Lowndes et al. *EPJ Quantum Technology* (2021) 8:15
https://doi.org/10.1140/epjqt/s40507-021-00101-2

EPJ Quantum Technology
a SpringerOpen Journal

LETTER Open Access

A low cost, short range quantum key distribution system

David Lowndes[1*], Stefan Frick[2], Andy Hart[1] and John Rarity[1]

*Correspondence:
david.lowndes@bristol.ac.uk
[1]Department of Electrical and Electronic Engineering, University of Bristol, Woodland Road, BS8 1UB, Bristol, UK
Full list of author information is available at the end of the article

Abstract

We present a miniaturized quantum key distribution system, designed to augment the more mature quantum key distribution systems currently commercially available. Our device is designed for the consumer market, and so size, weight and power are more important than raw performance. To achieve our form factor, the transmitter is handheld and the receiver is a larger fixed terminal. We envisage users would bring their transmitters to centrally located receivers and exchange keys which they could use at a later point. Transmitting qubits at 80 MHz, the peak key rate is in excess of 20 kbps. The transmitter device fits within an envelope of <150 ml, weighs 65 g and consumes 3.15 W of power.

Keywords: Quantum key distribution; Quantum cryptography; Quantum technology; Optics; Security

1 Introduction

The majority of current research in the field of quantum key distribution (QKD) focuses on either commercializing high speed fibre systems in networks [1–4] or long distance free space links to satellites [5–9]. A combination of these services will form the backbone of a global "Quantum Internet" [10] but this does not address access to this network for end-users. We propose small handheld devices which could be brought to a terminal, co-located with a quantum network node to top up a secret key store which could then be used to encrypt day-to-day activity on conventional platforms such as the internet. We are calling these terminals Quantum ATMs (QATMs). The requirements of the mass consumer market places a greater constraint on cost with a relatively low demand for key rate meaning that these handheld devices need not have state of the art performance, and as such can achieve drastic reductions in size, weight and power (SWaP) over other QKD systems.

The QATM concept also helps the SWaP reduction of the consumer devices by not having to be too concerned with the SWaP of the QATM itself. In our case, it makes most sense to place the receiver (Bob) in the QATM due to the relative difficulty in detecting single photon level signals compared to producing them. We will show later (Sect. 4.2) that the majority of the data post-processing can be performed on the QATM as well, so there is minimal requirement for computing hardware in the handheld device.

The design goal for the consumer QKD device is to produce a minimal device such that it could be made cheaply enough to be distributed widely, possibly by banks (like the chip and pin CAP readers) or even integrated into an existing consumer device (such as a mobile phone). These examples provide a good starting point to define our SWaP restrictions, namely that the devices should be approximately the size of a CAP reader (80 mm × 60 mm × 10 mm) [11], weigh no more than a mobile phone (<150 g) [12] and require only as much power as could be provided by a typical smartphone (≈2.5 W) [12].

2 Transmitter

2.1 Optics

Given that true on-demand deterministic single photon sources [13] are currently not sufficiently practical for a consumer device, it is clear that for now, the weak coherent pulse (WCP) method [14, 15] of approximating a single photon source is the best method for producing a low SWaP QKD transmitter. Given the SWaP reduction philosophy of this system, it was decided that the WCP source should use LEDs (LA HR070EP1, λ = 650 nm), rather than laser diodes. Although LEDs have limitations in electrical bandwidth compared with laser diodes, they have the advantage of not needing to be temperature stabilized [16], being inherently less polarized and not having a threshold current. The wide spectral bandwidth makes matching multiple sources to make them indistinguishable relatively easy using narrow band interference filters, ensuring security. This process is shown in Fig. 1, showing the spectra of the four LEDs in the transmitter, before and after filtering with a Thorlabs FBH650-10 bandpass filter. Comparing the maximum and minimum values of the spectra at each point gives an improvement of the correlation coefficient from 99.88% to 99.96%, and more importantly removes the features in the spectrum far from the peak (such as at ≈630 nm) which contain the majority of the variance between the LEDs.

The protocol chosen for this system is polarization encoded BB84. Polarization encoding was chosen since generation and detection can both be performed by passively combining and splitting the light using polarization sensitive components whereas encodings such as time-bin and phase require active modulation, high bandwidth pulse shaping [17] or interferometry which are not compatible with our low SWaP philosophy. BB84 is em-

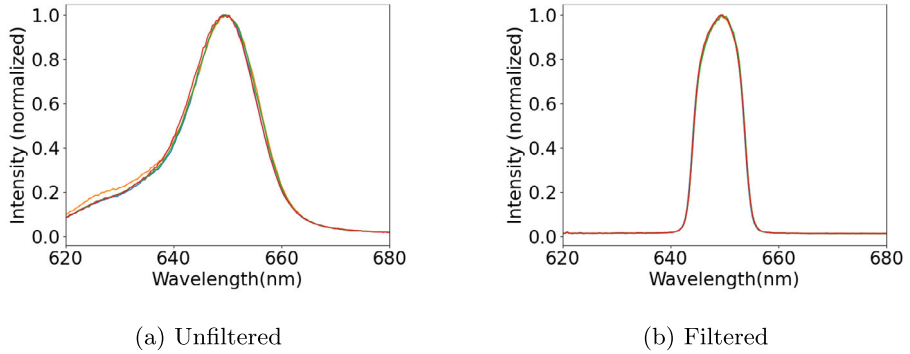


Figure 1 Spectra of the LEDs in the transmitter, before (a) and after (b) a Thorlabs FBH650-10 bandpass filter. The figure shows a narrow range to make the differences between the spectra clearer

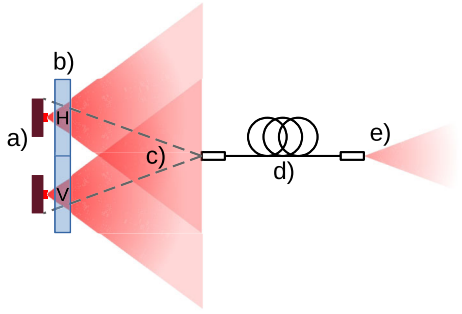
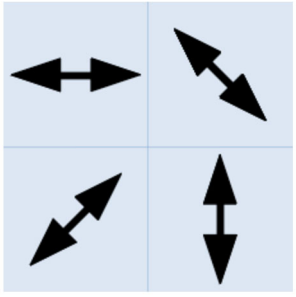


Figure 2 The scheme of combining multiple sources into one spatial mode. The LEDs (a) are individually polarized by a patterned polarizer (b). The LEDs are placed closely so their emission cones overlap and an optical fibre is placed such that its NA overlaps the LEDs (c). The fibre is bent to remove cladding modes (d) and the fibre output is single moded (e)

