Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol's Activities in the UK Quantum Communications Hub

P. Sibson,[1] D. Lowndes,[1] S. Frick,[1,2] A. Price,[1,2] H. Semenenko,[1,2] F. Raffaelli,[1] D. Llewellyn,[1] J. E. Kennard,[1] Y. Ou,[3] F. Ntavou,[3] E. Hugues Salas,[3] A. Hart,[1] R. Collins,[1] A. Laing,[1] C. Erven,[1] R. Nejabati,[3] D. Simeonidou,[3] M. G. Thompson,[1] and J. G. Rarity[1]

[1] *Centre for Quantum Photonics, University of Bristol, UK*
[2] *Quantum Engineering Centre for Doctoral Training, University of Bristol, UK*
[3] *High Performance Network, University of Bristol, UK*

(Dated: April 2017)

We present Bristol University's recent activities in the UK Quantum Communications Hub, where we are developing short-range free-space QKD technologies, chip-scale quantum communication systems and, quantum-secured networking applications and demonstrations. This work presents a coherent framework for the development of quantum-secured networks and applications from government and commercial transactions to consumers and the home.

Since its launch in 2015, the vision of the UK Quantum Communications Hub [1] is to develop new quantum communications technologies [2] that will reach new markets, enabling widespread use and adoption in many scenarios. To achieve this target, on-going work at the University of Bristol, one of the Hub's partner universities, spans the following areas

- Short range, free-space, QKD technologies
- Chip-scale QKD technology
- Quantum communication networking

I. SHORT RANGE, FREE-SPACE QKD

We demonstrate a credit card size quantum key distribution (QKD) transmitter linked to a rack sized, wall mounted receiver. This short-range free-space QKD technology enables many-to-one communications for consumer, commercial and defence markets.

The transmitter comprises 4 LED chips behind a patterned glass polarizer, the light from these LEDs is collimated by a short piece of fibre optic to prepare BB84 [3] states in polarization. This also provides spatial filtering of the light but at the expense of applying a random rotation to the states on the Bloch sphere, this is constant for all states and as such can be calibrated out.

We have developed a docking solution based on a card slot which aligns the fibre ferrule on the transmitter to the receiver optics. The fixed node receiver hardware (the "Quantum ATM") features modular optics and electronics hardware to enable easier development and integration of different QKD protocols. Our current optics module is a six state QKD receiver, which allows for a live characterisation of the QKD transmitter and also presents the opportunity to upgrade our transmitters to a six state or reference-frame-independent protocol with future developments involving active tracking systems.

This system is intended to allow access into a larger quantum network for a wide audience by providing many small, low-cost, medium bandwidth devices which communicates with the "Quantum ATM".

II. CHIP-BASED QUANTUM COMMUNICATIONS

We demonstrate chip-based approach to quantum communications delivering compact, lightweight, robust, low-cost, low-energy devices for mass manufacture and widespread deployment [4]. Integrated photonics has provided such miniaturisation, manufacturability and reconfigurability required for demanding applications within classical telecommunication and photonic technologies, and has recently been adopted in many quantum technologies [5].

A quantum photonic interconnect has demonstrated the coherent distribution of qubit entangled states between two silicon-based devices [6], and can lead the way to further experiments in teleportation and multi-party communications.

We have demonstrated a GHz clocked chip-to-chip quantum communication system is demonstrated, employing InP-based transmitter and SiON-based receiver devices [7]. Performance is comparable to state-of-the-art with multi-protocol QKD operation achieved. Secure rates were further increased by use of biased-basis protocols and wavelength-division-multiplexing of two QKD transmitters and receivers. By exploiting the miniaturised technology and ease of manufacturing, the integrated photonic platform offers a scalable approach to overcome data rate limitations.

Quantum random number generator technology with integrated photonics allows for low-footprint devices to be fabricated achieving $\geq$1 Gbps of post-processed random numbers, improving security of both classical and quantum cryptographic systems [8]. Further improvements in security can be explored through the use of measurement-device-independent QKD, relieving detector technology vulnerabilities.

