Multimode Fibers for Quantum-Secure Communication

Lyubov V. Amitonova
Complex Photonic Systems (COPS) and Biomedical Photonic Imaging (BMPI), University of Twente
Enschede, The Netherlands
l.amitonova@utwente.nl

Tristan B. H. Tentrup
Complex Photonic Systems (COPS)
University of Twente
Enschede, The Netherlands
t.b.h.tentrup@utwente.nl

Ivo M. Vellekoop
Biomedical Photonic Imaging (BMPI),
University of Twente
Enschede, The Netherlands
i.m.vellekoop@utwente.nl

Pepijn W. H. Pinkse
Complex Photonic Systems (COPS)
University of Twente
Enschede, The Netherlands
P.W.H.Pinkse@utwente.nl

***Abstract*—Multimode fibers support a multitude of transverse optical modes. These modes are mixed by the fiber. By complex wavefront shaping through the multimode fiber, we can undo this mixing, making it possible to communicate through the fiber even at very low light levels.**

Keywords—multimode fibers, quantum communication, high spatial dimension, wavefront shaping

I. INTRODUCTION HIGH DIMENSIONAL QUANTUM OPTICS

Textbooks in quantum optics usually start with low-dimensional systems, considering for instance the polarization degree of freedom of a photon. This two-dimensional Hilbert space already allows to treat key quantum-optical concepts such as entanglement, quantum interference and quantum cryptography. The latter requires a single spatial mode to transmit the photons from the sender to the emitter. For long distance communication without free sight, single-mode optical fibers are ideally suited.

Interestingly, for some applications like quantum-cryptography, one can get in the regime where one requires a quantum description with many more quanta of light by increasing the number of modes. This principle is used in quantum-secure authentication [1], where few-photon wavefronts are used to interrogate multiple-scattering media that serve as physical unclonable keys. Physical unclonable keys are a security primitive advocated in a seminal paper by Pappu *et al.* [2], in which it is argued that technology does not allow to copy a sufficiently complex and large multiple-scattering medium. Such keys naturally work with thousands of transverse optical modes coupled to each other, so that the ratio of the largest irreducible block of its scattering matrix to the size of the matrix is large, guaranteeing sufficient complexity. We could experimentally demonstrate that already a single photon in such a very high dimensional Hilbert space allows to encode more than 10 bit of information [3]. This high information density of single photons therefore allows, in principle, a higher communication rate. Moreover, the high transverse spatial dimensions allow to interface with physical unclonable keys. To transmit high-dimensional wavefronts one again needs a free line of sight or a multimode or a multicore optical fiber. It is therefore a highly relevant question to what extent multimode fibers are suitable for the transmission of complex (many spatial dimensions) wavefronts.

II. MULTIMODE FIBERS

Compared to single-mode fibers, the larger core of a multimode fiber allows a multitude of transverse optical modes, which can be used to transmit more information in parallel but also complicates their use, since these modes mix. This mixing leads to a speckle-like image at the output of the fiber even if only a single spatial mode at the input is excited. To some degree this mixing can be modeled [4]. An alternative approach is to treat the multimode fiber as a completely random multiple scattering medium and use the technique of complex wavefront shaping [5] to compensate for the distortion caused by the fiber [6]. Multimode fibers have eigenmodes that conserve orbital angular momentum. We found that this leads to a rotational memory effect: if only a single spot at the input facet is excited and rotated around the central axis of the fiber, the speckle-like pattern at the output -in a very good approximation- merely rotates over the same angle [7]. Only if the rotation becomes very large, the speckle pattern also decorrelates from the rotated original. A consequence of this finding is that in imaging applications where one would like to scan a spot at the output of the multimode fiber, one does not need to find as many independent complex input wavefronts; rotational scanning of the wavefront-shaped output focus spot can be performed by rotating the generating input wavefront. The spot size is limited by the NA of the fiber, which is set by the index contrast between core and cladding. By using custom-made photonic-crystal fibers, we have been able to make a record-small spot size with a subwavelength waist [8]. Interestingly, this spot can be aberration-free over a large fraction of the output facet [9]. With multimode fibers well-enough understood, we can now turn to incorporating them in a quantum-cryptography scheme.

The most popular quantum cryptography schemes are all based on the quantum-no-cloning theorem: The sender Alice sends photons in quantum states which are not all orthogonal. Bob measures these states along randomly chosen basis vectors. Later, Alice and Bob compare -via an authenticated classical channel- their choices of basis vectors and only keep those

We acknowledge funding by Netherlands Organisation for Scientific Research (NWO).

978-1-5386-5343-2/18/$31.00 ©2018 IEEE

events where they happened to choose the same. Since any intercept-and-resend attack by an eavesdropper will lead to extra noise, this will be detected. An issue with all quantum-secure cryptography schemes today, however, is that they require an authenticated classical or quantum channel to prevent man-in-the-middle attacks where an attacker impersonates Bob in his communication to Alice and vice versa. In practice the authentication is provided by an à priori shared key, which makes the scheme symmetric, which is disadvantageous

