Post-quantum MACsec in Ethernet Networks

Joo Yeon Cho* and Andrew Sergeev

ADVA Optical Networking SE, Fraunhoferstrasse 9a, Martinsried, 82152, Germany
E-mail: JCho@adva.com; ASergeev@adva.com
**Corresponding Author*

Received 30 November 2020; Accepted 01 December 2020;
Publication 11 March 2021

Abstract

The demand on MACsec in Ethernet is increasing substantially since MACsec fits well for industrial applications which require strong security as well as efficiency. To provide a long-term security, the MACsec protocol should be resistant to future attacks including quantum attacks. In this paper, MACsec is analysed under a quantum attack scenario. To achieve 128-bit quantum security, AES (Advanced Encryption Standard) algorithms defined in MACsec should mandate to use 256-bit keys. On the other hand, classical public-key cryptosystems in MKA are not secure at all against quantum attacks so that they need to be replaced by post-quantum crypto schemes in a quantum world. We propose an authenticated post-quantum key establishment protocol which is suitable for long-term secure MACsec. The proposed protocol is used in the hybrid mode, an ephemeral key exchange, and an end-to-end encryption. We verified by experiments that the proposed protocol can be deployed in existing a MACsec-enabled Ethernet network.

Keywords: MACsec, MKA, EAP, post-quantum cryptography, authentication.

Journal of Cyber Security and Mobility, Vol. 10_1, 161–176.
doi: 10.13052/jcsm2245-1439.1016

1 Introduction

Layer 2 links are commonly used for transporting a large volume of data 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 [1]. MACsec ensures integrity, confidentiality, and authenticity of Ethernet frames. MACsec offers strong security yet requires only a small amount of additional overhead, making the protocol suitable for secure Ethernet connections.

MACsec was originally developed for LAN (Local Area Network) security. However, using VLAN tags [2], MACsec can be adopted for wider networks such as WAN (Wide Area Network) and MAN (Metropolitan Area Network) security. Recently, MACsec draws lots of attention for securing the 5G network infrastructure since MACsec has capability to support secure communication of data with low latency for real-time 5G applications [3].

MKA (MACsec Key Agreement) is a companion protocol of MACsec that provides methods of cryptographic key establishment and authentication. After the MKA protocol is performed, a MSK (Master Session Key) is generated and subsequent keys are built in a hierarchical way [4]. Note that CAK (Connectivity Association Key), which is derived from MSK, becomes a root key of the key hierarchy.

1.1 Our Contribution

A quantum attack is a new and critical risk against network security. Popular public-key cryptosystems in use (e.g. RSA, ECC and Diffie-Hellman) could be broken by Shor's algorithm when large scale quantum computers are available [5]. Even though the threat of quantum computers should not be overstated, we need to be well prepared with a new countermeasure against such critical attack.

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 authentication. However, such symmetric keys themselves are established by the MKA protocol which is not immune to quantum attacks.

We propose an authenticated post-quantum (PQ) key exchange protocol for shaping the MACsec and MKA protocol to be quantum resistant. There are two scenarios for this purpose. The first scenario is to use a standard MKA key hierarchical structure. A MSK can be established by a PQ EAP (Extensible Authentication Protocol) method where the use of a quantum-resistant cipher suite is mandated. A CAK and other subsequent keys are derived from MSK in a hierarchical way. In the second scenario, an ephemeral key exchange is executed directly between two peers so that each session key is independently generated. In this scenario, a hierarchical key structure is not needed.

While the first scenario is suitable for the security of a small size of Ethernet network, it has a non-negligible risk that a security structure is entirely compromised if a root key is hacked. Since modern networks are often built in a wide area and require long-term security, the second scenario is more suitable in terms of key management. In fact, an ephemeral key exchange has been already widely adopted in industry, especially for WAN or MAN security. Therfore, we focus on the second scenario although this does not really comply with a standard MKA protocol.

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

2 Background

In this section, MACsec and MKA protocols are briefly described in terms of encryption, authentication, and key management framework. Then, PQ crypto algorithms are briefly described.

