Quantum-safe 10 Gbps Site-to-Site IPsec VPN Tunnel over 46 km Deployed Fibre

O. Alia,[1,*] A. Huang,[1] H. Luo,[1] O. Amer,[2] M. Pistoia,[2] and C. Lim[1]

[1] *Global Technology Applied Research, JPMorgan Chase, Singapore, 486036*
[2] *Global Technology Applied Research, JPMorgan Chase, New York, NY 10017, USA*

[*] *obada.alia@jpmchase.com*

Abstract: We successfully demonstrated a 10 Gbps QKD-secured IPsec VPN tunnel between two JPMorgan Chase datacenters in a metro network over 46 km of deployed telecom fiber with over 168 hours of continuous operation. © 2024 The Author(s)

1. Introduction

Quantum-safe technologies are required to mitigate the security risks posed by future quantum computers. A promising solution is to deploy *Quantum Key Distribution* (QKD), which exploits the laws of quantum mechanics to securely distribute secret truly random keys between authenticated users embedded in an untrusted optical network without the need for computational assumptions [1–4]. These secret keys can be used for data encryption, which protects sensitive information against unauthorized parties.

In recent years, QKD technology has made enormous progress in terms of its practical usability, in part due to its integration and compatibility with standard security protocols. More concretely, it has been integrated successfully within protocols at various communication layers, including optical encryption [5,6], Media Access Control security (MACsec) [7], and Internet Protocol security (IPsec) [8].

Among these protocols, IPsec is arguably the most important due to its relevance to Virtual Private Networks (VPNs), which are central to the security of enterprise networks and digital platforms, such as cloud services. It is, therefore, of significant interest to integrate QKD technology further into the high-speed IPsec networks and their underlying infrastructures [9].

In this abstract, we present a site-to-site 10 Gbps quantum-safe IPsec VPN tunnel over 46 km of deployed telecom fiber between two JPMorgan Chase datacenters across Singapore. We utilize the ETSI-QKD-014 REST-based Application Programming Interface (API) [10] to exchange the quantum-safe encryption keys between the key management server (KMS) in the ID Quantique Clavis XGR QKD system [11] and the Fortinet Fortigate 3601E Next-Generation Firewalls (NGFWs) [12] in order to encrypt and decrypt the data channel. The User Datagram Protocol (UDP) data stream is generated using a software tool and encrypted by the quantum-safe keys using the AES-256-GCM cipher suite. We successfully refreshed the encryption key every 120 seconds without affecting the VPN tunnel connectivity and performance during the 168 hours of operating time.

2. Experimental Setup

The experimental setup used in the field trial is shown in Fig. 1. The quantum (black) and service (purple) channels of the QKD system are connected via two separate 46 km dark fibers between two JPMorgan Chase data-

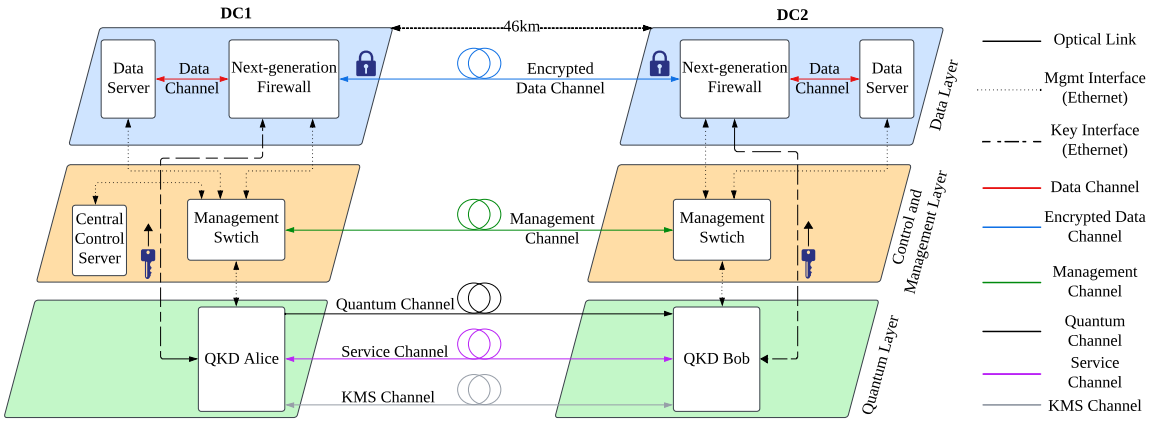

Fig. 1: Experimental Setup.

centers (DC1 & DC2). The KMS channel (gray) is connected via a 46 km 1 Gbps optical telecom circuit using 1G small form-factor pluggable (SFP) optics. A Management switch is utilized in the control and management layer to combine the management traffic of the QKD systems, NGFWs, compute, and data servers in DC1 and DC2 via the Mgmt interface links (dotted lines in Fig. 1). Similarly to the KMS channel, the management channel (green) is connected via a 46 km 1 Gbps optical telecom circuit to enable the management and control communication between DC1 and DC2. Finally, the encrypted data channel (Blue) is connected via a 46 km high-speed 100 Gbps optical telecom circuit using a 100G Quad SFP28 (QSFP28).

