Quantum Key Distribution Using Multiple Gaussian Focused Beams*

Boulat A. Bash[1], Nivedita Chandrasekaran[2], Jeffrey H. Shapiro[2], and Saikat Guha[1]
[1] *Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, MA 02138, USA*
[2] *Research Laboratory of Electronics, Massachusetts Institute of Technology,*
77 Massachusetts Avenue, Cambridge, MA 02139, USA

The extremely low key rates afforded by quantum key distribution (QKD) compared to computational cryptographic schemes pose a significant challenge to the wide-spread adoption of QKD. The main reason for the poor rate performance is that the QKD *capacity* of a single-mode lossy bosonic channel, i.e., the maximum key rate attainable using any direct-transmission QKD protocol, is proportional to the end-to-end transmissivity of the channel η in the high-loss regime. Formally, the capacity is $\nu \log_2\left(\frac{1}{1-\eta}\right) \approx 1.44\,\nu\eta$ bits/s when $\eta \ll 1$, where ν is the optical bandwidth in modes/s that can be used by the QKD protocol [1]. This corresponds to an exponential decay of key rate with distance L in fiber and atmospheric free-space propagation (since $\eta = e^{-\alpha L}$, even though the extinction coefficient α may be modest for the latter case in clear weather at a well-chosen wavelength), and to an inverse-square decay of rate with distance in vacuum propagation in the *far-field* regime (where $\eta \propto 1/L^2$). A free-space optical channel is characterized by the Fresnel number product $D_\lambda \equiv A_\mathrm{t}A_\mathrm{r}/(\lambda L)^2$, where A_t and A_r are the respective areas of the transmitter and receiver apertures, and λ is the transmission center wavelength. In the far-field regime $D_\lambda \ll 1$ and only one transmitter-pupil spatial mode couples significant power into the receiver pupil over an L-meter line-of-sight channel with input-output power transmissivity $\eta_0 \approx D_\lambda \propto 1/L^2$ [2]. Thus, employing multiple orthogonal spatial modes in the far-field regime cannot yield a perceptible improvement in the achievable QKD rate.

Our interest in this abstract and the accompanying full paper [3] is in the *near-field* propagation regime ($D_\lambda \gg 1$), which is relevant to metropolitan area QKD, as well as within-the-horizon over-the-surface maritime applications of QKD. In this near-field regime, approximately D_λ mutually-orthogonal spatial modes have near-perfect power transmissivity ($\eta \approx 1$) [2]. Therefore, multiplexing over multiple orthogonal spatial modes could substantially improve the total QKD rate with the gain in rate over using a single spatial mode (such as a focused centered Gaussian beam) being approximately proportional to D_λ, and hence more pronounced at lower range L (where D_λ is high).

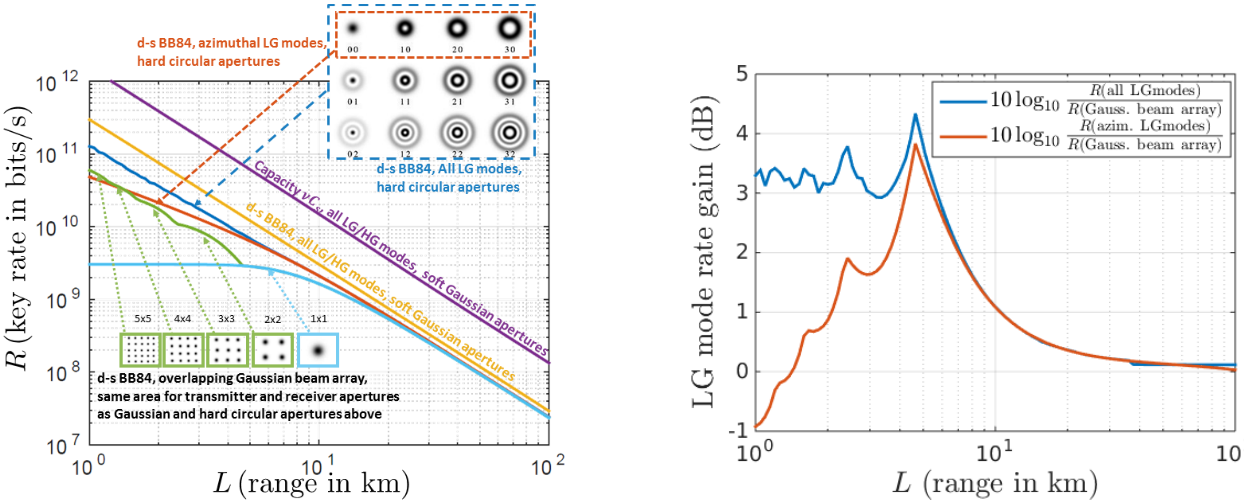
Laguerre-Gauss (LG) functions in the two-dimensional transverse coordinates form an infinite set of mutually-orthogonal spatial modes, which happen to carry orbital angular momentum (OAM). There have been several suggestions in recent years to employ LG modes for QKD, both based on laser-light and single-photon encodings [4–11], and the purported rate improvement has been attributed to the OAM degree of freedom of the photon. While multiplexing over orthogonal spatial modes could undoubtedly improve QKD rate in the near-field propagation regime as explained above:

(1) Can other orthogonal spatial mode sets that do *not* carry OAM be as effective as LG modes in achieving the spatial-multiplexing rate improvement in the near field?

