Post-quantum MACsec Key Agreement for Ethernet Networks*

Joo Yeon Cho
ADVA Optical Networking SE
Martinsried, Germany
JCho@adva.com

Andrew Sergeev
ADVA Optical Networking Israel Ltd.
Ra'anana, Israel
ASergeev@adva.com

ABSTRACT

The industrial demand on MACsec in Ethernet networks is increasing substantially, in particular for 5G networks, mainly due to its efficiency paired with strong security. MKA (MACsec Key Agreement) is a companion protocol of MACsec that provides methods of authentication and cryptographic key establishment. In this paper, the MACsec and MKA protocol are analysed under a quantum attack scenario. Even though the threat of quantum computers should not be overstated, it is necessary to provide a new countermeasure that is robust against this potential, yet critical risk. Symmetric-key crypto algorithms defined in MACsec and MKA can achieve 128-bit quantum security if 256-bit keys are mandated. However, classical public-key crypto schemes are known to be vulnerable to quantum attacks so that MKA protocol needs to support post-quantum public-key crypto schemes. We implemented a McEliece-based key establishment which is the most conservative post-quantum public-key cryptosystem with a large size of key, yet feasible for MKA. For entity authentication, we implemented a XMSS hash-based signature scheme that is standardised in IETF. We verified by experiments that selected schemes fit well for a MACsec-enabled Ethernet network.

ACM Reference Format:
Joo Yeon Cho and Andrew Sergeev. 2020. Post-quantum MACsec Key Agreement for Ethernet Networks. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3407023.3409220

1 INTRODUCTION

Layer 2 links are primarily used for transporting a large volume of data in LAN or WAN with high throughput and low latency. MACsec (Media Access Control security) is an IEEE standard protocol which is used to establish a secure channel over Layer 2 [17]. MACsec ensures integrity, confidentiality, and authenticity of Ethernet frames. MACsec can offers strong security, yet requires only a small bytes of overhead for efficient connections. MACsec was specifically developed for LAN security. However, using VLAN tags [21], MACsec has been adopted for wider networks such as WAN and MAN security. Recently, MACsec draws attention for securing the 5G network infrastructure since MACsec has capability to support secure communication of data with low latency for real-time applications such as AI/ML inference [9].

MKA (MACsec Key Agreement) is a companion protocol of MACsec which is used to authenticate devices attached to a network and derive encryption keys based on a hierarchical key structure [20]. A connectivity association key (CAK) is a root key of the key hierarchy.

A quantum attack is a new and critical risk against network security. Popular public-key cryptosystems in use (e.g. RSA, ECC, Diffie-Hellman) are broken by Shor's algorithm when large scale quantum computers are available [29]. One may claim that an existing MACsec protocol could be already quantum-resistant by enforcing the use of 256-bit symmetric keys for a payload encryption and an integrity check. However, such symmetric keys are actually established by a MKA protocol which is not immune to quantum attacks.

1.1 Our contribution

We investigate a MKA protocol in terms of quantum attacks. We apply a post-quantum key exchange protocol and an authentication scheme for shaping a MKA protocol to be quantum-resistant. To the best of our knowledge, this topic has never been investigated in details in the literature.

There are two scenarios for this purpose. Firstly, a standard MKA key hierarchical structure is unchanged. Then, a MSK is established by an post-quantum EAP method where the use of a quantum-resistant cipher suite is mandated. A CAK and other subsequent keys are derived from the MSK. Secondly, an ephemeral key exchange is established directly between peers without a key hierarchy. In fact, this approach has been already widely adopted in industry, especially for WAN or MAN security although this does not comply with a standard MKA protocol. In this paper, we focus on the second scenario since it is suitable for modern networks in terms of security. A hierarchical key structure has a non-negligible risk that if a root key is hacked, an entire security structure is compromised.

The rest of this paper is structured as follows: first, we briefly describe the background on MACsec and post-quantum cryptography. Then, we propose a framework of the post-quantum MACsec key agreement. Next, we describe our test platform and experimental results. Finally, we conclude the paper.

