PAPER • OPEN ACCESS

Large-alphabet quantum key distribution using spatially encoded light

To cite this article: T B H Tentrup *et al* 2019 *New J. Phys.* **21** 123044

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
31 July 2019

REVISED
4 November 2019

ACCEPTED FOR PUBLICATION
28 November 2019

PUBLISHED
18 December 2019

PAPER

Large-alphabet quantum key distribution using spatially encoded light

T B H Tentrup, W M Luiten, R van der Meer , P Hooijschuur and P W H Pinkse

Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands

E-mail: p.w.h.pinkse@utwente.nl

Keywords: quantum key distribution, high-dimensional quantum optics, single-photon detection, spatial light encoding

Supplementary material for this article is available online

Abstract

Most quantum key distribution protocols using a two-dimensional basis, such as HV polarization as first proposed by Bennett and Brassard in 1984, are limited to a key generation density of 1 bit per photon. We increase this key density by encoding information in the transverse spatial displacement of the used photons. Employing this higher-dimensional Hilbert space together with modern single-photon-detecting cameras, we demonstrate a proof-of-principle large-alphabet quantum key distribution experiment with 1024 symbols and a shared information between sender and receiver of 7 bit per photon.

1. Introduction

Human society relies increasingly on the availability of affordable and high-speed communication, which fosters the need of high key-rate generating cryptography. Recent progress in the development of quantum computers [1–5] threatens the widely used cryptographic methods, which rely on computational assumptions [6, 7]. A possible solution is quantum key distribution (QKD) of which the security is only based on quantum physics and not on any computational assumption. The first QKD protocol BB84 [8] uses the two-dimensional polarization basis to encode information in photons. Therefore, the alphabet is limited to two symbols, '0' and '1', with a maximum information content of 1 bit per photon. Since the generated key is used as a one-time pad, this is a bottleneck especially for encrypted video communication [9].

There are two approaches to increase the key generation rate. One is to increase the repetition rates of photon generation [10] and detection [11], which is inherently limited by dead times and jitter of the detectors [12]. The other approach is to exploit properties of photons besides the polarization to increase the dimensionality of the Hilbert space [13, 14]. A higher dimensional Hilbert space leads to a higher information content of the photons and finally increases the key generation rate. Moreover, the error rates introduced by eavesdropping are larger, resulting in an increased security [15–18].

Several methods of high-dimensional QKD have been demonstrated, including time-bin [19–22], orbital angular-momentum [23–26] and transverse momentum [27, 28]. Comparing the last two spatial encoding schemes, transverse momentum states have the following advantages. Assuming a realistic sender-receiver configuration with finite-size apertures, a diffraction-limited spot translated in an x, y-plane has a higher capacity limit than the pure OAM states, since they form a subset of Laguerre–Gauss modes [29, 30]. Together with the ease of generating a Fourier-transformed mutually unbiased basis with lens optics, spatial translation states of single photons is a promising candidate for very-high-dimensional QKD.

In this paper we experimentally demonstrate very-high-dimensional QKD with 1024 distinguishable symbols in two mutually unbiased bases with a shared information of 7 bit per sifted photon. This value is higher than previously reported values of 2.05 bit for OAM states [24] and comparable to the values demonstrated in time-energy QKD [21]. We give finite-key security arguments for claiming an error-corrected and privacy-amplified secret-key rate of the final key of more than 0.5 bit per photon.

