PQWAVE-MHT: Post-Quantum secure WAVE protocol based on Merkle Hash Tree for secure V2X communication

Yoonsun Han[1], Youngbeom Kim[2], and Seogchung Seo[2]

[1]Department of Automotive Engineering, Kookmin University
rlagksdbs12@kookmin.ac.kr
[2*]Department of Financial Information Security, Kookmin University
{darania, scseo}@kookmin.ac.kr

Abstract

Autonomous cars now share information with the other systems outside of them in a V2X communication. V2X protocol, Wireless Access in Vehicular Environment(`WAVE`), authenticates parties based on Signatures using the ECDSA-P256(IEEE 1609.2 Standard). In this paper, we conduct research on applying Post Quantum Cryptography(PQC) to the `WAVE` to prevent security threats caused by the development of quantum computing systems. We proposed `PQC-WAVE` applying Merkle Hash Tree (`PQWAVE-MHT`) which is designed as a framework to reduce the computational load of signing and verification required to authenticate basic security messages (`BSMs`) transmitted in `WAVE` protocol in real-time. We integrated the proposed `PQWAVE-MHT` into the V2Verifier which is a well-known V2X simulator and measured the signing and verification performance. As a result, about 82% and 74% of performance improvement were achieved for signing and verification, respectively.

Keywords: V2X, Post-Quantum Cryptography, WAVE, IEEE 1609.2, Merkle Hash Tree, Digital Signature Algorithm

1 Introduction

Vehicular technology is evolving into connected cars that can communicate with other systems outside of the vehicle. In a Vehicle-to-Everything (V2X) network, a vehicle participates as a node. V2X is classified into Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), etc. depending on what the vehicles communicate with. According to the National Highway Traffic Safety Administration (NHTSA) [1], V2X technology is expected to improve overall traffic safety by preventing 439,000 $\sim$ 615,000 accidents and reducing damage by 987 people. Additionally, according to a report by the European Commission (EC) [2], V2X has advantages such as reduced travel time, improved efficiency, reduced accident rate, and reduced fuel consumption. Vehicles with full automation capability in a V2X communication transmit Basic Safety Message `(BSM)` in order to exchange traffic-related information such as their location information, speed, and emergency safety. Thus, V2X may be subject to malicious threats such as fake BSMs or Maliciously modified BSMs. To prevent these attacks, vehicles need to verify whether the received BSMs are correct and authenticated or not.

To ensure stable V2X communication, various organizations including IEEE and 3GPP have established standards of latency, message transmission reliability, and maximum packet size. To date, it has been decided that IEEE standards-based The Wireless Access in Vehicular Environment `WAVE` and 3GPP-based 5G-V2X will be studied concurrently, utilizing separate

channels(5.9 GHz frequency band [3]). In this paper, we conducted research based on the IEEE standard WAVE protocol, which provides more limited definitions of maximum packet size compared to 5G-V2X. (`WAVE`) protocol uses IEEE 1609.2 as an underlying security standard, which defines the authentication method `BSMs`. According to IEEE 1609.2, `BSMs` are Signed by ECDSA-P256 algorithm for authenticating them. In other words, a BSM additionally conveys digital signature and signer's public key or certificate. Upon receiving a `BSM`, the vehicle checks the authenticity of the message by verifying the certificate signature. This process verifies whether the `BSM` has been generated by the claimed sending party and the integrity of the message.

1.0.1 Motivation

The advancement in quantum computers poses a threat to the widely used Elliptic Curve Digital Signature Algorithm (ECDSA) in various application protocols, not just in V2X protocols. Due to the Shor algorithm [4], ECDSA can be broken in polynomial time. Consequently, the National Institute of Standards and Technology (NIST) initiated a competition on Post-Quantum Cryptography (PQC) and selected two lattice-based algorithms (Dilithium [5] and Falcon [6]) and one hash-based algorithm (SPHINCS+ [7]) for digital signature algorithms. Initially, research on PQC migration was actively conducted, starting with TLS/SSL and SSH [8, 9]. The necessity for research on V2X protocol migration is undeniable, and recently, a PQC benchmarking study in a V2X environment was undertaken in [10] As pointed out in [10], there are limitations to embedding both Dilithium and SPHINCS+ in the `WAVE` protocol based on the IEEE 1609.2 standard. In the V2V environment, where signatures must be generated at least every 100 ms, the signature generation process of Falcon is not suitable in terms of speed. Moreover, compared to the previously used Elliptic Curve-based ECDSA, PQC algorithms incur more computational overhead when generating and verifying digital signatures. On-Board Units (`OBUs`) in vehicles, which need to process operations in real-time, typically have more limited resources than general computers, underscoring the need for research to reduce computational overhead. Therefore, this study discusses a method to migrate `PQC-DSA` to fit the IEEE 1609.2 standard of the `WAVE` protocol and proposes an authentication framework to alleviate computational load in `OBUs`. The contributions of this paper can be summarized as follows:

