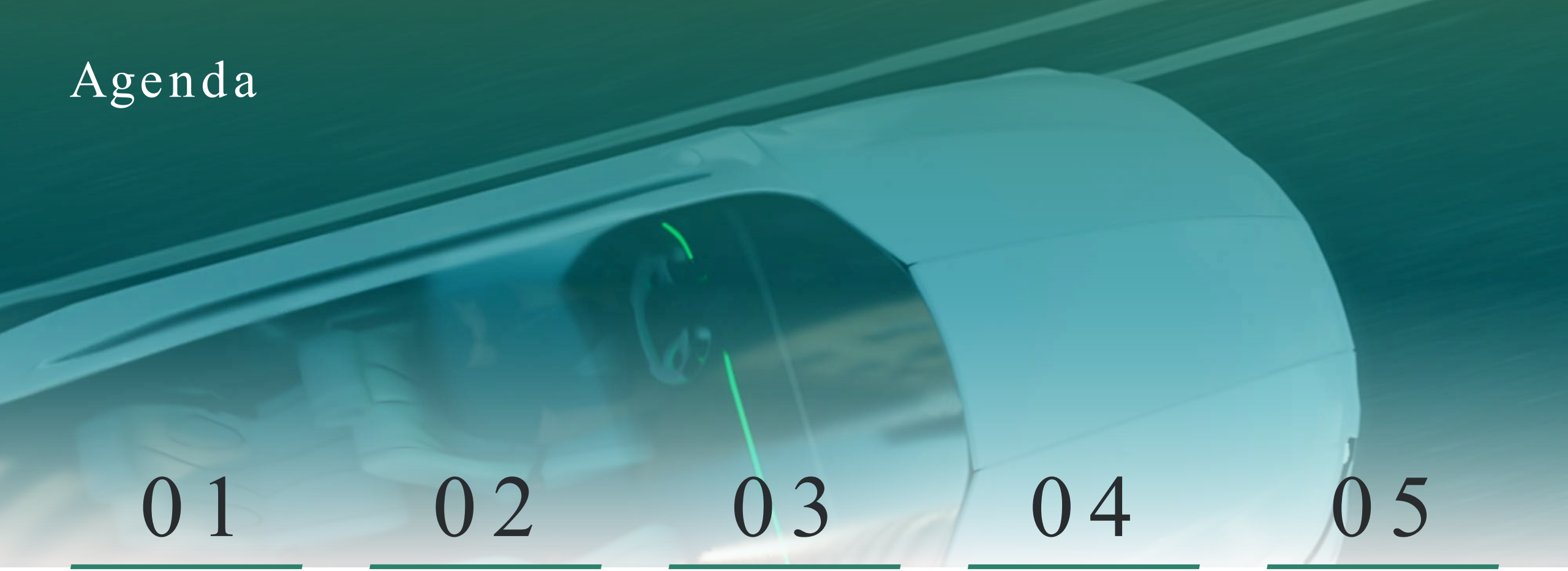
Post-Quantum Cryptography for Automotive

Dr. Ayoub Mars, Elektrobit Automotive GmbH
Maurice Heymann, Continental Automotive Technologies GmbH

