Experimental quantum key distribution certified by Bell's theorem

D. P. Nadlinger,[1] P. Drmota,[1] B. C. Nichol,[1] G. Araneda,[1] D. Main,[1] R. Srinivas,[1] D. M. Lucas,[1] C. J. Ballance,[1] K. Ivanov,[2] E. Y-Z. Tan,[3] P. Sekatski,[4] R. L. Urbanke,[2] R. Renner,[3] N. Sangouard,[5] and J-D. Bancal[5]

[1] *Department of Physics, University of Oxford, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, U.K.*
[2] *School of Computer and Communication Sciences, EPFL, 1015 Lausanne, Switzerland*
[3] *Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*
[4] *Department of Applied Physics, University of Geneva, Rue de l'École-de-Médecine, 1211 Geneva, Switzerland*
[5] *Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France*

(Dated: May 10, 2022; accepted version)

Cryptographic key exchange protocols traditionally rely on computational conjectures such as the hardness of prime factorisation[1] to provide security against eavesdropping attacks. Remarkably, quantum key distribution protocols like the one proposed by Bennett and Brassard[2] provide information-theoretic security against such attacks, a much stronger form of security unreachable by classical means. However, quantum protocols realised so far are subject to a new class of attacks exploiting a mismatch between the quantum states or measurements implemented and their theoretical modelling, as demonstrated in numerous experiments[3–6]. Here, we present the experimental realisation of a complete quantum key distribution protocol immune to these vulnerabilities, following Ekert's pioneering proposal[7] to use entanglement to bound an adversary's information from Bell's theorem[8]. By combining theoretical developments with an improved optical fibre link generating entanglement between two trapped-ion qubits, we obtain 95 628 key bits with device-independent security[9–12] from 1.5 million Bell pairs created during eight hours of run time. We take steps to ensure that information on the measurement results is inaccessible to an eavesdropper. These measurements are performed without space-like separation. Our result shows that provably secure cryptography under general assumptions is possible with real-world devices, and paves the way for further quantum information applications based on the device-independence principle.

Private communication over shared network infrastructure is of fundamental importance to the modern world. Classically, shared secrets cannot be created with information-theoretic security; real-world key exchange protocols rely on unproven conjectures regarding the computational intractability of certain operations. Quantum theory, however, promises that measurements on two correlated quantum systems can yield identical outcomes that are fundamentally unpredictable to any third party. This possibility of generating secret correlated outcomes at a distance forms the basic idea of quantum key distribution (QKD)[13–15]. Importantly, the security guarantees provided by QKD are unique in that they do not rely on the assumption that the adversary has limited computational power. Instead, the only required assumptions are that: (i) quantum theory is correct, (ii) the parties can isolate their systems to prevent information leaking to an adversary, (iii) they can privately choose random classical inputs to their quantum devices, and (iv) they can process classical information on trusted computers.

Existing QKD systems rely on an additional assumption that is hard to satisfy in practice: they require the quantum states and measurements used to distribute the key to be accurately characterised (e.g. including their dimension)[14–16]. In other words, the quantum devices are assumed to be trusted and to maintain perfect calibration. Deviations from the expected behaviour can be difficult to detect, which has been exploited in a number of demonstrations where real-world QKD systems were compromised[3–6]. So-called measurement-device-independent QKD protocols allow untrusted measurements to be used as part of the system but still require well-characterised sources[17–21].

Device-independent QKD (DIQKD) protocols[9–12] make no additional assumptions about the physical apparatus. According to Bell's theorem, one can guarantee that two systems produce outcomes sharing exclusive correlations – preventing a third party from knowing these results – without assuming how these outcomes are produced[22]. This remarkable fact can be used to construct key distribution protocols with security guarantees independent of any assumption about the states measured and measurements performed. Rather, the underlying state and measurements are certified in the process[9]. Imperfections that might lead to key leakage in conventional QKD due to an inappropriate description of the internal quantum state or measurement instead just result in the protocol aborting. However, this enhanced security comes at the cost of far more stringent experimental requirements. The certifiable amount of private information directly depends on the size of a Bell inequality violation, necessitating a platform capable of distributing and measuring high-quality entangled states while closing the detection loophole. To successfully extract a shared key using state-of-the-art devices, a tight theoretical analysis and an efficient classical post-processing pipeline are needed, in particular regarding finite-size effects resulting from practical limits on the

