PIC Technologies for Quantum Secure Communications

Taofiq K. Paraïso*, Thomas Roger, Davide G. Marangon, Innocenzo De Marco, Mirko Sanzaro, Robert I. Woodward, James F. Dynes, Zhiliang Yuan & Andrew J. Shields
Toshiba Europe Ltd. Cambridge, UK
* taofiq.paraiso@crl.toshiba.co.uk

PICs offer unique opportunities for low-cost, highly-scalable quantum cryptographic systems. However numerous challenges such as packaging, power consumption and interfacing multiple chips in real-time, have for long impeded the demonstration of a standalone PIC-based QKD system. Here we show how we tackled these challenges to realize such a system with strong capabilities including autonomous operation without user intervention over multiple days and high secure key rates over all metropolitan distances.
Keywords: *quantum communications; quantum key distribution; diode lasers; optical injection locking; direct modulation; photonic integrated circuits*

INTRODUCTION

Quantum key distribution (QKD) systems based on discrete optics have been demonstrated in many scenarios and are now widely considered a mature technology. New approaches are now required to reduce the size, weight and power and to stimulate its wide-scale deployment. Integrated quantum photonics is an excellent candidate to address this question as it can easily interface with existing infrastructure [1]. Indeed, quantum communications is expected to be one of the first applications of integrated quantum photonics to reach maturity [2]. Quantum photonic chips have already been used to demonstrate a variety of QKD protocols [3-6]. However, these developments were all limited to proof-of-concept demonstrations, without presenting a fully deployable chip-based QKD system [7-9]. This challenging step requires one to overcome a range of shortcomings within the photonic design, the choice of integrated platform and from incorporation with bespoke high-speed electronics. In this paper we achieve this milestone by demonstrating a complete and viable real-time point-to-point QKD system based on integrated photonic circuits packaged into compact pluggable modules.

The photonic hardware comprises a quantum transmitter (QTx) chip, quantum receiver (QRx) chip and two quantum random number generator (QRNG) chips, co-designed to form a QKD system capable of operating at GHz clock rates. We implement a mix of different integrated photonic platforms, which best suit the specific requirements of the various components within the system. Quantum keys are phase encoded on the emitted attenuated laser pulses using the T12-BB84 protocol [10] for elevated efficiency. The protocol uses multiple fluxes (decoy intensities) to ensure security. We use 4 phase states produced in 2 non-orthogonal bases (X [0, π] and Z [π/2, 3π/2]) and 3 pulse intensities (signal [u], decoy [v] and vacuum [w]). We demonstrate the stable system performance over multiple days of use with a feedback system acting only on the transmitter's phase.

The quantum transmitter chip is a directly phase-modulated light source that encodes photons via direct modulation and optical injection locking (OIL) [6]. The chip is built on the indium phosphide (InP) platform, which allows for integration of active components such as lasers and modulators. Fig. 1a shows an overview of the QKD system and the integrated photonic devices used within. The transmitter chip contains two distributed feedback (DFB) lasers, a Mach-Zehnder interferometer and an electro-absorption modulator (EAM). The direct-phase modulated light source scheme [12] has the advantage of producing phase-encoded pulses with high-fidelity, short duration and high repetition rate (2 GHz), without the need for electro-optic phase modulators, and therefore compact and power efficient for chip integration. The encoded pulses of light are then modulated in intensity using an EAM to produce decoy states. The selection probabilities used to encode the orthogonal bases and the pulse intensities are optimized to provide high secure key rates.

The quantum receiver includes a discrete optics high-speed phase modulator and a passive silicon-based photonic chip. The chip consists of an asymmetric Mach-Zehnder interferometer that has a relative temporal delay between the two arms of 500 ps. The interferometer measures the phase difference between consecutive pulses emitted by the transmitter. The phase modulator is used to choose the measurement basis. Photons exiting the interferometer outputs are detected via two avalanche photodiodes (APDs) and correspond to pulses measured in the two 'bit' values of each of the measurement bases (X, Z). The APDs are gated at 1 GHz and centered on the photon pulses carrying the encoded phase states.

