ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Quantum Key Distribution Using a Quantum Emitter in Hexagonal Boron Nitride

Ali Al-Juboori, Helen Zhi Jie Zeng, Minh Anh Phan Nguyen, Xiaoyu Ai, Arne Laucht, Alexander Solntsev, Milos Toth, Robert Malaney, and Igor Aharonovich**

Quantum key distribution (QKD) is considered the most immediate application to be widely implemented among a variety of potential quantum technologies. QKD enables sharing secret keys between distant users by using photons as information carriers. An ongoing endeavor is to implement these protocols in practice in a robust, and compact manner so as to be efficiently deployable in a range of real-world scenarios. Single photon sources (SPS) in solid-state materials are prime candidates in this respect. This article demonstrates a room temperature, discrete-variable quantum key distribution system using a bright single photon source in hexagonal-boron nitride, operating in free-space. Employing an easily interchangeable photon source system, keys with one million bits length, and a secret key of approximately 70000 bits, at a quantum bit error rate of 6%, with ε-security of 10^{-10} are generated. This study demonstrates the first proof of concept finite-key BB84 QKD system realized with hBN defects.

1. Introduction

Secure and hacking-proof communications are a vital requirement in today's world. Traditional public key cryptography relies on lengthy and hard to decipher mathematical functions to encrypt and decrypt data. However, with the advancement of quantum computers, secured communication is increasingly vulnerable to hacking attempts. Quantum Key Distribution (QKD)[1–3] , the best-known application of quantum cryptography, offers an information-theoretic secure communication system, largely on account of the quantum non-cloning theorem.[4] It enables two users to generate the exact same key without sharing any part of it publicly, providing a solution to secure key exchange. Since its inception in the mid-1980s, and the first successful proof-of-concept test,[5] QKD has evolved to include various approaches such as entanglement-based QKD,[6–9] measurement-device-independent QKD,[10] quantum teleportation-based QKD,[11] and satellite-based QKD.[12] So far the majority of QKD systems rely on either nonlinear down-converted sources or attenuated lasers.[13,14] The advantage of these latter sources is their potentially high repetition rate. One alternative approach is using a deterministic, triggered single photon source (SPS) that emits a single photon per excitation cycle.

Over the last few decades, significant effort has been put forward to develop such sources, with the prime challenges being their purity (i.e., minimization of multiphoton events) and extraction of light (i.e., collection efficiencies).[15,16] While semiconductor quantum dots are a great choice for a bright and pure source,[17–21] their operation is limited to cryogenic temperatures. For wide deployment and practical implementation of QKD in real-world settings, compact, room temperature, sources are required.[22–25] Among the various solid-state materials, single-photon sources in hexagonal boron nitride (hBN) are considered a prime candidate for QKD owing to the material's favorable physical and optical properties [26]. In particular, properties such as a high single-photon purity, and high-brightness operating in ambient conditions give a competitive advantage over other sources,[27] and a demonstration of the B92 QKD protocol has already been reported in Ref. [22] with a sifted key rate of 238 bit/s (similar to our raw key and bounded raw key rates below) and quantum bit error rates (QBERs) of 8.95%.

After having demonstrated the in-principle usability of hBN SPSs for QKD in Ref. [27], in this work, we include a full implementation of a free-space, discrete-level QKD system using an integrated SPS in hBN. We implement the BB84 protocol,

A. Al-Juboori, H. Z. J. Zeng, M. A. P. Nguyen, A. Solntsev, M. Toth, I. Aharonovich
School of Mathematical and Physical Sciences, Faculty of Science
University of Technology Sydney
Ultimo, New South Wales 2007, Australia
E-mail: igor.aharonovich@uts.edu.au

A. Al-Juboori, X. Ai, A. Laucht, R. Malaney
School of Electrical Engineering and Telecommunications
The University of New South Wales
Sydney NSW 2052, Australia
E-mail: a.laucht@unsw.edu.au

M. Toth, I. Aharonovich
ARC Centre of Excellence for Transformative Meta-Optical Systems
Faculty of Science
University of Technology Sydney
Ultimo, New South Wales 2007, Australia

