4 March 2025

5GAA – 5G Automotive Association e.V.
Neumarkter Straße 21
81673 Munich, Germany

Contact:
liaison@5gaa.org

Statement of Intent on the Quantum Threat and Mitigation Strategies for the Automotive Industry

As part of its cooperation agreement with GSMA, 5GAA intends to work with the GSMA Post-Quantum Telco Networks (PQTN) Task Force to explore the impacts that quantum computing and the migration to post-quantum cryptography has on the connected automotive sector and its customers. Through this cooperation, 5GAA and the GSMA PQTN Task Force will gain insights to help both the telco and automotive industries strengthen future connected automotive security with post-quantum cryptography and crypto-agility.

The rapid evolution of automotive E/E architecture and Software-Defined Vehicles has transformed modern vehicles into highly connected computing platforms, enabling advanced functionalities such as Vehicle-to-Everything (V2X) communication, autonomous driving, and over-the-air updates. This increasing connectivity significantly expands the attack surface for bad actors, making vehicles more exposed to cyber threats.

What is at stake for the automotive sector?

Today, connected vehicles extensively use cryptographic algorithms to provide essential security assurances, such as authenticating communicating parties, ensuring data confidentiality, and confirming the integrity of communications and software. Many of these assurances are provided by asymmetric or public key cryptographic algorithms. Classical or traditional versions of these asymmetric algorithms, as currently deployed, are underpinned by difficult mathematical problems, such as factoring large integers or the discrete log problem.

However, the emergence of a cryptographically relevant quantum computer (CRQC), namely a quantum computer (QC) with sufficient accuracy and size to execute Shor's algorithm at scale, could make such algorithms much easier to solve. This would undermine the important security assurances required by modern connected vehicles. Ensuring crypto-agility and adopting Post-Quantum Cryptography (PQC) solutions is critical to future-proofing vehicular security.

Concretely, the quantum threat could impact a range of automotive-relevant domains, potentially affecting road-user safety and leading to vehicle damage (e.g. by overwriting braking software), financial damage (e.g. by removing theft protection), threats to privacy (e.g. by remote monitoring) or operational damage (e.g. by deleting software) via the following highly scalable attack vectors:

- Remotely controlled operations on mainly remote type functionalities (remote software updates in contrast to customer-induced OTA-updates, remote driving functionality, remote diagnostics)
- The use of digital signatures for signing firmware, software and over-the-air updates; e.g. immutable hardware-based digital signatures used in Secure Boot and reliant on Read Only Memory (ROM) or using a public key burned into the OTPM (One-Time Programmable Memory);
- Data transfers from the telematics control unit (TCU) to vehicle manufacturers' backend systems; Vehicle-to-Everything (V2X) communications.

The above list of relevant domains and attack vectors are not intended to be comprehensive. Nonetheless, they demonstrate the potential relevance of the quantum threat to the automotive sector and motivate a more detailed emphasis on the issues that will likely have the greatest impact on the automotive industry and its customers. In addition, the automotive sector's specificities reinforce the need to consider migrating to quantum-safe status in the near-term i.e.:

- The long lifetime of automobiles, which can remain in the field for decades, and the use of embedded hardware with quantum-vulnerable cryptographic algorithms which cannot be easily updated, increase the likelihood that quantum-vulnerable algorithms will remain deployed when a CRQC emerges.
- In general, the new PQC algorithms cannot simply be deployed as drop-in replacements. They have different performance characteristics impacting computing power and memory capacity requirements. This is especially important in constrained environments such as the automotive industry, where small microcontroller units might run into memory problems because of the increased size of keys and signatures.
- Bad actors that access present-day encrypted communications can in principle store this data and decrypt it in the future once a CRQC becomes available. Consequently, long-lived data currently secured with quantum-vulnerable algorithms could be compromised in the future, necessitating safeguards in the present, to protect against this Harvest Now, Decrypt Later attack.

Towards quantum-safe

Replacing the quantum-vulnerable algorithms currently deployed by newly standardized PQC algorithms would mitigate the threat of quantum-empowered attacks. Organizations such as the US National Institute of Standards and Technology (NIST)[1] and the Korean National Security Research Institute (NSRI)[2] have already undertaken lengthy, multi-year processes to identify and standardize cryptographic algorithms resistant to quantum attacks. New algorithms such as the so-called ML-KEM[3] and ML-DSA[4] may be good candidates for securing vehicular communications. However, the large-scale migration from widely used cryptographic algorithms will be a complicated process due to the specific technical and operational constraints of the automotive industry, e.g., hardware, latency, standardization, or interoperability considerations.

In addition, the threat posed by a CRQC is widely recognized but the impact of regional PQC strategies needs to be better understood by the global automotive industry. Navigating the different sets of PQC algorithms standardised in distinct jurisdictions,[5] and the differing timelines for adopting PQC, adds to the complexity of the task at hand.

The timeline for the emergence of a CRQC is difficult to forecast, given the unpredictable dependence on rapidly developing and emerging technologies. Therefore anticipation will be key. Governments and other industries have already started investigating migrating to quantum-safe algorithms. For example, the United States government has indicated an intention to begin preferencing quantum-safe suppliers as early as 2025, potentially impacting organisations that supply secure services and products. Other industries are already seeing early adoption, with examples including Google's addition of PQC to TLS,[6] and the use of PQC in both Apple's iMessage[7] and Signal's messenger[8].

Through the newly announced partnership, 5GAA and the GSMA PQTN Task Force will explore the impact of the emerging quantum threat and the required mitigation strategies for the highly scalable attacks which currently pose the greatest threat to the automotive industry and its customers.

---

[1] https://csrc.nist.gov/projects/post-quantum-cryptography
[2] https://kpqc.cryptolab.co.kr
[3] https://doi.org/10.6028/NIST.FIPS.203
[4] https://doi.org/10.6028/NIST.FIPS.204
[5] Or to-be-standardized; e.g., China recently announced a separate PQC selection process. See: https://niccs.org.cn/en/notice
[6] https://security.googleblog.com/2024/08/post-quantum-cryptography-standards.html
[7] https://security.apple.com/blog/imessage-pq3/
[8] https://signal.org/blog/pqxdh/