# Desafios e oportunidades de pesquisa na adoção de criptografia pós-quântica em redes veiculares

**Caio Teixeira**[1], **Marco Aurélio Amaral Henriques**[1]

[1]Departamento de Engenharia de Computação e Automação (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (UNICAMP) – Campinas, SP – Brazil

***Resumo.*** *Redes veiculares viabilizam diversas aplicações importantes, como direção autônoma e prevenção de acidentes de tráfego, as quais exigem um alto nível de segurança nas comunicações. No entanto, para se comunicarem de forma protegida, essas redes se apoiam em algoritmos criptográficos vulneráveis a ataques dos futuros computadores quânticos, o que exige a adoção de alternativas mais seguras. Entretanto, os algoritmos de criptografia pós-quântica já padronizados têm se mostrado incompatíveis com as rigorosas exigências de latência impostas por tais redes, dificultando sua adoção. Nesse trabalho, identificamos alguns dos principais desafios em aberto na área, a partir da análise de padrões estabelecidos e trabalhos recentes, e apresentamos oportunidades de pesquisa para a superação dos mesmos.*

***Abstract.*** *Vehicular networks enable various important applications, such as autonomous driving and traffic accident prevention, which demand a high level of communication security. However, to communicate securely, these networks rely on cryptographic algorithms vulnerable to attacks from future quantum computers, necessitating the adoption of more secure alternatives. Nonetheless, the standardized post-quantum cryptography algorithms have proven incompatible with the stringent latency requirements imposed by such networks, making their adoption challenging. In this work, we identify some of the primary open challenges in the field, based on the analysis of established standards and recent research, and present research opportunities to overcome them.*

## 1. Introdução

A conectividade de veículos é uma tendência emergente, viabilizando uma série de aplicações que vão desde auxílios a motoristas para prevenção de acidentes, até a capacidade de direção autônoma. Há diversos tipos de comunicação definidas para esse cenário: comunicações veículo-a-veículo, veículo-a-infraestrutura, veículo-a-pedestres, veículo-a-rede e outros, formando as denominadas *comunicações veículo-a-tudo* (V2X).

O padrão IEEE 802.11p [Jiang and Delgrossi 2008] define a comunicação *Dedicated Short-Range Communication* (DSRC) para as camadas física e de acesso ao meio. Para as camadas superiores, duas abordagens diferentes despontam: nos EUA, foi adotado o padrão IEEE 1609 [IEEE 2019] (WAVE – *Wireless Acess in Vehicular Environments*), enquanto na Europa, foram adotadas as especificações do ETSI (*European Telecommunications Standards Institute*), sendo elas ETSI *Intelligent Transport Systems G5* e *Collaborative ITS* (C-ITS) [Yoshizawa and Preneel 2019]. Com o advento das redes 4G e 5G, o Projeto de Parceria de Terceira Geração (3GPP) também definiu novas interfaces de rádio

para essas mesmas aplicações, buscando superar diversos desafios do DSRC e expandir as capacidades de comunicação veicular. Essas interfaces são LTE-V2X [3GPP 2016] e 5G-V2X [3GPP 2020], denominadas em conjunto como *Cellular V2X* (C-V2X).

Cada um desses padrões e especificações define infraestruturas e protocolos diferentes, mas há diversas semelhanças. Um dos pontos centrais para a execução de aplicações, especialmente quando consideramos o cenário autônomo, é a emissão frequente de mensagens de coordenação que informam dados como posição, velocidade, trajetória, estado de freio, entre outros. No padrão IEEE, essas mensagens são denominadas *Basic Safety Messages* (BSM), enquanto na especificação ETSI, são denominadas *Cooperative Awareness Messages* (CAM). Estas mensagens devem assinadas, garantindo sua autenticidade e evitando injeção maliciosa de informações, e as chaves usadas para essas assinaturas devem ser publicadas através de certificados digitais.

Os processos de certificação e a correspondente infraestrutura de chaves públicas são definidos pelas normas IEEE 1609.2 [IEEE 2016] e 1609.2.1 [IEEE 2022] (SCMS – *Security Credential Management System*), para o WAVE, e ETSI TS 102 940 [ETSI 2021] (C-ITS *Security Management*), para o C-ITS. Em ambos, as assinaturas e certificados utilizam o algoritmo de criptografia baseada em curvas elípticas ECDSA (*Elliptic Curve Digital Signature Algorithm*). Além de ter assinaturas e certificados compactos, a propriedade de homomorfismo sobre adição de pontos em curvas elípticas possibilita a emissão de dezenas de certificados a partir de uma única chave inicial, a partir da estratégia denominada *Butterfly Key Expansion (BKE)* [Brecht et al. 2018]. Essa propriedade satisfaz um dos requisitos de privacidade em redes veiculares, que é o de possibilitar identidades rotativas, de forma a dificultar o rastreio de veículos, mesmo em longas janelas de tempo.

