REVIEW ARTICLE OPEN

Check for updates

Advances in device-independent quantum key distribution

Víctor Zapatero[1,2,3], Tim van Leent[4,5], Rotem Arnon-Friedman[6], Wen-Zhao Liu[7,8,9], Qiang Zhang[7,8,9], Harald Weinfurter[4,5,10] and Marcos Curty[1,2,3]✉

Device-independent quantum key distribution (DI-QKD) provides the gold standard for secure key exchange. Not only does it allow for information-theoretic security based on quantum mechanics, but it also relaxes the need to physically model the devices, thereby fundamentally ruling out many quantum hacking threats to which non-DI QKD systems are vulnerable. In practice though, DI-QKD is very challenging. It relies on the loophole-free violation of a Bell inequality, a task that requires high quality entanglement to be distributed between distant parties and close to perfect quantum measurements, which is hardly achievable with current technology. Notwithstanding, recent theoretical and experimental efforts have led to proof-of-principle DI-QKD implementations. In this article, we review the state-of-the-art of DI-QKD by highlighting its main theoretical and experimental achievements, discussing recent proof-of-principle demonstrations, and emphasizing the existing challenges in the field.

npj Quantum Information (2023)9:10 ; https://doi.org/10.1038/s41534-023-00684-x

INTRODUCTION

Quantum key distribution (QKD)[1–3] is the remote delivery of secret keys through an insecure channel by using quantum-mechanical information carriers. When combined with the one-time pad encryption scheme[4,5], QKD allows for information-theoretically secure communications, unbreakable even for an adversary with unlimited computational power. This is in sharp contrast to public-key cryptosystems, threatened by the advent of quantum computers and by the progress of classical computers as well.

Since its conception in 1984[6], QKD has evolved from a mere theoretical curiosity to a prolific industry at the forefront of quantum technologies. Nowadays, both metropolitan[7–10] and satellite-based[11,12] QKD networks are being built, record-breaking transmission distances are being reached over optical fiber[13–15], and QKD services are being supplied by companies around the globe. However, despite this success, various important challenges must still be addressed for the widespread application of QKD, related to its security, its performance and its integration with the existing optical communication infrastructure.

In particular, a major difficulty is guaranteeing that the QKD devices behave according to the mathematical models presumed in the security proofs, a problem often termed "implementation security". Any disparity between these models and the actual operation of the QKD equipment might invalidate the security claims and potentially opens a security loophole. The importance of this problem is evidenced by the amount of quantum hacking attacks reported in the last two decades[16]. Remarkably, a breakthrough in this respect was the invention of measurement-device-independent (MDI) QKD[17], together with its most recent variant, called twin-field (TF) QKD[18]. Both solutions remove all security loopholes from the measurement unit but require that the functioning of the QKD transmitter is perfectly characterized. Nevertheless, given the complexity of its multiple optical and electronic components[19,20], exhaustively characterizing a QKD transmitter is still an open task.

In this context, device-independent (DI) QKD[21–28] can be considered the ultimate solution to the problem of implementation security, because it does not require to characterize the internal functioning of any device. Conceptually, it is based on the historical Ekert 91 protocol[29], where a central untrusted source distributes entangled photon pairs between two parties, say Alice and Bob—each provided with a measurement unit—and the violation of a Bell inequality[30,31] signals the security of the quantum channel. By performing adequate local measurements on the incident photons, the parties can certify the presence of monogamous correlations between their measurement outcomes[32,33] on the basis of their input-and-output statistics alone[21,34]. Indeed, when their statistics violate a Bell inequality[30,35], it is guaranteed that their outcomes do not arise from a pre-determined strategy attributable to an adversary, usually called Eve.

Much progress has been made to quantitatively link the amount of Bell violation to Eve's uncertainty on the parties' measurement outcomes, and to formally prove that a Bell violation enables the extraction of a secure key (see e.g., Refs. [23–28,36–41] among other works).

The experimental realization of a so-called "loophole-free Bell test" is, however, a major challenge. Entanglement has to be distributed among remote observers, which must be capable of performing random measurements at a high speed and with very high efficiency. In a technological tour de force, several loophole-free Bell tests have been performed in the last years[42–46]. Notably though, for all studied protocols, the possibility to perform DI-QKD is more stringent than the Bell test itself because it demands a large Bell violation. Notwithstanding, proof-of-principle DI-QKD demonstrations have recently been reported[47–49].

[1]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain. [2]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain. [3]AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain. [4]Fakultät für Physik, Ludwig-Maximilians-Universität München, Schellingstr. 4, 80799 München, Germany. [5]Munich Center for Quantum Science and Technology (MCQST), Schellingstr. 4, 80799 München, Germany. [6]Department of Physics of Complex Systems, Weizmann Institute of Science, Rechovot, Israel. [7]Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China. [8]Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China. [9]Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China. [10]Max-Planck Institut für Quantenoptik, Hans-Kopfermann-Str. 1, 85748 Garching, Germany. ✉email: mcurty@com.uvigo.es

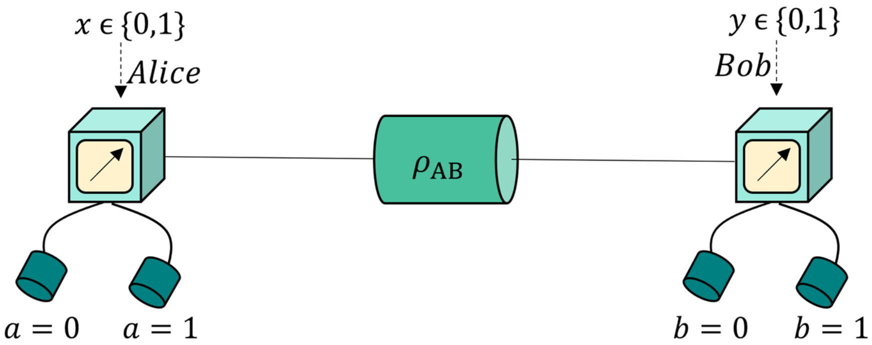

Fig. 1 CHSH test setup. A central source distributes quantum states ρ_{AB} to Alice and Bob, who interact with their measurement devices by providing binary inputs (x and y) and recording binary outputs (a and b) to estimate their CHSH winning probability, ω. As an example, the Tsirelson's bound $\omega = (2+\sqrt{2})/4$ is reached if $\rho_{\mathrm{AB}} = |\Phi^+\rangle\langle\Phi^+|\Phi^+{}_{\mathrm{AB}}$ (with $|\Phi^+\rangle_{\mathrm{AB}} = (|00\rangle_{\mathrm{AB}} + |11\rangle_{\mathrm{AB}})/\sqrt{2}$) and the inputs x and y determine the measurement of the observables A_x and B_y, where $A_0 = \sigma_{\mathrm{Z}}$, $A_1 = \sigma_{\mathrm{X}}$, $B_0 = (\sigma_{\mathrm{Z}} + \sigma_{\mathrm{X}})/\sqrt{2}$ and $B_1 = (\sigma_{\mathrm{Z}} - \sigma_{\mathrm{X}})/\sqrt{2}$ (σ_{Z} and σ_{X} being Pauli matrices). In this ideal example, Alice records output a upon observation of the eigenvalue $(-1)^a$, and similarly for Bob.

In this article, we summarize the progress in the field of DI-QKD. First, we revisit the DI paradigm in "Security assumptions of the DI setting", after which we review the main challenges and theoretical progress in "DI-QKD protocols and challenges" and "Security of DI-QKD". Thereafter, we turn our attention to the emerging topic of experimental DI-QKD in "DI-QKD implementations", with an emphasis on the recent proof-of-principle demonstrations. To finish with, prospects in the field are outlined in "Outlook".

SECURITY ASSUMPTIONS OF THE DI SETTING

Let us first summarize the assumptions on which DI-QKD relies. (1) Quantum mechanics (QM) is correct. By this we mean that, in particular, the measurement statistics of the QKD devices obey Born's rule for some quantum states and some quantum measurements (which need not be known to the users). Of course, this hypothesis is justified by the perfect agreement between QM and experiments. (2) The parties pre-share a short secret key for the authentication of classical messages. (3) The parties can faithfully generate local randomness. Remarkably, this enables the "free" selection of the measurement settings in a precise sense[50], which suffices to establish the completeness of QM for the prediction of measurement outcomes[51]—a frequently invoked assumption by itself— via the exclusion of more predictive theories compatible with it. (4) The parties hold faithful classical post-processing units. (5) No unwanted information leakage occurs through the boundaries of the parties' locations.

The above assumptions are a subset of the assumptions made in the non-DI setting. As long as they hold, no further device characterization enters the security analysis of DI-QKD, which provides a significant security upgrade.

Arguably though, assumption (5)—which is also needed in conventional cryptosystems—might be hard to assure in practice, especially given that entanglement needs to be distributed. In fact, (5) may be replaced by more tenable assumptions modeling the information leakage, to quantify its effect on the secret key rate at the price of slightly undermining the DI feature, as it is done in ref. [47]. Indeed, this approach has also been studied in the non-DI setting[52].

