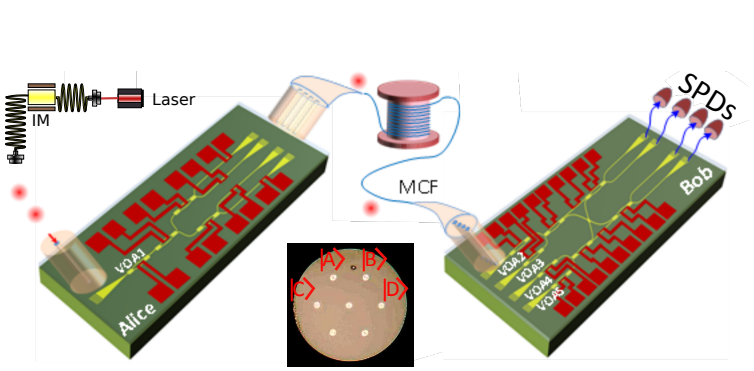
Quantum key distribution over multicore fiber based on silicon photonics.

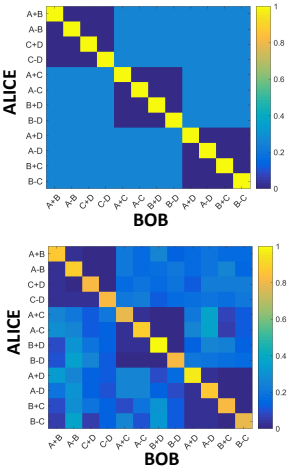
Yunhong Ding[†] [1], **Davide Bacco***[1], **Kjeld Dalgaard**[1], **Xinlun Cai**[2], **Xiaoqi Zhou**[3], **Karsten Rottwitt**[1], **and Leif Katsuo Oxenløwe**[1]

[1] *Department of Photonics Engineering, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark.*
[2] *School of Electronics and Information Technology, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou, China*
[3] *School of Physics and Engineering, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou, China*
[†] *yudin@fotonik.dtu.dk, * dabac@fotonik.dtu.dk*

Introduction In contemporary society, communication security has become increasingly important. The security of the current cryptosystems, based on mathematical assumptions, will not be guaranteed when quantum computers become available [1]. This has spurred investigations into new security technologies based on quantum physics. In order to exchange secure information between users, quantum key distribution (QKD), a branch of Quantum Communications (QCs), provides good prospects for ultimate security based on the laws of quantum mechanics [2–7]. Most of QKD systems are implemented in a point-to-point link using bulky, discrete and expensive devices. Consequently, a large scale deployment of this technology has not been achieved. In a future scenario, where QCs will become standard technology, and where infrastructures like banks and government buildings, will be connected through a quantum network, different requirements in terms of key generation are needed. A solution may be represented by new technologies applied to quantum world. In particular multicore fiber (MCF) open a new scenario for quantum communications, from high-dimensional (HD) spatial entanglement generation, to HD QKD and multi-user key generations, to HD-entanglement distribution. Furthermore, MCFs are expected as a good candidate for overcoming the capacity limit of a current optical communication system, as example the record capacity of 661 Tbits/s was obtained last year with a 30-cores fiber [8]. Proof of concept experiment has already proved the coexistence of classical and quantum communications transmitted into different cores of MCF [9]. On the other hand, photonic integration has played a critical role in recent quantum information revolution by integrating functionalities of traditional discrete bulky components into ultra-compact chips [10, 11]. In fact, integrated photonic circuits provides excellent performances (compacts, good optical phase stability, access to new degrees of freedom), and are particularly suitable for the manipulation of quantum states. Some recent experiments have already demonstrated conventional binary QKD systems, using polarization and phase reference degrees of freedom [12, 13]. Moreover, by using integrated solution new high-dimensional quantum states can be generated and propagated. Based on compact silicon photonic integrated circuits, we here show how a MCF can be used for quantum communications protocols by proving decoy-state HD-QKD and multi-users quantum key generations.



(a) Experimental setup



(b) MUBs

Fig. 1 The setup used in the HD-QKD proof of concept experiment in (a). In (b) are reported MUBs tomographies (theoretical and experimental). By using the (classical) definition of fidelity ($F(x,y) = \sum_i \sqrt{p_i q_i}$, we obtain 0.977 ± 0.01