Symposium Post-Quantum Cryptography - Episode V
June 13, 2023

Agenda



01 Motivation

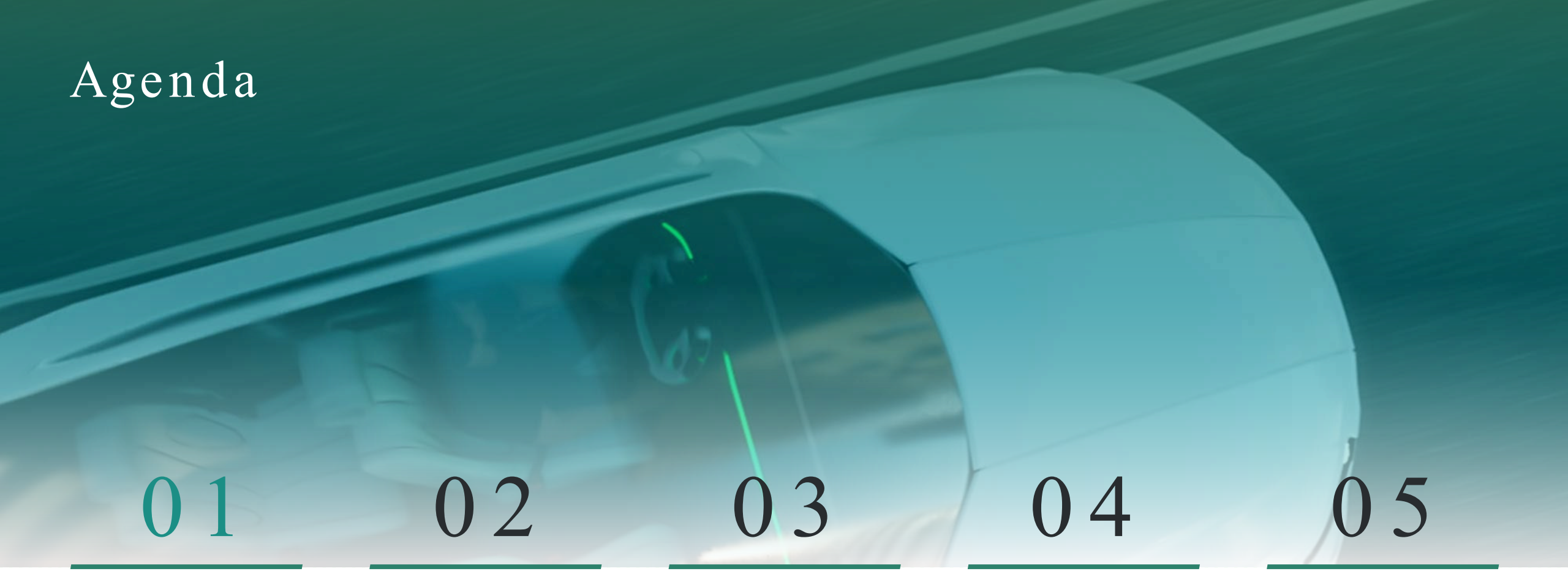
02 Automotive Cybersecurity

03 PQC Migration Challenges

04 Demonstrator

05 Summary

Agenda



01 **Motivation**

02 Automotive Cybersecurity

03 PQC Migration Challenges

04 Demonstrator

05 Summary

Industry experts talk about „Quantum Computers“

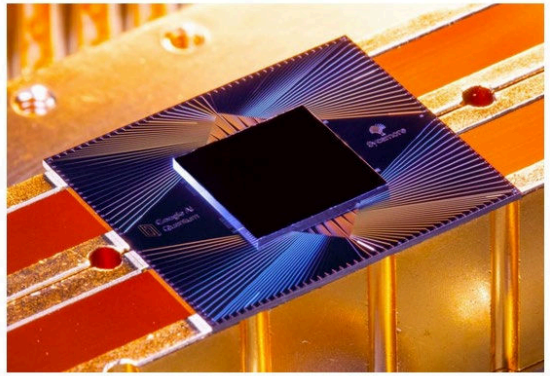
nature › news › article

NEWS | 23 October 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Elizabeth Gibney



The Sycamore chip is composed of 54 qubits, each made of superconducting loops. Credit: Erik Lucero

IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two

Company Outlines Path Towards Quantum-Centric Supercomputing with New Hardware, Software, and System Breakthrough

Nov 9, 2022

Dario Gil, Jay Gar

Intel Newsroom / Intel Hits Key Milestone in Quantum Chip Research

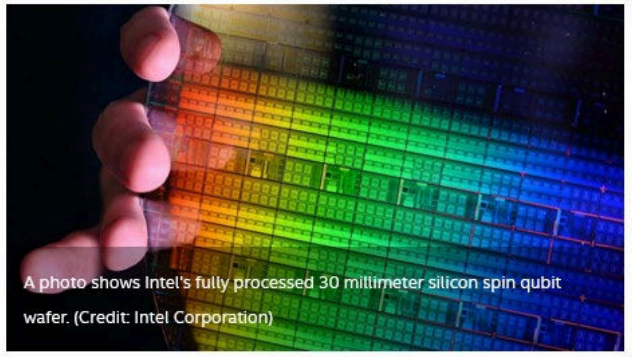
Intel Hits Key Milestone in Quantum Chip Production Research

Intel demonstrates exceptional yield of quantum dot arrays, showing promise for large-scale qubit production using transistor fabrication technology.