(2) Does one truly need orthogonal modes to obtain this spatial-multiplexing gain or are there simpler-to-generate mode profiles that might suffice?

Question (1) was answered affirmatively for classical [2, 12] and quantum-secure private communication (without two-way classical communication as is done in QKD) [13] over the near-field vacuum propagation and turbulent atmospheric optical channel: Hermite-Gauss (HG) modes are unitarily equivalent to the LG modes and have identical power-transfer eigenvalues $\{\eta_m\}$, $1 \le m < \infty$. Since the respective communication capacity of mode m is a function of η_m and the transmit power on mode m, HG modes, which do *not* carry OAM, can in principle achieve the same rate as LG modes, notwithstanding that the hardware complexity and efficiency of generation and separation of orthogonal LG and HG modes could be quite different.

* This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations. BAB acknowledges the support of the SECANT program funded by the Sandia National Laboratories under PO# 1628276. NC and JHS acknowledge support from the Air Force Office of Scientific Research (AFOSR) grant number FA9550-14-1-0052. SG acknowledges the support from the SeaKey program, through the US Office of Naval Research (ONR) contract number N00014-14-C-0002.



(a) QKD rates for all systems

(b) Comparison of OGBA and LG modes

FIG. 1. QKD rate with various beam and aperture geometries, and the comparison of the QKD rates achieved for hard apertures of equal areas using overlapping Gaussian beam array (OGBA, green plot) and LG mode sets (blue plot for the infinitely many LG modes, and red plot for the infinitely many azimuthal-only LG modes). We assume $\lambda = 1.55\ \mu$m center wavelength, and 0.005π m^2 aperture area. All the rate plots other than the capacity assume a laser-light decoy-state BB84 protocol with detector dark-click probability $p_{\rm d} = 10^{-6}$, detection efficiency $\eta_{\rm d} = 0.9$, visibility of Bob's interferometer $V = 0.99$, and availability of capacity-achieving error correcting codes. We assume $\nu = 10^{10}$ modes/s, i.e., a system limited by the bandwidth of the electro-optical modulator and/or detector, noting a possibility of $\nu = 10^{12}$ modes/s using an amplified spontaneous emission noise source as in Floodlight QKD [14].

Our goal is to address questions (1) and (2) above for QKD. The answer to (1) is trivially affirmative, at least for the case of vacuum propagation (no atmospheric turbulence and extinction), based on an argument similar to the one used in Refs. [2, 12, 13]. Figure 1a shows potential gain of between 1 to 2 orders of magnitude in the key rate by using multiple spatial modes over a 1 km link, assuming $A = 0.005\pi$ m^2 area transmitter and receiver apertures, and $\lambda = 1.55\mu$m laser-light transmission.

The bulk of our analysis addresses question (2) for the optical vacuum propagation channel, which we answer negatively. We show that most of the spatial-multiplexing gain afforded by mutually-orthogonal modes (either HG or LG) in the near field can be obtained using a focused overlapping Gaussian beam array (OGBA) with optimized beam geometry where beams are individually amplitude and/or phase modulated to realize the QKD protocol. These Gaussian focused beams (FBs) are *not* mutually-orthogonal spatial modes, and therefore the power that leaks into FB m from the neighboring FBs has the same effect on the key rate $R_m(L)$ of that FB as do excess noise sources like detector dark current or electrical Johnson noise. Non-zero excess noise causes the rate-distance function $R_m(L)$ to fall to zero at a minimum transmissivity threshold $\eta_{\rm min}$, or, equivalently, at a maximum range threshold $L_{\rm max}$ such that $R_m(L) = 0$ for $L > L_{\rm max}$. Thus, while packing the FBs closer increases the spatial-multiplexing gain, it also increases the excess noise on each FB channel, resulting in decreased $L_{\rm max}$. For any given range L there should exist an optimal (key-rate-maximizing) solution for spatial geometry (tiling) of the FBs, power allocation across the FBs, and beam widths. For shorter range L the optimal solution should involve a greater number of FBs, and the number of beams employed should be approximately proportional to D_λ.