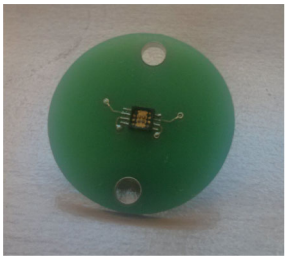
Figure 3 The regions of the patterned polarizer. The dimensions of our polarizer are 3 × 3 mm, with a 50 μm undefined region between sections. The polarization contrast was specified as approximately 200:1



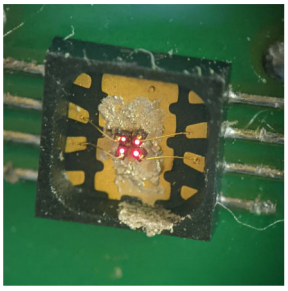
ployed due to its simplicity, and due to the low loss regime we are operating in, many of the more complex protocols do not provide much of a benefit to performance.

As mentioned above, using active modulation of the photons to produce the states was dismissed on all three SWaP criteria. Instead four separate sources are polarized in their respective BB84 polarizations and combined. This has previously been done with diffraction gratings [18], mirrors [19], beamsplitters [20, 21] and waveguides [22]. In the interest of reducing the cost as much as possible our device uses, a short single mode fibre (SMF) (Thorlabs SM600), positioned to collect equal amounts of light from each source (Fig. 2), this has the additional benefit of ensuring that the output from the device is single moded, an important criterion for indistinguishability. A drawback of this method is that due to birefringence, SMF is not polarization maintaining and the polarizations will be rotated. This rotation is, however a unitary process so it can be corrected using an appropriate selection of wave plates. The requirement for extra wave plates is acceptable for our application as these can be placed in the QATM, therefore not increasing the SWaP of our transmitter.

Given the small NA of our single mode fibre [23] (NA = 0.1), to maximize coupling from the device, the LEDs need to be closely spaced. For this an LED package was assembled placing a 2 × 2 grid of LEDs in a chip carrier with 300 μm spacing (Fig. 4. This allows for a minimum fibre-LED distance of 3 mm. A custom glass polarizer was commissioned (Codixx Colorpol) with linear polarization regions corresponding to the LED positions (Fig. 3), this was glued to the package which also served as a protective window over the LED dies.



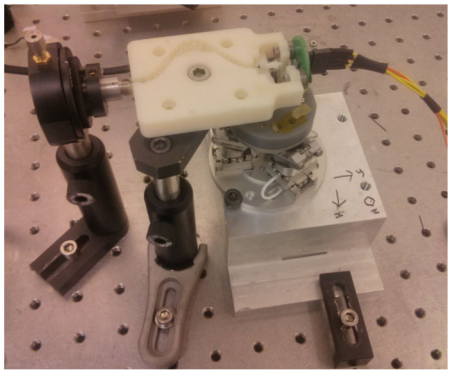
(a) On a 1 inch diameter PCB.



(b) LEDs lit in the package.

Figure 4 The LED package, with the polarizer removed to show the LEDs

Figure 5 Assembly apparatus for the transmitter. An optical fibre is glued into a channel in the transmitter body with an unglued length facing the LEDs. The unglued ferrule is connected to a six axis stage (SmarAct SMARPOD 70.42) which scans the fibre position across the LEDs to find the optimal position. The ferrule is then glued to the transmitter body in this position and its connection to the stage is severed



Using the apparatus shown in Fig. 5, the fibre position was scanned (in 100 μm steps) in front of the LEDs to find the best position to collect the maximum amount of light with high degree of polarization.

Figure 6(a) shows the total counts received as the fibre is scanned across the LEDs. There are four overlapping peaks corresponding to slightly different points for maximum light collection from each LED. Mostly this step is used to ensure that the LEDs are relatively centred in the scan area and as corroboration for the later steps.

Figure 6(b) shows the same data as Fig. 6(a), but only for the weakest coupled of the LEDs at each position. The peak occurs at the point corresponding to the middle of the LEDs where there is an amount of light coupled from each LED large enough to ensure WCP with a mean photon number compatible with QKD.

Figure 6(c) shows the ratio of the brightest to the dimmest LED at each position. Ideally at some position, this value would be unity, showing equal coupling between all LEDs. This is similar to Fig. 6(b) but shows a better idea of the balance between the LED brightnesses.

The peaks at Fig. 6(b) and 6(c) are at the same position. Qualitatively, this position is also inside the square defined by the four peaks in 6(a), as expected. The fibre was then glued in this optimum position using low shrinkage UV cured adhesive (Norland NOA63).

2.2 Electronics

As the aim of this work is to build a fully functioning low SWaP QKD system, the control electronics must also adhere to that philosophy and hence the transmitter electronics is a

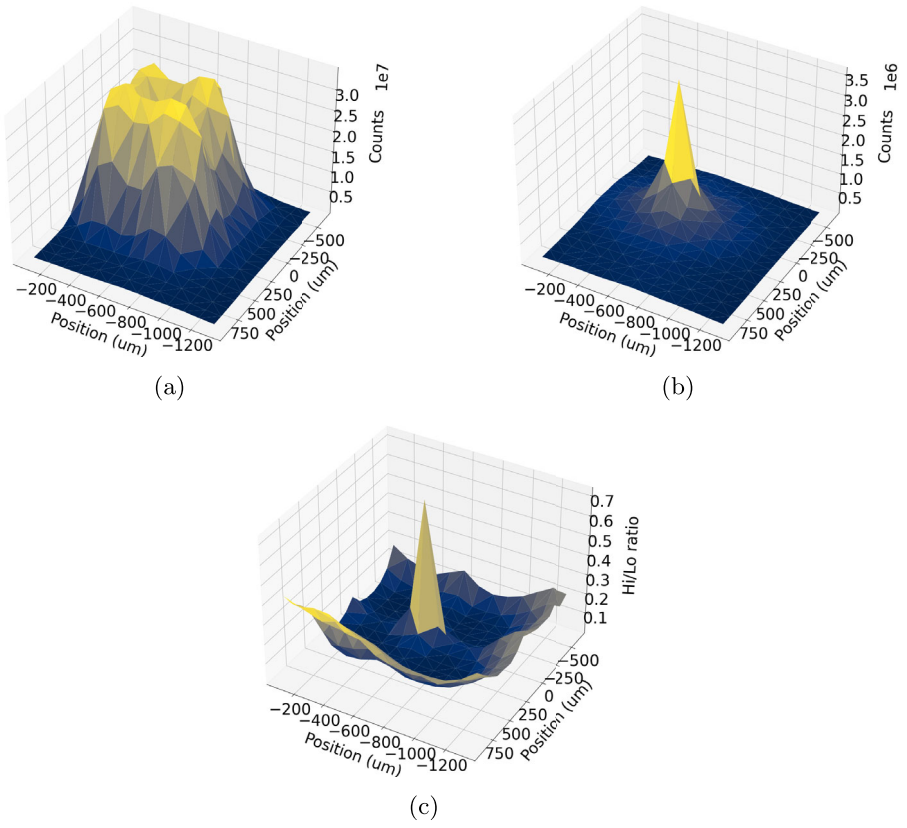
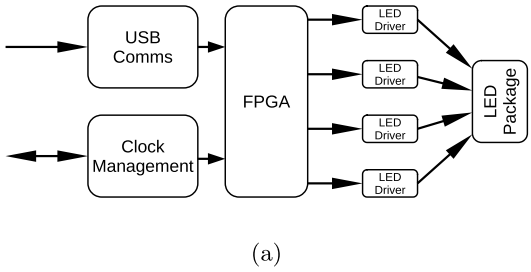


