Experimental Demonstration of Programmable 100 Gb/s SDN-Enabled Encryptors/Decryptors for QKD Networks

E. Arabul, R. S. Tessinari, O. Alia, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, D. Simeonidou

High Performance Network Group, University of Bristol, Woodland Road, Bristol, United Kingdom

ekin.arabul@bristol.ac.uk

Abstract:

We successfully demonstrated on-demand and programmable encryption/decryption using SDN-enabled FPGA-based technology over a QKD network. Data rate over 90 Gb/s with maximum data encryption of 11.25 GB/s for different encryption schemes were achieved.

1. Introduction

Optical transport network (OTN) systems have been identified as major technology enablers for providing physical layer security, exploiting the properties of the optical medium for secure key exchange while benefiting from the high bandwidth, low latency and large transmission capacity of the optical fibre [1]. Currently, quantum key distribution (QKD) is a well established technology to offer proven quantum-safe secure exchange of encryption/decryption keys [2] utilising OTN. Powerful hardware-based cryptographic engines have also been developed to demonstrate high speed data-in-motion encryption at line bit rates of 100 Gb/s, with dynamic Diffie-Hellman key exchange for secure key generation and with key rotation every minute, and compatible with quantum-safe security [3, 4]. Also, an extreme rate of 482 Gb/s Advanced Encryption Standard (AES) throughput has been achieved using a Xilinx Ultrascale FPGA [5].

All aforementioned systems rely on a single encryption policy, AES, without reconfiguration capabilities. Such encryption and decryption schemes are well fitted for static configurations assuming point-to-point QKD links using pre-defined encryption algorithms with fixed operational parameters for the generation and use of the keys [6]. However, recent dynamic QKD network field deployments [7] have been demonstrated to offer enhanced rerouting capabilities in the distribution of keys, while when combined with the software defined networking (SDN) control principles present today in all modern OTN networks they allow for ultimate flexibility on the key management [8]. In such a dynamic and programmable landscape, in-motion reconfigurable hardware encryption schemes offering an on-demand choice of encryption algorithms and key consumption rate would be highly advantageous. Such flexibility would allow adaptation of the encryption scheme and key refresh rate that can vary depending on the security preference of the users at a given time, condition of the network, processing overhead of the algorithms and application security requirements. Based on this programmability, in [9] a quasi-reconfigurable hardware encryptor has been implemented with a throughput of 200 Gb/s with an AES encryption performance limited to 48.38 Gb/s with AES being the fixed the encryption core.

In this paper we propose, for the first time, a highly programmable hardware-based encryptor utilising a SDN controller that can change its encryption algorithm on-the-fly and upon request from user/application while supporting 100G encrypted data transport with a capability of key consumption of 6912 b/s, providing a maximum data encryption of 12.8 GB/s. We experimentally demonstrated flexibility and capability of this novel programmable encryptor in a SDN controlled QKD network.

2. Programmable Encryption/Decryption Network Architecture

Fig. 1 shows an overview of the network architecture used for the real-time demonstration of 100 Gb/s, FPGA-based, programmable encryption and decryption. Each node of this network consists of an encryption/decryption subsystem, quantum key distribution (QKD) equipment and an optical cross-connect (OXC). The flexible encryption/decryption units used contain firmware implemented on Xilinx Virtex UltraScale FPGA (XVCU095) located on the Xilinx VCU108 development board. From the client side, users are connected to the FPGA via small form-factor pluggable (SFP) transceivers mounted to the FPGA from the FPGA Mezzanine Card (FMC) which accommodates 10 SFP connections. Each SFP is capable of 10 Gb/s and so a total data rate of 100 Gbit/s can be achieved. A 10G medium access control (MAC) has been implemented using a Xilinx 10G Ethernet core for each SFP connection, so 10 $\times$ 10G Ethernet core has been used for 100G on the client side. From the optical network line side, the 100 Gb/s data transmission of the FPGA system is implemented employing a 100G Ethernet subsystem. Quad Small Form-Factor Pluggable (QSFP) transceivers operating at the 1310 nm wavelength are used for establishing 100G Ethernet connection between nodes.

