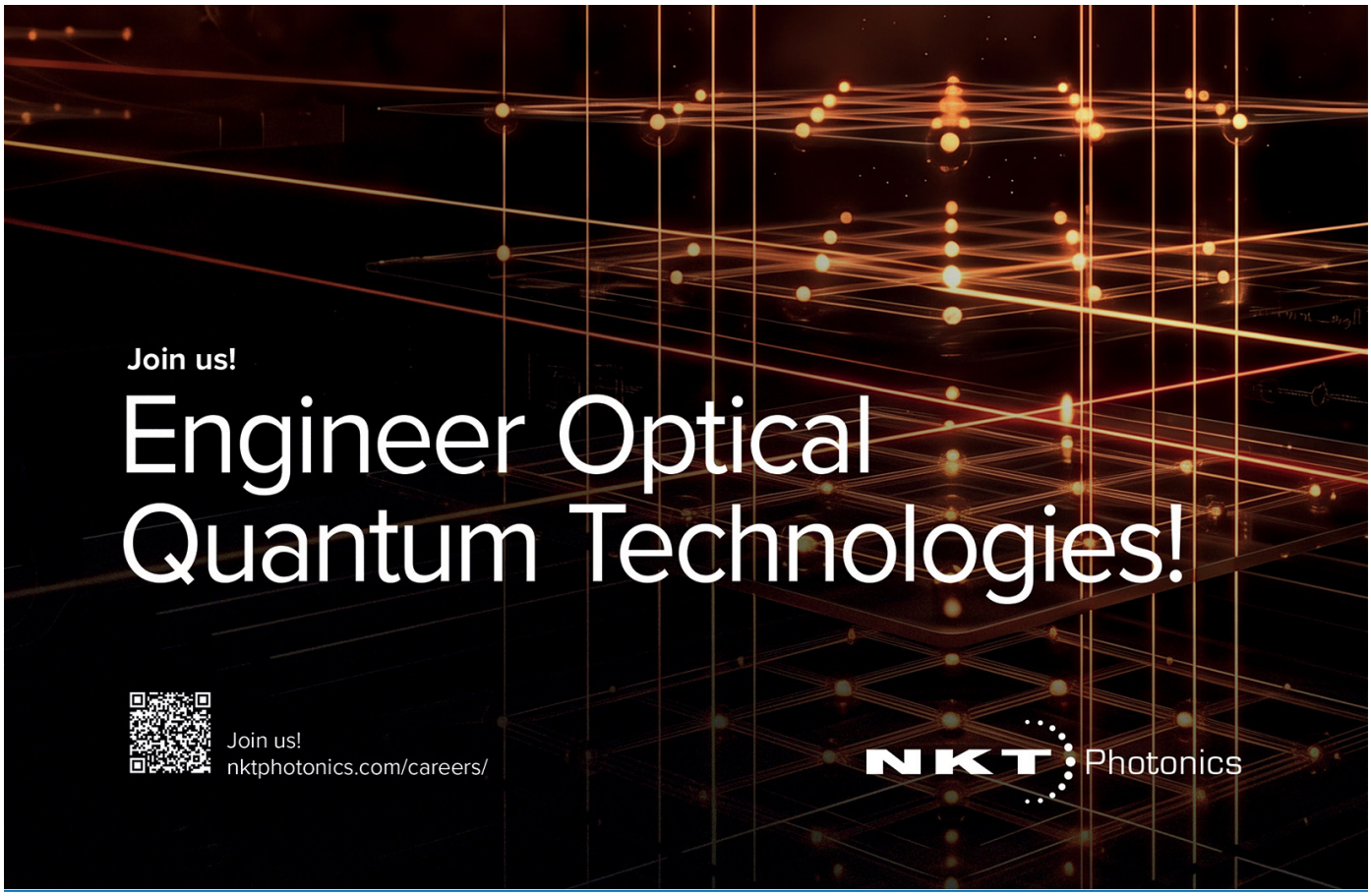
Quantum Science and Technology

PAPER • **OPEN ACCESS**

Quantum key distribution using hBN single-photon emitters at a 40 MHz clock rate

To cite this article: Ömer S Tapşın *et al* 2026 *Quantum Sci. Technol.* **11** 025058



Quantum Science and Technology

OPEN ACCESS

RECEIVED
29 December 2025

REVISED
10 April 2026

ACCEPTED FOR PUBLICATION
1 May 2026

PUBLISHED
27 May 2026

PAPER

Quantum key distribution using hBN single-photon emitters at a 40 MHz clock rate

Ömer S Tapşın[1,2,7,8], Furkan Ağlarcı[1,2,8], Roberto G Pousa[4,5], Daniel K L Oi[5], Mustafa Gündoğan[6] and Serkan Ateş[1,3,*]

[1] QLocked Technology Development Inc., İzmir 35430, Türkiye
[2] Department of Physics, İzmir Institute of Technology, İzmir 35430, Türkiye
[3] Faculty of Engineering and Natural Sciences, Sabanci University, İstanbul 34956, Türkiye
[4] ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
[5] SUPA Department of Physics, University of Strathclyde, Glasgow, G4 0NG, United Kingdom
[6] Institut für Physik, Humboldt-Universität zu Berlin, Berlin 12489, Germany
[7] Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[8] The authors contributed equally to this work.
[*] Author to whom any correspondence should be addressed.

E-mail: serkan.ates@sabanciuniv.edu

Keywords: solid-state emitters, 2D materials, hexagonal boron nitride, single photon sources, quantum key distribution

Abstract

Room-temperature (RT) solid-state quantum emitters are essential for building practical and scalable quantum communication systems, yet their application has been critically hindered by the slow operational speeds of corresponding modulation technologies. In this work, we overcome this key performance bottleneck. We demonstrate a quantum key distribution (QKD) system using a single defect in hexagonal boron nitride (hBN) with dynamic polarization encoding at a 40 MHz clock rate, an order of magnitude faster than previous demonstrations with similar sources. Implementing the B92 protocol, our system yields a secure key rate of 7 kbps in the finite-key regime with a quantum bit error rate of 6.49%, establishing a new performance benchmark for RT single-photon QKD. Furthermore, to chart a path beyond the limits of direct transmission, we present the first quantitative performance analysis of hBN spin-defects as quantum repeater nodes. Overall, our high-speed experimental demonstration, supported by a foundational analysis of the system architecture, suggests that hBN defects represent a promising and technically feasible platform for scalable, quantum communication.

1. Introduction

Among various quantum technologies, quantum key distribution (QKD) stands out as one of the most mature and well-established applications, laying the foundation for future quantum networks and distributed quantum computing [1–3]. By leveraging fundamental quantum principles such as the no-cloning theorem, nonlocality, and the uncertainty principle, QKD enables secure shared random key generation between remote parties. QKD protocols are typically categorized into prepare-and-measure (PM) schemes [4–7] and entanglement-based schemes [8, 9]. In PM QKD, weak coherent pulses are commonly used to generate flying qubits as quantum information carriers. However, their multi-photon emissions are exploitable by an eavesdropper through photon number splitting (PNS) attacks, which compromise the security of the protocol in lossy channels. This vulnerability, coupled with the limited source brightness, further constrains the achievable key generation rate. Decoy-state methods address these challenges by mitigating the risks of multi-photon emissions, albeit at the cost of increased protocol complexity [10–12]. Alternatively, deterministic single-photon generation by quantum emitters provides an on-demand solution for practical quantum communication, allowing extended transmission distances with enhanced security [13, 14]. Implementing decoy-state QKD using imperfect single

photon sources for enhanced secure key rate (SKR) at longer distances have also been reported [15] and demonstrated [16].

Semiconductor quantum dots (QDs), as one of the most studied quantum emitters, have demonstrated significant potential for PM QKD due to their high purity and brightness [17–19], as well as for entanglement-based QKD through cascaded exciton-biexciton emission [20–23]. Tremendous efforts have been made to enhance these key properties of QDs [24, 25]. However, the implementation of QD sources in QKD requires significant growth infrastructure and cryogenic environments, which introduces considerable complexities [26]. In contrast, quantum emitters that operate efficiently at room temperature have garnered considerable attention. For example, fiber-based QKD has been demonstrated using single photons generated in the telecom O-band from defects in GaN [27]. Similarly, defects in diamond emitting in the visible band have been employed for free-space QKD [28–30]. In addition to these materials, defects in hexagonal boron nitride (hBN) are attracting increasing attention due to their efficient single-photon generation at room temperature [31], their 2D nature, and their ease of integration with quantum photonic and plasmonic structures [32, 33]. Thanks to its wide bandgap, hBN hosts several optically active defects that emit over a broad spectral range, from the visible (VIS) to near-infrared (NIR) [34], enabling a diverse range of applications in quantum technologies [35]. The potential of hBN defects has been demonstrated as single-photon sources (SPS) in QKD implementations, successfully employing the B92 [36] and BB84 [37] protocols in free-space, and leading to their inclusion in an upcoming space-based mission [38]. Furthermore, the recently discovered electronic spin [39, 40] associated with the optical transition opens up the potential for developing spin-photon interfaces that could serve as quantum registers for quantum networking.

All QKD demonstrations mentioned above rely on the active polarization encoding of single photons using electro-optic modulators (EOMs). Practical QKD would benefit from a bright, room-temperature (RT) SPS and a high-speed polarization modulator. Fiber-based QKD with defects in GaN leverages commercially available high-speed electro-optic phase modulators operating at telecom wavelengths [27]. In contrast, free-space QKD demonstrations with defects in diamond and hBN are constrained by free-space EOMs operating in the visible spectrum. These modulators are limited to practical speeds of 1 MHz due to their high voltage requirements for polarization modulation [30, 36, 37], although the emitters can support much higher speeds thanks to their short lifetime.

