Post-Quantum Impacts on V2X Certificates – Already at The End of The Road

Takahito Yoshizawa
imec-COSIC KU Leuven
Kasteelpark Arenberg 10 Bus 2452
Leuven, B-3001, Belgium
takahito.yoshizawa@esat.kuleuven.be

Bart Preneel
imec-COSIC KU Leuven
Kasteelpark Arenberg 10 Bus 2452
Leuven, B-3001, Belgium
bart.preneel@esat.kuleuven.be

***Abstract*—The current certificate definition for vehicle-to-everything (V2X) communication does not support forward compatibility as it does not take migration toward Post Quantum Cryptography (PQC) into account. As a result, introducing PQC-compatible certificates in V2X can result in similar to Distributed Denial-of-Service (DDoS) attack to both legacy and PQC-ready vehicles. This situation will make the deployment of PQC certificates a stalemate situation. In addition, due to the larger public key and signature sizes in PQC algorithms, V2X message size will significantly increase, causing the channel capacity and effective transmission range to decrease. This situation will negatively impact the operation of V2X communication. In this sense, any unnecessary channel usages need to be avoided. We propose to revise the certificate definitions in IEEE 1609 and ETSI Intelligent Transport System (ITS) standards to address and mitigate these issues and pave the way for the migration toward PQC algorithm.**

***Index Terms*—Vehicular communication, V2X, Post-Quantum Cryptography, PKI, Certificate**

I. Introduction

Vehicular communication is intended to improve road safety by reducing accidents [10]. This is achieved by vehicles sharing their information with one another to establish and maintain situational awareness of their surroundings, and disseminate warning situations when needed so that receiving vehicles can assess the situation and take necessary action.

Vehicles protect the message integrity using digital certificates and digital signatures. Transmitting vehicles generate a message, calculate a message signature for it, and attach a certificate upon transmission. Using this information, receiving vehicles verify the transmitting vehicle's authenticity and message integrity by verifying the certificate chain and the received signature using the public key in the certificate. In this sense, the generation and distribution of certificates in the PKI system is an essential part of the security mechanism in the V2X communication.

In recent years, advancing capabilities of quantum computers pose significant threats to the security of computer systems. Specifically, public-key-based algorithms are vulnerable to quantum computers [7]. This situation led governments, industries, and academia to research and investigate alternative algorithms that can withstand against the threats and attacks using quantum computers [3].

To address the continuing evolution of quantum computers and their threats, migration to PQC algorithms will occur in the future, although its capability to run Shor's algorithm is expected to be still 25 to 30 years away [22]. To stay ahead of this situation, the National Institute of Standards and Technology (NIST) recommends migrating to post-quantum algorithms by 2030 [18].

We have examined the existing V2X standards from the perspective of migrating to PQC algorithms, and identified issues in the existing certificate definitions. We believe these issues are significant to the extent that its migration itself will cause major disruption to the normal operation of both legacy and new PQC-ready vehicles. In this sense, we propose that IEEE 1609 and ETSI ITS address the necessary changes to support forward compatibility in these standards immediately. In addition, we propose to reduce any unnecessary use of communication channel from these standards to minimize the impact of increasing channel use due to large certificates.

The rest of this paper is organized as follows. We describe the background and issues in the existing standards in Sec. II, propose the solution to address these issues in Sec. III, and give proposals in Sec. IV. In Sec. V, we discuss related work, followed by a conclusion in Sec. VI.

II. Background

A. Certificate Definition in V2X Standards

The IEEE 1609.2 standard for the US [20] and the ETSI TS 103.097 [12] for Europe define certificate formats used in V2X communication. The former was standardized first in 2006, leading the latter to adopt and modify it as a European standard in 2013. Instead of reusing an existing certificate format such as X.509 [21], IEEE 1609.2 defined a custom-tailored certificate format. Certificates from these standards [12], [20] are used by entities in the V2X certificate management system including root Certificate Authority (RCA) and intermediate CAs (ICA) to secure the communication among them, as well as end-entities such as vehicles and Road Side Units (RSUs). Certificates used by vehicles are called *pseudonym certificates* due to the intended purpose of being anonymous in

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

order to protect vehicle owners' privacy. For message integrity protection purposes, these standards require to use Elliptic Curve Digital Signature Algorithm (ECDSA) to generate digital signatures. In ECDSA, the public key (PK) and the signature length are 32 and 64 bytes, respectively.