2.1 Overview of MACsec

MACsec is an IEEE standard protocol for Layer-2 security [1]. 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. AES-GCM-128 is a default cipher suite. GCM-AES-256 is added to IEEE 802.1AEbn-2011 [6] as an optional cipher suite to allow a

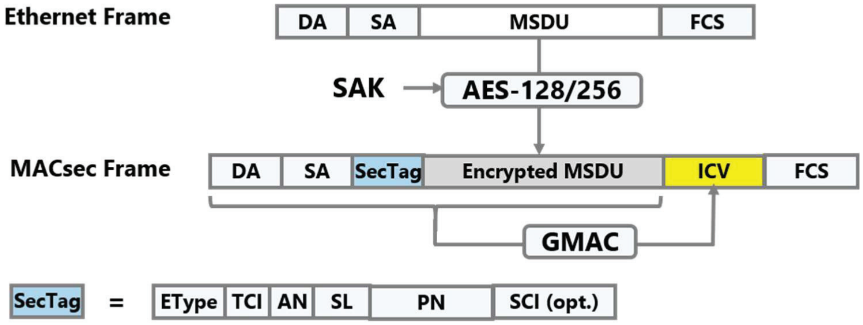


Figure 1 IEEE 802.1AE MACsec encryption and integrity check.

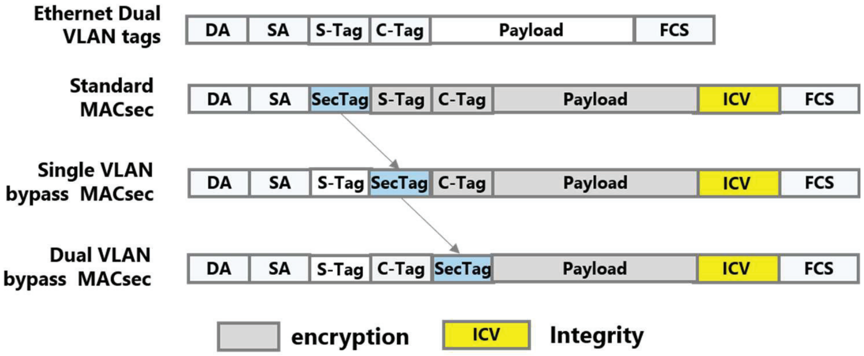


Figure 2 Dual Tag Bypass for multi-hop MACsec.

256-bit key. GCM-AES-XPN-128 and GCM-AES-XPN-256 are added to IEEE 802.1AEbw-2013 [7] 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.

Although MACsec was developed for LAN security, a MACsec frame can transverse across local networks by applying VLAN tags defined in IEEE 802.1Q [2]. See Figure 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.

MACsec is now part of the Linux kernel from the version 4.6 [8]. 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 [9].

2.2 MACsec Key Agreement

MKA is a companion protocol of MACsec that provides methods of the cryptographic key establishment for MACsec [4]. 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 by an EAP method. A CAK is derived from the MSK.

2.3 Overview of PQ Cryptography

The goal of PQ cryptography is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks [10]. PQ 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, PQ cryptography has drawn lots of attention from the community mainly due to the NIST PQC project [10]. Code-based crypto has strength on KEM (Key Encapsulation Mechanism). It has been studied for a long time 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 third round [11] and NIST plans to announce the winner(s) around 2022/2024. The third-round candidates of NIST PQC project are listed in Table 1. In addition, hash-based signatures should be counted since they have been already standardized in IETF and supported by NIST [12–14]. Note that KEM stands for Key Encapsulation Mechanism by which a data encryption key is derived. Signature schemes are typically used for the entity authentication.