Here, we present, to the best of our knowledge, the fastest dynamically modulated QKD system based on the B92 protocol [5], utilizing polarization-encoded single photons emitted from a single defect in hBN at a 40 MHz clock rate. Additionally, temporal filtering based on the emitter's decay time is employed to optimize the quantum bit error rate (QBER) and the sifted key rate (SiKR) [41], alongside performing both asymptotic [42, 43] and finite-key analysis [44, 45]. We will conclude the paper with an analysis of the performance requirements for a potential spin-photon interface based on hBN to function as a quantum repeater node capable of surpassing the direct transmission limit.

2. Optical characterization of the single photon source

Figure 1 shows the detailed experimental setup used for the optical excitation of defects, the analysis of the emission spectrum, the verification of the single-photon nature of the emission, and the execution of the QKD protocol. The sample is excited with a 483 nm pulsed laser using a high numerical aperture objective (NA $= 0.9$), which is also used for the efficient collection of emission. Additionally, a Hanbury-Brown and Twiss interferometer equipped with two single-photon detectors with low dark counts (40 Hz) is employed to perform photon correlation experiments on the spectrally filtered emission from the defect. For the QKD demonstration, the filtered single-photon emission is guided to the polarization encoding part via a polarization-maintaining fiber (PMF). The details of the QKD scheme and setup are described below.

Multilayer hBN flakes (obtained from Graphene Supermarket) dropcasted on a SiO_2/Si substrate are used as the material system. While the drop casting method inherently results in a spatially random distribution of flakes, a single prepared substrate typically yields several high-quality single-photon emitters exhibiting robust spectral stability at room temperature without the need for subsequent thermal annealing, allowing for reliable operation during the protocol execution. Among approximately ten characterized defect centers on the substrate, the specific emitter presented in this work was selected for its optimal brightness, short excited-state lifetime, and superior photo-stability. This selection was necessary to ensure reliable QKD operation, particularly in light of the well-documented photobleaching and blinking behaviors often observed in red/yellow-emitting hBN defects [46].

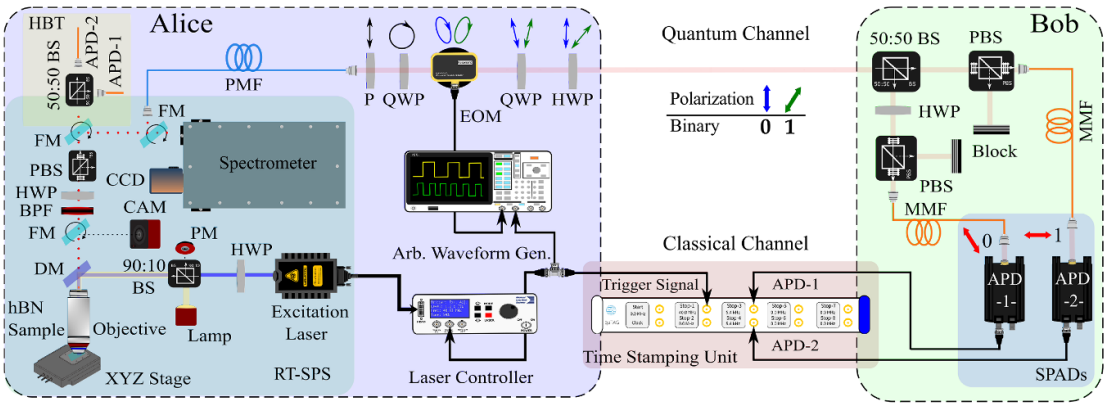


Figure 1. Schematic diagram of the experimental configuration employed for the optical investigation of defects in hBN and the implementation of B92 QKD protocol. The Alice module on the left integrates the RT-SPS box, which includes a μ-PL setup used for excitation of defects and collection of emission for spectral analysis. It also includes HBT box, which illustrates the Hanbury-Brown and Twiss interferometer to demonstrate the single photon nature of the collected emission. Alice implements a resonant electro-optic modulator (EOM) for the polarization encoding of individual photons, while the Bob module on the right randomly measures the photons having non-orthogonal polarization states prepared by Alice.

Photoluminescence (PL) spectrum of the defect investigated in this work is shown in figure 2(a). The sharp peak at 626 nm is identified as the zero-phonon line (ZPL), while the weaker and broader signals around 680 nm correspond to the optical phonon sidebands (PSB). The energy difference between ZPL and PSB matches very well with the energy of the high-energy Raman-active and infrared optical phonon modes of hBN [47]. The inset of figure 2(a) shows the linear polarization behavior of the ZPL emission [48]. Time-resolved PL spectroscopy is employed on the ZPL emission to determine its decay time. Figure 2(b) shows the result of the experiment with a lifetime of 4.58 ns obtained from a single-exponential decay model. Finally, to demonstrate the single-photon nature of the collected emission, a photon correlation experiment is performed on the spectrally filtered ZPL emission under a 40 MHz excitation rate at saturation, which also represents the experimental conditions for the QKD demonstration, as discussed later. The inset of figure 2(b) shows the histogram of correlations with an antibunching value of $g^2(0) = 0.24 \pm 0.06$ at zero delay, normalized to the correlations at long time delays. The deviation from the ideal value of $g^{(2)}(0) = 0$ is mainly attributed to the imperfect spectral filtering of the emission using a bandpass filter with a 10 nm FWHM around the ZPL wavelength. The purity of the emission can further be enhanced via post-growth processes, such as thermal annealing [49] that also narrows the spectral width. The emission dynamics and photon statistics of the hBN defect are characterized using the standard three-level rate equation framework [50, 51]. Within this model, the saturation counts and the anti-bunching depth in the $g^{(2)}(\tau)$ measurement are directly related to the radiative decay and shelving rates of the defect's internal energy levels, providing a quantitative link between the emitter's physics and the system's modulation limits. The bunching near zero delay in the $g^{(2)}(\tau)$ originates from a metastable shelving state in the defect's three-level structure, causing photon correlations on microsecond timescales, which does not contribute to the purity of the single photon emission of the source. Our $g^{(2)}(0)$ is normalized using long-delay values where bunching has decayed (in ms time scale), ensuring an accurate purity measurement [52].

3. Free-space QKD

Despite its drawbacks compared to BB84—namely lower loss and error tolerances and greater vulnerability to certain attacks—we use the B92 protocol for practical, experimental reasons, primarily to showcase the versatility of hBN emitters at room temperature. In the B92 (or two-state) protocol, QKD is implemented between Alice (transmitter) and Bob (receiver). As shown in figure 1, spectrally filtered single photons are sent via a PMF, and Alice actively encodes the polarization states $|V\rangle, |D\rangle$, corresponding to the linear and diagonal bases $\mathbb{X}, \mathbb{Z}$ which map to bits $\{0, 1\}$. The use of non-orthogonal polarization states reflects a fundamental feature of quantum mechanics, namely the impossibility of perfectly distinguishing non-orthogonal states. This originates from the non-commutativity of quantum measurements, giving rise to measurement induced disturbance and forming the basis for the security of the protocol. Beyond its implementation in this PM protocol, the high-speed active modulation demonstrated here

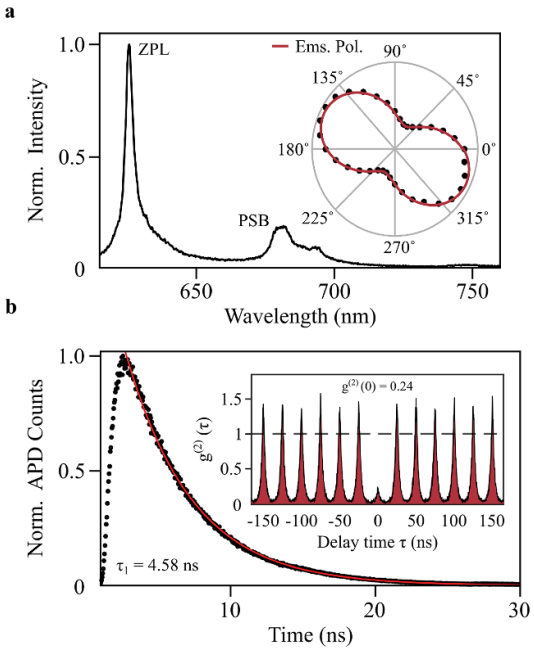


Figure 2. Optical characterization of investigated defect (a) PL spectrum of the defect showing a ZPL emission at 626 nm and phonon sidebands near 680 nm. Inset: linear polarization of ZPL emission. (b) Time-resolved ZPL emission from the defect, where a single-exponential decay model yields a decay time of 4.58 ns. Inset: second-order correlation measurement under pulsed excitation at 40 MHz, with an antibunching value of $g^2(0) = 0.24 \pm 0.06$, normalized to the correlations at long delays.

also represents an enabling technology for foundational experiments requiring rapid basis selection to satisfy locality constraints, such as in loophole-free Bell inequality tests.