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202300038

DOI: 10.1002/qute.202300038

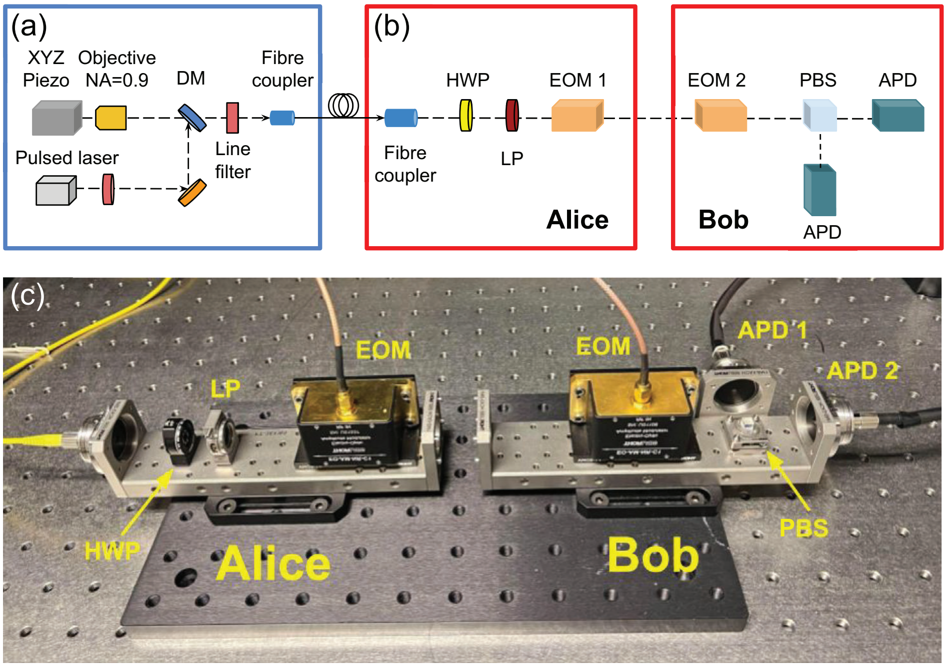

Figure 1. a) Schematic diagram of the single-photon source. DM, dichroic mirror. b) Schematic diagram of the QKD setup. EOM, electro-optic modulator; LP, linear polariser; APD, avalanche photodiode; PBS, polarizing beam splitter; HWP, half-wave plate. c) The optical components of the transmitter (Alice) and the receiver (Bob).

demonstrating the sending, receiving, and encryption/decryption process of an image from one device to another. We perform all security protocols, including privacy amplification, to demonstrate the most reliable QKD realized with SPSs to date.

2. Results and Discussion

The optical apparatus used to perform the measurements as a whole can be split into two main systems; the source to generate the single photons, and the QKD apparatus to perform the key distribution measurements. The hBN single photon sources are the primary source of photons for the QKD system. The sources are integrated with a solid immersion lens and packaged into a compact, portable device as described previously[27] and shown schematically in **Figure 1**a. For the QKD experiments, the sources are excited using a 515 nm pulsed laser (PicoQuant PDL-800D), and the collection is coupled via single mode optical fiber to the QKD sender (Alice).

The QKD-side setup is shown in Figure 1b. The management and distribution of keys are performed by elements that modulate and/or measure the polarization of the photons. The elements lie in a transmitter and receiver, termed Alice, and Bob, respectively, that are separated by tens of centimetres in free space. The signal from the source is sent to the Alice, first. Alice consists of a half-wave plate (FBR-AH1, Thorlabs), linear polarizer (FBRP, Thorlabs), and an electro-optic modulator (EOM) (EO-AM-NR-C1, Thorlabs). The half-wave plate and linear polarizer are used to align and filter vertically polarized photons, respectively, minimizing losses as they enter the EOM - a requirement for its function. The EOM is driven by a digital-to-analogue converter (DAC) (EVAL-AD5754REBZ, Analog Devices), multiplexer (MUX36D04EVM-PDK, Texas Instruments), and a high voltage amplifier (HVA 200, Thorlabs), supplying the four voltages (two voltages in Bob's case) to the EOMs to induce the desired polarization states. Bob consists of an EOM, polarizing beam splitter (PBS052, Thorlabs), and two avalanche photodiodes (APD, SPCMAQRH-12-FC, Excelitas).

We start by choosing the most appropriate hBN SPSs – in particular, those with a high single-photon purity. **Figure 2**a shows the spectrum of the hBN SPS used in all QKD runs reported here. This SPS has a characteristic sharp zero-photon line (ZPL) at 645 nm (see Figure 2a), with an intrinsic linear polarization of 95.6%. The emission was then bandpass filtered (Semrock, 650 ± 13 nm) to select only photons from around the ZPL for the QKD experiment. The bandpass filtering was crucial in overcoming the wavelength dependence of the EOM and ensuring that the single-photon purity remains as low as possible, with Figure 2b showing the second-order autocorrelation function $g^{(2)}(0) = 0.08$. From the $g^{(2)}(t)$ measurement, we can also extract the radiative emission time of $\tau = 3.87$ ns.

Additionally, the count rate was measured as a function of average pulsed excitation power at a pulse repetition rate of 40 MHz, as shown in Figure 2c. By fitting the curve to $I = I_{\mathrm{Sat}}[P/(P + P_{\mathrm{Sat}})]$, we find the SPS to saturate at a power of $P_{\mathrm{Sat}} = 217$ μW, with a count rate of $I_{\mathrm{Sat}} = 5.08 \times 10^5$ cts/s as out-coupled from the single-mode fibre. From this, the calculation of the source-side total setup efficiency can be quantified with a mean photon number per pulse of $\mu = 0.012$. This value was not corrected and includes contributions from single-photon emitter collection, optical losses, and detector efficiency - giving a realistic characterization of the entire system. The number of photons per pulse