1.0.2 Contribution

: In this paper, we overcome the limitations of PQC migration by proposing an authentication framework tailored for the V2V environment. Initially, to accelerate the signature generation/verification while adhering to the maximum packet size grounded in the IEEE 1609.2 standard, we introduce the Merkle Hash Tree (`MHT`). Furthermore, we bring forth the concept of weak authentication, authenticating with a hash function before proceeding to the PQC signature verification process. This negates the need for the signature generation process for every packet, while also streamlining the verification process. We consider various scenarios to assess the feasibility of implementing `MHT`. Taking into account packet transmission order in a broadcasting environment, `BSMs`, and the size of the `MHT` tree, we suggest an optimal framework fit `PQWAVE-MHT` for the V2V setting. Ultimately, we validate the efficiency of our framework by benchmarking the performance during Sign and Verify operations in V2Verifier which is a well-known V2X simulator. Within V2Verifier, for Falcon-512, `PQWAVE-MHT` demonstrates performance enhancements of 82% in `Sign` and 74 % in `Verify`. Likewise, for Falcon-1024, we observe improvements of 81 % and 73 % in `Sign` and `Verify`, respectively.

2 Preliminary

2.1 V2X standard

Various standards need to be considered when migrating `PQC-DSA` to the `WAVE` protocol. In particular, this study focuses on IEEE 802.11p, a 2016 amendment that standardizes vehicle communication systems, and IEEE 1609.2, which is a security standard for establishing application layers. Vehicles that utilize the `WAVE` protocol authenticate communication parties, including Roadside Units (`RSUs`), within their communication radius, using Certificate-based and Digital Signature methods, for the exchange of traffic data. Table 1 shows that the IEEE standard for the `WAVE` protocol offers a more restricted Quality of Service (`QoS`) compared to 3GPP. According to the standard, the `WAVE` protocol is required to transmit Secure Protocol Data Units (`SPDUs`) that concatenate headers, Basic Safety Messages (`BSMs`), and Signatures within 2000 bytes, with a delay ranging from 50 ms to 100 ms.

2.2 Migration to Post Quantum Cryptography

NIST has been overseeing the standardization work in PQC algorithms. In Round 4, held on June 3, 2022, NIST selected one scheme for Key Encapsulation Mechanism (Crystals-Kyber) and three schemes for Digital Signature Algorithms (Crystals-Dilithium, Falcon, and SPHINCS+). Table 2 shows the primitive, public key, and signature size of each algorithm. The Signature size of the PQC-`DSAs` at security level 1 is much longer than the 32 bytes Signature size defined in [11] for ECDSA-P256.

Table 1: QoS requirement for V2X communication

Protocol	WAVE	C-V2X	eC-V2X	5G-V2X
Processing Rate	3 ∼ 27 Mbps	10 ∼ 100 (Maximum 1000) Mbps		Maximum 2000 Mbps
Payload	2000 bytes	400 (Ad : 12,000) bytes		Pl : 6 Kbytes Ad : 12 Kbytes Au : 42 Kbytes
Maximum Communication Radius	1,000 m	320 m	1,000 m	Pl : 350 m Ad : 700 m Au : 1,000 m
Latency	100 ms		100 (Pl : 10) ms	Pl : 25 ms Ad : 100 ms Au : 5 ms
Vehicle Maximum Relative speed	200 km/h	280 km/h		500 km/h
Reliability	90 ∼ 95 %	80 ∼ 95 %	90 ∼ 100 %	