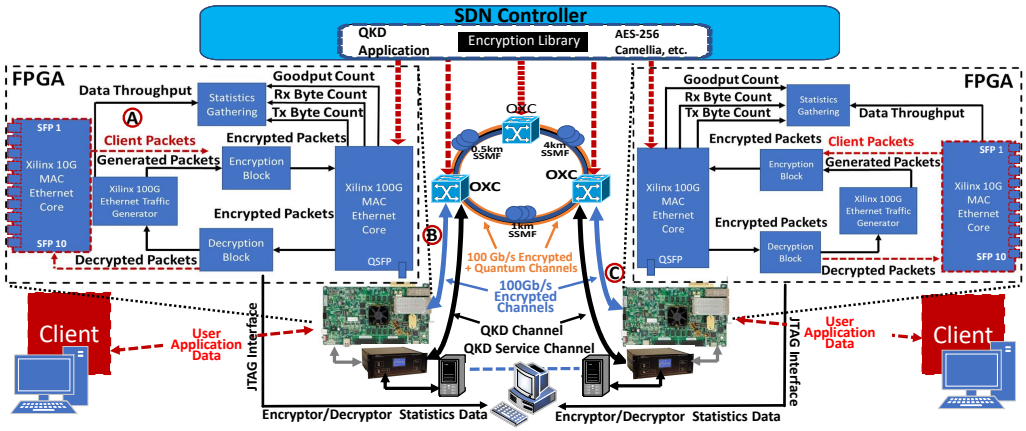


Fig. 1. Testbed of the Encryption/Decryption Network Architecture

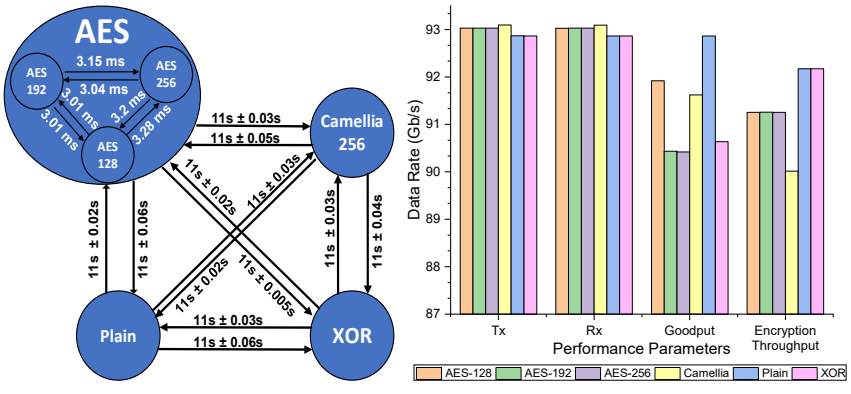
As shown in Fig. 1, each FPGA's encrpytion/decryption block operates bidirectionally with changeable keys. Client frames are received through the 10G Ethernet core and then frames are encrypted by the encryption block before the 100G Ethernet core. Decryption performs in the opposite direction of the encryption. Keys are pushed to the FPGA via a PCI-Express bus and a RAM block was used for storing the key IDs and keys together. The Xilinx traffic generator and the statistics gathering subsystem were used for performance tests of the system.

For the symmetric key generation, IDQuantique Discrete Variable (DV)-QKD systems are used implementing the BB84 protocol (ID3100 Clavis2). A server is used per each QKD unit to undertake the quantum protocol and to retrieve the keys generated by the quantum channels which are used by the encryptor. The key servers use as classical channel a standard Ethernet connection to undertake the post-processing required to transform the photons exchanged via QKD into secure keys. The optical ports of the QKD units and FPGA-based encryptors/decryptors are connected to low-insertion loss (<1dB), SDN-enabled OXCs which function is to route the encrypted data to the suitable path of the optical network. These OXCs enable the interconnection of three nodes in a ring topology, as shown in Fig. 1, via using spools of standard single-mode fiber (SSMF).

For the control plane, a SDN controller is implemented with two extensions: a) a QKD application capable to start and stop the QKD operation to manage the key generation process, and b) an access to a library of encryption algorithms. According to the requirements of the network operator and the resource optimisation algorithm, any of the available encryption algorithms in the library can be downloaded into the FPGAs, adapting its configuration on-demand and real-time. Since the encryption schemes are stored in the SDN instead of the firmware, unlimited number of encryption schemes can be accommodated in the library. For each new implemented algorithm, the controller is updated and the available algorithms are AES (128, 192, 256), Camelia-256, and XOR.

3. Experimental Results

Programmability of the system has been tested by measuring the switching times between different encryption schemes. Fig. 2a shows the measured times for re-configuration between AES, Camellia, XOR or Plain (unencrypted) schemes in our system. As observed, due to the internal switching reconfiguration among the AES encryption schemes (256, 192 or 128), switching times could be as low as 3.01ms since FPGA routing on the fabric is unnecessary as the AES-128 and 192 schemes are a subset of the AES-256. On the other hand, in case of



a) b)

Fig. 2. Encryption/Decryption Performance Parameters: a) Switching times between schemes, b) 100G Ethernet performance

Table 1. Key Consumption Time.

Keys	Total Time (μs)	Agent Time (μs)	FPGA Time (μs)
1	36920	36599	321
5	180519	179231	1288
8	293209	291138	2071
15	543734	539976	3758

Table 2. Optical QKD Network Parameters.