B. Emergence of PQC Algorithms

Since 2012, standardization work has been in progress, organized by the NIST, to select PQC algorithms that are resistant to attacks using post-quantum computers. This competition includes both Key-Encapsulation Mechanisms (KEM) and signature algorithms. In June 2022, the third round evaluation result was finalized and published [1]. Signature algorithms selected for the fourth round include: CRYSTALS-Dilithium [9], Falcon [15], and SPHINCS+ [28]. The first two are lattice-based and the last one is a hash-based scheme.

One notable characteristic of these PQC algorithms is that their PK and signature are longer than conventional signature algorithms such as ECDSA. Their exact sizes vary from one algorithm to another. In an extreme case, PK size reaches close to 2 Mbytes in the Rainbow-V signature algorithm.[1] From V2X communication's perspective, this implies that a PQC certificate and its corresponding digital signature will make messages significantly longer than the ones using conventional ECDSA. This incurs additional processing burden and certificate storage in the vehicle On-Board Unit (OBU). Furthermore, this will incur a higher load on the communication channel. This is a concern from the perspective of real-time systems such as V2X communication in which messages among moving vehicles need to be processed in the order of milliseconds to avoid accidents and improve road safety.

C. Migration to PQC Algorithm

There will be a transition period in which a new PQC signature algorithm is introduced and disseminated. As different types of vehicles made by multiple vehicle manufacturers coexist on the road, V2X communication will be a mixture of both *legacy* vehicles (ECDSA-based PKs and signatures) and the new *PQC-capable* vehicles (PQC-based PKs and signatures) during this transition period. As introducing new technologies can take a long time, especially when durable goods such as automobiles are involved, this transition period can last years. In fact, as vehicles are driven for as long as 23 years [23], this migration needs to occur seamlessly. This implies that new *PQC-capable* vehicles need to be backward compatible as well as *legacy* vehicles need to be forward compatible. Doing so will ensure that migration from the legacy to a new PQC algorithm over a long period does not impact the overall functionalities of V2X communication. As discussed in Sec. I, NIST recommends that mitigation against quantum attacks should be in place by 2030 [18]. This implies V2X PKI systems must also migrate to the PQC algorithm according to this time frame.

[1]Rainbow was not selected to the fourth round in the NIST competition [1].

III. Discussion

A close examination of the existing standards for V2X communication [12], [20] indicates that this intended smooth migration we discussed in Sec. II-C will not occur. On the contrary, introduction of a new PQC algorithm likely create significant disruptions to both *legacy* and new *PQC-capable* vehicles equally. The observable symptom is equivalent to a variation of DDoS attacks.

A. Absence of Forward Compatibility

The most prominent issue in the existing certificate format is the absence of *forward compatibility*. Forward compatibility means that legacy implementations accept and process certificates used by newer implementations. This is ensured by the use of an optional *extension* field. In fact, X.509 certificate definition [21] includes an extension field. This field allows newer version certificate to include additional data as *non-critical* information. As a comparison, the existing certificate definition in IEEE 1609.2 [20] is shown in Fig. 1.[2] It is also used as a baseline of ETSI ITS certificate definition [12].

```
Certificate ::= CertificateBase (ImplicitCertificate |
                                 ExplicitCertificate)
SequenceOfCertificate ::= SEQUENCE OF Certificate

CertificateBase ::=
      SEQUENCE  { version                 Uint8(3),
                  type                    CertificateType,
                  issuer                  IssuerIdentifier,
                  toBeSigned              ToBeSignedCertificate,
                  signature               Signature OPTIONAL
                }


ToBeSignedCertificate ::= SEQUENCE  {
  id                    CertificateId,
  cracaId               HashedId3,
  crlSeries             CrlSeries,
  validityPeriod        ValidityPeriod,
  region                GeographicRegion OPTIONAL,
  assuranceLevel        SubjectAssurance OPTIONAL,
  appPermissions        SequenceOfPsidSsp OPTIONAL,
  certIssuePermissions  SequenceOfPsidGroupPermissions OPTIONAL,
  certRequestPermissions SequenceOfPsidGroupPermissions OPTIONAL,
  canRequestRollover    NULL OPTIONAL,
  encryptionKey         PublicEncryptionKey OPTIONAL,
  verifyKeyIndicator    VerificationKeyIndicator,
  ...
}
(WITH COMPONENTS { ..., appPermissions PRESENT} |
 WITH COMPONENTS { ..., certIssuePermissions PRESENT} |
 WITH COMPONENTS { ..., certRequestPermissions PRESENT})
```