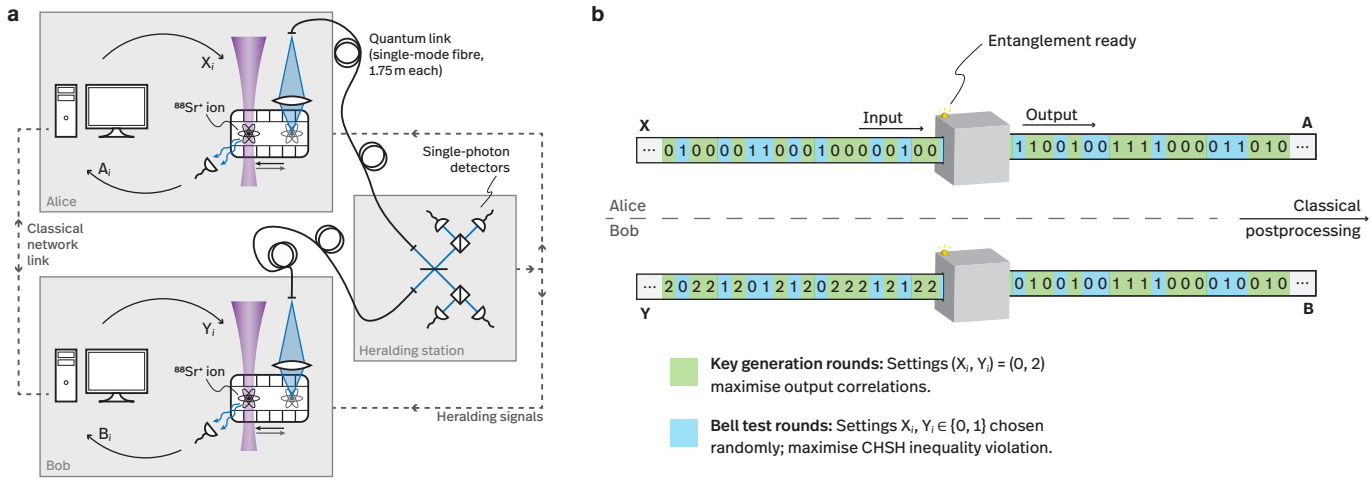

Fig. 1: DIQKD with trapped ions. a, Alice and Bob each operate independent ion-trap nodes, here separated by about 2 m, where one $^{88}Sr^{+}$ qubit is confined in a vacuum chamber. To establish entanglement the ions are simultaneously excited to an electronic state which spontaneously decays, during which a single photon each is emitted whose polarisation is entangled with the ion's internal state. These photons are collected into optical fibres using free-space optics and sent to a central station, where a probabilistic Bell-basis measurement is performed. This projects the ions into a maximally entangled state, heralded by the coincident detection of a pair of photons. On success, the ions are each transported to a different location in the trap to disconnect the photonic link such that local projective measurements can be applied without either the measurement basis settings X_i, Y_i or the outcomes $A_i, B_i \in \{0, 1\}$ leaking into the environment. The state is then reset and the link reconnected, and the process is repeated for a large number of rounds. **b,** In the device-independent security proof, no further assumptions are made about the internal workings of the quantum devices; they are modelled as "black boxes" with classical inputs and outputs. By randomly alternating between measurement settings realising a Bell test and settings which lead to highly correlated outputs, the output bit strings can be certified to originate from appropriate measurements on a quantum state that is close to being maximally entangled, ensuring secrecy.

number of measurements. Despite significant theoretical progress[10–12,23–31] a practical demonstration of these protocols has remained out of reach.

Here we report the first experimental distribution of a key with device-independent security guarantees. Using a hybrid system where heralded entanglement between stationary trapped ion qubits is established via flying photonic qubits (see Fig. 1), we are able to generate high-quality entangled states between two ions separated by about 2 m, resulting in a record-high detection-loophole-free Bell inequality violation with isolated systems. We propose a concrete, practical DIQKD protocol, design a universal capacity-approaching error-correction code optimised for this context, use extractors and authentication schemes that are frugal in their randomness consumption, and provide a detailed finite-statistics security proof. Combining these theoretical and experimental advances, we successfully obtain a key whose length is more than two orders of magnitude greater than the amount of private shared randomness consumed by the protocol.