Table 1 The 3rd round candidates of NIST PQC project [11] and IETF PQC standards

SDO	Family	KEM	Signature
NIST	Lattice-based	CRYSTALS-KYBER [15] NTRU [16] SABER [17]	CRYSTALS-DILITHIUM [18] FALCON [19]
	Code-based	Classic McEliece [20]	
	Multivariate		Rainbow [21]
IETF	Hash-based		XMSS [13] LMS [14]

3 PQ Cryptographic Primitives

The substantial increase in demand for layer 2 network are due to its efficiency paired with cost savings. A PQ 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. It is noted that an end-to-end MACsec for WAN is more challenging because MACsec packets need to travel through multiple networking switches and routers. Hence, a new protocol should be transparent to intermediate devices. An authenticated key exchange protocol is integrated into an existing protocol in a hybrid way; PQ crypto primitives are added independently on top of the classical crypto protocol so that the overall security is at least as strong as the weakest one.

3.1 Symmetric-key Encryption

The MACsec standard supports AES-GCM-(XPN)-128 and AES-GCM-(XPN)-256 for payload encryption and subsequent key derivation. It is known that Grover's algorithm can achieve quadratic speedup of brute-force attack against symmetric key encryption [22]. Hence, it is generally agreed that symmetric-key encryption can be quantum-resistant if 256-bit keys are mandated. Table 1 shows the summary of symmetric-key crypto algorithms that should be applied for PQ MACsec.

3.2 Key Establishment

Although the NIST PQC standardization process is currently on-going, the 3rd round finalists of the project would be the best candidates for PQ key exchange and signature primitives, which are listed in Table 1. Each primitive provides multiple parameter-sets for different security levels.

Among various parameter sets, the security level equivalent to that of AES-256 is the category 5, which is the strongest level in the NIST

Table 2 Migration of symmetric-key crypto algorithm in MACsec and MKA [1, 4]

Protocol	Standard	Classical Security	Quantum Security
MKA	IEEE 802.1X	AES-128 KeyWrap AES-128-CMAC	AES-256 KeyWrap AES-256-CMAC
MACsec	IEEE 802.1AE	AES-GCM-128 AES-GCM-XPN-128	AES-GCM-256 AES-GCM-XPN-256

project. Hence, our choice for KEM is as follows: mceliece6960119 (Classic McEliece), ntruhps4096821 (NTRU), kyber1024 (Crystal-Kyber) and FireSaber (Saber). In addition, FrodoKEM is recommended by BSI as the most conservative choices for PQ crypto key exchange [23, 24].

In particular, the most conservative choice is to use a key establishment scheme based on Classic McEliece KEM [25]. 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. Other quantum-resistant key exchange schemes using a smaller key size might provide better performance. However, they could not provide as strong confidence as the Classic McEliece cryptosystem.

3.3 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 PQ signature schemes. The NIST PQC competition includes several candidates of signature scheme. PQ PKI schemes have been already proposed in public, for instance, in [26, 27].

For signature primitives, our choices include Crystal-Dilithium and Falcon, which are listed in Table 1. Note that the security of Rainbow is not fully evaluated. In addition, hash-based signatures such as XMSS and LMS became already the Internet Engineering Task Force (IETF) standards [13, 14]. Hash-based signature (HSS) was initially proposed by Merkle in the late 1970s [28]. HSS does not rely on the conjectured hardness of mathematical problems. Instead, it relies only on the properties of proven 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.

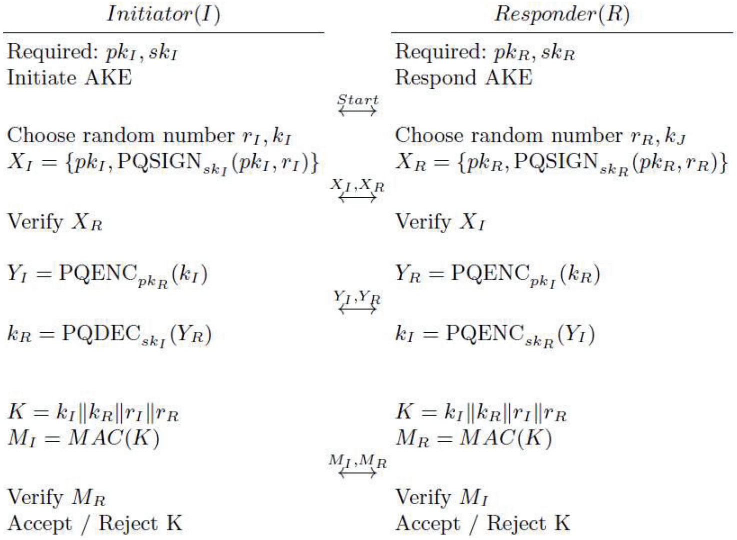
4 PQ MKA

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 PQ cipher suites and the other is to apply a PQ ephemeral key exchange and authentication without a key hierarchy.

