Redefining Security

QUANTUM-SAFE SECURITY
WHITE PAPER

# The impact of quantum technologies on the future V2X ecosystem

October 2019

Guest editor:
Joachim Taiber, Chief Technology Officer, International Transportation Innovation Center (ITIC)

## Table of contents

**ID Quantique SA**
Ch. de la Marbrerie, 3
1227 Carouge
Switzerland

Tel: +41 (0)22 301 83 71
Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

**Information in this document is subject to change without notice.**

## Executive summary

Quantum Computers promise to perform calculations exponentially faster than conventional digital computers by leveraging the principle of superposition and using qubits instead of binary bits. Although quantum computing is still in its infancy and quantum computers currently exist only as prototypes, it is estimated that within the next 10-15 years cyberattacks could be performed with the help of quantum computers. This requires that existing cryptographic methods are modified to withstand such quantum attacks. The development of so-called quantum-safe cryptography is a strategic effort, which will ultimately reach all industry verticals – and in particular those where safety critical infrastructure or devices are involved as for example in the transportation sector.

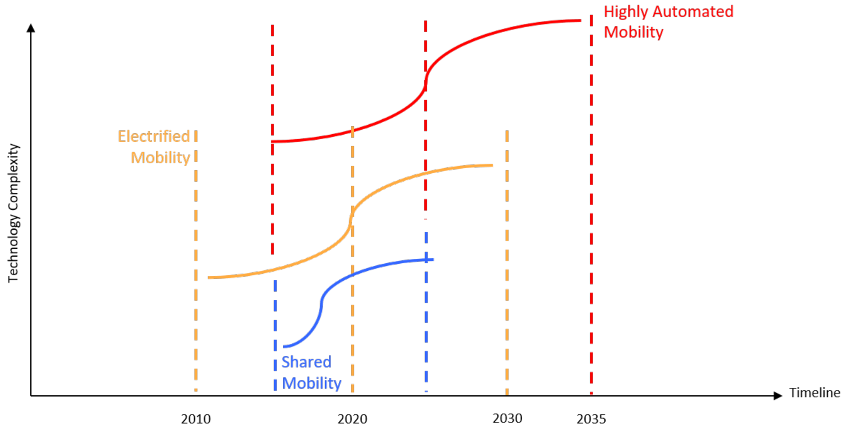
The automotive industry is currently in a major transition to connect, automate and electrify vehicles and to offer Mobility-as-a-Service (MaaS) to users. This requires the use of a V2X ecosystem where data is transmitted on demand between the data centres, the vehicle sensors and the vehicle controllers using high performance networks. The need to exchange data between back-end systems and vehicles as well as between vehicles directly makes the system vulnerable to cyberattacks, which could lead to significant safety risks for human life and hence to substantial liability risks.

Recent cybersecurity reports show that in the automotive sector, black hat attacks have become a real threat with not only frontal attacks of vehicle control systems but also backend breaches of data communication layer. This leads to the need for both automotive Original Equipment Manufacturers (OEMs) and MaaS providers to invest in cloud security, network security and in-vehicle security.

With the need to secure data both within the vehicle and in the interaction between the vehicle and the back-end, the introduction of quantum-safe cryptography becomes a strategic topic for the vehicle industry. As vehicles stay in service typically for more than 10 years it is necessary to enable them to go through many software update iterations with the same hardware platform without the risk of being compromised by cyberattacks. Making the V2X ecosystem quantum resistant is a first step to prepare for the quantum computing age. This process has to start early, before “outdated” vehicles become the potential victims of quantum attacks.