Figure 6 Measured photo-counts when the source is scanned in 100 μm increments over various launch positions using the apparatus shown in Fig. 5(a): Total counts at each scan position. (b): Counts at each scan position only of the dimmest LED at that position. (c): The ratio between the brightest and dimmest LED at each position

bus powered USB device. USB is a ubiquitous communications protocol which provides a simple interface to many consumer devices such as to a mobile phone via USB on-the-go (OTG). The electronics module does not store or generate any random data, instead it takes a stream of bits sent over USB, converts each byte into four qubit values (using one bit to encode the basis and one to encode the bit value) and based on this value pulses one of the four LEDs per clock cycle. A block diagram and photograph of the device is shown in Fig. 7.

The LED driving is performed by commercial laser driver chips (TI ONET1101L), this allows for fine control of parameters such as drive current and biasing of the LEDs. An FPGA (Xilinx Spartan 6) performs the demultiplexing of the data stream sent over USB and also controls routing of any configuration messages for the driver chips. The FPGA output is amplified by the driver chips and used to drive the four LEDs with a maximum pulse frequency of 80 MHz. Pulse width is configurable with a resolution of 1ns which allows for control of the optical pulse width. A USB chip (Cypress EZ-USB FX2) is used for communication with the host controller and is also used to program the FPGA configuration memory on power up, eliminating the need for the additional cost of external flash memory.

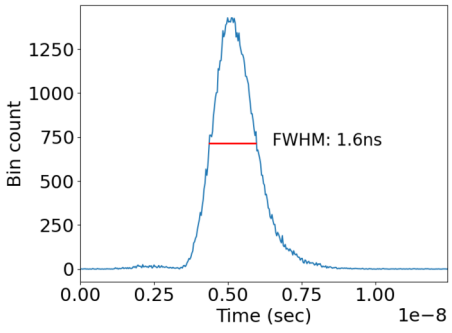


(a)

(b)

Figure 7 (a): Block diagram of the transmitter electronics. (b): The transmitter electronics with credit card for size comparison

Figure 8 The optical pulse width of an LED being driven by the electronics module



The FPGA clock is provided by a 100 MHz oven controlled crystal oscillator (OCXO) or from an external clock input if synchronisation to other devices is required. Additionally the FPGA generates a 10 MHz output derived from the OCXO, to allow optional external synchronisation. This 10 MHz output was connected to a Picoquant Picoharp300 to perform a time correlated single photon counting (TCSPC) measurement to determine the optical pulse with of the LEDs shown in Fig. 8. The FWHM pulse width was measured to be 1.6 ns from a 1 ns driving pulse from the FPGA. The drive pulse width of 1 ns was the shortest achievable with our current electronics design.

The current bill of materials for circuits and optics is below £500 and for large scale deployment one would certainly design bespoke optics and application specific integrated circuits (ASICs), which would dramatically decrease the cost per unit.

3 Receiver

The optics in the QATM comprise the standard beamsplitter design, using beamsplitters (BSs) (for passive basis choice) and polarizing beam splitters (PBSs) (for basis measurement) [24]. Even though this system uses the BB84 protocol, measuring in the rectilinear (H/V) and diagonal (D/A) bases, this receiver also measures in the circular basis (R/L) - this is to characterize the birefringence in the transmitter mentioned in Sect. 2.1, a schematic and photograph is shown in Fig. 9. Using all three bases allows measurement of the full Stokes parameters of the incoming light and from this the waveplate correction angles can be found using Mueller calculus. This does have an impact on the QKD rate, since during the transmission R/L detections do not contribute to the key, however the

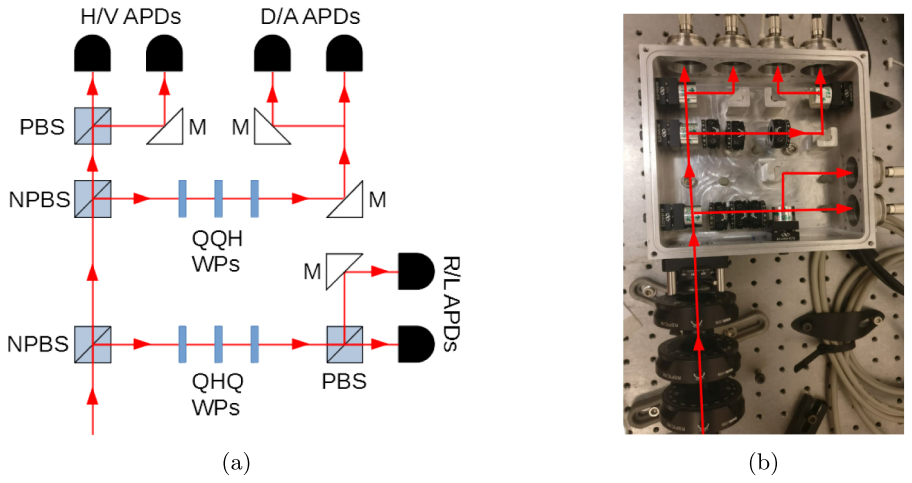


Figure 9 The six state QKD receiver, (a) shows a schematic of the layout, including the fold mirrors to ensure the output ports are on the perimeter of the optics box. (b) shows the actual device, with the optical path superimposed. Note the beamsplitters are all on tip/tilt stages (Newport MM-075-HEX-M), to allow for fine corrections to alignment

fraction diverted to this channel can be minimized using an appropriately chosen asymmetric BS. Each of the six outputs from the optics is coupled into an optical fibre (Thorlabs M43L01) to deliver the light to single photon avalanche diodes (SPADs) (2× Excelitas SPCM-AQ4C).

