, V. Krcmarsky, V. Krutyanskiy, M. Meraner, T. Northup, and B. Lanyon, Interface between trapped-ion qubits and traveling photons with close-to-optimal efficiency, *PRX Quantum* **2**, 020331 (2021).
 - [47] T. van Leent et al., Entangling Single Atoms over 33 km Telecom Fiber, to be published.
 - [48] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Device-independent quantum key distribution (2021), arXiv:2109.14600 [quant-ph].
 - [49] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, High-speed device-independent quantum key distribution against collective attacks (2021), arXiv:2110.01480 [quant-ph].
 - [50] D. Burchardt, A rigorous test of bell's inequality and quantum teleportation employing single atoms, PhD thesis, Ludwig-Maximilians-Universität München (2017).

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [ExptDIQKDSM.pdf](#)