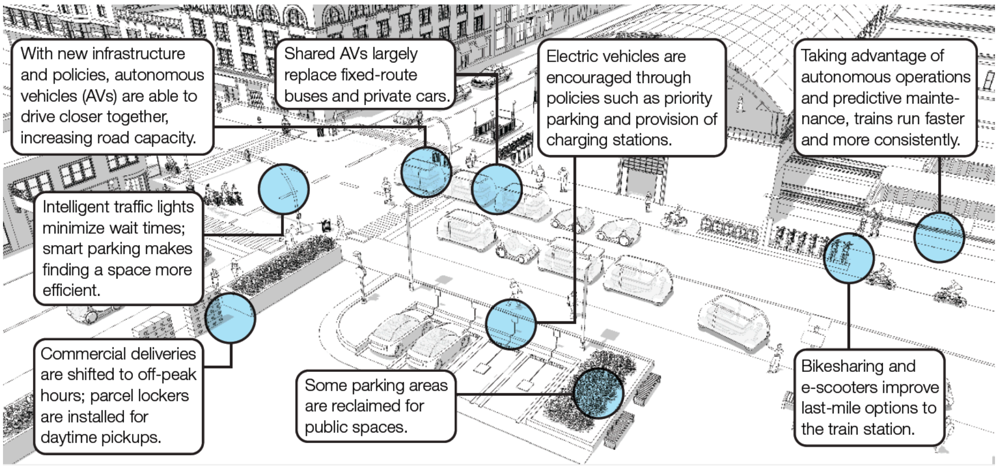
## Trends in the automotive industry

The Automotive industry is currently being transformed from a product and hardware-centric business model to a more software service and data-driven business model. The traditional automotive sales model emphasizes ownership of physical cars, typically resulting in an underutilisation of a high overhead cost consumer good which would be much more efficacious if commercially shared instead. For example, the huge success of on-demand shared mobility services (MaaS), in particular with urban citizens, demonstrates the growing need to adopt a new form of mobility that prioritises the utilisation of a mobility service rather than ownership of a specific car model. This requires close coordination among shared fleet vehicles with robust data connectivity and optimal operational performance backend. Furthermore, fleet operators are interested to replace the human driver with automated vehicles as long as the cost of automation are lower than manual labour. Another important trend is vehicle electrification, in reducing transportation carbon emission levels. Electrified vehicles need intensive data monitoring of the battery system as well as active route guidance to reach usable electric charging stations within the given electric range of the vehicle to support zero emission operation.



Source: INTRA Group

Considering these transformative trends in Automotive, data accessibility, authenticity, and ownership become essential in the safe, secure and cost-efficient operation of vehicle fleets. A key question is which data belongs to the vehicle owner or user and which data belongs to the OEM or fleet operator. In either case, the data must be protected from illegitimate use. This protection needs to cover the entire technology stack: the vehicle side, the V2X network side, and the backend side for the full life cycle of the vehicle.


With new infrastructure and policies, autonomous vehicles (AVs) are able to drive closer together, increasing road capacity.
Shared AVs largely replace fixed-route buses and private cars.
Electric vehicles are encouraged through policies such as priority parking and provision of charging stations.
Taking advantage of autonomous operations and predictive maintenance, trains run faster and more consistently.
Intelligent traffic lights minimize wait times; smart parking makes finding a space more efficient.
Commercial deliveries are shifted to off-peak hours; parcel lockers are installed for daytime pickups.
Some parking areas are reclaimed for public spaces.
Bikesharing and e-scooters improve last-mile options to the train station.

Source: McKinsey, An integrated perspective on the future of mobility

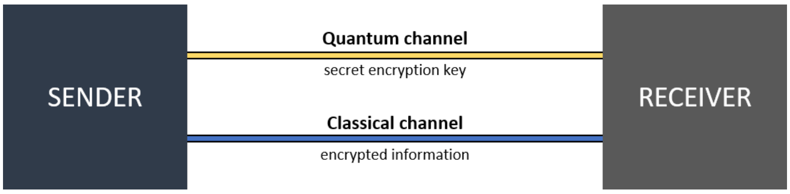
## Overview about quantum technologies

Quantum Mechanics (QM), the physical theory, which pertains to explain the behaviour of matter at the smallest scale, has been with us for more than one century. It is associated with the famous names of Bohr, Heisenberg, Schrödinger, Einstein and many others. Initially, QM was about understanding Nature at these incredibly small scales. How are atoms constructed from the basic components? Why do chemical elements have this or that structure, or this specific property? The change from our classical world view to a quantum one was so large, that it took many years to accept. And many more to move to the application level: how can we use QM? However, devices relying on quantum properties are now ubiquitous. From the high-power processors in our smart phones and computers, to the lasers reading our CD's, the detectors in our cameras, and the medical devices imaging the insides of our bodies, none would be here without our understanding of Nature brought by QM.

We have now reached the next step. Quantum Technologies are not only about understanding, but about engineering. We have begun to build things which do not exist in Nature. We control and organise matter at the quantum level.

In this white paper, we will examine one aspect of quantum technologies: quantum information technologies (QIT). In QIT, the basic element of a computation is not the classical bit, which can be a zero or a one, but a qubit, a quantum system, which can also be in a so-called coherent superposition of the two states.

**Quantum communication** leverages the laws of quantum physics to transmit data securely. In modern cryptographic systems, sending secure data over insecure communication infrastructure is done in two steps. In the first step, a secret key has to be shared by the two users. In the second step, the secret key is used in so-called symmetric algorithms in order to encrypt the data. The first step often relies on asymmetric cryptography algorithms, which will be broken by a future quantum computer (see next section). Quantum Key Distribution, or QKD, allows the users to generate this secret key. A random stream of qubits, which will build the secret encryption key, is sent via the quantum channel (using a QRNG – Quantum Random Number Generator). The property of the quantum channel ensures that any attempt by an eavesdropper to discover the key will generate errors in the transmission. Through measurement and interaction processes over a classical channel, the sender and the receiver will be able to discover the errors, correct them, and reduce the potential information leakage to the eavesdropper to any infinitesimal value they choose. Once the sender and the receiver know that they hold the same key and that it is secure, they can send the encrypted information over the classical channel.