Link	Fibre Length (km)	Hops	Power Budget (dB)	QBER (%)	SKR (b/s)
L1	0.5	1	5.19	1.30564	1762.06
L2	1	1	5.7	1.43335	1414.15
L3	4.7	1	7	1.90579	895.541
L2/L3	1 + 4.7	2	9.14	3.02854	430.564

the external switching , (i.e from the AES to the Camellia), loading of a new FPGA configuration from the SDN controller is required together with the re-routing on the FPGA fabric (≈11 s).

To further evaluate the performance of the system, the 100G Ethernet core was fed by a continuous burst of packets for saturating the Ethernet connection, and data throughput, goodput, transmitted and received data statistics were collected by using the Xilinx Ethernet Core statistics gathering functions as it is shown in Fig. 2b. The transmitted data is measured after the 100G Ethernet encapsulation process and before the transmission over the optical fiber links via the optical switches. The receiver data is measured before the reciprocal 100G Ethernet process in the encryptor/decryptor (points B and C in Fig. 1). Simultaneously, the data throughput and goodput are measured at the monitoring points A and C of Fig. 1. As observed in Fig. 2b, the transmitted and received data rates were at least 1 Gb/s higher than the encryption throughput due to the Ethernet overheads added to the incoming data into the 100G MAC Ethernet core. Moreover, the encryption throughput ranged between 90 Gb/s and 92.2 Gb/s due to different cycles of encryption operation for different schemes. The other parameter obtained by the Xilinx statistics was goodput, which indicates the number of bytes received with correct Frame Check Sequence. This parameter can be affected by various factors such as applied optimisation, design timings and implementation techniques. As observed in Fig. 2b, AES-128 had the lowest number of errors amongst encryption techniques with a goodput rate of 91.91 Gb/s whilst the AES-256 had the lowest goodput rate of 90.42 Gb/s.

To assess the encryption and decryption proposed with respect to the QKD network, in Table 1, key switching timings are measured using Transaction Control Language (TCL) scripts with Xilinx Virtual Input Output (VIOs) IPs. Total time is defined as the time between a key is being pushed to the FPGA and decryption successfully synchronises with the new key ID. Agent Time referrers to the time lost to the software and FPGA Time is internal latency of the FPGA. In Table 1, pushing a single key from the QKD system takes roughly 3.7 ms and most of the time is lost to the FPGA Agent software, whilst for the FPGA it only takes 321 μs. However, FPGA time tends to reduce if the keys are located in adjacent RAM addresses to ≈240 μs. In our implemented network, the highest SKR (L1) is 1762.06 b/s which gives 1.88 GB of encrypted data per 256 bits key, assuming AES-256 and replacing keys as fast as possible. It should be noted that 3.7 ms latency corresponds to 27 keys consumption per second and this key consumption rate and assuming the AES-256 goodput, the minimum granularity our encryptor can do is 474 MB per key.

4. Conclusion

A programmable SDN-enabled encryptor/decryptor was demonstrated with QKD networking for secure key exchange. The FPGA-based encryptor/decryptor achieved the configuration of different encryption schemes with switching times of ≈3 ms between AES encryption methods in the internal operation mode. Considering data throughput and goodput, the encryption schemes achieved data rates higher than 90 Gb/s. Also, our system has shown a capability of key consumption of 6912 b/s, providing a maximum data encryption of 11.25 GB/s.

Acknowledgements

This work was funded by EU funded projects 5G-COMPLETE (871900) and UNIQORN (820474) and part of the research leading to this work has been supported by the Quantum Communication Hub funded by the EPSRC grant ref. EP/T001011/1.

References

1. K. Guan et al.,"Secure Transport-as-a-Service (TaaS) in Core and Metro Networks," *ECOC*, 2016.
2. H.K. Lo et al., "Secure quantum key distribution" *Nature Photonics*, 8, 595-604, 2014.
3. ADVA "FSP 3000 ConnectGuard™ Optical" https://www.adva.com/
4. IDQ "Centauris CN9000 Series" https://www.idquantique.com/
5. B. Buhrow, "A Highly Parallel AES-GCM Core for Authenticated Encrypt. 400Gb/s Network Prot." *ReConFig*, 2015.
6. M. Mehic et al., "Quantum key distribution: a networking perspective," *ACM Comp. Surveys*, 53, pp.1-41, 2020.
7. R. S. Tessinari et al.,, "Field Trial of Dynamic DV-QKD Networking in the SDN-Controlled Fully-Meshed Optical Metro Network of the Bristol City 5GUK Test Network" *ECOC*, 2019.
8. A. Aguado, "Secure NFV Orch. over SDN-Contr. *Opt. Network* Time-Shared QKD Resources." *J. Lightw.Tech*, 2017.
9. Z. Martinasek et al., "200 Gbps Hardware Accelerated Encryption System for FPGA Network Cards," *ASHES*, 2018.