4.1 Ephemeral Key Exchange

A centralized key hierarchy framework is sometimes not suitable for a medium or large size networks such as 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 take industrial modifications to overcome the limitations of the MACsec standard, as shown in Figure 2. In this scenario, an ephemeral session key exchange protocol between two ends would be simple and efficient. Recently several frameworks have been proposed for integrating a PQ key exchange into IKEv2 [29, 30] or a noise protocol [31].

An example of a PQ session key exchange protocol is depicted in Figure 3. Suppose Initiator and Responder perform an AKE protocol. Both peers are assumed to have generated a pair of public and secret key. To agree upon



$Initiator(I)$		$Responder(R)$
Required: pk_I, sk_I Initiate AKE		Required: pk_R, sk_R Respond AKE
	$\overset{Start}{\longleftrightarrow}$	
Choose random number r_I, k_I $X_I = \{pk_I, \text{PQSIGN}_{sk_I}(pk_I, r_I)\}$		Choose random number r_R, k_J $X_R = \{pk_R, \text{PQSIGN}_{sk_R}(pk_R, r_R)\}$
	$\overset{X_I, X_R}{\longleftrightarrow}$	
Verify X_R		Verify X_I
$Y_I = \text{PQENC}_{pk_R}(k_I)$		$Y_R = \text{PQENC}_{pk_I}(k_R)$
	$\overset{Y_I, Y_R}{\longleftrightarrow}$	
$k_R = \text{PQDEC}_{sk_I}(Y_R)$		$k_I = \text{PQENC}_{sk_R}(Y_I)$
$K = k_I \| k_R \| r_I \| r_R$ $M_I = MAC(K)$		$K = k_I \| k_R \| r_I \| r_R$ $M_R = MAC(K)$
	$\overset{M_I, M_R}{\longleftrightarrow}$	
Verify M_R Accept / Reject K		Verify M_I Accept / Reject K

Figure 3 A PQ authenticated key exchange protocol.

a new session key, two peers execute an AKE protocol using PQ crypto primitives listed in Table 1.

4.2 Key Hierarchy in MKA

An EAP method in MKA is used for authentication and produces an 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 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 PQ cipher suite, which supports certificate-based mutual authentication and a key derivation. An instance of a PQ EAP-TLS protocol is depicted in Figure 4. 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 PQ crypto schemes.

5 Experiments

In this section, we describe the results of our experiments on the PQ MACsec protocol in Ethernet.

5.1 Chosen Primitives

As described in Section 3.2, we chose the Classic McEliece public-key cryptosystem for KEM 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 to offer the same security level of AES-GCM-256 in MACsec. For certificate-based authentication, hash-based signatures using a 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

