Post-Quantum Cryptography Based Secure Mutual Authentication Mechanism for TDM-PONs

Cristian Bermudez Serna*, Justus Roßmeier*, Lena Wosinska† and Carmen Mas-Machuca‡
*Chair of Communication Networks (LKN), Technical University of Munich (TUM), Germany
†Electrical Engineering Department, Chalmers University of Technology, Gothenburg, Sweden
‡Chair of Communication Networks, University of the Bundeswehr Munich (UniBW), Germany
{cristian.bermudez-serna, justus.rossmeier}@tum.de, wosinska@chalmers.se, cmas@unibw.de

***Abstract*—Passive Optical Networks (PONs) are widely used in fixed-access networks for delivering connectivity to domestic, commercial and industrial users. Authentication and encryption are required in PONs, because of their vulnerability to Optical Network Unit (ONU) impersonating or downstream data sniffing attacks. The research community has pointed out the vulnerabilities of the authentication mechanisms enforced in PON, and has proposed Shared Mutual Authentication (SMA) using Public-Key Cryptography (PKC) based on Diffie-Hellman. However, this last is vulnerable to attacks from quantum computers. This work proposes using Post-Quantum Cryptography (PQC) for SMA in Time-Division Multiplexing (TDM)-PONs. Kyber is selected for the proposed SMA mechanism. This algorithm is the finalist in the PQC standardization process of the National Institute of Standards and Technology (NIST). The feasibility of the proposed Kyber SMA mechanism is shown in a simulation, and it is compared against a baseline SMA from the 10-Gigabit-capable Passive Optical Network (XG-PON) and a state-of-the-art SMA based on Diffie-Hellman. The proposed Kyber SMA mechanism requires more random bytes, has a longer execution time than the baseline and its overhead is similar to the state-of-the-art mechanism with similar security features but based on classical cryptography. According to the presented evaluations, the proposed approach is feasible and offers an SMA resistant to threats from traditional and quantum computers.**

***Index Terms*—Post-Quantum Cryptography (PQC), Secure Mutual Authentication (SMA), Passive Optical Network (PON)**

I. Introduction

Time-Division Multiplexing (TDM)-Passive Optical Networks (PONs)[1] are widely used for delivering broadband connectivity services to residential and commercial users. Due to their versatility, their scope has expanded into use cases such as the industry and modern mobile networks. In industrial applications, PONs can be used in interconnecting large machines consisting of multiple Time-Sensitive Networking (TSN) domains, while providing for the strict time determinism required in such systems [1]. Moreover, in 5G networks PONs can connect base stations in the Radio Access Network (RAN) with the 5G core. Using the Cooperative Transport Interface (CTI), base stations inform the PON about future traffic demands, enabling it to adjust bandwidth assignments proactively and provide low-latency services [2].

This work is partially funded by the Federal Ministry of Education and Research in Germany (BMBF) as part of the projects AI-NET-ANTILLAS (grant ID 16KIS1318) and FRONT-RUNNER (grant ID 16KISR009).

[1]The term PON in this work refers to Time-Division Multiplexing (TDM)-Passive Optical Network (PON).

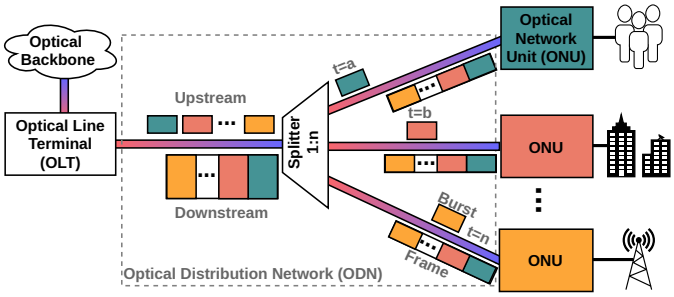


Fig. 1. TDM-PON architecture.