News

- October 5, 2022
- Contact Intel PR

More New Technologies News



A photo shows Intel's fully processed 30 millimeter silicon spin qubit wafer. (Credit: Intel Corporation)

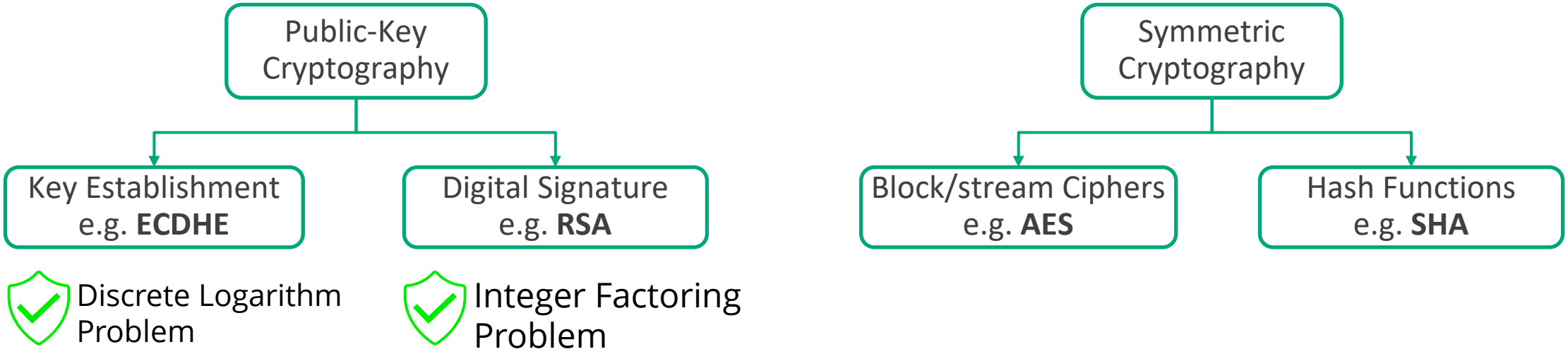
Sources:

https://www.nature.com/articles/d41586-019-03213-z/

Intel Hits Key Milestone in Quantum Chip Production Research

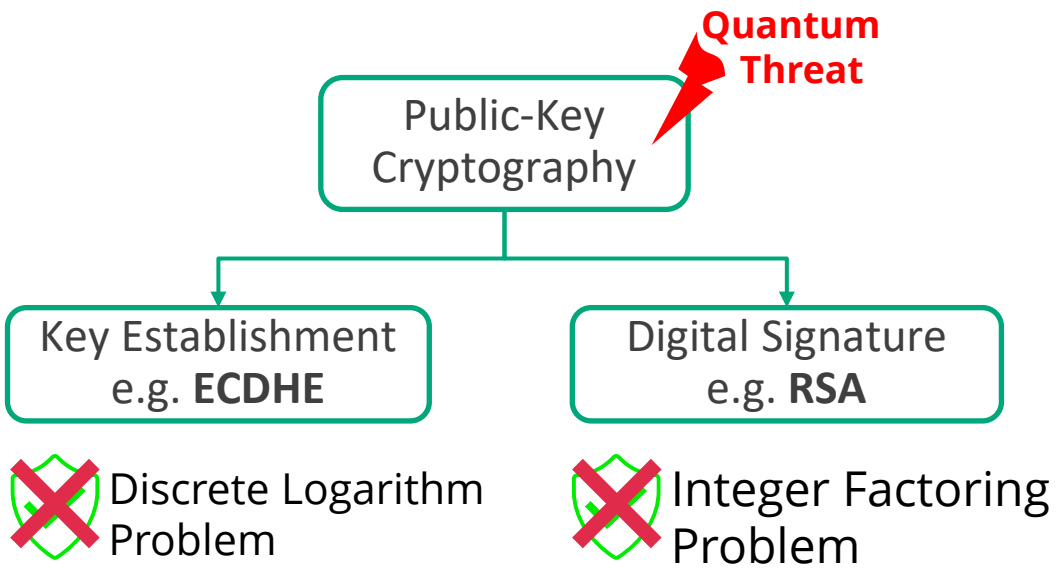
IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two