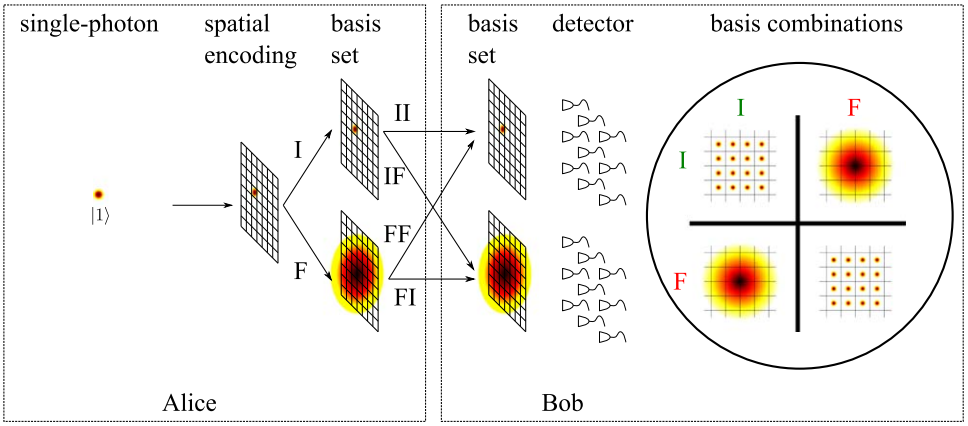

Figure 1. Illustration of our spatial encoding and decoding scheme and possible basis choices therein. The single-photon state $|1\rangle$ is encoded in the x, y-translation basis formed by shifting a focus over a two-dimensional grid. Alice can send an image of the focus (I) or its Fourier transform (F) to Bob. Bob randomly switches between the two bases I and F. Only if the two bases are compatible (II or FF), the information encoded by Alice can be read out by Bob. In the two other cases (IF or FI), the information is low. Just like in the original BB84 protocol, a public channel is used for post processing including revealing the bases choices, detection of eavesdropping, error correction and privacy amplification.

2. Experiment

We implement a high-dimensional version of the BB84 protocol using the x, y spatial translation of single photons to encode information [27, 31]. The working principle of the protocol is illustrated in figure 1. We define detection areas on the two-dimensional plane representing the symbols of our alphabet. The detection areas span 10×10 pixels on our single-photon sensitive detector. All the areas are arranged in a two-dimensional grid of 32×32 symbols. In this way, we are able to encode $d = 32^2 = 1024$ symbols in total, which allows a theoretical maximum of $I_{\max} = 10$ bit encoded in a single photon. Quantum key distribution requires a second, mutually unbiased, basis to guarantee that a measurement in the wrong basis yields no information. It is always possible to use a Fourier transform to form this second basis [32]. In optics, a single lens performs this task. Therefore, switching between an Imaging path and a Fourier path corresponds to selecting the basis. Only two of the four possible combinations will reveal all the information that the sender (Alice) encoded to the receiver (Bob). The two remaining cases will not provide any information.

The setup implementing such a protocol is shown in figure 2. Here Alice has a 2 mm periodically poled KTP (PPKTP) crystal, pumped with 3 ps pulses of 395 nm. This results in photon pairs of 790 nm. One photon is directly measured and used as a herald to gate the single-photon sensitive camera. The other photon is sent to a phase-only spatial light modulator (Hamamatsu LCOS-SLM), which is used to implement blazed gratings. We typically operate at a single-photon count rate of 280 kHz, which results in a probability of <0.1 % to have more than the one photon pair. The blazed gratings route the photon to different positions in the x, y-plane for encoding. Alice uses a half-wave plate to randomly select the Imaging arm (4f-setup) or Fourier arm (2f-setup). The half-wave plate after the second polarization beam splitter scrambles the polarization to erase encoding information. After the quantum channel, a 50: 50 beam splitter at Bob's side randomly selects between the two bases and from that the photons are detected on the intensified CCD (ICCD, Lambert HICAM 500S).

The ICCD consists of an intensifier stage, fiber-coupled to a CMOS camera of 1280×1024 pixels. The photocathode of the ICCD acts as a gate and is triggered by the herald photons at 280 kHz. In order to reduce dark counts, the gate time is set to 5 ns. The CMOS camera is read out with 500 frames per second. The readout noise of the ICCD can be suppressed by setting a threshold for the signal intensity on the CMOS camera [33, 34]. The variance of the readout noise of the CMOS is 0.4 counts and a threshold of 5 counts is set to filter the readout noise from the data. Moreover, a threshold on the size and intensity of detection events is set to between 2 and 10 pixels and between 1 and 60 counts, respectively, to remove unwanted spurious ion events. After this postprocessing, the probability of detecting a dark count is found to be on the order of 10^{-6} per pixel per second exposure time.

3. Results

We begin with characterizing the information content of the transmission from Alice to Bob. For this purpose, we analyze the two compatible bases choices of Alice and Bob (II and FF). Alice sends each symbol x out of her