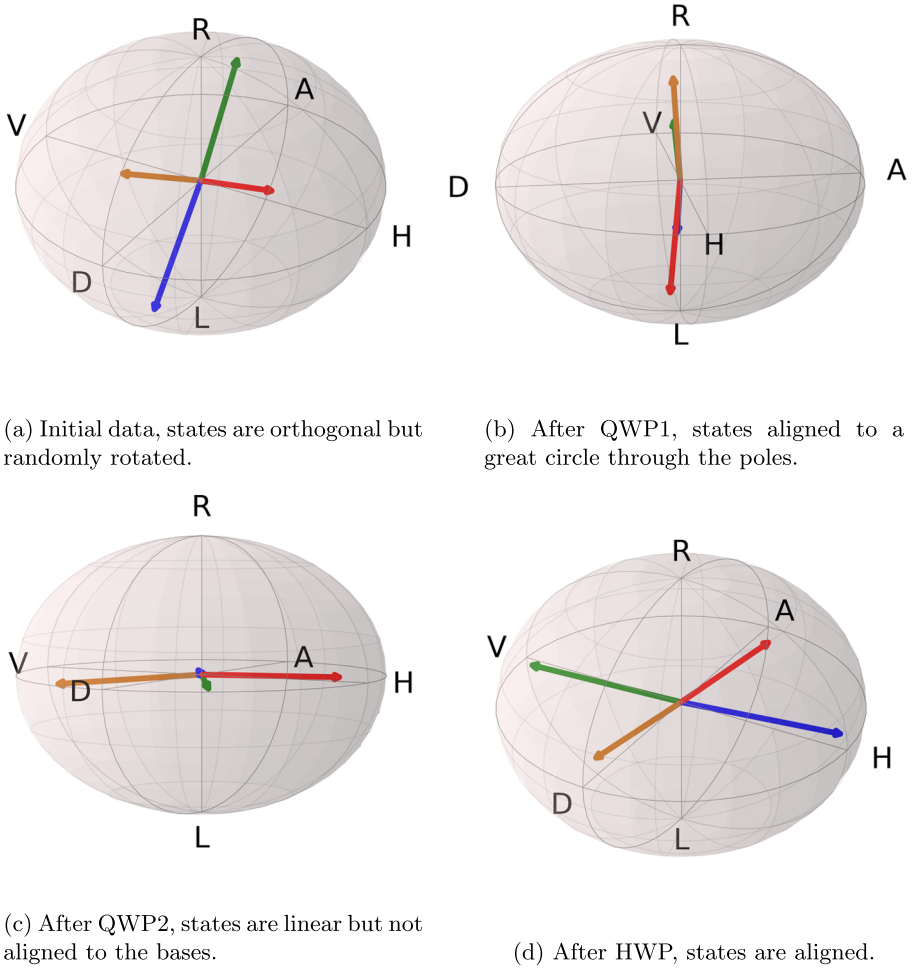
There exists many methods for aligning optical channels, previously we have used kinematic magnetic mounts (Newport M-BK-2A) [25] but these were large and unwieldy. Active beamsteering [20, 26] is a compelling addition to the system but it adds extra complexity for an initial prototype device. For system simplicity, a 3D printed dock was designed. The transmitter fibre output ferrule protrudes from the device and is guided by the dock into a fixed focus collimator, pre-aligned with the receiver optics. Between the dock and detector optics is a stack of three waveplates (2× Thorlabs WPQ05M-633, 1× WPH05M-633) in motorized rotation mounts (Thorlabs DDR25), which perform on-demand correction of the transmitter birefringence.

The electronic pulses from the SPADs are connected to individual channels on a time tagger developed in house at the University of Bristol with a resolution of ≈50 ps and a maximal event rate of ≈1 MHz [27]. The time tagger digitizes the pulse arrival times for processing by a computer. The computer processes the received data and performs the calibration and key distillation.

4 System operation

4.1 Calibration

Before the QKD process can begin, the bases of the transmitter and receiver must be aligned. This process is performed by the transmitter lighting each LED in turn and the receiver measuring count rates in each detector for each LED. The ratio of counts in each basis is used to calculate the $S_{1,2,3}$ parameters of the Stokes vectors for each LED. Using the process of [28], the waveplate angles θ_{Q1}, θ_{Q2}, θ_H are calculated and applied, the intermediate steps of this process are shown in Fig. 10.



(a) Initial data, states are orthogonal but randomly rotated.

(b) After QWP1, states aligned to a great circle through the poles.

(c) After QWP2, states are linear but not aligned to the bases.

(d) After HWP, states are aligned.

Figure 10 The intermediate steps of correcting for fibre birefringence using quarter, quarter, half (QQH) wave plates. In this example, angles for the QQH wave plates were 66.2°, 40.6°, 77.2°, respectively. Using Mueller matrices of polarizers, a predicted error rate of 5.6% is obtained. This is an upper limit. When we confine ourselves to measurements in the equatorial plane (V/H;D/A), and include postprocessing, a lower error rate is measured (see Sect. 5)

To collect the data shown in Fig. 10, one second of counts in the six channels of the receiver was collected for each LED, with 0.5 second blank periods between to ensure no crosstalk between LEDs. Calculating the waveplate angles took 4.5 seconds and the waveplates set in less than 0.5 seconds. The total time for this process was 11 seconds.

While fibre birefringence is dependent on environmental conditions such as temperature [29], over the time scale of a QKD transmission, they are stable and this correction does not have to be carried out live. However, if QKD data processing could be performed in real time, an alternative calibration method could be used in which the transmitter simply starts transmitting QKD data and the receiver uses this data to work out the calibration angles, the receiver would then simply ignore the detections from before the system was adequately calibrated. This has been shown in [30] to only require a small number of detections. Another advantage of doing live calibration is that if the docking method of establishing the channel is replaced with an actively tracked method, the half wave plate could be used to compensate the rotation of the transmitter. Given our philosophy of re-

ducing complexity in the transmitter, this method of compensating rotation is preferable to using other methods, such as the RFI protocol [31], which would require adding extra channels into the transmitter. There is no theoretical issue with implementing a real-time correction although the increased interactivity between processing algorithms and control logic will require careful implementation to ensure smooth operation of both.