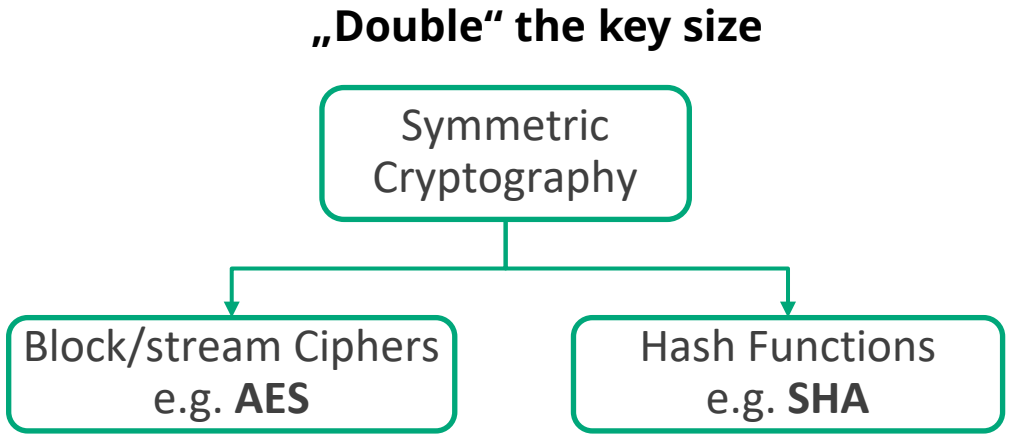
Contemporary Cryptography



Contemporary Cryptography

Quantum Threat





- Shor’s algorithm (1994)
  - Quantum algorithm giving exponential speed-up over classical computers
  - It can be used for Factoring large integers and Finding discrete logarithms

- Grover’s algorithm (1996)
  - Polynomial speed-up in unstructured search, from $O(N)$ to $O(\sqrt{N})$

Status of NIST PQC Standardization

Current Status

- KEMs
  - » Kyber, BIKE, Classic McEliece, HQC
- Digital Signatures
  - » Dilithium, FALCON, SPHINCS+

The four Candidates to be Standardized

Fourth round candidates

Call for Quantum-Resistant Digital Signatures

- Deadline was June 1st, 2023
- Preferably signatures based on non-lattice problems
- Interest in signature schemes that have short signatures and fast verification

Agenda

01 Motivation

02 **Automotive Cybersecurity**

03 PQC Migration Challenges

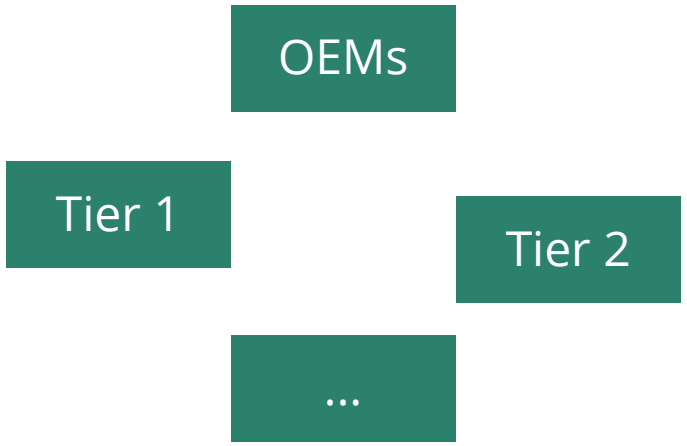
04 Demonstrator

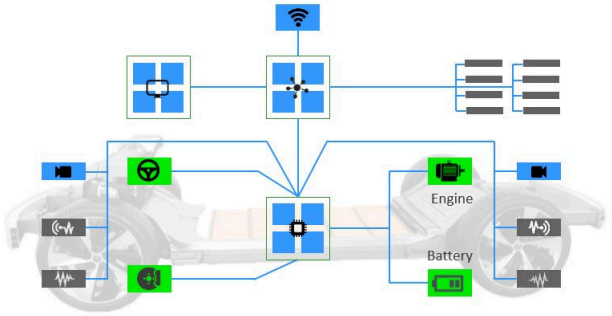
05 Summary

Challenges for OEMs and Automotive Suppliers

Challenges

- Security costs
- Availability of HW/SW security features
- Increasing supply chain interaction
- Managing and securing open source software





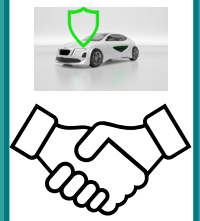
Pressure

- Cybersecurity legislation worldwide
- Privacy protection (e.g. GDPR)
- Unclear distribution of risks
- Financial & brand reputation risks