No entanto, a criptografia baseada em curvas elípticas está ameaçada pelo algoritmo de Shor [Shor 1994], que é capaz de resolver seu problema matemático subjacente em tempo polinomial em um computador quântico que tenha *qubits* suficientes para executá-lo. Para enfrentar essa ameaça, estão sendo propostos pela academia e pela indústria novos esquemas denominados algoritmos pós-quânticos, que são baseados em problemas para os quais não se espera que um computador quântico tenha vantagem em resolver. Alguns algoritmos pós-quânticos já foram padronizados pelo órgão de padronização americano NIST [Alagic 2022], três deles para assinatura digital e um para prover acordo de chaves criptográficas simétricas. O mesmo concurso que estabeleceu esses padrões ainda está em vigência, agora em sua quarta rodada, avaliando candidatos remanescentes de acordos de chaves, bem como foi aberta uma chamada específica para novos algoritmos de assinatura pós-quânticos [NIST 2023], visando estabelecer novos padrões de assinatura que não sejam baseados em reticulados. No entanto, comparados ao ECDSA, o custo de comunicação dos esquemas pós-quânticos é muito maior [Alagic 2022], representando assim um grande desafio para sua adoção em redes veiculares.

Neste artigo, são detalhados alguns dos principais desafios na transição de protocolos de comunicação veicular para criptografia pós-quântica, bem como são apontadas e discutidas algumas oportunidades de pesquisa na área.

## 2. Desafios decorrentes da adoção de criptografia pós-quântica

Um dos principais desafios de redes veiculares é a saturação de banda, especialmente em ambientes com alta densidade de dispositivos. O intervalo entre mensagens de

coordenação é de 50 a 100ms e, portanto, a construção da mensagem, sua assinatura e o envio de ambas devem acontecer bem abaixo dos limites desse intervalo, pois ainda será necessária a validação da assinatura pelo(s) receptor(es). Apesar do desafio da velocidade de processamento das assinaturas ser importante nesse cenário, esse trabalho tem como foco os desafios de transmissão, que impactam a latência do protocolo devido ao tempo de envio e potencial de perda das mensagens caso o canal seja sobrecarregado.

Além desse desafio, o tamanho das mensagens de coordenação é variável e ambos os padrões especificam campos opcionais que podem ser omitidos para diminuir o tamanho do pacote transmitido. Enquanto CAMs variam de 200 a 800 bytes [C2C-CC 2018], incluindo assinaturas e certificados, BSMs variam de 122 a 481 bytes [Cominetti et al. 2023]. Em ambos os casos, as assinaturas ocupam 64 bytes, enquanto os certificados, que se enquadram como campos opcionais, ocupam 117 bytes.

No entanto, ao olhar para os novos padrões de criptografia pós-quântica, o cenário é bem desafiador. Na Tabela 1, são relatados os tamanhos de chave pública (uma parte dos certificados) e de assinatura do algoritmo usado atualmente (ECDSA), de cada um dos três algoritmos de assinatura padronizados pelo NIST (FALCON e CRYSTALS-Dilithium, baseados em reticulados, e SPHINCS+, baseado em funções de *hash*) [Alagic 2022] e de dois outros algoritmos com segurança pós-quântica (LMS[1] e XMSS[2], também baseados em funções de *hash*), padronizados pela IETF (Internet Engineering Task Force).

| **Algoritmo** | **Chave Pública** | **Assinatura** | **Certificado** |
|---|---|---|---|
| ECDSA | 32 | 64 | 96+$\epsilon$ |
| FALCON | 897 | 666 | 1563+$\epsilon$ |
| CRYSTALS-Dilithium | 1312 | 2420 | 3732+$\epsilon$ |
| SPHINCS+ | 64 | 17088 | 17152+$\epsilon$ |
| LMS | 56 | 2508 | 2564+$\epsilon$ |
| XMSS | 64 | 2500 | 2564+$\epsilon$ |

**Tabela 1. Tamanhos em bytes de chave pública e assinatura para os principais algoritmos de assinatura digital, em seu menor nível de segurança. O parâmetro $\epsilon$ representa o tamanho dos metadados dos certificados.**

Esse maior volume de dados dos algoritmos pós-quânticos vai contra os requisitos de comunicação de redes veiculares por exigirem tempos maiores de transmissão e recepção, podendo saturar os canais. Além disso, ele viola os limites de espaço previstos nos pacotes dos protocolos DSRC e C-V2X. Em DSRC, o tamanho máximo de um *frame* é de 2304 bytes; já no C-V2X, o tamanho limite em um canal padrão de 10MHz é de apenas 437 bytes [Twardokus et al. 2024]. Isso torna impraticável o envio de assinaturas e certificados que utilizam tais algoritmos de forma direta sem alterações no protocolo.