In addition, (5) restricts Eve's capability to sabotage the DI-QKD equipment. This is so because, by hypothesis, it prevents a corrupted device from covertly leaking private information, which could in principle be done in very contrived ways[2,53,54]. In this regard, practical solutions to weaken assumption (5)—and also (4)—are introduced in refs. [53–55]. Particularly those presented in refs. [54,55] combine the use of redundant QKD devices and secret sharing to deal with truly malicious equipment.

Furthermore, another paradigm is being explored to perform DI-QKD with communicating devices—thus violating assumption (5)—as long as (i) they are restricted by a post-quantum computational assumption and (ii) Eve does not have direct access to the channel[56].

DI-QKD PROTOCOLS AND CHALLENGES

The most frequently used Bell inequality in the bipartite scenario is the Clauser-Horne-Shimony-Holt (CHSH) inequality[31], which completely characterizes the set of local correlations in the binary inputs and outputs setting[35,57]. A "CHSH test" can be formulated as a two-party non-local game, as illustrated in Fig. 1.

In every round of the game, Alice and Bob independently provide random binary inputs x and y to their devices, and win the game if their binary outputs a and b fulfill the CHSH winning condition,

$$a \oplus b = x \cdot y, \tag{1}$$

where "$\oplus$" and "$\cdot$" denote addition and multiplication modulo 2, respectively. In this context, the CHSH inequality is an upper bound on the winning probability ω attainable by any probability distribution $p(a,b|x,y)$ that admits a local description:

$$\omega \leq 75\%. \tag{2}$$

Famously, QM enables a maximum winning probability of $(2+\sqrt{2})/4 \approx 85.4\%$ known as the Tsirelson's bound[58], attainable by the measurement statistics of Bell pairs upon careful selection of the measurement settings.

Naturally then, a CHSH-based DI-QKD protocol[24,25,36] runs sequentially, randomly alternating between key rounds —where the parties measure their shares in fixed correlated bases— and test rounds —where they play the CHSH game to quantify Eve's information on the outcomes of the key rounds—. The key basis is chosen to be one of Alice's test bases, and Bob's device incorporates an extra setting to operate in the same basis. As usual, irrelevant basis choice pairings are dismissed a posteriori.

After the quantum communication phase, the generated raw key material undergoes several standard classical post-processing steps (not necessarily in the following order): sifting —where the data from unsuitable basis choice pairings is discarded, thus obtaining the sifted keys—, parameter estimation —where the average score of the CHSH test is calculated—, error correction (EC) —where, say, Bob computes an estimate of Alice's sifted key with the aid of some public discussion, to ensure that both strings match with a high probability— and privacy amplification (PA) —where these latter keys are shrunk into shorter secure bit strings, whose length is prescribed by the parameter estimation step—.

In what follows, we focus on the requirements of implementing CHSH-based DI-QKD. As stated in "Introduction", any DI-QKD protocol fundamentally relies on the violation of a Bell inequality, and the conclusiveness of the latter is subject to the closure of two main loopholes[35]: a locality loophole[59], and a detection loophole[60–62]. The closure of the locality loophole demands that[35,36] (i) the measurement setting choice of one party may not influence the measurement outcome of another party and (ii) the local measurement settings be free choices[50,51]. If either condition is not met, a Bell violation may admit a local description. Although the orthodox approach to enforce (i) is to ensure the space-like separation between the delivery of one party's input and the return of the other party's output, it is widely accepted that proper isolation of the labs —in the lines of assumption (5)— suffices to accomplish (i) for the purpose of DI-QKD[36]. Similarly, condition (ii), which can be relaxed to assuming partial free choice —see[63–65], is in fact guaranteed by assumption (3) (an inevitable assumption in all of cryptography).

On the other hand, the detection loophole demands more attention. In practical Bell tests, signals are lost due to absorption in the channel or device inefficiencies. If lost signals are simply rejected, Eve can fake a Bell violation with a locally deterministic strategy (as long as the loss rate is high enough). Consequently, all the signals must be accounted for in the Bell test —e.g., assigning a specific outcome to undetected signals[35]— which strongly undermines the loss tolerance of DI-QKD as we discuss below.

Hereafter, we refer to the original CHSH-based protocol presented in ref. [25]. For illustration purposes, let us consider an implementation of the protocol using entangled photon pairs, where the parties close the detection loophole by deterministically mapping lost signals to a fixed photo-detector, as mentioned above. In addition, for benchmarking purposes, we contemplate a typical limited-efficiency model[36] where each photon is independently lost with a fixed probability, $\eta_{\rm det}$, which determines the overall detection efficiency of the system. Further assuming perfect preparation of Bell states, a positive asymptotic key rate (that is, considering that the parties execute infinitely many protocol rounds) demands that the efficiency of the photodetectors satisfy $\eta_{\rm det}>92.4\%$ if only detection (but no channel) losses occur[36]. This can be reduced to 90.9% if Bob undoes the assignment of undetected signals for EC purposes[66]. Complementarily, if only channel (but no detection) losses occur, a positive key rate demands that the user-to-user distance satisfy $L<3.5$ km, considering a typical optical fiber with an attenuation coefficient of 0.2 dB/km at telecom wavelength (see e.g., ref. [67]).

While a noticeable progress exists towards close-to-perfect single-photon detection, the constraint on the tolerated channel loss is prohibitive. In fact, if one wants to cover larger distances, the closure of the detection loophole demands the usage of a heralding mechanism, as explained next.

Heralding mechanisms

A heralding mechanism is an instrument that informs the parties about the arrival of a photon or the successful distribution of entanglement between them. In this way, one can decouple channel loss from the measurement settings by simply postponing the choice of the latter until the heralding occurs. Naturally, this allows to discard the signals lost in the channel without opening the detection loophole.

As an example, a quantum non-demolition measurement for the non-destructive detection of a photonic qubit may play the role of a heralding mechanism, and significant progress has recently been reported in this direction[68]. Alternatively, another solution are the so-called 'qubit amplifiers' (QAs)[67,69–73]. Leaving the technicalities aside, a QA essentially is a teleportation gate located at one party's site, such that a successful teleportation locally warns that party about the arrival of a photon. An example of QA-assisted DI-QKD is illustrated in Fig. 2.

Similarly, a related approach more symmetric with respect to both parties is to deliver entanglement via entanglement swapping[74]. In this case, local quantum systems at both sites are respectively entangled with photonic states sent to a central node where the swapping occurs. From there, a successful entanglement distribution is communicated back to both parties. As discussed later in "DI-QKD implementations", this approach provides the foundation for the recent memory-based DI-QKD experiments[47,48], where the heralded entanglement is established between long-lived matter-based quantum memories.

Undoubtedly, heralding mechanisms seem to be a mandatory breakthrough to enlarge the distance potentially covered by DI-QKD. However, various aspects must still be improved for their applicability. In particular, a general bottleneck of heralding schemes is that, with current technology, very long DI-QKD sessions would be required to gather the data block sizes necessary to deliver a positive finite key length at relevant distances[67]. Also, in an all-photonic implementation, the performance of the heralding scheme is limited when one considers practical entanglement sources that sometimes emit vacuum pulses or multiple photon pairs, like e.g., those based on spontaneous parametric down-conversion (SPDC)[67,75–77] (note

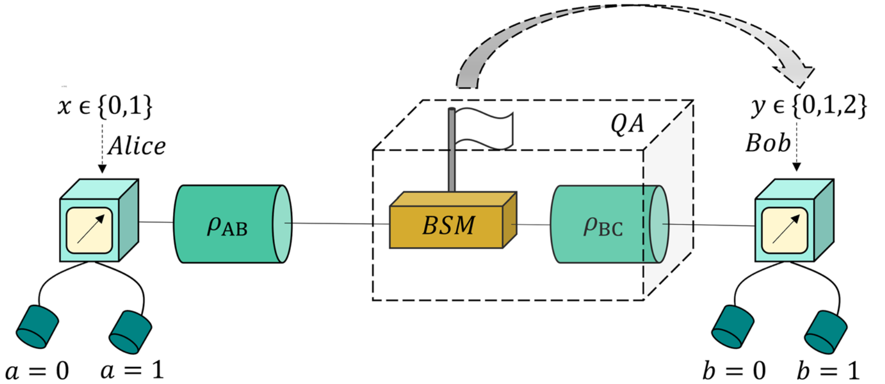

Fig. 2 QA-assisted DI-QKD. One possibility consists of locating the entanglement source $\rho_{\rm AB}$ at Alice's site, such that only Bob experiences channel loss, and thus he is the one equipped with a QA. Alternatively, one can place $\rho_{\rm AB}$ in the channel and equip both Alice and Bob with QAs. For instance, the QA may be constructed with an auxiliary entanglement source $\rho_{\rm BC}$ and a Bell state measurement (BSM). In the BSM, a traveling photon from $\rho_{\rm AB}$ interferes with a photon from $\rho_{\rm BC}$. Upon success of the BSM, Bob is warned of the arrival of a photon—which is symbolized by a flag within the QA—and the entanglement is swapped to the extreme photons entering Alice's and Bob's measurement devices. Only in this successful event, Bob selects his measurement setting. In this way, unheralded signals can be withdrawn without opening the detection loophole. For the purpose of key generation, Bob's device admits a third input setting ($y=2$) matching one of Alice's test bases.

that, in the unheralded setting, fundamental limits on the maximum CHSH violation attainable with SPDC sources have been derived[78,79]).