Compliance with UN R155 by Applying ISO/SAE 21434

UN Regulation No. 155
On Cybersecurity

- Cybersecurity Management System (CSMS) (incl. Obligation to manage supply-chain)
- Requirements for vehicle types approval



ISO/SAE 21434 "Road vehicles – Cybersecurity Engineering"

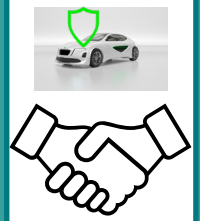
- Baseline for CSMS
- Requirements and recommendation for secure product development

- Enforced in January 2021
- Mandatory for all new vehicle types from July 2022 onwards
- Mandatory for all new vehicles produced from July 2024 onwards.

Compliance with UN R155 by Applying ISO/SAE 21434

UN Regulation No. 155
On Cybersecurity

- Cybersecurity Management System (CSMS) (incl. Obligation to manage supply-chain)
- Requirements for vehicle types approval



ISO/SAE 21434 "Road vehicles – Cybersecurity Engineering"

- Baseline for CSMS
- Requirements and recommendation for secure product development

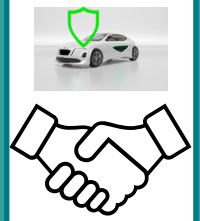
Quantum threat shall be considered in the all-levels to comply with UN R155

Non-compliance → No sales of vehicles in the UNECE member countries

Compliance with UN R155 by Applying ISO/SAE 21434

UN Regulation No. 155
On Cybersecurity

- Cybersecurity Management System (CSMS) (incl. Obligation to manage supply-chain)
- Requirements for vehicle types approval



ISO/SAE 21434 "Road vehicles – Cybersecurity Engineering"

- Baseline for CSMS
- Requirements and recommendation for secure product development

Other Cybersecurity Standards/Regulations in Automotive

VDA QMC ACSMS

ISO/NP PAS 5112 CD Guidelines for auditing Cybersecurity engineering

VDA QMC ASPICE Extension for cybersecurity

UN Regulation 156 on SW updates

ISO 24089 Road vehicles Software update engineering

etc.

PQC in G7 Leaders' Communiqué

> We reaffirm our commitment to the framework of responsible state behaviour in cyberspace, and are working together to develop and implement robust international cyber norms. We are taking steps to strengthen our collective cyber defences, including in response to new and disruptive digital technologies, such as quantum computing, … . We will continue to discuss implementation of international norms and review of lessons-learned from existing efforts to include the attribution of cyber incidents, including by intensifying and elevating our cooperation on cyber within the relevant G7 Working Group. We will also continue to discuss ways to cooperate on emerging technologies, **including new quantum-resistant cryptographic standards.**
>
> **G7 Leaders' Communiqué**
> G7 Germany 2022

How soon should we start worrying?

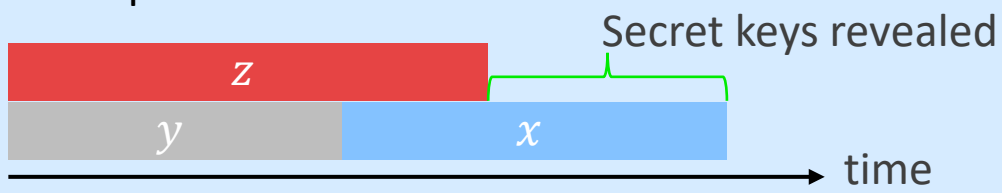
Theorem (Mosca's Inequality). If $x + y > z$, then worry.

Where:

x: security shelf-life

y: migration time (standardization + adoption)

z: collapse time



– $z = ?$:… a $^1/_7$ chance of breaking RSA-2048 by 2026 and a ½ chance by 2031

Challenges for the automotive

- $x + y > z \rightarrow$ vehicles getting on road will be vulnerable after z-time, e.g.
  - $x = 15$ years after SOP
  - $z = 9$ years with probability ½
- Quantum threat might occur in the vehicles produced now