**Quantum computers** can solve a subset of problems much faster than a classical computer.

In traditional computing bits are processed sequentially. A computation starts with an initial state of the computer, say a register with N bits. It performs a series of operations on these N bits and reaches a final state at the end of the computation. If you want to test another value of the register, you need to perform a new computation. The number of possible values of the N bit register is $2^N$. Therefore, the number of different states you may have to test, or the number of computations you may have to perform, scales exponentially with the number of bits.

In quantum computation, you first generate a coherent superposition of many possible states of the register. This step is only linear in the number of qubits in the register (i.e. of the order of N) and can be done quickly. This initial state of the register is known as an entangled state: all the qubits are somehow connected with one another. You then run the computation on this very large entangled state. Since QM is a probabilistic theory, you may not reach the right answer, but by running the computation several times you will eventually get the answer with large probability. A single quantum processor is therefore "similar" to a massively parallel classical processor, without requiring parallelised hardware such as several processor kernels.

So far, not many problems have lent themselves to this type of processing. The most famous one, factorisation of large integers, has been solved by the Shor algorithm. This problem is the basis of all current asymmetric cryptographic algorithm. The quantum computer will therefore break existing cryptography.

To date, only experimental quantum processors of small to medium sized arrays of controllable quantum bits have been developed. Commercially available quantum computers are still in a very early stage of development though.

The term **post-quantum cryptography** (PQ crypto) – also referred to as quantum-safe, or quantum-resistant cryptography – is being used in context of cryptographic algorithms, which should be able to withstand cyberattacks performed by quantum computers. So far, however, due to the lack of a real quantum computer, only a few quantum algorithms, such as Shor's algorithm, have been invented. It is possible (some say even probable), that new, as of yet undiscovered, quantum algorithms may break some PQ algorithms. Using quantum technologies, such as QKD, to counter the quantum computer threat, is therefore an interesting alternative.

## Overview of automotive security mechanisms

The term V2X (vehicle-to-everything) refers to a smart, holistic transportation ecosystem where all vehicles and their surrounding infrastructure are interconnected. Through continuous communication within this system, the traffic situation can be interpreted at all times in a precise manner across the entire road network.

This provides the following benefits:

1) streamline the flow of traffic
2) lower the risk of congestion
3) reduce the risk of accidents
4) lower greenhouse emissions

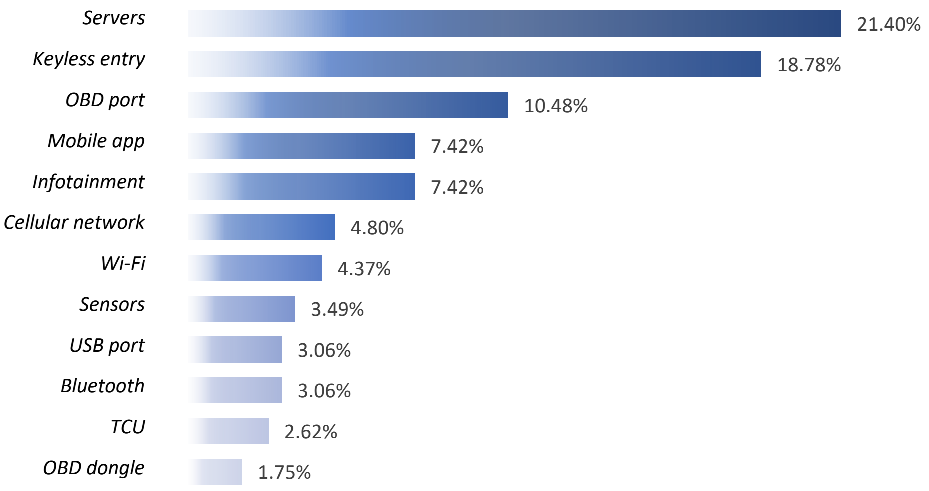
Wireless communication with stable signal coverage is required to ensure seamless communication throughout the V2X ecosystem.