Fig. 1: Certificate Definition in IEEE 1609.2 [20]

In the context of PQC migration, a PK and an issuing CA's signature using the new PQC algorithm can be carried in this field. Legacy implementations that do not understand any *non-critical* extension ignore it, while accepting and using legacy content. This enables an introduction of *hybrid* certificates, as shown in Fig. 2.(a), which contains a PK and an issuing CA's signature of both legacy ECDSA (PK_E, $CASig_E$) and PQC algorithms (PK_P, $CASig_P$). The resulting message format of Cooperative Awareness Message (CAM) [13] or Basic Safety Message (BSM) [26] is shown in Fig. 2.(b). This message contains signatures of both ECDSA ($MsgSig_E$) and

[2]Only the essential part of the ASN.1 definition is shown.

PQC ($MsgSig_P$), implying that the message format is also extended to carry the second signature. This type of *hybrid certificate* based on X.509 to address migration toward PQC algorithm has already been tested and verified to work for TLS, OCSP and other protocols [16], [27].

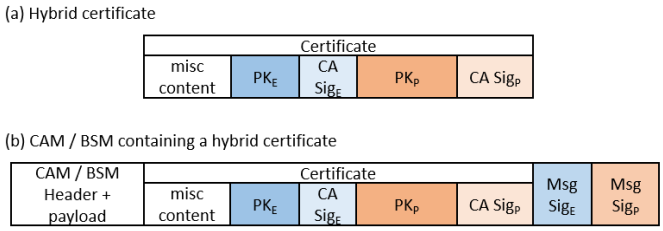

Fig. 2: Hybrid certificate and a message that contains it

B. Impacts on Pseudonym Certificates

In this section, we examine the impacts of the absence of an optional *extension* field in V2X certificates [12], [20] from the perspective of direct communication among vehicles using pseudonym certificates. It has two implications.

First, *legacy* vehicles will consider that *hybrid* certificates do not conform to the standardized format, and thus reject them. Moreover, these *legacy* vehicles most likely consider new *PQC-capable* vehicles as misbehaving due to constantly sending *malformed* certificates and messages. A plausible reaction by these vehicles is to report these *PQC-capable* vehicles to the Misbehaviour Authority (MA) for investigation. This means that the MA also needs to be able to treat these alleged *misbehaviour* reports as invalid and ignore such reports rather than accepting them. A possible outcome of erroneously judging as misbehaviour can result in the MA to revoke all certificates of all *PQC-capable* vehicles soon after they start using this new certificate type. In this case, these *PQC-capable* vehicles can no longer transmit V2X messages, resulting in a type of DDoS attack situation.

One possible approach is for *PQC-capable* vehicles to duplicate every message, one using the legacy ECDSA and another using the PQC algorithm to generate signatures. However, it does not solve the problem as *legacy* vehicles still consider messages containing PQC-compatible certificates as malformed, thus may consider these transmitting vehicles as misbehaving. In addition, this approach requires the PKI system to issue two sets of pseudonym certificates to every *PQC-capable* vehicle. It further implies that communication channel usage will grow even faster. Therefore, it is clearly a sub-optimal and unscalable solution.