Pl : platooning driving, Ad : Advanced driving, Au : Autonomous driving

This paper primarily concentrates on evaluating the performance of Falcon at security level 1, 5 which meets the 2,000 bytes payload size standard required by the WAVE protocol. However, the IEEE, WAVE standard, should be expanded in preparation for PQC migration [12]. Additionally, it is evident from prior PQC migration research [10] that Dilithium's Signature generation and verification processes are faster than Falcon's. SPHINCS+ was not measured, but as shown in [13], Sign and Verify achieved noticeably slower performance compared to the other two PQC-DSAs. The WAVE protocol mandates real-time verification of signatures of parties within a 1km communication radius, according to IEEE standards. Additionally, vehicles should broadcast their traffic data, including signature, at intervals of up to 100 ms. This is a very important part of V2X communication, which processes data in milliseconds. Reducing communication and computing overhead will prevent accidents and improve road safety.

2.3 Performance Evaluation in the V2Verifier

We evaluate the performance of PQC-WAVE applying Merkle Hash Tree(PQWAVE-MHT) and compare it with the performance of simply porting PQC-DSA to the WAVE protocol. The performance is measured using the V2Verifier which is a well-known V2X simulator. Unfortunately, we were unable to use HW Universal Software Radio Peripheral(USRP), the original V2Verifier test equipment, in this research. V2Verifier can measure the time it takes to Sign and Verify signatures transmitted to and from a vehicle. WAVE protocol, which has a Signature-based authentication system, should repeatedly perform PQC operations (Sign and Verify) on BSMs generated in real-time in the vehicle. We experimented with the PQC-DSA algorithm Falcon,

Table 2: Parameters of PQC-DSA

Scheme (Primitive)	Dilithium (Module-LWE)			Falcon (NTRU)			SPHINCS+ (Hash function)		
parameters* (Security level)	*pk*	*sk*	*sig*	*pk*	*sk*	*sig*	*pk*	*sk*	*sig*
(1)	-	-	-	897	1,281	690	32	64	7,856
(2)	1,312	2,528	2,420	-	-	-	-	-	-
(3)	1,952	4,000	3,293	-	-	-	48	96	16,224
(5)	2,592	4,864	4,595	1,793	2,305	1,330	64	128	29,792

*The notation units for *pk*, *sk*, and *sig* are bytes

which complies with the maximum payload size specified in IEEE 1609.2 (2).

1330 bytes (signature of Falcon (security level 5)) < 2000 bytes(IEEE Standard) (2)

3 PQWAVE-MHT

3.1 Assumptions

In this paper, we propose `PQWAVE-MHT`, a `WAVE` protocol that migrates `PQC-DSA` by applying Merkle Hash Tree, accelerating the computational load during Sign and Verify. We measure the `Sign` and `Verify` performance using `PQWAVE-MHT` for V2V, a Peer-to-Peer link. To measure performance in V2Verifier, this experiment is based on several assumptions:

1. The local vehicles broadcast their public key to the `RSU` in the `WAVE` communication radius. As a result, we do not measure the performance of key generation and Certificate verification, assuming that the remote vehicle has already been received. Merkle Hash Tree-based authentication can also be applied for `RSU`, which can be shown [14].

2. This experiment solely focuses on comparing the performance between simple migration `PQC-WAVE` and Merkle Hash Tree-based. A comprehensive interpretation of the results is presented in Section 5.

3. `PQWAVE-MHT` incorporates a logic designed to address threat models, such as DoS attacks like seluge, using Merkle Hash trees [15], as it does not rely on hardware equipment like USRP.

4. The Notation used to describe the framework of `PQWAVE-MHT` are defined in Table 3.

Table 3: Notation and Description

Notation	Description
BSM	Basic Safety Message
DSA	Digital Signature Algorithm
MHT	Merkle Hash Tree
MHV	Missing Hash Values of MHT
OBU	On-Board-Unit
RSU	Roadside-Unit
SPDU	Secure Protocol Data Unit
WAVE	Wireless Access in Vehicular Environment
ID-H	PSID||MHT Internal Index Number of the packt$\|\|h_r$
Sign	signature generation process of Falcon
Verify	Falcon verifying algorithm
PQWAVE-MHT	PQC migrated WAVE protocol using Merkle Hash Tree
QoS	Quality of Service
pk_{remote}, sk_{remote}	Public and Private keys of remote car
pk_{local}, sk_{local}	Public and Private keys of local car
$Sign(BSM_i, sk)$	Generate BSM_i's signature using sk
$Verify(BSM_i, pk)$	Verify BSM_i's signature using pk
H(m)	for m, generating digest using SHA-256 hash function
h_i	$H(BSM_i)$
h_k	$k = nm, H(H(BSM_n)\|\|H(BSM_m))$
h_r	Root hash packet in MHT