The protocol is implemented in the following manner. Alice generates 20 MHz and 40 MHz signals that are synchronized with the FPGA clock of the arbitrary waveform generator. The 40 MHz signal is used to trigger the single-photon generation, while the 20 MHz control signal is used to drive the resonant EOM for dynamic polarization manipulation of the single-photons. It is important to note that this high-speed operation is a result of a complete system optimization. While the resonant EOM enables the fast polarization switching, such a high clock rate is only feasible due to the intrinsically short excited-state lifetime (4.58 ns) of the pre-selected hBN defect, which minimizes emission overlap between subsequent excitation pulses. The successful demonstration further relied on the precise electronic synchronization of the laser, modulator, and detection modules. The EOM is driven by 7 V_{pp}, such that polarization encoding is achieved by overlapping the control (20 MHz) and trigger (40 MHz) signals in a structured pattern, alternating between high and low voltage states, represented as a "1–0–1–0..." sequence. While the present demonstration utilizes a deterministic alternating sequence to validate the 40 MHz physical modulation limit of the hBN single photon source, a fully secure quantum network requires true randomness. Upgrading the drive electronics to incorporate an arbitrary waveform generator driven by a high-speed quantum random number generator represents the immediate next step to deploy this RT architecture in secure, real-world cryptographic links. In addition, passive-polarization components are employed by Alice for state preparation. Before the EOM, a linear polarizer (P) and a quarter-wave plate (QWP) are used to first select the vertical polarization state and convert it to circular polarization, which is then modulated by the EOM, resulting in elliptically polarized light. A second QWP is used after the EOM to linearize the polarization state to –22.5 ° and 22.5 °. A half-wave plate (HWP) is then used to rotate the reference frame to acquire non-orthogonal states, corresponding to vertical and diagonal (45 °) polarization, providing ±3.5 V. Subsequently, the prepared states are transmitted to Bob over the free-space quantum channel, where a 50:50 beam splitter (BS) is first used for the random selection of the measurement basis. The polarizing BS (PBS) in the transmission path represents the linear basis ($\mathbb{X}$), while the reflection path, along with the HWP and PBS, represents the diagonal ($\mathbb{Z}$) basis, corresponding to bits 1, 0, respectively. Photon detection is carried out by fiber-coupled single-photon detectors, which are also used for the measurement of second-order photon correlation function, as described above.

The QKD experiment was performed with spectrally filtered ZPL emission. The brightness of the emitter was characterized based on a measured total count rate of 851 kHz using a single avalanche

photodiode (APD) at the output port of the HBT setup. Taking into account all losses in the μPL setup and a 70% detector efficiency (Excelitas AQRH-16), a count rate of 2.085 MHz was obtained after the microscope objective, indicating an overall collection efficiency of 5.2% under 40 MHz excitation rate and a unit quantum efficiency (QE) of the source conditions as a lower bound. While a direct measurement of the QE is exceptionally challenging without precise knowledge of the local electromagnetic environment, recent studies on similar hBN defects report QE values ranging from 50% to over 87% [53, 54], which can lead to a higher collection efficiency and therefore a higher mean photon number for the QKD. From a total count rate of 2.085 MHz measured after the objective, we couple the emission into a PMF that leads to the QKD module. The fiber-coupled single-photon brightness at the input of the QKD system was measured to be 821 kHz at saturation. The degree of linear polarization for this emission was 70% (figure 2(a), inset). Therefore, the effective brightness of usable, correctly polarized photons for the QKD experiment is 575 kHz. A critical parameter for QKD is the mean photon number, μ, before the quantum channel. Considering the efficiency of the μPL setup, the PM fiber coupling, and the losses in the polarization encoding part of Alice's system, the efficiency of the transmitter, η_{tran}, was calculated to be 0.252, yielding a mean photon number, μ, of 0.0131. A short PMF before the quantum channel is used only for mode matching into the modulator, guiding the single-photon emission between different parts of the setup, and enabling stable calibration. In future free-space setups, direct coupling could remove this stage, reducing loss and increasing the key rate, as discussed in detail later. On Bob's side, the system, consisting of basic optics and two single-photon detectors, resulted in a receiver efficiency, η_{rec}, of 0.42. This includes detector efficiency, transmission of the optics, and coupling into the multimode fibers used before APDs. The efficiency of the QKD setup, from the microscope objective to the APDs in the receiver, was estimated by measuring each component individually with an attenuated laser at 637 nm, which closely matches the ZPL wavelength of the single-photon emission.

To obtain the QKD parameters, the SiKR and the QBER, the trigger signal at 40 MHz is recorded alongside the APD detections at Bob. This enables sifting and QBER calculations to be performed over the classical channel. Time tags corresponding to QKD events are selected based on the recorded trigger signal, and double-detection events as well as empty pulses are discarded during sifted key generation at Bob. Additionally, a periodic bit sequence of '1–0–1–0...' is generated in correspondence with the trigger signal, representing the original bit sequence sent from Alice to Bob. The clicks from APD-1 and APD-2, which are used for the bit sequences of 1's and 0's measured by Bob, are then compared to Alice's bit sequence to extract the QBER. To specifically benchmark the maximum performance of the physical hardware, a periodic polarization sequence was used. This approach is consistent with other initial demonstrations of novel QKD emitters [27, 36, 55] where the primary goal is to establish the physical layer's capabilities. Our use of a resonant EOM, while highly efficient for the fixed-frequency operation, restricts the ability to apply the arbitrary waveforms of a true random sequence. We note that a full implementation for generating a usable cryptographic key would require significant future engineering to integrate a high-speed random number generator with the resonant modulator, representing an important next step for this technology.

Figure 3(a) shows the normalized histogram of APD detection events at Bob, together with the decay curve of the emission obtained from the time-resolved PL measurement. As observed, while the single-photon emission is stronger in the early part of the detection window, the weaker signal at later times leads to a reduced signal-to-noise ratio. As discussed earlier, linearly polarized single-photon emission is used as the source for the QKD process. However, the degree of linear polarization strongly depends on the decay time of individual single photon generation [48, 56], which consequently affects the generated bit rate and the QBER. Additionally, the dark counts distributed across the detection window play a significant role in determining the QBER. To optimize the key rate and QBER in relation to the emitter's decay time, a temporal filtering process is applied [41]. The unshaded region shown in figure 3(a) represents the window used for temporal filtering, characterized by a start time t_0 with respect to the synchronized trigger signal and a width Δt. By varying Δt between 3 and 12 ns for each t_0 from 0 to 4 ns (in 100 ps steps), the SiKR and QBER are calculated from the measured raw key, as shown in figure 3(b). The high-speed operation of the QKD system enables the generation of a SiKR up to 17.5 kbps. Noting that the efficiency of the B92 protocol is half that of BB84, the observed SiKR is, to the best of our knowledge, the highest achieved from a room temperature SPS with active polarization encoding [27, 28, 30, 36, 37]. In addition to SiKR, the effect of temporal filtering on QBER is demonstrated in figure 3(c).

Finite key analysis for the B92-protocol [44] is performed for SKR calculations, as described in the appendix B, considering the same temporal filtering parameters used for SiKR and QBER calculations from raw data. For this purpose, leak estimation is carried out following the one-way error reconciliation method [57] such that the secure key length l is bounded by,

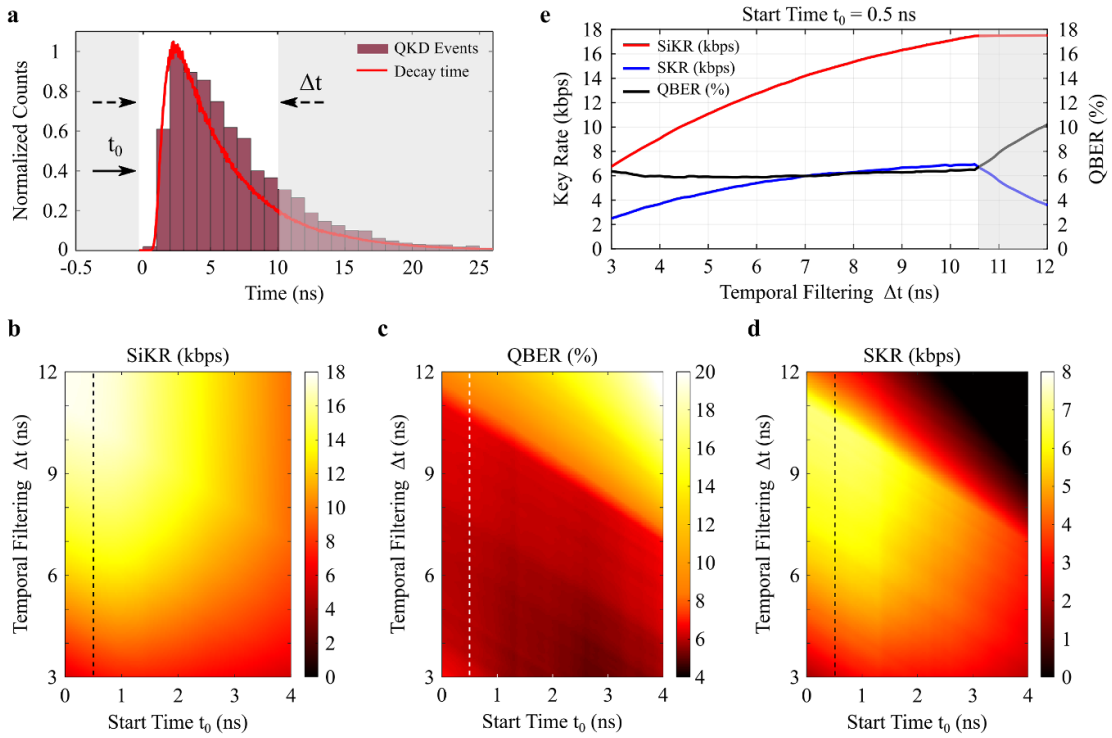


Figure 3. Results of QKD experiment with the B92 protocol. (a) Normalized histogram of APD detection events on Bob module. The red solid line on the histogram is the decay curve of the ZPL emission. The unshaded region shows the start (t_0) and the width (Δt) of temporal filtering. (b) A two-dimensional representation of the sifted key rate, (c) quantum bit error rate, and (d) secure key rate as a function temporal filtering parameters t_0 and Δt extracted from the measured QKD data. Vertical dashed lines on each map indicate the optimal temporal filtering parameters for maximizing SKR. (e) SiKR, QBER, and SKR results for the indicated dashed lines. We follow the method presented in [44] for these calculations as explained in the text.