V2X consists of different subcategories:

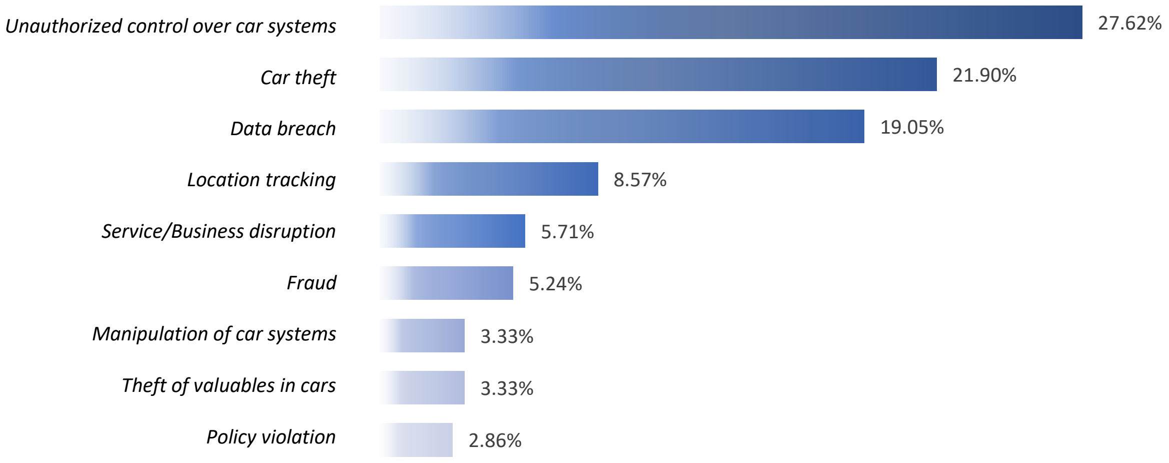
a) V2I (vehicle-to-infrastructure)
b) V2N (vehicle-to-network)
c) V2V (vehicle-to-vehicle)
d) V2P (vehicle-to-pedestrian)
e) V2D (vehicle-to-device)
f) V2G (vehicle-to-grid)

For each subcategory, there are two technologies currently being used: WLAN-based communication and cellular-based communication. In 2016, a specification for V2X based on LTE was first published by 3GPP, referred to as cellular V2X (C-V2X), supporting V2V, V2I and V2N. In contrast to the first specification ever published for V2X, the WLAN-based IEEE 802.11p from 2012, it enables a native migration to 5G.

With the rise of V2X connectivity, research on threats and risks on CAV's (connected and automated vehicles) has risen significantly over the last few years. V2X ecosystems are dynamic and interchangeable, leaving them vulnerable to blind spots and gaps that form during system updates and maintenance. The physical distance of the attack needs to be considered in the risk assessment of potential attack vectors. In the most recent 2019 cybersecurity report performed by Upstream Security Ltd which is focused on the connected vehicle world it was revealed that the number of black hat attacks (malicious intent) have overtaken white hat attacks (research-intent) and the threat patterns shift from physical (mechanical connection to vehicle required, for example OBD-port) and wireless short-range (amplified devices via near-field, often interfering with vehicle security controls) towards a rising percentage of long-range attacks (via Wi-Fi or cellular, mostly from backend). Apart from keyless entry, the most imminent threat is represented by attacks on servers which can range from a single affected vehicle to a fleet-wide interference that could have catastrophic, life-endangering effects, up to the full control over a fleet of vehicles by a malicious 3rd party.



Top smart mobility attack vectors (source: Upstream Security)



Top impacts of cyber-attacks on automotive (source: Upstream Security)

To evaluate the security level of the V2X ecosystem, we need to look at three domains: in-vehicle security, network security, and cloud security, as well as their interaction with each other. In-vehicle security protects the individual components of the vehicle and can ward off close-proximity attacks as well as some remote attacks. Network security keeps a stronghold at the IT network and backend. Automotive cloud security is used to detect and resolve cyber-attacks or misuse through smart mobility devices, single and multiple-vehicle attacks as well as attacks on telematics and mobility services in hybrid or cloud-based environments.

The following table[1] gives an overview about vehicle-relevant security features and their OEM deployment maturity level:

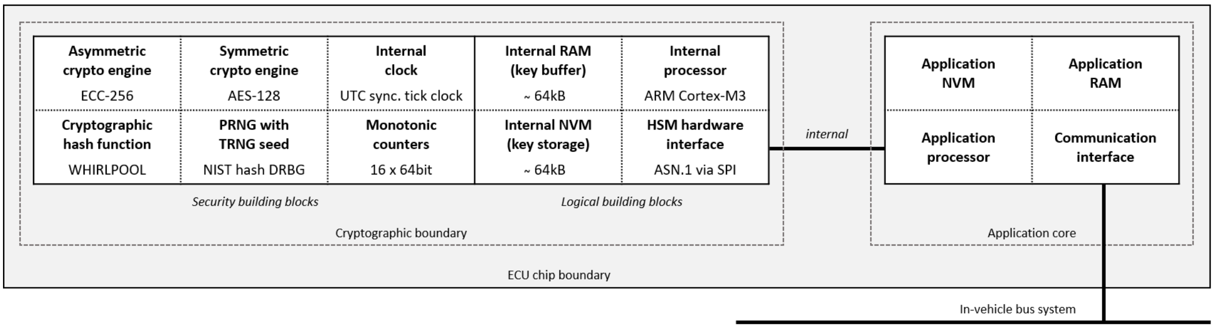
| Feature | 2018 | 2023 |
|---|---|---|
| Domain separation | Seldom | Common |
| PKI | Seldom | Many |
| Hardware Trust Anchor and/or HSM | Seldom | Many |
| AUTOSAR Security Modules | Seldom | Many |
| Signed SW Updates | Seldom | Many-Common |
| Secure Diagnostic Services | Seldom (with weaknesses) | Many |
| Secure Boot | Seldom | Many |
| Authenticated Boot | Seldom | Many |
| Secure Communication with Backend | Many | Common |
| Secure Car Internal Communication | None | Many |
| Firewall | Many | Common |
| IDS/IPS | None | Seldom-Many |
| Wi-Fi/Bluetooth Security | Common (with weaknesses) | Common |

PKI: Public-Key-Infrastructure
HSM: Hardware Security Module
IDS/IPS: Intrusion Detection System / Intrusion Prevention System

The HSM is a customer-programmable physical computing device embedded into the automotive microcontroller architecture with dedicated functionality to perform cryptographic information processing and to manage digital keys. It typically contains a secure CPU inside, security-specific peripherals, cryptographic engine and dedicated blocks of RAM for secure data and code storage.

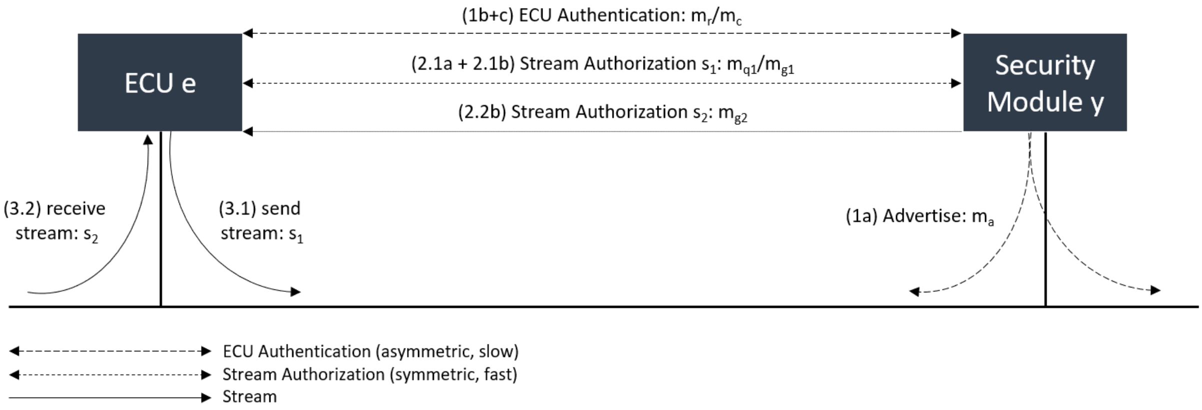
[1] Cybersecurity Evaluation of Automotive E/E Architectures

Here is an example of an HSM system architecture:



Source: Cybersecurity Evaluation of Automotive E/E Architectures

An example how automotive ECU’s (Electronic Control Unit) interact with the HSM for secure data communication is provided below. Please note that in the shown framework, every ECU is authenticated against the security module (1a-1c). Subsequently, the ECU can request the keys for a message stream (2.1a-2.1b) and start transmitting (3.1). If the ECU is to start receiving a message stream, it is notified by the security module with the message stream key (2.2b) before it receives the stream (3.2).


(1b+c) ECU Authentication: $m_r/m_c$
ECU e
(2.1a + 2.1b) Stream Authorization $s_1$: $m_{q1}/m_{g1}$
Security Module y
(2.2b) Stream Authorization $s_2$: $m_{g2}$
(3.2) receive stream: $s_2$
(3.1) send stream: $s_1$
(1a) Advertise: $m_a$
ECU Authentication (asymmetric, slow)
Stream Authorization (symmetric, fast)
Stream

Source: Security in Automotive Networks: Lightweight Authentication and Authorization

## The need for future-proof cybersecurity

There are two major trends that are driving the need for computing power both in the vehicle and backup data centre: connected and automated driving. Just like how quantum computing can be used for machine and deep learning algorithms required to enable self-driving cars, it can also pose a cybersecurity threat to the entire V2X ecosystem architecture.

Currently, there is a parabolic growth in both the software complexity and the computing power in a car. Through reconfigurable hardware and V2X connectivity, a vehicle has a much better chance to last through its multiple-years' service life if its regular software updates are reliably safe and secure.