3.2 Authentication Framework using Merkle hash tree

PQWAVE-MHT which is migrated to Falcon, a PQC-DSA that complies with 2000 bytes defined in the WAVE protocol standard IEEE 1609.2. Digital Signatures using Falcon impose a real-time computational overhead in V2V communication and are slower processes compared to other DSAs, including ECDSA [10]. The PQWAVE-MHT proposed here utilizes the Merkle Hash Tree structure in Sign and Verify operations to alleviate the computational overhead that could otherwise burden a wireless network with more cost-effective operations.

Fig. 1 shows a local OBU using Merkle Hash Tree before transmitting the SPDU generated during driving. The vehicle on the left generates a Signature using only DSA, and the vehicle on the right generates a Signature using Merkle Hash Tree. The structure of MHV is $h_j||h_k||h_r||Signature$ as shown in Fig. 1 and its size is 96 bytes excluding the Signature. The logic for MHV generation and Verify is explained alongside [Algorithm 1], which will be introduced below. PQWAVE-MHT was performed using 4 BSMs as the most basic Tree configuration. When using HW equipment such as USRP, Tree configuration can be optimized to comply with the latency standards of IEEE 802.11p. Finally, the BSMs to which the MHV is concatenated are broadcast to parties within communication radius. PQWAVE-MHT replaces the 4 Signature operations for the existing 4 BSMs with 1 Signature operation and SHA-256 operation. The computational load of Falcon, the migration target PQC-DSA, is as follows (1).

$$4 \text{ Falcon} -> 1 \text{ Falcon} + 7 \text{ SHA-256}. \quad (1)$$

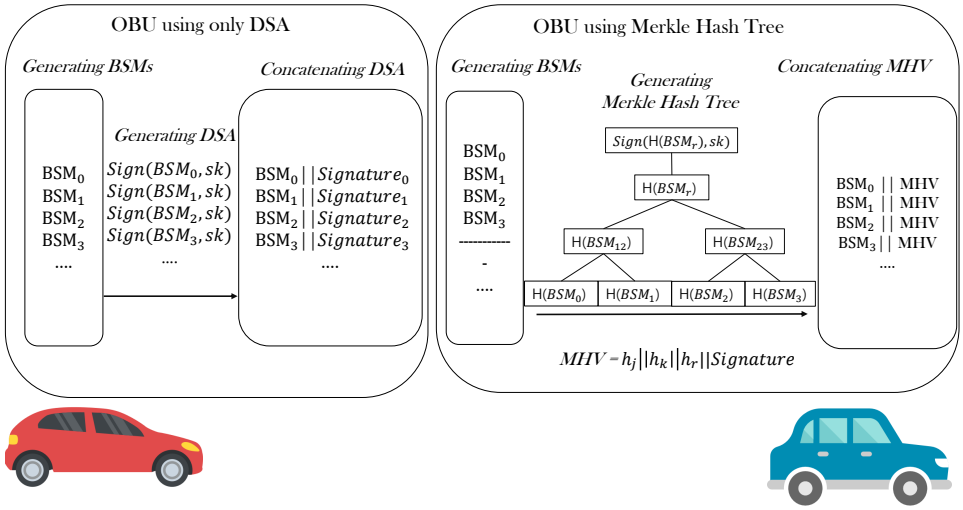

Figure 1: Comparison of signature generation between the original case and our proposal using Merkle Hash Tree

The V2Verifier measures the Latency at which local vehicles `Sign` and `verify` signatures according to [Algorithm 1]. `PQWAVE-MHT` filters and verifies vehicles within the `WAVE` protocol radius based on PSID. `PQWAVE-MHT` prevents computational overhead and communication failures by replacing PSID and Falcon with SHA-256, a more cost-effective operation. The FrameWork, which measures performance on a simulator, focuses on computational speed when `Sign` and `Verify` Signatures without taking into account noise or external attacks. `SPDU` is broadcast in the form of `MHV` concatenated with `BSM`, incorporating timestamp and PSID log to respond to replay attacks, and uses weak authentication prior to Falcon operation. || means for Concatenate, H(x) is SHA-256 operation on x, and $Sign(x, sk)$ is the operation that `Signs` for x using the private key sk.