$$l \leqslant N_R\left[1 - H_{\min}\left(X_A|E\right)\right] - L_{EC} - 2\log_2\left(\frac{1}{2\epsilon_{PA}}\right) - \log_2\left(\frac{2}{\epsilon_{cor}}\right). \tag{1}$$

Here, N_R is the number of total measured events per second, $H_{\min}$ is the minimum entropy, L_{EC} is the leak bits during error reconciliation, ϵ_{PA} is the privacy amplification failure probability and ϵ_{cor} is the correctness failure probability. Figure 3(d) shows the 2D map of the calculated SKR for the temporal filtering parameters given above using equation (1). The dashed lines on the plots highlight the optimal temporal filtering parameters, determined to be $(t_0, \Delta t) = (0.5\,\text{ns}, 3\text{–}10.5\,\text{ns})$ for achieving the best SiKR, QBER and SKR values. As shown in figure 3(e), a QBER of 6.49% is achieved for the highest SiKR of 17.5 kbps and SKR of 7 kbps under the given temporal filtering conditions. This represents one of the highest reported SKR obtained from a QKD system with active modulation of polarization states from a RT SPS. The abrupt changes in the behavior of SiKR, QBER, and SKR at 10.5 ns, observed in figure 3(e) (shaded region), are attributed to the pulse shape of the 40 MHz trigger signal, which has a roughly 10 ns flat region after the rising and falling edges. In this context, temporal filtering helps select the optimal portion of the data for the calculation of QKD parameters within the flat region of the trigger signal, in addition to the conventional purpose of signal-to-noise improvement, as previously reported [36, 41]. Therefore, to fully exploit the performance of a SPS with a slow decay time, the shape of the pulse driving the EOM must be optimized such that the flat region of the pulse is wider than the decay time. Achieving this condition is not trivial under high-speed modulation conditions.

Here, we should note that the unconditional security of the B92 protocol relies on perfect positive-operator-valued measurements, but practical systems, such as this experiment, only use two projective measurements. This limitation weakens security, allowing Eve to exploit imperfections through unambiguous state discrimination (USD) measurements [58]. Although some countermeasure strategies against USD attacks for the B92 protocol exist in the literature [59], the security of our B92 implementation is established using a composable finite-key framework based on entropic uncertainty relations. While B92 is known to be susceptible to USD attacks in lossy channels, our analysis provides security against the most general class of attacks. In this framework, any potential information leakage, including that stemming from USD measurements, is fundamentally bounded by the smooth min-entropy. Consequently, the privacy amplification process yields a secure key by assuming a worst-case

scenario for an eavesdropper's information gain, ensuring the protocol remains robust under our specific experimental parameters. On the other hand, unlike B92, the BB84 protocol, with its larger state set, is more resilient to such attacks and offers well-established frameworks for lossy channels [60]. Therefore, to assess the platform's capabilities beyond B92, we evaluate its performance under hypothetical BB84 conditions, which offer improved security and advantages as explained above. In order to do so, we benchmark our RT source using asymptotic [42, 43] and finite key frameworks [45, 61] for the BB84 protocol, with the experimental parameters given in the appendix B, against channel loss. The solid green line in figure 4 shows the result of the asymptotic key rate analysis with a maximum tolerable loss of 24 dB. The dashed green lines represent the SKR obtained with the finite key analysis based on multiplicative Chernoff bounds, by estimating lower bounds of the sent non-multiphoton events ($\underline{N}^{X,Z}_{S,nmp}$) and upper bound of the phase error rate ($\bar{\phi}^{X}$). Here, tighter bound estimations offer a considerably larger key rate for a fixed block size, together with optimized basis bias (P_x) and pre-attenuation. Regarding to this calculation, a block size of sent $N_{S,BB84} = 4 \cdot 10^9$ signal/pulse, corresponding to $t_S = 10^2$ seconds of acquisition time, is used to reach the tolerable loss of 23 dB. Meanwhile, $t_S = 1$ s of acquisition still yields positive key rates at around 17 dB of channel loss, benchmarking the performance of our RT emitter in its simplest form.

4. Discussion

Channel loss is primarily limited by suboptimal single-photon purity, limited collection efficiency of the source, and losses in the experimental setup, all of which can be improved using reported values for defects in hBN. Indeed, the performance projections for our improved source shown in figure 4 are based on established techniques, such as coupling to a tunable open microcavity, that have been proven effective at room temperature. For example, the work by Vogl *et al* [62] provides a clear precedent, demonstrating that the integration of such a cavity offers a multi-faceted path to improving system performance. The Purcell enhancement reported in that work shortens the emitter's lifetime, directly enabling higher clock rates and increasing the SKR. Simultaneously, the cavity improves single-photon purity (lower $g^{(2)}(0)$) and enhances collection efficiency, which both increase the SKR per pulse and overall security via a reduced QBER. Finally, the resulting spectral narrowing can lead to a lower QBER by allowing for more precise polarization control. It is important to note that for this polarization-encoding application, the modulation speed is primarily limited by the emitter's lifetime, not its spectral linewidth. However, for future applications, like quantum repeaters that do require indistinguishable photons, managing spectral diffusion at any temperature remains a key challenge, as we discuss in the following section. By incorporating such a RT-compatible cavity and removing the polarization maintaning fiber in the experimental setup, the mean photon number of our source could be enhanced to $\mu = 0.264$, enabling the significantly improved key rates shown by the blue curves in figure 4. With these improvements, our hBN-based platform has the potential to reach SKRs in the Mbps regime, allowing our RT system to approach the performance of well-established cryogenic QD sources [19] (black lines).

To translate the channel loss shown in figure 4 into practical transmission distances, the specific communication channel must be considered. For satellite-ground free-space links, attenuation is mainly dominated by geometric beam divergence and has contributions from atmospheric absorption. The average channel loss can therefore exceed 35 dB during a single fly over. For terrestrial communication through standard single-mode fiber, the loss is strongly wavelength-dependent; at the wavelength of our source emission at 626 nm, attenuation in specialty fiber is approximately 12 dB km^{-1}, limiting direct transmission to very short, intra-city distances. A proven path to long-haul fiber communication would involve high-efficiency quantum frequency conversion to translate the visible photons to the ultra-low-loss telecom C-band (0.2 dB km^{-1}). This highlights that for a fair comparison of different source technologies, channel loss (dB) is the most fundamental metric.

We acknowledge the QBER of 6.49% observed in our implementation. A significant contributing factor is the imperfect polarization purity of the single photons emitted by the hBN defect, which can include non-linear components arising from dipole orientation misalignment or local strain. These imperfections lead to increased projection errors when measured in linear polarization bases, a known challenge for hBN emitters that has been explored via, for example, time-resolved Stokes analysis [48, 56]. To confirm the origin of our error, we performed a control measurement using attenuated laser pulses with a high degree of linear polarization in the same setup. This control experiment yielded a significantly lower QBER of 1.35%, confirming that the higher QBER in our QKD experiment is primarily dominated by the intrinsic polarization characteristics of the emitter, not the transmission or detection

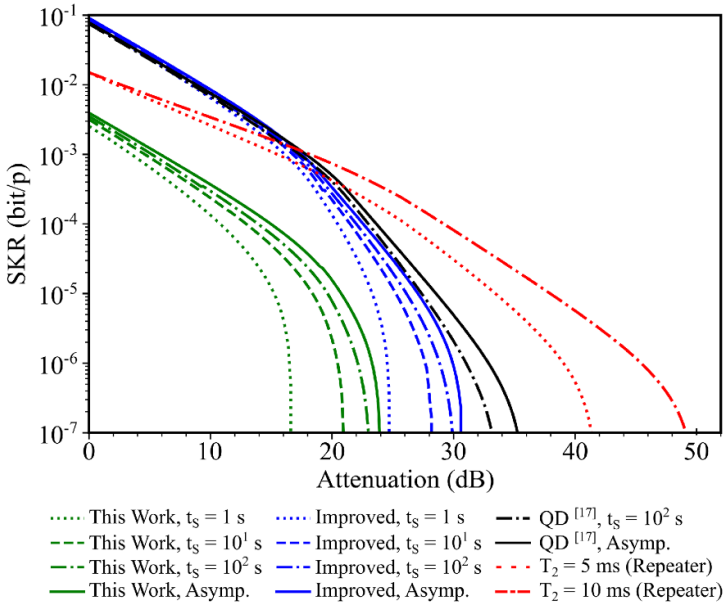


Figure 4. Comparative analysis of secure key rates (SKR) relative to channel loss for point-to-point QKD and a prospective quantum repeater scheme. For the demonstrated room-temperature point-to-point scenario, the SKR is calculated using the non-decoy BB84 protocol with optimized parameters for our emitter (green), a cavity-coupled improved version (blue), and a reference cryogenic quantum dot (QD) [19] (black). In a separate prospective scenario representing a future hBN-based quantum network, we present a theoretical roadmap for a cryogenic repeater node utilizing two quantum memories with coherence times (T_2) of 5 ms (dotted red) and 10 ms (dash-dot red) with optimized node positioning [63]. The analysis accounts for finite-key effects with acquisition times (t_S) of 1 s (dotted), 10 s (dashed), or 100 s (dot–dash), as well as the asymptotic limit (solid lines). Note that differing excitation rates between emitters result in different block sizes for a given t_S (see appendix A).

system. Future improvements in the QBER will therefore rely on pre-selecting emitters with even higher intrinsic polarization purity or the development of active polarization correction techniques.

