Field Trial of Quantum-Secured IPsec Tunnels with Chip-based QKD

Philip Sibson[1], Jake Kennard[1], Tom Crabtree[1], Paul Wright[2], Catherine White[2], Emilio Hugues Salas[2], Andrew Lord[2], Gert Grammel[3], Bill Mead[3], Radko Radev[3], Melchior Aelmans[3], Steven Jacques[3]
[1] KETS Quantum, Bristol, UK, [2] BT Adastral Park, Ipswich, UK, [3] Juniper Networks, Sunnyvale, California
Philip.sibson@kets-quantum.com

Abstract: We report a field trial of chip-based QKD over 28.5km of deployed G.652 fibre, integrated using RFC 8784 with Juniper routers, with concurrent IPsec tunnels consuming independent keys. This illustrates practical quantum-resilient transport layer communication.

1. Introduction

Quantum Key Distribution (QKD) is an important technology for secure symmetric key distribution which provides immunity against computational attacks on the method of key exchange. The evolution from deploying isolated point-to-point QKD links to deploying networks of quantum links drives the need for the integration of external key material from QKD systems, to the network and transport layer. The IETF RFC 8784 standard [1] provides a method for integrating external keys for encryption into an IPsec IKEv2 connection.

The success of QKD also depends on the stability and scalability of the supply chain. QKD photonic integrated circuits ('chip-based') subsystems [2] remove many of the barriers to scaling up the manufacturing process, as well as having promise for creating highly uniform devices with potential for interoperability between general QKD transmitters and QKD receivers.

2. Chip-based QKD over Deployed G.652 Field Fibre

2.1 Chip-based DV-QKD System

The KETS DV-QKD v0.3 is a chip-based QKD System, utilising a biased-basis decoy-state BB84 scheme. The encoding is achieved with weak-coherent states, time-bin based-encoding, in the C-band wavelength range. A synchronisation channel distributes a constant clock signal, via SFP transceiver, between transmitter and receiver to enable alignment, and post-processing communication occurs over a Gbps Ethernet connection (both SFP and RJ45 options are configurable.) The keys are then delivered to authorised key consuming devices such as encryptors over the ETSI GS QKD 014 standard [3], which is implemented over HTTPS. Active stabilisation (including polarisation) maintains the maximum achievable performance (secure key rate) over the link.

The transmitter and receiver are 19-inch rack-mounted systems and are each 2U standard height containing the Photonic Integrated Circuits (PICs), gated InGaAs single photon detectors, bespoke digital and analogue electronics, FPGA-based control, and computer hardware for post-processing.

2.2 Field trial of chip-based QKD

Fig.1 shows the deployed QKD link, in which the quantum channel was transmitted over a 28.5km fibre on loopback between the BT research centre and an exchange. Further work is planned to multiplex both quantum and classical communication channels to reduce the number of optical connections required.

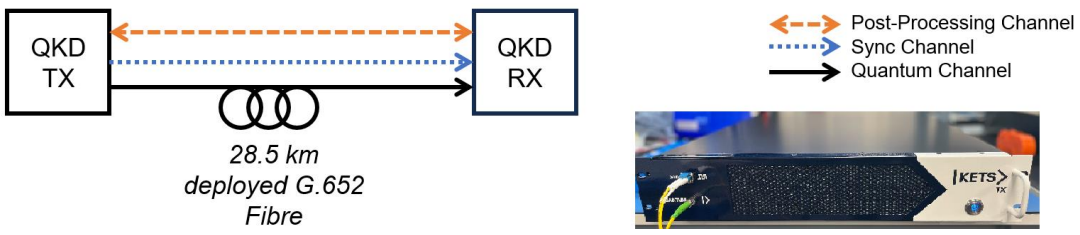

Fig.1 Field trial of Chip-Based QKD System (image of QKD endpoint inset)

3. Integration with IPsec Tunnels

3.1 IKEv2 and RFC 8784

IPsec Virtual Private Networks (VPNs) rely on the Internet Key Exchange (IKE) protocol for establishing and maintaining security parameters that protect the data traffic. These parameters include encryption and authentication algorithms as well as associated keys along with the lifetime of the key material after which new keys must be negotiated. It is known that current security protocols that rely on public-key cryptography (PKC) for establishing keys are considered susceptible to attacks once quantum computers become powerful enough to solve the math by executing Shor's algorithm. IKE, specifically version 2 [4], is an example of one such vulnerable protocol as it relies on Diffie Hellman (DH) or Elliptic Curve Diffie Hellman (ECDH) operation for generating the shared key material.