Our DIQKD protocol is illustrated in Fig. 2. All parameters are chosen before the start of the protocol. The data acquisition phase of our protocol consists of n sequential rounds. At the start of each, Alice and Bob wait for a valid heralding signal from the central heralding station indicating the creation of remote entanglement. For Bell test rounds, Alice and Bob randomly select inputs $X_i, Y_i \in \{0, 1\}$ for their measurements, which are implemented so that the outcomes $A_i, B_i \in \{0, 1\}$ maximise the probability of winning the Clauser-Horne-Shimony-Holt (CHSH) game[32] $A_i \oplus B_i = X_i \cdot Y_i$. A high winning probability ω, customarily expressed in terms of the CHSH score $S = 4\,(2\omega - 1)$, tightly bounds the information any adversary can have about the outcomes. For so-called key generation rounds, the inputs are fixed to $X_i = 0$ and $Y_i = 2$, maximising output correlations as quantified by a low quantum bit error rate $Q = P(A_i \neq B_i | X_i = 0, Y_i = 2)$. Bob randomly chooses between the round types after the heralding signal is received and the links are disconnected, choosing Bell test rounds with probability γ, and communicates this choice to Alice, which avoids sifting (discarding of rounds with mismatched measurement bases). The parties keep private records of their measurement settings $\mathbf{X} = X_1 X_2 \ldots$ and $\mathbf{Y} = Y_1 Y_2 \ldots$ as well as the outcomes $\mathbf{A} = A_1 A_2 \ldots$ and $\mathbf{B} = B_1 B_2 \ldots$. After the n measurement rounds are complete, Alice and Bob need to verify the CHSH score and extract a shared key from the noisy output correlations. Alice openly sends her inputs $\mathbf{X}$ to Bob, along with a shorter error-correction syndrome string $\mathbf{M}$ which allows Bob to reconstruct a copy $\tilde{\mathbf{A}}$ of Alice's outcomes $\mathbf{A}$. Now holding $\mathbf{X}\mathbf{Y}\tilde{\mathbf{A}}\mathbf{B}$, Bob is able to verify whether