The US Department of Homeland Security[2] (DHS) recommends certain key tenets for what they term "Life Critical Embedded Systems" which neatly summarise the ubiquity of cryptography in machine to machine security.

- All interactions between devices MUST be mutually authenticated
- Continuous authentication SHOULD be used when feasible and appropriate
- All communications between devices SHOULD be encrypted
- Devices MUST NEVER trust unauthenticated data or code during boot-time
- Devices MUST NEVER be permitted to run unauthorised code
- Devices SHOULD NEVER trust unauthenticated data during run-time
- When used, cryptographic keys MUST be protected

Moreover, the report goes on to state that devices and systems MUST be built to include mechanisms for in-field update, and that devices and systems for managing updates MUST be mutually authenticated and secured: *"Threat models must recognize that some systems will need to be in place for decades, while others may refresh annually or more frequently […] Life critical embedded systems should be engineered to include enough compute capacity for stronger cryptographic and runtime protections that will need to be added within the lifetime of the systems."*

A key requirement for automotive information security system is crypto-agility: an alternative to the original encryption method or cryptographic primitive can be found without a major change of the system architecture. This means that a vehicle must be designed today with a proactive and modular security approach that can handle updating existing cryptographic primitives to future quantum-resistant cryptography without affecting the underlying hardware. Currently however, it is expected that post-quantum cryptographic algorithms are compute-intensive and require dedicated hardware for live security processing. This hardware needs to be reconfigurable enough to anticipate cryptosystem updates and upgrades leading, to a more flexible cybersecurity system architecture.

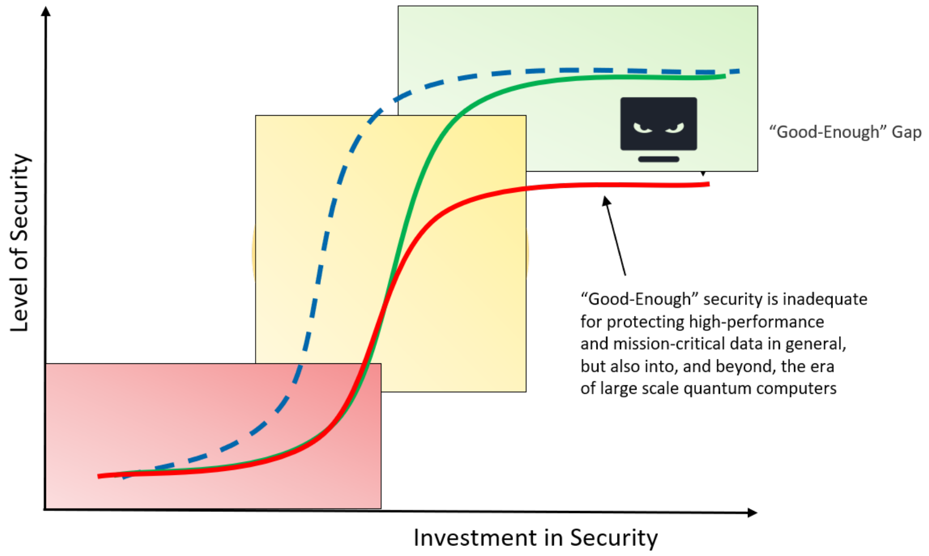
With the advent of quantum computing, existing public key cryptography standards need to be revisited, so that new vehicles today can transition to quantum-resistant cryptographic primitives

[2] DHS Security Tenets for Life Critical Embedded Systems https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

during their life-cycle. The most common public-key cryptographic schemes are based on the discrete logarithm problem over elliptic curves and the RSA problem. Those schemes will become insecure once powerful quantum computers are commercially available. Further, cryptographic primitives such as hash functions and symmetric key encryption will become vulnerable with quantum cyber-attacks and require to increase the key length. This will in turn demand more computing power.

In order to prepare a holistic and future-proof "cryptosystem", it is important to consider processing efficiency, scalability and flexibility. A hybrid approach is needed where software code is running on standard CPU/GPU cores while more computationally intensive cryptographic applications are processed directly on specialised hardware with quantum-resistant cryptographic primitives and methods.

