Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication –Extended Abstract

Nina Bindel[1], Sarah McCarthy[1], Hanif Rahbari[2], and Geoff Twardokus[2]

[1] University of Waterloo and Institute for Quantum Computing,
{nina.bindel,sarah.mccarthy}@uwaterloo.ca
[2] Rochester Institute of Technology, rahbari@mail.rit.edu, gdt5762@rit.edu

Direct wireless communication between vehicles could prevent up to 600,000 non-alcohol-related vehicle crashes in the U.S. every year [3]. The core of the two main vehicle communication protocols, namely Dedicated Short Range Communication/Wireless Access in Vehicular Environments based on IEEE 802.11p [6] and Cellular Vehicle-to-Everything [5], consists of sending so-called Basic-Safety-Messages (BSMs). In these messages, information about the status of the car such as its location, direction, speed, status of the brake and acceleration system and time is collected and broadcast once every 100 ms. Based on this information, other cars can compute the sender car's path and react, e.g. brake or accelerate, accordingly to ensure the safety of traffic participants.

To protect vehicle-to-vehicle (V2V) communication against malicious use, the IEEE 1609.2 [1, 2] standard specifies *secure* wireless vehicle communication. In particular, it describes the secure transmission of authenticated data, certificate management and the cryptographic operations involved. Since all cryptographic building blocks used in the standard are based on elliptic curve cryptography, they are not quantum-safe. It is an open question whether and how they can be replaced by quantum-safe alternatives.

In our presentation we will first explain the basics about secure V2V communication to enable a discussion about the suitability of the finalists of NIST's post-quantum standardization in IEEE 1609.2.

We identified two potential challenges involving packet size and verification time. Firstly, the BSM packets consist of the collected data for the BSM, a signature over the BSM, and a certificate for the corresponding public key that is used to verify the signature. The combined signature and public key size of all three finalists is larger than the corresponding ECDSA size. Will the larger sizes lead to packet loss or issues in jammed intersections? Secondly, it is important to analyze how many signatures can be sent and verified per second. Is this number sufficient or even higher compared to the current IEEE 1609.2 instantiation using ECDSA? We will answer all these questions during our talk.

To enable this discussion, we extended the hardware testbed *V2Verifier* [7], an open-source wireless testbed for secure V2V communication based on IEEE 1609.2, to use Dilithium, Falcon or Rainbow instead of ECDSA. Our extension makes use of the open-source crypto library *liboqs* [4] which consists of reference implementations of the NIST finalists. Using the post-quantum adaptation of

V2Verifier, we are planning on testing different scenarios, ranging from static senders and receivers in a lab environment to moving sending and receiving cars without visual contact.

We already provide the benchmarks for the scenario when the sender and receiver are static in our slides included in this submission. Interestingly, we can already observe that while Dilithium-II seems to be a very good candidate regarding runtime (verification is faster than ECDSA verification), unfortunately the signature is larger than the allowed maximum BSM size in the IEEE 802.11p standard.

Upon acceptance, we will provide results for all considered scenarios. Moreover, based on our findings, we will present the results of our analysis regarding the effect of traffic density on each signing algorithm. For example it might turn out that only Falcon can be used in high density situations, such as congested intersections, if our implementations follows the V2V standard specifications.

While our presentation discusses the suitability of the signature finalists mostly from a performance point of view, we will also highlight limitations regarding functionality. For example, the certificate management described in IEEE 1609.2 relies heavily on implicit certs to save space. To our knowledge, it is unclear how to construct implicit certs over anything else than elliptic curves. Hence, using quantum-safe *explicit* certs means to increase sizes not only to add quantum security but also because explicit certs are larger than implicit certs.

We hope that our analysis and presentation will stimulate further research on this topic. For example, depending on our results an important next step might be to optimize the reference implementations to the platforms used in vehicles. Given the lifespan of vehicles, it is necessary to discuss the suitability of post-quantum signature schemes and find solutions in cooperation with the V2V community as soon as possible to enable secure vehicle communication in the future.

References

1. IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages (2016)
2. IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Certificate Management Interfaces for End Entities (2020)
3. Administration, N.H.T.S.: V2v communications factsheet. U.S. Department of Transportation, Tech. Rep. (2014), accessed: Jan. 9, 2021
4. Allen, N., Anvari, M., Crockett, E., Drucker, N., Gheorghiu, V., Gueron, S., Paquin, C., Lepoint, T., Mishra, S., Stebila, D.: liboqs – nist-branch: C library for quantum-resistant cryptographic algorithms (2018), gitHub at `https://github.com/open-quantum-safe/liboqs`
5. 3rd Generation Partnership Project, E.: TR 121 914 V14.0.0. Tech. rep. (2018)
6. Society, I.C.: IEEE Std. 802.11p-2010. Tech. rep. (2010)
7. Twardokus, G., Rahbari, H.: Evaluating V2V Security on an SDR Testbed. CNERT 2021-IEEE INFOCOM Workshop on Computer and Networking Experimental Research using Testbeds (2021)