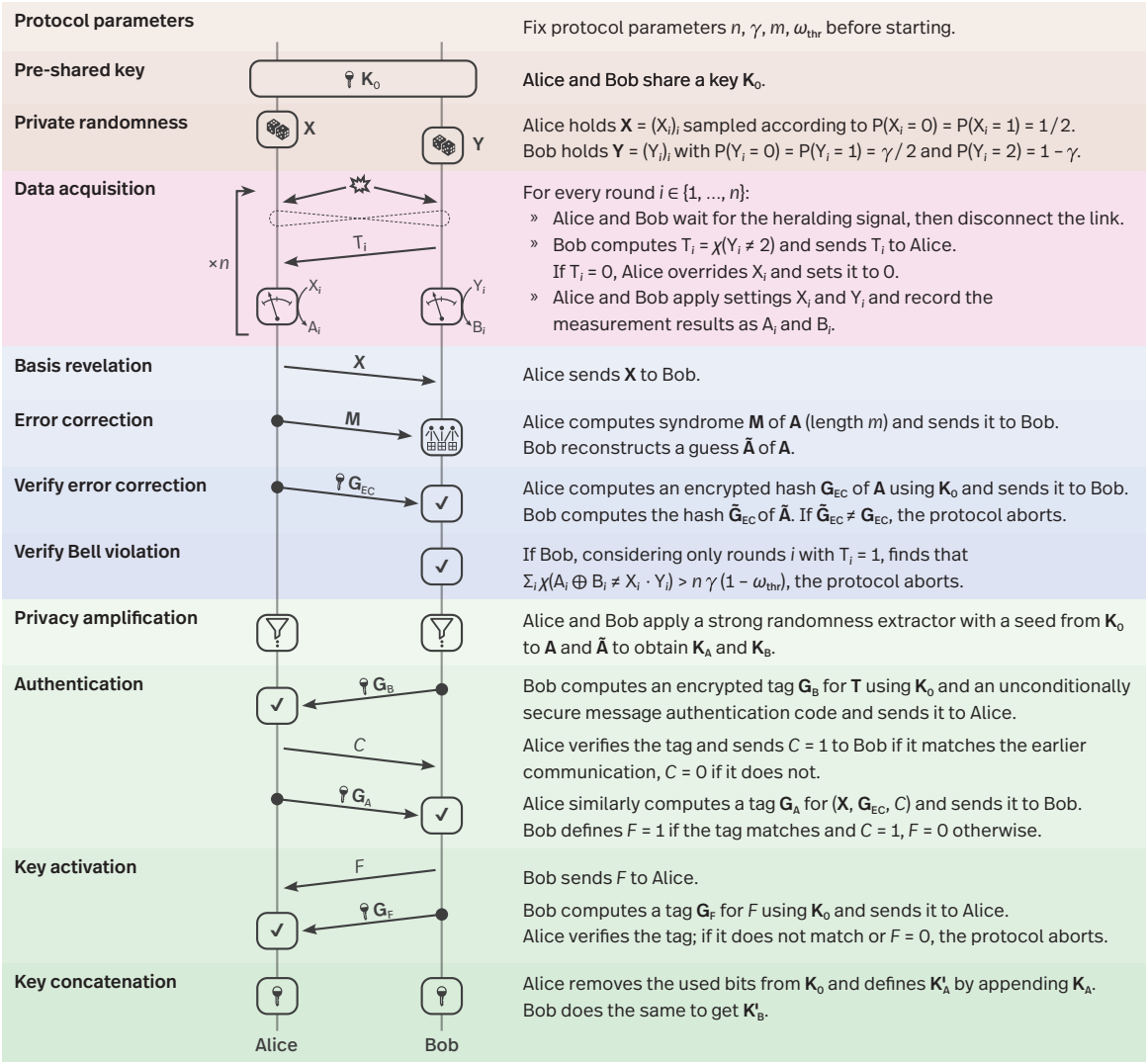

Fig. 2: DIQKD protocol structure. Before the protocol starts, the number of rounds n, the probability γ of each round being chosen to be Bell test round, an acceptance threshold ω_{thr} for the CHSH winning probability, and the length m of the error correction syndrome are fixed. An initial key $\mathbf{K_0}$, mostly reusable, is required to seed the privacy amplification and authentication algorithms, and as a one-time pad to encrypt a few short messages (indicated using a key symbol). Arrows indicate the classical messages exchanged between the parties, bold letters strings consisting of multiple bits, χ the indicator function with $\chi(P) = 1$ if P is true and 0 otherwise.

the CHSH score achieved during the Bell test rounds exceeds a pre-agreed threshold. If this it not the case, or if the reconstruction of $\tilde{\mathbf{A}}$ fails, the security might be compromised so the protocol aborts. Otherwise, the parties locally process the outcomes $\mathbf{A}$ and $\tilde{\mathbf{A}}$ to extract identical final keys, with a guaranteed, arbitrarily low, bound on the information leaked to any adversary.

A crucial step in the security analysis is to infer an upper bound on the knowledge an adversary can have about Alice's outcomes. In the device-independent setting, where quantum states and measurements are a priori uncharacterised and where we allow memory effects to correlate successive measurement rounds, obtaining a precise bound is nontrivial. A recent breakthrough in this respect is the entropy accumulation theorem (EAT)[12,33]. It shows that in an n-round protocol characterised by a CHSH score S, the amount of randomness generated by both parties, with respect to an adversary limited by quantum theory, is lower-bounded by $n\,h(S)$ up to a correction of order $\sqrt{n}$, where $h(S)$ is the worst-case von Neumann entropy of the outcomes for an individual round of the protocol compatible with the score S. Using this result, we derive a bound on Alice's private randomness from the CHSH winning probability threshold ω_{thr} chosen before start of the protocol[12]. We use a recent version of the EAT[34] for its improved statistical performance, proving security against the most general types of attacks (as detailed in the Supplementary Material).

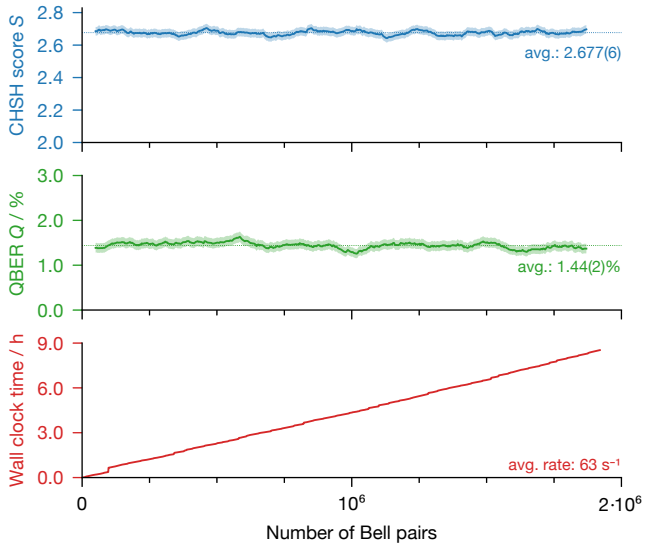

Fig. 3: Quantum link performance. A separate characterisation run of 1 920 000 total Bell pairs shows stable link performance. Inputs and outputs from both nodes were collected to compute a moving average for CHSH score and quantum bit error rate (window length: 100 000 rounds; test round fraction: $\gamma = 1/2$). Shaded bands indicate 95 % confidence intervals from binomial statistics in each window. The bottom panel shows the acquisition timestamp for each Bell pair during the 8.5 h experiment duration. The vertical steps, where time passed without heralds, correspond to ion loss and recalibration events.