*Produces the permission block, and copyright information

ARES 2020, August 25–28, 2020, Virtual Event, Ireland

ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3409220

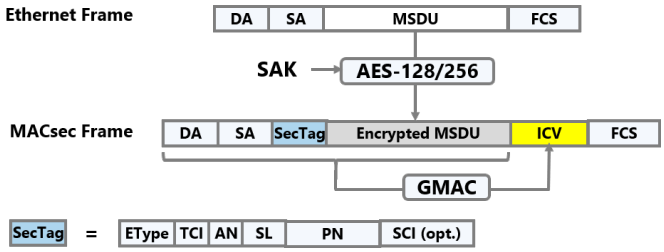

Figure 1: IEEE 802.1AE MACsec encryption and integrity check

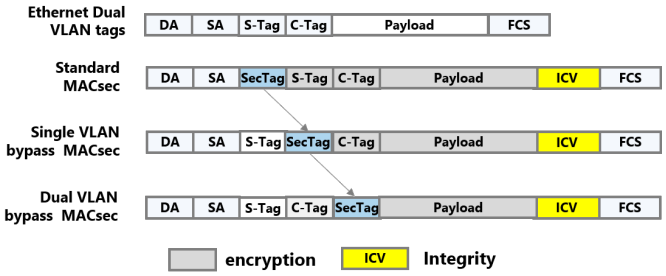

Figure 2: Dual Tag Bypass for multi-hop MACsec

2 BACKGROUND

In this section, MACsec and MKA protocols are briefly described in terms of encryption, authentication and key management framework. Then, a brief introduction on the post-quantum crypto algorithms is given.

2.1 Overview of MACsec

MACsec is an IEEE standard protocol for Layer-2 security [17]. A MACsec packet is formed with an Ethernet frame by adding a SecTAG (Security TAG) and an ICV (Integrity Check Value). A SecTAG conveys information on the protocol, the cipher suites, as well as the PN (packet number) for replay protection. An ICV is a compressed value of the MAC address, SecTAG, and secure data to ensure the integrity of a packet. Note that payload encryption is optional. If a packet-authentication-only mode is configured, MACsec can verify only the integrity of a transmitted packet. Figure 1 shows the structure of a MACsec frame.

MACsec supports a limited number of symmetric-key cipher suites: AES-GCM-128 and AES-GCM-256 with a usage of XPN (eXtended PN) as an option [17]. AES-GCM-128 is a default cipher suite. IEEE 802.1AEbn-2011 [18] adds GCM-AES-256 as an optional cipher suite to allow a 256-bit key. IEEE 802.1AEbw-2013 [19] adds GCM-AES-XPN-128 and GCM-AES-XPN-256 for further optional cipher suites that make use of a 64-bit (PN) to allow more than 2^{32} MACsec protected frames to be sent with a single SAK. MACsec is now part of the Linux kernel from the version 4.6 [23]. Note that the National Security Agency (NSA) designed the Ethernet Security Specification (ESS) on top of MACsec for providing a hardened layer 2 encryption scheme [28].

Although MACsec was developed for LAN security, a MACsec frame can transverse across local networks by applying VLAN tags defined in IEEE 802.1Q [21]. See Fig. 2. This technique allows MACsec to be used for WAN (wide area network) security and provide the end-to-end network encryption over carrier Ethernet.

2.2 MACsec Key Agreement

MKA is a companion protocol of MACsec that provides methods of the cryptographic key establishment for MACsec [20]. MKA is based on a hierarchical key derivation structure. A CAK is a root of the key hierarchy. Each payload of an Ethernet frame is encrypted by a SAK (Secure Association Key) which is derived from a CAK during a key lifetime.

The possession of a CAK is a prerequisite for MACsec membership. All potential members possess the same CAK. Each CAK is identified by a secure connectivity association key name (CKN). There are two ways to establish CAK; one is to configure it as a pre-shared key and the other is to derive a MSK (master session key) by an EAP (Extended Authentication Protocol) method. A CAK is derived from a MSK.