Regarding the actually implemented memory-based approach—on which we elaborate later—the use of SPDC sources is circumvented by exploiting ion-photon or atom-photon entanglement, but the time issue is further magnified by quantum memory inefficiencies.

Protocol improvements and variants

To relax the requirements of DI-QKD, various modifications of the original CHSH-based protocol have been proposed as well, which must in any case be combined with the use of a heralding mechanism to achieve long distances. In what follows, we briefly discuss some of them. For this purpose, it is convenient to quantify the Bell violation with the CHSH value,

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle, \qquad (3)$$

where the correlators $\langle a_x b_y \rangle$ are defined as $\langle a_x b_y \rangle = p(a = b|x, y) - p(a \neq b|x, y)$. Straightforwardly, the CHSH winning probability and the CHSH value are related as $\omega = S/8 + 1/2$, such that the CHSH inequality and the Tsirelson's bound respectively read $S \leq 2$ and $S \leq 2\sqrt{2}$.

This said, a possible improvement is the addition of a noisy preprocessing step[80] after the estimation of S, where Alice independently flips each sifted key bit with a certain probability. Remarkably, it was shown in ref. [80] that noisy preprocessing can decrease the minimum detection efficiency with an SPDC source to 83.2%, if a multi-mode approach is deployed for photon counting with threshold detectors, and the refined data-processing of ref. [66] is incorporated for EC. This suggests that the development of perfect entanglement sources might not be a priority for all-photonic DI-QKD.

Another possibility to slightly decrease the minimum detection efficiency and enhance the secret key rate is to test asymmetric[81] or generalized[82] CHSH inequalities, where one suitably modifies S by incorporating non-unit weights in the first and the second pairs of correlators appearing in Eq. (3). Given an accurate model of the devices' behavior (which does not enter the security analysis and hence does not compromise the DI feature), the free weights can be optimized in a model-dependent way to enhance the bounds on the secret key rate. In particular, combining this technique with the noisy preprocessing idea, the authors of ref. [81] report a minimum detection efficiency of 82.6% for DI-QKD. This value is attained by considering partially entangled states with an optimized bias and optimized measurement settings as well. Indeed, the possibility of reducing the critical efficiency of a Bell test by using non-maximally entangled states was already pointed out in ref. [83]. Similarly, it was shown in ref. [78] that, with unit efficiency threshold detectors, the maximum CHSH violation accessible to an SPDC source without a heralding mechanism ($S \sim 2.35$) is attained with non-maximally entangled states.

In a similar fashion, instead of simply estimating the CHSH value, one could use the test rounds of the protocol to fully characterize the input-output statistics $p(a, b|x, y)$ of the measurement devices with the available data. It has been shown in refs. [84,85] that this finer-grained analysis (which in fact is not restricted to the CHSH setting, but also applicable to general Bell inequalities) allows to tighten the security bounds and significantly lower the minimum detection efficiency. To be precise, the formerly established threshold of 90.9%[36,66] is reduced to 84% in[85] without noisy preprocessing. A related approach exploiting both the complete statistics and the noisy preprocessing is given in ref. [86], where a DI-QKD protocol with a random post-selection technique is proposed. This technique, originally presented in ref. [87] and limited to the independent and identically distributed (IID) setting discussed in "Security of DI-QKD", which is essential for the proof-of-principle experiment reported in ref. [49].

Also, a suggested protocol modification to enhance the noise-tolerance is to randomly alternate between two different key-generating bases[88,89]. Precisely, both of Alice's test bases are used for key generation in this proposal, and Bob incorporates a new measurement setting accordingly. The intuition behind this idea is that Eve cannot tune her attack to simultaneously maximize her information gain of the measurement outcomes in both (incompatible) key bases. Importantly, in the high noise regime, this additional difficulty for Eve compensates the extra sifting arising from the basis-mismatch probability in the key rounds. Notwithstanding, although the random-key-basis idea increases the tolerated quantum bit error rate (QBER) between the parties' key strings by ~1% within the typical depolarizing-noise model[36]—for instance, in the experiment reported in ref. [48]—, it might not be advantageous in the limited-efficiency model.

Lastly, the authors of ref. [89] also consider the original single-key-basis protocol with deterministic assignments of the lost signals[36], and combine the noisy preprocessing idea with the possibility of taking into account the expected value of Alice's key generation outcome (in addition to the CHSH value) for the parameter estimation. Using this approach and deliberately contemplating partially entangled states, full optimization of the bias of the latter and the measurement settings allows to decrease the minimum detection efficiency to 80.3%.

Needless to say, in all these protocol variants, the minimum detection efficiency is expected to increase if one takes into account any additional form of noise not present in the limited-efficiency model (see e.g., ref. [81]). In this respect, it has been shown that higher-dimensional Bell inequalities offer lower minimum efficiencies and better robustness to noise than the CHSH inequality (see for instance[85,90,91]). Note, however, that solutions like these rely on the possibility of entangling two particles in higher-dimensional degrees of freedom, which is a more complex task from an experimental point of view. But of course, technology is improving, and these ideas may eventually become a feasible experimental alternative for DI-QKD.

Multipartite DI-QKD

To finish this section, it is worth mentioning that the alternative of multipartite DI-QKD —sometimes termed DI conference key agreement (CKA)[92]—has also been explored in theory. The goal here is to distribute an equal secret key among $n > 2$ users. In ref. [92], a non-trivial generalization of the CHSH inequality is devised for the implementation of a DI-CKA protocol with the n-partite Greenberger-Horne-Zeilinger (GHZ) state[93]—which is a natural extension of a Bell state to the multipartite setting. Considering a depolarizing-noise model for every qubit subsystem, the authors of ref. [92] show that, in the low noise regime, their DI-CKA protocol reaches larger asymptotic key rates than the combination of multiple bipartite DI-QKD protocols (as long as Alice cannot perform all the bipartite protocols at the same time).

SECURITY OF DI-QKD

So far, we have mentioned the term "security" (of a DI-QKD protocol) without explicitly saying what is meant by that. Informally, a DI-QKD protocol is secure if, for any device that implements the protocol, either a "good key" is produced, or the protocol aborts with high probability. A "good key" refers to one that is sufficiently close to a key with the following two properties: (a) The key is unknown to the adversary (b) Alice and Bob hold the same key. These statements can be made precise by formal definitions that capture the above and ensure that the produced key can be used freely in subsequent applications; see refs. [94–96] for didactic and rigorous explanations. To prove the security of a protocol, one must show that the considered protocol fulfills the requirements set by the security definitions.

For most protocols, the main theoretical challenge when proving security is to provide a lower bound on a quantity called the smooth conditional min-entropy[97–99] $H^{\varepsilon}_{\min}(\mathbf{A}|E)$, where $\mathbf{A}$ stands for Alice's sifted data, E denotes the information that Eve gathers on $\mathbf{A}$ (including all knowledge leaked to her during the execution of the protocol) and $\varepsilon \in (0,1)$ is a security parameter. Roughly speaking, the smooth conditional min-entropy quantifies the (lack of) knowledge that the adversary has about the sifted data. Once a sufficiently high lower bound on the smooth conditional min-entropy is derived, the PA step of the protocol, in which a function called a strong quantum-proof extractor[100–103] is being applied, guarantees that the final key produced from $\mathbf{A}$ is indeed unknown to the adversary, even when the adversary knows which function was applied. Thus, for the rest of this section, we mainly focus on explaining the main techniques used in order to lower bound $H^{\varepsilon}_{\min}(\mathbf{A}|E)$.

For simplicity, let us first assume that the devices behave in an identical and independent manner in each round of the protocol, i.e., that they use the same set of measurements on the same state in each round. This is also called the IID assumption. In this case, the quantum asymptotic equipartition property (AEP)[104] tells us that, to the first order in the total number of rounds n,

$$H^{\varepsilon}_{\min}(\mathbf{A}|E) \approx nH(A|E), \tag{4}$$

where $H(A|E)$ is the conditional von Neumann entropy "produced" in a single round. Informally, we can say that the total amount of entropy in the system is the sum of its parts. Note that the transition from the smooth conditional min-entropy to the conditional von Neumann entropy, as written above, is of great importance: this is what allows one to get bounds on the amount of randomness —and via this, on the key rate— which are tight to the first order in n. Under the IID assumption, it remains to find a (tight as possible) lower bound on $H(A|E)$, as a function of the winning probability in the considered non-local game. For the CHSH game, this bound was derived in ref. [36] considering the asymptotic regime. Alternatively, for other Bell inequalities or when utilizing the full statistics, one may use the approach of e.g., refs. [85,105] to find a lower bound on the von Neumann entropy, building among others on the Navascués-Pironio-Acín hierarchy[106].