Further miniaturisation has been achieved by demon-

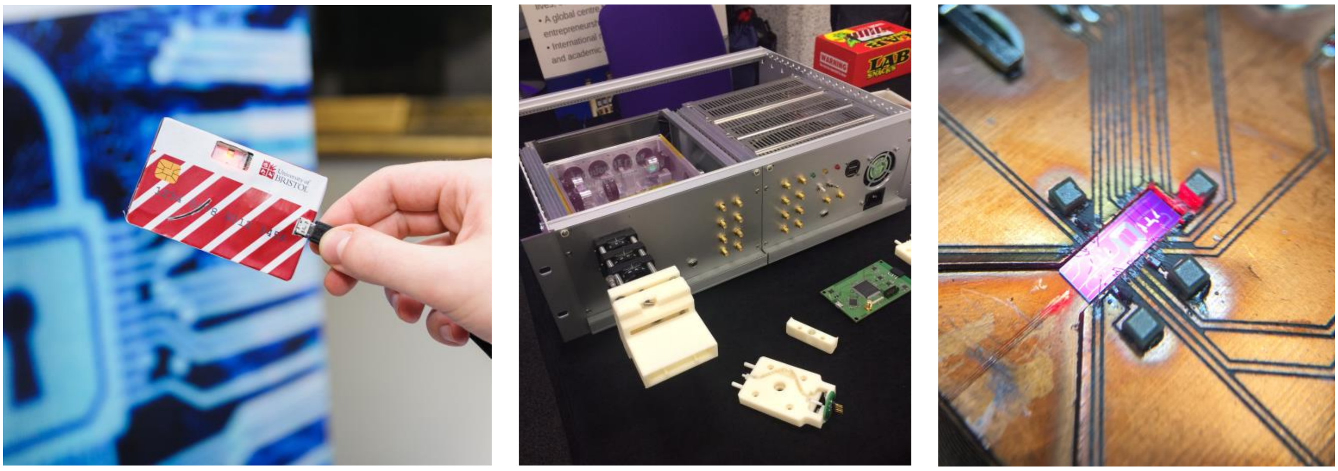

FIG. 1: **Short Range, Free-Space QKD and Chip-based Quantum Communications:** Prototype quantum-enabled "credit-card" and "ATM" as well as an integrated photonic QKD transmitter chip.

strating novel operation of circuits in a standard integrated silicon photonic platform [9]. By utilising high-speed carrier depletion modulation we have demonstrated QKD transmitters in a platform that is compatible with micro-electronic fabrication that could lead to the seamless integration of quantum photonic and electronic devices.

On-going development of bespoke photonic and electronic hardware and real-time software will enable remote deployment of chip-based QKD solutions, and the collaboration to develop suitable calibration and certification techniques with the UK National Physical Laboratory [10] will contribute to the effort towards standardisation for commercial devices.

III. QUANTUM-SECURED NETWORKS

We are developing technology for ubiquitous application of quantum security in communication networks, addressing the vital issues of telecommunications and cryptographic integration. We are working to establish a UK Quantum Network (UKQN) which integrates QKD into secure communication infrastructures at access, metropolitan and inter-city scales. Our networks are facilitating device and system trials, integration of quantum and conventional communications, and demonstrations for stakeholders, customers, the media and the wider public.

We have demonstrated the use of quantum-secured network-function-virtualisation (NFV) orchestration over an software-defined-network (SDN) controlled optical network with time-shared QKD resources [11]. This work enabled the secure orchestration of network functions with the use of commercial QKD systems [12]. This demonstration provides a real-world application and quantum-aware networks, with a reduced capital expenditure by time-sharing the transmitters and receivers of each node to ease adoption.