Algorithm 1 Authentication of 4 BSMs from V_A to V_B based on PQWAVE-MHT.

Sender A do:
1: configures each BSM_i, ($i \in [0,3]$) and generates $h_i \leftarrow \mathsf{H}(\text{BSM}_i)$
2: generates $sig \leftarrow \mathsf{Sign}(h_r, sk_{\mathbf{A}})$, where $h_r \leftarrow \mathsf{H}(\mathsf{H}(h_0||h_1)||\mathsf{H}(h_2||h_3))$
3: combines MHV with BSM
▷ MHV : $h_j||h_k||h_r$, k=nm, and $h_k \leftarrow \mathbf{H}(h_n||h_m)$
▷ broadcasting and **B** received

Receiver B do:
4: checks timestamp of $SPDU$ ▷ prevant replay attacks
5: **if** invalid timestamp **then**
6: **return** fail
7: **else**
8: retrieves PSID in logged ID-H ▷ weak authentication
9: **if** ID-H is not stored **then**
10: $t \leftarrow \mathsf{H}(\mathsf{H}(\mathsf{H}(\text{BSM}_i)||h_j)||h_k)$ ▷ if $i \leq 1, j \in \{0,1\}\backslash\{i\}$ and $k = 23$
11: **if** $t \neq h_r$ **then** ▷ if $i \geq 2, j \in \{2,3\}\backslash\{i\}$ and $k = 01$
12: **return** fail
13: **else**
14: $flag \leftarrow \mathsf{Verify}(sig, pk_{\mathbf{A}})$ ▷ verify signature
15: **if** $flag \neq$ success **then**
16: **return** fail
17: BSM_i : authenticated
18: stores BSM_i to ID-H
▷ ID-H : PSID||MHT internal Index Number of packet|| h_r
19: $t \leftarrow \mathsf{H}(\mathsf{H}(\mathsf{H}(\text{BSM}_i)||h_j)||h_k)$
20: **if** $t \neq h_r$ **then**
21: **return** fail
22: **else**
23: BSM_i : authenticated
24: **return** Success

As demonstrated in `Sender A do:` line 3, the advantage of Merkle Hash Tree is that faster `Verify` is possible if there is a specific value required in the Tree structure. In the `MHT` structure, only 2 source parameters and 3 SHA-256 operations are required to create the Root Hash value, which is a parameter for creating a Signature using Falcon operation without transmitting all values. Line 10 of `Receiver B do` represents a key operation within `PQWAVE-MHT`. BSM_i refers to the `BSM` subject to verification, and h_j and h_k are values required for `Verify` in the Merkle Hash Tree structure. For example, if i is 0, BSM_0 is hashing(H()) and H(BSM_0) is concatenated with H_j, which is the H(BSM_1) received through `MHV`. Afterward, h_{01} is concatenated with h_{23} which is H(H(h_2)||H(h_3)) received from `MHV`. Finally, we obtain h_r, which is the input value of Falcon-based `Sign` and the value used for `MHT Verify`.

In the overall authentication framework, `PQWAVE-MHT` verifies whether the first received `BSM` has previously completed a valid Falcon-based verification. If there is an **ID-H** logged with that PSID and value, the h_r value is compared to complete the verification.

4 Analysis

Fig. 2 shows the Latency of `Sign` and `Verify` for two versions of the `WAVE` protocol with a migration of PQC. The protocol framework is `PQC-WAVE`, which only performs simple migration, and `PQWAVE-MHT`, which applies Merkle Hash Tree to the `PQC-WAVE` protocol. The platform used for simulating V2Verifier is Intel(R) Core(TM) i7-8700 CPU 3.20GHz, 16GB of RAM, and Linux operating system 5.15.0-84-generic Kernel. Latency is calculated as the average of 400 measurements for each framework.