Fig. 1 depicts a high-level architecture of a PON. The Optical Line Terminal (OLT) is connected to multiple Optical Network Units (ONUs) using a passive Optical Distribution Network (ODN), which may consist of several power splitters and has a tree-like topology. The OLT is located at the operator's central office and is connected to the optical backbone network. ONUs can be placed in cabinets, basements, homes, antennas, etc., depending on the Fiber to the x (FTTx) use case. PONs use standard-specific wavelengths for downstream and upstream channels. The OLT broadcasts in the downstream channel frames, a data structure encapsulating information segments to different ONUs. All ONUs receive the same attenuated signal representing the frame, where the attenuation depends on the splitter's splitting ratio and the optical fiber's length. In the upstream channel, the ONU sends unicast information segments called bursts. These are transmitted according to the operator's bandwidth assignment policy and the equalization delay, which is computed by the OLT using an estimation of the ONU's distance. The synchronization of bursts in PONs prevents collisions in the upstream channel.

There are two main security issues with PONs. First, the passive ODN can be tampered to add a malicious OLT or ONU. This can result in a malicious ONU forging bursts to impersonate a legitimate ONU. Hence, Shared Mutual Authentication (SMA) mechanisms are needed in PONs to mutually authenticate the OLT and ONUs. Second, frame broadcasting in the downstream channel can result in a malicious ONU accessing the downstream information of any other ONU. Therefore, data encryption mechanisms are required in PONs to prevent a malicious ONU from accessing unintended

information. Moreover, robust data encryption mechanisms are needed, as preventing a malicious ONU from recording frames for posterior decryption is impossible.

A. State of the Art

In current PONs specifications, authentication and encryption are related. After authentication of the OLT and ONU, these devices agree on a shared secret, which is used to derive the keys needed for encryption. PONs commonly enforce only the *Registration ID-based Authentication*, a mechanism in which the OLT compares a static pre-shared secret, against a secret sent by the ONU. The research community [3]–[6] has pointed out the issues of this mechanism, as it does not authenticate the OLT to the ONU. Moreover, the pre-shared secret is sent before a secure channel is established, compromising the secret, if a malicious OLT sniffs upstream bursts. The International Telecommunication Union (ITU) 10-Gigabit-capable Passive Optical Network (XG-PON) [7] has considered these problems and has added optional mechanisms for SMA, which will be discussed in Section II-B3.

Aiming at improving the security of PONs, Malina et al. [3] and Li et al. [4] proposed the use of Public-Key Cryptography (PKC) for SMA based on Diffie-Hellman. Malina et al. focused on ITU Gigabit Passive Optical Network (GPON). Li et al. focused on the Institute of Electrical and Electronics Engineers (IEEE) Gigabit Ethernet Passive Optical Network (GEPON). Diffie-Hellman allows two parties to negotiate a shared secret over an insecure channel and bases its security on the complexity of the discrete logarithm problem. Unfortunately, as stated by Shor [8], quantum computers can solve this problem in polynomial time. However, Post-Quantum Cryptography (PQC) offers security mechanisms resistant to threats imposed by traditional and quantum computers.

The works of Horvath et al. [5], [6] proposed using physical properties in the PON as a source for shared secret generation. In [5], the authors used the estimated equalization delay between the OLT and ONU as a shared secret for GPON. In [6], the authors used Physical Unclonable Functions (PUFs) in ITU Next Generation Passive Optical Networks stage 2 (NG-PON2), to exploit ONU's unique physical properties for shared secret generation. However, none of the works by Horvath et al. address any SMA mechanism.

Existing works propose novel mechanisms for improving security in various PON technologies. However, they neither provide any implementation in an actual or simulated PON, nor study the overhead imposed by the proposed mechanisms.

B. Contribution

The contributions of this work are: *i)* The use of PQC for SMA in PONs. *ii)* The implementation of the proposed PQC-based SMA mechanism in a simulation. *iii)* To the best of our knowledge, the first performance evaluation of the proposed PQC-based SMA mechanism against a baseline SMA from the XG-PON [7] and a state-of-the-art SMA based on Diffie-Hellman, as proposed by Malina et al. [3] and Li et al. [4].

C. Structure

This work is structured as follows: Section II covers the basics of XG-PON. Section III explains the problem with SMA in PONs. Section IV covers the design and implementation of the proposed PQC-based SMA mechanism. Section V describes the performance evaluation. Section VI highlights the main findings and discusses further research directions.