Further work includes the automated testing and characterisation of fibre networks for the deployment of QKD. This includes both Bristol-is-Open (BiO) [13] and the National Dark Fibre Infrastructure Service (NDFIS), where both metro-scale and long-haul QKD operation are demonstrated in single core bundles as well as multi-core fibres. This work provides infrastructure and resource for a quantum test-bed for experimental and commercial systems, as well as field-trials of quantum-enhanced applications.

[1] Quantum Communications Hub. http://www.quantumcommshub.net/, 2017.

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

[3] C. Bennett and G. Brassard in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, (New York), p. 175, 1984.

[4] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Npj Quantum Information*, vol. 2, no. 16025.

[5] A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," *Journal of Optics*, vol. 18, no. 8, p. 083002, 2016.

[6] J. Wang, D. Bonneau, M. Villa, J. W. Silverstone, R. Santagati, 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,

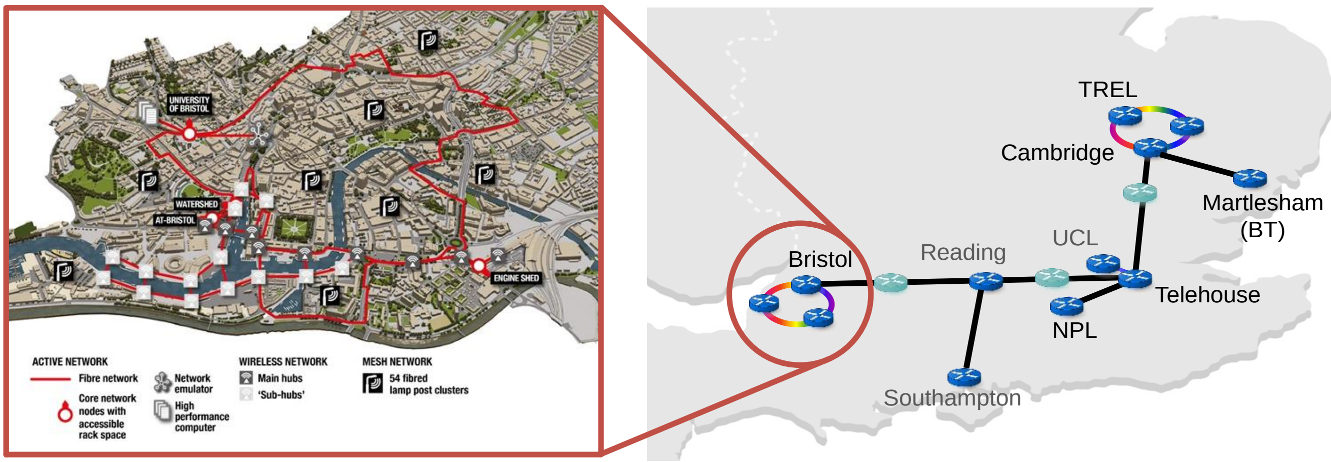

FIG. 2: **Quantum-Secured Networks:** The Bristol is Open (BiO) metro-scale network, and incorporation in to the UK Quantum Backbone utilising the National Dark Fibre Infrastructure Service (NDFIS) connecting partners from the the UK Quantum Communication Hub.

"Chip-to-chip quantum photonic interconnect by path-polarization interconversion," *Optica*, vol. 3, pp. 407–413, Apr 2016.

[7] 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. OBrien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Communications*, vol. 8, no. 13984.

[8] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "An On-chip Homodyne Detector for Measuring Quantum States and Generating Random Numbers," *ArXiv e-prints*, Dec. 2016.

[9] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," *Optica*, vol. 4, pp. 172–177, Feb 2017.

[10] National Physical Laboratory. http://www.npl.co.uk/, 2017.

[11] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, *et al.*, "Secure nfv orchestration over an sdn-controlled optical network with time-shared quantum key distribution resources," *Journal of Lightwave Technology*, 2016.

[12] idQuantique. http://www.idquantique.com/, 2017.

[13] Bristol is Open. http://www.bristolisopen.com/, 2017.