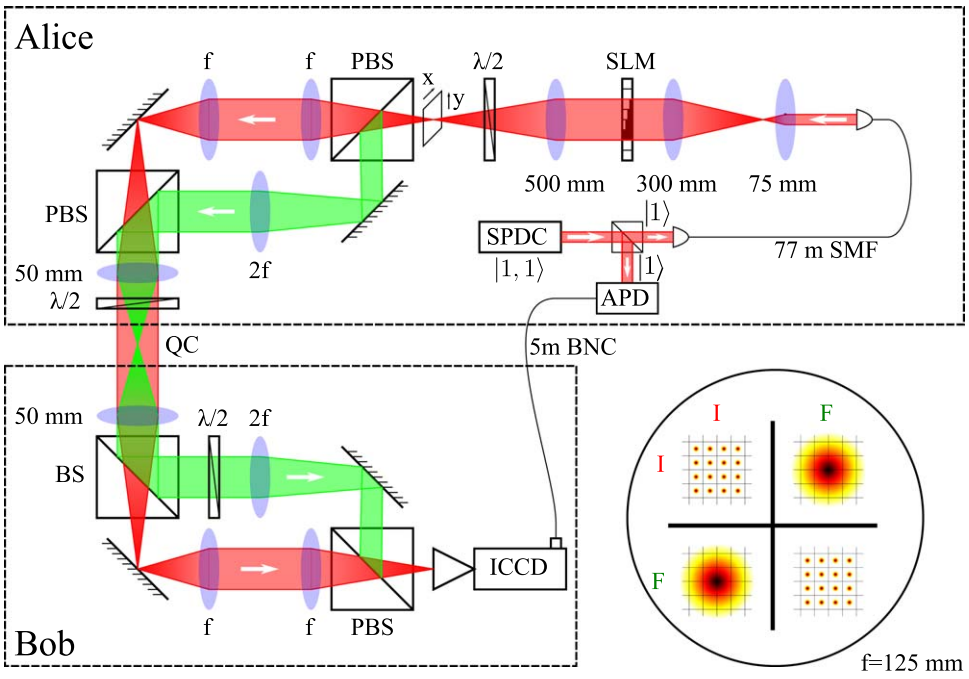

Figure 2. Schematic representation of the setup. We generate photon pairs at 790 nm by spontaneous parametric down-conversion (SPDC). One of the photons is coupled into a single-mode fiber (SMF) and the other is sent to an avalanche photodiode (APD) and used to trigger the camera. Information is encoded into the signal photon by translating the x and y position of the focus with a spatial light modulator (SLM) and a 500 mm lens. Alice chooses between two paths with a half-wave plate and a polarizing beam splitter (PBS), one (green) with a single lens (2f) and one (red) with two lenses (f). After the two beams are merged again by a second PBS and the polarization information is erased by a second half-wave plate, the light is guided through the quantum channel (QC) with two 50 mm lenses. Bob has the same set of lenses as Alice. His two paths are chosen randomly by a beam splitter (BS). The additional half-wave plate makes sure that all the light is directed to the intensified CCD (ICCD) by the last PBS.

alphabet X individually, while Bob receives the symbol y out of the alphabet Y. Per symbol 1000 images are recorded on Bob's side for the FF and the II bases configuration. In figure 3 the number of photons detected per symbol is shown in a log–log plot. In this figure, the joint probability function $p(x, y)$ is sampled, where x is an element of the sent alphabet X and y from the received alphabet Y. We quantify the shared information between Alice and Bob by the mutual information [35]

$$I(X;\,Y) = \sum_{x\in X, y\in Y} p(x,\,y)\log_2\left(\frac{p(x,\,y)}{p(x)\;p(y)}\right), \tag{1}$$

where $p(y)$ is the probability to measure symbol y and $p(x)$ the probability of a sent symbol x. The maximum information Alice can send per symbol is $I(\text{Alice}) = 10$ bit. Due to noise in the channel and in the detection and imperfections in the information encoding, the shared information between Alice and Bob is smaller. For the II and FF basis configuration, we calculated the sampled mutual information to be $I(X;\,Y)_{\text{II}} = 8.3$ bit and $I(X;\,Y)_{\text{FF}} = 8.1$ bit, respectively. The two main contributions to the noise are the cross talk to the neighboring detection areas, which was 13.3% and the dark counts of the detector which was 13.8%. With respect to these numbers, it should be noted that despite considerable experimental efforts, the probabilities used in the calculation of the mutual information are under-sampled with an average of 73 detection events per symbol. This means that neighboring pixel crosstalk events are not accurately sampled, a problem that gets increasingly severe for larger alphabets.