4.2 Data processing

4.2.1 Transmission isolation

To ensure the full transmission is collected by the receiver, the protocol requires that the receiver turns on their detectors before the transmitter starts sending photons and waits for the transmitter to declare they have finished sending photons before turning off the detectors. There is no high accuracy time synchronization between the devices however, so the first step in the processing is for the receiver to isolate the transmission in their received data stream. This is simply performed by examining the differences between successive time tags and observing where the intervals get smaller, indicating an increased count rate, this process can identify the start detection to approximately 10^3 clock cycles.

4.2.2 Clock synchronization

There is no shared clock reference between the transmitter and receiver, so small discrepancies in the on-board clocks of both devices will quickly cause the devices to desynchronize. To resolve this, the receiver reconstructs the transmitter clock by using the nominal rate (100 MHz in this case) as an initial value for the transmission frequency and refining this by processing the detections.

If the exact clock period is known, the received time tags can be divided modulo the clock period and plotted on a histogram to produce a peak (this is a variation on time correlated single photon counting — where the clock signal is exchanged using a wire — as such these histograms will be referred to TCSPC histograms). If the clock period guess is wrong, there will be no correlation and the histogram will be flat. Critically, over a short time scale, a slightly incorrect clock period will just lead to a widening of the histogram peak. This means that a guess can be refined by applying small adjustments $\pm$ from the guess and observing the peak width, as in Fig. 11(a). The histogram peak for 5 ms of received data is shown in Fig. 11(b). Performing a high resolution search here would be time

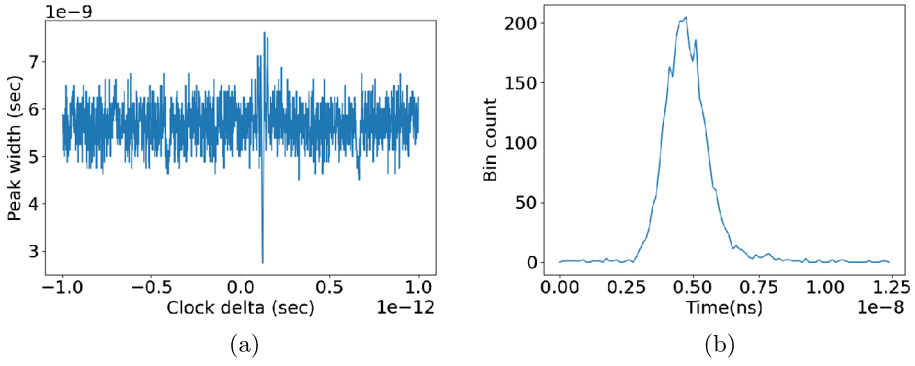


Figure 11 (a): The width of a TCSPC histogram peak as the clock period guess (12.5 ns) is varied by some delta. (b): The TCSPC histogram at the best delta value (narrowest peak)

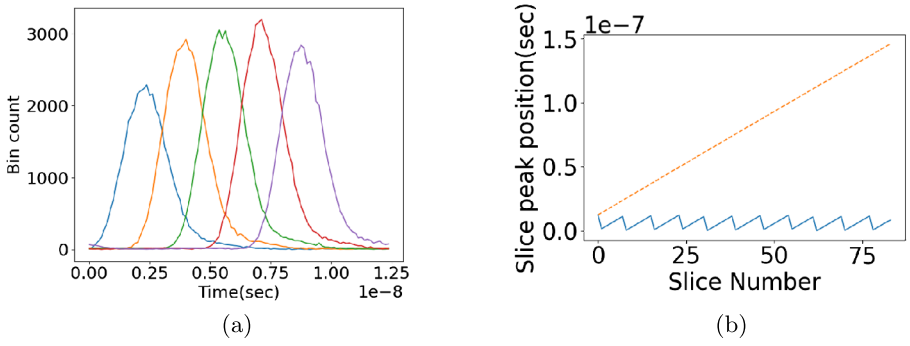


Figure 12 (a): The first 5 TCSPC histograms of subsequent 20ms time slices of data. (b): The position of the peaks of all of the 20ms slices (blue, solid) and the same data corrected for the "wrapping" around of the histograms as they under/over flow around the x axis of figure (a) (orange, dashed). The gradient of this line gives the discrepancy between the guessed clock and the actual clock

consuming so a coarser search is performed, refining the guess only enough to perform the next step.

Following this bruteforce clock search, the clock drift is small enough to observe by plotting TCSPC histograms for subsequent small time slices of the data. Figure 12(a) shows the first 5, 20 ms slices which can be seen to "drift" along the x-axis, showing the clocks are not perfectly synchronized. This drift can be quantified by plotting the progression of the histogram peaks along the x-axis (Fig. 12(b), blue). The peak positions "wrap" around the x-axis so this must be corrected by adding/subtracting a clock period at the discontinuities.

If the clock drift trend (Fig. 12(b), orange), is constant, the gradient of the line can be used to correct an offset factor to correct all the received time tags to synchronize them. If the trend is not constant, the time tags in each received slice can be corrected by subtracting that slice's peak position (Fig. 12(b)'s y axis). This is not as accurate since it does not take the exact position of a time tag in the slice into account but it allows this method to be used in a wider range of circumstances.

4.2.3 Gating and reconciliation

The tags are then divided modulo the recovered clock period (Fig. 13(a), and any detections with a remainder outside of the peak are discarded as these do not correspond to photons emitted by the transmitter. The quotient of the division is retained as a pulse number corresponding to the Nth transmitted photon ($\pm$ K, an integer offset). The offset (K) is then found during reconciliation, where the transmitter sends a subset of their transmitted bits and the receiver tries to correlate it to their received data for varying offset values. Invalid K-values will produce uncorrelated results (error rate 50%) but one value will yield an acceptable error rate which can then be used to generate key (Fig. 13(b)).

The gating process can also be used to estimate the temporal matching of the sources from the transmitter. By using one of the R/L channels in the receiver, where the collection from all the transmitted polarizations is equal, separate gating histograms can be plotted, observing the difference between their peaks. Since this is from one detector in the receiver, there is no effect of the receiver on the timing. Making this measurement optically is also preferred over measuring the logic pulses from the FPGA since it is the temporal matching of the optical pulses which is most important.

