European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

# Experimental Demonstration of High-Speed Self-Reconfiguration and Key Slicing for 100 Gbps Multi-User Programmable Hardware Encryptor

E. Arabul[(1)], R. D. Oliveira[(1)], R. Wang[(1)], O. Alia[(1)], G. T. Kanellos[(1)], R. Nejabati,[(1)] D. Simeonidou[(1)]

[(1)] High Performance Network Group, University of Bristol, Woodland Road, Bristol, United Kingdom
ekin.arabul@bristol.ac.uk

***Abstract*** *High-speed self-reconfiguration and key slicing for 100 Gbps multi-user hardware encryptor have been successfully implemented. The reconfiguration time of 16.7 ms with the encryption throughput of 160 Gbps has been reported. The reconfiguration rate was 676.01 CLB/ms, and the total system latency was 817.6 ns. ©2022 The Author(s)*

## Introduction

As the amount of information transported over Optical Transport Networks (OTNs) escalated, network solutions supporting large bandwidths became a necessity, and many vendors started adapting their products to align with this trend[1]. An increase in the amount of information flowing through the networks also raised concerns regarding the security vulnerabilities, and so, research to encrypt and decrypt high bandwidth networks became important. The multi-user and dynamic nature of the large networks requires solutions to be highly programmable and flexible[2], as well as support high bandwidth capabilities[3]. In addition, encryption solutions can be combined with Quantum Key Distribution (QKD) for unconditional security, and flexibility is needed based on the secret key rates (SKR)[4]. However, current solutions fail to provide flexible security and high transmission capabilities together.

The important commercial hardware encryptors available today could be listed as ADVA's FSP3000[5] and ID Quantique (IDQ)'s CN9000[6], where both devices were QKD-enabled and utilise firmware-locked Advanced Encryption Standard (AES)-256 based 100 Gbps encryption. The highest throughput programmable Field Programmable Gate Array (FPGA) encryptor has been reported in[7], where a 98.8 Gbps encryption rate with 164.14 ms reconfiguration time was achieved. Also, other fast reconfiguring FPGA encryptors were reported in[8],[9] where reconfiguration times were in the range of 49.1 ms - 141 ms and throughput ranges were 2.74 Gbps - 24.9 Gbps.

In this work, we demonstrate a QKD-enabled reconfigurable hardware encryptor/decryptor system of up to 100 Gbps Ethernet bandwidth, which provides flexibility by allowing different encryption schemes and interfaces for key generation sources to co-exist together for multiple clients in the same chipset. To ensure minimum data delay/loss during the dynamic encryption switching process, fast dynamic self-reconfiguration capabilities have been introduced. To our knowledge, our new architecture implementation is the fastest reconfiguring hardware encryptor with the largest transmission capacity in the literature. The theoretical encryption throughput can reach 160 Gbps for 100G Ethernet interface with reconfiguration times of 24.1 ms for decryption and 16.7 ms for encryption blocks. The reconfiguration rate has been recorded up to 676.01 Configurable Logic Block (CLB)/ms, and total system latency could be as low as 817.6 ns for a single Ethernet frame.

## Self-Reconfiguring and Key Slicing Multi-User Hardware Encryptor

Previously, we have demonstrated a programmable hardware encryptor for 100 Gbps Ethernet in[10],[11] of 160 Gbps encryption rate and 91.3 Gbps network throughput with reconfiguration times of 2 s to 2.6 s. However, the reconfiguration times were impractical for rapid change of encryption schemes between multiple clients. Also, the support for interfacing multiple QKD and key exchange systems was not considered. For instance, keys had to be generated by a single key exchange protocol, and different key exchange protocols such as BB84[12] and BBM92[13] could not be used together.

In this work, the proposed system has been designed to provide fast reconfiguration speeds while providing a high-data rate and key slicing for multi-users. Key slicing can be defined as allowing users to encrypt data with different