2.3 Overview of Post-quantum Cryptography

The goal of post-quantum cryptography is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks [8]. Post-quantum cryptography is usually classified into five families: code-based, lattice-based, multivariate, symmetric-based, and supersingular isogeny-based. Each family is based on a different mathematical problem that is not feasible so far to solve both with traditional computers as well as quantum computers.

Recently, post-quantum cryptography has drawn lots of attention from the community mainly due to the NIST PQC project [8]. Code-based crypto has strength on KEM. It has been studied for a long time (like RSA) and, the theory is well developed and understood. However, the key size is usually quite large, compared to other families. It seems not suitable for signature schemes. Lattice-based crypto is the most popular among other families. It is applicable to both KEM and signature. However, selecting security parameters is challenging since their security is still not well-understood. Multivariate crypto is suitable for signature but not for KEM. Isogeny-based crypto is relatively new but very promising for KEM in terms of the key size. The project is currently in the stage of the second round [2] and NIST plans to announce the winner(s) around 2022/2024. Table 1 shows the second round candidates of NIST PQC project [2]. Note that NIST supports some hash-based signatures that have been published on IETF [10, 16, 25].

3 CRYPTOGRAPHIC PRIMITIVES

The substantial increase in demand for layer 2 network are due to its efficiency paired with cost savings. A post-quantum key exchange and signature should be conservatively secure as well as sufficiently fast so that they should not be a bottleneck of Layer 2 performance. In particular, an end-to-end MACsec for WAN is more challenging because MACsec packets should travel through multiple networking switches and routers. Hence, a network and

Table 1: The 2nd round candidates of NIST PQC project [2]

Family	*KEM*	*Signature*
Lattice-based	CRYSTALS-KYBER, FrodoKEM, LAC, NewHope, NTRU, SABER, NTRU Prime, Round5, Three Bears	CRYSTALS-DILITHIUM, FALCON, qTESLA
Code-based	Classic McEliece, NTS-KEM, BIKE, HQC, RQC, LEDAcrypt, ROLLO	-
Multivariate	-	GeMSS, LUOV, MQDSS, Rainbow
Symmetric-based	-	Picnic, SPHINCS+
Isogeny-based	SIKE	-

device agnostic protocol is required. Each key exchange and authentication protocol are integrated into an existing protocol in a hybrid way; post-quantum crypto primitives are added independently on top of the current protocol so that the overall security is not compromised.

3.1 Symmetric-key encryption

Currently MACsec supports AES-GCM-(XPN)-128 and AES-GCM-(XPN)-256 for payload encryption and key derivation. It is known that Grover's algorithm can achieve quadratic speedup of brute-force attack against symmetric key encryption [15]. Hence, it should be mandated to use an AES-256 encryption algorithm to achieve 128-bit quantum security. Table 2 shows the summary of post-quantum crypto algorithms that should be applied for post-quantum MACsec.

3.2 Post-quantum key exchange

Candidates of the NIST PQC competition have been evaluated in terms of their security maturity and applicability to protocols in use [2]. While the second round of the NIST competition is still on-going, candidates belonging to code-based cryptography are promising since their background theory and methodology are well developed and understood. We propose a McEliece-based key establishment mechanism which is known to be secure against quantum attacks [24]. Even though a key size is quite large, the security level of the McEliece system has remained remarkably stable, despite dozens of attack papers over 40 years [4]. Other

Table 2: Symmetric-key crypto algorithm used in MACsec and MKA [17, 20]

Name	*Standard*	*Crypto*	*PQ crypto*
MKA	IEEE 802.1X	AES-128 KeyWrap AES-128-CMAC AES-256-CMAC	AES-256 KeyWrap AES-256-CMAC
MACsec	IEEE 802.1AE	AES-GCM-128 AES-GCM-256 AES-GCM-XPN-128 AES-GCM-XPN-256	AES-GCM-256 AES-GCM-XPN-256

quantum-resistant key exchange schemes using a smaller key size might provide better performance. However, they could not provide as strong confidence as the McEliece cryptosystem. Recently, Classic McEliece cryptosystem [4], together with FrodoKEM [13], is recommended by BSI as the most conservative choices for post-quantum crypto key exchange [7]. It is recommended to combine post-quantum key exchange and digital signature schemes with classical crypto primitives in order to achieve crypto agility and reduce attack probability.