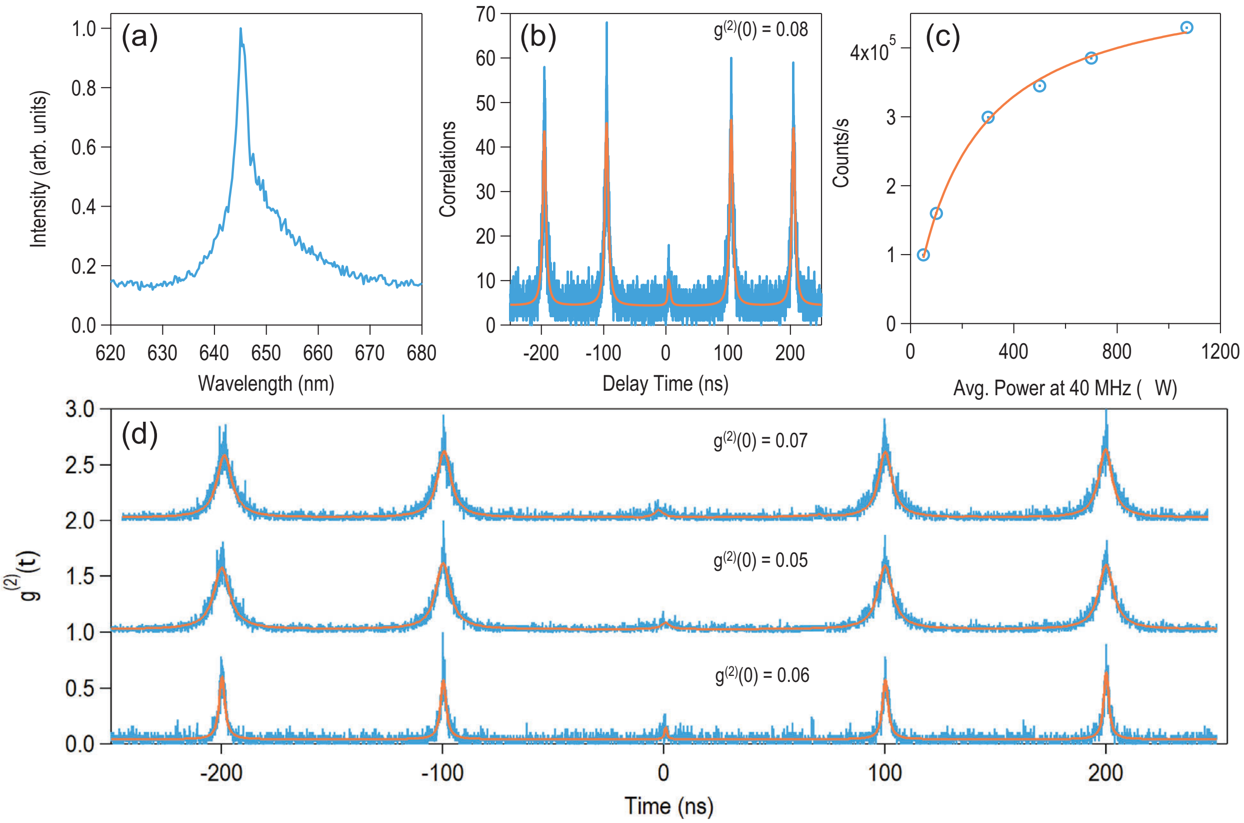

Figure 2. Optical characteristics of the hBN SPS as measured through the SIL. a) Spectrum of the SPS used for QKD, showing a sharp ZPL at 645 nm. b) Pulsed second-order autocorrelation function of the QKD SPS at 10 MHz, showing a $g^{(2)}(0) = 0.08$. The background in this measurement originates from the dark counts of our detectors. c) Power-dependent saturation measurements showing count rate as a function of pulsed excitation power at 40 MHz repetition rate. d) Pulsed second-order autocorrelation measurements of three characteristic SIL-integrated hBN SPSs, showing typical single-photon purity. All measurements were performed at 10 MHz repetition rate.

can be substantially improved by optimizing the collection further, employing different designs.[28,29] Our experimental setup enables rapid characterization and swapping of other sources, and we show examples of three other suitable sources with low $g^{(2)}(0)$ values in Figure 2d.

Having characterized and established the source of single photons, the testbed for the QKD system was then initiated. **Figure 3**a shows the operation sequence of the QKD process. The process starts with Alice generating a sequence of random integer numbers, each of which is 0, 1, 2, or 3, while Bob generates a sequence of random numbers between 0 and 1 [30]. Alice's numbers are used to encode the measurement bases and bit values onto the photons, while Bob's numbers are used to select the measurement bases for the measurements.

More specifically, Alice's numbers map to one of four polarization states imparted to the photons, horizontal (H,↔), vertical (V,↕), right-handed circular (R,↻), or left-handed circular (L,↺). For each laser pulse cycle, at a rate of 500 kHz, Alice's randomly generated number switches a multiplexer to select a specific one of four channels from the digital-to-analogue converter (DAC) to apply a predetermined voltage to the EOM and, as such, encodes the desired polarization state onto the photon.

Bob uses a corresponding setup to randomly select a basis, H/V or R/L, and measure the photon to obtain one of four outcomes. Bob's EOM either leaves the incoming photon in its polarization base or interchanges linear and circular polarization. The PBS (polarizing beam splitter) then separates linearly polarized photons with certainty to be detected at one of two detectors, whereas circularly polarized photons are unpredictably registered at either one of the two detectors. Bob's APDs are gated to the laser pulse with a gating time of 40 ns, and only the detection event of a single photon by one of the APDs per time bin is considered a valid bit and stored to the computer.

After revealing their bases used, Alice and Bob "sift" their events, discarding those that have mismatched bases. By defining H and R to correspond to a bit value of "0", and V and L to correspond to a bit value of "1"„ respectively, Alice and Bob retain a partially-correlated string of random bits. This string must be processed further to obtain the 'secret key'.

The required number of bits in the partially-correlated string must be large enough to provide a non-zero secret key rate at the pre-assigned ϵ-security (total failure probability),[31–33] as discussed in the appendix. After accumulating the required number of bits, the post-processing procedure is initiated, the first component of which is parameter estimation (see Table A1 for an overview of all parameters). After this, a next phase is commenced, which consists of reconciliation and privacy amplification, after that the final secret key is generated.