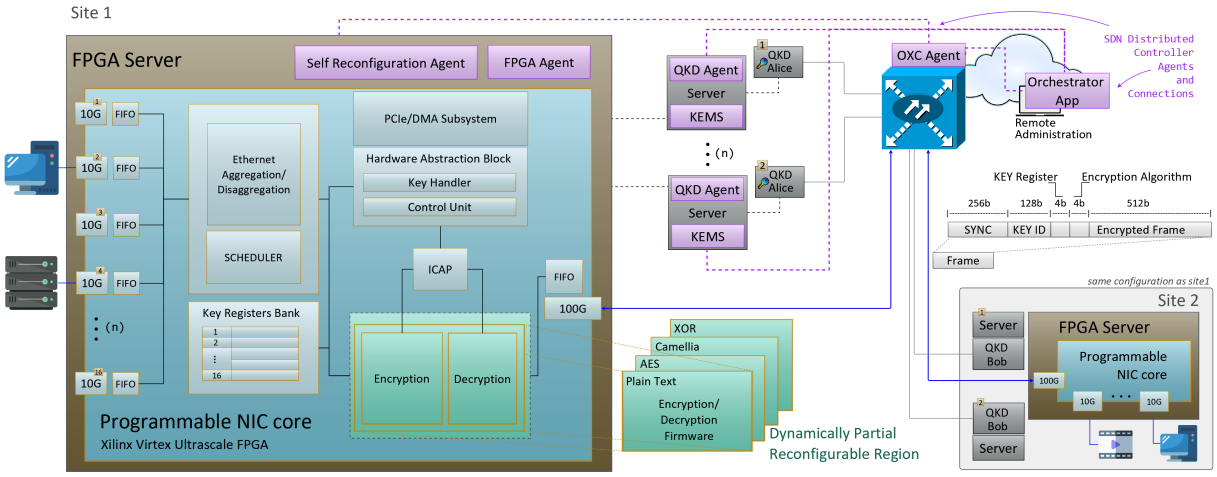


**Fig. 1:** Dynamically Self-Reconfigurable and Key Slicing Encryptor Architecture

keys from different key sources in the same hardware. Thus, independent assignment of Key Management Systems (KMS) to different clients, and co-existence of multiple key exchange devices across multiple clients is possible. Our system can be seen in Fig. 1. We have used the Xilinx VCU108 FPGA board to implement the system. Our design supports up to 16×10 Gbps clients, which are connected via Small Factor Pluggable (SFP) transceivers located on 2 FPGA Mezzanine Cards (FMC). For the 100 Gbps link, a Quad-Small Factor Plugable (QSFP) have been used. Xilinx 10G/100G Ethernet and PCI-Express (PCIe) DMA/Bridge subsystems IPs have been used to implement the interfaces. Network Aggregation module handles frame synchronisation, 10G to 100G interface conversion and Round-Robin based multi-user frame scheduling.

Internal Configuration Access Port (ICAP) has been used to enable the dynamic self-reconfiguration for clients. ICAPs are provided in Xilinx FPGAs to allow users to internally change the configuration of a fabric block inside the FPGA[14]. Thus, partially reconfigured FPGAs can be reprogrammed rapidly by providing configuration files to the ICAP pins. Change in the encryption scheme is noticed by the local self-programming agent, which loads the configuration file via PCIe through a fully pipelined path. Key slicing for each client has been implemented by extending the key handler support up to 16 users. Each client has a dedicated Block Random Access Memory (BRAM) block named Key Register Bank and independently filled via FPGA agent by the KMS.

## Results: Algorithm Reconfiguration Times

In this work, we are reporting the 24.1 ms reconfiguration times for the decryption block, which had 34782 Look Up Table (LUT), 626 BRAM and 8110 CLB. For the encryption block, the reconfiguration time is reported as 16.7 ms, where 60709 LUT, 50 BRAM and 10884 CLB were located. Encryption and Decryption configuration bin file sizes were 6.7 MB and 9.6 MB, respectively, and Xilinx ICAP reconfiguration throughput was limited at 400 MBps. The reconfiguration times have been measured by using the timer functionality of the Xilinx XDMA Drivers. Reconfiguration rates for the encryption block were 676.01 CLB/ms, and for the decryption block, it was 336.5 CLB/ms. Partial reconfiguration blocks (PBlocks) of the design can be seen in Fig 2.

A comparison of reconfiguration times between our previous works can be seen in Fig.3, where 11 s for both encryption and decryption were achieved in[10], in[11] 2 s for the encryption, 2.6 s for decryption were implemented, and this work reports 24.1 ms for the decryption and 16.7 ms for the encryption. Therefore, reconfiguration times were reduced by around 119% for the encryption and 107% for the decryption.

## Results: Encryption Overhead

The latency impact of the 10G/100G interfaces, encryption schemes and network aggregation on time per frame have been measured. Results were obtained by employing a counter to capture the time between the beginning and end of a frame after each module. Each configuration