Of course, making the IID assumption in the DI setting is not justified: there is no reason for the device to behave in an independent and identical way in every round of the protocol. What we do know, however, is that the entire operation of the device is sequential, meaning that the protocol is executed one round after the other. Hence, the operations of the device in one round may impact the following rounds, while future rounds cannot affect the past.

This sequential structure lies at the heart of the techniques used to prove the security of DI-QKD protocols against general attacks. In particular, the entropy accumulation theorem (EAT)[107–109] can be seen as an extension of the above mentioned AEP, where instead of the IID assumption the sequential structure (satisfying certain conditions) is used. As the AEP, the EAT states that $H^{\varepsilon}_{\min}(\mathbf{A}|E) \approx nH(A|E)$. Now, however, $H(A|E)$ should be understood as the "worst-case von Neumann entropy" in a single round, which is consistent with the observed average statistics (see ref. [95] for a didactic explanation). Then, using the EAT, the security of DI-QKD can be proven in full generality, i.e., for the strongest possible adversary[40,41].

Other proof techniques that are used to lower bound $H^{\varepsilon}_{\min}(\mathbf{A}|E)$, such as those based on quantum probability estimators[110,111] or the complementarity approach[112], also exploit the sequential structure of the protocols. An exception is the approach of refs. [113,114], that considers "parallel-input" protocols in which the device may perform many rounds all at once, and thus the sequential structure is broken.

Importantly, quantifying Eve's uncertainty about Alice's key for PA purposes is not the only necessary task. As Alice's and Bob's final keys should be identical, we also need to make sure that their bit strings match in the key generation rounds. For this, Alice and Bob need to employ a classical EC protocol on their data, during which some information is transferred between Alice and Bob and, via this, leaks to Eve and increases her knowledge about the data. Therefore, we wish to minimize the amount of communication needed in this step. The quantity that allows one to calculate the minimum amount of communication required for successful EC is the QBER, which we recall is defined as the probability that Alice's and Bob's measurement outcomes are different in the key generation rounds. When optimizing a DI-QKD protocol for a specific setup, one should consider the expected QBER in the actual experiment and choose the parameters of the EC protocol accordingly.

A few last remarks regarding key rates are in order. We did not give explicit equations for the secret key rates achieved in the above works, because these depend on many parameters and are not very informative by themselves. Asymptotically though, the works that exploit the sequential structure of the protocols achieve a key rate that matches the "DI Devetak-Winter key rate"[115–117], i.e., the one that is also achieved under the IID assumption, but without making this assumption in the first place (see Fig. 3a). Some of the cited works (such as e.g., refs. [40,88,118]) and various others derive explicit bounds in the finite key regime, that is to say, for any finite number of rounds. For completeness, Fig. 3b, c illustrate the finite key security bounds obtained in ref. [40]. For a more detailed review about the various security proof techniques see ref. [119].

DI-QKD IMPLEMENTATIONS

In a nutshell, the implementation of DI-QKD requires an experimental platform that distributes entanglement with high fidelity, detection efficiency, and rate, over distances that are relevant for cryptography. More specifically, a sufficiently entangled state and highly efficient appropriate measurements are required to largely violate a Bell inequality while achieving a low QBER, which is mandatory for key generation. With current technology, it remains a major challenge to simultaneously achieve all these conditions, however, proof-of-principle demonstrations have recently been reported[47–49].

Photons are the physical system of choice to distribute entanglement. For instance, one can encode a quantum state in the polarization or time degrees of freedom of a photon, and guide it to a distant location using an optical fiber[120].

For the purpose of DI-QKD, we can distinguish two main implementation categories: all-photonic setups in which the qubits are encoded using photons only, or memory-based setups employing long-lived matter states to generate and store heralded entanglement. Both types of setups have different advantages and face different implementation challenges.

All-photonic setups can generate and distribute entangled states at high rates and with high fidelities, which makes this approach promising for cryptographic applications. For instance, in the ubiquitous example of SPDC sources, the generation of entanglement originates from a single-photon conversion process[75], which is very convenient for a high rate. In fact, minimizing photon-coupling losses and being capable of fastly and randomly switching between different measurement bases enabled the violation of Bell inequalities while closing the detection loophole[121,122], even over distances sufficient to simultaneously enforce space-like separation[43,44]. Despite the preliminary success of photonic Bell tests though, single-photon detectors and distribution through fibers limit the global detection efficiency

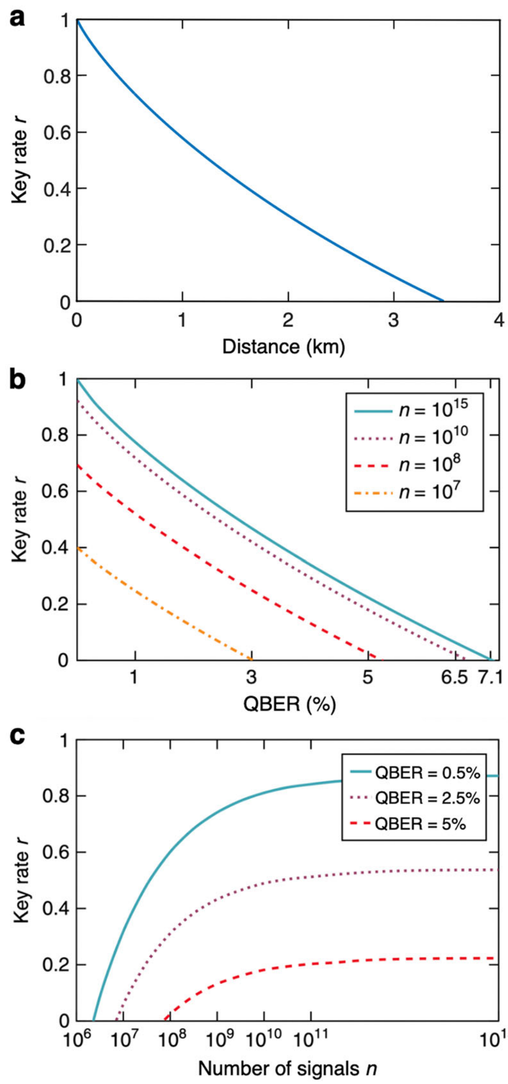

Fig. 3 **Secret key rate performance of DI-QKD.** **a** Asymptotic DI Devetak-Winter secret key rate as a function of the distance[115–117]. An idealized scenario is assumed where Alice and Bob implement unit efficiency measurements on their shares of a perfect Bell pair, delivered by an entanglement source equidistant from both of them. Moreover, the standard approach where undetected signals are mapped to a fixed outcome is presumed for the closure of the detection loophole. Noticeably, even in this idealized setup, the absence of a heralding mechanism implies that the distance covered by DI-QKD is below 3.5 km, considering an attenuation coefficient of 0.2 dB/km (referred to the third telecom window). The limited-efficiency model is considered for the channel loss[36]. **b**, **c** Finite secret key rate as a function of the QBER and the number of transmitted signals, *n*, assuming a depolarizing-noise model for a perfect Bell pair and no losses of any kind. For illustration purposes, some typical finite-key parameters are selected. Both figures, b and c, are reproduced from ref. [40] under the Creative Commons license.

and hence the distance of all-photonic DI-QKD, unless the heralded approach presented in “DI-QKD protocols and challenges” is deployed. Nevertheless, DI-QKD based on all-photonic heralding schemes has not been realized so far, although all the necessary experimental methods have been demonstrated individually.

On the other hand, memory-based approaches generate heralded entanglement between two matter-based quantum memories. Such schemes have been demonstrated using different systems as quantum memories and allow to close the detection loophole[42,45]. Essential here is, however, to realize efficient light-matter interfaces and high-speed entanglement generation procedures to shorten the necessary duration of a potential DI-QKD session.

Photonic-based implementations

The most efficient photonic experiment reported until recently[123] (deployed for DI randomness expansion) reached a single-photon detection efficiency of around 84%. At the time the experiment was carried out, the CHSH-based protocol variants that lower the detection efficiency below that value had not been proposed yet (e.g., refs. [80,81,85]), and hence it was considered that the system did not keep up with the requirements of DI-QKD in practice. Very recently, the combination of various experimental simplifications with the post-selection technique of ref. [86] enabled the realization of a proof-of-principle all-photonic DI-QKD experiment without a heralding mechanism[49]. Specifically, the applied random post-selection technique significantly reduces the error events, leading to tolerable detection efficiencies as low as 68.5% in the limited-efficiency model. However, this technique—which is central to enable the delivery of a positive asymptotic key rate in the experiment— relies on the IID assumption in a fundamental way (see ref. [87]). Therefore, more research is needed to investigate whether it can be extended to the fully DI setting against general adversaries.