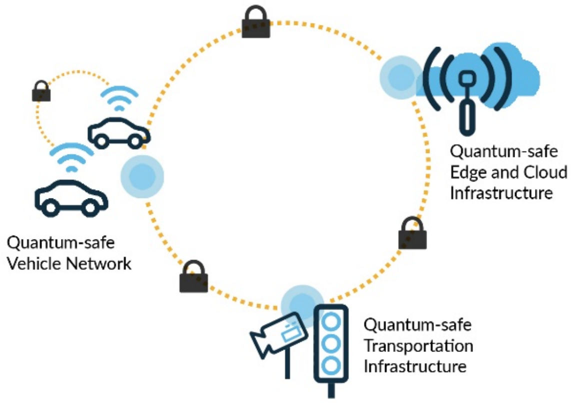
A major challenge is companies' nativity towards near-future cybersecurity risks and hence inadequate resources allocated to cybersecurity investments. Organisations with high-security awareness and that are proactive to put the best possible protection in place are best positioned for long-run success and sustainability. The Automotive Industry is using organisations such as Auto-ISAC (Automotive Information Sharing and Analysis Center) to leverage existing standards and share best practices to manage and mitigate the cybersecurity risk.


Level of Security
Investment in Security
"Good-Enough" Gap
"Good-Enough" security is inadequate for protecting high-performance and mission-critical data in general, but also into, and beyond, the era of large scale quantum computers

Companies' risk attitude: "good-enough" security model

## Strategy to make the V2X ecosystem quantum-safe

From a V2X ecosystem security perspective we need to look into the following domains: vehicle system, vehicle-to-vehicle network, vehicle-to-infrastructure network and backend system.



V2X network (Source: INTRA Group)

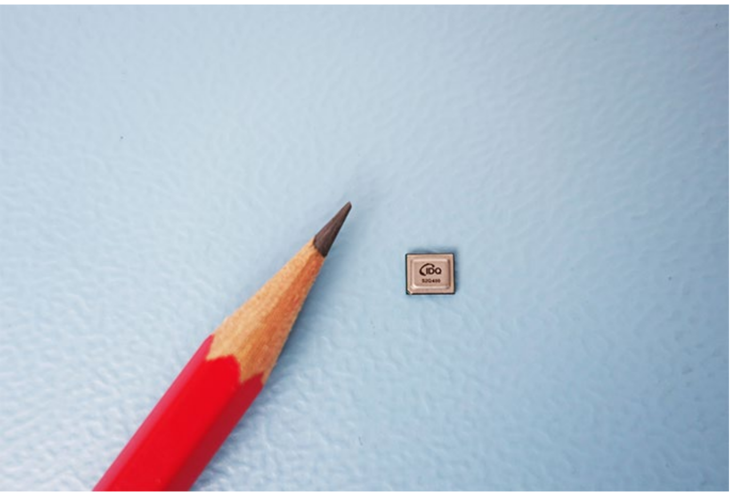
An important trend is the development of 5G networks that enable low latency system response for vehicle to backend communication as well as very high data communication rates. However, we will see that vehicles need to be configured in order to automatically handle so-called mixed networks (i.e. LTE, 5G, DSRC, BT, Wi-Fi). Within vehicles the Automotive Ethernet protocol will develop into the communication backbone allowing data rates of up to 20 Gbps. Because sensor data are shared among vehicles as well as between vehicle and backend, their data integrity (correctness & authenticity) must be ensured at all times. In particular, for assisted and automated driving, sensor data that is critical to safety needs to run via secure communication channels. On the other hand, safety critical data is processed both inside of the vehicle in electronic control units as well as in the backend on server units. The distributed data processing and data storage as well as the data transmission within the V2X ecosystem must be **quantum-safe** in the future.

RSA/ECC-based asymmetric cryptosystem are currently widely used in the automotive world. However, they cannot be considered quantum-safe. For example, ECC-256 which in the classical world has 128-bit security has almost no security in the quantum world.

In symmetrical cryptography quantum-safe standards such as AES-256, SHA-512 or SHA3-512 need to be adopted. For example, AES-128 has 128-bit security in the classical world but only 64-bit security in the quantum world.

In order to identify data anomalies in vehicle security, both network security and backend security need to work in synchronisation to prevent harm to human beings and physical systems. Through the use of low latency communication networks such as 5G, anomalies can be detected earlier in the V2X ecosystem. However, the application of PQ algorithms also requires more computing power and when longer quantum-safe encryption keys are being deployed, system performance and latency deteriorate which needs to be compensated for by hardware-encoded cybersecurity systems as described before.