Outro desafio é a distribuição de certificados de pseudônimos, apoiada no esquema *Butterfly Key Expansion* [Brecht et al. 2018]. Esse esquema possibilita a criação, com baixo custo, de certificados de curta validade (em geral, uma semana) que correspondem ao veículo e que podem ser rotacionados durante o trajeto para mitigar ataques de rastreamento. Em um esquema de certificação comum, o veículo seria responsável por gerar um

[1] `https://www.rfc-editor.org/rfc/rfc8554.html`
[2] `https://www.rfc-editor.org/rfc/rfc8391.html`

par de chaves para cada pseudônimo, e enviá-los um a um para certificação. No entanto, o esquema BKE permite que o veículo envie apenas um par de chaves e receba um número arbitrário de certificados como resposta, podendo então calcular as chaves privadas correspondentes a cada um de forma segura, diminuindo assim o custo de processamento e de comunicação das requisições. O que possibilita que novas chaves sejam derivadas no esquema é uma propriedade da criptografia baseada em curvas elípticas chamada *homomorfismo sobre adição*; ou seja, se somamos duas chaves públicas, a chave privada correspondente à chave pública resultante será a soma das respectivas chaves privadas.

Sejam $G$ o ponto gerador do grupo sobre a curva, $k$ a chave privada (um inteiro não-nulo menor do que a ordem da curva) gerada aleatoriamente pelo veículo, $K = k \cdot G$ a chave pública correspondente e $n$ o número de certificados a serem emitidos. Ao receber $K$, a partir de uma função pública predefinida no esquema $f(i)$ ($0 \leq i < n$), são derivadas novas chaves $K'_i$ (que serão correspondentes aos pseudônimos) na infraestrutura, calculando $K'_i = K + f(i) \cdot G$. Os certificados são então gerados para o conjunto de chaves $K'_i$ e o veículo, ao receber os certificados e tendo conhecimento de $f(i)$, pode calcular as chaves privadas correspondentes pela soma $k'_i = k + f(i)$. No entanto, como pode ser visto no padrão NIST, nenhum dos algoritmos pós-quânticos padronizados tem um problema subjacente que apresente homomorfismo sobre adição, impossibilitando o uso dessa técnica. Logo, torna-se necessário adotar um algoritmo pós-quântico que tenha essa propriedade (como algoritmos especializados para encriptação homomórfica), ou adotar uma outra estratégia de provisionamento de certificados que se adeque à infraestrutura de cada padrão, com eficiência e baixo custo de comunicação.

Há também o desafio da vida útil de veículos e da compatibilidade entre aqueles que usam protocolos atuais e os que usam protocolos pós-quânticos. Veículos em geral são bens de alta durabilidade, podendo operar e receber suporte por décadas após sua fabricação [Yoshizawa and Preneel 2023]. Sendo assim, quando um computador quântico capaz de executar o algoritmo de Shor surgir, há uma alta probabilidade de que ainda haverá necessidade de uso de protocolos vulneráveis a ataques quânticos, o que pode levar a, por exemplo, ataques de *downgrade*, forçando dispositivos com resistência quântica a se comunicarem por um canal vulnerável ou aceitarem credenciais inválidas.

É possível constatar, portanto, que a necessidade de adoção de criptografia pós-quântica em redes veiculares traz desafios significativos. São necessárias a redução do volume de dados trafegados para evitar congestionamento da rede e a adaptação da infraestrutura de derivação de chaves para o cenário pós-quântico, os quais exigem um grande esforço de engenharia para serem vencidos.

## 3. Trabalhos relacionados

Os desafios levantados já têm sido explorados na literatura, mas ainda sem soluções definitivas. Em [Yoshizawa and Preneel 2023], os autores identificam as incompatibilidades na adoção de algoritmos pós-quânticos no padrão IEEE 1609.2 e ETSI ITS, especialmente dada a falta de flexibilidade nos padrões para inclusão de novas assinaturas. Os autores citam que, ao receber assinaturas pós-quânticas ou híbridas (aquelas produzidas por algoritmos pré e pós-quânticos), veículos mais antigos rejeitariam tais mensagens por estarem mal-formadas e, ao receber um grande volume de dados das mesmas, possivelmente denunciariam veículos com capacidade pós-quântica como atores maliciosos, que tentam

congestionar a rede. O trabalho citado propõe que maior extensibilidade seja incluída desde já, visando compatibilidade futura, e chama a atenção para a necessidade de maior investigação de algoritmos pós-quânticos no cenário de redes veiculares.