The expression for the mutual information of equation (1) can be simplified by introducing the average symbol hit probability (averaged over II and FF), P_{av}

$$I(P_{\text{av}}) = \log_2(d) + P_{\text{av}}\log_2(P_{\text{av}}) + (1 - P_{\text{av}})\log_2\left(\frac{1 - P_{\text{av}}}{d - 1}\right), \tag{2}$$

where d is the dimensionality of the basis. In our experiment, $P_{\text{av}} = 68.7\%$. Since a large portion of the photons hits the neighboring areas, equation (2) is an underestimate of the mutual information between Alice and Bob and can be refined by adding the hit probabilities P_0, P_1, P_2 and P_{rest} defined in the top left corner of figure 3. We assume the values P_0, P_1, P_2 and P_{rest} do not vary from symbol to symbol and derive

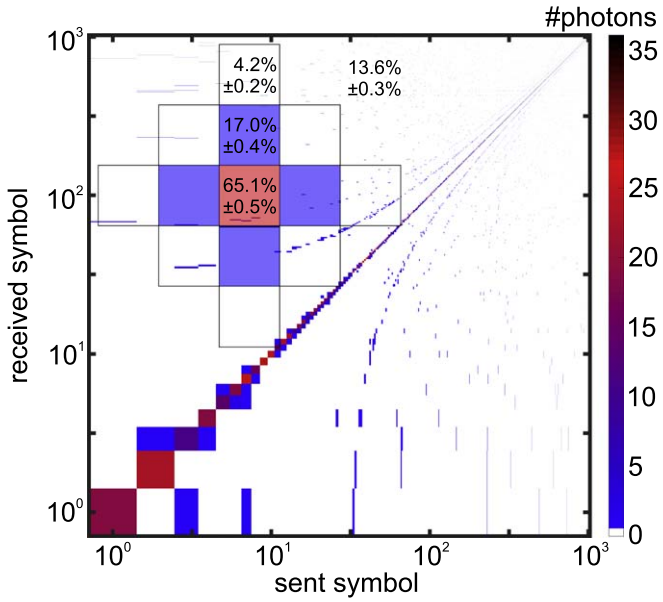

Figure 3. Correlation map of the received symbol index versus the sent symbol index on a logarithmic scale in II configuration. The diagonal line indicates a strong correlation between the sent and the received symbols. The other lines parallel to the diagonal show crosstalk between neighboring symbols. In the top left corner, the hit distribution to the nearest and next-nearest neighbor symbols is shown. The events are visible in the correlation map as the lines shifted by the number of columns of the map. The average hit probability of the target area (red) is P_0, that of the four nearest neighbors (blue) is P_1, that of the eight next nearest neighbors (white) P_2. The remaining probability is summed in $P_{\text{rest}} = 1 - P_0 - P_1 - P_2$.

$$I_{\text{AB}} = \log_2(d) + P_0 \log_2(P_0) + P_1 \log_2\left(\frac{P_1}{4}\right) + P_2 \log_2\left(\frac{P_2}{8}\right) + P_{\text{rest}} \log_2\left(\frac{P_{\text{rest}}}{d-13}\right). \tag{3}$$

The resulting mutual information is 6.75 ± 0.08 bit in the II configuration and 7.03 ± 0.04 bit in the FF configuration.

Thus far only a measurement in the correct basis has been considered. We now consider measuring in an incompatible basis, i.e. FI or IF. Such a basis combination should ideally not provide any information, which can be either the sent symbol or Alice's basis choice. This, however, does not hold trivially for our protocol. For this it is important to realise that Gaussian beams are used in our protocol. As a result, we have Gaussian foci with finite width in the focus plane. The corresponding measurement in the incompatible basis is the Fourier transform of the Gaussian beam, and hence it becomes a large Gaussian spot. This can be exploited by a potential eavesdropper Eve, since a photon detection at the edge of the detector is more likely to have been sent in an incompatible basis. Hence the position of the detection reveals information on what basis Alice has chosen. Figure 4 shows a sample from the resulting distribution of measuring in an incompatible basis, together with a Gaussian fit. The width in the columns is 89.9 ± 1.7 pixel and 106.7 ± 1.9 pixel in the rows together with 96.3 ± 2.5 pixel and 102 ± 3 pixel in the FI configuration. To close the leak, Alice can adjust her send probability $p(k)$ to match this Gaussian distribution. As a result, the information sent by Alice $I(\text{Alice}) = -\sum_{k=0}^{d-1} p(k)\log_2(p(k))$ reduces from 10 bit to $I(\text{Alice})_{\text{II}} = 9.4$ bit and $I(\text{Alice})_{\text{FF}} = 9.4$ bit. Consequently, the sampled mutual information with the hidden basis drops to [27]