Figure 2: PQWAVE-MHT and Basic PQC-WAVE Latency comparison

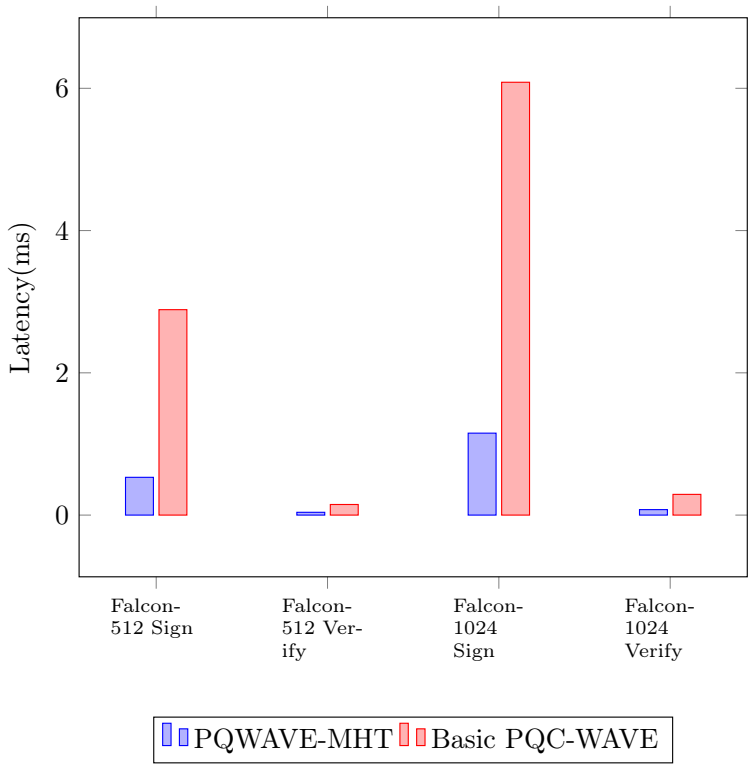

Table 4: PQWAVE-MHT and Basic PQC-WAVE performance measurements

	Falcon-512		Falcon-1024	
	Sign	Verify	Sign	Verify
PQWAVE-MHT	0.53	0.039	0.15	0.077
Basic PQC-WAVE	2.89	0.077	6.09	0.29
Acceleration Rate	82%	74%	81%	73%

Table 4 shows detailed performance. On Falcon-512, `PQWAVE-MHT` shows a performance improvement of 82% in `Sign` and 74% in `Verify`. Similarly, for Falcon-1024, there are 81% and 73% performance improvements in `Sign` and `Verify`. These experimental results show that using `PQWAVE-MHT` enables PQC migration while reducing computational overhead, enabling reliable communication. The performance improvements for a single `BSM` imply that more information can be shared with reduced communication delays in V2X.

We implement `PQWAVE-MHT` using Falcon, compling with the maximum packet size specified in the IEEE 802.11p standard and achieves a maximum latency of 100ms through accelerated operations. To use HW USRP, the Merkle Hash Tree was configured with the most basic structure, and `PQWAVE-MHT`, composed of 4 `BSMs`, replaced 4 Falcon operations with 1 Falcon and 7 SHA-256 operations as shown in Equation (1). When conducting experiments with USRP, we can design an optimized Merkle Hash Tree structure that takes latency and processing speed into account. As a result, `PQWAVE-MHT` shows high computational acceleration in `Sign` and `Verify`. The computational overhead in embedded `OBUs`, where real-time performance is crucial, can help ensure the stability of V2X communication.