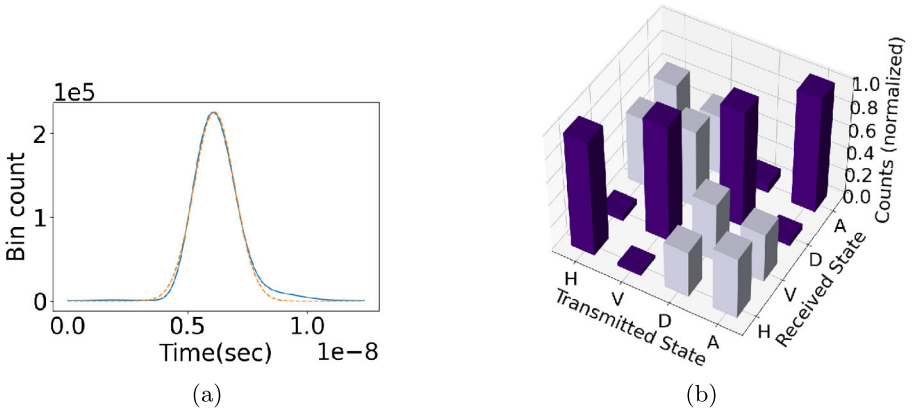
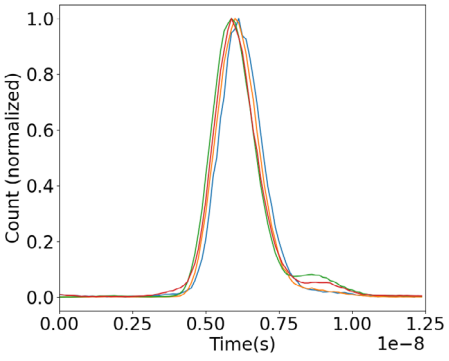


Figure 13 (a): The TCSPC histogram of all 1.6 seconds of data once clocks are synchronized (blue, solid), and a Gaussian fit (orange, dashed) of the data confirming the peak is approximately Gaussian (assumed by the processing algorithms). (b): Extinction matrix showing the states received compared to the states transmitted. The situations where the bases do not match, coloured grey, are discarded by the algorithm and do not contribute to the key or the error rate. The bars representing the unmatched bases should all have equal height (0.5 in this normalized figure), we suspect the slight deviation here represents a small misalignment in the angle between the H/V and D/A bases



Channel	Peak position (ns)	Offset from H (ps)
H	6.18	0
V	6.06	120
D	5.91	270
A	5.98	200

Figure 14 TCSPC histograms of counts made in the right circular channel by the H, V, D, A sources in the transmitter. Peak position can be used to estimate temporal distinguishablity of the sources. Peak positions and their distance from an arbitrary channel (H) are shown in the table

Figure 14 shows that at maximum the photons are 270 ps from perfectly overlapped, ideally this would be corrected in the FPGA by adding delays to the relevant channels. Unfortunately this functionality is not working as intended in the device as described in Sect. 2.2, but will be designed in to the next generation transmitter electronics that will replace this. This process also shows some sources have a small secondary pulse after the

main pulse which is obviously harmful to temporal indistinguishability. This will be solved with more sophisticated driving electronics in future iterations.

5 Results

To test the system performance thoroughly, the QKD process was repeated many times with varying levels of background light, provided by a daylight simulating alarm clock (Lumie Bodyclock Glow 150). This was set to go from full brightness to off in 45 minutes, corresponding to approximately 150 QKD data collections. Figure 15 shows the error rate and predicted secret key rate over this period (for now, using the asymptotic regime [14, 32] for simplicity), and also these metrics plotted against an estimate of the background rate obtained by counting the detections falling outside of the gate width.

Even at background light levels comparable to standard room lighting, non-zero key was achievable. In total darkness, the key rate reached up to 25 kbps.

Due to the wide range of conditions in which this system may be deployed, we analysed the effect of the gate width on the secret key rate. Naively one might think to set the gate width to the optical pulse width, but at high backgrounds this will likely allow too many errors and at low backgrounds will reject too much signal. To investigate this, the data was processed as described in Sect. 4.2 up to the point of gating, and then gating and reconciliation were performed repeatedly while changing the gate width. The results are shown in Fig. 16 for a high and low background data point (5 and 40 from Fig. 15). It can be seen that as the gate width increases, the error rate also increases since a wider gate allows more noise. Up to some point this error rate increase is counteracted by an increase in the signal also allowed through the gate. However beyond this point the increase in signal does not overcome key loss due to the increased error rate and the projected secret key rate starts to drop again [32].

6 Conclusion

We have demonstrated a prototype QKD system using a handheld transmitter and a large fixed terminal. The prototype device shows non-zero secret key rate in a range of background light levels. The system achieved a maximum key rate of over 20 kbps, sufficient for re-keying symmetric cryptographic algorithms and one-time pad protection of short high security messages such as in remote PIN verification.

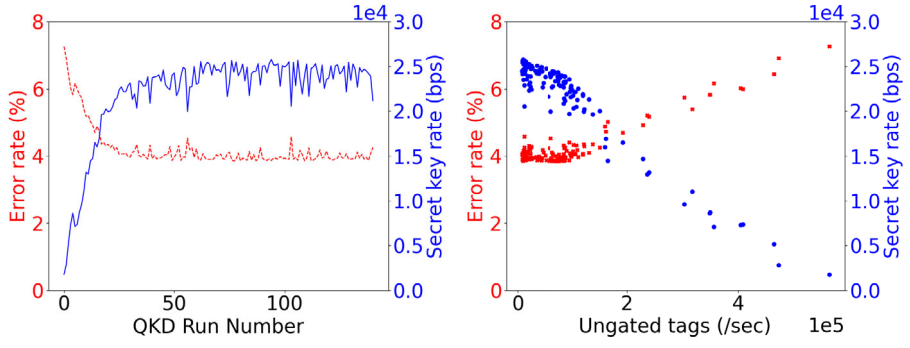


Figure 15 The performance of the system given by the error rate (red, dashed/crosses) and secret key rate(blue, solid) as the background light was gradually dimmed (left), and same data from but plotted against the number of ungated tags (right), which estimates the level of background light

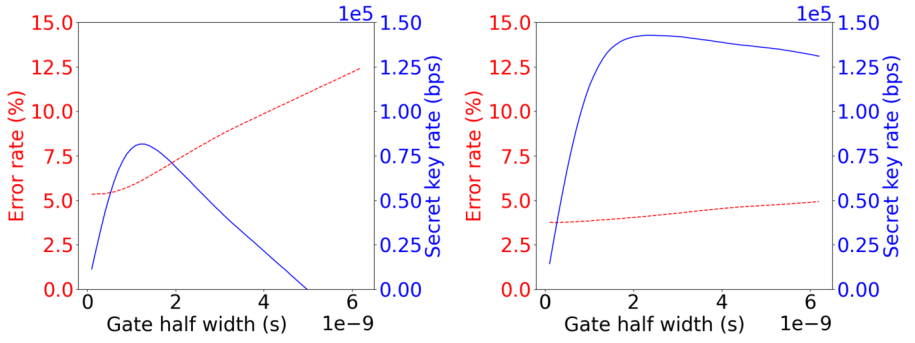


Figure 16 Determining the optimum gate width by maximizing the secret key rate (blue, solid). This process is shown for high background (left) and low background (right). The values determined in this process were 2 ns and 4.2 ns respectively. Error rate is also shown as a guide (red, dashed)

Table 1 Comparison of the transmitter SWaP compared to the target from Sect. 1

SWaP item	Our system	Target
Size	146.24 ml	<48 ml
Weight	65 g	150 g
Power	3.15 W	2.5 W

The SWaP of our prototype transmitter is shown in Table 1, compared to the targets discussed in Sect. 1. It is clear that we have achieved weight goals but are slightly over power and size budgets. However with careful engineering of optics and electronics we should be able to achieve these specifications.