$$I_{\text{hb}} = I(\text{Alice}) + \sum_{k=0}^{d-1} p(k) F_{\text{eff}} \log_2(F_{\text{eff}}) + \sum_{k=0}^{d-1}\sum_{j=0,j\neq k}^{d-1} \frac{p(k)(1-F_{\text{eff}})p(j)}{1-p(k)} \log_2 \times \left(\frac{(1-F_{\text{eff}})p(j)}{1-p(k)}\right) \tag{4}$$

with the effective fidelity F_{eff} defined by $I(F_{\text{eff}}) = I_{\text{AB}}$ in combining equations (2) and (3). This results in $(F_{\text{eff}})_{\text{II}} = 75.5\%$ and $(F_{\text{eff}})_{\text{FF}} = 77.9\%$ leading to $(I_{\text{hb}})_{\text{II}} = 6.3$ bit and $(I_{\text{hb}})_{\text{FF}} = 6.6$ bit. In table 1 we give an overview over the amount of mutual information between Alice and Bob considering the various assumptions on the mutual information in this section.

Having characterised the transmission behavior of the symbols of our alphabet, we now have to devise a scheme to encode bits of (random) data in x, y coordinates of the photons. Encoding a string of 5 bits in an x coordinate and the next 5 bits into a y coordinate would lead to a high error rate in the likely case that a photon does not hit the target symbol but one of its neighbors. For instance, the bit string 01111 corresponds to the digital coordinate 15, but if the photon is detected at the neighboring symbol 16, it encodes for 10 000 which

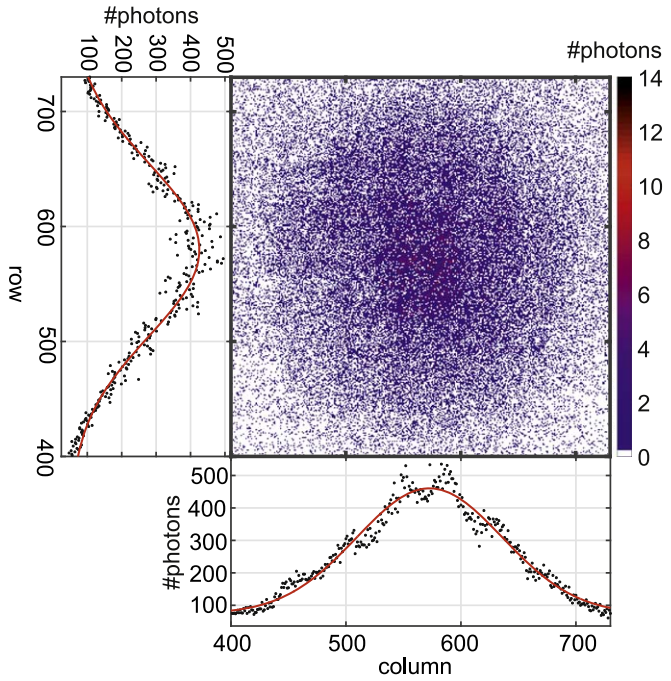

Figure 4. Image integrated over all Bob's 1024 different spot positions in the IF configuration. Projections of the signal are shown left of and below the plot by summing over the columns (lower panel) and rows (left panel). The photon counts follow a Gaussian spatial distribution as is evident from the red fit curves.

Table 1. Table with a summary of the values for the mutual information in the II and FF configuration as well as the average over both configurations.

Mutual Information	II	FF	Average
Theoretical maximum	10 bit	10 bit	10 bit
Sampled	8.3 bit	8.1 bit	8.2 bit
$I(P_{\text{av}})$	5.58 bit	6.38 bit	5.97 bit
I_{AB}	6.75 bit	7.03 bit	6.89 bit
I_{hb}	6.3 bit	6.6 bit	6.45 bit

means that 5 bits are read out wrongly. To alleviate this, we used the Gray code [36] to encode the x and y position of the symbol in a bit string. In this way we can reduce the bit error rate, since 31.3% of the error is due to crosstalk to neighboring symbols. In the Gray code, neighboring symbols have a Hamming distance of only 1. This means that the bit strings corresponding to neighboring symbols in the same column or row only differ by a single bit flip. Subsequently, the bit string differs from the next-nearest neighboring symbol by 2 bit flip. This allows us to calculate the quantum bit error rate for the II and FF configuration by $(P_0 \cdot 0 + P_1 \cdot 1 + P_2 \cdot 2 + P_{\text{rest}} \cdot 5)/10$. Here P_0, P_1 and P_{rest} denote the detection probability as shown in figure 3. These probabilities are multiplied by the corresponding number of bit flips. We calculated the averaged quantum bit error rate over all symbols to be $Q_{\text{II}} = 7.8$ % for the II configuration and $Q_{\text{FF}} = 7.4$ % for the FF configuration. This is low enough to be corrected with standard error correcting methods.