Table 1 summarizes several PM QKD demonstrations using SPSs and their corresponding parameters. The sources are categorized based on their operating conditions, specifically RT (hBN, diamond, GaN, and single molecules) and cryogenic operation (QDs and TMDCs). Additionally, the implementations are categorized based on whether they include active or passive encoding. We highlight that a direct comparison of these reported QKD parameters is non-trivial, as they are obtained under varying experimental conditions, security frameworks, and operating wavelengths. Specifically, the high channel attenuation inherent to the visible spectrum (12 dB km^{-1}) contrasts sharply with telecom-band fiber losses (0.2 dB km^{-1}), fundamentally dictating the achievable distance and rate for each platform. Consequently, the relevant experimental conditions and losses are provided in the table footnotes for transparency. As observed, RT sources offer a practical implementation with modest SKR, while QD-based sources provide superior performance and telecom-band compatibility, despite the added complexity of cryogenic requirements.

In order to go beyond point-to-point QKD applications and towards entanglement-based quantum networking, electronic or nuclear spins of such single emitters can be utilized to act as quantum memories and registers [67–69]. Recent experimental work has shown that emitters in hBN and other 2D materials possess electronic spins [39, 40, 70, 71], albeit with coherence times (T_2) currently limited to the microsecond range at room temperature. As indicated by our analysis in figure 5, building a repeater network over long distances requires extending these times into the millisecond regime. Encouragingly, first-principles calculations predict that some of these defects could exhibit T_2 times of around 30 ms [72, 73], indicating that these spins may indeed become the foundation of quantum registers. Alongside the spin coherence requirements, the performance of a quantum repeater node relies critically on the indistinguishability of successively emitted photons. Achieving the near-unity indistinguishability required for high-fidelity entanglement swapping is severely hampered at room temperature by phonon-induced dephasing and spectral diffusion from local charge fluctuations. Consequently, realizing such entanglement-based networks will necessitate operating these emitters in a cryogenic environment to suppress these mechanisms and enable Fourier-transform-limited emission. Recent breakthroughs have demonstrated resonance fluorescence and two-photon interference with a visibility of 0.92 from boron-vacancy centers in hBN at cryogenic temperatures [74], representing a significant step toward the high-speed photonic interfaces required for repeater applications.

Table 1. Summary of QKD experiments with various SPS sources.

Single-photon Source, λ_0 (nm)	Clock rate (MHz)	Active Encoding	Room Temp.	QBER (%)	Bit-rate (kbps)
This work[a], 626	40	✓	✓	6.49	7 (SKR)
GaN, 1310 [27]	80	✓	✓	5	0.247 (SKR)[b]
hBN, 671[a] [36]	1	✓	✓	8.95	0.24 (SiKR)
hBN, 650 [37]	0.5	✓	✓	6	0.026 (SKR)
Mol., 785 [64]	80	NO	✓	3.4	500 (AKR)
NV, 637 [30]	1	✓	✓	3	2.6 (SKR)
SiV, 739 [30]	1	✓	✓	3.2	1 (SKR)
QD, 880 [17]	76	✓	NO	2.5	25 (SKR)
QD, 898 [55]	200	✓	NO	3.8	35 (SiKR)
QD, 1545 [18]	72.6	✓	NO	3.25	13.2 (SKR)[c]
QD, 884.5 [19]	76.13	✓	NO	2.54	82 (SKR)[d]
QD, 1550 [61]	160.7	NO	NO	2	689 (AKR)
QD, 1556 [65]	228	NO	NO	0.099	68 (AKR)[e]
TMDC, 807 [66]	5	NO	NO	0.69	NaN

Note: SiKR stands for sifted key rate, AKR for asymptotic key rate, and SKR for secure key rate.

[a] based on B92-protocol.

[b] for 4.0 dB loss.

[c] for 9.6 dB loss.

[d] for 15.2 dB loss.

[e] for fiber spool distance of 80 km.

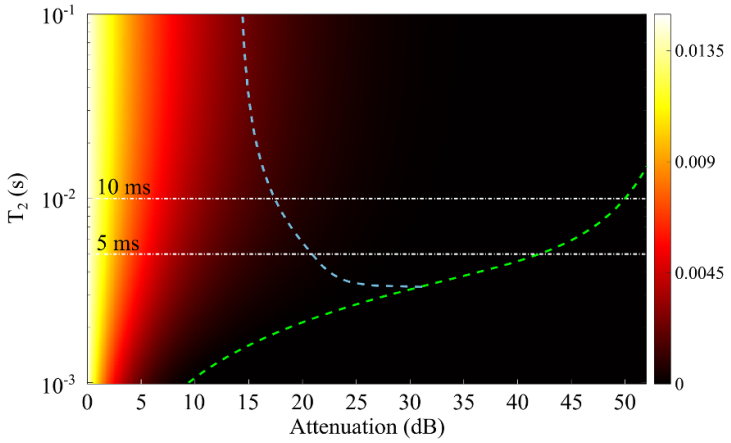


Figure 5. Theoretical roadmap for hBN-based quantum communication: Attainable SKR in a single-node quantum repeater configuration. This analysis establishes the performance thresholds required for a future cryogenic hBN node. The horizontal dotted lines correspond to the 5 ms and 10 ms memory time scenarios (T_2) used in the prospective analysis in figure 4. The blue dashed line indicates the point beyond which the repeater configuration starts having an advantage over the performance of the reference cryogenic QD in [19], whereas the green dashed line shows the limit beyond which the repeater configuration cannot produce a positive key rate. These projections assume a cryogenic operational environment to access the necessary spin coherence and suppressed phonon-induced decoherence required for entanglement swapping.

While the experimental demonstration in this work focuses on a room-temperature architecture for practical QKD, the potential for hBN defects to serve as nodes in a quantum repeater network demands this transition to cryogenic operation. To evaluate the performance required for such advanced networking applications, we use a single quantum repeater node [75] as a benchmark. This scheme [63] requires at least two identical quantum registers for entangled state distribution and synchronization. Such a node reduces the effective distance between the communicating parties by half, thereby providing superior performance beyond certain distances. This is illustrated with the red lines in figure 4, where we plotted the SKR in the asymptotic limit for two different memory times, 5 ms and 10 ms. The reduced slope of the curves up to around 25 dB loss with respect to point-to-point QKD schemes is indicative of the quantum repeater behaviour, which provides better performance over a certain crossover point and better overall loss tolerance. Although we assume the repeater node is placed halfway

between Alice and Bob in the low-loss regime, once dephasing becomes significant in the high-loss regime, the optimized position of the repeater node is found to be closer to Bob and at some point becomes fixed. This position optimization helps minimize dephasing errors by providing Alice's quantum memory less time to experience dephasing. As a result, beyond ~ 25 dB, the optimized key rate scaling behavior changes from $e^{-L/(2L_{\text{att}})}$ to $e^{-L/L_{\text{att}}}$ i.e. direct transition between Alice and Bob [63]. Figure 5 shows the SKR as a function of channel loss and memory time. This analysis quantitatively shows that a memory time in the order of $\mathcal{O}(10^{-3})$ s would be sufficient for practical applications. The details of the model and the parameters used for these calculations are given in Appendix B.

Building upon these physical requirements, we establish a hardware-agnostic roadmap to define the performance thresholds necessary for a functional hBN-based quantum node. We identify a spin coherence time in the millisecond regime and a single-shot readout fidelity exceeding 90% as the critical benchmarks for viable networking. While RT spin coherence has been demonstrated in hBN, reaching the millisecond thresholds analyzed in figure 5 will likely depend on identifying defect centers with greater resilience to environmental noise or employing advanced dynamical decoupling sequences. Furthermore, for our system modeling, we adopt a conservative Bell state measurement efficiency of $\eta_{\text{BSM}} = 0.175$. While record single-source visibilities have reached [74], our adopted value (corresponding to $V \approx 0.35$) accounts for the remote-interference penalty inherent in a multi-node network. This lower bound incorporates the cumulative impact of residual spectral diffusion and emitter heterogeneity between independent nodes, providing a robust and realistic framework to evaluate the scaling potential of hBN-based quantum architectures.

In summary, we have confronted a key performance bottleneck in solid-state quantum communication. By integrating a resonant EOM with an hBN quantum emitter, we demonstrated a RT QKD system operating at a 40 MHz dynamic encoding rate. This demonstrates a ten-fold increase in encoding rate over existing visible-regime benchmarks, successfully bypassing a long-standing modulation bottleneck. Achieving a SKR of 7 kbit s^{-1} demonstrates that hBN emitters have reached the performance thresholds required for practical visible-spectrum quantum communication. Although the simplicity of the B92 protocol facilitated this high-speed hardware demonstration, transitioning to a BB84 implementation would inherently provide greater robustness against USD-type attacks and double the theoretical efficiency, representing a natural next step for this architecture. Our demonstration proves that hBN-based SPSs can enable high-speed QKD links strictly at room temperature, offering a practical path for cost-effective point-to-point security. Beyond this immediate application, applying established analytical models to this promising material system for the first time, serves as a quantitative benchmark for the broader field of spin-photon entanglement. While the transition from'flying qubits' to stationary quantum memories inherently requires cryogenic temperatures to maximize ZPL emission and preserve spin coherence, the high-speed temporal and polarization modulation protocols remain identical. Situating our RT results within this roadmap, we highlight a scaling trajectory for hBN: from robust, RT cryptographic devices to fully integrated, cryogenic quantum repeater nodes, shows a clear path to overcoming the rate-versus-distance limitations of direct point-to-point transmission. These combined results, comprising a high-frequency experimental demonstration and a foundational analysis of the network architecture, provide a definitive roadmap for transitioning hBN from a laboratory source to a functional component in high-speed, secure networks. Future improvements through photonic cavity integration to enhance source brightness [76–78] and electrical excitation for miniaturization [79, 80] will undoubtedly pave the way for the deployment of this technology in practical, long-distance, and satellite-based quantum networks [62, 81]. For high-loss, free-space applications like satellite downlinks, a practical implementation would also require the ground station to incorporate adaptive optics to compensate for atmospheric turbulence in addition to the enhanced source brightness. Finally, future work will involve adapting these bright, RT sources for next-generation QKD protocols, such as those based on time-phase encoding [82, 83], which will require significant advances in controlling photon indistinguishability.