Second, because *hybrid* certificates are significantly larger in size, their usage will decrease communication channel capacity. As the number of *PQC-capable* vehicles increases on the road, the proportions of these *PQC-compatible* messages increase in the communication channel, and the rate of increase in the channel usage is significantly higher than legacy messages due to their larger message size. Consequently, the channel capacity will saturate quicker, the number of legacy messages that can access the channel will decrease, resulting in a type of DDoS attack situation from *legacy* vehicles' perspective. Table I lists the PK and signature size of three PQC signature algorithms and their resulting CAM message sizes [13] using *hybrid* certificates discussed in Sec. III-A. The use of *hybrid* certificates will reduce the number of vehicles that can occupy the communication channel, effectively reducing the transmission range of V2X communication. The amount of reduction in the channel capacity is directly proportional to the PK and signature size increase in each PQC algorithm. As a simple comparison, if we consider the increase in CAM message size directly translates to the channel usage, then PHINCS+128f has the worst case where the message size increase by a factor of 95 times compared to the legacy ECDSA. The least impacting case is Falcon-512 with a factor of 7 times. From the perspective of communication channel capacity, Figure 3 illustrates the relationship between the proportion of certificate types (i.e. % of *PQC-capable* vehicles vs. *legacy* vehicles) and its impact on the channel capacity (i.e. the maximum number of vehicles before the channel is saturated) for various PQC signature algorithms.[3] This figure shows that the channel capacity decreases rapidly even with a relatively small proportion (∼10%) of *legacy* vehicles are replaced by *PQC-capable* vehicles. For example, even the least impacting algorithm (Falcon-512) will reduce the channel capacity to half when 30% of vehicles are PQC-capable. In effect, the transmission range will decrease by approximately 30% assuming the vehicle density is the same.

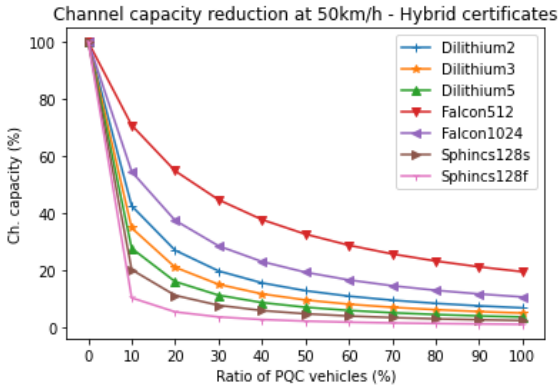

Fig. 3: Channel Capacity Reduction (hybrid certificates)

C. Mitigating Ineffective Channel Usage

Another approach to mitigate the increasing communication channel usage is to re-evaluate the existing mechanisms in the standards and eliminate functionalities that ineffectively uses the communication channel. One example is the resolution of unknown certificate digests, called Peer-to-Peer Certificate Distribution (P2PCD). The current standards [12], [20] specify that CAM and BSM messages are sent up to 10 times/sec. However, only one message in every second contains a full

[3]We calculated vehicle speed of 50, 70, 90, and 110 km/h each. However, we only show the 50 km/h case as an example as the results are similar.

TABLE I: Certificate and message size for the legacy and PQC algorithms

Algorithm	Security Level	|PK| (byte)	|Sig| (byte)	|Cert| (byte)	|Hybrid cert| (byte)	|CAM_f| (byte)	Ratio_f	|CAM_d| (byte)	Ratio_d
ECDSA	n/a	32	64	150	n/a	364	x1.00	222	x1.00
Dilithium2	2	1,312	2,420	3,786	3,882	6,516	x17.90	2,842	x12.80
Dilithium3	3	1,952	3,293	5,299	5,395	8,902	x24.46	3,795	x17.09
Dilithium5	5	2,592	4,594	7,240	7,336	12,144	x33.36	5,200	x23.42
Falcon-512	1	897	666	1,617	1,713	2,593	x7.12	972	x4.38
Falcon-1024	5	1,793	1,280	3,127	3,223	4,717	x12.96	1,666	x7.50
SPHINCS+128s	1	32	7,856	7,942	8,038	16,108	x44.25	8,499	x38.28
SPHINCS+128f	1	32	17,088	17,174	17,270	34,572	x94.98	18,224	x82.09

Note: CAM_f: CAM message with full certificate, CAM_d: CAM message with certificate digest.
Ratio_f: message length increase compared to ECDSA-based full certificate.
Ratio_d: message length increase compared to ECDSA-based certificate digest.

certificate, leaving the remaining messages to contain a certificate *digest*. A certificate *digest* is a compact representation of a certificate by taking the least significant 8 bytes of the hash output of the certificate (i.e. $digest \leftarrow LSB8(Hash(cert))$). The use of this *digest* effectively reduces the overall message size. On the other hand, its use implies that receiving vehicles may need to resolve a *digest* if this vehicle does not have the corresponding certificate. Such situation occurs when the first CAM or BSM message from a vehicle contains a *digest*. In this situation, P2PCD mechanism dynamically resolves the unknown certificate by querying vehicles within the communication range to send the missing certificate for a *digest*.

