QKD-based MACsec Control Plane for the Open-RAN Fronthaul

D. Dik[1,2], R. D. Oliveira[3], E. Arabul[3], M. S. Berger[1], R. Nejabati[3], D. Simeonidou[3]

[1] Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark, danro@dtu.dk
[2] Comcores ApS, Kgs. Lyngby, Denmark
[3] High Performance Network Group, University of Bristol, Woodland Road, Bristol, United Kingdom

Abstract *We demonstrate an FPGA-based architecture integrating QKD with MACsec Key Agreement protocol to quantum-secure the Open-RAN Fronthaul. This includes a protocol for key synchronization in the MACsec control plane. A key rate of 1 key/sec was achieved providing high reliability for critical applications. ©2023 The Author(s)*

Introduction

There is a trend in 5G networks towards a disaggregated and open Radio Access Network (RAN). The Open-RAN (O-RAN) Alliance has defined the O-RAN Fronthaul (O-FH) as the interface between the O-RAN Radio Unit (O-RU) and the O-RAN Distributed Unit (O-DU). In this disaggregated and dynamic environment, security becomes critically important and the O-FH needs to be upgraded like the rest of the 5G system[1].

The O-FH carries data over its Ethernet-based transport network with strict performance requirements[2] and these data are not protected by default. Therefore, the O-FH is exposed to Layer 2 threats that risk the operation of the RAN. The Media Access Control Security (MACsec) protocol, standardized in IEEE 802.1AE[3], is a Layer 2 security protocol that operates on Ethernet frames. Its security features of authentication, confidentiality, integrity, and replay protection, together with its ability to respect high performance requirements make it a suitable candidate to secure the O-FH[4],[5].

MACsec works with a control and a data plane. The control plane implements the MACsec Key Agreement protocol (MKA)[6], which is based on Extensible Authentication Protocol (EAP) messages using public keys signed by a certificate authority (CA). The data plane protects and verifies frames applying Advanced Encryption Standard with Galois Counter Mode (AES-GCM) cryptography[7][8] with parameters set by the control plane. While the data plane protects the O-FH traffic between O-RU and O-DU with AES-GCM, the prior and continuous control plane's EAP message exchange applies public key cryptosystems (PKC) schemes for authentication and key negotiation and can still be exposed to quantum attacks.

Quantum computers can impose a challenge to PKC when they become powerful enough to perform Shor's[9] algorithm for large numbers. At present, the symmetric-key encryption AES-256 is still believed to be quantum-resistant[10]. With the prospect of reaching enough computing power to break the computational hardness of PKC, it is reasonable to consider quantum security at the stage of 5G architecture design[5].

Considering these aspects, MACsec contributions to the O-FH can be twofold. First, it performs encryption with ultra low latency when implemented in hardware[11],[12] and, second, it is suitable to be used in hybrid approaches for key exchange with Quantum Key Distribution (QKD)[13],[14]. Recently, the industry has put an increasing effort in this direction[12],[15],[16]. At the same time, academia and industry are not only working on the integration of QKD[17] systems and deployed networks[18]–[20], but also pursuing ways to standardize and protect control planes[21],[22].

Standards have been developed for QKD deployment including RESTful APIs for key distribution[23]. MACsec control plane, however, does not provide native compatibility with current QKD specifications. At the time being, there is no recommended or *de facto* manner to map QKD identifiers, such as SAE-ID and key-ID directly into MACsec key objects, such as CAK and SAK.

In light of this, the main contribution of this paper is the integration of QKD and the MACsec control plane to quantum-secure the O-FH. We demonstrate how to use QKD integrated with the MACsec control plane in order to refresh both connectivity and security association keys. Building upon recent standards, we propose a framework to push and synchronize QKD keys into an FPGA-based MACsec implementation and we deploy the system on the edges of a 5G network.

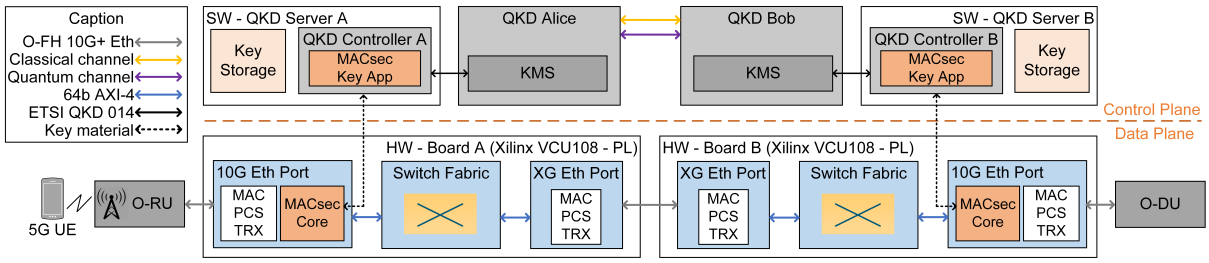


Fig. 1: Top-level system architecture of the QKD-based MACsec control plane for the O-FH