In order for Alice and Bob to find out if an eavesdropper is present, they need to perform a postprocessing step where they communicate via the public channel. In this step, Alice and Bob reveal their basis choices and disregard measurement results whenever they chose a different basis. To check for eavesdropping, the fidelity (or error rate) of this sifted key needs to be calculated. The presence of an eavesdropper is revealed in an increase of the quantum bit error rate.

Let us now turn to possible attack strategies of Eve. If Eve uses an optimal cloner [37], then the minimum fidelity Bob requires to overcome cloning-based individual attacks (where Eve monitors the qudits separately) is 51.6% [15]. Another, more general approach Eve can pursue is a collective attack, where Eve monitors several qudits jointly. In order to analyze the security against these collective attacks, we used finite-key considerations given in [38–40]. In the case of a finite key length, $N < \infty$, failure probabilities in each step of postprocessing need to be considered. After sifting the key and removing the incompatible basis choices of Alice and Bob, the

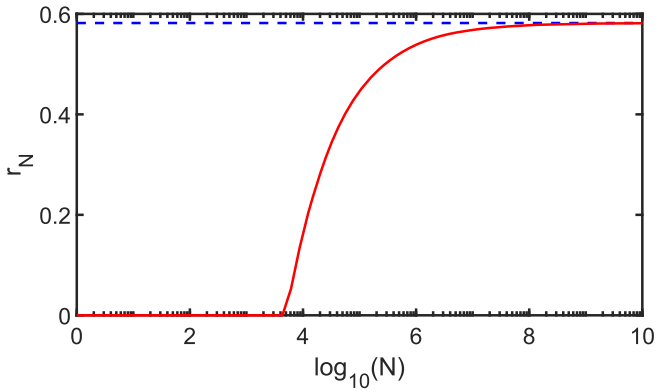

Figure 5. The lower bound of the secret-key rate r_N per detected photon as a function of the logarithm of the key length N (red). The blue dashed line represents the asymptotic limit of infinite key length. The failure probabilities are $\epsilon_{\mathrm{EC}} = 10^{-5}$ and $\epsilon_{\mathrm{PA}} = 2^{-15}$ after error correcting and privacy amplification, respectively. The quantum bit error rate is $Q = 0.08$.

key length bisects. From this reduced key length, half the symbols are used to check for the presence of an eavesdropper. The next step is error correction to achieve an error-free key. Due to the finite key length the error correction has a finite failure probability and not all errors can be removed. Assuming a two-way cascade code [41], this failure probability is $\epsilon_{\mathrm{EC}} \sim 10^{-5}$ [42, 43] in case of a 8% bit error rate. To limit the maximum information of Eve, a privacy amplification step needs to be performed. With average bound privacy amplification [44, 45], the information of Eve can be bound to 3×10^{-10} bit with a failure probability of $\epsilon_{\mathrm{PA}} = 2^{-15}$. The overall failure probability of the protocol is $\epsilon = 10^{-5}$, which is comprised of the failure probability of the privacy amplification ϵ_{PA} and the failure probability of the error correction ϵ_{EC}. The lower bound for the secret-key rate per photon is given by [38–40]

$$r_N = \frac{n}{N}\left(I_{\mathrm{AB}} - I(\mathrm{Eve}) - \frac{1}{n}\log_2\left(\frac{2}{\epsilon_{\mathrm{EC}}}\right) - \frac{2}{n}\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right)\right). \tag{5}$$

We neglect the failure probability introduced by smoothening the entropies. If both bases are used with equal probability, $n = 0.25N$ symbols can be used to create a key while $m = 0.25N$ symbols are used for parameter estimation to detect the presence of an eavesdropper. I_{AB} is defined in equation (3) and is the mutual information between Alice and Bob and

$$\begin{aligned} I(\mathrm{Eve}) = &-(1 - P_{\mathrm{av}} + \Delta P_{\mathrm{av}}/\sqrt{m})\log_2 \times \left(\frac{1 - P_{\mathrm{av}} + \Delta P_{\mathrm{av}}/\sqrt{m}}{d-1}\right) \\ &- (P_{\mathrm{av}} - \Delta P_{\mathrm{av}}/\sqrt{m})\log_2(P_{\mathrm{av}} - \Delta P_{\mathrm{av}}/\sqrt{m}) \end{aligned} \tag{6}$$

is Eve's information assuming all channel errors are attributed to her presence [15]. We assume the worst-case values in parameter estimation for the fidelity P_{av} by taking the standard deviation ΔP_{av} of the measured fidelity into account. This uncertainty in the fidelity is reduced by taking larger samples m for parameter estimation. The remaining terms in equation (5) are the influence of the failure probabilities on the secret-key rate.