Without RFC8784, IKEv2 provides a built-in method for an existing preshared secret to be used during authentication, but this key does not contribute to data encryption. To address the challenge posed by Quantum Computers, RFC8784 introduces a method to add an additional secret (symmetric key) that is present at, or delivered to, both the initiator and the responder side via some strict out-of-band method (for example QKD) and that is used in the process of establishing shared key material, including the keys used for data encryption. This additional secret key is called Post-quantum Preshared Key (PPK). In this way, the additional key material provides quantum resistance to the IKE Security Associations (SAs) and any child SAs i.e., initial negotiated IPsec SA and any subsequent rekeyed IKE and IPsec SAs. The same secret is also mixed with a peer authentication key so that both sides can detect any mismatch. This function is supported by the Juniper SRX product line in JunOS 22.4 or later.

3.2 Live Trial of IPsec tunnels with QKD

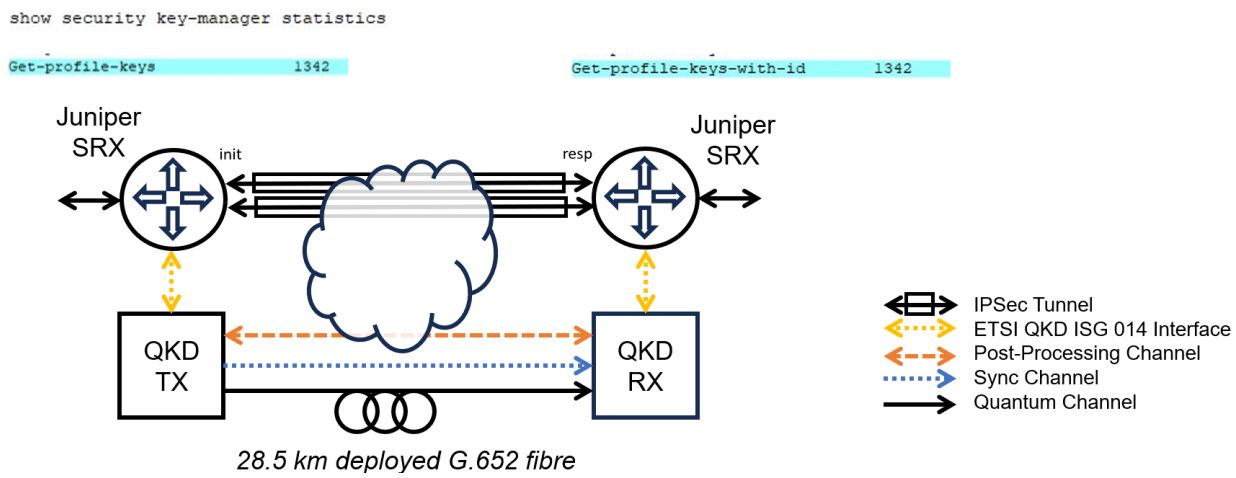

Fig.2 Deployed Chip-Based QKD System in Field Trial

Two Juniper SRX4600 firewalls were used to encrypt data utilising 256 bit keys from the QKD system. The firewalls were connected together using a 100G Ethernet interface connected to 4 x 100G muxponders linked via a 400G OpenZR+ transceiver over 50km of G.652 fibre.

Two separate IPsec VPN tunnels were created between the firewalls that utilised separate IPsec and IKEv2 instances. The firewalls support RFC8784 as described previously, and configured to obtain PPK material from the KETS QKD system via the ETSI GS QKD 014 REST API interface.

The IKEv2 implementation with RFC 8784 can be used to set up a secure tunnel using a one-time use PPK. However, for a long lifetime tunnel - as here, it may be desirable to refresh the PPK regularly in order to mix new entropy into the derived data encryption keys. For RFC 8784, this cannot be triggered just by rekeying the IKE child SA [1], but can be achieved by triggering reauthentication of the IKE SA. Within the tunnel configuration, reauth-frequency can be set to an integer *n* which triggers full reauthentication (and recreation of the seed key material) of the IKE SA on every *n*th rekey. This is used in combination with the *IKE proposal* lifetime-seconds parameter, which sets the rekey frequency.

The Juniper devices are configured to have an IPsec and IKE SA lifetime of 180 seconds and the IKE reauthenticated on each rekey causing the Juniper devices to request new QKD keys. The IPsec tunnels encrypted 25G of bi-directional UDP traffic (generated by an Ethernet tester) sent between the two firewalls and showed no packet loss. We were able to set the PPK refresh period to 180 seconds for the lifetime of the test, which ran for 17 hours.