It has been realized that encoding in higher dimensions increases the security of a quantum cryptography scheme [10], and substantial progress has been made in encoding in time-frequency bins [11-12], orbital angular momentum [13-15] or other transverse schemes [16]. In [17] we combine these ideas and devise a communication scheme of which the basis idea is sketched in Fig. 1: Alice sends information to Bob in a few-photon wavefront that will focus to a spot at Bob's side of the fiber. Different spots encode for different symbols of an alphabet. Assuming a part of the fiber is under Bob's control, an eavesdropper will necessarily see a speckle-like pattern instead of a focused spot, so that the exact position of photon clicks in her photon-sensitive camera are to a large degree random. Important in this respect is that the number of photons should be less than the number of spatial modes of the fiber. In [17] we analyze bounds on the amount of information that can be collected by Eve in comparison to the amount of information that is shared between Alice and Bob, given realistic parameters. This of course depends on the number of photons and their statistics that is used in sending the information. In the ideal situation with a single-photon light source and perfect wavefront shaping, the maximum amount of information that Bob can read out per received photon is $H_{\mathrm{B}} = \log_2(S)$. Where S is the number of symbols used which is only limited by the number of fiber modes. For thousands of fiber modes H_{B} can be more than 10 bit of information. In contrast, Eve gains only $\langle H_{\mathrm{E}} \rangle = 0.61$ bit of information at maximum, regardless of the number of symbols or modes.

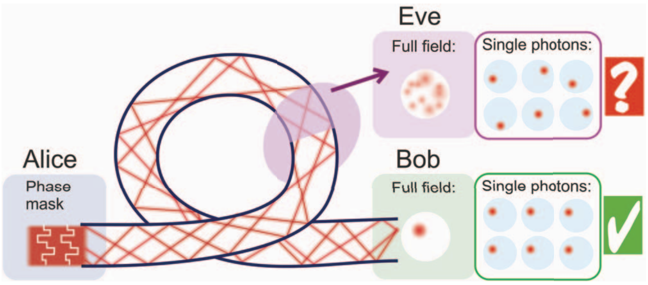

Fig. 1. Idea of quantum communication via a multimode fiber: a few-photon wavefront is sent by Alice to Bob. The wavefront is chosen such that it will focus to a specific spot encoding for a symbol at Bob's end. Eve, who can only tap off the fiber at an intermediate spot, will see a speckle-like image which can learn her much less.

An important assumption is that an Eavesdropper cannot make a passive optical devise that can mimic the transformation properties of Bob's piece of the fiber. In [17] we assume that Bob can make random perturbations to his part of the fiber, making a passive optical device that mimics this reconfiguring part of the fiber a daunting task. In future, we would like to exploit these results to incorporate authenticated communication via a true multiple-scattering medium [18] in combination with readout via a multimode fiber.

Acknowledgment

We acknowledge Cornelis Harteveld, Allard Mosk, Boris Škorić, Ravitej Uppu, and Willem Vos for support and discussions.

References

[1] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, "Quantum-secure authentication of a physical unclonable key," Optica 1, pp. 421-424, 2014.

[2] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," Science 297, pp. 2026-2030, 2002.

[3] T. B. H. Tentrup, T. Hummel, T. A. W. Wolterink, R. Uppu, A. P. Mosk, and P. W. H. Pinkse, "Transmitting more than 10 bit with a single photon," Opt. Express 25, pp. 2826-2833, 2017.

[4] T. Cižmár and K. Dholakia, "Exploiting multimode waveguides for pure fibre-based imaging," Nat. Commun. 3, pp. 1027:1-9, 2012.

[5] A. P. Mosk, A. Lagendijk, G. Lerosey, and M. Fink, "Controlling waves in space and time for imaging and focusing in complex media (Review)," Nat. Photon. 6, pp. 283-292, 2012.

[6] T. Čižmár and K. Dholakia, "Shaping the light transmission through a multimode optical fibre: complex transformation analysis and applications in biophotonics," Opt. Express 19, pp. 18871–18884, 2011.

[7] L. V. Amitonova, A. P. Mosk, and P. W. H. Pinkse, "The rotational memory effect of a multimode fiber," Opt. Express 23, pp. 20569-20575, 2015.

[8] L. V. Amitonova, A. Descloux, J. Petschulat, M. H. Frosz, G. Ahmed, F. Babic, X. Jiang, A. P. Mosk, P. S. J. Russell, and P. W. H. Pinkse, "High-resolution wavefront shaping with a photonic crystal fiber for multimode fiber imaging," Opt. Lett. 41, pp. 497-500, 2016.

[9] A. Descloux, L. V. Amitonova, and P. W. H. Pinkse, "Aberrations of the point spread function of a multimode fiber due to partial mode excitation," Opt. Express 24, pp. 18501-18512, 2016.

[10] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Phys. Rev. Lett. 88, pp. 127902:1-4, 2002.

[11] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States," Phys. Rev. Lett. 98, pp. 060503:1-4, 2007.

[12] T. Zhong, *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New J. Phys. 17, pp. 022002:1-10, 2015.

[13] M. Mafu, *et al.*, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," Phys. Rev. A 88, pp. 032305:1-8, 2013.

[14] M. Mirhosseini, *et al.*, "High-dimensional quantum cryptography with twisted light," New J. Phys. 17, pp. 033033:1-12, 2015.

[15] M. Krenn, *et al.*, "Generation and confirmation of a (100×100)-dimensional entangled quantum system," Proc. Natl. Acad. Sci. U.S.A. 111, pp. 6243-6247, 2014.

[16] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, "Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits, " Phys. Rev. Lett. 96, pp. 090501:1-4, 2006.

[17] L. V. Amitonova, T. B. H. Tentrup, I. M. Vellekoop, and P. W. H. Pinkse, "Multimode-fiber-based high-dimensional quantum secure communication," ArXiv.org\1801.07180, 2018.

[18] R. Uppu, T. A. W. Wolterink, S. A. Goorden, B. Chen, B. Škorić, A. P. Mosk, and P. W. H. Pinkse, "Asymmetric Cryptography with Physical Unclonable Keys," ArXiv.org\1802.07573, 2018.