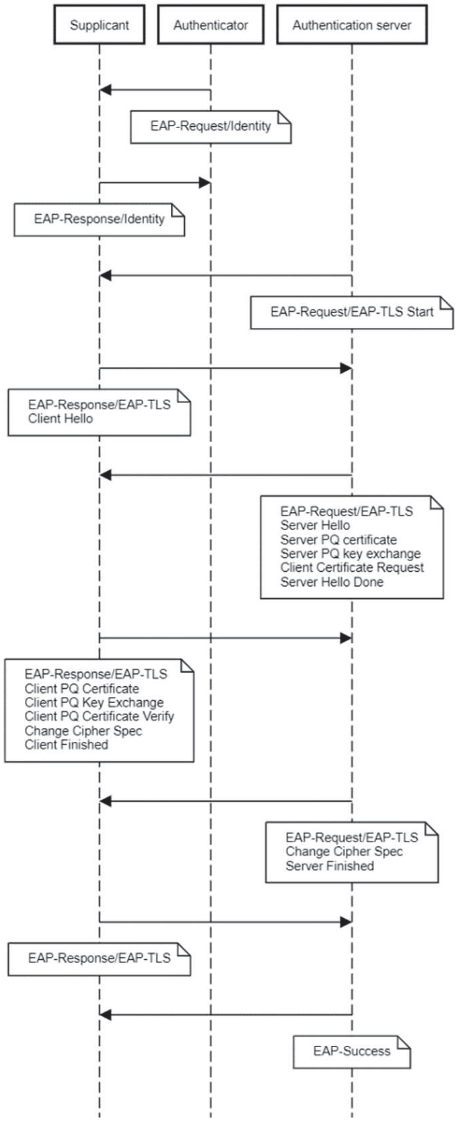


Figure 4 Post-quantum EAP-TLS protocol.

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 to achieve crypto agility and reduce attack probability. A hybrid key exchange and authentication is an on-going research topic e.g. [32].

5.3 Results

An overall structure of the test platform is shown in Figure 5. We set up a direct MACsec connection between two sets of ADVA FSP150 ProVMe, each of which is composed of a FPGA and a Linux host using DPDK [33]. 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) [34]. An authentication using XMSS signature scheme is performed through the client port, interacted with a 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

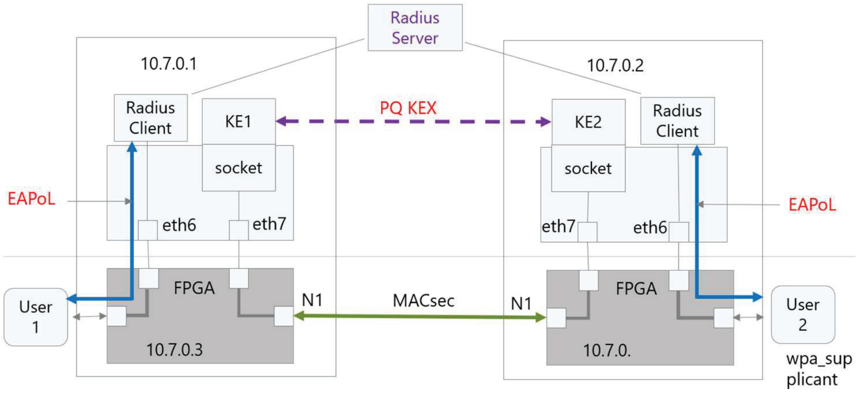


Figure 5 A test platform for post-quantum MACsec key agreement.

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 usec
1420 bytes (max.)	9000 Mbps	149 usec

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 Figure 2.

For a point-to-point direct link, ASIC-based MACsec adds approximately 1–3 usec 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 [35] 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 usec, respectively. Whereas, for 1420 bytes of packets, they are around 9000 Mbps and 149 usec, respectively.

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 analyse 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] I. 802.1AE-2018, “IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security,” 2018. [Online]. Available: https://1.ieee802.org/security/802-1ae/.

[2] I. S. 802.1Q-2018, “IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks,” IEEE.

[3] 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)*, 2019.

[4] I. 802.1X-2010, “Standard for local and metropolitan area network – port-based network access control,” IEEE.

[5] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring.,” *35th annual IEEE symposium on the foundations of computer science*, 1994.

[6] 802.1AEbn-2011, “Media Access Control (MAC) Security Amendment 1: Galois Counter Mode–Advanced Encryption Standard–256 (GCM-AES-256) Cipher Suite,” IEEE.

[7] I. 802.1AEbw-2013, “Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering”.

[8] KernelNewbies, “802.1AE MAC-level encryption (MACsec), Linux 4.6,” 2016.

[9] N. S. Agency, “Ethernet Security Specification, version 0.5,” 2011.

[10] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, “Report on Post-Quantum Cryptography, NISTIR 8105,” 2016.