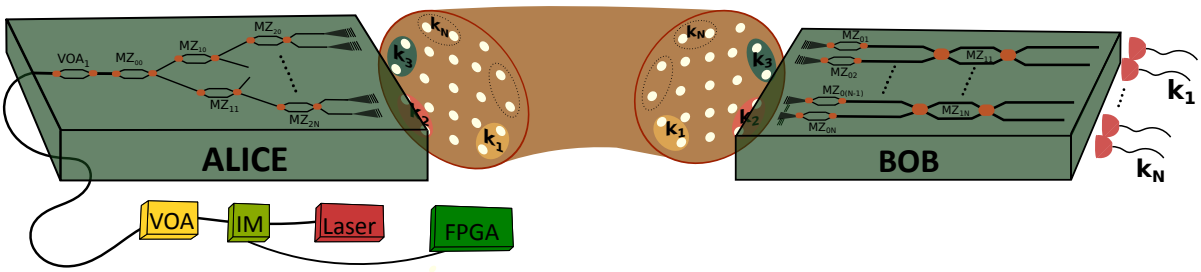
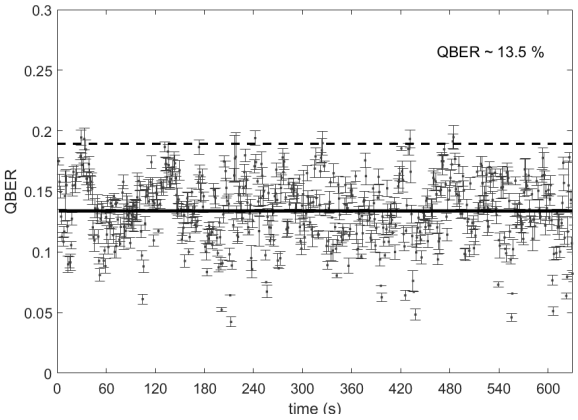


Fig. 2 The setup used in the multi-user BB84 QKD experiment. A train of weak coherent pulses is injected into a silicon chip. By actively tuning the MZIs, independent quantum keys are encoded in symmetric decoy-state BB84 protocol based on space division multiplexing. In this way Alice can generate multiple keys with Bob $(k_1, k_2, \cdots, k_N)$

Results High-dimensional quantum states are suitable for longer transmission distance and higher secret key rate transmission, being more robust to noise level and allowing an higher channel capacity [14]. In (Fig. 1(a)) we reported the chip design of the HD decoy-state quantum key distribution protocol based on spatial degrees of freedom (the cores of a multi-core fiber -MCF-). By tuning cascaded Mach-Zehnder interferometers (MZIs), it is possible to prepare HD quantum states in different mutually unbiased basis (MUBs) (Fig. 1 (b)). In particular we used three MUBs defined as: basis $M_0 = \{A+B, A-B, C+D, C-D\}$, basis $M_1 = \{A+C, A-C, B+D, B-D\}$, and basis $M_3 = \{A+D, A-D, B+C, B-C\}$, where $|A\rangle$, $|B\rangle$, $|C\rangle$ and $|D\rangle$ are the quantum states related to the four individual cores. In order to exchange the key between Alice and Bob, a train of weak coherent pulses is injected into the transmitter chip, where multiple variable optical attenuators (VOAs) are used to decrease the number of photons per pulse ($\mu < 1$) [15]. Furthermore, through a combination of active MZIs and VOAs, a decoy state-technique is implemented to avoid particular eavesdropping intrusion, like photon-number-splitting (PNS) attack. During the key generation process, Alice, by using an FPGA board (Fig. 1(a)), randomly chooses one of the bases and one of the four states to transmit to Bob. The ququart are matched to four cores of a multi-core fiber, through a highly efficient MCF grating coupler. After the transmission link, the quantum states are coupled into Bob's chip (Fig. 1(a)) through the MCF coupler, and randomly measured in one of the bases. In the subsequent distillation process, counts measured in the wrong bases are discarded [16]. Acquired experimental data, see Fig. 3(a), show stable and good results for more than 11 minutes of measurement with a quantum bit error rate (QBER) below the threshold of individual and coherent attacks. Recently other works, based on a similar use of multicore fiber for quantum communication and high-dimensional spatial entanglement generation, were demonstrated [17, 18].



(a) QBER of HD-QKD

(b) QBER of multi-user QKD

Fig. 3 The quantum bit error rate (QBER) for HD-QKD is reported in (a) for 11 minutes of measurement. Solid black line is the average QBER of 13.4%; black dashed line (18.93%) is the limit of the coherent attacks. In (b) the measured QBER for one key (k_1) of the multi-user experiment. Solid black line is the average QBER of 4.7%; black dashed line (11%) is the limit of the coherent attacks.