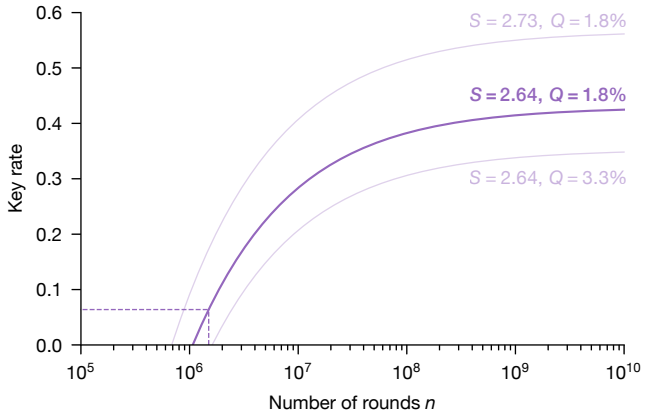

Fig. 4: Finite-statistics key rate. Certified key rate as a function of the number of rounds for $S = 2.64$, $Q = 1.8\%$, $\gamma = 13/256$ and $\varepsilon_{\text{snd}} = 10^{-10}$. We operate the DIQKD protocol at the point $n = 1.5 \times 10^6$ on this curve, corresponding to a threshold winning probability of $\omega_{\text{thr}} \approx 0.825538$ and a key rate of $95\,884/n \approx 6.39\%$. Two key rate curves for alternate parameter choices illustrate its sensitivity to the link performance.

The length of the final key is given by the difference between the amount of entropy certified by the EAT and the amount of information revealed through the classical messages exchanged by the parties as part of the protocol. To obtain a positive key rate it is therefore crucial to reconcile Alice and Bob's outcomes with an error correction syndrome that is as short as possible. Asymptotically, the cost of reconciliation per round is given by $\mathrm{H}(\mathbf{A}|\mathbf{XYB})$, the entropy of Alice's outcomes conditioned on the knowledge of inputs and Bob's outcomes. Reconciliation in presence of finite statistics however comes at a higher price and the best algorithms are often not realisable in practice. In fact, all finite-statistics DIQKD analyses so far have assumed computationally intractable error correction schemes with decodings involving hash pre-image computations[11,12,35,36]. We address this challenge using a custom error correction solution based on spatially-coupled low-density parity-check (SC-LDPC) encoding. Our scheme admits an efficient decoding algorithm and requires less overhead than some previously considered impractical codes (see Supplementary Material).

In our experiment, Alice and Bob each control a trapped-ion quantum network node[37,38] holding a single $^{88}\mathrm{Sr}^+$ ion qubit each. Dissipative and coherent operations are implemented using resonant laser fields, which each node derives from a shared set of laser sources. Entanglement between the ion and the polarisation of a spontaneously emitted 422 nm photon is locally created at each node by excitation to a short-lived state with two decay paths to the Zeeman-split qubit states in the ground level. The photons are coupled into single-mode optical fibres connecting the nodes to a central heralding station, where a linear optics setup and four avalanche photodetectors implement a Bell-basis measurement (see Fig. 1a and Supplementary Material). The overall detection efficiency for each spontaneous decay photon is $\approx 2\,\%$, necessitating many attempts to observe a two-photon coincidence heralding the successful creation of entanglement between Alice's and Bob's ion qubits. We perform state tomography to characterise the ion-ion entanglement, measuring a fidelity to the closest maximally entangled state of 96.0(1) %, which exceeds previously reported measurements for remote entanglement between matter qubits[38–43].

To implement the "black box" primitives for DIQKD, each node first disconnects the qubit from the optical link following a herald event by shuttling it away from the focus of the fibre-coupling objective lens, which ensures the basis choices and measurement results do not leak to a third party (see Methods). Bob decides between Bell test and key generation rounds using private randomness obtained from a commercial quantum random number generator, sending the result to Alice in real time. In case of a Bell test round, both nodes then similarly use a private random string to choose between the coherent operations defining the measurement bases, i.e. the inputs X_i and Y_i. As each DIQKD round only starts after a heralding success, this approach is intrinsically detection-loophole-

Protocol step	Consumed	Used (reusable)	Generated
Validation of error correction	64	1280	0
Authentication	128		0
Key activation	64		0
Privacy amplification	0	1 201 886	95 884
Total	256	1 203 166	95 884