3.3 Post-quantum digital signature

In the EAP-TLS protocol, an authentication server and a supplicant exchange their X.509 certificates to validate their authenticity in a mutual way. The X.509 certificate is based on the public key infrastructure (PKI) and their security relies on cryptographic digital signature such as RSA or ECDSA. To defeat quantum attacks, the X.509 certificates need to support post-quantum signature schemes. The NIST PQC competition includes several candidates of signature scheme. Post-quantum PKI schemes have been already proposed in public, for instance, in [6, 22].

In addition, hash-based signatures such as XMSS and LMS became already the Internet Engineering Task Force (IETF) standards [16, 25]. We propose Hash-based signatures for PQ certificates. Hash-based signature (HSS) was initially proposed by Merkle in the late 1970s [27]. HSS does not rely on the conjectured hardness of mathematical problems. Instead, it is proven that it relies only on the properties of cryptographic hash functions. Hash-based signature schemes generally feature small private and public keys as well as fast signature generation and verification but large signatures and relatively slow key generation [5, 16, 26].

4 POST-QUANTUM MKA

As introduced in Section 1, we propose two approaches to achieve the quantum security for MKA. One is to re-shape a key hierarchy of MKA using post-quantum cipher suites and the other is to apply a post-quantum ephemeral key exchange and authentication without a key hierarchy.

4.1 Key hierarchy in MKA

An EAP method in MKA is used for authentication and produces a MSK, followed by a CAK. When EAP is used for authentication, it involves a supplicant (client device), authenticator (switch), and authentication server. According to the MKA standard, any EAP

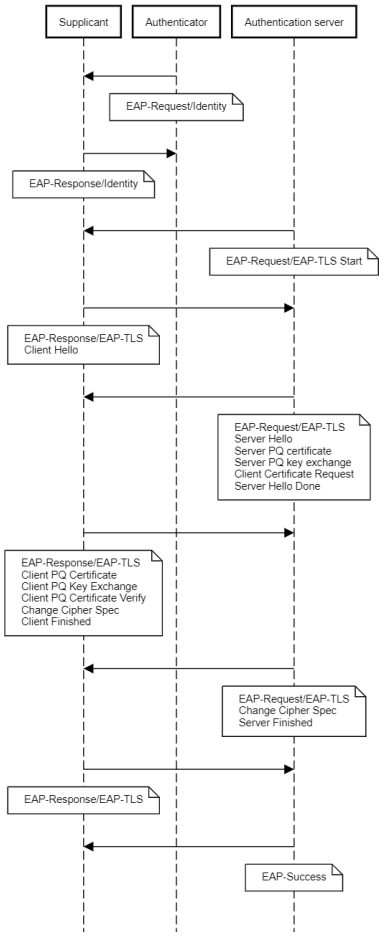

Figure 3: Post-quantum EAP-TLS protocol

method is allowed as long as it supports mutual authentication and a minimum key length. we propose a EAP-TLS-PQ method mandated to use post-quantum cipher suite, which supports certificate-based mutual authentication and a key derivation. An instance of a post-quantum EAP-TLS protocol is depicted in Fig. 3. The main difference to a normal EAP-TLS is to use a PQ key exchange and a PQ certificate exchange between an authentication server and a supplicant. The EAP-TLS method provides a support for fragmentation and reassembly. If the EAP packet size exceeds the EAP MTU of the link, other EAP methods may encounter difficulties due to the large size of public keys of post-quantum crypto schemes.