Besides that, the concept of a multi-user QKD, where customers require parallel independent keys for everyday actions, must be explored for future quantum networks. Multiple structures, based on various principles, and different realization systems, can be explored to meet these challenges. In particular, diverse topology schemes can be examined: wavelength division multiplexer (WDM), code division multiplexer (CDM), time division multiplexer (TDM) or active multiple switch, are acceptable solutions for a concrete implementation in a quantum network [19, 20]. Nonetheless, all of these methods require extra devices on the line introducing additional losses

and cross-talk, which can compromise the final key rate and the security of the systems. We provide a solution for generating parallel and independent quantum keys, by using a silicon chip transmitter and exploiting the concept of space division multiplexing in a MCF. By adopting a single laser source we realized a proof of concept (POC) experiment that demonstrates the generation of multiple quantum keys implementing decoy-state BB84 protocol. Particularly we encoded the qubits on multiple cores of a MCF, in such a way that, every two cores, a set of two mutually unbiased bases is generated. The basis $\mathcal{X}_1$ is defined as $(|A\rangle\,;|B\rangle)$ and basis $\mathcal{Z}_1$ like $(|A+B\rangle\,;|A-B\rangle)$. On the other side, it follows that the states $\{|C\rangle\,,|D\rangle\} \in \mathcal{X}_2$ and $\{|C+D\rangle\,,|C-D\rangle\} \in \mathcal{Z}_2$ as reported in Figure 2. In this way is possible to generate at the same time multiple quantum keys (k_1, k_2, $\cdot$, k_N), which will be independent one to each other and ready to be used by different customers at the receiver side. In relation to the HD-QKD, also in this case the acquired data, see Fig. 3(b), proved a stable result for more than 10 minutes of acquisition, by showing an average QBER of 4.7% well below the threshold of individual and coherent attacks.

Conclusion Advanced silicon technology was used to prove multiple quantum communication protocols over a multicore fiber. Decoy-state HD-QKD and multi-user QKD were designed and implemented. The combination of space division multiplexing with silicon photonics will be a major player in the future of quantum technology.

Funding This work is supported by the Danish Council for Independent Research (DFF-1337-00152 and DFF-1335-00771), by the Center of Excellence, SPOC (Silicon Photonics for Optical Communications (ref DNRF123) and from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA grant agreement n° 609405 (COFUNDPostdocDTU).

References

[1] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)
[2] C. H. Bennett, G. Brassard, Quantum Cryptography: public key distribution and coin tossing, in Proceeding of IEEE International Conference on Computer, Systems & Signal Processing 175–179 (1984).
[3] V. Scarani et al., The security of practical quantum key distribution. *Reviews of Modern Physics*, **81(3)**, 1301–1350 (2009)
[4] X. Ma et al., Practical decoy state for quantum key distribution, *Phys. Rev. A*, **72(1)**, 012326 (2005)
[5] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
[6] D. Bacco et al., Two-dimensional distributed-phase-reference protocol for quantum key distribution, *Sci. Reports* **6**:36756 (2016)
[7] T. Zhong et al., Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding, *New J. Phys.*, **17**, 022002 (2015).
[8] H. Hu et al. "Single-Source AlGaAs Frequency Comb Transmitter for 661 Tbit/s Data Transmission in a 30-core Fiber," Proc. CLEO, (San Jose, USA), paper JTh4C.1, June 2016.
[9] J. F. Dynes et al., Quantum key distribution over multicore fiber, *Opt. Exp.* **24**, 8081-8087 (2016)
[10] J. C. F. Matthews, A. Politi, A. Stefanov, J. L. O'Brien, Manipulation of multiphoton entanglement in waveguide quantum circuits, *Nature Photon.*, **3**, 346-350 (2009).
[11] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu. J. L. O'Brien, Silica-on-silicon waveguide quantum circuits, *Science* **320**, 646-649 (2008).
[12] P. Sibson et al., "Chip-based Quantum Key Distribution," *Nat. Commun.* **8**:13984 (2017)
[13] C. Ma et al., "Silicon photonic transmitter for polarization-encoded quantum key distribution," *Optica* **3** (2016)
[14] N. J. Cerf et al. Security of Quantum Key Distribution Using d-level system. *Phys. Rev. Lett.* **88** (2002)
[15] Y. Ding et al., "High-Dimensional Quantum Key Distribution based on Multicore Fiber using Silicon Photonic Integrated Circuits," arXiv:1610.01812 (2016)
[16] K. Saitoh and S. Matsuo, Multicore Fiber Technology *Journal of Lightwave technology*, **34**, (2016)
[17] G. Cañas et al., High-dimensional decoy-state quantum key distribution over 0.3 km of multicore telecommunication optical fibers, *arXiv:1610.01812* (2016)
[18] H. J. Lee, S. K. Choi, and H. S. Park, Experimental demonstration of high-dimensional photonic spatial entanglement between multi-core optical fibers, *arXiv:1610.04359* (2016)
[19] M. Smania et al., Experimental quantum multiparty communication protocols. *Npj Quantum Information*, **2** 16010 (2016)
[20] B. Fröhlich et al., A quantum access network. *Nature*, **501(7465)** (2013)