No trabalho de [Barreto et al. 2018] é apresentada uma proposta de provisionamento de certificados pós-quânticos para a infraestrutura de chave pública de V2X. A técnica se apoia no algoritmo qTESLA, que chegou até a segunda rodada do processo de padronização do NIST e oferece a propriedade de homomorfismo sobre adição, possibilitando assim o uso do *Butterfly Key Expansion*. No entanto, o protocolo resultante é inviável na prática: mesmo no menor nível de segurança, as chaves públicas e assinaturas tem por volta de 3KB e, portanto, o certificado final tem por volta de 6KB.

Em [Twardokus et al. 2024], os autores dão enfoque ao desafio do envio de assinaturas pós-quânticas e híbridas no protocolo DSRC. Devido às limitações de tamanho de *frame* e a partir de uma leitura de que o envio de certificados é majoritariamente redundante em diversos cenários, é proposta uma técnica que torna esse envio mais esparso, enviando apenas um *hash* do certificado em conjunto com as mensagens BSM e requisitando o certificado, se necessário, a partir do protocolo *Peer-to-Peer Certificate Distribution* (P2PCD), já estabelecido no padrão IEEE 1609.2. Assim, é possível desacoplar o envio do certificado das mensagens em si, enviando o certificado completo em um intervalo maior de tempo e com menor restrição de espaço utilizado no *frame*. Na prática, o atraso de uma mensagem de requisição a mais, bem como o envio do certificado completo, pode gerar atrasos intoleráveis na validação das informações.

De forma similar, em [Cominetti et al. 2023], os autores propõem uma otimização na verificação de mensagens de coordenação de forma encadeada, que não se limita ao cenário pós-quântico. Os autores observam que apenas mensagens que implicam em uma tomada de decisão precisam ser validadas, a partir do mecanismo já estabelecido de *Verify-on-Demand*. Além disso, em geral, tais mensagens vêm em conjuntos sequenciais (como no caso de um carro que passa a frear), necessitando apenas a verificação em bloco das mesmas. A proposta é de um esquema de encadeamento de mensagens a partir de funções de *hash*, de forma que a verificação de uma única mensagem autentique todo um bloco, diminuindo o atraso gerado por múltiplas verificações na tomada de decisão.

## 4. Oportunidades de pesquisa

Frente a esses desafios, são identificadas algumas lacunas de conhecimento e oportunidades de pesquisa. A primeira lacuna é a falta de trabalhos sobre adoção de criptografia pós-quântica no cenário C-V2X. Apesar da visão de redes 6G já considerar a viabilização da aplicação de carros autônomos apoiada no C-V2X, as limitações impostas pelos padrões ainda representam um grande desafio para a segurança em contexto pós-quântico.

Portanto, seria interessante para a área explorações mais aprofundadas que meçam os impactos no uso do canal, considerando diferentes densidades de dispositivos, ao se expandir o tamanho dos *frames*, para possibilitar o uso de diferentes algoritmos pós-quânticos, incluindo aqueles com possibilidade de padronização futura, como algoritmos baseados em códigos corretores de erro ou isogenias entre curvas elípticas (desconsiderando aqueles já considerados inseguros, como os baseados no problema SIDH) [Alagic 2022, NIST 2023]. A partir de tal avaliação, é possível que surjam novos *insights* sobre quais classes de algoritmos são mais adequadas e qual a perda esperada

para cada uma, indicando assim as possibilidades de readequação do padrão ou direcionando a pesquisa para algoritmos melhor adaptados. Tal possibilidade é corroborada por alguns algoritmos apresentados no processo de padronização de assinaturas pós-quânticas que dispõem de assinaturas e chaves públicas muito pequenas, como o SQISign (baseado em isogenias), com apenas 64B de chave pública e 177B de assinatura [NIST 2023].