As for the experimental simplifications, the measurement settings were not randomly changed from round to round in the experiment, but rather waveplates were set manually to determine all the correlators for evaluating *S*. In addition, aiming to simulate longer distances, optical fibers with a total length of 220 m were placed behind the state analysis to avoid the otherwise required stabilization of the polarization.

In any case, within this preliminary simplified scenario, after 2.4×10^8 rounds of experiment for each of the six combinations of measurement settings, the observed statistics would yield an asymptotic secret key rate of 2.33×10^{-4} secret key bits per round. A schematic of the setup is depicted in Fig. 4, which consists of three modules. Pairs of polarization-entangled photons at the wavelength of 1560 nm are generated probabilistically via the SPDC process in the central module (a). These pairs of photons are sent over a short distance to two receiver modules (b). In each module, approximately 100 m of fiber precede the single photon detectors where the measurements are performed to generate the raw data. The overall single-photon detection efficiencies are respectively determined to be $87.16 \pm 0.22\%$ and $87.82 \pm 0.21\%$ for Alice and Bob, which significantly surpass the record values in previous experiments with photons.

In short, despite the great progress that the experiment represents[49], an all-photonic implementation delivering a positive finite key length may still require further technological improvements. On top of it, needless to say, the deployment of all-photonic heralding schemes is also a must aiming to cover relevant distances.

Memory-based implementations

Quantum memories with light-matter interfaces enable the generation of heralded entanglement between distant locations. For this, the memories first emit a photon to generate entanglement between light and matter[124–126] or interact with incoming light in a state dependent manner[127,128]. Two distant memories can then be entangled by using, for example, heralded storage of an entangled photon pair, entanglement swapping from two light-matter pairs, or enhanced light-matter interaction by resonators. Various quantum systems are under active research to facilitate entanglement distribution, and heralded entanglement has been generated for platforms including ions[129], atoms[130,131], and NV-centers[132], even over long distances and

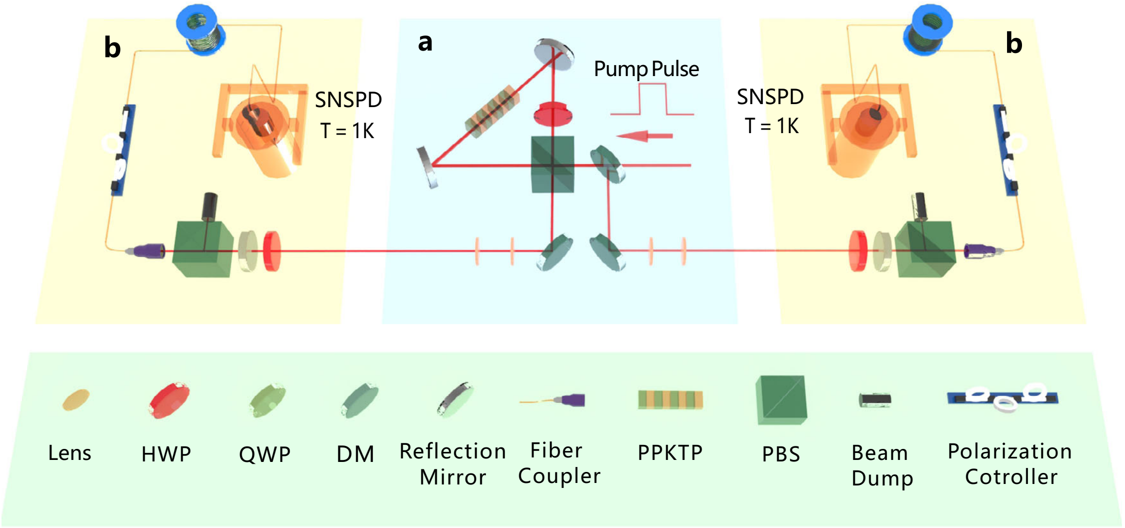

Fig. 4 Schematic of the all-photonic DI-QKD implementation reported in ref. [49]. **a** Entanglement source. For the creation of pairs of entangled photons, light pulses of 10 ns are injected at a repetition pulse rate of 2 MHz into a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop to generate polarization-entangled photon pairs. The two photons of an entangled pair at 1560 nm travel in opposite directions towards Alice and Bob, where they are subject to polarization projection measurements. **b** Alice's and Bob's QKD receivers. In her (his) measurement site, Alice (Bob) uses a set of HWP and QWP to project the polarization of the incoming single photons into a pre-determined measurement basis. After being collected into the fiber, the photons travel through a certain length of fiber and then are detected by a superconducting nanowire single-photon detector (SNSPD) operating at 1K. HWP half-wave plate, QWP quarter-wave plate, DM dichroic mirror, PBS polarizing beam splitter. Reprinted figure with permission from ref. [49] (https://doi.org/10.1103/PhysRevLett.129.050502), Copyright 2022 by the American Physical Society.

with readout speeds capable of simultaneously enforcing space-like separation[42,45].

Heralded entanglement generation between quantum memories allows to close the detection loophole in a Bell test regardless of channel loss, however, DI-QKD is more demanding than this alone[133]. The current challenge is to distribute high-quality entangled states and, at the same time, to achieve entanglement rates over distances that are relevant for cryptography. The highest entanglement fidelity reported so far equals 96%, employing two distant ion based quantum memories[47,134]. These fidelities are not fundamentally limited though, and could be increased by further reducing state generation or readout errors. Generation rates of high quality entangled states up to 100 Hz have been reported[134–136], and higher rates could still be achieved employing cavities to improve photon collection efficiencies[137,138]. Moreover, single-photon interference provides a promising venue for entanglement generation protocols[139–141], although so far only at the price of reducing the quality of the entanglement.

While the memory-based heralding schemes do not have a fundamental distance limitation, due to absorption the entanglement generation rate decreases exponentially over the distance. To minimize channel loss and hence maximize the rate using optical fibers, operation at telecom wavelengths is indispensable. Indeed, entanglement between quantum memories has already been distributed over tens of km employing quantum frequency conversion[131,141] or absorptive quantum memories[142,143].

Recently, two similar proof-of-principle implementations of memory-based DI-QKD have been reported: one using single $^{88}\mathrm{Sr}^{+}$ ions in Oxford[47] and the other using single $^{87}\mathrm{Rb}$ atoms in Munich[48]. The experiments employ charged or neutral single atoms as quantum memories which are isolated from the environment inside ultra-high vacuum setups and spatially confined using electrically or optically induced trapping potentials, respectively. Other than the trapping techniques, the concepts used to distribute entanglement are very similar for the two implementations, and Fig. 5 shows a high-level schematic of the quantum network link that is representative for both setups. Also, Fig. 6 shows a picture of the single-atom trap employed in ref. [48].

Each link consists of two distant quantum memories that are entangled in an event-ready scheme. First, each of the atomic spin states is entangled in a spontaneous decay with the polarization of the emitted photon. The two photons are guided with single-mode fibers to a BSM device where a joint measurement on the photons heralds the entanglement between the ions or atoms, respectively. The quantum state of the memories is measured after every heralding signal with unit detection efficiency, thereby closing the detection loophole for the Bell test.

Performance parameters of the two quantum links are listed in Table 1. The rate at which the links generate entanglement critically depends on the success probability of the entanglement generation tries and their repetition rate. The former is mainly limited by the efficiency to collect photons emitted by the memories, which is typically up to a few percent using free-space optics. Including channel and detection losses, this leads to heralding probabilities on the order of 10^{-4} to 10^{-6}. For the implemented event-ready schemes, the entanglement generation tries can only be repeated after a period that allows for two-way communication between the devices and the BSM setup, thus introducing a trade-off between distance and rate. The achieved fidelities of the states shared between the distant quantum memories belong to the highest reported so far (see Table 1) and allow one to achieve positive key rates in DI-QKD protocols.