4.2 Ephemeral key exchange

A centralized key hierarchy framework is sometimes not suitable for end-to-end security, in particular, for WAN or MAN security. In fact, MACSec is not an end-to-end but a hop-by-hop encryption for LAN security. However, the vast majority of MACSec-based solutions is using industrial modifications to overcome the limitations of the MACsec standard for LANs, as shown in Fig. 2. In this scenario, an ephemeral session key exchange protocol between two ends would be simple and efficient. An example of a post-quantum session key

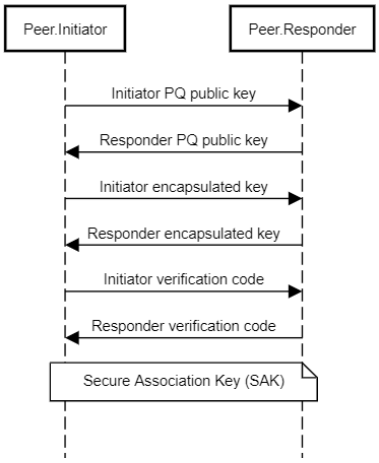

Figure 4: Post-quantum session key exchange

exchange protocol is depicted in Fig. 4. Recently several frameworks have been proposed for integrating a post-quantum key exchange into IKEv2 [14, 31] or a noise protocol [3].

5 EXPERIMENTS

5.1 Chosen primitives

As described in Section 4, we chose the Classic McEliece public-key cryptosystem for a key exchange since it is conservatively designed for strong security and fast encryption/decryption. Various parameter sets were evaluated to achieve high security as well as reasonably good performance, which is required for Layer 2 network in use. We chose two sets of parameters of Classic McEliece; mceliece6960119 and mceliece8192128 in order to offer the same security level of AES-GCM-256 in MACsec. For certificate-based authentication, hash-based signatures using 512-bit hash function were selected for matching the security level of the key exchange.

5.2 Implementation

MACsec and MKA use a limited number of cryptographic primitives due to the efficiency. A secure connection is quickly established and operated with a small overhead. Hence, it is unnecessary to maintain a full package of crypto library; post-quantum crypto primitives can be implemented independently in software. However, there are several requirements for secure implementation in software. For instance, an implemented protocol should run in constant time. There is no data flow from secrets to branch conditions. In particular, MACsec is possibly operated on embedded platforms which may have limited computing power and memory resources. A new security protocol should be implemented using a low level programming language and with optimized usage of resources in mind.

Layer 2 is primarily used for transporting a large volume of data in LAN or WAN with high throughput and low latency. While MACsec offers a strong security solution for Layer 2 (e.g. AES-GCM-256), it adds a small bytes of security overhead and supports a limited set of configurations for efficient connections. Hence, a

post-quantum key exchange and signature should be conservatively secure as well as sufficiently fast so that they should not be a bottleneck of Layer 2 performance. In particular, an end-to-end MACsec for WAN is more challenging because MACsec packets should travel through multiple networking switches and routers. Hence, a network and device agnostic protocol is required. A size of a public-key is another important point of consideration for the MACsec protocol since a maximum payload size of an Ethernet frame is only 1500 bytes and exceeding a payload size may cause unexpected security weaknesses and performance degradation.

It is recommended to combine post-quantum key exchange and digital signature schemes with classical standard crypto primitives such as Diffie-Hellman key exchange and the RSA signature scheme in order to achieve crypto agility and reduce attack probability. A hybrid key exchange and authentication is an on-going research topic e.g. [30].

5.3 Results

An overall structure of the test platform is shown in Fig. 5. We set up a direct MACsec connection between two sets of ADVA FSP 150 ProVMe, each of which is composed of a FPGA and a Linux host using DPDK [1]. A post-quantum key exchange, together with Diffie-Hellman key exchange, is performed on the application running in the host. Actual data communication is occurred through an in-band channel established by DPDK KNI (Kernel NIC Interface) [12]. An authentication using XMSS signature scheme is performed through the client port, interacted with an Radius server.

A session key exchange can be occurred based on the volume of traffic or the time interval. For high capacity links, a key lifetime should be carefully set in such a way that the targeted security level is ensured by encrypting a limited amount of data with a single key. Every MACsec frame contains a unique 32-bit or 64-bit packet number (PN). The (Extended) Packet Number can be used to configure a key lifetime parameter and becomes an initial vector of the GCM-AES-(XPN-)256 cipher suite under the defined MKA policy.