Acknowledgments

The authors thank Serkan Paçal, Çağlar Samaner and Kadir Can Doğan for the fruitful discussions during the preparation of the manuscript and NETES Inc. for their provision of equipment for this research. S A acknowledges the support from the Turkish Academy of Sciences (TUBA-GEBIP) and the BAGEP Award of the Science Academy. M G acknowledges support from Einstein Foundation Berlin through an Independent Researcher Grant.

Data availability statement

The data cannot be made publicly available upon publication because no suitable repository exists for hosting data in this field of study.

Author contributions

Ö T, F A and S A conceived and designed the experiments. R P performed the finite key analysis related to the BB84 protocol. M G and D O supervised the theoretical and analytical aspects of the work. S A supervised the overall project. All authors contributed to discussions and reviewed the manuscript.

Funding

This work was supported by the QuantERA II Programme that has received funding from the EU Horizon 2020 research and innovation programme under GA No 101017733 (Comphort), and with funding organisation Scientific and Technological Research Council of Turkey (TUBITAK) under GA Nos. 124N110 and 124N115. This work was also supported by the EPSRC Quantum Technology Hub in Quantum Communication (EP/T001011/1), International Network in Space Quantum Technologies (EP/W027011/1), and the Integrated Quantum Networks Research Hub (EP/Z533208/1). M.G. acknowledges funding from the DLR through funds provided by the Federal Ministry for Economic Affairs and Climate Action (Bundesministerium für Wirtschaft und Klimaschutz, BMWK) under Grant No. 50WM2347.

Appendix A. Baseline quantum key distribution (QKD) parameters

QKD parameters used for asymptotic and finite key analysis are presented in table 2.

Table 2. Baseline QKD and security parameters.

Description	Parameter	Value
Excitation (QKD) rate	R	40 MHz 80 MHz$^{\nabla}$
Collection efficiency	μ_{SPS}	0.052 0.521$^{\nabla}$
Transmitter efficiency	η_{tran}	0.252 0.507$^{\nabla}$
Single-photon purity	$g^2(0)$	0.24 0.018$^{\nabla}$
Mean-photon number	μ_{tran}	0.0131 0.264$^{\nabla}$
Misalignment probability	P_{mis}	0.0176 0.01$^{\nabla}$
Dark count probability	p_{dc}	$8 \cdot 10^{-7}$
Receiver efficiency	η_{rec}	0.42
Privacy amplification failure prob.	$\epsilon_{\mathrm{PA}}, \epsilon$	10^{-10}
Smoothing parameter	$\bar{\epsilon}$	$(\epsilon/8)^2$
Error reconciliation efficiency	f_{EC}	1.16
Error reconciliation failure prob.	ϵ_{EC}	ϵ
Parameter estimation failure prob.	ϵ_{PE}	4ϵ

[∇] Parameters used for the improved work [62].

Appendix B. Key rate calculations

B.1. Finite key analysis for B92 protocol

To calculate the experimentally achieved secret key rates that are presented in figure 3, we employ the security proof for B92-protocol [44] with smooth-Rényi entropies for the finite-key analysis, such that, length of the secure key fraction after post-processing is bounded by,

$$l \leqslant N_R\left[1 - H_{\min}\left(X_{\mathrm{A}}|E\right)\right] - L_{\mathrm{EC}} - 2\log_2\left(\frac{1}{2\epsilon_{\mathrm{PA}}}\right) - \log_2\left(\frac{2}{\epsilon_{\mathrm{cor}}}\right) \tag{2}$$

then the protocol is $\epsilon_{qkd} \geqslant \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{sec}}$ secure, if its ϵ_{cor} correct and $\epsilon_{\mathrm{sec}} \geqslant (2\bar{\epsilon} + \epsilon_{\mathrm{PA}})$ secret.

Harnessing the uncertainty relation for smooth-Rényi entropies [84], Bob's raw key derived from Alice's raw key (A) that conditioned with respect to Eve's uncertainty on the A is quantified as $H^{\bar{\epsilon}}_{\min}(X_{\mathrm{A}}|E)$. Further, the information that Bob requires to correct errors utilizing an error reconciliation protocol, is based on Eve's and Bob's uncertainty about A, is also measured in terms of smooth-Rényi entropies $H^{\bar{\epsilon}}_{\max}(Z_{\mathrm{A}}|B)$, results the bound of [85];

$$H^{\bar{\epsilon}}_{\min}\left(X_{\mathrm{A}}|E\right) + H^{\bar{\epsilon}}_{\max}\left(Z_{\mathrm{A}}|B\right) \geqslant q \tag{3}$$

where $\bar{\epsilon} \geqslant 0$ is the smoothing parameter and $q = -\log_2(c)$ is the quality factor quantifies the incompatibility between the measurements $\mathbb{X}^{\otimes n}$ and $\mathbb{Z}^{\otimes n}$ characterized by POVM elements of the non-orthogonal states. Considering perfect qubits prepared and sent by Alice, we set $q = 1$. In other words, equation 3 is expressed as follows: once Bob achieves the highest accuracy in estimating Alice's raw key in the Z_{A} basis, Eve's ability to guess Alice's raw key in the X_{A} basis is minimized, and vice versa. Further, the measure of Bob's uncertainty can only increase if $H^{\bar{\epsilon}}_{\max}(Z_{\mathrm{A}}|B) \leqslant H^{\bar{\epsilon}}_{\max}(Z_{\mathrm{A}}|Z_{\mathrm{B}})$, for measurement Z_{B} taken place at Bob which is highly correlated with Z_{A}, such that the maximum uncertainty $H^{\bar{\epsilon}}_{\max}(Z_{\mathrm{A}}|Z_{\mathrm{B}})$ is small and bounded by,

$$H^{\bar{\epsilon}}_{\max}\left(Z_{\mathrm{A}}|Z_{\mathrm{B}}\right) \leqslant N_R\ h(Q) \tag{4}$$

where $h(Q)$ is the binary Shannon entropy and -N_R- is the received noisy key size in bits. Then, minimum entropy conditioned on Eve's knowledge on X_{A} basis is expressed as,

$$H^{\bar{\epsilon}}_{\min}\left(X_{\mathrm{A}}|E_{\mathrm{EC}}\right) \geqslant N_R\ q - H^{\bar{\epsilon}}_{\max}\left(Z_{\mathrm{A}}|Z_{\mathrm{B}}\right) \tag{5}$$

such that Eve's information on X_{A} after error reconciliation process is quantified by,

$$H^{\bar{\epsilon}}_{\min}\left(X_{\mathrm{A}}|E\right) \geqslant H^{\bar{\epsilon}}_{\min}\left(X_{\mathrm{A}}|E_{\mathrm{EC}}\right) - L_{\mathrm{EC}} - \log_2\left(\frac{2}{\epsilon_{\mathrm{cor}}}\right) \tag{6}$$

where L_{EC} is the amount of information leakage during error reconciliation process. Following the one-way error reconciliation method [57], the number of leaked bits (L_{EC}) is lower bounded by,

$$\begin{aligned} L_{\mathrm{EC}} \geqslant\ & N_R^X h(Q) \\ & + \left[N_R^X(1-Q) - F^{-1}\left(\epsilon_{\mathrm{cor}}; N_R^X, 1-Q\right)\right]\log_2\left(\frac{1-Q}{Q}\right) \\ & - \frac{1}{2}\log_2 N_R^X - \log_2\left(\frac{1}{\epsilon_{\mathrm{cor}}}\right) \end{aligned} \tag{7}$$

provided that $F^{-1}(\epsilon_{\mathrm{cor}}; N_R^X; 1-Q)$ is the inverse of the cumulative distribution of the binomial distribution and ϵ_{cor} is the correctness failure probability of the reconciliation protocol.

In the context of privacy amplification, Alice and Bob employ a two-universal hash function, utilizing the quantum leftover hash lemma [86], the final secure key length (l) is upper bounded by,

$$l \leqslant H^{\bar{\epsilon}}_{\min}\left(X_{\mathrm{A}}|E\right) - 2\log_2\left(\frac{1}{2\epsilon_{\mathrm{PA}}}\right) \tag{8}$$

such that combining equations (6) and (8), final secure key length given in equation 2 is obtained.

B.2. Finite key analysis for BB84 protocol

We employ the finite-key analysis described by [45, 61] based on multiplicative Chernoff bounds, to analyse our experimental platform's expected performance in an efficient BB84 scenario, which we plot in figure 4. This method provides greater key rate for fixed block sizes, by estimating lower bounds of the received non-multiphoton events and upper bound of the phase error rate. Furthermore, lower bounds of received number of signals in key generation ($\mathbb{X}$) and parameter estimation basis ($\mathbb{Z}$) corresponding to non-multiphoton events are defined as, $\underline{N}^{X}_{R,nmp} = N^{X}_{R} - \bar{N}^{X}_{R,mp}$ and $\underline{N}^{Z}_{R,nmp} = N^{Z}_{R} - \bar{N}^{Z}_{R,mp}$, as the number of received signals are described by $N^{X}_{R} = N_S p^2_X P_{\mathrm{clk}}$ and $N^{Z}_{R} = N_S p^2_Z P_{\mathrm{clk}}$ respectively, for number of sent signals ($N_S = CR \cdot t_S$), determined by the clock rate and the acquisition time, which is defined as the block size used to distill the key. Here, employing the Chernoff bound, the upper bound for the received multi-photon events $\bar{N}^{X}_{R,mp}$ and $\bar{N}^{Z}_{R,mp}$ are estimated as, $\bar{N}^{X,Z}_{R,mp} = \bar{N}^{X,Z*}_{R,mp} + \Delta^{U}$, with $\Delta^{U} = (\beta + \sqrt{8\beta\bar{N}^{X,Z*}_{R,mp} + \beta^2})/2\bar{N}^{X,Z*}_{R,mp}$, for $\beta = -ln\epsilon_{\mathrm{PE}}$, which is bounded by the parameter estimation failure probability (ϵ_{PE}).

