The Journal of Open Source Software

QComms QKD Software Toolkit

Mr Richard Collins[1] **and Djeylan Aktas**[1]

1 University of Bristol

DOI: 10.21105/joss.01119

Software

- Review
- Repository
- Archive

Submitted: 29 October 2018
Published: 17 June 2019

Summary

The purpose of this software is to provide a set of interfaces, algorithms and tools to produce a full QKD system. The aim is to reduce the barrier to entry into QKD systems by developing a strong architecture with well defined interfaces. The separation of responsibility into components will allow researchers to concentrate on a specific component, the rest of the system being provided by existing algorithms or simulators.

Quantum key distribution (QKD) uses properties of quantum states such as the no-cloning theorem to share randomness between different locations, without the need to physically transport the key material. This randomness is known to be secure because the probability of an eavesdropper can be calculated. This means that symmetric encryption instead of public key can be used, which can prevent attacks from quantum computers. Symmetric keys are only as secure as the medium they are transported over. Unlike QKD, manually exchanged key is expensive (e.g. physically driving somewhere with a flash drive) and has to be used sparingly. Making guaranteed secure key available as a resource makes symmetric keys more viable.

The system demonstrates that the symmetric keys can be used in a disposable manner rather than the current model where valuable keys are derived to extend their use. There are many utilities in place to simplify the use of the toolkit such as statistics collection for gathering data.

As well as optical device research, the system can be used to develop key management for networks.

Components

Statistics

The statistics component provides a means for publishing data from within an algorithm without adversely affecting the system's performance and allowing the data to be collected through a simple external interface.

Device drivers

The system currently include drivers for the IDQuantique Clavis 2 QKD devices. To use a device with the system, a driver needs to be written to provide data to one of the entry points of the pipeline. The driver could provide raw qubits, ready to use key or anything in between. Once a driver for specific hardware is written, the standard set of post processing tools can be used to extract usable key and provide statistics on the operation of the system as a whole.

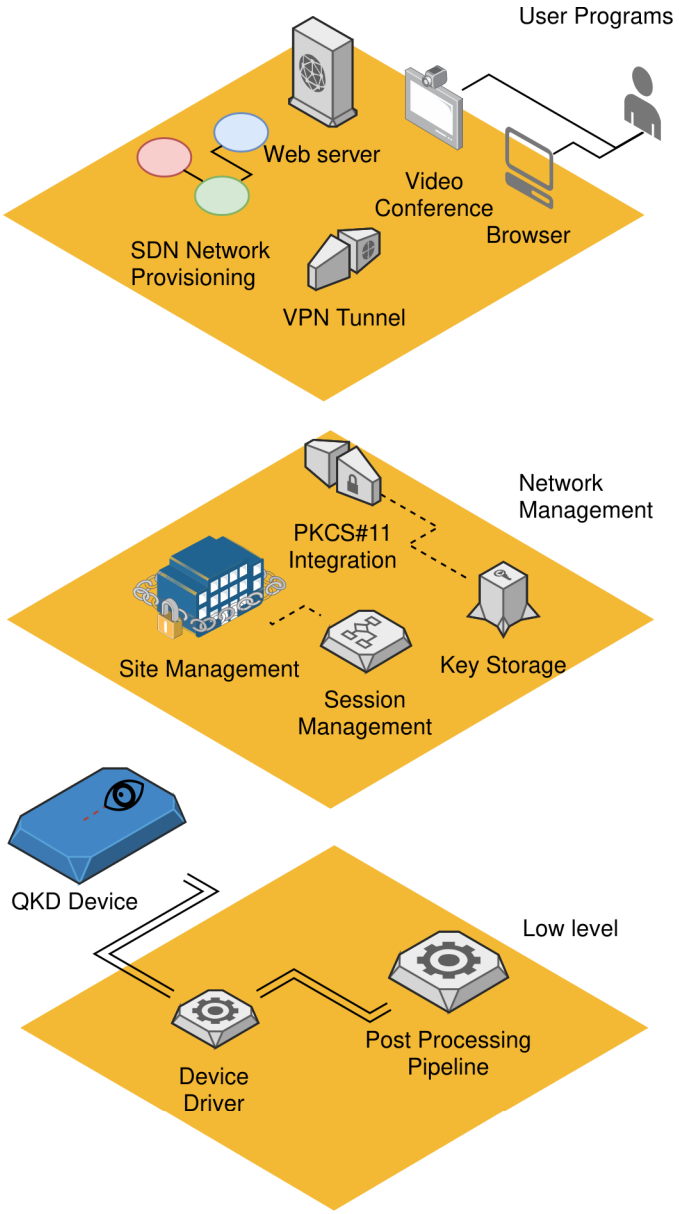

Figure 1: Toolkit Stack

Post Processing

Processing of Qubits is split into 4 sections:

- Alignment of receiver with transmitter, which involve a hardware check-up loop (laser power, noise measurement...) and a line length measurement loop.
- Sifting procedure (plug & play BB84 (Ribordy, Gautier, Gisin, Guinnard, & Zbinden, 2000)) that chose the proper states after an optical setting loop of phase adjustments and visibility measurements.
- Error correction of detected bits.
- Privacy amplification to obtain the final distilled key.

Once the key is produced by the post processing it is passed to the key store. Some of the algorithms have been adapted from David Lowndes paper (Lowndes, 2016).

Key Management

There are some issues unique to shared secrets which the current public key systems do not provide for, the system tackles some of these issues by providing a standardised interface to the keys. The key store classes hold keys for specific links between two sites, while session management starts and stops the key generation.

Site Management

Each collection of key stores constitute trusted nodes of the network, Site agents manage the connections with other sites and feature several functions (Aguado et al., 2017) that can be integrated with software defined networks for dynamic key generation (Hugues-Salas et al., 2018).

Acknowledgements

This project has been funded by EPSRC under the Quantum communications hub. We acknowledge contributions from Dr Djeylan Aktas, Dr David Lowndes, Prof. John Rarity, Dr Chris Erven at the University of Bristol.

References

Aguado, A., Hugues-Salas, E., Haigh, P. A., Marhuenda, J., Price, A. B., Sibson, P., Kennard, J. E., et al. (2017). Secure nfv orchestration over an sdn-controlled optical network with time-shared quantum key distribution resources. *Journal of Lightwave Technology*, *35*(8), 1357–1362. doi:10.1109/JLT.2016.2646921

Hugues-Salas, E., Ntavou, F., Ou, Y., Kennard, J. E., White, C., Gkounis, D., Nikolovgenis, K., et al. (2018). Experimental demonstration of ddos mitigation over a quantum key distribution (qkd) network using software defined networking (sdn). In *Optical fiber communication conference* (p. M2A.6). Optical Society of America. doi:10.1364/OFC.2018.M2A.6

Lowndes, D. (2016). Low cost, short range, free space quantum key distribution. *Photon 16*. Retrieved from https://research-information.bris.ac.uk/explore/en/publications/

low-cost-short-range-free-space-quantum-key-distribution(e656b18e-db5f-4fb8-92da-22ee3d31c2cb).html

Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., & Zbinden, H. (2000). Fast and user-friendly quantum key distribution. *Journal of Modern Optics*, *47*(2-3), 517–531. doi:10.1080/09500340008244057