II. XG-PON

This work selects as baseline one of the SMA mechanisms defined for XG-PON, as this technology is expected to become soon the most common PON deployed in Europe. XG-PON is specified in the ITU Telecommunication Standardization Sector (ITU-T) G.987 recommendation series [7], where ITU-T G.987.3 covers the Transmission Convergence (TC) layer as well as security and authentication [9]. There are three management channels between the OLT and ONU defined in XG-PON. The ONU Management and Control Interface (OMCI) supports higher service layers. The Operation, Administration and Management (OAM) channel transports general control information. Finally, the Physical Layer OAM (PLOAM) carries time-urgent control messages.

A. ONU Activation Process

The ONU activation process is depicted in Fig. 2. This process starts when the ONU is powered on entering the state *(01)*. In this state, the ONU listens to downstream frames coming from the OLT and transitions to the state *(O2-3)*. In this state, the ONU waits for serial number grants from the OLT. During serial number grants, the OLT temporally preempts upstream bursts from other ONUs already in the PON. Once the ONU receives a grant, it turns on its transmitter, backs off for a random delay to avoid collisions with other ONUs potentially joining the PON and sends an upstream burst containing its serial number. The OLT answers the ONU with a downstream frame carrying the ONU's serial number and an assigned unique ONU ID. After this, the ONU transitions to the state *(O4)*. In this state, the OLT sends the joining ONU directed ranging grants and temporally preempts upstream bursts from other ONUs already in the PON. The ONU answers the OLT each time it receives a directed ranging grant. The OLT estimates equalization delay during this message exchange and reports it to the ONU. After this, the ONU transitions to state *(O5)*. Our work focuses on this state, as here the execution of any SMA mechanism takes place, before the ONU transmits upstream bursts with user data as scheduled by the OLT.

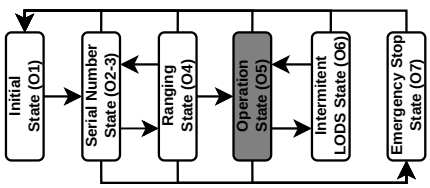


Fig. 2. Simplified ONU activation state diagram. The execution of any SMA mechanism takes place once the ONU reaches the highlighted *Operation State (O5)*. Refer to XG-PON specification [9] for a detailed explanation.

Ideally, an ONU joining the PON transits the states of the activation process sequentially and remains in the state *(O5)*. However, it is possible to transit to the state *(06)*, if the ONU loses synchronization with downstream frames. Moreover, the OLT may instruct one or multiple ONUs to transition into state *(O7)*, if an operational anomaly in the PON is detected.

B. Authentication and Master Session Key

XG-PON [9] defines three mechanisms for authentication of the OLT and ONU. After authentication, the resulting shared secret is used for Master Session Key (MSK) derivation. The MSK is the root used to compute all keys needed in the PON.

1) Registration ID-based Authentication: It relies on the *Registration ID*, a pre-shared secret that is statically set up into the OLT and ONU. Authentication is based on comparing the OLT's *Registration ID* against the one sent by the ONU. For this, the *Registration ID* is sent in an upstream burst before a secure channel is established. Upon successful authentication, the MSK is derived by hashing the *Registration ID* with other default parameters. This authentication mechanism is the only one with mandatory implementation in XG-PON. It is not further discussed, due to its lack of support for SMA and the exposure of the pre-shared secret to upstream sniffing attacks.

2) IEEE 802.1X-based authentication: In this approach, the OLT offloads all authentication procedures to a server offering the authentication mechanisms within IEEE 802.1X. Upon successful authentication, the server creates the MSK and derives the keys needed in the PON. Then, the keys are sent to the OLT and connectivity to the ONU can be provided. The support for this authentication mechanism is optional in XG-PON. It will not be further discussed, due to its dependency on an external server.

3) OMCI-based Shared Mutual Authentication: It performs a hash-based SMA of the OLT and ONU over the OMCI channel using a pre-shared secret. The support for this SMA mechanism is optional in XG-PON. It is selected as the baseline, since SMA is supported and its implementation does not rely on an external server. This mechanism is hereafter named Hash-based Message Authentication Code (HMAC) SMA mechanism[2].