4. Performance

The performance of the QKD system can be seen below :

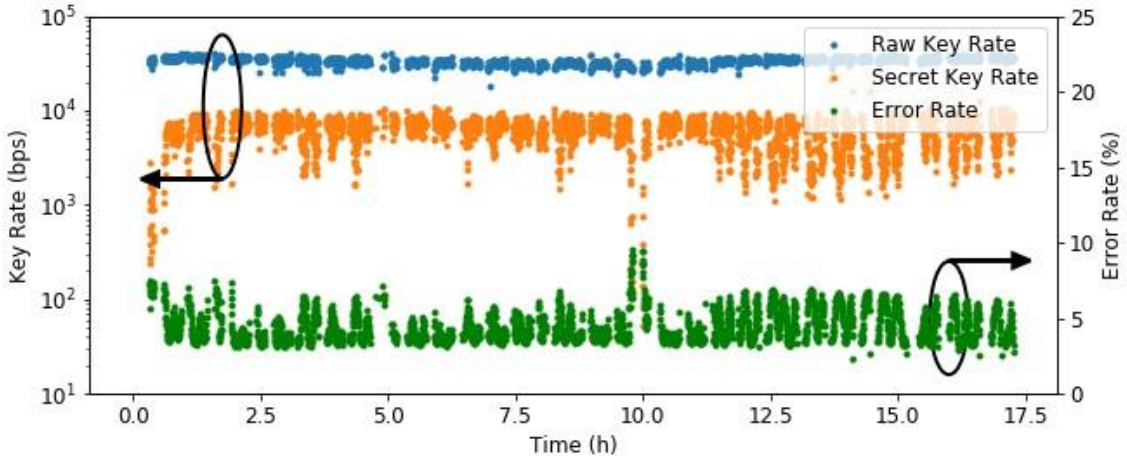

Fig.3 Representative Chip-based QKD link performance over 28.5km of fiber (arrows indicate respective axis)

During a 17-hour data collection period the average signal-intensity error rate was 4.5%, with an average secret key rate of 6.2kbps, and with a key generation up-time of >65%.

The performance of packet transport over the IPsec tunnels was established using an ethernet tester. No packet loss was seen over the 17 hour trial period.

5. Conclusions and Outlook

A chip-based QKD system has been tested over a 28.5km deployed fibre and exhibited stable operation over the 17h trial period. It was used to supply independent one-time keys to multiple IPsec tunnels, which used IKEv2 with RFC8784 for quantum resistance.
Next steps for QKD and VPN will include testing of many-to-many tunnels over a network, with PPK's distributed over QKD key relay layer. We will evaluate of the stability of the tunnels over long time periods, rapid set-up and tear-down of larger numbers of tunnels, use of group PPKs, and graceful fallback in the absence of external key material.

This work illustrates a route to large-scale adoption of quantum-secured communication by addressing key barriers. Future work will continue to reduce and remove these barriers by utilising the integrated photonics platform to decrease the size, weight, and power of QKD systems, and to scale production whilst reducing system cost. Further effort towards assurance and standards is also required to establish and build trust in quantum-secured networks technology, along with continuing applications development to demonstrate increasing integration of quantum-resilient technologies into wider telecommunication networks and cryptographic systems.

Acknowledgements: The authors would like to acknowledge the KETS Quantum Security staff including Francesco Raffaelli, Gaetano Di Martino, Robert Starkwood, Richard Collins, Robert Denman, Charles Shaw, Patrick Buckle, Ben Sayers, and James Garvey who have contributed to the design and development of the DV-QKD v0.3 system.

5. References

[1] Fluhrer, Scott, et al. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-Quantum Security. Request for Comments, RFC 8784, Internet Engineering Task Force, June 2020. IETF, https://datatracker.ietf.org/doc/rfc8784/.
[2] Sibson, P., et al. 'Chip-Based Quantum Key Distribution'. Nature Communications, vol. 8, no. 1, Feb. 2017, p. 13984. www.nature.com, https://doi.org/10.1038/ncomms13984.
[3] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf
[4] Kaufman, Charlie, et al. Internet Key Exchange Protocol Version 2 (IKEv2). Request for Comments, RFC 7296, Internet Engineering Task Force, Oct. 2014. IETF, https://datatracker.ietf.org/doc/rfc7296/.