Além disso, a validade de apenas uma semana dos certificados de pseudônimo apresenta uma oportunidade interessante para o desenvolvimento de protocolos mais eficientes e especializados para redes veiculares. Esquemas de provisionamento capazes de produzir certificados que garantam segurança pós-quântica apenas dentro de uma janela limitada de tempo podem permitir o uso de parâmetros menos rigorosos e, portanto, mais compactos e mais adequados às limitações do cenário de V2X, caso sejam respaldados a longo prazo por esquemas mais robustos. Algoritmos baseados em *hash* com estados, como XMSS e LMS, apesar de resultarem em assinaturas maiores que esquemas com a mesma segurança, apresentam uma boa flexibilidade nos parâmetros, o que abre possibilidades de que possam ser ajustados para esse contexto.

Outra questão importante a se considerar é o provisionamento de certificados pós-quânticos em infraestruturas como C-ITS e SCMS *(Security Credential Management System)*. Criptografia homomórfica é uma técnica com muitas possibilidades e que poderia viabilizar outros algoritmos de assinatura que atendam o homomorfismo de adição requerido pelo BKE. Da mesma forma, outras estruturas podem ser propostas, como, por exemplo, aquelas baseadas em expansões de chave a partir de árvores de Merkle, estrutura que já é parte integrante de algoritmos de assinatura baseados em *hash*. Além disso, propostas baseadas em criptografia funcional, na qual é possível derivar novas chaves secretas a partir de uma função de uma chave mestra, também podem se adequar ao cenário.

Por fim, técnicas como autenticação de mensagens por blocos e divulgação esparsa de certificados podem se tornar substrato protocolos que minimizam, de forma indireta, o impacto da adoção de algoritmos de maior custo, viabilizando assim sua adoção mais ampla. No entanto, ainda se faz necessário um estudo mais aprofundado dos limites de tais técnicas, e em que momento elas se tornam mais custosas por, por exemplo, requererem mais trocas de mensagem, como é o caso do P2PCD, mencionado na Seção 3.

## 5. Conclusões

Neste trabalho, foi feita uma análise dos desafios em aberto para que a criptografia pós-quântica possa ser adotada no cenário de redes veiculares. A partir da identificação de desafios, como a necessidade de se transmitir poucos dados para evitar a saturação do canal e a dificuldade de se adaptar esquemas de provisionamento de certificados de pseudônimos, foram apresentadas oportunidades de pesquisa que podem contribuir com a superação do desafio, como a exploração de algoritmos pós-quânticos com características interessantes para o cenário e a avaliação dos impactos de forma concreta.

## Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Este trabalho também foi parcialmente financiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), processo 2021/00199-8, CPE SMARTNESS.

## Referências

3GPP (2016). Release 14. Technical Specification, 3rd Generation Partnership Project.

3GPP (2020). Release 16. Technical Specification, 3rd Generation Partnership Project.

Alagic, G. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. Internal Report (IR) IR 8413, NIST.

Barreto, P., Ricardini, J., Simplicio, M., and Patil, H. (2018). qSCMS: Post-quantum certificate provisioning process for V2X. Cryptology ePrint Archive, Paper 2018/1247.

Brecht, B., Therriault, D., Weimerskirch, A., Whyte, W., Kumar, V., Hehn, T., and Goudy, R. (2018). A Security Credential Management System for V2X Communications. *IEEE Transactions on Intelligent Transportation Systems*, 19(12):3850–3871.

C2C-CC (2018). Survey on ITS-G5 CAM statistics. Technical Report, CAR 2 CAR Communication Consortium.

Cominetti, E. L., Silva, M. V. M., Simplicio, M. A., Kupwade Patil, H., and Ricardini, J. E. (2023). Faster verification of V2X basic safety messages via Message Chaining. *Vehicular Communications*, 44:100662.

ETSI (2021). Intelligent Transport Systems (ITS); Security, ITS communications security architecture and security management. Technical Specification (TS) TS 102 940, European Telecommunications Standard Institute (ETSI).

IEEE (2016). IEEE Std. for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages. *IEEE Std 1609.2-2016*, pages 1–240.

IEEE (2019). IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. *IEEE Std 1609.0-2019*, pages 1–106.

IEEE (2022). IEEE Std. for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities. *IEEE Std 1609.2.1-2022*, pages 1–261.

Jiang, D. and Delgrossi, L. (2008). IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In *VTC Spring 2008 - IEEE Vehicular Technology Conference*, pages 2036–2040.

NIST (2023). Round 1 additional signatures. Post-Quantum Cryptography: Digital Signature Schemes. `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.

Twardokus, G., Bindel, N., Rahbari, H., and McCarthy, S. (2024). When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications. *Proceedings 2024 Network and Distributed System Security Symposium*.

Yoshizawa, T. and Preneel, B. (2019). Survey of Security Aspect of V2X Standards and Related Issues. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–5.

Yoshizawa, T. and Preneel, B. (2023). 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.