As discussed in “Security assumptions of the DI setting”, proper isolation of the users' locations is a way to practically close the locality loophole in the Bell test. The generation of entanglement, however, requires the photonic channel, i.e., a connection

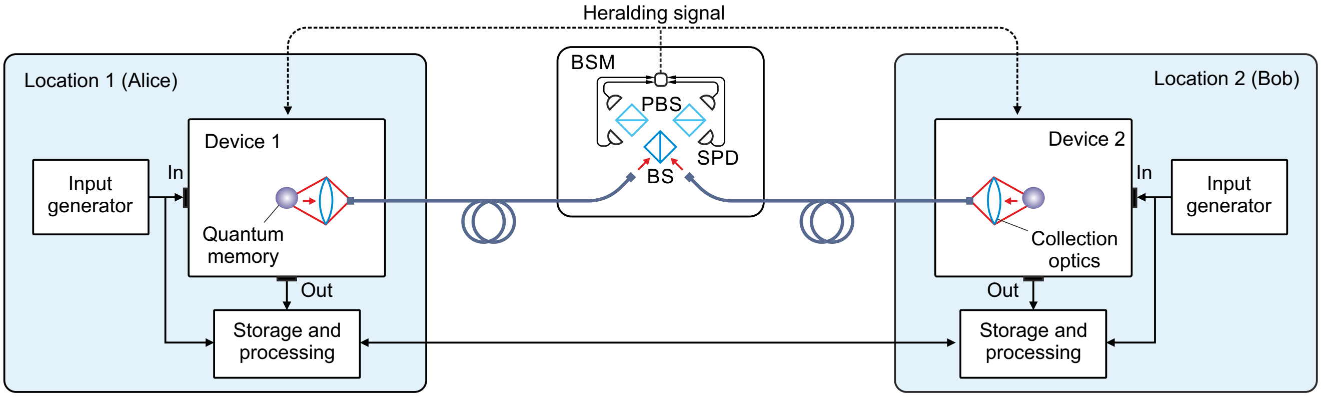

Fig. 5 Schematic of the memory-based DI-QKD implementations reported in refs. [47,48]. Alice and Bob are situated at distant locations and equipped with an input generator, storage and process unit, and a device containing a single ion or atom quantum memory. The memories are entangled as follows. First, via spontaneous decay entangled atom-photon pairs are generated in each device. The photons are collected into fibers that guide them to a Bell-state measurement (BSM) setup. There, they interfere at a beam splitter (BS) where in each output port the photon polarization is analysed with a polarizing BS (PBS) and two single photon detectors (SPD). The entanglement generation tries are repeated till a photonic coincidence detection occurs and heralds shared entanglement between the quantum memories. Next, the DI-QKD protocol starts with a random seed from the input generators to select the measurement orientation, perform the measurement, and output the result. These measurement in- and outputs of every round are stored in a local storage. The storage and processing unit are connected via an authenticated classical channel to facilitate the post-processing steps of the key generation procedure.

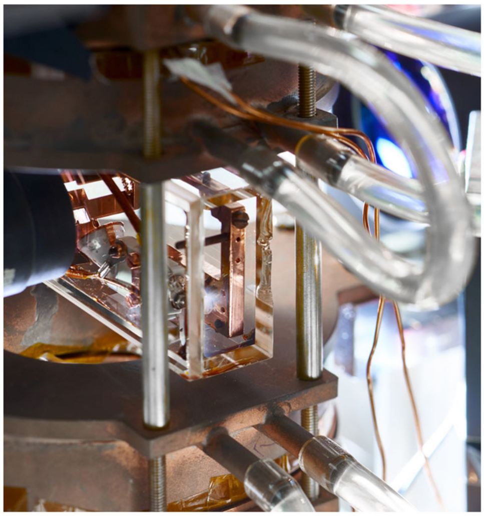

Fig. 6 Picture of a single-atom trap employed in ref. [48]. Shown is the ultra-high vacuum glass cell in which a single rubidium atom is stored (authorized by the copyright owner Jan Gruene, from LMU).

between the quantum memories, and hence opens a back door to the outside environment. Therefore, after distributing the entanglement, this link should be disconnected. For this, in the Oxford experiment, the ions are moved out of the focus of the optics and hence prevent fluorescence from coupling into the fiber leaving the laboratory. In the Munich experiment, a shutter closes the atomic fluorescence light path leaving the laboratory. Moreover, before repositioning the ions or opening the shutter, the atomic states are scrambled or the atoms are ejected from the trap to avoid information leakage to the environment when reconnecting the quantum link. These processes must be well-characterized, to ideally quantify any possible information leakage and account for it in the security proof.

The key distribution capability of the ion-based system was evaluated by generating a secret key between Alice and Bob. For this, a finite-key security analysis was considered, together with a protocol that implemented EC, authentication and PA. A total of 1.5×10^6 Bell pairs were generated during a period of 7.9 h, achieving a CHSH value of $S = 2.677(6)$ and a QBER of $Q = 0.0144(2)$. After a post-processing time of 5 min, the protocol generated 95 884 shared secret bits (i.e., 0.064 bits per entanglement generation event), while only 256 bits were consumed during the key generation process.

Table 1. Performance of the quantum links.

	Oxford[47]	Munich[48]
Fidelity	0.960(1)	0.892(23)
Rate (s^{-1})	100	1/82
Fiber length (m)	3.5	700

Key parameters that characterize the quantum link performance employed in the proof-of-principle memory-based DI-QKD experiments. The line-of-sight distance between the two quantum memories is 2 and 400 m for the Oxford and Munich experiments, respectively.

For the atom-based system, an asymptotic security analysis was made, since the generation of a key secure under finite statistics would have taken months of quantum communication. In particular, over a period of 75 h, a total of 3342 entanglement generation rounds were executed, observing a CHSH value of $S = 2.578(75)$ and a QBER of $Q = 0.078(9)$. This translates into an asymptotic secret key rate of 0.07 bits per entanglement generation event (compared to the maximum of 0.25 for the protocol used).

Single photons with respective wavelengths of 422 and 780 nm distributed the entanglement, corresponding to an attenuation loss of a factor two for every 100 and 700 m of optical fiber in each case. To achieve entanglement distribution over more than a few kilometers of fiber, it is required to operate at low-loss telecom wavelengths. In this regard, conversion of light from 422 nm to the telecom regime was recently achieved in a demonstration setup[144]. Moreover, fully polarization-preserving quantum frequency conversion was implemented in the atom-based experiment, which converts the wavelength from 780 nm to telecom wavelength for a single photon while maintaining its quantum state[145]. The high conversion efficiency of about 57% allowed to distribute entanglement of atomic quantum memories over tens of kilometers of fiber[131]. However, besides providing an even lower entanglement generation rate, the achieved fidelity would not be sufficient for DI-QKD yet, due to the decoherence of the atomic quantum memories.

OUTLOOK

Over the last years, crucial theoretical and experimental advancements have been made, which enabled proof-of-principle QKD demonstrations in the DI setting. For practical implementations, however, more effort is required.

On the theory side, the analysis of the studied schemes is tight when considering CHSH-based protocols. To improve the performance, more sophisticated protocols including e.g., two-way classical communication in the post-processing stage[146] or exploiting higher-dimensional Bell inequalities[90,91] might be an option, though they seem to be challenging at the moment.

On the experimental side, all-photonic approaches including heralding schemes are a promising venue towards DI-QKD over tens of kilometers, where fully integrated photonics could further improve the efficiencies of the devices. In memory-based implementations, the achieved entanglement fidelities between distant matter qubits allow for positive key rates in the DI setting, but a severe challenge is to achieve high entanglement rates over distances which are relevant for key distribution. For this, using e.g., cavities could increase the efficiencies of the light-matter interfaces. Especially for event-ready schemes, parallelization of the entanglement generation tries can potentially increase the entanglement generation rate by orders of magnitude. For this, hardware architectures that were initially proposed for quantum simulation and computation applications could be exploited, for example, using strings of trapped ions or atom arrays[147,148].

Another interesting research direction is "other forms" of DI protocols. That is, protocols in which we do not characterize the devices but the assumptions we do make are not comparable to those described in "Security assumptions of the Di setting"[17,18,56,149] being examples of such scenarios. It is for the theoreticians and experimentalists together to investigate which models are of relevance and develop both the security proofs and the necessary equipment for the implementation of the upcoming protocols.

On the long run, quantum networks might be employed to efficiently transfer quantum states over long distances and provide connections between quantum computers. These networks will supply shared entanglement between the nodes, which will be accessed with very high efficiency. As all the necessary tools are available, DI-QKD may become a regular application for secure communications of the highest level.

Received: 29 August 2022; Accepted: 11 February 2023;
Published online: 18 February 2023