Table I: Secret key balance sheet. The experiment requires an initial 1 203 422-bits long key $\mathbf{K}_0$ shared between Alice and Bob. 256 of these bits are consumed by the protocol while generating 95 884 new secret shared bits. This results in the creation of a longer 1 299 050-bits long shared secret key $\mathbf{K}_1 = \mathbf{K}'_A$ between Alice and Bob, effectively extending the initial key by 95 628 bits.

free; losses in the optical links and limited detector quantum efficiencies, which pose a challenge for DIQKD on photonic platforms[35], affect the heralding rate, but not S or Q. The measurements of one party are not space-like separated from the choice of measurements of the other party. We characterise the link performance by measuring the probabilities $P(A_iB_i|X_iY_i)$ in a separate experiment. A representative dataset, shown in Fig. 3, results in a CHSH score of $S = 2.677(6)$ and a quantum bit error rate of $Q = 1.44(2)\,\%$.

We now implement the complete protocol as described in Fig. 2, using Trevisan's quantum-proof construction as a strong randomness extractor and short tags based on a strongly universal hash family for classical message authentication. The two nodes are operated completely independently: they have independent control systems, and the input and output data is only exchanged over a classical network link as prescribed by the protocol (see Methods). In order to guarantee a high success probability of the protocol, we conservatively choose $n = 1.5\times10^6$, $\gamma \approx 5.1\,\%$, $\omega_{\text{thr}} \approx 0.825\,538$, and an error correction code with syndrome length $m = 296\,517$ based on the previous link characterisation (see Supplementary Material for more details). We acquire data over 7.9 h of wall-clock time (with one pause of 4.4 h due to a laser failure), and successfully extract a secret key of 95 884 bits with soundness error $\varepsilon_{\text{snd}} = 10^{-10}$, with a post-processing time of 5 min (see table I). This greatly exceeds the 256 bits of private randomness consumed during the protocol, thus marking the first demonstration of a fully device-independent QKD.

The resulting key is secure under very general assumptions, including attacks where the adversary can act arbitrarily on the quantum side information from all rounds. Moreover, the measurement devices can have memory and operate according to the results of previous rounds, and the security of the protocol is composable with other cryptographic protocols using different devices[44,45]. Out of the remaining assumptions (i)-(iv), isolation is arguably the most critical one from a practical perspective. Space-like separation between measurement events could exclude some types of leakage but does not guarantee isolation[35,46–48] (see Methods). We envision that a stronger confidence in the isolation of the nodes will be possible when all quantum systems can be distributed and stored in advance[49], thereby avoiding the necessity for quantum communication during the protocol. The present apparatus could potentially be adapted to span building-scale local-area networks, with optical fibre losses at the 422 nm wavelength reducing the rate by approximately a factor of two every hundred metres. Key distribution over kilometres is in principle possible with downconversion to the telecom band[50], or through free-space optics. Improved key-generation rates might be achievable through improvements to the photon collection efficiency, for instance through the use of optical cavities[51]. Combining multiple instances of telecom and cavity-enhanced links into a quantum repeater architecture[52] might enable fully quantum-secure long distance communication.

METHODS

Loopholes. In the context of Bell experiments seeking to disprove local causality, several "loopholes" have been discussed[22], referring to requirements in the theoretical analysis not met in experimental realisations (consequently permitting a locally causal explanation for the observations even in the presence of a Bell inequality violation). One of them, known as the "locality loophole", is the requirement that no information about the input of one party be known by the device of the other party before it produces an outcome. In a fundamental test of local causality, information transfer of any kind must be excluded, even that potentially described by an as-yet-unknown theory. Under the assumption that measurement choices are made locally in a truly random manner so that no information about them is available in advance, it is generally admitted that this loophole can be closed through space-like separation by requiring that the measurements of both parties are space-like separated from the events defining the other party's setting choice. The condition that the inputs of one party be unknown to the other party upon measurement is also necessary for DIQKD (see Supplementary Material for more details). Space-like separation between the parties' measurement events is advantageous for this and can possibly already eliminate specific attacks by itself. However, the cryptographic context is more demanding. Not only must the input choices be unknown at other locations but also, even more obviously, the output results. Moreover, no cryptographic security can be achieved if information is allowed to travel to another party (e.g. the adversary), even if the speed of that transfer is limited to that of light. There-

fore, space-like separation is not sufficient for DIQKD and instead, the parties must be well isolated[47,48]. Isolation of each node, i.e. control over the flow of information from and to the outside, is thus an unavoidable assumption in any key exchange protocol and must be achieved through separate means. The locality condition being a consequence of the isolation assumption, no further conditions such as space-like separation are needed: if local information can be kept locally, then it is not available to a distant device. The isolation assumption has however no consequence on the "detection loophole", implying that a similar treatment of this loophole is needed in the context of DIQKD as for conventional Bell tests.