The central control server in DC1 is used to access, configure, manage, and control the quantum and classical equipment in DC1 and DC2. Moreover, the data server is emulating a layer 3 traffic generator and is used to run the iPerf software to generate UDP data streams and measure the throughput of the network [13]. This data server transmits unencrypted UDP data streams to the NGFW via the data channel (Red) using 100G QSFP28 optics. The data streams are then encrypted in the NGFW using quantum-safe keys. The QKD-generated keys are transmitted via the Key interface link (dashed line in Fig. 1) from the QKD system to the NGFW using the ETSI QKD 014 REST-based API. These keys are fed into the NGFW pseudorandom function (PRF+) which is a Hash-based Message Authentication Code (HMAC) Key Derivation Function (HKDF). The HKDF expands the QKD-generated keys into multiple quantum-safe keys that are used for integrity protection, authentication and encryption. The HKDF is utilized following the Internet Engineering Task Force (IETF) RFC 7296 [14]. Finally, the NGFW encrypts the data stream from the data channel as IPsec with AES-256-GCM cipher suite using the quantum-safe keys derived from the PRF+.

3. Results and Discussions

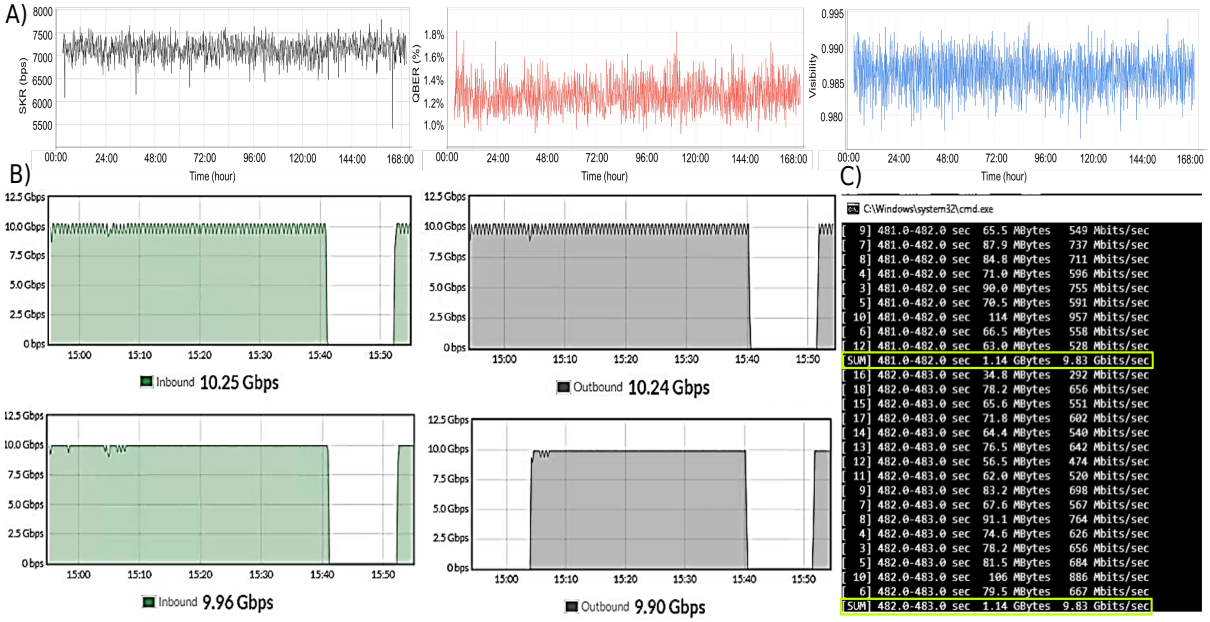

Fig. 2: Results of the field trial: A) SKR, QBER and visibility of the QKD system. B) WAN link throughput (top); VPN tunnel throughput (bottom). C) iPerf test performance.