Figure 5 shows the minimum secret-key rate as a function of the number of symbols. With increasing key length, the secret-key rate approaches its asymptotic limit, which is the difference between the shared information between Alice and Bob and the information of Eve. As seen in the figure, we can establish a non-zero secret-key rate starting from a key length of $5 \cdot 10^3$ symbols. Assuming an SLM with a maximum frame rate of 60 fps, such a key can be generated in ≈3 min. The secure key rate per photon asymptotically approaches 0.58 bit per photon. With the overall losses throughout the setup averaged over the four possible bases of 18.2% and a quantum efficiency of our ICCD detector of 28%, we end up with a final secure key rate of 8 bit per second. This rate can be improved straightforwardly by replacing the SLM in our setup by galvo mirrors. With an ICCD with 5000 fps the final key rate can go up to 660 bit per second.

In principle, there could be a security loophole caused by the limited measurement range of the detection system, which is in our case the finite aperture of the ICCD [46]. However, with the SLM we have full control of the prepared wavefronts and can therefore avoid that the light falls outside the detector. For the Fourier-transformed light, straightforward additional spatial filtering can be applied by Alice to not overfill Bob's detector and avoid this loophole.

Finally, some thoughts about further increasing the size of the alphabet. Following arguments as presented in [18], we demonstrated a high noise resistance of high-dimensional quantum states. Increasing the dimensionality, the noise is spread over quadratically many off-diagonal elements of the correlation map

(figure 3). The correlated events on the diagonal spread linearly with the dimension. Although this might limit further upscaling of the dimensionality by orders of magnitude, with an alphabet of 1024 characters we have already shown record-high information density with our method and have not yet reached the limits set by the dark counts, which amount to only 10^{-6} per pixel per second exposure time.

4. Conclusion

In this paper, we experimentally demonstrate high-dimensional QKD using spatially encoded photons. We encode an alphabet of 1024 symbols and achieve a channel capacity of 7 bit per detected photon. We discuss a solution to hide Alice's basis choice from Eve. Taking error correction and privacy amplification into account for finite key length, we show a secret-key fraction of 0.5 bit per photon. For longer-distance communication, the combination of this work with multimode fibers [47] appears attractive.

Acknowledgments

We would like to thank the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) for funding this research via ViCi grant 680-47-614 and QuantERA project QUOMPLEX (no. 731473). We thank Lyuba Amitonova, Jelmer Renema, Ravitej Uppu and Willem Vos for support and discussions. We also like to thank Valerio Scarani for giving us useful input for the finite-key formalism.

ORCID iDs

R van der Meer https://orcid.org/0000-0002-7230-3241
P W H Pinkse https://orcid.org/0000-0001-7912-9322