For each bases, number of errors (m_X, m_Z) are determined by error probability P_{err}, expressed in terms of misalignment probability P_{mis} as,

$$P_{\mathrm{err}} = \frac{P_0 P_{\mathrm{dc}}}{2} + P_{\mathrm{dc}} + (1 - P_{\mathrm{dc}})\, T\mu_{\mathrm{tran}} P_{\mathrm{mis}} \tag{9}$$

given that, $m_X = N_S p^2_X P_{\mathrm{err}}$ and $m_Z = N_S p^2_Z P_{\mathrm{err}}$ for each bases. Considering only parameter estimation basis ($\mathbb{Z}$) is revealed during error correction process, then the phase error rate with received non-multiphoton fraction is estimated as, $\phi^X = m_Z/\underline{N}^{Z}_{R,nmp}$. On the other hand, for the key generation basis (N^{X}_{R}), which is never revealed, the phase error rate is upper-bounded by $\bar{\phi}^X = \phi^X + \gamma^U(N^{Z}_{R}, N^{X}_{R}, \phi^X, \epsilon)$, such that the function γ^U is defined as,

$$\begin{aligned} \gamma^U(n,k,\lambda,\epsilon) &= \frac{1}{2 + 2\frac{A^2 G}{(n+k)^2}} \left\{ \frac{(1-2\lambda)AG}{n+k} + \sqrt{\frac{A^2G^2}{(n+k)^2} + 4\lambda(1-\lambda)G} \right\} \\ A &= \max\{n,k\}, \quad G = \frac{n+k}{nk} \ln\left(\frac{n+k}{2\pi nk\lambda(1-\lambda)\epsilon^2} \right) \end{aligned} \tag{10}$$

where, $\epsilon = \epsilon_{\mathrm{PA}}$. Then the protocol $\epsilon_{\mathrm{QKD}} \geqslant \epsilon_{\mathrm{sec}} + \epsilon_{\mathrm{cor}}$ is secure, if $\epsilon_{\mathrm{sec}} \geqslant \epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{EC}}$ secret (10^{-10}) and ϵ_{cor} correct (10^{-15}). Finally, equation (2) can be expressed as,

$$l \leqslant \underline{N}^{X}_{R,nmp}\left[1 - h\left(\bar{\phi}^X\right)\right] - L_{\mathrm{EC}} - 2\log_2\left(\frac{1}{2\epsilon_{\mathrm{PA}}}\right) - \log_2\left(\frac{2}{\epsilon_{\mathrm{cor}}}\right) \tag{11}$$

to estimate the final key fraction, for the key rate $r = l/N_S$.

B.3. Asymptotic framework

The asymptotic key rate for the BB84 protocol is given by the Devetak-Winter bound [87],

$$S_\infty \geqslant S(A|E) - S(A|B), \tag{12}$$

where the conditional von Neumann entropies $S(\cdot|\cdot)$ quantify the uncertainty of Alice's subsystem A given the knowledge of Eve's (E) and Bob's (B) subsystems.

In the asymptotic limit, an infinite number of transmissions is assumed. Consequently, Bob's count rates converge to their underlying true expectation values. As a result, no Chernoff bound is applied to the expected multi-photon events, hence $\bar{N}^{X}_{\mathrm{R,nmp}} = \bar{N}^{X,Z*}_{\mathrm{R,nmp}}$. The arbitrarily large block of statistics justifies the following additional simplifications for efficient BB84. First, there is no need to perform parameter estimation ($p_Z \to 0$), hence all detection events can be used to generate the key ($p_X \to 1$). Second, in classical postprocessing, we assume perfect error correction efficiency ($f_{\mathrm{EC}} \to 1$), since classical coding theory shows that, with arbitrarily long code blocks, one can approach the Shannon limit arbitrarily closely. Expressing the entropies of equation (12) in terms of probabilities and incorporating these asymptotic considerations yields

$$\begin{aligned} S_\infty &\geqslant \lim_{\substack{p_X, f_{\mathrm{EC}} \to 1 \\ p_Z \to 0}} p^2_X P_{\mathrm{clk}} \left[\Delta\left(1 - h(Q/\Delta)\right) - f_{\mathrm{EC}} h(Q)\right] \\ &\geqslant P_{\mathrm{clk}}\left[\Delta\left(1 - h(Q/\Delta)\right) - h(Q)\right]. \end{aligned} \tag{13}$$

Table 3. Parameters used in MA-QKD calculations.

Description	Parameter*	Value
Entangled state preparation efficiency	η_{p}	0.7
Preparation time	T_{p}	10^{-6} s
Fiber coupling and frequency conversion efficiency	η_{c}	0.7
Detection efficiency	η_{d}	0.7
BSM ideality parameter	λ_{BSM}	1
BSM success probability	η_{BSM}	0.175
Error correction inefficiency	f	1.16
Misalignment errors	$e_{\mathrm{mA,B}}$	10^{-2}
Memory time	T_2	varied
Attenuation length	L_{att}	22 km

* We adopt the same parameter notation as in [63] for consistency.

The parameter $\Delta = (P_{\mathrm{clk}} - P_{\mathrm{m}})/P_{\mathrm{clk}}$ is calculated using two probabilities. First, the total detection probability $P_{\mathrm{clk}} \approx P_{\mathrm{dc}} + (1 - P_{\mathrm{dc}})T\mu_{\mathrm{tran}}\eta_{\mathrm{tr}}$, where P_{dc} is the dark count probability of the detectors within a single pulse; $T = \eta_{\mathrm{tran}}\eta_{\mathrm{Ch}}\eta_{\mathrm{rec}}$ is the total transmittance (with η_{Ch} channel loss and $\eta_{\mathrm{rec}} = \eta_{\mathrm{Bob}} \cdot \eta_{\mathrm{detector}}$ the receiver efficiency); $\mu_{\mathrm{tran}} = \mu_{\mathrm{SPS}} \cdot \eta_{\mathrm{tran}}$ is the mean photon number of the SPS; and η_{tr} is the trasmissivity of Alice's attenuator, used to pre-attenuate her SPS before the quantum channel. Second, the multi-photon emission probability, which is upper-bounded by $P_{\mathrm{m}} \leqslant g^2(0)\mu_{\mathrm{tran}}^2\eta_{\mathrm{tr}}^2/2$.

Introducing pre-attenuation in Alice's source, defined by the attenuator transmittance η_{tr}, significantly extends the QKD system's tolerable loss range. In the high-loss regime, dark counts and multi-photon events dominate, the latter depends quadratically on this transmittance, $P_{\mathrm{m}}\alpha\eta_{\mathrm{tr}}^2$, whereas the detection probability scales linearly, $P_{\mathrm{clk}}\alpha\eta_{\mathrm{tr}}$. Consequently, the multi-photon probability decreases more rapidly, enhancing the key generation rate.

For the simulations, the expected QBER (Q) is defined by,

$$Q = \frac{P_{\mathrm{mis}}T\mu_{\mathrm{tran}} + P_{\mathrm{dc}}/2}{P_{\mathrm{clk}}} \tag{14}$$

where the parameter -P_{mis}- represents the misalignment probability, described as static error contribution due to component imperfections. We note that while the baseline QBER is primarily driven by the finite polarization extinction ratio of the optical components and detector dark counts, the non-zero $g^{(2)}(0)$ value of the source does not directly increase this baseline error. Instead, the multi-photon emission probability critically bounds the final SKR by defining the system's vulnerability to PNS attacks.

B.4. Single quantum repeater node calculations

The scheme analyzed in [63] relies on two quantum registers, or memories (QM-A and QM-B), each capable of creating a photon-memory entangled state. A photon entangled with QM-A is prepared (with efficiency η_{p} and over time T_p) and sent to Alice, who performs a BB84 measurement on it, repeating the process until she successfully detects a photon. The same procedure is then carried out with Bob and QM-B. Once both photons have been measured, a Bell measurement is performed on the two QMs, and the result is shared with Bob. Depending on the outcome, Bob may need to apply a bit flip to his BB84 measurement result to obtain the same bit as Alice, —specifically, if he measured in the Z basis and the Bell measurement resulted in $|\psi^+\rangle$ or $|\psi^-\rangle$, or if he measured in the X basis and the Bell measurement resulted in $|\phi^-\rangle$ or $|\psi^-\rangle$. Table 3 shows the relevant parameters used in the calculations that are shown in figure 4 and 5. The position of this central node with respect to Alice and Bob can be optimized for a given channel loss to maximize the achievable key rate. Exact formulae for these calculations are not reproduced here and can be found in [63].