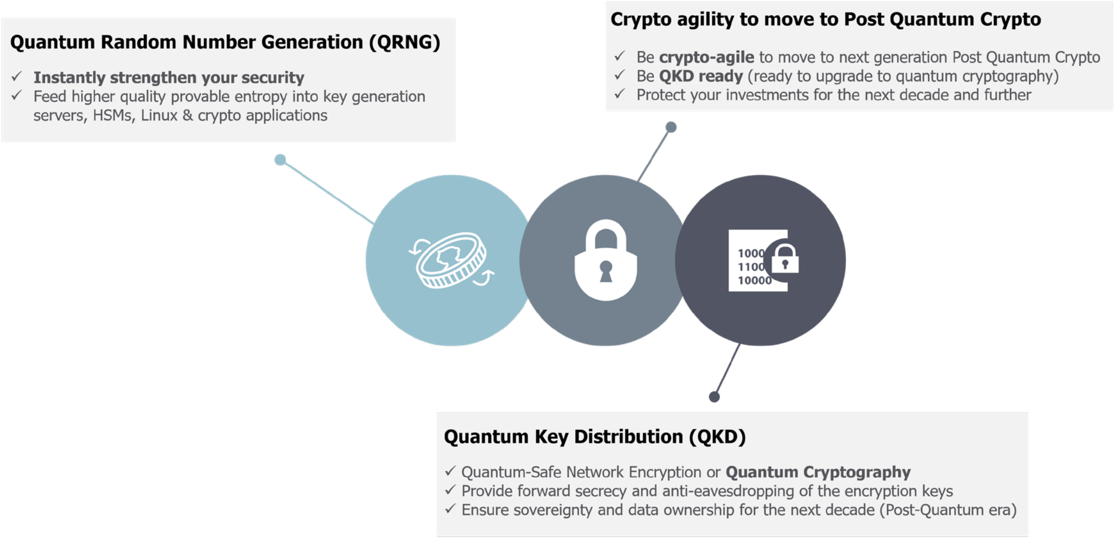
In cryptography, what really and ultimately matters is the key. Cryptography's effectiveness derives from the fact that the key is kept secret or as Kerckhoff would have put it: "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge". Any crypto system – existing or future – must be underpinned by strong key generation. This process is essential in the sense that it must not be possible for a third party to guess or deduce the key. Therefore, the use of truly random numbers is crucial. Quantum Random Number Generation (QRNG) serves this purpose well. It instantly strengthens existing security/crypto mechanism and ensures that the new QRAs will get enough high-quality randomness to remain robust. In order to generate secure keys, it is already best practice in automotive security to use TRNGs (True Random Number Generators) as an entropy source. In the quantum world QRNGs need to be used such as one offered by ID Quantique (IDQ). In particular the form factor and price of IDQ's QRNG chip make it relevant for integration into automotive HSMs. It is also AEC-Q100 certified, with integrated NIST 800-90A/B/C compliant DRBG post-processing.



Quantis QRNG Chip

Blockchain and other distributed ledger technologies (DLTs) are currently an active area of research in the automotive world, especially in the V2X context. Block hash addresses, nonces, and public-private keys are generated with random numbers and cryptographic hashing algorithms, such as SHA-256. These functions require very strong random number generation where QRNGs can be applied.

Another important method is Quantum Key Distribution (QKD), as explained before. In an automotive context, QKD can be used to protect data exchange inside the back-end infrastructure, which is a primary target for attackers due to the massive amount of sensitive data that can be stolen at a time.



**Quantum Random Number Generation (QRNG)**

- ✓ **Instantly strengthen your security**
- ✓ Feed higher quality provable entropy into key generation servers, HSMs, Linux & crypto applications

**Crypto agility to move to Post Quantum Crypto**

- ✓ Be **crypto-agile** to move to next generation Post Quantum Crypto
- ✓ Be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further

**Quantum Key Distribution (QKD)**

- ✓ Quantum-Safe Network Encryption or **Quantum Cryptography**
- ✓ Provide forward secrecy and anti-eavesdropping of the encryption keys
- ✓ Ensure sovereignty and data ownership for the next decade (Post-Quantum era)

ID Quantique’s recommended path to quantum safety

In summary, the critical path for a quantum-safe V2X ecosystem is to implement **crypto-agility** in both the vehicle platform and the network/backend infrastructure. The security bottleneck is typically the physical vehicle obsolescence due to its longevity whereas network and backend infrastructure can be regularly updated both from a hardware and software perspective to stay secure. On the contrary, the hardware in a car is typically static and only software updates are possible once the vehicle is in operation which poses over time an increasing cybersecurity risk. Using quantum enabled hardware components such as QRNG will be critical to generate quantum safe keys. Applying post-quantum algorithms for encryption which result in longer keys will lead to highly resilient automotive security system architectures that utilize hardware-based acceleration and are configurable in nature.

## The need for quantum risk assessment on all system levels

In order to analyse where in the automotive world quantum technologies can pose a risk, a systematic assessment at all system levels end-to-end is required.

The key steps of such a quantum risk assessment are:

1. Analyse all assets and determine their cryptographic protection

2. Map the technological progress in quantum technologies to the state-of-the-art technology being used in the target system

3. Test and validate quantum-safe cryptography methods

4. Identify potential threat actors and estimate the time until they could apply quantum technologies for attacks which determines the timeline to make the target system quantum-safe

5. Develop a plan to bring the target system into a quantum-safe system state and prioritise activities to anticipate the highest risks