A MACsec packet starts with an Ethernet header with EtherType `0x88E5`. Because MACsec is usually PHY port-based, it supports easy upgrade and high-speed connectivity up to 100G at low power and low cost. The disadvantage of the standard MACsec is that all traffic traversing the link requires matching and verifying secret keys at each node. However, MACsec can be extensively applied to wider networks with VLAN tags, as shown in Fig. 2. For a point-to-point direct link, ASIC-based MACsec adds approximately 1-3 μsec of the latency and about 32 extra bytes of overhead. For the sake of completeness, we also checked a software-based AES-GCM-256 MACSec implementation. To get the best from x86 CPU, we used DPDK [11] with aes-ni-gcm driver for symmetrical encryption. The throughput and average latency varied with IP packet sizes as shown in Table 3. For 64 bytes of packets, the throughput and latency of MACsec are around 2300 Mbps and 34 μsec, respectively. Whereas, for 1420 bytes of packets, they are around 9000 Mbps and 149 μsec, respectively.

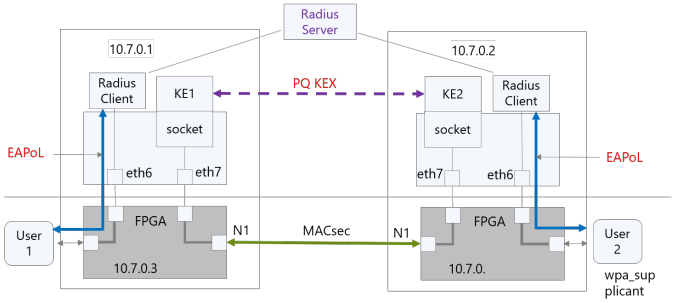

Figure 5: A test platform for post-quantum MACsec key agreement

Table 3: Experimental throughput and average latency of MACsec on a point-to-point direct link

Packet size	Throughput	Avg. latency
64 bytes (min)	2300 Mbps	34 μsec
1420 bytes (max)	9000 Mbps	149 μsec

6 CONCLUSION

A concern about quantum attacks is increasing on network security. Even though the advent of a large scale of quantum computers is not clear yet, it is widely agreed that implementing countermeasures based on the current available methods would be beneficial for a long term security. In this paper, we analyze the MACsec key agreement, defined in IEEE 802.1X-2010. Since the security of key hierarchy stems from a master session key which is derived from the EAP method, it suffices to use post-quantum crypto suites for EAP, in particular, for a key exchange and a certificate-based authentication. As a non-standard way, we propose an ephemeral session key exchange protocol that can derive an encryption key directly from a post-quantum public-key scheme. This is useful for end-to-end security and a standard key hierarchy framework is too complicated to apply. It is noted that a key size of post-quantum cipher suites usually exceeds greatly the Ethernet MTU (around 1500 bytes). Hence, a strategy of fragmentation and reassembly is crucial to protect against denial-of-service attacks. In the future, we will extend our experiments for wide networks under several attack scenarios.

ACKNOWLEDGMENT

This research is co-funded by the Federal Ministry of Education and Research of Germany under the QuaSiModO project (Grant agreement No 16KIS1051).

REFERENCES

[1] ADVA Optical Networking: FSP 150 ProVMe Series. https://www.adva.com/en/products/packet-edge-and-aggregation/edge-computing/fsp-150-provme-series
[2] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D.: Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process (January 2019)
[3] Appelbaum, J., Martindale, C., Wu, P.: Tiny wireguard tweak. Cryptology ePrint Archive, Report 2019/482 (2019), https://eprint.iacr.org/2019/482

[4] Bernstein, D., Chou, T., Lange, T., Maurich, I., Misoczki, R., Niederhagen, R., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Wang, W.: Classic McEliece: conservative code-based cryptography (2019), https://classic.mceliece.org/nist/mceliece-20190331.pdf

[5] Bernstein, D., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O'Hearn, Z.: Sphincs: Practical stateless hash-based signatures. In: Advances in Cryptology – EUROCRYPT 2015. pp. 368–397 (2015)

[6] Bindel, N., Herath, U., McKague, M., Stebila, D.: Transitioning to a quantum-resistant public key infrastructure. Cryptology ePrint Archive, Report 2017/460 (2017), https://eprint.iacr.org/2017/460