REFERENCES

1. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
2. 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).
3. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
4. Miller, F. Telegraphic code to insure privacy and secrecy in the transmission of telegrams. CM Cornwell (1882).
5. Vernam, G. S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *J. AIEE* **45**, 109–115 (1926).
6. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *In Proc. IEEE International Conference on Computers, Systems & Signal Processing*, 175–179 (IEEE, NY, Bangalore, India, 1984).
7. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409 (2011).
8. Stucki, D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *N. J. Phys.* **13**, 123001 (2011).
9. Dynes, J. F. et al. Cambridge quantum network. *NPJ Quantum Inf.* **5**, 101 (2019).
10. Yang, Y. H. et al. All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Opt. Express* **29**, 25859–25867 (2021).
11. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
12. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4600 kilometres. *Nature* **589**, 214–219 (2021).
13. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
14. Chen, J. P. et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photonics* **15**, 570–575 (2021).
15. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
16. Jain, N. et al. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemp. Phys.* **57**, 366–387 (2016).
17. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
18. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
19. Pereira, M., Curty, M. & Tamaki, K. Quantum key distribution with flawed and leaky sources. *NPJ Quantum Inf.* **5**, 1–12 (2019).
20. Pereira, M., Kato, G., Mizutani, A., Curty, M. & Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **6**, eaaz4487 (2020).
21. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. *In Proceedings 39th Annual Symposium on Foundations of Computer Science* 503–509 (IEEE, 1998).
22. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).
23. Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
24. Acín, A., Massar, S. & Pironio, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *N. J. Phys.* **8**, 126 (2006).
25. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
26. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* **2**, 1–7 (2011).
27. Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
28. Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM* **63**, 1–63 (2016).
29. Ekert, A. K. Quantum cryptography based on Bell's Theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
30. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Phys. Phys. Fiz.* **1**, 195 (1964).
31. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880 (1969).
32. Coffman, V., Kundu, J. & Wootters, W. K. Distributed entanglement. *Phys. Rev. A* **61**, 052306 (2000).
33. Terhal, B. M. Is entanglement monogamous? *IBM J. Res. Dev.* **48**, 71–78 (2004).
34. Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Information & Computation* **4**, 273–286 (Rinton Press, Paramus, NJ, 2004).
35. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419 (2014).
36. Pironio, S. et al. Device-independent quantum key distribution secure against collective attacks. *N. J. Phys.* **11**, 045021 (2009).
37. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
38. Acín, A., Massar, S. & Pironio, S. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.* **108**, 100402 (2012).
39. Tomamichel, M. & Hänggi, E. The link between entropic uncertainty and nonlocality. *J. Phys. A: Math. Theor.* **46**, 055301 (2013).
40. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **9**, 1–11 (2018).
41. Arnon-Friedman, R., Renner, R. & Vidick, T. Simple and tight device-independent security proofs. *SIAM J. Comput.* **48**, 181–225 (2019).
42. Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
43. Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
44. Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
45. Rosenfeld, W. et al. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017).
46. Li, M. et al. Test of local realism into the past without detection and locality loopholes. *Phys. Rev. Lett.* **121**, 080404 (2018).

47. Nadlinger, D. P. et al. Experimental quantum key distribution certified by Bell's theorem. *Nature* **607**, 682–686 (2022).
48. Zhang, W. et al. A device-independent quantum key distribution system for distant users. *Nature* **607**, 687–691 (2022).
49. Liu, W. Z. et al. Toward a photonic demonstration of device-independent quantum key distribution. *Phys. Rev. Lett.* **129**, 050502 (2022).
50. Bell, J. S. Free variables and local causality. *In Speakable and unspeakable in quantum mechanics*, chapter 12 (Cambridge University Press, 1987).
51. Colbeck, R. & Renner, R. The completeness of quantum theory for predicting measurement outcomes. *In Quantum theory: informational foundations and foils*, 497–528 (Springer, Dordrecht, 2016).
52. Tamaki, K., Curty, M. & Lucamarini, M. Decoy-state quantum key distribution with a leaky source. *N. J. Phys.* **18**, 065008 (2016).
53. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).
54. Curty, M. & Lo, H.-K. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *NPJ Quantum Inf.* **5**, 1–11 (2019).
55. Zapatero, V. & Curty, M. Secure quantum key distribution with a subset of malicious devices. *NPJ Quantum Inf.* **7**, 1–8 (2021).
56. Metger, T., Dulek, Y., Coladangelo, A. & Arnon-Friedman, R. Device-independent quantum key distribution from computational assumptions. *N. J. Phys.* **23**, 123021 (2021).
57. Froissart, M. Constructive generalization of Bell's inequalities. *Nuovo Cim. B* **64**, 241–251 (1981).
58. Cirelson, B. S. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4**, 93–100 (1980).
59. Bell, J. S. La nouvelle cuisine. *In Speakable and unspeakable in quantum mechanics*, chapter 24 (Cambridge University Press, 2004).
60. Pearle, P. M. Hidden-variable example based upon data rejection. *Phys. Rev. D.* **2**, 1418 (1970).
61. Clauser, J. F. & Horne, M. A. Experimental consequences of objective local theories. *Phys. Rev. D.* **10**, 526 (1974).
62. Gisin, N. & Gisin, B. A local hidden variable model of quantum correlation exploiting the detection loophole. *Phys. Lett. A* **260**, 323–327 (1999).
63. Colbeck, R. & Renner, R. Free randomness can be amplified. *Nat. Phys.* **8**, 450–453 (2012).
64. Pütz, G., Rosset, D., Barnea, T. J., Liang, Y. C. & Gisin, N. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality. *Phys. Rev. Lett.* **113**, 190402 (2014).
65. Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization. *IEEE J. Sel. Areas Inf. Theory* **1**, 568–584 (2020).
66. Ma, X. & Lütkenhaus, N. Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD. *Quantum Inf. Comput.* **12**, 203–214 (2012).
67. Zapatero, V. & Curty, M. Long-distance device-independent quantum key distribution. *Sci. Rep.* **9**, 1–18 (2019).
68. Niemietz, D., Farrera, P., Langenfeld, S. & Rempe, G. Nondestructive detection of photonic qubits. *Nature* **591**, 570–574 (2021).
69. Gisin, N., Pironio, S. & Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.* **105**, 070501 (2010).
70. Pitkanen, D., Ma, X., Wickert, R., Van Loock, P. & Lütkenhaus, N. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Phys. Rev. A* **84**, 022325 (2011).
71. Curty, M. & Moroder, T. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A* **84**, 010304 (2011).
72. Meyer-Scott, E. et al. Entanglement-based linear-optical qubit amplifier. *Phys. Rev. A* **88**, 012327 (2013).
73. Kołodyński, J. et al. Device-independent quantum key distribution with single-photon sources. *Quantum* **4**, 260 (2020).
74. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287 (1993).
75. Kwiat, P. G. et al. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337 (1995).
76. Ma, X., Fung, C. H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
77. Seshadreesan, K. P., Takeoka, M. & Sasaki, M. Progress towards practical device-independent quantum key distribution with spontaneous parametric down-conversion sources, on-off photodetectors, and entanglement swapping. *Phys. Rev. A* **93**, 042328 (2016).
78. Vivoli, V. C. et al. Challenging preconceptions about Bell tests with photon pairs. *Phys. Rev. A* **91**, 012107 (2015).
79. Tsujimoto, Y. et al. Optimal conditions for the Bell test using spontaneous parametric down-conversion sources. *Phys. Rev. A* **98**, 063842 (2018).
80. Ho, M. et al. Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 230502 (2020).
81. Woodhead, E., Acín, A. & Pironio, S. Device-independent quantum key distribution with asymmetric CHSH inequalities. *Quantum* **5**, 443 (2021).
82. Sekatski, P. et al. Device-independent quantum key distribution from generalized CHSH inequalities. *Quantum* **5**, 444 (2021).
83. Eberhard, P. H. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A* **47**, R747 (1993).
84. Tan, E. Y. Z., Schwonnek, R., Goh, K. T., Primaatmaja, I. W. & Lim, C. C. W. Computing secure key rates for quantum cryptography with untrusted devices. *NPJ Quantum Inf.* **7**, 1–6 (2021).
85. Brown, P., Fawzi, H. & Fawzi, O. Computing conditional entropies for quantum correlations. *Nat. Commun.* **12**, 1–12 (2021).
86. Xu, F., Zhang, Y. Z., Zhang, Q. & Pan, J. W. Device-Independent quantum key distribution with random postselection. *Phys. Rev. Lett.* **128**, 110506 (2022).
87. de la Torre, G., Bancal, J. D., Pironio, S. & Scarani, V. Randomness in post-selected events. *N. J. Phys.* **18**, 035007 (2016).
88. Schwonnek, R. et al. Device-independent quantum key distribution with random key basis. *Nat. Commun.* **12**, 1–8 (2021).
89. Masini, M., Pironio, S. & Woodhead, E. Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints. *Quantum* **6**, 843 (2022).
90. Miklin, N., Chaturvedi, A., Bourennane, M., Pawłowski, M. & Cabello, A. Exponentially decreasing critical detection efficiency for any Bell inequality. *Phys. Rev. Lett.* **129**, 230403 (2022).
91. Xu, Z. P. et al. Graph-theoretic approach to Bell experiments with low detection efficiency. Preprint at https://arxiv.org/abs/2205.05098 (2022).
92. Holz, T., Kampermann, H. & Bruß, D. Genuine multipartite Bell inequality for device-independent conference key agreement. *Phys. Rev. Res.* **2**, 023251 (2020).
93. Greenberger, D. M., Horne, M. A. & Zeilinger, A. Going beyond Bell's theorem. *In Bell's theorem, quantum theory and conceptions of the universe* pp. 69–72 (Springer, Dordrecht, 1989).
94. Portmann, C. & Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).
95. Arnon-Friedman, R. Device-Independent Quantum Information Processing: A Simplified Analysis. *Springer Nature* (2020).
96. Wolf, R. Quantum Key Distribution: An Introduction with Exercises. *Springer Nature*, Vol. **988** (2021).
97. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **6**, 1–127 (2008).
98. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **56**, 4674–4681 (2010).
99. Tomamichel, M. Quantum information processing with finite resources: mathematical foundations. *Springer*, Vol. **5** (2015).
100. Renner, R. & König, R. Universally composable privacy amplification against quantum adversaries. *Theory of cryptography. Springer*, pp. 407–425 (2005).
101. König, R. & Terhal, B. M. The bounded-storage model in the presence of a quantum adversary. *IEEE Trans. Inf. Theory* **54**, 749–762 (2008).
102. Fehr, S. & Schaffner, C. Randomness extraction via δ-biased masking in the presence of a quantum attacker. *Theory of cryptography conference. Springer*, pp. 465–481 (2008).
103. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.* **41**, 915–940 (2012).
104. Tomamichel, M., Colbeck, R. & Renner, R. A fully quantum asymptotic equipartition property. *IEEE Trans. Inf. Theory* **55**, 5840–5847 (2009).
105. Brown, P., Fawzi, H. & Fawzi, O. Device-independent lower bounds on the conditional von Neumann entropy. Preprint at https://arxiv.org/pdf/2106.13692.pdf (2021).
106. Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *N. J. Phys.* **10**, 073013 (2008).
107. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. *Commun. Math. Phys.* **379**, 867–913 (2020).
108. Dupuis, F. & Fawzi, O. Entropy accumulation with improved second-order term. *IEEE Trans. Inf. Theory* **65**, 7596–7612 (2019).
109. Metger, T., Fawzi, O., Sutter, D. & Renner, R. Generalised entropy accumulation. *In 63rd Annual Symposium on Foundations of Computer Science* 844–850 (IEEE, 2022).
110. Zhang, Y., Knill, E. & Bierhorst, P. Certifying quantum randomness by probability estimation. *Phys. Rev. A* **98**, 040304 (2018).
111. Zhang, Y., Fu, H. & Knill, E. Efficient randomness certification by quantum probability estimation. *Phys. Rev. Res.* **2**, 013016 (2020).
112. Zhang, X., Zeng, P., Ye, T., Lo, H. K. & Ma, X. Quantum complementarity approach to device-independent security. Preprint at https://arxiv.org/abs/2111.13855 (2021).