Link disconnection and isolation. By design, the trapped-ion quantum bits are well-coupled to the optical fibre linking the nodes during the entanglement generation phase. To meet the isolation assumption, the ions in each node are shuttled 3 µm from the focus of the imaging system after a successful herald by modifying the trapping potential. This way, the coupling from Alice's and Bob's qubits to the outside of their laboratories is reduced by a factor of $> 10^4$ before the basis choices are applied and the states are read out. Similarly, the qubit state left after readout is scrambled by applying deshelving and cooling lasers for 100 µs (> 10 time constants) before reconnecting the link. The information that could possibly leak through the remaining weak coupling is insufficient to compromise our conclusion of a positive key rate. If desired, one could arbitrarily reduce the amount of leaked information by shuttling the ion a further distance from the focus (> 1 mm is accessible in the trap chips used here), or by adding a macroscopic mechanism to disconnect the optical fibre, e.g. a fast micro-electromechanical fibre switch. The laser control fields for both nodes were derived from the same set of sources. An independent set of laser sources could be used instead, as the only synchronisation requirements are for the qubit frequencies to be matched and for the single-photon wave packets at the heralding station to be well-aligned compared to their 7 ns duration.

Data handling. We make extensive efforts to perform our experiments in a fashion representative of a real deployment and compatible with the security and isolation assumptions throughout. Each node is driven by an independent instance of the Advanced Real-Time Infrastructure for Quantum physics (ARTIQ) open-source real-time control system[53]; the combination of personal computer (PC) and Field Programmable Gate Arrays (FPGA) makes up the trusted local classical computation hardware as per the assumptions. The random bit strings for the CHSH basis and round type choices are derived from a commercial quantum random number generator and stored in computer memory before the start of the experiment. No post-selection takes place; a heralding event always results in a bit added to the final **A** and **B** strings. The outcome strings, along with other private data, neither leave the respective node PCs, nor are they manually inspected. A classical network link connects the two nodes, used to exchange the public messages required by the protocol (e.g. the error correction syndrome data), and to coordinate the overall experiment schedule (e.g. for periodic calibrations, or to remedy ion loss events).

DATA AVAILABILITY

The datasets generated during the current study are available from DPN and CJB on reasonable request.

CODE AVAILABILITY

The custom code generated during the current study is available from the corresponding authors on reasonable request.

[1] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM **21**, 120 (1978).

[2] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing., Theor. Comput. Sci. **560**, 7 (1984).

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

[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[5] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 10.1038/ncomms1348 (2011).

[6] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, New J. Phys. **13**, 073024 (2011).

[7] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[8] J. S. Bell, On the Einstein Podolsky Rosen paradox, Phys. Phys. Fiz **1**, 195 (1964).

[9] D. Mayers and A. Yao, Self Testing Quantum Apparatus, Quantum Info. Comput. **4**, 273–286 (2004).

[10] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[11] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[12] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryp-