Despite its usefulness, its effectiveness is limited in certain scenarios, resulting in an ineffective use of communication channel. An analysis in [29] shows that a large majority ($\sim$89%) of pseudonym certificate digest resolution events of received CAM messages occur for vehicles moving in the opposite direction in highway scenarios. Dynamically resolving unknown digests for vehicles in the opposite direction has less benefit due to the short lifetime vehicles stay in each other's communication range. In such situation, it makes sense to withhold P2PCD mechanism by being aware of the situation the vehicle is in, e.g. a highway or a regular road, and determine if its usage is effective or not. Such decision helps mitigate the communication channel usage when its load is already high.

D. Impacts on RCA and ICA Certificates

We now shift our attention to the communication among CAs in the PKI system due to the absence of compatibility in *legacy* and *PQC-capable* certificates. Similar migration issue exists in the PKI system entities. RCAs, ICAs, and vehicles use certificates to verify their authenticity and deliver a public key to encrypt messages between them. ICAs include entities such as Enrolment Authority (EA), Authorization Authority (AA), and Misbehaviour Authority (MA) in ETSI architecture [11]. Without forward compatibility in the legacy certificates, migration toward PQC requires significantly tighter coordination among them. Because legacy entities do not recognize or accept *hybrid* certificates, all RCAs and ICAs need to be upgraded at the same time to a new implementation that can process it. In addition, all RCAs and ICAs first need to be upgraded so that pseudonym certificates to vehicles using the PQC algorithm can be generated and distributed to vehicles. In a large system where there are number of RCAs and ICAs exist, it becomes a significant challenge from the system administration perspective.

IV. Proposals

Based on the discussion in the previous sections, we propose that IEEE 1609 and ETSI C-ITS working groups to take the following actions.[4]

1) Revise IEEE 1609.2 [20] and ETSI TS 103 097 [12] by including a *non-critical extension* in the certificate definition. We believe this change requires an urgent attention so that legacy vehicle implementations will not reject future PQC-ready pseudonym certificates and report them as a misbehaviour. In addition, introduce a new clause in [20] and [12] to discuss a future need to extend the existing certificate definition by adding a PQC public key and issuing CA's signature.[5]
2) Revise BSM (SAE J2735 [26]), CAM (ETSI TS 302 637-2 [13]) and DENM (TS 302 637-3 [14]) specifications by introducing an extension field to their respective message formats for future extensibility, such as the inclusion of a message signature using a PQC algorithm.
3) Revise [20] and [12] by recommending not to use P2PCD and inlineP2PCD mechanisms when the usage level of communication channel is high. Such provision covers multiple situations: (1) reduce unnecessary overhead in the channel even in the legacy vehicles, and (2) migitate impacts when migration to PQC algorithm occurs by eliminating non-essential usage of the channel.
4) Investigate the usability of NIST competition round 4 candidates [1] from the real-time cyber-physical systems' perspective, such as V2X communication, specifically focusing on the impact of communication channel usage and OBU message processing, and define a path toward PQC migration.

[4]Some of these activities, such as investigating and evaluating solutions, may be conducted by other industry groups such as C2C-CC [6].

[5]Given that the NIST competition is still in progress, it is prudent to leave specifications of this new public key size unspecified in these standards.

5) When the NIST competition is finalized and the PQC algorithms are selected, make further updates to the relevant specifications such as [20] and [12] by reflecting the result of the investigation mentioned above.