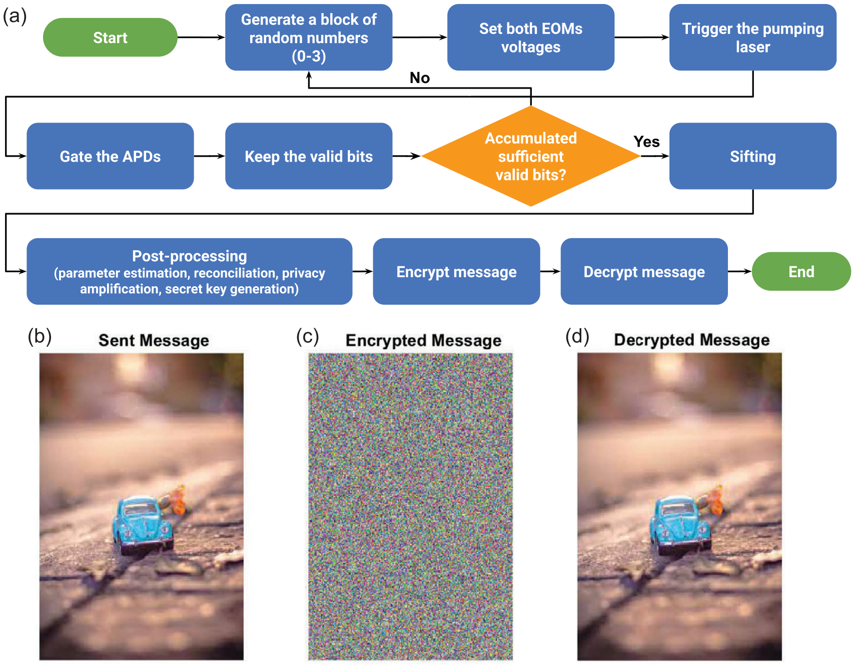
(a)
Start
Generate a block of random numbers (0-3)
Set both EOMs voltages
Trigger the pumping laser
No
Gate the APDs
Keep the valid bits
Accumulated sufficient valid bits?
Yes
Sifting
Post-processing (parameter estimation, reconciliation, privacy amplification, secret key generation)
Encrypt message
Decrypt message
End
(b) Sent Message
(c) Encrypted Message
(d) Decrypted Message

Figure 3. QKD operation sequence. a) Flowchart of the QKD process. b) Original image, c) image encrypted with Alice's secure key, and d) the decrypted image after decoding it using Bob's secure key.

Table 1. Selected experimental runs with their respective parameters.

Experiment no.	1	2	3	4	5	6
Clock rate (Hz)	500,000	500,000	500,000	500,000	500,000	500,000
Photon detection rate at Bob (cts/s)	1527	1486	1375	1722	1666	1001
Raw key length (bits)	1,000,000	1,000,000	100,000	100,000	10,000	10,000
Raw key rate (bits/s)	88	96	80	100	96	56
Bounded raw key rate (bits/s)	396	432	360	450	432	252
QBER	0.07	0.06	0.08	0.05	0.03	0.08

In the QKD experiments, we transmitted blocks of one million random bits at a clock rate of 500 kHz (limited by the voltage amplifier and the EOM), resulting in a 2 s transmission phase during which Bob received photons at a detection rate of ≈ 1500 cts/s. After this transmission phase, our system required 7 s for the data processing phase (dominated by the data transfer between the FPGA board and the PC), resulting in a total of 9 s per block of one million random bits. During the experiments no. 1 and no. 2 (in **Table 1**) we repeated the transmission of these blocks until four million valid bits were accumulated (see also the flow chart in Figure 3a). 50% of the accumulated bits are sacrificed during the sifting process, while another 50% of the remaining bits are used for the quantum bit error rate (QBER) estimation. The partially-correlated keys that exist at this phase are referred to as the 'raw keys'. Error correction is then initiated to turn the partially-correlated pair of keys into identical keys. Following this, the now correlated keys are input to the privacy amplification process of which, approximately $1/16^{\text{th}}$ end up as the final secret keys (see appendix for details on error correction and privacy amplification).

We repeated the QKD measurement numerous times, accumulating raw keys of lengths up to 10^6 bits (after sifting and QBER estimation). Representative results for several independent runs of different lengths are shown in Table 1, with QBER values ranging between 3% and 8%. We attribute the variation in QBER values to changes in the experimental conditions, such as drifts in the gain of the high voltage amplifiers (HVA200, Thorlabs) and background light in the room.

Our experimental set up was primarily aimed at the development of the most reliable key in terms of ϵ-security, not the key rate. Hardware limitations imposed certain constraints on us, related to the amount of quantum information that could be transferred before classical protocols were implemented (e.g., TCP socket connections, memory-read functions), which led to time delays of 7 s per million bit-transfer attempts. Of course, such processing delays can never be set to zero in any implementation, but if we simply set all such delays to zero, we derive what we refer to as the 'bounded raw key rate' in Table 1. Beyond the time delays, the three most important factors influencing the raw key rate are i) the input pump rate; ii) capture rates from the photon source; and iii) losses in our optical components. Achievable improvements in these three factors alone would readily lead us into the ≈ 10 kHz raw key rate range.

For runs no. 1 and no. 2 (in Table 1) we also performed privacy amplification at ϵ-security levels of 10^{-10} and below, and achieved secret key lengths of 33176 bits & 68516 bits at secret key rates of 4 (bits/s) & 6 (bits/s) or bounded secret key rates of 18 (bits/s) & 26 (bits/s), respectively. For the other runs in Table 1, finite key effects result in zero secret key rates at a ϵ-security level of 10^{-10}.

Finally, to demonstrate the QKD utility, we transfer an image in a secured way from Alice to Bob. The image of a toy car consisting of 48 kbits is shown in Figure 3b. We use the key from the QKD experiment no. 2 (see Table 1) as a one-time keypad to encrypt the image (Figure 3c). Alice then transmits the image to Bob classically, and Bob decrypts the image using the secure key at his end, as shown in Figure 3d. In more detail, encryption is achieved by performing a bitwise XOR operation between the plain text and the key, while decryption is carried out by XORing the cipher text with the same key, resulting in the original plain text.