System Architecture and QKD Integration

Fig. 1 illustrates the system architecture. It comprises software (SW) and hardware (HW) co-design. The SW domain implements the integration of MACsec control plane, QKD unit, and FPGA. It includes a QKD Controller, MACsec Key App, and Key Storage. The HW domain performs the O-FH data processing pipeline with three subsystems: i) 10G Ethernet Port including MACsec Core; ii) Switch Fabric; and iii) XG Ethernet Port.

One pair of IDQ Cerberis XGR QKD was used as source of keys. At any time, both QKD units have the same set of keys. They communicate with each other using a quantum channel and a classical service channel. The quantum channel transports single photons for key material and the classical channel deals with synchronization and post-processing for key distillation. Keys are distributed via LAN from the Key Management Store (KMS) - a companion software within the QKD unit - following the ETSI GS QKD 014 API for key consumption. The QKD Controller is the main interface between the QKD and the HW MACsec Core. This controller retrieves keys from the QKD and stores them in the Key Storage. Also, it hosts the MACsec Key App which maintains all the control plane parameters for the MACsec data plane.

The 10G Ethernet Port serves a 10 Gbps O-RU or O-DU client and includes the MACsec HW Core that implements the data plane. It performs confidentiality, integrity, and replay protection to the O-RU/O-DU Ethernet frames. The Switch fabric performs additional Ethernet processing, such as port switching and aggregation. The XG Ethernet Port provides a 10 to 100 Gbps interface according to the O-FH network topology.

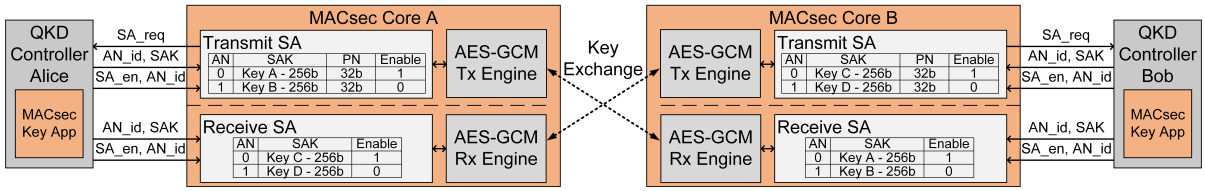
The system architecture was implemented using two Xilinx boards VCU108, which includes a Virtex UltraScale XVCU095 FPGA. One board served an O-RU client and the other one served an O-DU. They were connected to each other using a point-to-point 10 Gbps O-FH channel. However, the architecture supports higher-speed O-FH topologies such as 100 Gbps network of switches using Optical Cross Connect (OXC). The O-DU client and radio controller software were provided by Accelleran, while the O-RU client was from Benetel (RAN 650). For User Equipment (UE), in-house developed Multiple Radio Access Technology (multi-RAT) Customer Premises Equipment (CPE) devices were used.

MACsec Key Synchronization Protocol

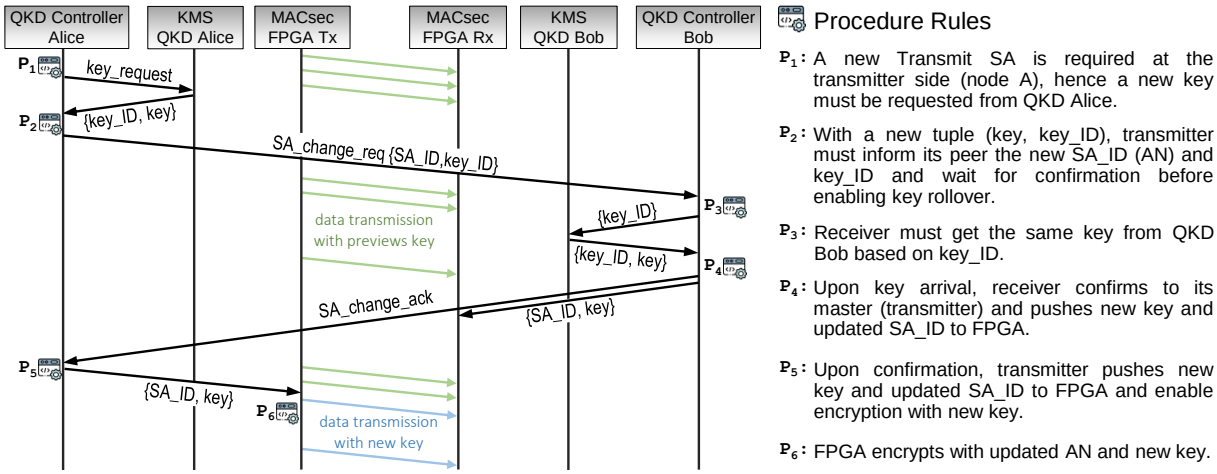
The MACsec control plane maintains security relationships between peers. A long-lived Secure Channel (SC) is created for each MACsec data plane entity. Each SC is identified by a Secure Channel Identifier (SCI) comprising a 48-bit MAC address concatenated with a 16-bit Port Identifier. For key updates during MACsec operation, also referred to as key rollover, the SCs persist through the succession of short-lived Secure Associations (SA). A SA, identified by a two-bit Association Number (AN), consists of a unique Secure Association Key (SAK) and a Packet Number (PN) counter. Throughout the MACsec operation, each frame uses a different PN, and once the PN counter reaches its maximum value, the SC swaps to a new SA. As a result, different SAKs are used in the cryptography process.