The baseline HMAC SMA procedure starts once the ONU reaches the *Operation State (O5)* of the activation process depicted in Fig. 2. From there on, the OLT and ONU execute the steps in Fig. 3 to perform the baseline HMAC SMA and the MSK derivation depicted in Fig. 4. In step ①, the OLT starts the SMA procedure by setting into the ONU its cryptography capabilities, a random challenge (*OLTChall*) and the challenge status. The ONU selects a subset of cryptography functions (*ONUSelCryptoCap*) out of the ones offered by the OLT, selects a random challenge (*ONUChall*) and computes its authentication result (*ONUAuthRes*) using Eq. 1. Where $|$ is concatenation, Pre-Shared Key (PSK) is a pre-shared secret between the OLT and ONU, the hex $0x00$ repeated eight times is the default serial number of the OLT and *SelHashFun* is a hash function offered by the OLT and selected by the ONU.

[2]Baseline HMAC SMA refers to a SMA mechanism based on HMAC.

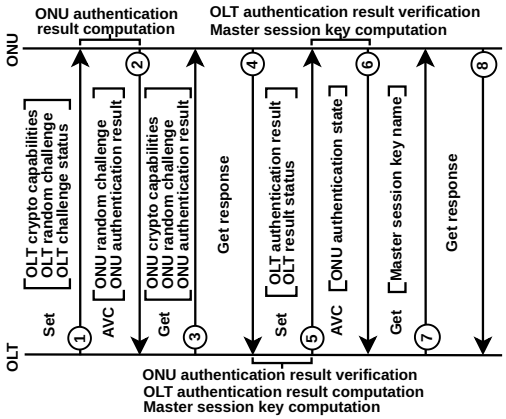


Fig. 3. Baseline HMAC SMA procedure. Some operations may require the exchange of multiple messages. Refer to the ITU-T G.988 [10] specification for a detailed explanation.

$$ONUAuthRes = SelHashFun(PSK, (ONUSelCryptoCap|OLTChall|ONUChall|(0x00)_8)) \quad (1)$$

In step ②, the ONU emits an Attribute Value Change (AVC) signaling the OLT that the random challenge and the authentication result can be retrieved. In step ③, the OLT requests the ONU to provide the selected subset of cryptography capabilities, the random challenge and the authentication result. In step ④, the ONU sends the requested information. Once the OLT receives the response, it verifies the ONU authentication result with the result of its computation for this value. If there is an inconsistency, the authentication procedure is aborted. Otherwise, the ONU to OLT authentication succeeds and the OLT computes its authentication result (*OLTAuthRes*) using Eq. 2, where *ONUSN* is the serial number of the ONU. Finally, the OLT computes the MSK using Eq. 3.

$$OLTAuthRes = SelHashFun(PSK, (ONUSelCryptoCap|ONUChall|OLTChall|ONUSN)) \quad (2)$$

$$MSK = SelHashFun(PSK, (OLTChall|ONUChall)) \quad (3)$$

In step ⑤, the OLT sets its authentication result and the status into the ONU. Then, the ONU verifies the OLT authentication result by comparing the provided value with the result of its computation. If there is an inconsistency, the authentication procedure is aborted. Otherwise, the OLT to ONU authentication succeeds and the ONU computes the MSK using Eq. 3. In step ⑥, the ONU issues an AVC signaling that the authentication state can be retrieved. In step ⑦, the OLT requests the MSK name (*MSKName*) from the ONU. The MSK name is a hash of the MSK computed using Eq. 4. In step ⑧, the ONU sends the requested information.

$$MSKName = SelHashFun(PSK, (ONUChall |OLTChall|0x31415926535897933141592653589793)) \quad (4)$$