A direct comparison with other reported single-photon QKD secure key rates is not straightforward given the difference in assumptions used (finite vs asymptotic, security equations, etc.) and technology used across the different reported works. Nonetheless, it may still be of value to attempt some form of key-rate comparison. We believe the raw key rate is best in this regard as most security assumptions have no impact on this rate.

In the prototype reported here, we found a raw key rate of 100 bits/s at 0.5 MHz clock rate. This is almost comparable to that reported in Ref. [7] using a GaAs quantum dot (106 bits/s at 320 MHz clock rate), a factor 40× less than Ref. [23] using the NV in diamond (3.99 kbits/s at 1 MHz clock rate), a factor 100× less than Ref. [34] using an electrically driven InAs quantum dot (5–17 kbits/s at 125 MHz clock rate), and a factor 270× less than that reported in Ref. [18] using InP and InAs quantum dots (27–35 kbit/s at 182.6 MHz clock rate). Furthermore, recent experiments have performed QKD with frequency-converted quantum dot SPSs over longer distances, achieving 1–689 kbits/s depending on fiber length at 160 MHz clock rate in Ref. [20] and 5–6 kbits/s at 72.6 MHz clock rate in Ref. [35].

We caution again, that direct comparison of rates across different experiments, even when just raw key rates, is not straightforward. Many factors, including clock rates, processor speeds, sifting protocol used, and fractions sacrificed for error estimation are in play. Additional issues are raised when secure key rates are to be compared.

3. Conclusion

We report a functional, free-space, room-temperature QKD prototype with high-purity hBN SPSs. We implement a complete BB84 protocol, including privacy amplification and QBER corrections, at a security level (total failure probability) of 10^{-10}. As discussed further in the appendix, although our rates are lower relative to others seen in the literature,[23,34,36] straightforward comparison of the many published results should be done with caution as many different assumptions and security settings can be in place. In addition, our clock rate operates at 500 kHz, compared to other experiments that trigger at a few MHz rates, or faster.

Furthermore, we have included all possible assumptions in our derivation of security in the finite key limit. We have assumed the photons from our source contain no significant vacuum contributions, and therefore the issues raised in Refs. [37, 38] are neglected. We believe our experimental secret key rates currently represent the most reliable in terms of security for the type of photon source used. Increasing the rate at a given security level, can be achieved via various improvements in the system – including an increased photon collection rate from the SPS, increased speed in the electronics, and increased computational power for the classical reconciliation. For instance, one key limitation originates from the high voltage amplifiers needed to drive the EOMs, which can be improved using alternative hardware. Using different field-programmable gate array (FPGA) hardware and data transfer protocols, can also further increase the rates.

All in all, our source has a robust performance at room temperature, with high brightness exceeding 4×10^5 photons/s under pulsed excitation and operation under ambient conditions that promises a straightforward employment in the field. Our work paves the way for scalable implementation of QKD systems and holds great promise for using triggered room temperature SPSs based on hBN.

Appendix A: Parameters

Table A1.

Table A1. Summary table of the experimental parameters required for calculating the secret key rate.

Parameter	Value	Comment
ϵ-security level, ϵ	10^{-10}	Security requirement set by the user.
Error correction factor, f_{ec}	1.1	Derived from the efficiency of the error correction scheme (relief propagation protocol).
Detector efficiency, η	0.65	From Excelitas SPCM-AQRH Family datasheet.
Multi-photon probability, μ	0.08	Measured via a pulsed second-order autocorrelation measurement (Figure 2c).
Photon detection prob., p_{det}	0.0015	Calculated from photon count rate and pulse rate.
Multi-photon prob., P_m	$2.3 \cdot 10^{-5}$	Calculated from multi-photon count rate and pulse rate.
Multi-photon correction term, A	0.985	Calculated from $1 - c/m$, where c is the number of double-photon events, and m is the number of single-photon events.
Photon detection rate (cts/s)	1000 – 1700	Measured with Bob's APDs during the QKD experiment.
Raw key rate (bits/s)	88 – 100	Calculated from raw key length and experiment duration.
Bounded raw key rate (bits/s)	396 – 450	Calculated from raw key length and exp. duration without processing time.
Quantum bit error rate (QBER)	0.03 – 0.08	Determined from comparing Alice's and Bob's keys after sifting.
Binary Shannon-entropy, H	0.402	Calculated from $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, where x = QBER.

Appendix B: Reconciliation

Reconciliation is a classical post-processing step that corrects the discrepancies between Alice and Bob's bit strings. Let us assume the estimated QBER, Q, is already achieved (via the prior sacrifice of m bits) and that Alice and Bob start reconciliation with two bit strings (the raw keys), K_A and K_B, each of length n bits. The common treatment is to break K_A and K_B into shorter sub-blocks and then reconcile them in parallel.[39] Applying this treatment to our experiments, the procedure of reconciliation is as follows:

- **Step 1: Partition**. Alice breaks her K_A into multiple sub-blocks and the size of each sub-block is set to n_{block} ($n_{\text{block}} \leq n$). Bob does the same to his K_B. Then, Alice and Bob will apply Step 2 and 3 to each of their sub-blocks. In our experiments we set $n_{\text{block}} = 10^4$, and note that a maximum of eight sub-blocks can be simultaneously reconciled due to the limited number of threads available at Alice.
- **Step 2: Syndrome Calculation**. Bob applies an LDPC matrix, $\mathbf{H}$, to his sub-block and obtains syndrome bits. Then, Bob sends the syndrome bits, S_B (of length s_B), to Alice via classical communications. We adopted an LDPC code designed to maximize its decoding threshold at a code rate, $R_c = 0.5$. [Note, the decoding threshold of a given LDPC code is the maximal bit error rate so that a belief-propagation decoder is guaranteed to correct all the errors in an LDPC block[40] - it can be maximized by using *Density Evolution*.[40]] The degree distribution polynomials of the adopted code can be found in Table I of [41]. The matrix $\mathbf{H}$ (with $n_{\text{block}}(1 - R_c)$ rows and n_{block} columns) was constructed by the Progressive Edge Growth (PEG) algorithm[42] based on the above mentioned polynomials.
- **Step 3: Decoding**. Alice uses Bob's syndrome bits, her sub-block, Q, and $\mathbf{H}$ as inputs to her LDPC decoder to correct all the discrepancies between Alice and Bob's sub-block. The LDPC decoder used is a serial-scheduled belief propagation decoder[43] implemented in C++.
- **Step 4: Reorganising**. After all the sub-blocks are reconciled, Alice reorganises all her sub-blocks into a single bit string (the reconciled key), $\hat{K_A}$, again of length n (similarly Bob to get $\hat{K_B}$).