The results of the field trial tests are shown in Fig. 2. To evaluate the performance and stability of our QKD system, we measured the Secret-Key Rate (SKR), Quantum Bit Error Rate (QBER) and visibility over 168 hours with a link distance of 46 km and an optical loss of ≈ 12 dB. As shown in Fig. 2A, we achieved an average SKR of 7.2 kbps (≈ 28 256-bit AES keys per second), an average QBER of 1.3%, and an average visibility of 98.6%. Fig. 2B shows the throughput of the wide-area network (WAN) link (top) and VPN tunnel (bottom) for the inbound traffic in green (DC2 ⇒ DC1) and the outbound traffic in gray (DC1 ⇒ DC2). As shown in Fig. 2B, the outbound throughput for the WAN link and the VPN tunnel is 10.24 Gbps and 9.90 Gbps respectively. Additionally, the inbound throughput for the WAN link and the VPN tunnel is 10.25 Gbps and 9.96 Gbps respectively. It can be observed that the WAN link throughput is higher than the VPN tunnel throughput, this is because the WAN link throughput includes the VPN tunnel throughput (the payload) and packet headers. As shown in Fig. 2B, the inbound and outbound VPN tunnel throughput in the field setup is limited to ≈ 10 Gbps. We managed to run 13 VPN tunnels between DC1 and DC2, however, due to equipment limitations, we could only utilize one VPN tunnel at a time.

Fig. 2C shows the network load testing performance using the iPerf tool. We used different IP sockets (number on the left) to maximize the traffic between DC1 and DC2. In one second, we measured a sum of 1.14 Gbyte transferred between DC1 and DC2 with a throughput of 9.83 Gbps from all different sockets (green rectangle). To put that into perspective, each Amazon Web Services (AWS) site-to-site VPN connection has two tunnels and each tunnel supports a maximum throughput of up to 1.25 Gbps [15]. Compared to AWS VPN throughput, we achieve almost 4 times the throughput between DC1 and DC2.
As mentioned before, we achieved a SKR of 7.2 kbps resulting in ≈ 28 256-bit AES keys per second. Therefore in 120 seconds, the QKD system generates 3360 256-bit AES keys. The encryption key refresh rate for the VPN tunnel is 120 seconds, where a new QKD-generated key is sent to the NGFW before the old key expires. Only 0.03% of the keys are consumed every 120 seconds since we only use 1 key out of the 3360 keys that are generated. Even if we refresh the key every second, we would have only consumed 3.6% of the available keys. The 120-second fast key refresh rate was implemented by custom messaging within the IPsec Internet Key Exchange child security association (IKEv2 child SA) sequence phase 2 [14]. The key refresh process occurs seamlessly without any loss of connectivity or disruption in the VPN tunnel.

4. Conclusion

We demonstrated a quantum-safe 10 Gbps IPsec VPN tunnel over 46 km between two datacenters with over one week of continuous operation. We managed to transmit ≈ 8.7 Tbyte over a period of two hours (≈ 1.19 Gbytes per second) via the VPN tunnel using QKD derived secret keys to encrypt the data with the AES-256-GCM cipher suite. Such throughput supports site-to-site VPN tunnels for different use cases, such as between on-premises locations (DC to DC, or DC to office), between on-premises locations and public cloud providers (DC to AWS, Microsoft Azure or Google Cloud Platform), and to secure traffic between radio access networks (RANs) and backbone core networks. We utilized ETSI 14 for the encryption keys exchange with a key refresh rate of 120 seconds with a key consumption rate of 0.03%.

References

1. Miralem Mehic et al. Quantum key distribution: A networking perspective. *ACM Comput. Surv.*, 53(5), 2020.
2. Purva Sharma et al. Quantum key distribution secured optical networks: A survey. *IEEE Open Journal of the Communications Society*, 2:2049–2083, 2021.
3. Yuan Cao et al. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2):839–894, 2022.
4. M Stanley et al. Recent progress in quantum key distribution network deployments and standards. *Journal of Physics: Conference Series*, 2416(1):012001, 2022.
5. Erwan Pincemin et al. 400g transmission of qkd-secured 100g data stream over 184km ssmf through three qkd links and two trusted nodes. In *European Conference and Exhibition on Optical Communication*, M.A.4.4, 2023.
6. Marco Pistoia et al. Paving the way toward 800 gbps quantum-secured optical channel deployment in mission-critical environments. *Quantum Science and Technology*, 8(3):035015, 2023.
7. Juniper Networks. Validation of a quantum safe macsec implementation, 2023.
8. Toshiba. Toshiba digital solutions and softbank corp. successfully complete field experiment of ipsec qkd-vpn, 2023.
9. Sami Ullah et al. Ipsec for high speed network links: Performance analysis and enhancements. *Future Gener. Comput. Syst.*, 107(C):112–125, 2020.
10. ETSI and GSQKD. 014. quantum key distribution (qkd); protocol and data format of rest-based key delivery api, 2019.
11. ID Quantique. Xgr series – qkd platform, 2023.
12. Fortinet. Fortigate 3600e series, 2023.
13. Ajay Tirumala. Iperf: The tcp/udp bandwidth measurement tool. *http://dast. nlanr. net/Projects/Iperf/*, 1999.
14. Charlie Kaufman et al. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296, 2014.
15. Amazon Web Services. *AWS Site-to-Site VPN User Guide*, 2023.

Disclaimer