Here, instead of evaluating the optimal rate-maximizing solution as explained above (which is extremely difficult), we find a numerical solution to a constrained optimization problem assuming a square-grid tiling of the FBs in the receiver aperture and restricting our attention to the discrete-variable (DV) laser-light decoy-state BB84 protocol [15]. The rationale behind this is to obtain an *achievable* rate-distance envelope for the OGBA transmitter to compare with the ultimate key capacity attainable by employing infinitely many LG (or HG) modes. Since we restrict our attention to DV QKD, we assume that the OGBA transmitter is paired with a single-photon detector (SPD) array at the receiver with square-shaped pixels and unity fill factor where each FB is focused at the center of a detector pixel and there are as many detector pixels as the number of FBs (the optimal number of which is a function of L as discussed above). We find that the achievable rate using our restricted-optimized OGBA architecture is at most 4.3 dB less than the theoretical maximum for a system that uses the entire set of orthogonal LG (or, HG) modes, while using hard transmitter and receiver apertures of same areas and the same center wavelength.

If one is only allowed to employ the azimuthal LG modes (generating and separating of which have been the subject of much experimental work [16, 17]), and assuming these azimuthal LG modes can be perfectly generated and losslessly separated (note that the azimuthal LG modes retain their orthogonality when propagated between hard circular apertures in vacuum propagation), the rate gain compared to using our OGBA architecture is at most 3.8 dB. However, the losses associated with generating and separating the LG modes are likely to offset this potential rate improvement. Furthermore, relaxing the restriction to a square-grid tiling for the FBs (e.g., using a "hexagonal-packed" beam geometry) is likely to reduce the aforesaid rate gap to less than 3 dB. Current technology for optical communication using orthogonal modes use bulky and expensive components [18]. While advances in enabling technology could reduce the device size, weight and cost of orthogonal mode generation and separation, our results show that using OAM modes for QKD may not be worth the trouble: the gain in QKD key rate in the near field is modest compared to what can already be obtained by our fairly simple-to-implement OGBA architecture. Finally, in the near-field regime, CV QKD can improve rate substantially over the DV BB84 protocol since the CV scheme can leverage effectively a "high-order" constellation in the low-loss regime. Therefore, it would be instructive to evaluate an OGBA architecture employing CV QKD with a heterodyne detection array.

We assumed vacuum propagation in the results reported in this abstract and the accompanying full paper [3]. We are extending them to account for the atmospheric turbulence in the ongoing work. Clearly, turbulence will adversely affect all systems. It is known to break the orthogonality of the azimuthal LG modes [12]. While the classical and private capacities of systems using multiple HG, LG, and FB modes are similar in turbulence [13], the effect of turbulence on the QKD systems using (or not using) adaptive optics at the transmitter and/or the receiver is still unclear.

[1] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "The ultimate rate of quantum communications," arXiv:1510.08863 [quant-ph] (2015).

[2] J. H. Shapiro, S. Guha, and B. I. Erkmen, Journal of Optical Networking **4**, 501 (2005).

[3] B. A. Bash, N. Chandrasekaran, J. H. Shapiro, and S. Guha, "Quantum key distribution using multiple gaussian focused beams," arXiv:1604.08582 [quant-ph] (2016).

[4] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, Phys. Rev. Lett. **105**, 153601 (2010).

[5] M. Mirhosseini, O. S. Magaa-Loaiza, M. N. OSullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, New Journal of Physics **17**, 033033 (2015).

[6] N. Horiuchi, Nat Photon **9**, 352 (2015), research Highlights.

[7] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Phys. Rev. Lett. **113**, 060503 (2014).

[8] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, New Journal of Physics **16**, 113028 (2014), arXiv:1402:2602 [physics.optics].

[9] M. Malik, M. O'Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. J. Lavery, M. J. Padgett, and R. W. Boyd, Opt. Express **20**, 13195 (2012).

[10] I. Djordjevic, Photonics Journal, IEEE **5**, 7600112 (2013).

[11] L. Jun-Lin and W. Chuan, Chinese Physics Letters **27**, 110303 (2010).

[12] N. Chandrasekaran and J. Shapiro, J. Lightw. Technol. **32**, 1075 (2014).

[13] N. Chandrasekaran, J. Shapiro, and L. Wang, J. Lightw. Technol. **32**, 1088 (2014).

[14] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gbps secret-key rates," arXiv:1510.08737 [quant-ph] (2015).

[15] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[16] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, Nat Commun **4** (2013), article.

[17] M. P. J. Lavery, D. Roberston, M. Malik, B. Robenburg, J. Courtial, R. W. Boyd, and M. J. Padgett, in *Proc. SPIE 8542* (2012) pp. 85421R–85421R–7.

[18] A. E. Willner, H. Huang, Y. Yan, Y. Ren, N. Ahmed, G. Xie, C. Bao, L. Li, Y. Cao, Z. Zhao, J. Wang, M. P. J. Lavery, M. Tur, S. Ramachandran, A. F. Molisch, N. Ashrafi, and S. Ashrafi, Adv. Opt. Photon. **7**, 66 (2015).