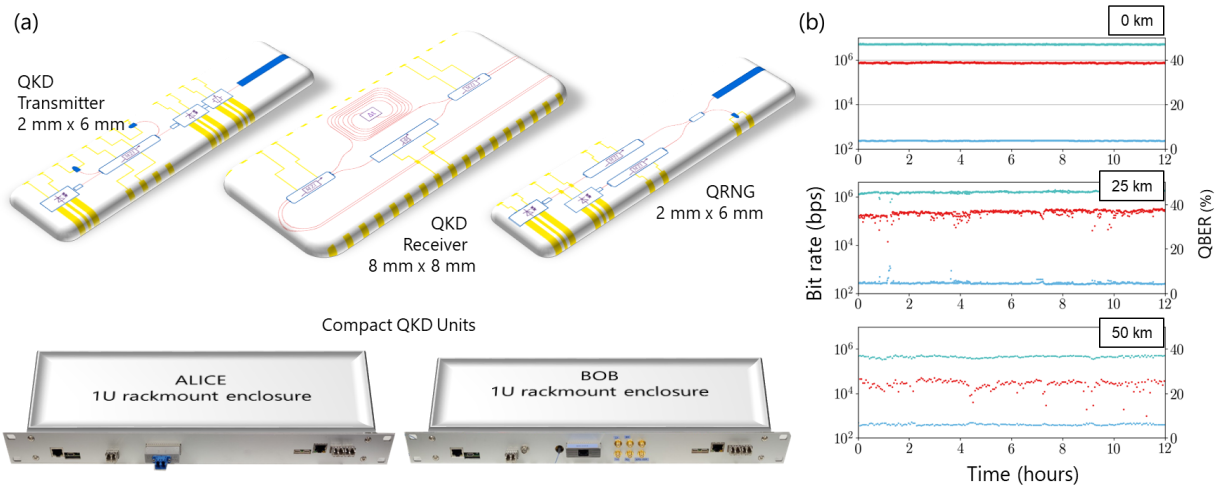

Fig. 1. (a) Photonic integrated quantum key distribution system. The system consists of a QTx unit and a QRx unit, each featuring a QRNG chip and a quantum communication chip. Random numbers generated continuously are used in real-time to encode and decode the quantum key information. Pluggable modules are used to package the QKD optics and the complete optoelectronics electronics is assembled in compact 1U rackmount enclosures. (b) Stable operation over extended periods of time is achieved over all metropolitan distances.

The QRNGs are also based on InP photonic chips, similar to the transmitter. These devices are typically omitted from QKD demonstrations, as sources of pseudo-random numbers can be used in their place as proof-of-concept. However, such omission is an important drawback for real QKD systems as the security of a QKD key directly relies on it being impossible to predict how the photons are encoded. We use QRNGs that exploit spontaneous emission phase noise in gain-switched laser diodes [9, 13]. Due to the typically low bit rates of these types of devices their implementation in QKD systems has been challenging. Here, we overcome this challenge by demonstrating QRNGs that produce verified random numbers at 4 Gb/s.

Table 1. Secure key rates achieved over different length quantum channels

Quantum channel length	**SKR**	**QBER**
0 km	**726 kbps**	**3.72 %**
10 km	**470 kbps**	**4.50 %**
25 km	**235 kbps**	**4.66 %**
50 km	**28 kbps**	**6.15 %**

RESULTS

The system capabilities were initially proven by connecting the transmitter and receiver with a short (few meters of single-mode fiber) quantum channel. QKD keys were generated with a sifted rate of 5.02 Mbps. Following error correction and privacy amplification algorithms, information theoretic secure keys are generated with a rate of 726 ± 35 kbps (see Fig. 1b). Measurements with 10 to 50 km of standard SMF-28e fiber were then acquired. The fibers spools were stored locally and connected between the two system units in the quantum channel. Table 1 reports the performance over different channel lengths. At 10 km, we found an average secure key rate of 470 ± 110 kbps.

To confirm the compatibility with real-life deployment, classical data encryption systems were connected to the system. The encryptors withdraw quantum keys from the units every minute. 352 bits of quantum key information are then used to form AES-256 keys (with a 96-bit initialization vector), which are capable of encrypting 100 Gb/s of data. These commercially available encryptors operate seamlessly with our chip-based QKD system, demonstrating its compatibility within existing optical communication infrastructure. We report continuous operation without user intervention over 11 days, at a rate sufficient to serve 1335 AES-256 keys per second and therefore to supply multiple encryptors simultaneously [14].

DISCUSSION

Our results establish the viability of quantum photonic integration for use in realistic quantum communications systems. This marks an important step for the practical deployment of quantum communication technologies based on quantum photonic chips. Reducing the cost and size of devices will allow for a significant increase in the manufacturability and reliability of these systems. As the fabrication processes for photonic integration continue to improve in terms of reproducibility, cost and volume, their use within commercial systems will become ubiquitous, allowing for easily upgradeable QKD systems, with reduced operational costs.

Acknowledgements: This work has been funded by the Innovate UK project AQUASEC, as part of the UK National Quantum Technologies Program.

References

[1] J. Wang, F. Sciarrino, A. Laing & M. G. Thompson, "Integrated photonic quantum technologies," Nat. Photonics **14,** 273–284 (2020).
[2] N. Gisin, G. Ribordy, W. Tittel & H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74,** 145 (2002).
[3] D. Bacco, Y. Ding, K. Dalgaard, K. Rottwitt & L. K. Oxenløwe, "Space division multiplexing chip-to-chip quantum key distribution," Sci Rep **7,** 1–7 (2017).
[4] C. Ma, *et al.* "Silicon photonic transmitter for polarization-encoded quantum key distribution. Optica **3,** 1274–1278 (2016).
[5] C. Ma, *et al.* "Integrated Silicon Photonic Transmitter for Polarization-Encoded Quantum Key Distribution," Optica Vol. 3 (2016).
[6] T. K. Paraïso, *et al.* "A modulator-free quantum key distribution transmitter chip," NPJ Quant. Inf. **5,** 1–6.
[7] F. Xu, X. Ma, Q. Zhang, H.-K. Lo & J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92,** 25002 (2020).
[8] P. Sibson, *et al.* "Chip-based quantum key distribution," Nature communications **8,** 13984 (2017).
[9] T. Roger *et al.* "Real-time interferometric quantum random number generation on chip," JOSAB **36,** B137-B142 (2019).
[10] M. Lucamarini, *et al.* "Efficient decoy-state quantum key distribution with quantified security," Optics express **21,** 24550–24565 (2013).
[11] J. Qiu, "Quantum communications leap out of the lab," Nature News **508,** 441 (2014).
[12] Z. L. Yuan, *et al.* "Directly Phase-Modulated Light Source," Phys. Rev. X **6,** 325 (2016).
[13] C. Abellan, *et al.* "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica **3,** 989 (2016).
[14] T. K. Paraïso, *et al.* "A photonic integrated quantum secure communication system", Nature Photonics **15**, 850-856 (2021).