V. Related Work

There are several literature on hybrid certificates in the context of migration toward PQC. Alnahawi et al. [2] present comprehensive coverage of PQC and their issues such as downgrade attack. Fan et al. [16] discuss their experiment of hybrid certificates on protocols such as TLS1.2, OCSP, CMP, and EST, and showed that most of the protocols and libraries worked with hybrid certificates using X.509 certificate with post-quantum extensions. Yunakovsky et al. [30] recommend using hybrid cryptographic schemes using current and post-quantum solutions for PKI against attacks using quantum computers. They also emphasize the importance of the concept of crypto-agility.

From the perspective of PQC impacts on V2X communication, Bindel and McCarthy [4] explain that they failed to construct implicit certificates from lattice-based algorithms (Dilithium and Falcon). Oliveira [24] also reached the same conclusion in his PhD thesis. This situation is significant given that explicit certificates will be the only choice with PQC algorithms. Bindel et al. [5] discuss an approach to split a certificate into multiple frames due to its larger PK size in PQC algorithm. This approach introduces a new vulnerability where a potential loss of any fragmented frame will render transmission of the large certificate void. In this sense, further improvement of this idea is needed. Dharminder et al. [8] proposes a new approach to introduce edge computing into V2X message verification by offloading this task to RSUs rather than receiving vehicles to do it themselves. This idea necessarily creates a dependency on the presence and availability of RSUs for vehicles' normal operation, thus limiting its practicality.

From the perspective of the hardware implementation of PQC algorithm, Ravi et al. [25] implemented Kyber for KEM and Dilithium for signature algorithm on an automotive-grade platform. They conclude that post-quantum cipher suites performance reduces by half of its existing counterparts due to the communication channel as the bottleneck. Fritzmann et al. [17] also implemented PQ algorithms on a vehicle platform and recommended that a specific HW product to be used as a PQC implementation due to its higher performance with an optimization. Gonzalez et al. [19] implemented NIST round-3 candicate algorithms on a hardware platform with 8 KB of RAM. Their work shows an interesting insight into the level of constraints PQC algorithms pose on limited hardware resources.

All of the work mentioned above does not address the certificate format and compatibility issue in the IEEE 1609.2 and ETSI C-ITS standards. We consider our paper is the first to identify this issue and proposed changes in these standards.

VI. Conclusion and Future Work

We have identified an issue in the existing certificate definition in V2X communication standards. Future migration to PQC algorithm will not be possible unless this issue is resolved in the standards. Otherwise, the introduction of PQC algorithm will create significant disruption in which both legacy and new PQC-capable vehicles potentially face unintentional DDoS attack situation. We propose IEEE 1609 and ETSI ITS standards to update the relevant specifications. Specifically, the *non-critical extension* should be introduced to the certificate definition at the earliest opportunity so that legacy vehicles will not erroneously report the use of PQC-capable pseudonym certificates as a misbehaviour. Further, implication of incompatible certificates among the CAs will cause operational issues when PQC algorithm is introduced in V2X communication.

Longer public key and signature in PQC signature algorithm will significantly reduce the channel capacity and hinder performance of the real-time cyber-physical systems such as V2X communication. In this sense, mitigation approaches of the use of PQC algorithms in real-time cyber-physical systems are an important open research question.

References

[1] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", IR 8413. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf, [Accessed: 19-Oct-2022].

[2] N. Alnahawi, A. Wiesmaier, T. Grasmeyer, J. Geißler, A. Zeier, P. Bauspieß and A. Heinemann, "On the State of Post-Quantum Cryptography Migration", INFORMATIK 2021, Gesellschaft für Informatik, Bonn, 2021

[3] D, Bernstein, T. Lange, "Post-quantum cryptography", Nature, vol. 549, no. 7671, pp. 188–194, Nature Publishing Group, 2017

[4] N. Bindel, S. McCarthy, "The Need for Being Explicit When Communicating". [Online]. Available: https://cryptomccarthy.com/wp-content/uploads/2022/01/CFAIL_final.pdf. [Accessed: 06-Sept-2022]

[5] N. Bindel, S. McCarthy, G. Twardokus, H. Rahbari, "Drive (Quantum) Safe!–Towards Post-Quantum Security for V2V Communications", Cryptology ePrint Archive, 2022

[6] Car 2 Car Communication Consortium (C2C-CC) TR2052, "Survey on ITS-G5 CAM Statistics", Dec. 2018

[7] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, "Report on Post-Quantum Cryptography", NIST IR 8105, 2016

[8] D. Dharminder, S. Kumari, U. Kumar, "Post quantum secure conditional privacy preserving authentication for edge based vehicular communication", Transactions on Emerging Telecommunications Technologies, vol. 32, no. 11, P. e4346, Wiley Online Library, 2021

[9] "Crystals Dilithium". [Online]. Available: https://pq-crystals.org/dilithium/. [Accessed: 06-Sept-2022].