113. Jain, R., Miller, C. A. & Shi, Y. Parallel device-independent quantum key distribution. *IEEE Trans. Inf. Theory* **66**, 5567–5584 (2020).
114. Vidick, T. Parallel DIQKD from parallel repetition. Preprint at https://arxiv.org/abs/1703.08508 (2017).
115. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A: Math., Phys. Eng. Sci.* **461**, 207–235 (2005).
116. Kaur, E., Wilde, M. M. & Winter, A. Fundamental limits on key rates in device-independent quantum key distribution. *N. J. Phys.* **22**, 023039 (2020).
117. Arnon-Friedman, R. & Leditzky, F. Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture. *IEEE Trans. Inf. Theory* **67**, 6606–6618 (2021).
118. Bhavsar, R., Ragy, S. & Colbeck, R. Improved device-independent randomness expansion rates from tight bounds on the two sided randomness using CHSH tests. Preprint at https://arxiv.org/abs/2103.07504 (2021).
119. Primaatmaja, I. W. et al. Security of device-independent quantum key distribution protocols: a review. Preprint at https://arxiv.org/abs/2206.04960 (2022).
120. Gisin, N. & Thew, R. Quantum communication. *Nat. Photonics* **1**, 165–171 (2007).
121. Giustina, M. et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227–230 (2013).
122. Christensen, B. G. et al. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
123. Liu, W. Z. et al. Device-independent randomness expansion against quantum side information. *Nat. Phys.* **17**, 448–451 (2021).
124. Blinov, B. B., Moehring, D. L., Duan, L.-M. & Monroe, C. Observation of entanglement between a single trapped atom and a single photon. *Nature* **428**, 153–157 (2004).
125. Matsukevich, D. N. & Kuzmich, A. Quantum state transfer between matter and light. *Science* **306**, 663–666 (2004).
126. Volz, J. et al. Observation of entanglement of a single photon with a trapped atom. *Phys. Rev. Lett.* **96**, 030404 (2006).
127. Julsgaard, B., Sherson, J., Cirac, J. I., Fiurášek, J. & Polzik, E. S. Experimental demonstration of quantum memory for light. *Nature* **432**, 482–486 (2004).
128. Wilk, T., Webster, S. C., Kuhn, A. & Rempe, G. Single-atom single-photon quantum interface. *Science* **317**, 488–490 (2007).
129. Matsukevich, D. N., Maunz, P., Moehring, D. L., Olmschenk, S. & Monroe, C. Bell inequality violation with two remote atomic qubits. *Phys. Rev. Lett.* **100**, 150404 (2008).
130. Hofmann, J. et al. Heralded entanglement between widely separated atoms. *Science* **337**, 72–75 (2012).
131. van Leent, T. et al. Entangling single atoms over 33 km telecom fibre. *Nature* **607**, 69–73 (2022).
132. Bernien, H. et al. Heralded entanglement between solid-state qubits separated by three metres. *Nature* **497**, 86–90 (2013).
133. Farkas, M., Balanzó-Juandó, M., Łukanowski, K., Kołodyński, J. & Acín, A. Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. *Phys. Rev. Lett.* **127**, 050503 (2021).
134. Stephenson, L. J. et al. High-rate, high-fidelity entanglement of qubits across an elementary quantum network. *Phys. Rev. Lett.* **124**, 110501 (2020).
135. Humphreys, P. C. et al. Deterministic delivery of remote entanglement on a quantum network. *Nature* **558**, 268–273 (2018).
136. Stockill, R. et al. Phase-tuned entangled state generation between distant spin qubits. *Phys. Rev. Lett.* **119**, 010503 (2017).
137. Schupp, J. et al. Interface between trapped-ion qubits and traveling photons with close-to-optimal efficiency. *PRX Quantum* **2**, 020331 (2021).
138. Brekenfeld, M., Niemietz, D., Christesen, J. D. & Rempe, G. A quantum network node with crossed optical fibre cavities. *Nat. Phys.* **16**, 647–651 (2020).
139. Pompili, M. et al. Realization of a multinode quantum network of remote solid-state qubits. *Science* **372**, 259–264 (2021).
140. Cabrillo, C., Cirac, J. I., Garcia-Fernandez, P. & Zoller, P. Creation of entangled states of distant atoms by interference. *Phys. Rev. A* **59**, 1025 (1999).
141. Yu, Y. et al. Entanglement of two quantum memories via fibres over dozens of kilometres. *Nature* **578**, 240–245 (2020).
142. Lago-Rivera, D., Grandi, S., Rakonjac, J. V., Seri, A. & de Riedmatten, H. Telecom-heralded entanglement between multimode solid-state quantum memories. *Nature* **594**, 37–40 (2021).
143. Liu, X. et al. Heralded entanglement distribution between two absorptive quantum memories. *Nature* **594**, 41–45 (2021).
144. Wright, T. A. et al. Two-way photonic interface for linking the Sr+ transition at 422 nm to the telecommunication C band. *Phys. Rev. Appl.* **10**, 044012 (2018).
145. Ikuta, R. et al. Polarization insensitive frequency conversion for an atom-photon entanglement distribution via a telecom network. *Nat. Commun.* **9**, 1–8 (2018).
146. Tan, E. Y. Z., Lim, C. C. W. & Renner, R. Advantage distillation for device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 020502 (2020).
147. Ramette, J. et al. Any-to-any connected cavity-mediated architecture for quantum computing with trapped ions or Rydberg arrays. *PRX Quantum* **3**, 010344 (2022).
148. Dordevic, T. et al. Entanglement transport and a nanophotonic interface for atoms in optical tweezers. *Science* **373**, 1511–1514 (2021).
149. Van Himbeeck, T., Woodhead, E., Cerf, N. J., García-Patrón, R. & Pironio, S. Semi-device-independent framework based on natural physical assumptions. *Quantum* **1**, 33 (2017).

ACKNOWLEDGEMENTS

V.Z. and M.C. acknowledge support from the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2020-118178RB-C21, Cisco Systems Inc., and MICINN —with funding from the European Union NextGenerationEU (PRTR-C17.I1)— and the Galician Regional Government—with own funding—through the “Planes Complementarios de I+D+I con las Comunidades Autonomous” in Quantum Communication. R.A.F. was generously supported by the Peter and Patricia Gruber Award, the Daniel E. Koshland Career Development Chair and by the Israel Science Foundation (ISF), and the Directorate for Defense Research and Development (DDR&D), grant No. 3426/21. T.vL. and H.W. acknowledge funding by the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung (BMBF)) within the project QR.X (Contract No. 16KISQ002) and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy - EXC-2111 - 390814868. W.Z.L. and Q.Z. acknowledge support from the National Natural Science Foundation of China (No. T2125010) and the Shanghai Municipal Science and Technology Major Project (No. 2019SHZDZX01).

AUTHOR CONTRIBUTIONS

All authors discussed the work together and decided the structure and contents of the paper. V.Z., T.vL., R.A.F., and W.Z.L. wrote the manuscript, with feedback from the rest. All authors critically read it and revised it. M.C. supervised the project.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Marcos Curty.

Reprints and permission information is available at http://www.nature.com/reprints

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