Wavelength-Division-Multiplexed QKD with Integrated Photonics

P. Sibson,[1] C. Erven,[1] and M. G. Thompson[1]

[1] *Centre for Quantum Photonics, University of Bristol, UK*

(Dated: April 2016)

This work experimentally demonstrates Wavelength-Division-Multiplexed QKD with integrated photonics for high-rate QKD. We use two GHz rate Indium Phosphide transmitters and a Silicon Oxynitride receiver with integrated wavelength de-multiplexing and two reconfigurable receivers for multi-protocol QKD. The increase in rates and the ability to scale up these circuits opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secured communications.

Quantum Key Distribution (QKD) provides a provably secure approach to share keys used to encrypt secret information by transmitting single photons through a quantum channel [1]. Integrated photonics provides a stable, compact, miniaturized, and robust platform to implement complex photonic circuits amenable to manufacture and therefore provide a compelling technology to implement future QKD systems [2]. We have previously demonstrated integrated technologies for QKD, including integrated "client" chips for Reference-Frame-Independent QKD [3], and the first chip-to-chip QKD with an Indium Phosphide device for GHz clock rates transmitter and a Silicon Oxynitride receiver providing compact, robust, stable, and reproducible photonics circuits for QKD [4].

The rates of QKD are severely limited due to channel loss and receiver efficiency, but channel capacity can be increased by multiplexing multiple signals on the same fibre, separated in wavelength (Wavelength-division-multiplexing QKD [5]). Although current QKD systems made from discrete components drastically restrict this approach due to practicality and size constraints in optical networks, the use of miniaturised integrated photonics can allow for higher component density and a manufacturable approach that can reproduce many copies of the same photonic circuitry.

Here, we demonstrate WDM-QKD with two GHz clocked InP QKD transmitters and a Silicon Oxynitride receiver with integrated de-multiplexing. The integrated transmitters and receiver allow for multiple protocols, including an efficient biased basis decoy state BB84 [6] operating at 565MHz with error rates ~1.5%, and an estimated secret key rate of 1.1 Mbit/s at 4dB loss (the equivalent of 20 km of fibre), compared to 571 kbit/s from a single operating channel.

The transmitting laser cavities are formed by two tunable-distributed Bragg reflectors surrounding a semiconductor optical amplifier, allowing for current injection to shift the wavelength of the central mode by approximately 10 nm with and applied voltage of 1.2 V. The two channels are separated by 200 GHz (standard dense-WDM channel spacing) and combined with a 50:50 fibre beam splitter, with which one arm can monitor the output power and allows for flexible tuning of the transmitter channels to match the receiver. The integrated circuitry is designed to encode time bin information for fibre communication (Figure 1 (left)) and allows for multi-protocol QKD transmission including BB84, COW, and DPS.

Using an on chip asymmetric MZI filter for wavelength de-multiplexing, the receiver splits the two channels in to

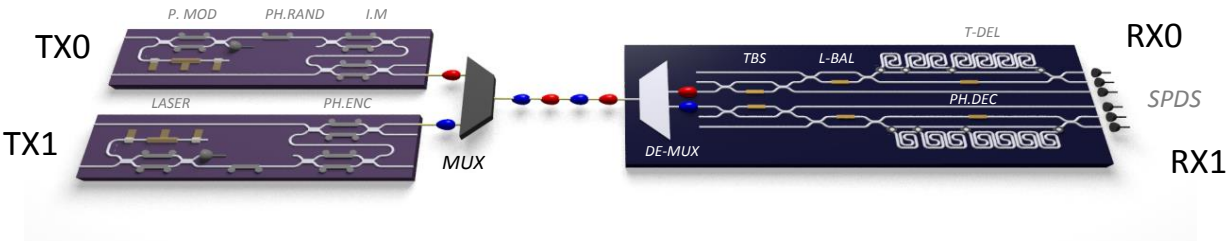

FIG. 1: **Integrated Photonic Devices for WDM-Quantum Key Distribution**. Schematic of the GHz clock rate, reconfigurable, multi-protocol, and integrated indium phosphide transmitter devices, which encode quantum information using time-bin encoded, weak coherent light to be transmitted over optical fibre. The silicon oxynitride receiver circuit passively decodes the quantum information using off-chip single photon detectors. The two transmitter lasers are offset by 200GHz, are passively combined with a beam splitter, and are temporally offset by half a period to decrease cross talk once the detector events are gated. The receiver unit includes on-chip de-multiplexing via an unbalanced MZI, with a free-spectral range of 200GHz, followed by two copies of reconfigurable multi-protocol receivers. These devices are capable of independently implementing BB84, COW, and DPS, and at multiple clock rates, allowing for extremely flexible operation of quantum secured communications in optical networks.

independent copies of the reconfigurable decoding circuitry (Figure 1 (right)). An MZI is used as a tunable beam splitter (TBS) to directly measure time of arrival information (Z basis) for a portion of the incoming signals. The other portion of the transmitted states enter an AMZI allowing the measurement of both the X and Z bases. This scheme allows for the implementation of biased basis measurements with independent channel control.

Although the AMZI filtering allows finite extinction in wavelength, temporal offsets of half a period between neighbouring channels also decreases cross-talk when gating the detector events in time. These two techniques allow for a negligible effect on the measured QBER compared to single transmitter communications and an estimated secure key rates ∼1.1Mbit/s for an emulated 20 km channel loss.

Improvements to the rates and channel capacity can be further made by reducing loss in the receiver module, moving towards scalable WDM de-multiplexing with array waveguide gratings (AWG), allowing for increased channels for a fixed insertion loss, and decreasing channel spacing.

This work experimentally demonstrates the feasibility of WDM-QKD with integrated photonics for high-rate QKD. By exploiting complex circuitry obtainable through integrated photonic technology, the practicality of WDM-QKD is improved due to the increase in component density, miniaturisation, robustness, and manufacturability of devices. The increase in rates and ability to scale up these circuits opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secured communications.

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

[2] J. M. J. O. M.G. Thompson, A. Politi, "Integrated waveguide circuits for optical quantum computing," *IET Circuits, Devices & Systems*, 2011.

[3] 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.

[4] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based Quantum Key Distribution," *ArXiv e-prints*, Sept. 2015.

[5] K. ichiro Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of wdm quantum key distribution system through a field fiber over 30 days," *Opt. Express*, vol. 21, pp. 31395–31401, Dec 2013.

[6] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, "Decoy-state quantum key distribution with biased basis choice," *Scientific reports*, vol. 3, 2013.