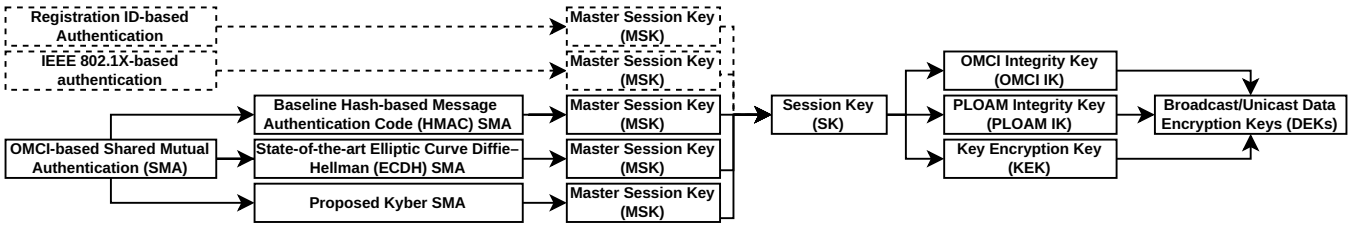


Fig. 4. Authentication and key generation flow. Dashed lines represent the authentication mechanisms not implemented. Solid lines represent the implemented baseline, state-of-the-art and proposed SMA mechanisms compatible with the message exchange for SMA over the OMCI channel as specified for the XG-PON [10]. The MSK is specific to the SMA mechanism and is used to derive all other keys needed in the PON.

C. Key Generation

Fig. 4 describes the authentication and the key generation flow. After a successful SMA, an MSK is generated particular to the SMA mechanism. The MSK is the root for deriving the six keys needed in the PON. Key generation is independent of the SMA mechanism. The functions and parameters for key generation are defined in the XG-PON TC specification [9].

The first key generated is the Session Key (SK). This key links the MSK to the session between the OLT and ONU. The SK becomes the root key for subsequent key generation. The second generated key is the OMCI Integrity Key (OMCIIK). This key is used to verify the integrity of messages transmitted over the OMCI channel. The third generated key is the PLOAM Integrity Key (PLOAMIK). This key is used to verify the integrity of messages transmitted over the PLOAM channel. The fourth generated key is the Key Encryption Key (KEK). This key is used to encrypt and decrypt keys carried over the OMCI and PLOAM channels. Finally, the fifth and sixth generated keys are the broadcast and unicast Data Encryption Keys (DEKs). The OLT generates the broadcast DEK using a Random Number Generator (RNG). It is securely transferred to the ONUs using the OMCI channel and the KEK. The ONU generates the unicast DEK using an RNG upon request by the OLT. This key is securely transferred to the OLT using the PLOAM channel and the KEK. The broadcast and unicast DEKs can be updated anytime.

III. Problem Definition

Among the three authentication mechanisms defined in XG-PON, the specification enforces only the *Registration ID-based Authentication* [9]. In this mechanism, SMA is not possible, as only the authentication of the ONU to the OLT is supported. Moreover, the pre-shared secret is transmitted before a secure channel is established, which exposes the secret to sniffing attacks in a compromised ODN infrastructure. As a technician sets up the pre-shared secret, updating the secret in the OLT at the central office and the ONU at the customer premises can take minutes or even hours.

The works by Malina et al. [3] and Li et al. [4] proposed the use of SMA based on PKC in PONs. The authors use Diffie-Hellman to securely negotiate a shared secret between the OLT and ONU, which is later used in MSK derivation. PKC solves the previously mentioned disadvantages of *Registration ID-based Authentication*, as it allows the dynamical agreement of a shared secret over an insecure infrastructure. However, the authors do not provide insights about the overhead imposed by their proposals, which is relevant for ONUs, as these devices are typically realized using constrained-capacity hardware. Moreover, the invention of the quantum computer poses a threat to algorithms for PKC. For instance, Diffie-Hellman bases its security on the complexity of the discrete logarithm problem, which can be solved in polynomial time with a quantum computer using Shor's algorithm [8].

Hence, modern PONs require: *i)* SMA of the OLT and ONU. *ii)* dynamic and secure agreement on shared secrets between the OLT and ONU. *iii)* resistance to threats posed by traditional and quantum computers. And *iv)* algorithms compatible with constrained-capacity devices.

IV. Proposal

This work extends the OMCI-based SMA mechanism of XG-PON using PQC to address the discussed problems. The Key Encapsulation Mechanism (KEM) Kyber of the Cryptographic Suite for Algebraic Lattices (CRYSTALS) [11] was chosen. Kyber is the winning KEM of the National Institute of Standards and Technology (NIST) PQC standardization. The proposed Kyber SMA mechanism[3] performance is compared to implementations for the baseline HMAC SMA mechanism and the state-of-the-art Elliptic Curve Diffie–Hellman (ECDH) SMA mechanism[4] based on curve 25519 cryptography.