5 Discussion and Conclusion

In this paper, we present the design, and implementation of `PQWAVE-MHT`. IEEE standard-based `WAVE` can only migrate to Falcon among `PQC-DSA`, and the computational overhead in `OBU` is effectively reduced by using Merkle Hash Tree. Ultimately, we succeeded in accelerating performance by 82% for `Sign` and 74% for `Verify`, and completed PQC migration. `PQWAVE-MHT` can be expanded to formal verification using Tamarin-prover and research on actual communication using HW such as USRP. In actual communications, `PQWAVE-MHT` takes into account various factors, including the reliability and noise of communication packets. Vehicles communicating in a V2X environment using HW radio devices must `Verify` the Signatures of vehicles within their radius in real-time. Furthermore, technology to handle this without packet confusion, using techniques like multi-processing, may be necessary. `PQWAVE-MHT` can also establish time boundaries that take into account packet dropping and replay attacks comprehensively.

`PQWAVE-MHT` is a cryptographic protocol and its secrecy can be verified using formal verification such as tamarin-prover. Security protocol analysis tool, tamarin-prover is being widely researched [16, 17]. Additionally, attacks such as DoS are a challenge to overcome in wireless network environments. `PQWAVE-MHT` uses a logical framework to resist replay attacks. By reducing the Falcon operation and replacing it with SHA-256 operation, weak authentication that resists DoS can be used, but DoS can be responded to with the cheaper operation introduced in Seluge [15]. Wireless network security against these malicious attacks must be evaluated by designing a real test-bed.

5.0.1 Acknowledge

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) ((No. 2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security, 50%) and Korea Evaluation Institute of Industrial Technology(KEIT) grant funded by the Korea government and partly supported by The National Research Foundataion of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1C1C1013368, 50%).

References

[1] NHTSA. 2016. Preliminary regulatory impact analysis, fmvss no. 150 vehicle-to-vehicle communication technology for light vehicless.

[2] Nick Asselin-Miller, Marius Biedka, Gena Gibson, Felix Kirsch, Nikolas Hill, Ben White, and Kotub Uddin. Study on the deployment of c-its in europe: Final report, Report for DG MOVE MOVE/C 3 (2016), 2014–794.

[3] IEEE Standards Association. 802.11 p-2010-ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. *URL http://standards. ieee. org/findstds/standard/802.11 p-2010. html*, 2010.

[4] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[5] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS–Dilithium. Submission to the NIST Post-Quantum Cryptography Standardization Project [18], 2020. https://pq-crystals.org/dilithium/.

[6] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon. Submission to the NIST Post-Quantum Cryptography Standardization Project [18], 2020. https://falcon-sign.info/.

[7] Andreas Hulsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS$^+$. Submission to the NIST Post-Quantum Cryptography Standardization Project [18], 2020. https://sphincs.org/.

[8] Maximilian Schöffel, Frederik Lauer, Carl C Rheinländer, and Norbert Wehn. On the energy costs of post-quantum kems in tls-based low-power secure iot. In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, pages 158–168, 2021.

[9] Manohar Raavi, Simeon Wuthier, Pranav Chandramouli, Xiaobo Zhou, and Sang-Yoon Chang. Quic protocol with post-quantum authentication. In *Information Security: 25th International Conference, ISC 2022, Bali, Indonesia, December 18–22, 2022, Proceedings*, page 84–91, Berlin, Heidelberg, 2022. Springer-Verlag.

[10] Nina Bindel. Suitability of 3rd round signature candidates for vehicle-to-vehicle communication, June 07, 2021. available online: https://csrc.nist.gov/Presentations/2021/suitability-of-3rd-round-signature-candidates-for.

[11] 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.

[12] Takahito Yoshizawa and Bart Preneel. Post-quantum impacts on v2x certificates–already at the end of the road. In *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, pages 1–6. IEEE, 2023.

[13] Open Quantum Safe. 2021. Oqs algorithm performance visualizations, June 07, 2021. https://openquantumsafe.org/benchmarking/.

[14] Shafika Showkat Moni and D Manivannan. An efficient rsu authentication scheme based on merkle hash tree for vanets. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2020.

[15] Sangwon Hyun, Peng Ning, An Liu, and Wenliang Du. Seluge: Secure and dos-resistant code dissemination in wireless sensor networks. In *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, pages 445–456. IEEE, 2008.

[16] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, and Thyla van der Merwe. A comprehensive symbolic analysis of tls 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1773–1788, 2017.

[17] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 1383–1396, 2018.

[18] NIST, the US National Institute of Standards and Technology. Post-quantum cryptography standardization project. https://csrc.nist.gov/Projects/post-quantum-cryptography.