Integrated Photonic Devices for Quantum Key Distribution

Philip Sibson[1], Chris Erven[1], Mark Godfrey[1], Shigehito Miki[2], Taro Yamashita[2], Mikio Fujiwara[3], Masahide Sasaki[3], Hirotaka Terai[2], Michael G. Tanner[4], Chandra M. Natarajan[4], Robert H. Hadfield[4], Jeremy O'Brien[1], Mark G. Thompson[1]

Centre for Quantum Photonics, H.H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom

National Institute of Information and Communications Technology (NICT), 588-2 Iwaoka, Kobe 651-2492, Japan

National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan

School of Engineering, University of Glasgow, G12 8QQ, United Kingdom

We demonstrate a fully integrated photonic transmitter and receiver for time-bin based multi-protocol quantum key distribution. This GHz rate Indium Phosphide device prepares states for Coherent One Way (COW), Differential Phase Shift (DPS), and BB84 protocols and is decoded by a Silicon Oxynitride (Triplex) receiver.

Quantum Key Distribution (QKD) is one of the first commercially available quantum technologies and provides a means for distributing shared secret random keys between two users (Alice and Bob) in order to encrypt information sent between them. It has seen a number of long range demonstrations using either fibre or free-space links and many groups are actively working towards satellite communications [1–5]. Very recently, integrated photonics has developed to the point where it can provide a stable, compact, miniaturized and robust platform which can be used to implement and manufacture complex photonic circuits including those required for QKD [6]. The phase stability of integrated photonics makes it particularly suitable for manipulating quantum information encoded in different time-bins, an encoding extensively used in fibre-based QKD communication systems.

A number of examples have demonstrated integrated components for QKD [7–11], while this work demonstrates a fully integrated Indium Phosphide (InP) transmitter (Alice) modulated at GHz rates for telecommunications channels and an integrated Silicon Oxynitride receiver (Bob), illustrated in Figure 1.

Figure 1(b) shows the 2x6mm^2 transmitter chip which incorporates an integrated tuneable laser, electro-optic modulators and photodiode that allow for multi-protocol reconfigurable operation. Figure 1(c) shows the 32x16mm^2 receiver chip which includes passive waveguide structures and thermo-optic phase modulators to allow for reconfigurable multi-protocol decoding.

The electro-optic modulators can operate at frequencies up to 10GHz and have been used to demonstrate 150ps FWHM pulses with a 600ps temporal separation. Using this, we have demonstrated multiple protocols including: Coherent One Way (COW) operating at 833MHz, Differential Phase Shift (DPS) at 1.67GHz, and BB84 at 556MHz clock rate. The receiver includes a reconfigurable delay within the decoding asymmetric-MZI for system flexibility, tuneable in steps of 300ps up to 2.1ns.

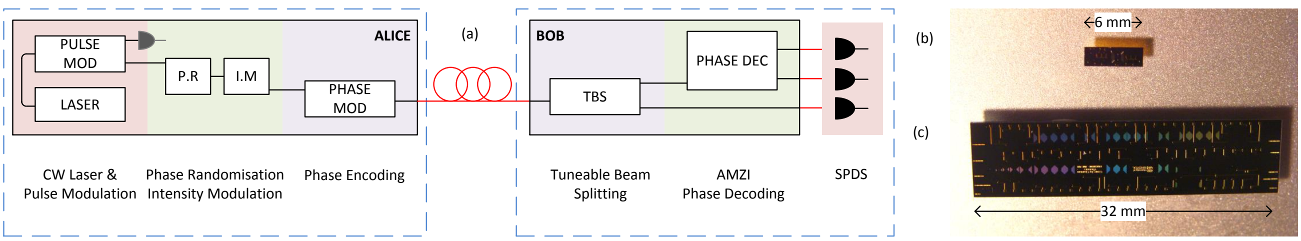

FIG. 1: (a) Schematic of the integrated reconfigurable multi-protocol QKD transmitter (Alice) and integrated receiver (Bob). Alice includes an integrated laser temporally modulated by an electro-optic amplitude modulator (PULSE MOD) monitored with an on-chip photodiode. The signal is phase randomised (P.R) and intensity modulated (I.M) before encoding relative phases between successive time-bins (PHASE MOD). The receiver includes a tuneable reflectivity optical splitter (TBS) for COW, followed by an asymmetric Mach-Zehnder interferometer (PHASE DEC) to decode DPS and BB84. (b) Scale of Indium Phosphide transmitter device (6mm x 2mm) and (c) Silicon Oxynitride photonic receiver device (32mm x 16mm).

This InP integrated photonic device in Figure 1(a) contains a wavelength-tuneable semiconductor laser source, constructed of a semiconductor optical amplifier and two tuneable distributed Bragg reflectors to form a cavity and produces light in the standard 1550nm telecommunication band. The continuous wave laser source is temporally modulated into 150ps FWHM pulses with a 600ps temporal separation, in pairs for BB84 or as pulse trains for COW and DPS. The pulse intensity can be monitored by the on-chip photodiode, and be used as feedback to stabilise the laser current. The temporally modulated coherent state is phase randomised, attenuated and intensity modulated with relative phases being encoded for both DPS and BB84.

The transmitted signals are decoded by an integrated Silicon Nitride (Triplex) receiver chip. The device has passive waveguide structures with thermo-optic phase modulators that are tuned to split the incoming signal, a proportion of which is directed towards single photon detectors directly for generating key in COW, the other proportions enters an asymmetric Mach-Zehnder interferometer with a reconfigurable discrete delay. To achieve good visibility a loss balancing MZI splits a higher proportion of the light into the long arm of the MZI. The two outputs of the decoding circuit are coupled to off chip superconducting single photon detectors, allowing for the reconfigurable multi-protocol operation.

This work demonstrates the feasibility of using fully integrated devices within QKD systems and the benefits of miniaturisation, reliability, manufacturability and reconfigurability that integrated photonics can provide for quantum communications and cryptography. This could lead to further adoption within practical telecommunication networks, mobile applications and personal devices.

[1] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[2] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, p. 010504, Jan 2007.

[3] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307km of optical fibre," *Nature Photonics*, vol. 9, pp. 163–168, Mar. 2015.

[4] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, no. 5, pp. 382–386, 2013.

[5] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, pp. 387–393, May 2013.

[6] M. G. Thompson, A. Politi, J. C. Matthews, and J. L. O'Brien, "Integrated waveguide circuits for optical quantum computing," *IET circuits, devices & systems*, vol. 5, no. 2, pp. 94–102, 2011.

[7] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with aplanar light-wave circuit mach-zehnderinterferometer," *Opt. Lett.*, vol. 29, pp. 2797–2799, Dec 2004.

[8] H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, and Y. Yamamoto, "10-ghz clock differential phase shift quantum key distribution experiment," *Opt. Express*, vol. 14, pp. 9522–9530, Oct 2006.

[9] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. Nock, J. Munns, D. Bonneau, P. Jiang, H. Li, *et al.*, "Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client," *Physical review letters*, vol. 112, no. 13, p. 130501, 2014.

[10] B. Korzh, N. Walenta, R. Houlmann, and H. Zbinden, "A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator," *Optics express*, vol. 21, no. 17, pp. 19579–19592, 2013.

[11] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, pp. 1–7, May 2015.