[7] Bundesamt für Sicherheit in der Informationstechnik: Kryptographische verfahren: Empfehlungen und schlüssellängen. BSI TR-02102-1 (March 2020)

[8] Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D.: Report on post-quantum cryptography (2016), nISTIR 8105

[9] Cho, J.Y., Sergeev, A., Zou, J.: Securing ethernet-based optical fronthaul for 5g network. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES '19 (2019)

[10] Cooper, D., Apon, D., Dang, Q., Davidson, M., Dworkin, M., Miller, C.: Recommendation for stateful hash-based signature schemes. Draft NIST Special Publication 800-208 (December 2019), NIST.SP.800-208-draft.pdf

[11] DPDK: Data plane development kit, https://www.dpdk.org

[12] DPDK documentation: Kernel nic interface. https://doc.dpdk.org/guides/prog_guide/kernel_nic_interface.html

[13] E. Alkim, J.W. Bos, L.D.P.L.I.M.M.N.V.N.C.P.A.R.D.S.: Frodokem: Learning with errors key encapsulation (July 2019), https://frodokem.org/files/FrodoKEM-specification-20190702.pdf

[14] Fluhrer, S., Kampanakis, P., McGrew, D., Smyslov, V.: Mixing Preshared Keys in IKEv2 for Post-quantum Security (January 2020), draft-ietf-ipsecme-qr-ikev2-11

[15] Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. pp. 212–219. STOC '96, ACM (1996)

[16] Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., Mohaisen, A.: XMSS: Extended Hash-Based Signatures. Internet-Draft draft-irtf-cfrg-xmss-hash-based-signatures-12, Internet Engineering Task Force (Jan 2018), work in Progress

[17] IEEE: Local and metropolitan area networks–media access control (mac) security. 802.1AE: MAC Security (MACsec), https://1.ieee802.org/security/802-1ae/

[18] IEEE: Media access control (mac) security amendment 1: Galois counter mode–advanced encryption standard– 256 (gcm-aes-256) cipher suite. 802.1AEbn-2011, https://1.ieee802.org/security/802-1aebn/

[19] IEEE: Media access control (mac) security amendment 2: Extended packet numbering. 802.1AEbw-2013, https://1.ieee802.org/security/802-1aebw/

[20] IEEE: Local and metropolitan area networks–port-based network access control. IEEE Std 802.1X-2010 (Revision of IE EE Std 802.1X-2004) pp. 1–205 (Feb 2010)

[21] IEEE: Ieee standard for local and metropolitan area network–bridges and bridged networks. IEEE Std 802.1Q-2018 (Revision of IEEE Std 802.1Q-2014) pp. 1–1993 (July 2018)

[22] Kampanakis, P., Panburana, P., Daw, E., Geest, D.V.: The viability of post-quantum x.509 certificates. Cryptology ePrint Archive, Report 2018/063 (2018), https://eprint.iacr.org/2018/063

[23] KernelNewbies: 802.1ae mac-level encryption (macsec), linux 4.6 (May 2016)

[24] McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. In: Deep Space Network Progress Report. vol. 44, pp. 114–116 (January 1978)

[25] McGrew, D., Curcio, M., Fluhrer, S.: Leighton-Micali Hash-Based Signatures. RFC 8554 (Apr 2019), https://rfc-editor.org/rfc/rfc8554.txt

[26] McGrew, D., Curcio, M., Fluhrern, S.: Hash-based signatures (2018), draft-mcgrew-hash-sigs-10

[27] Merkle, R.: A certified digital signature. In: Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings. pp. 218–238 (1989)

[28] National Security Agency: Ethernet security specification, version 0.5 (October, 2011)

[29] Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. SFCS '94, IEEE Computer Society (1994)

[30] Steblia, D., Fluhrer, S., Gueron, S.: Hybrid key exchange in TLS 1.3 (Feb 2020)

[31] Tjhai, C., Tomlinson, M., Bartlett, G., Fluhrer, S., Geest, D.V., Garcia-Morchon, O., Smyslov, V.: Multiple Key Exchanges in IKEv2, Internet-Draft (Jan 2020), draft-ietf-ipsecme-ikev2-multiple-ke-00