References

[1] Barends R *et al* 2016 *Nature* **534** 222
[2] Brecht T, Pfaff W, Wang C, Chu Y, Frunzio L, Devoret M H and Schoelkopf R J 2016 *npj Quantum Inf.* **2** 16002
[3] Aasen D *et al* 2016 *Phys. Rev.* X **6** 031016
[4] Saffman M 2016 *J. Phys. B: At. Mol. Opt. Phys.* **49** 202001
[5] Wang Y, Li Y and Zeng B 2018 *npj Quantum Inf.* **4** 46
[6] Shor P W 1994 *Algorithms for quantum computation: Discrete logarithms and factoring 35th Annual Symp. on Foundations of Computer Science, 1994 Proc.* (Piscataway, NJ: IEEE) pp 124–34
[7] Menezes A J, Van Oorschot P C and Vanstone S A 1996 *Handbook of applied cryptography* (Boca Raton, FL: CRC press)
[8] Bennet C H 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Comp. (Bangalore, India, 10-12 December)*
[9] Liao S K *et al* 2017 *Nature* **549** 43
[10] Yuan Z L, Fröhlich B, Lucamarini M, Roberts G L, Dynes J F and Shields A J 2016 *Phys. Rev.* X **6** 031044
[11] Patel K A, Dynes J F, Lucamarini M, Choi I, Sharpe A W, Yuan Z L, Penty R V and Shields A J 2014 *Appl. Phys. Lett.* **104** 051123
[12] Brougham T, Wildfeuer C F, Barnett S M and Gauthier D J 2016 *Eur. Phys. J.* D **70** 214
[13] Bechmann-Pasquinucci H and Tittel W 2000 *Phys. Rev.* A **61** 062308
[14] Bechmann-Pasquinucci H and Peres A 2000 *Phys. Rev. Lett.* **85** 3313
[15] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[16] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[17] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[18] Ecker S *et al* 2019 arXiv:1904.01552
[19] Ali-Khan I, Broadbent C J and Howell J C 2007 *Phys. Rev. Lett.* **98** 060503
[20] Nunn J, Wright L J, Söller C, Zhang L, Walmsley I A and Smith B J 2013 *Opt. Express* **21** 15959–73
[21] Zhong T *et al* 2015 *New J. Phys.* **17** 022002
[22] Islam N T, Lim C C W, Cahall C, Kim J and Gauthier D J 2017 *Sci. Adv* **3** e1701491
[23] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 *Phys. Rev.* A **88** 032305
[24] Mirhosseini M, Magaña-Loaiza O S, O'Sullivan M N, Rodenburg B, Malik M, Lavery M P J, Padgett M J, Gauthier D J and Boyd R W 2015 *New J. Phys.* **17** 033033
[25] Krenn M, Huber M, Fickler R, Lapkiewicz R, Ramelow S and Zeilinger A 2014 *Proc. Natl Acad. Sci. USA* **111** 6243–7
[26] Sit A *et al* 2017 *Optica* **4** 1006–10
[27] Walborn S P, Lemelle D S, Almeida M P and SoutoRibeiro P H 2006 *Phys. Rev. Lett.* **96** 090501
[28] Etcheverry S, Cañas G, Gómez E S, Nogueira W A T, Saavedra C, Xavier G B and Lima G 2013 *Sci. Rep.* **3** 2316
[29] Zhao N, Li X, Li G and Kahn J M 2015 *Nat. Photon.* **9** 822–6
[30] Kahn J M, Li G, Li X and Zhao N 2016 To twist or not to twist: capacity limits for free-space channels *Signal Processing in Photonic Communications* (Optical Society of America) pp SpM4E–1
[31] Tentrup T B H, Hummel T, Wolterink T A W, Uppu R, Mosk A P and Pinkse P W H 2017 *Opt. Express* **25** 2826–33
[32] Bengtsson I 2007 *AIP Conf. Proc.* **889** 40–51
[33] Morris P A, Aspden R S, Bell J E C, Boyd R W and Padgett M J 2015 *Nat. Commun.* **6** 1–6

[34] Aspden R S, Tasca D S, Boyd R W and Padgett M J 2013 *New J. Phys.* **15** 073032
[35] Nielsen M A and Chuang I L 2002 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[36] Gray F 1953 Pulse code communication *US patent* 2,632,058
[37] Bruß D and Macchiavello D 1999 *Phys. Lett.* A **253** 249–51
[38] Sheridan L and Scarani V 2010 *Phys. Rev.* A **82** 030301
[39] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[40] Cai R Y Q and Scarani V 2009 *New J. Phys.* **11** 045024
[41] Brassard G and Salvail L 1994 Secret key reconciliation by public discussion *Lecture Notes in Computer Science* vol 765 (Berlin: Springer) pp 410–23
[42] Martinez-Mateo J, Pacher C, Peev M, Ciurana A and Martin V 2015 *Quantum Inf. Comput.* **15** 453–77
[43] Tomamichel M, Martinez-Mateo J, Pacher C and Elkouss D 2014 Fundamental finite key limits forinformation reconciliation in quantum key distribution *2014 IEEE Int. Symp. on Information Theory (ISIT)* (Piscataway, NJ: IEEE) pp 1469–73
[44] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 *IEEE Trans. Inf. Theory* **41** 1915–23
[45] Gilbert G, Hamrick M and Thayer F J 2001 arXiv:0108013
[46] Bourassa J E and Lo H K 2019 *J. Opt. Soc. Am.* B **46** 65–76
[47] Amitonova L V, Tentrup T B H, Vellekoop I M and Pinkse P W H 2018 arXiv:1801.07180