tography via entropy accumulation, Nat. Commun. **9**, 459 (2018).
[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).
[15] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595–604 (2014).
[16] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (2006).
[17] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).
[18] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[19] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).
[20] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (2013).
[21] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).
[22] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[23] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).
[24] L. Masanes, Universally Composable Privacy Amplification from Causality Constraints, Phys. Rev. Lett. **102**, 140501 (2009).
[25] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature **496**, 456 (2013).
[26] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **124**, 230502 (2020).
[27] 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, Nat. Commun. **12**, 2880 (2021).
[28] E. Woodhead, A. Acín, and S. Pironio, Device-independent quantum key distribution with asymmetric CHSH inequalities, Quantum **5**, 443 (2021).
[29] P. Sekatski, J.-D. Bancal, X. Valcarce, E.-Z. Tan, R. Renner, and N. Sangouard, Device-independent quantum key distribution from generalized CHSH inequalities, Quantum **5**, 444 (2021).
[30] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, arXiv:2106.13692 (2021).
[31] M. Masini, S. Pironio, and E. Woodhead, Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints, arXiv:2107.08894 (2021).
[32] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23**, 880 (1969).
[33] F. Dupuis, O. Fawzi, and R. Renner, Entropy Accumulation, Commun. Math. Phys. **379**, 867 (2020).
[34] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent randomness expansion against quantum side information, Nat. Phys. **17**, 448 (2021).
[35] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, Towards a realization of device-independent quantum key distribution, Quantum Sci. Technol. **4**, 035011 (2019).
[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, arXiv:2012.08714 (2020).
[37] D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M. Duan, and C. Monroe, Entanglement of Single-Atom Quantum Bits at a Distance, Nature **449**, 68 (2007).
[38] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network, Phys. Rev. Lett. **124**, 110501 (2020).
[39] P. Maunz, S. Olmschenk, D. Hayes, D. N. Matsukevich, L.-M. Duan, and C. Monroe, Heralded Quantum Gate between Remote Quantum Memories, Phys. Rev. Lett. **102**, 250502 (2009).
[40] M. Lettner, M. Mücke, S. Riedl, C. Vo, C. Hahn, S. Baur, J. Bochmann, S. Ritter, S. Dürr, and G. Rempe, Remote Entanglement between a Single Atom and a Bose-Einstein Condensate, Phys. Rev. Lett. **106**, 210503 (2011).
[41] S. Ritter, C. Nölleke, C. Hahn, A. Reiserer, A. Neuzner, M. Uphoff, M. Mücke, E. Figueroa, J. Bochmann, and G. Rempe, An elementary quantum network of single atoms in optical cavities, Nature **484**, 195 (2012).
[42] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature **526**, 682 (2015).
[43] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Event-Ready Bell Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes, Phys. Rev. Lett. **119**, 010402 (2017).
[44] C. Portmann and R. Renner, Security in Quantum Cryptography, arXiv:2102.00021 (2021).
[45] J. Barrett, R. Colbeck, and A. Kent, Memory Attacks on Device-Independent Quantum Cryptography, Phys. Rev. Lett. **110**, 010503 (2013).
[46] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random num-

bers certified by Bell's theorem, Nature **464**, 1021 (2010).
[47] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).
[48] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).
[49] K. Heshami, D. G. England, P. C. Humphreys, P. J. Bustard, V. M. Acosta, J. Nunn, and B. J. Sussman, Quantum memories: emerging applications and recent advances, Journal of Modern Optics **63**, 2005 (2016).
[50] T. A. Wright, R. J. A. Francis-Jones, C. B. E. Gawith, J. N. Becker, P. M. Ledingham, P. G. R. Smith, J. Nunn, P. J. Mosley, B. Brecht, and I. A. Walmsley, Two-way photonic interface for linking the Sr+ transition at 422 nm to the telecommunication C band, Phys. Rev. Appl. **10**, 044012 (2018).
[51] 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).
[52] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).
[53] S. Bourdeauducq *et al.*, m-labs/artiq: 6.0 (Version 6.0) (2021).

ACKNOWLEDGEMENTS

JDB and EYZT would like to thank Rotem Arnon-Friedman for discussions. We thank Sandia National Laboratories for supplying HOA2 ion traps. This work was supported by the UK EPSRC Hub in Quantum Computing and Simulation (EP/T001062/1), the E.U. Quantum Technology Flagship Project AQTION (No. 820495), and CJB's UKRI Fellowship (MR/S03238X/1). EYZT and RR acknowledge funding by the Swiss National Science Foundation (SNSF), through the National Centers for Competence in Research QSIT and SwissMAP, and by the Air Force Office of Scientific Research (AFOSR) through grant FA9550-19-1-0202. JDB and NS acknowledge funding by the Institut de Physique Théorique (IPhT), Commissariat à l'Énergie Atomique et aux Energies Alternatives (CEA) and the Region Île-de-France in the framework of DIM SIRTEQ.

AUTHOR INFORMATION

Contributions

DPN, PD, BCN, GA, DM, and RS built and operated the experimental apparatus. DPN and PD led the collection of the experimental data and performed the data analysis. JDB and DPN extracted the key from the raw data. KI, RLU and JDB designed the error correction code. JDB, EYZT, NS, PS and RR established the detailed protocol steps and derived the corresponding security proof. NS, JDB, DPN and CJB wrote the manuscript. CJB and DML supervised the experimental work, JDB and NS the theoretical work. NS and JDB initiated the project. All authors contributed to the discussion and interpretation of results, and contributed to the manuscript.

Competing interests

CJB is a director of Oxford Ionics. The remaining authors declare no competing interests.

Corresponding authors

Correspondence regarding experimental work should be addressed to DPN or CJB, that concerning theoretical aspects to JDB or NS.

ADDITIONAL INFORMATION

Supplementary Information is available for this paper.