In our system, the MACsec Key App installs SAs in the MACsec Core for transmission and reception, each with its corresponding SAKs. The MACsec Core uses one SA at a time to protect and verify each Ethernet frame. Fig. 2a shows with more detail the registers and signals associated with the hardware prototype for the control plane. The combination of the registers AN and Enable indicate which key is to be used for every frame. It is worth remembering that MACsec uses AES-GCM cryptography which is based on symmetric keys, hence, the MACsec entities on both ends must have the same keys.

A new SA is required in three cases. First, when MACsec is initialized and the core doesn't have any SA installed. The second is when the SA reaches its maximum use time based on its PN counter, this can be as fast as every 220 seconds for a 10 Gbps interface with minimum-sized Ethernet frames. The third case is any other



(a) FPGA block diagram of the MKA key exchange mechanism



(b) Sequence diagram and Procedure Rules for the key exchange protocol

Fig. 2: Key exchange protocol and hardware prototype

shorter time required to refresh keys, which can be, for instance, when systems host critical applications such as military and defense.

For all the cases, accurate key synchronization between the two peers is required during SA installation. To achieve this, the key negotiation protocol illustrated in Fig. 2b was proposed. The protocol services and vocabulary are presented together with a sequence diagram. Additionally, the procedure rules guarding the consistency of message exchanges[24] are also explained.

Whenever a new Transmit SA is required at the transmitter, a key request is made to the QKD obeying the ETSI QKD 014 API. With a new key, the transmitter requests its peer to update the corresponding Receive SA with a tuple [AN, key-ID]. This is a confirmed service and only upon confirmation from the receiver the transmitter enables protection with the new SAK. In the end, both sides have the new SA before transmitting.

Key Generation and Consumption

To evaluate the MACsec Core performance with respect to the QKD integration, key switching time is measured between the host and FPGA. The total time is defined as the time between a key request to the QKD and a new key successfully load into the FPGA. Transferring data from Host to Card takes up to 6.2 ms for each 32B transfer. It should be noted that the agents are predominantly written in Python with device drivers written in C to interface the PCIe subsystem. In practical terms, loading a single key from the QKD system takes roughly $\approx$ 1 s. Most of this time is due to remote communications between the Controller and KMS, and also processing at the software level.

The Secret Key Rates (SKR) achieved were on average 2.26 kbps. There was no observed impact caused specifically by the use of MACsec with QKD. The key rollover process happens regardless of the key source. The delay added on each frame by the MACsec protection overhead is not dependent on the key distribution, no matter if is classical PKC or QKD-based.

Conclusions

We successfully demonstrated the integration of QKD with the MACsec control plane to quantum-secure the O-FH. The QKD ability to distribute keys in a proven secure way meets the requirements of the Security Association Keys update. With our implemented architecture, we were able to update approximately 1 key/second and push it to the FPGA with hitless key rollover and no impact to the MACsec data plane performance. With this rate, the system is capable of protecting every 1.25 GB of data with a new key, offering a high security robustness for critical applications.

Acknowledgements

This work is supported by Comcores ApS, by Innovationsfonden Denmark through grant 0153-00126A, and by the EU-funded project 5GCOMPLETE (871900).

References

[1] M. Wong, A. Prasad, and A. C. K. Soong, "The Security Aspect of 5G Fronthaul", *IEEE Wireless Communications*, vol. 29, no. 2, pp. 116–122, 2022. DOI: 10.1109/MWC.002.2100445.

[2] O-RAN Alliance, "Xhaul Transport Requirements", O-RAN Alliance, Technical Specification O-RAN.WG9.XTRP-REQ-v01.00, Feb. 2021, Available: https://orandownloadsweb.azurewebsites.net/specifications.