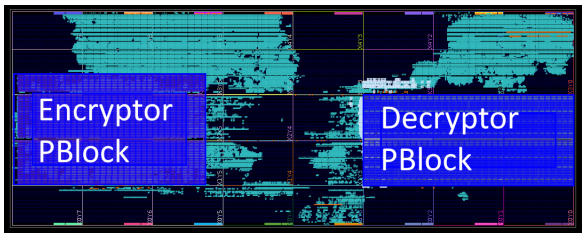


**Fig. 2:** Partial Reconfiguration Blocks inside the FPGA fabric-Virtex UltraScale XCVU095-2FFVA2104E FPGA

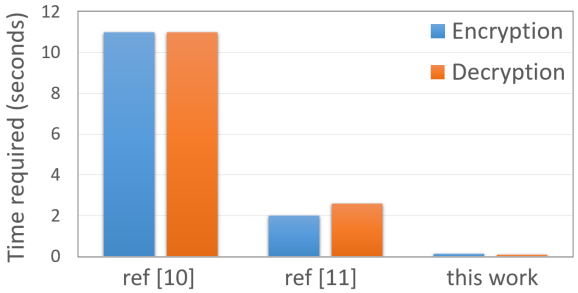


**Fig. 3:** Time Required to Reconfigure the FPGA

has been tested with 1518 B, and 64 B Ethernet frame sizes and results can be seen in Tab. 1.

No encryption (Plain) could be assumed for the time it took for aggregation/dis-aggregation and scheduling, and it was measured as 92.8 ns for the smallest Ethernet frame (64 B) and 678.4 ns for the largest frame (1518 B). The impact of the XOR was only extra 1-2 clock cycles (6.4 ns) due to the additional synchronisation registers. Meanwhile, AES-256 implementation needed 307.2 ns for encrypting the 64 B while the 1518 B frame took 1030.4 ns. Thus, AES-256 was added between 67 (214.4 ns) and 110 (352 ns) clock cycles. The difference between AES variations was observed to be 8 clock cycles (25.6 ns), and each standard round of the AES implementation took 4 clock cycles (12.8 ns). On the other hand, Camellia-256 has been the quickest encryption scheme due to fewer pipeline registers, and the latency between 243.2 ns - 966.4 ns which corresponds to 47 and 90 additional clock cycles, was achieved. Each standard Camellia round took 2 clock cycles (6.4 ns). The additional pipeline registers used to meet timing requirements resulted in additional clock cycles in each encryption round.

Also, back-to-back (B2B) latency has been reported for Xilinx 100G/10G Ethernet IPs and SFP transceivers in Tab. 2. 100G IP latency was measured between 180.8 ns - 241.6 ns, and 10G IP latency was 393.6 ns - 2171.2 ns. 30 cm single-mode fibre has been used for this measurement. Therefore, the lowest encryption latency introduced for a single Ethernet frame could be as low as 817.6 ns when Camellia-256 and 10G/100G interface latencies are considered.

**Tab. 1:** Encryptor Internal Latency per Frame Transmission

| Encryption Scheme | Time per frame (ns) | |
|---|---|---|
| | ***Size: 1518B*** | ***Size: 64B*** |
| Plain | 678.4 | 92.8 |
| XOR | 681.6 | 99.2 |
| Camellia-256 | 966.4 | 243.2 |
| AES-128 | 979.2 | 256.0 |
| AES-192 | 1004.8 | 281.6 |
| AES-256 | 1030.4 | 307.2 |

**Tab. 2:** Interface B2B Latency per Frame Transmission

| B2B Ethernet Interfaces | Time per frame (ns) | |
|---|---|---|
| | ***Size: 1518B*** | ***Size: 64B*** |
| 100 Gbps | 241.6 | 180.8 |
| 10 Gbps | 2171.2 | 393.6 |

## Results: Key Refresh Rates

Our encryptor supports a consumption rate of 27 keys/s corresponding to 6912 b/s for 256-bit key[10]. This limit is imposed by the interfaces to the software controller. With the current system capability to host 16×10 Gbps clients, each client could have keys refreshed in each 0.6 s. It means a secret key rate (SKR) of 1.6 key/s per client and less than 10 Gb of data encrypted with the same key.

Previously[15], by employing the IDQ Clavis2 QKD system as the source of keys, the controller delivered 1 key/s. By duplicating this configuration with another QKD pair also delivering 1 key/s, the SKR per client would be 1 key per 8 s and so forth. Key slicing is limited in practical terms by the amount of key sources available; besides, the lower the number of connected clients, the faster the SKR for the others.

## Conclusion

To sum up, we have successfully implemented high-speed self-reconfiguration and key slicing for our QKD-enabled multi-user 100 Gbps Hardware Encryptor. Our proposed design is unique in a way that it allows the co-existence of interfaces for different key generation devices and encryption schemes across multiple clients.

In addition, we are reporting the fastest reconfiguring hardware encryptor with largest transmission capacity. Reconfiguration times of 24.1 ms and 16.7 ms were reported for the decryption and encryption blocks. The highest reconfiguration rate was reported as 676.01 CLB/ms. Our Camellia-256 implementation, the encryption latency was observed between 243.2 ns - 966.4 ns, and, the total system latency could be as low 817.6 ns for an Ethernet frame.