Alice and Bob then proceed to privacy amplification to generate two identical and secure keys for cryptography purposes. Let us define the ratio, $r = s_{\text{final}}/n$, where s_{final} is the final key length required to achieve a set security level. To determine r we consider the security analysis in the finite-key length regime in Refs. [31–33, 44]. Let us further define *ε-security* as the total failure probability, ε, of the protocol. Specifically, $\varepsilon = \tilde{\varepsilon} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PE}}$, where $\tilde{\varepsilon}$ is the smoothing parameter for the smooth min-entropy calculation, ε_{PA} is the failure probability of privacy amplification, and ε_{EC} is the failure probability of error correction. The probability ε_{PE} is somewhat more involved.[31,32,45] Consider the key, K_B^N, held by Bob (similar to K_B but including the m states that are to be sacrificed, i.e., $N = n + m$), and the key, E^N, held by the eavesdropper. Defining the combined quantum state held by Bob and the eavesdropper as $\rho_{K_B^N E^N} = (\sigma_{KE})^{\otimes N}$, where K and E represent individual components of K_B^N and E^N, respectively, then σ is contained in the set Γ_ξ defined by $\{\sigma : ||\lambda_m - \lambda_\infty(\sigma)|| \leq \xi\}$, except with probability ε_{PE}. Here, λ_m are the statistics derived from measurements on m samples of σ; $\lambda_\infty(\sigma)$ is the probability distribution defined by the measurements on σ; and $\xi = \frac{1}{2}\sqrt{\frac{2\log_2(\frac{1}{\varepsilon_{\text{PE}}}) + d\log_2(m+1)}{m}}$, where $d = 2$ is set due to the positive operator valued measure with two outcomes. These expressions are used to form an upper limit, Q^u, to Q that is used in determining the final key length. In many QKD variants this takes the simple form $Q^u = Q + \xi$. In more simpler terms, we can set an upper limit to what we think the true QBER, $\hat{Q}$, is and then determine the probability that this upper bound does not encompass $\hat{Q}$. For our protocol implementation, we use a similar analysis to [32] but with equal probability for each basis usage. Parameter estimation from individual bases was investigated, but in our experiments the QBER from each basis was found to be the same.

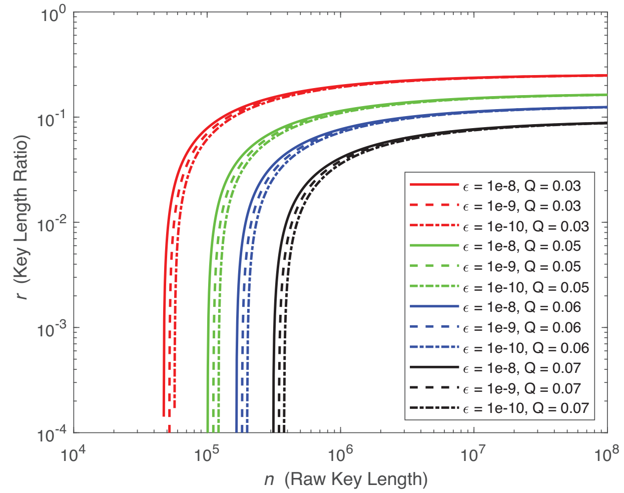

Figure B1. The ratio of key lengths, r, versus the raw key length, n, for different security levels and different Q values. Here, the number of bits used for parameter estimation, m, is set at $m = n$.

All of the above discussion leads us to a relation for r given by [27,44,46]

$$r = \frac{s_{\text{final}}}{n} = A\left(1 - h\left(\frac{Q^u}{A}\right)\right) - (1 - R_c) - \Delta(n) \tag{B1}$$

where $A = \frac{p_{\text{det}} - P_{\text{m}}}{p_{\text{det}}}$, is the correction term due to the multi-photon emission at the single-photon source. In this latter relation, p_{det} is the probability of detecting at least one photon, P_{m} is the probability of multi-photon emission at the source. We obtain a determination of A from a direct measurement of the ratio of $P_m/p_{\text{det}} = 0.015$, leading to $A = 0.985$.

In Equation (B1), $h(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$ is the binary entropy function, and $\Delta(n)$ is an additional penalty term given by

$$\Delta(n) = \frac{7n\sqrt{\frac{1}{n}\log_2\frac{2}{\tilde{\varepsilon}}} + 2\log_2\frac{1}{\varepsilon_{\text{PA}}} + \log_2\frac{2}{\varepsilon_{\text{EC}}}}{n} \tag{B2}$$

We use the term $(1 - R_c)$ to compute the fraction of information leakage during reconciliation instead of the commonly used term $f_{\text{E}}h(Q)$, where f_{E} is the reconciliation efficiency. Noting that only the syndrome bits are disclosed during reconciliation, this efficiency can be written[47] $f_{\text{E}} = \frac{s_B}{nh(Q)} = \frac{1-R_c}{h(Q)}$, since $\frac{n-s_B}{n} = R_c$ holds for a given LDPC matrix.