[3] IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Media Access Control (MAC) Security", *IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006)*, pp. 1–239, 2018. DOI: 10.1109/IEEESTD.2018.8585421.

[4] D. Dik and M. S. Berger, "Transport Security Considerations for the Open-RAN Fronthaul", in *Proceedings of 2021 IEEE 4th 5G World Forum (5GWF)*, 2021, pp. 253–258. DOI: 10.1109/5GWF52925.2021.00051.

[5] J. Y. Cho, A. Sergeev, and J. Zou, "Securing Ethernet-Based Optical Fronthaul for 5G Network", in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES'19)*, ser. ARES '19, Canterbury, CA, United Kingdom: ACM, 2019, ISBN: 9781450371643. DOI: 10.1145/3339252.3341484.

[6] "IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control", *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, pp. 1–205, 2010. DOI: 10.1109/IEEESTD.2010.5409813.

[7] M. Dworkin, E. Barker, J. Nechvatal, *et al.*, "Advanced Encryption Standard (AES)", NIST, Computer Security Standard, Cryptography. FIPS 197, Nov. 2001. DOI: https://doi.org/10.6028/NIST.FIPS.197.

[8] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST, Recomendation. Special Publication 800-38D, Nov. 2007, Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51288.

[9] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (SFCS '94)*, IEEE, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[10] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum Security Analysis of AES", *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 2, pp. 55–93, Jun. 2019. DOI: 10.13154/tosc.v2019.i2.55-93.

[11] D. Dik and M. S. Berger, "Open-RAN Fronthaul Transport Security Architecture and Implementation", *IEEE Access*, 2023, In Press.

[12] ADVA, "FSP 150-XG118Pro (CSH)-G. 10G Secure Network Acccess with Hardware-Encryption and Edge Compute", Data Sheet, Jan. 2023, Available: https://www.advasecurity.com/en/products-and-services/secure-network-access.

[13] ITU-T, "Overview of Hybrid Approaches for Key Exchange with Quantum Key Distribution", ITU, Technical Report XSTR-HYB-QKD, May 2022, Available: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-1-PDF-E.pdf.

[14] J. Y. Cho and A. Sergeev, "Using QKD in MACsec for Secure Ethernet networks", *IET Quantum Communication*, vol. 2, no. 3, pp. 66–73, 2021. DOI: https://doi.org/10.1049/qtc2.12006.

[15] Juniper Networks Inc., "Validation of a Quantum Safe MACsec Implementation. Is ETSI-QKD REST-API Fit for Purpose", White Paper 2000792-001-EN, Jul. 2022, Available: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/2022/validation-of-quantum-safe-macsec-white-paper.pdf.

[16] Comcores ApS, "O-RAN Fronthaul Security using MACsec", White Paper, Sep. 2022, Available: https://www.comcores.com/o-ran-fronthaul-security-using-macsec/.

[17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public Key Distribution and Coin Tossing", *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, Theoretical Aspects of Quantum Cryptography - Celebrating 30 years of BB84, ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025.

[18] A. Aguado, V. Lopez, J. P. Brito, A. Pastor, D. R. Lopez, and V. Martin, "Enabling Quantum Key Distribution Networks via Software-Defined Networking", in *Proceedings of the 2020 International Conference on Optical Network Design and Modeling (ONDM)*, IEEE, 2020, pp. 1–5. DOI: 10.23919/ONDM48393.2020.9133024.

[19] 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.

[20] A. Lord, R. Woodward, S. Murai, *et al.*, "London Quantum-Secured Metro Network", in *Proceedings of the Optical Fiber Communication Conference (OFC) 2023*, Available: https://opg.optica.org/abstract.cfm?URI=OFC-2023-W4K.4, Optica Publishing Group, 2023, W4K.4.

[21] ETSI, "Quantum Key Distribution; Control Interface for Software Defined Networks", ETSI, Group Specification ETSI GS QKD 015 v2.1.1, Apr. 2022, Available: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf.

[22] R. S. Tessinari, R. I. Woodward, and A. J. Shields, "Software-Defined Quantum Network Using a QKD-Secured SDN Controller and Encrypted Messages", in *Proceedings of Optical Fiber Communication Conference (OFC'23)*, Available: https://opg.optica.org/abstract.cfm?URI=OFC-2023-W2A.38, Optica Publishing Group, 2023, W2A.38.

[23] ETSI, "Quantum Key Distribution (QKD); Protocol and Data Format of REST-based Key Delivery API", Group Specification ETSI GS QKD 014 v1.1.1, Feb. 2019, Available: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf.

[24] G. J. Holzmann, *Design and Validation of Computer Protocols*. USA: Prentice-Hall, Inc., 1990, ISBN: 0135399254.