[10] European Commission, "COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document, Commission Delegated Regulation, supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems", 2019

[11] European Telecommunication Standard Institute (ETSI), *TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*, Ver.2.1.1, July 2018.

[12] European Telecommunication Standard Institute (ETSI), *TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats*, Ver.2.1.1, Oct. 2021.

[13] European Telecommunication Standard Institute (ETSI), "EN 302637-2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," Ver.1.4.1, Apr. 2019.

[14] European Telecommunication Standard Institute (ETSI), "EN 302637-2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," Ver.1.3.1, Apr. 2019.

[15] "Falcon". [Online]. Available: https://falcon-sign.info/. [Accessed: 06-Sept-2022].

[16] J. Fan, F. Willems, J. Zahed, J. Gray, S. Mister, M. Ounsworth, C. Adams, "Impact of post-quantum hybrid certificates on PKI, common libraries, and protocols", International Journal of Security and Networks, vol. 16, no. 3, pp. 200–211, Inderscience Publishers (IEL), 2021

[17] T. Fritzmann, J. Vith, J. Sepúlveda, "Post-quantum key exchange mechanism for safety critical systems", Ruhr-Universität Bochum, 2019

[18] M. Gardiner, A. Truskovsky, G. Neville-Neil, A. Mashatan, "Quantum-safe trust for vehicles: The race is already on", Communications of the ACM, vol. 64, no. 9, pp. 54–61, ACM New York, NY, USA, 2021

[19] R. Gonzalez, A. Hülsing, M.J. Kannwischer, J. Krämer, T. Lange, M. Stöttinger, E. Waitz, T. Wiggers, B. Yang, "Verifying post-quantum signatures in 8 kb of RAM", International Conference on Post-Quantum Cryptography, pp. 215–233, Springer, 2021

[20] IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," IEEE Std 1609.2-2016, 2016

[21] ITU-T, "Recommendation ITU-T X.509, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks", 2019

[22] J. P. Mattsson, B. Smeets, E. Thormarker, "Quantum technology and its impact on security in mobile networks", Ericsson Technology Review, vol. 12, 2021

[23] M. Oguchi, M. Fuse, "Regional and longitudinal estimation of product lifespan distribution: a case study for automobiles and a simplified estimation method", Environmental Science & Technology, vol. 49, no. 3, pp. 1738–1743, ACS Publications, 2015

[24] J.E.R.F de Oliveira, "qSCMS: post-quantum security credential management system for vehicular communications", PhD thesis, Universidade de São Paulo, 2019

[25] P. Ravi, V.K. Sundar, A. Chattopadhyay, S. Bhasin, A. Easwaran, "Authentication protocol for secure automotive systems: Benchmarking post-quantum cryptography", 2020 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, pp. 1–5, 2020

[26] SAE International, *Surface Vehicle Standard, V2X Communications Message Set Dictionary*, SAE Int'l. J2735-2006

[27] D. Sikeridis, P. Kampanakis, M. Devetsikiotis, "Post-quantum authentication in TLS 1.3: a performance study", Cryptology ePrint Archive, 2020

[28] "SPHINCS+". [Online]. Available: https://sphincs.org/. [Accessed: 06-Sept-2022]

[29] T. Yoshizawa, B. Preneel, "On Handling of Certificate Digest in V2X Communication", International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2022

[30] S.E. Yunakovsky, M. Kot, N. Pozhar, D. Nabokov, M. Kudinov, A. Guglya, E.O. Kiktenko, E. Kolycheva, A. Borisov, A.K. Fedorov, "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era", EPJ Quantum Technology, vol. 8, no. 1, P. 14, Springer Berlin Heidelberg, 2021