In the main text we investigated the achievable r with respect to $\varepsilon = 10^{-10}$ with the results reflected in the main text. In all our reported secret key rates, we have set $m = n = 10^6$ to ensure a non-zero secret key rate at our required security level.

We note that our achievable r is a lower bound and can be further improved by optimizing some of the parameters (e.g., $\tilde{\varepsilon}$) under defined constraints on the probabilities. Such optimization was not carried out in our results. We have fixed $\tilde{\varepsilon} = \varepsilon_{\text{PA}} = \varepsilon_{\text{EC}} = \varepsilon_{\text{PE}} = \frac{\varepsilon}{4}$. Typical examples of r as a function of n are shown in **Figure** B1.

Although an emphasis was put on the inclusion of all known effects impacting the derived security level, we do remind the reader that all BB84 implementations come with a host of assumptions on the anticipated behavior of devices, including the lack of side-channel attacks. That is, BB84 security is device-dependent. The ultimate QKD security, achievable via device-independent QKD, requires entangled photon sources and measurements of Bell violations.

We close by outlining how our privacy amplification is actually implemented.

- **Step 1: Calculating** r. Alice uses Equations B1 and B2 to obtain r based on Q, ε, $\tilde{\varepsilon}$, $\varepsilon_{\mathrm{PA}}$, $\varepsilon_{\mathrm{EC}}$, $\varepsilon_{\mathrm{PE}}$, n, and m.
- **Step 2: Creating the hash function**. Following the procedure described in Section II.E of [48], Alice creates a Toeplitz matrix, $\mathbf{T}$, with n columns and $\lfloor rn \rfloor$ rows, where $\lfloor \cdot \rfloor$ is the floor operation. Alice sends $\mathbf{T}$ to Bob.
- **Step 3: Secure hashing**. Alice and Bob apply $\mathbf{T}$ to $\hat{K}_{\mathrm{A}}$ and K_{B}, respectively, and obtain two identical and secure key strings for cryptography purposes. [At some points, an a priori secret key will be consumed by Alice and Bob for authentication before the use of any key to encrypt/decrypt classical messages - we assume that such authentication is completed successfully.] A final check (hash) is taken on some small part of the keys to check the keys are identical - if they are not the protocol is aborted.

Acknowledgements

A.A.-J. and H.Z.J.Z. contributed equally to this work. The authors thank Timm Kupko, Tobias Heindel, Oliver Benson, Esteban Gómez-López, Çağglar Samaner, Serkan Ateş, Maja Colautti, and Francois Ladouceur for useful discussions. The authors also thank Rich Mildren and Adam Bennett for the initial assistance of the source integration. This work was supported by the Australian Research Council (CE200100010), and the Office of Naval Research Global (N62909-22-1-2028). The authors thank the NSW Defence Innovation Network, the NSW State Government, and the Next Generation Technologies Fund for financial support of this project funded by the DIN Strategic Investment Initiative. Lastly, the authors thank the two anonymous referees for their helpful comments that improved the quality of the manuscript.

Open access publishing facilitated by University of New South Wales, as part of the Wiley - University of New South Wales agreement via the Council of Australian University Librarians.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Keywords

BB84, hexagonal boron nitride, quantum key distribution, single photon

Received: February 13, 2023
Revised: June 11, 2023
Published online: June 22, 2023