## Acknowledgements

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

## References

[1] Coriant. "The role of otn switching in 100g & beyond transport networks managing bandwidth for long haul and metro network evolution". (2016), [Online]. Available: https://www.ofcconference.org/getattachment/90c0e6a4-08c1-45fb-a7f2-2957d444dc7d/The-Role-of-OTN-Switching-in-100G-Beyond-Transpo.aspx (visited on 05/09/2022).

[2] S. Perez, J. L. Hernandez-Ramos, S. N. Matheu-Garcia, *et al.*, "A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios", *IEEE Access*, vol. 6, pp. 11 738–11 750, 2018. DOI: 10.1109/ACCESS.2018.2801383.

[3] Thales. "Thales cn9120 network encryptor 100 gbps high speed data in motion encryption". (2020), [Online]. Available: https://cpl.thalesgroup.com/sites/default/files/content/product_briefs/field_document/2020-05/ethernet-encryptor-cn9120-pb.pdf (visited on 05/09/2022).

[4] R. Wang, R. S. Tessinari, E. Hugues-Salas, *et al.*, "End-to-end quantum secured inter-domain 5g service orchestration over dynamically switched flex-grid optical networks enabled by a q-roadm", *Journal of Lightwave Technology*, vol. 38, no. 1, pp. 139–149, 2020. DOI: 10.1109/JLT.2019.2949864.

[5] ADVA. "Fsp 3000 : Open optical transport". (2021), [Online]. Available: https://www.adva.com/en/products/open-optical-transport (visited on 05/09/2022).

[6] IDQ. "Centauris cn9000 series". (Jan. 2021), [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/centauris-cn9000-series/ (visited on 05/09/2022).

[7] S. Burman, P. Rangababu, and K. Datta, "Development of dynamic reconfiguration implementation of aes on fpga platform", in *2017 Devices for Integrated Circuit (DevIC)*, 2017, pp. 247–251. DOI: 10.1109/DEVIC.2017.8073945.

[8] J. M. Granado-Criado, M. A. Vega-Rodriguez, J. M. Sanchez-Perez, and J. A. Gomez-Pulido, "A new methodology to implement the aes algorithm using partial and dynamic reconfiguration", *Integration, The VLSI Journal*, vol. 43, no. 1, pp. 72–80, 2010, ISSN: 0167-9260. DOI: https://doi.org/10.1016/j.vlsi.2009.05.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167926009000261.

[9] Z. Wang, Y. Yao, X. Tong, Q. Luo, and X. Chen, "Dynamically reconfigurable encryption and decryption system design for the internet of things information security", *Sensors*, vol. 19, no. 1, p. 143, 2019. DOI: 10.3390/s19010143.

[10] E. Arabul, R. S. Tessinari, O. Alia, *et al.*, "Experimental demonstration of programmable 100 gb/s sdn-enabled encryptors/decryptors for qkd networks", in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, 2021, pp. 1–3. DOI: 10.1364/OFC.2021.Tu1I.2. [Online]. Available: http://opg.optica.org/abstract.cfm?URI=OFC-2021-Tu1I.2.

[11] E. Arabul, R. S. Tessinari, O. Alia, *et al.*, "100 gb/s dynamically programmable sdn-enabled hardware encryptor for optical networks", *Journal of Optical Communications and Networking*, vol. 14, no. 1, A50–A60, Jan. 2022. DOI: 10.1364/JOCN.439677. [Online]. Available: http://opg.optica.org/jocn/abstract.cfm?URI=jocn-14-1-A50.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014. DOI: 10.1016/j.tcs.2014.05.025. [Online]. Available: https://doi.org/10.1016%2Fj.tcs.2014.05.025.

[13] S. Mishra, A. Biswas, S. Patil, *et al.* "Bbm92 quantum key distribution over a free space dusty channel of 200 meters". (2021), [Online]. Available: https://arxiv.org/abs/2112.11961.

[14] Xilinx. "Ultrascale architecture configuration (v1.16)". (Jan. 2022), [Online]. Available: https://www.xilinx.com/support/%20documentation/v/u/en-US/ug570-ultrascale-configuration (visited on 05/09/2022).

[15] R. S. Tessinari, E. Arabul, O. Alia, *et al.*, "Demonstration of a dynamic qkd network control using a qkd-aware sdn application over a programmable hardware encryptor", in *Optical Fiber Communication Conference (OFC) 2021*, Optica Publishing Group, 2021, M2B.3. DOI: 10.1364/OFC.2021.M2B.3. [Online]. Available: http://opg.optica.org/abstract.cfm?URI=OFC-2021-M2B.3.