Beyond the SWaP of the system, there are some outstanding issues with the design which we will continue to work on, these include:

QRNG: Minimally, our transmitter requires 200 Mbps random numbers. This is without decoy states or unbalanced bases. There is not currently an off-the-shelf quantum random number generator with compatible SWaP available, although it has been shown that mobile phone cameras can be appropriated for quantum random number generator (QRNG) purposes [33]. For our prototypes the best we can do is settle for some other randomness source or rely on a large cache of randomness which is slowly replenished when the system is not generating key. We hope to investigate using recent IDQuantique devices such as IDQ20MC1 [34].

Processing speed: The clock recovery process is currently about 2x slower than the data collection so real time processing is not currently feasible. This does not appear to be a fundamental limitation, rather that the algorithm is a fairly brute-force method and further effort should be made into investigating more nuanced methods of clock synchronisation. Alternatively, we could take advantage of the fact that the algorithm is highly parallelizable, since each clock guess can be optimised independently. Equipping the receiver with hardware capable of fast parallel execution (such as GPUs), would significantly improve the performance of the existing methods and not violate our philosophy of cheap transmitter.

Device size: While the device is unarguably handheld, the optics module is too big for anything other than a standalone device. For example at its current size this device could not practically be integrated into a mobile phone. That said much of the size of

the optics module is "useless" plastic which is simply to aid manufacture and testing. The next generation optics is planned to be 50% smaller by better integrating the optical, mechanical and electronic components.

Channel establishment: The slot dock demonstrated here is a simple proof of concept that enables the devices to be demonstrated. However practically this places unnecessary constraints on further development. For example any devices which wished to incorporate our QKD transmitter would have to be a certain shape to be compatible with the dock. A much more sensible evolution of this system would be to include active tracking to establish the link while the user continues to hold the device in their hand. Going forward we have partnered with the University of Oxford, integrating our system with a beamsteering solution based on their work in [20].

Brightness: The existing mean photon number is quite low ($\mu = 0.025$), we suspect this is due to the driving electronics, namely the ONET 1101L chips which were designed to driver laser diodes not LEDs. Whilst there are no commercial LED driver chips with ≈GHz bandwidth, we have identified promising alternatives which have a higher maximum current capacity which would be able to counteract the higher junction capacitance of LEDs compared to laser diodes. In terms of security as our channel loss is less that 10 dB we can expect to be able to increase mean photon number to $\mu = 0.1$ with needing to use additional security schemes such as decoy states.

Security Analysis: This work has mainly focused on the engineering aspects of building a QKD system, and whilst Sect. 5 quoted secret key rate estimates using [14, 32], finite key effects [35, 36] have not yet been considered in the key rate calculations.

Acknowledgements
Not applicable

Funding
The research leading to this work has been supported by the Quantum Communications Hub funded by the EPSRC grant ref. EP/M013472/1 and EP/T001011/1.

Availability of data and materials
Data presented in this paper can be found at: https://doi.org/10.5523/bris.2jhamuznu717y2dts7wbwy9shl

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
All authors read and approved the final manuscript.

Author details
[1]Department of Electrical and Electronic Engineering, University of Bristol, Woodland Road, BS8 1UB, Bristol, UK. [2]Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, 6020 Innsbruck, Austria.

Publisher's Note

Received: 19 January 2021 Accepted: 29 April 2021 Published online: 26 May 2021

References

1. Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes JF, Fasel S, Fossier S, Fürst M, Gautier J-D, Gay O, Gisin N, Grangier P, Happe A, Hasani Y, Hentschel M, Hubel H, Humer G, Länger T, Legré M, Lieger R, Lodewyck J, Lorünser T, Lütkenhaus N, Marhold A, Matyus T, Maurhart O, Monat L, Nauerth S, Page J-B, Poppe A, Querasser E, Ribordy G, Robyr S, Salvail L, Sharpe AW, Shields AJ, Stucki D, Suda M, Tamas C, Themel T, Thew RT, Thoma Y, Treiber A, Trinkler P, Tualle-Brouri R, Vannel F, Walenta N, Weier H, Weinfurter H, Wimberger I, Yuan ZL, editors. Zbin: the SECOQC quantum key distribution network in Vienna. New J Phys. 2009;11(7):075001. https://doi.org/10.1088/1367-2630/11/7/075001.

2. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A, Yoshino K, Nambu Y, Takahashi S, Tajima A, Tomita A, Domeki T, Hasegawa T, Sakai Y, Kobayashi H, Asai T, Shimizu K, Tokura T, Tsurumaru T, Matsui M, Honjo T, Tamaki K, Takesue H, Tokura Y, Dynes JF, Dixon AR, Sharpe AW, Yuan ZL, Shields AJ, Uchikoga S, Legré M, Robyr S, Trinkler P, Monat L, Page J-B, Ribordy G, Poppe A, Allacher A, Maurhart O, Länger T, Peev M, Zeilinger A. Field test of quantum key distribution in the Tokyo QKD network. Opt Express. 2011;19(11):10387. https://doi.org/10.1364/oe.19.010387.
3. Mao Y, Wang B-X, Zhao C, Wang G, Wang R, Wang H, Zhou F, Nie J, Chen Q, Zhao Y, Zhang Q, Zhang J, Chen T-Y, Pan J-W. Integrating quantum key distribution with classical communications in backbone fiber network. Opt Express. 2018;26(5):6010. https://doi.org/10.1364/oe.26.006010.
4. Aguado A, Hugues-Salas E, Haigh PA, Marhuenda J, Price AB, Sibson P, Kennard JE, Erven C, Rarity JG, Thompson MG, Lord A, Nejabati R, Simeonidou D. Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. J Lightwave Technol. 2017;35(8):1357–62. https://doi.org/10.1109/jlt.2016.2646921.
5. Jennewein T, Grant C, Choi E, Pugh C, Holloway C, Bourgoin JP, Hakima H, Higgins B, Zee R. The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. In: Emerging technologies in security and defence II; and quantum-physics-based information security III. Bellingham: SPIE; 2014. https://doi.org/10.1117/12.2067548.
6. Bedington R, Arrazola JM, Ling A. Progress in satellite quantum key distribution. npj Quantum Information. 2017;**3**(1). https://doi.org/10.1038/s41534-017-0031-5.
7. Liao S-K, Cai W-Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J-G, Liu W-Y, Li Y, Shen Q, Cao Y, Li F-Z, Wang J-F, Huang Y-M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N-L, Koidl F, Wang P, Chen Y-A, Wang X-B, Steindorfer M, Kirchner G, Lu C-Y, Shu R, Ursin R, Scheidl T, Peng C-Z, Wang J-Y, Zeilinger A, Pan J-W, editors. Satellite-relayed intercontinental quantum network. Physical Review Letters. 2018;**120**(3). https://doi.org/10.1103/physrevlett.120.030501.
8. Polnik M, Mazzarella L, Carlo MD, Oi DKL, Riccardi A, Arulselvan A. Scheduling of space to ground quantum key distribution. EPJ Quantum Technology. 2020;**7**(1). https://doi.org/10.1140/epjqt/s40507-020-0079-6.
9. Mazzarella L, Lowe C, Lowndes D, Joshi SK, Greenland S, McNeil D, Mercury C, Macdonald M, Rarity J, Oi DKL. QUARC: quantum research cubesat — a constellation for quantum communication. Cryptography. 2020;4(1):7. https://doi.org/10.3390/cryptography4010007.
10. Wehner S, Elkouss D, Hanson R. Quantum Internet: a vision for the road ahead. Science. 2018;362(6412):9288. https://doi.org/10.1126/science.aam9288.
11. https://www.onespan.com/sites/default/files/2019-08/Digipass-836_datasheet.pdf. Accessed 12/03/2020.
12. https://www.devicespecifications.com/en/model/17ed4dee. Accesseed 12/03/2020.
13. Palacios-Berraquero C, Barbone M, Kara DM, Chen X, Goykhman I, Yoon D, Ott AK, Beitner J, Watanabe K, Taniguchi T, Ferrari AC, Atatüre M. Atomically thin quantum light-emitting diodes. Nature Communications. 2016;**7**(1). https://doi.org/10.1038/ncomms12978.
14. Gottesman D, Lo H-K, Lütkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. Quantum Inf Comput. 2004;4(5):325–60.
15. Eisaman MD, Fan J, Migdall A, Polyakov SV. Invited review article: single-photon sources and detectors. Rev Sci Instrum. 2011;82(7):071101. https://doi.org/10.1063/1.3610677.
16. Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H, Weinfurter H. Information leakage via side channels in freespace BB 84 quantum cryptography. New J Phys. 2009;11(6):065001. https://doi.org/10.1088/1367-2630/11/6/065001.
17. Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner MG, Natarajan CM, Hadfield RH, O'Brien JL, Thompson MG. Chip-based quantum key distribution. Nature Communications. 2017;**8**(1). https://doi.org/10.1038/ncomms13984.
18. Duligall JL, Godfrey MS, Harrison KA, Munro WJ, Rarity JG. Low cost and compact quantum key distribution. New J Phys. 2006;8(10):249. https://doi.org/10.1088/1367-2630/8/10/249.
19. Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity JG, Zeilinger A, Weinfurter H. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Physical Review Letters. 2007;**98**(1). https://doi.org/10.1103/physrevlett.98.010504.
20. Chun H, Choi I, Faulkner G, Clarke L, Barber B, George G, Capon C, Niskanen A, Wabnig J, O'Brien D, Bitauld D. Handheld free space quantum key distribution with dynamic motion compensation. Opt Express. 2017;25(6):6784. https://doi.org/10.1364/oe.25.006784.
21. Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Frick S, Weinfurter H. Air-to-ground quantum communication. Nat Photonics. 2013;7(5):382–6. https://doi.org/10.1038/nphoton.2013.46.
22. Vest G, Rau M, Fuchs L, Corrielli G, Weier H, Nauerth S, Crespi A, Osellame R, Weinfurter H. Design and evaluation of a handheld quantum key distribution sender module. IEEE J Sel Top Quantum Electron. 2015;21(3):131–7. https://doi.org/10.1109/jstqe.2014.2364131.
23. https://www.thorlabs.com/thorproduct.cfm?partnumber=SM600. Accessed 12/03/2020.
24. Rarity JG, Owens PCM, Tapster PR. Quantum random-number generation and key sharing. J Mod Opt. 1994;41(12):2435–44. https://doi.org/10.1080/09500349414552281.
25. Lowndes D. Low cost, short range free space quantum cryptography for consumer applications: Pocket size for pocket change. PhD thesis. University of Bristol; 2014.
26. Mélen G, Freiwang P, Luhn J, Vogl T, Rau M, Rosenfeld W, Weinfurter H. Handheld quantum key distribution. In: 2018 conference on lasers and electro-optics (CLEO). 2018. p. 1–2.
27. Nock R, Dahnoun N, Rarity J. Low cost timing interval analyzers for quantum key distribution. In: 2011 IEEE international instrumentation and measurement technology conference. IEEE; 2011. https://doi.org/10.1109/imtc.2011.5944324.
28. Nauerth S. Air to ground quantum key distribution. PhD thesis. Ludwig Maximilians Universität München; 2013.
29. Yin S, Ruffin PB, Yu FTS. Fiber optic sensors. Boca Raton: CRC Press; 2019.
30. Higgins BL, Bourgoin J-P, Jennewein T. Practical polarization-frame alignment for quantum key distribution with single-photon-level resources. 2018. arXiv:1810.04112 [quant-ph].

31. Laing A, Scarani V, Rarity JG, O'Brien JL. Reference-frame-independent quantum key distribution. Physical Review A. 2010;**82**(1). https://doi.org/10.1103/physreva.82.012304.
32. Ma X. Unconditional security at a low cost. Phys Rev A. 2006;74(5):052325.
33. Sanguinetti B, Martin A, Zbinden H, Gisin N. Quantum random number generation on a mobile phone. Phys Rev X. 2014;4:031056. https://doi.org/10.1103/PhysRevX.4.031056.
34. https://www.idquantique.com.
35. Scarani V, Renner R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys Rev Lett. 2008;100:200501. https://doi.org/10.1103/PhysRevLett.100.200501.
36. Cai RYQ, Scarani V. Finite-key analysis for practical implementations of quantum key distribution. New J Phys. 2009;11(4):045024. https://doi.org/10.1088/1367-2630/11/4/045024.