A. Design

1) Kyber: The proposed Kyber SMA mechanism is implemented into the OMCI-based SMA message exchange of Fig. 3. The defined four-way message exchange of random challenges and authentication results with arbitrary size is reused to fit the two-way key exchange required by Kyber. New entries for Kyber are defined in the cryptography capabilities supported by the OLT and ONU. As recommended by the authors of Kyber, the Kyber512 set of parameters is used to match the security of the Advanced Encryption Standard (AES)-128 used in XG-PON. Kyber's has an asymmetric nature with client and server roles, where the client performs more calculations than the server. In the proposed approach, the OLT acts as the client and ONUs as the server, as in PONs the OLT typically has more resources than ONUs.

[3]Proposed Kyber SMA refers to a SMA mechanism based on Kyber.

[4]State-of-the-art ECDH SMA refers to a SMA mechanism based on ECDH.

The OMCI-based SMA message exchange of Fig. 3 was altered to support the proposed Kyber SMA mechanism in the following way. In step ①, the OLT generates the random challenge using Kyber and sets it into the ONU. In step ②, the ONU uses Kyber to: validate the OLT random challenge, calculate the shared secret and generate its random challenge. After step ④, the OLT uses Kyber to: validate the ONU random challenge and calculate the shared secret. After this, the OLT and ONU have the same information to derive the MSK using Kyber. In step ⑦, the MSK name is obtained by calculating the SHA-256 hash of the shared secret so MSK equality at both devices can be checked.

2) Elliptic Curve Diffie–Hellman: The implemented state-of-the-art ECDH SMA mechanism uses x25519 with ephemeral keys for key exchange, signs messages with static ed25519 keys and has a symmetrical execution at the OLT and ONU. The OMCI-based SMA message exchange of Fig. 3 was altered to support ECDH in the following way. Before step ①, each device computes an ephemeral x25519 ECDH secret whose public version is concatenated with a signature generated using a static ed25519 private key. The public secrets are used as the respective OLT and ONU random challenges. In step ①, the OLT sets its random challenge into the ONU. Then, the ONU verifies the signature using the OLT ed25519 public key and computes the shared secret using x25519. In step ④, once the OLT has received the ONU random challenge, it verifies the signature using the ONU ed25519 public key and computes the shared secret using x25519. After this, the OLT and ONU have the same information to derive the MSK using x25519. In step ⑦, the MSK name is obtained by calculating the SHA-256 hash of the shared secret so MSK equality at both devices can be checked.

B. Implementation

A proof of concept of the baseline HMAC, state-of-the-art ECDH and proposed Kyber SMA mechanisms was implemented in a simulation[5] written in Rust. The OLT and ONU roles of the OMCI-based SMA message exchange in Fig. 3 were modeled as programming interfaces, that can be populated with the different implementations in a modular way. Rust was chosen for its trade-off between simplicity and high performance, ensuring a repeatable and realistic simulation. For the implementation of Kyber, the Rust Kyber library [12] in version 0.6 was used. All curve 25519 operations are implemented using the Dalek cryptography [13] library in version 2.0. The code was compiled using Rust version 1.70.0 with the default release profile and no extra flags. Hardware optimizations provided by the Rust standard library or Rust Kyber were not used, as they are often not available on embedded devices used to implement OLTs and ONUs.

V. Evaluation

A. Measurement Methodology

Aiming at measuring and comparing the presented approaches, the metrics: *Random bytes* and the *Time in CPU* were tracked in the simulation environment at the OLT and ONU for the baseline HMAC, the state-of-the-art ECDH and the proposed Kyber SMA mechanisms. *Random bytes* measures the number of random bytes required during the SMA procedure. The *Time in CPU* tracks the time needed by the CPU to conclude the SMA procedure as reported by the Linux kernel. The values reported for these metrics are averaged over 1000 executions of each SMA mechanism. Moreover, the SMA mechanisms have been executed on two different computer architectures: an x86_64 Intel Core i5-8265U, hereafter named x86, and an aarch64 A-53 Rockchip RK3328, hereafter named ARM.