[1] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, *npj Quantum Inf.* **2016**, *2*, 1.
[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, *Rev. Mod. Phys.* **2020**, *92*, 025002.
[3] D. A. Vajner, L. Rickert, T. Gao, K. Kaymazlar, T. Heindel, *Adv. Quantum Technol.* **2022**, *5*, 2100116.
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.
[5] C. H. Bennett, G. Brassard, *Theor. Comput. Sci.* **2014**, *560*, 7.
[6] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, J.-W. Pan, *Nature* **2020**, *582*, 501.
[7] F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, R. Trotta, *Sci. Adv.* **2021**, *7*, eabe6379.
[8] C. Schimpf, M. Reindl, D. Huber, B. Lehner, S. F. Covre Da Silva, S. Manna, M. Vyvlecka, P. Walther, A. Rastelli, *Sci. Adv.* **2021**, *7*, eabe8905.
[9] F. Basso Basset, M. Valeri, J. Neuwirth, E. Polino, M. B. Rota, D. Poderini, C. Pardo, G. Rodari, E. Roccia, S. Covre da Silva, G. Ronco, N. Spagnolo, A. Rastelli, G. Carvacho, F. Sciarrino, R. Trotta, *Quantum Sci. Technol.* **2022**, *8*, 025002.
[10] H.-K. Lo, M. Curty, B. Qi, *Phys. Rev. Lett.* **2012**, *108*, 130503.
[11] M. Bashar, M. Chowdhury, R. Islam, M. Rahman, S. Das, in *2009 International Conference on Computer and Automation Engineering*. IEEE, Bangkok **2009**.
[12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu et al, *Nature* **2017**, *549*, 43.
[13] X. Ma, H.-K. Lo, *New J. Phys.* **2008**, *10*, 073018.
[14] T. Kupko, M. von Helversen, L. Rickert, J.-H. Schulze, A. Strittmatter, M. Gschrey, S. Rodt, S. Reitzenstein, T. Heindel, *npj Quantum Inf.* **2020**, *6*, 29.
[15] P. Senellart, G. Solomon, A. White, *Nat. Nanotechnol.* **2017**, *12*, 1026.
[16] I. Aharonovich, D. Englund, M. Toth, *Nat. Photonics* **2016**, *10*, 631.
[17] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, Y. Yamamoto, *Nature* **2002**, *420*, 762.
[18] T. Heindel, C. A. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W.-M. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth, M. Lermer, H. Weier, M. Jetter, M. Kamp, S. Reitzenstein, S. Höfling, P. Michler, H. Weinfurter, A. Forchel, *New J. Phys.* **2012**, *14*, 083001.
[19] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, Y. Arakawa, *Sci. Rep.* **2015**, *5*, 14383.
[20] C. L. Morrison, R. G. Pousa, F. Graffitti, Z. X. Koong, P. Barrow, N. G. Stoltz, D. Bouwmeester, J. Jeffers, D. K. Oi, B. D. Gerardot, A. Fedrizzi, *arXiv preprint c* **2022**.
[21] M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler, P. Walther, *npj Quantum Inf.* **2022**, *8*, 104.
[22] Ç. Samaner, S. Paçal, G. Mutlu, K. Uyanık, S. Ateş, *Adv. Quantum Technol.* **2022**, *5*, 2200059.
[23] M. Leifgen, T. Schröder, F. Gädeke, R. Riemann, V. Métillon, E. Neu, C. Hepp, C. Arend, C. Becher, K. Lauritsen, O. Benson, *New J. Phys.* **2014**, *16*, 023021.
[24] N. L. Piparo, M. Razavi, W. J. Munro, *Phys. Rev. A* **2017**, *95*, 022338.
[25] G. Murtaza, M. Colautti, M. Hilke, P. Lombardi, F. S. Cataliotti, A. Zavatta, D. Bacco, C. Toninelli, *Opt. Express* **2023**, *31*, 9437.
[26] I. Aharonovich, J.-P. Tetienne, M. Toth, *Nano Lett.* **2022**, *22*, 9227.
[27] H. Z. J. Zeng, M. A. P. Ngyuen, X. Ai, A. Bennet, A. S. Solnstev, A. Laucht, A. Al-Juboori, M. Toth, R. P. Mildren, R. Malaney, I. Aharonovich, *Opt. Lett.* **2022**, *47*, 1673.
[28] X.-W. Chen, S. Götzinger, V. Sandoghdar, *Opt. Lett.* **2011**, *36*, 3545.
[29] L. Sortino, P. G. Zotev, C. L. Phillips, A. J. Brash, J. Cambiasso, E. Marensi, A. M. Fox, S. A. Maier, R. Sapienza, A. I. Tartakovskii, *Nat. Commun.* **2021**, *12*, 6063.
[30] The random number generation happens in software. In an actual deployment this software implementation will be replaced by an embedded quantum random number generator.
[31] V. Scarani, R. Renner, *Phys. Rev. Lett.* **2008**, *100*, 200501.
[32] R. Y. Cai, V. Scarani, *New J. Phys.* **2009**, *11*, 045024.
[33] P. Chaiwongkhot, S. Sajeed, L. Lydersen, V. Makarov, *Quantum Sci. Technol.* **2017**, *2*, 044003.
[34] M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, M. Kamp, A. Forchel, S. Höfling, H. Weinfurter, *New J. Phys.* **2014**, *16*, 043003.

[35] M. Zahidy, M. T. Mikkelsen, R. Müller, B. Da Lio, M. Krehbiel, Y. Wang, M. Galili, S. Forchhammer, P. Lodahl, L. K. Oxenløwe, D. Bacco, L. Midolo, *arXiv preprint arXiv:2301.09399* **2023**.

[36] T. Gao, L. Rickert, F. Urban, J. Große, N. Srocka, S. Rodt, A. Musiał, K. Żołnacz, P. Mergo, K. Dybka, W. Urbańczyk, G. Sęk, S. Burger, S. Reitzenstein, T. Heindel, *Appl. Phys. Rev.* **2022**, *9*, 011412.

[37] P. Grünwald, *New J. Phys.* **2019**, *21*, 093003.

[38] J. R. Chavez-Mackay, P. Grünwald, B. M. Rodríguez-Lara, *Phys. Rev. A* **2020**, *101*, 053815.

[39] Y. Guo, C. Gao, D. Jiang, L. Chen, *SN Comput. Sci.* **2021**, *2*, 1.

[40] T. J. Richardson, M. A. Shokrollahi, R. L. Urbanke, *IEEE Trans. Inf. Theory* **2001**, *47*, 619.

[41] D. Elkouss, A. Leverrier, R. Alléaume, J. J. Boutros, in *Proceedings of IEEE International Symposium on Information Theory*. IEEE, Finland **2009**, pp. 1879–1883.

[42] X.-Y. Hu, E. Eleftheriou, D.-M. Arnold, *IEEE Trans. Inf. Theory* **2005**, *51*, 386.

[43] E. Sharon, S. Litsyn, J. Goldberger, *IEEE Trans. Inf. Theory* **2007**, *53*, 4076.

[44] P. Chaiwongkhot, S. Hosseini, A. Ahmadi, B. L. Higgins, D. Dalacu, P. J. Poole, R. L. Williams, M. E. Reimer, T. Jennewein, *arXiv preprint arXiv:2009.11818* **2020**.

[45] D. Bunandar, L. C. G. Govia, H. Krovi, D. Englund, *npj Quantum Inf.* **2020**, *6*, 104.

[46] A typographical error in [44] (and carried over into [27]) is corrected for here.

[47] D. Elkouss, J. Martinez-Mateo, V. Martin, *Quantum Inf. Comput.* **2011**, *11*, 0226.

[48] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, T. Jennewein, *Phys. Rev. A* **2015**, *92*, 5.