ORCID iDs

Ömer S Tapşın 0009-0001-1718-3670
Furkan Ağlarcı 0009-0003-3033-209X
Roberto G Pousa 0009-0001-8717-653X
Daniel K L Oi 0000-0003-0965-9509

Mustafa Gündoğan 0000-0002-0069-4386
Serkan Ateş 0000-0001-5452-6727

References

[1] Wehner S, Elkouss D and Hanson R 2018 *Science* **362** eaam9288
[2] Lu C Y and Pan J W 2021 *Nat. Nanotechnol.* **16** 1294–6
[3] Gyongyosi L and Imre S 2022 *Commun. ACM* **65** 52–63
[4] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7–11
[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121–4
[6] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–21
[7] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3
[9] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557–9
[10] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[11] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[12] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[13] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[14] Couteau C, Barz S, Durt T, Gerrits T, Huwer J, Prevedel R, Rarity J, Shields A and Weihs G 2023 *Nat. Rev. Phys.* **5** 326–38
[15] Cholsuk C, Aglarci F, Oi D K L, Ateş S and Vogl T 2025 arXiv:2510.09454
[16] Barnes F B, Pousa R G, Morrison C L, Koong Z X, Ho J, Graffitti F, Jeffers J, Oi D K L, Gerardot B D and Fedrizzi A 2025 arXiv:2512.05101
[17] Waks E, Inoue K, Santori C, Fattal D, Vuckovic J, Solomon G S and Yamamoto Y 2002 *Nature* **420** 762
[18] Zahidy M *et al* 2024 *npj Quantum Inf.* **10** 2
[19] Zhang Y *et al* 2025 *Phys. Rev. Lett.* **134** 210801
[20] Dzurnak B, Stevenson R M, Nilsson J, Dynes J F, Yuan Z L, Skiba-Szymanska J, Farrer I, Ritchie D A and Shields A J 2015 *Appl. Phys. Lett.* **107** 261101
[21] Basset F B *et al* 2021 *Sci. Adv.* **7** eabe6379
[22] Schimpf C, Reindl M, Huber D, Lehner B, Silva S F C D, Manna S, Vyvlecka M, Walther P and Rastelli A 2021 *Sci. Adv.* **7** eabe8905
[23] Basset F B *et al* 2023 *Quantum Sci. Technol.* **8** 025002
[24] Lodahl P and Stobbe S 2013 *Nanophotonics* **2** 39–55
[25] Arakawa Y and Holmes M J 2020 *Appl. Phys. Rev.* **7** 021309
[26] Vajner D A, Rickert L, Gao T, Kaymazlar K and Heindel T 2022 *Adv. Quantum Technol.* **5** 2100116
[27] Xingjian Z, Haoran Z, Chua R M, Eng J, Meunier M, Grieve J A, Weibo G and Ling A 2025 *Natl Sci. Rev.* **12** nwaf147
[28] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J P and Grangier P 2002 *Phys. Rev. Lett.* **89** 187901
[29] Alléaume R, Treussart F, Messin G, Dumeige Y, Roch J F, Beveratos A, Brouri-Tualle R, Poizat J P and Grangier P 2004 *New J. Phys.* **6** 92
[30] Leifgen M *et al* 2014 *New J. Phys.* **16** 023021
[31] Tran T T, Bray K, Ford M J, Toth M and Aharonovich I 2016 *Nat. Nanotechnol.* **11** 37–41
[32] Kianinia M, Xu Z Q, Toth M and Aharonovich I 2022 *Appl. Phys. Rev.* **9** 011306
[33] Montblanch A R P, Barbone M, Aharonovich I, Atatüre M and Ferrari A C 2023 *Nat. Nanotechnol.* **18** 555–71
[34] Cholsuk C, Zand A, Çakan A and Vogl T 2024 *J. Phys. Chem. C* **128** 12716–25
[35] Çakan A, Cholsuk C, Gale A, Kianinia M, Paçal S, Ateş S, Aharonovich I, Toth M and Vogl T 2025 *Adv. Opt. Mater.* **13** 2402508
[36] Samaner C, Paçal S, Mutlu G, Uyanik K and Ateş S 2022 *Adv. Quantum Technol.* **5** 2200059
[37] Al-Juboori A, Zeng H Z J, Nguyen M A P, Ai X, Laucht A, Solntsev A, Toth M, Malaney R and Aharonovich I 2023 *Adv. Quantum Technol.* **6** 2300038
[38] Ahmadi N *et al* 2024 *Adv. Quantum Technol.* **7** 2300343
[39] Stern H L *et al* 2022 *Nat. Commun.* **13** 618
[40] Durand A *et al* 2023 *Phys. Rev. Lett.* **131** 116902
[41] Kupko T, Helversen M v, Rickert L, Schulze J H, Strittmatter A, Gschrey M, Rodt S, Reitzenstein S and Heindel T 2020 *npj Quantum Inf.* **6** 29
[42] Waks E, Santori C and Yamamoto Y 2002 *Phys. Rev. A* **66** 042315
[43] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325–60
[44] Mafu M, Garapo K and Petruccione F 2013 *Phys. Rev. A* **88** 062306
[45] Pousa R G, Oi D K L and Jeffers J 2024 arXiv:2405.19963
[46] Li S X *et al* 2023 *Commun. Mater.* **4** 19
[47] Cuscó R, Gil B, Cassabois G and Artús L 2016 *Phys. Rev. B* **94** 155435
[48] Kumar A *et al* 2024 *ACS Nano* **18** 5270–81
[49] Li C, Xu Z Q, Mendelson N, Kianinia M, Toth M and Aharonovich I 2019 *Nanophotonics* **8** 2049–55
[50] Castelletto S, Inam F A, Sato S i and Boretti A 2020 *Beilstein J. Nanotechnol.* **11** 740–69
[51] Novotny L and Hecht B 2012 *Principles of Nano-Optics*
[52] Martínez L J, Pelini T, Waselowski V, Maze J R, Gil B, Cassabois G and Jacques V 2016 *Phys. Rev. B* **94** 121405
[53] Nikolay N, Mendelson N, Özelci E, Sontheimer B, Böhm F, Kewes G, Toth M, Aharonovich I and Benson O 2019 *Optica* **6** 1084
[54] Yamamura K, Coste N, Zeng H Z J, Toth M, Kianinia M and Aharonovich I 2024 *Nanophotonics* **14** 1715–20
[55] Heindel T *et al* 2012 *New J. Phys.* **14** 083001
[56] Samaner Ç and Ateş S 2025 *ACS Photon.* **12** 5042–9
[57] Tomamichel M, Martinez-Mateo J, Pacher C and Elkouss D 2017 *Quantum Inf. Process.* **16** 280
[58] Dušek M, Jahma M and Lütkenhaus N 2000 *Phys. Rev. A* **62** 022306
[59] Ko H, Choi B S, Choe J S and Youn C J 2017 *Quantum Inf. Process.* **17** 17
[60] Tamaki K and Lütkenhaus N 2004 *Phys. Rev. A* **69** 032316
[61] Morrison C L *et al* 2023 *Nat. Commun.* **14** 3573
[62] Vogl T, Lecamwasam R, Buchler B C, Lu Y and Lam P K 2019 *ACS Photon.* **6** 1955–62

[63] Luong D, Jiang L, Kim J and Lütkenhaus N 2016 *Appl. Phys. B* **122** 96
[64] Murtaza G, Colautti M, Hilke M, Lombardi P, Cataliotti F S, Zavatta A, Bacco D and Toninelli C 2023 *Opt. Express* **31** 9437
[65] Yang J *et al* 2024 *Light: Sci. Appl.* **13** 150
[66] Gao T, Helversen M v, Antón-Solanas C, Schneider C and Heindel T 2023 *npj 2D Mater. Appl.* **7** 4
[67] Bradley C, Randall J, Abobeih M, Berrevoets R, Degen M, Bakker M, Markham M, Twitchen D and Taminiau T 2019 A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute *Phys. Rev. X* **9**
[68] Stas P *et al* 2022 Robust multi-qubit quantum network node with integrated error detection *Science* **378** 557–60
[69] Appel M Hayhurst *et al* 2025 A many-body quantum register for a spin qubit *Nat. Phys.* **21** 368–73
[70] Gottscholl A, Diez M, Soltamov V, Kasper C, Sperlich A, Kianinia M, Bradac C, Aharonovich I and Dyakonov V 2021 Room temperature coherent control of spin defects in hexagonal boron nitride *Sci. Adv.* **7**
[71] Stern H L *et al* 2024 *Nat. Mater.* **23** 1379–85
[72] Ye M, Seo H and Galli G 2019 *npj Comput. Mater.* **5** 44
[73] Sajid A and Thygesen K S 2022 *Phys. Rev. B* **106** 104108
[74] Gérard D, Buil S, Watanabe K, Taniguchi T, Hermier J P and Delteil A 2026 *Nat. Commun.* **17** 1843
[75] Langenfeld S, Thomas P, Morin O and Rempe G 2021 Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution *Phys. Rev. Lett.* **126**
[76] Haußler S, Bayer G, Waltrich R, Mendelson N, Li C, Hunger D, Aharonovich I and Kubanek A 2021 *Adv. Opt. Mater.* **9** 2002218
[77] Sakib M A *et al* 2024 *Nano Lett.* **24** 12390–7
[78] Dowran M, Kilic U, Lamichhane S, Erickson A, Barker J, Schubert M, Liou S, Argyropoulos C and Laraoui A 2025 *Laser Photon. Rev.* **19** 2400705
[79] Yu M, Lee J, Watanabe K, Taniguchi T and Lee J 2024 *ACS Nano* **19** 504–11
[80] Zhigulin I, Park G, Yamamura K, Watanabe K, Taniguchi T, Toth M, Kim J and Aharonovich I 2025 *ACS Appl. Mater. Interfaces* **17** 24129–36
[81] Abasifard M, Cholsuk C, Pousa R G, Kumar A, Zand A, Riel T, Oi D K L and Vogl T 2024 *APL Quantum* **1** 016113
[82] Liu Y *et al* 2023 *Phys. Rev. Lett.* **130** 210801
[83] Li Y H *et al* 2025 arXiv:2503.17744
[84] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506
[85] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[86] Tomamichel M, Schaffner C, Smith A and Renner R 2011 *IEEE Trans. Inf. Theory* **57** 5524–35
[87] Devetak I and Winter A 2005 *Proc. R. Soc. A* **461** 207–35