[5]https://github.com/crisbermud/pqc_sma_for_pon

B. Random Bytes

The number of required *Random bytes* by the different SMA mechanisms is described in Tbl. I. This metric does not depend on the computer architecture nor changes across the executions for each particular SMA mechanism. The proposed Kyber SMA mechanism generally requires more random bytes than the baseline HMAC or the state-of-the-art ECDH. With Kyber the OLT and ONU require six and four times more random bytes than HMAC, and three and two times more than ECDH. The random bytes are required only once per SMA execution and they could be pre-collected in the background. Moreover, the OLT could be equipped with a True Random Number Generator (TRNG) hardware, as it needs to execute the SMA procedure for all ONUs in the PON.

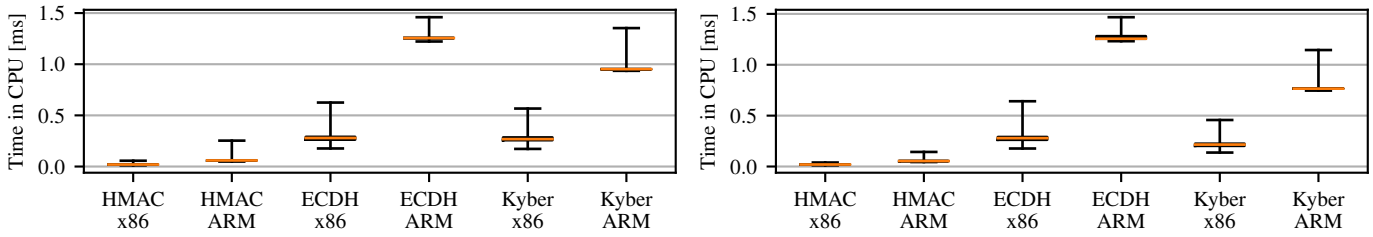
TABLE I
Number of random bytes needed in the OLT and ONU for the different Shared Mutual Authentication (SMA) mechanisms.

		HMAC	ECDH	Kyber
Random bytes	**OLT**	16	32	96
	ONU	16	32	64

C. Time in CPU

Fig. 5 describes the *Time in CPU* needed for executing the SMA mechanisms at the OLT and ONU on the considered computer architectures. As shown in Fig. 5a for the OLT, the execution time of the proposed Kyber SMA mechanism lasts longer than the baseline HMAC and is shorter than the state-of-the-art ECDH. Moreover, for each SMA mechanism the execution in ARM lasts longer than on the x86. For this last architecture, the execution time of Kyber takes approximately fourteen times more than HMAC and subtly less than ECDH. For ARM, the execution time of Kyber takes approximately sixteen times more than HMAC and a quarter less than ECDH. Additionally, the execution time of Kyber in ARM is approximately four times more than on x86.

As depicted in Fig. 5b for the ONU, the execution time of the SMA mechanisms follow the same trend as for the OLT. For x86, the execution time of the proposed Kyber SMA mechanism takes approximately eleven times more than the baseline HMAC and subtly less than the state-of-the-art ECDH. For ARM, the execution time of Kyber takes



(a) Required *Time in CPU* at the OLT.

(b) Required *Time in CPU* at the ONU.

Fig. 5. Fig. 5a and Fig . 5b describe the *Time in CPU* at the OLT and ONU for executing the baseline HMAC, the state-of-the-art ECDH and the proposed Kyber Shared Mutual Authentication (SMA) mechanisms on the x86 and the ARM computer architectures.

approximately fourteen times more than HMAC and a third less than ECDH. The execution time of Kyber in ARM is approximately four times more than on x86.

When comparing Figs. 5a and 5b, the asymmetric nature of Kyber is seen. The execution time for the proposed Kyber SMA mechanism takes approximately a fifth less time at the ONU than at the OLT for both computer architectures, as in the presented implementation the OLT is the Kyber client. In Kyber, the client performs more operations than the server. Hence, offloading the client role to the device with more resources is desirable, which in PONs is the OLT, as ONUs are commonly implemented using constrained-capacity devices.