[11] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson and D. Smith-Tone, “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process,” 2020.

[12] D. Cooper, D. Apon, Q. Dang, M. Davidson, M. Dworkin and C. Miller, “Recommendation for Stateful Hash-Based Signature Schemes, Draft NIST Special Publication 800-208”.

[13] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld and A. Mohaisen, “XMSS: Extended Hash-Based Signatures,” Internet Engineering Task Force, 2018.

[14] D. McGrew, S. Fluhrer and M. Curcio, “Leighton-Micali Hash-Based Signatures, RFC 8554,” RFC, 2019.

[15] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, G. Seiler and D. Stehle, “CRYSTALS-Kyber,” 2019.

[16] C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijneveld, J. Schanck, P. Schwabe, W. Whyte and Z. Zhang, “NTRU,” 2019.

[17] J. D’Anvers, A. Karmakar, S. Roy and F. Vercauteren, “SABER: Mod-LWR based KEM”.

[18] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler and D. Stehle, “CRYSTALS-Dilithium”.

[19] T. Prest, P. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte and Z. Zhang, “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU”.

[20] D. Bernstein, T. Chou, T. Lange, I. Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer and W. Wang, "Classic McEliece: conservative code-based cryptography".

[21] J. Ding, M. Chen, A. Petzoldt, D. Schmidt and B. Yang, "Rainbow".

[22] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96*, 1996.

[23] E. Alkim, J. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Ragunathan and D. Stebila, "FrodoKEM: Learning With Errors Key Encapsulation".

[24] BSI, "Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1," Bundesamt für Sicherheit in der Informationstech-niK, 2020.

[25] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Deep Space Network Progress Report, 1978.

[26] N. Bindel, U. Herath, M. McKague and D. Stebila, "Transitioning to a Quantum-Resistant Public Key Infrastructure," 2017.

[27] P. Kampanakis, P. Panburana, E. Daw and D. V. Geest, "The Viability of Post-quantum X.509 Certificates," 2018.

[28] R. Merkle, "A Certified Digital Signature," Advances in Cryptology – CRYPTO '89, 1989.

[29] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. V. Geest, O. Garcia-Morchon and V. Smyslov, "Multiple Key Exchanges in IKEv2, Internet-Draft".

[30] S. Fluhrer, P. Kampanakis, D. McGrew and V. Smyslov, "Mixing Preshared Keys in IKEv2 for Post-quantum Security".

[31] J. Appelbaum, C. Martindale and P. Wu, "Tiny WireGuard Tweak".

[32] D. Steblia, S. Fluhrer and S. Gueron, "Hybrid key exchange in TLS 1.3," 2020.

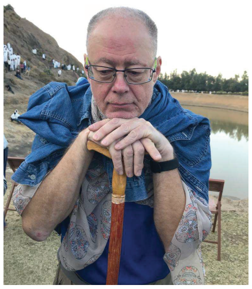
[33] ADVA, "FSP 150 ProVMe Series," ADVA Optical Networking.

[34] "Kernel NIC Interface, DPDK documentation," [Online]. Available: https://doc.dpdk.org/guides/prog_guide/kernel_nic_interface.html.

[35] DPDK, "Data Plane Development Kit," [Online]. Available: https://www.dpdk.org.

Biographies

Joo Yeon Cho received the Ph.D. degree in cryptography from the Macquarie University, Australia, in 2007. He has worked on the research and development of cryptography and data security for more than 10 years. He is currently a Principal Engineer in the Advanced Technology group at ADVA Optical Networking in Munich, Germany. His expertise comprises cryptography, network security, quantum security and cybersecurity.



Andrew Sergeev is currently a senior principal engineer in the Advanced Technology department at ADVA Optical Networking, actively participating in various projects in the field of Network Function Virtualization (NFV) and of modern cryptography. Andrew has a broad hands-on experience in software development, system engineering and design for data communications and wireless data services. He is the author of more than twenty inventions in the networking area. Andrew graduated from the Saint Petersburg State Electrotechnical University with a M.Sc. in electrical engineering.