VI. Conclusion

Passive Optical Networks (PONs) are the dominating technology in modern fixed-access networks. However, PONs are vulnerable to Optical Network Unit (ONU) impersonating attacks and traffic sniffing in the downstream channel. Authentication and encryption are required in PONs to prevent these issues. Nevertheless, the specification of PONs, such as the 10-Gigabit-capable Passive Optical Network (XG-PON), enforces only a vulnerable authentication mechanism based on pre-shared secrets. The research community [3]–[6] has proposed Shared Mutual Authentication (SMA) mechanisms using Public-Key Cryptography (PKC) based on Diffie-Hellman. However, quantum computers threaten PKC, as they can solve the mathematical problems upon which its security is based.

This work proposes a Post-Quantum Cryptography (PQC)-based SMA mechanism for PONs, which uses PKC for authentication and is resistant to threats imposed by traditional and quantum computers. The SMA mechanism is implemented using Kyber, the finalist algorithm of the National Institute of Standards and Technology (NIST) PQC standardization process. The proposed Kyber SMA mechanism is used in a simulation that mutually authenticates the Optical Line Terminal (OLT) and ONU, and negotiates the keys, while following the procedures defined for XG-PON. A baseline Hash-based Message Authentication Code (HMAC) SMA mechanism following XG-PON specification and a state-of-the-art Elliptic Curve Diffie–Hellman (ECDH) SMA mechanism are used in a comparison on the x86 and ARM computer architectures.

Our simulation results show that the proposed Kyber SMA mechanism requires more random bytes than the baseline HMAC or the state-of-the-art ECDH. Moreover, the execution time of Kyber lasts approximately fourteen times longer than HMAC and subtly less than ECDH. As the SMA procedure is executed only once during the ONU activation process, the PON system can assume the extra overhead and in return offer improved security. The asymmetric nature of Kyber also allows offloading the most intensive tasks onto the OLT. Hence, preserving resources in the constrained-capacity ONUs. Implementing and testing the proposed Kyber in a real PON remains for future work.

References

[1] K. Christodoulopoulos, S. Bidkar, T. Pfeiffer, and R. Bonk, "Deterministically scheduled PON for industrial applications," in *2023 Optical Fiber Communications Conference and Exhibition (OFC)*, 2023, pp. 1–3.

[2] S. Bidkar, R. Bonk, and T. Pfeiffer, "Low-Latency TDM-PON for 5G Xhaul," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, 2020, pp. 1–4.

[3] L. Malina, P. Munster, J. Hajny, and T. Horvath, "Towards secure Gigabit Passive Optical Networks: Signal propagation based key establishment," in *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, vol. 04, 2015, pp. 349–354.

[4] L. Li, X. Shouting, and D. De-Gong, "Research of DBA schemes and QoS in PON system," in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, 2016, pp. 2148–2153.

[5] T. Horvath, P. Munster, and M. Filka, "A Novel Unique Parameter for Increasing of Security in GPON Networks," *Journal of Communications Software and Systems*, vol. 12, pp. 112–116, 06 2016.

[6] T. Horvath, V. Clupek, P. Munster, and V. Oujezsky, "Key Exchange with PUF in NG-PON2 Networks," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 2019, pp. 118–121.

[7] ITU-T. "G.987 10-Gigabit Passive Optical Networks". Accessed: May 11, 2023. [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/2022-2024/15/Documents/flyers/Flyer_ITU-T_G.987.pdf

[8] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[9] ITU-T. "G.987.3 10-Gigabit-capable Passive Optical Networks (XG-PON): Transmission Convergence (TC) layer specification". Accessed: May 11, 2023. [Online]. Available: https://www.itu.int/rec/T-REC-G.987.3/en

[10] ——. "G.988 ONU Management and Control Interface (OMCI) specification". Accessed: May 27, 2023. [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.988-202211-I!!PDF-E&type=items

[11] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber algorithm specifications and supporting documentation," *NIST PQC Round*, vol. 2, no. 4, pp. 1–43, 2019.

[12] Argyle Software. "Kyber". Accessed: July 10, 2023. [Online]. Available: https://github.com/Argyle-Software/kyber

[13] The Dalek Cryptography Developers. "Dalek Cryptography". Accessed: July 12, 2023. [Online]. Available: https://github.com/dalek-cryptography