Agenda

01 Motivation

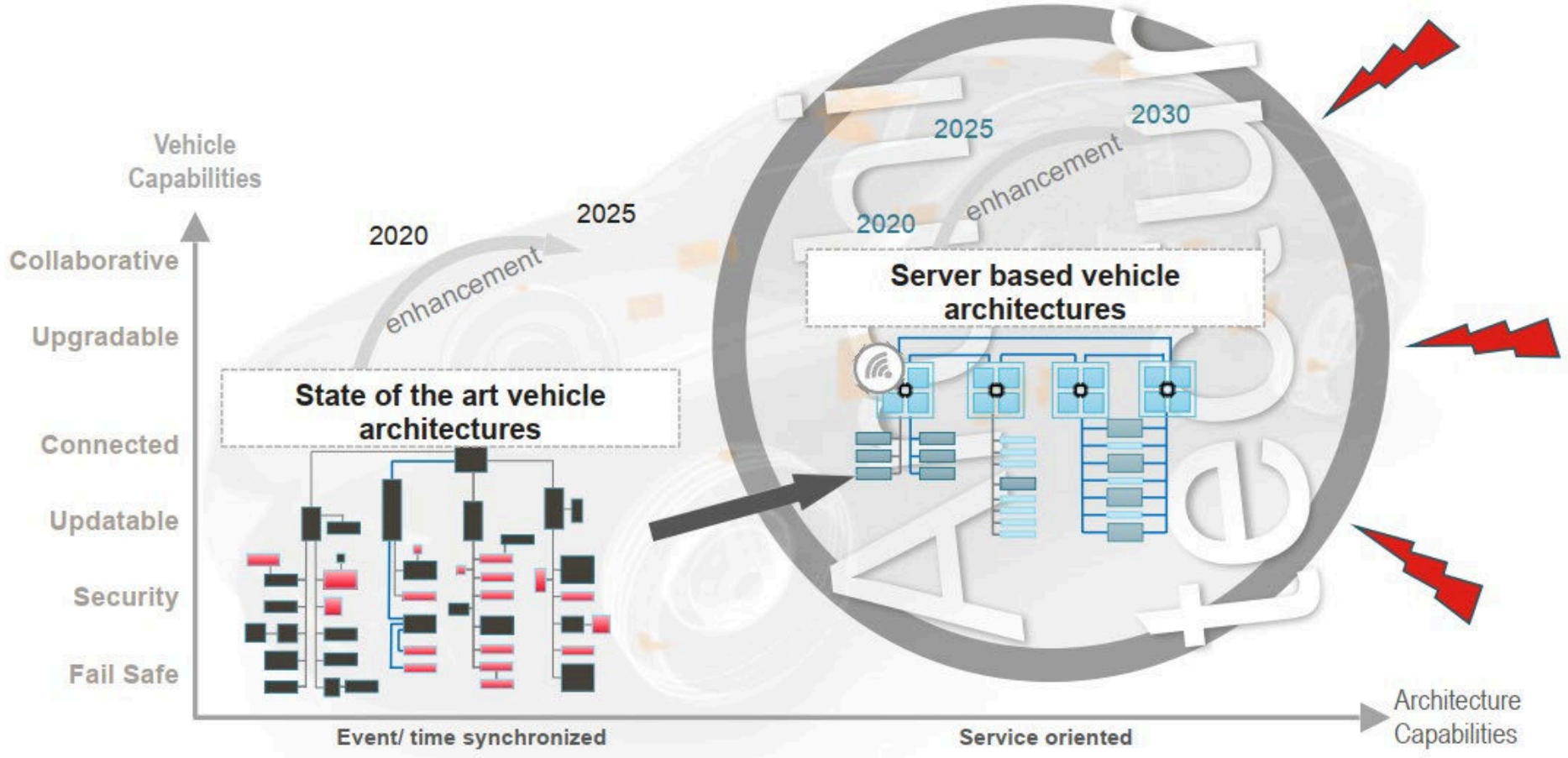
02 Automotive Cybersecurity

03 **PQC Migration Challenges**

04 Demonstrator

05 Summary

Impacted Vehicle Architecture



Migration to PQC

Perform	PQC performance testing in automotive HW/SW platforms
Identify	risk assessment, asset discovery tool– products use-cases
Understand	Requirements from each affected use-case
Select	PQC algorithms that should be supported in crypto-libraries
Adapt/Define	Security concepts (key management, etc.)
Update	The infrastructure in development and production
Establish	Processes and architectures for exchange of crypto systems - crypto agility

Security on Vehicle Level

- Functionality on vehicle level is provided by one or multiple ECUs
- Example Use Cases on vehicle level:
  - V2X communication
  - Feature activation
  - Secure time distribution
  - Session-based secure channel – TLS

Security on Vehicle Level

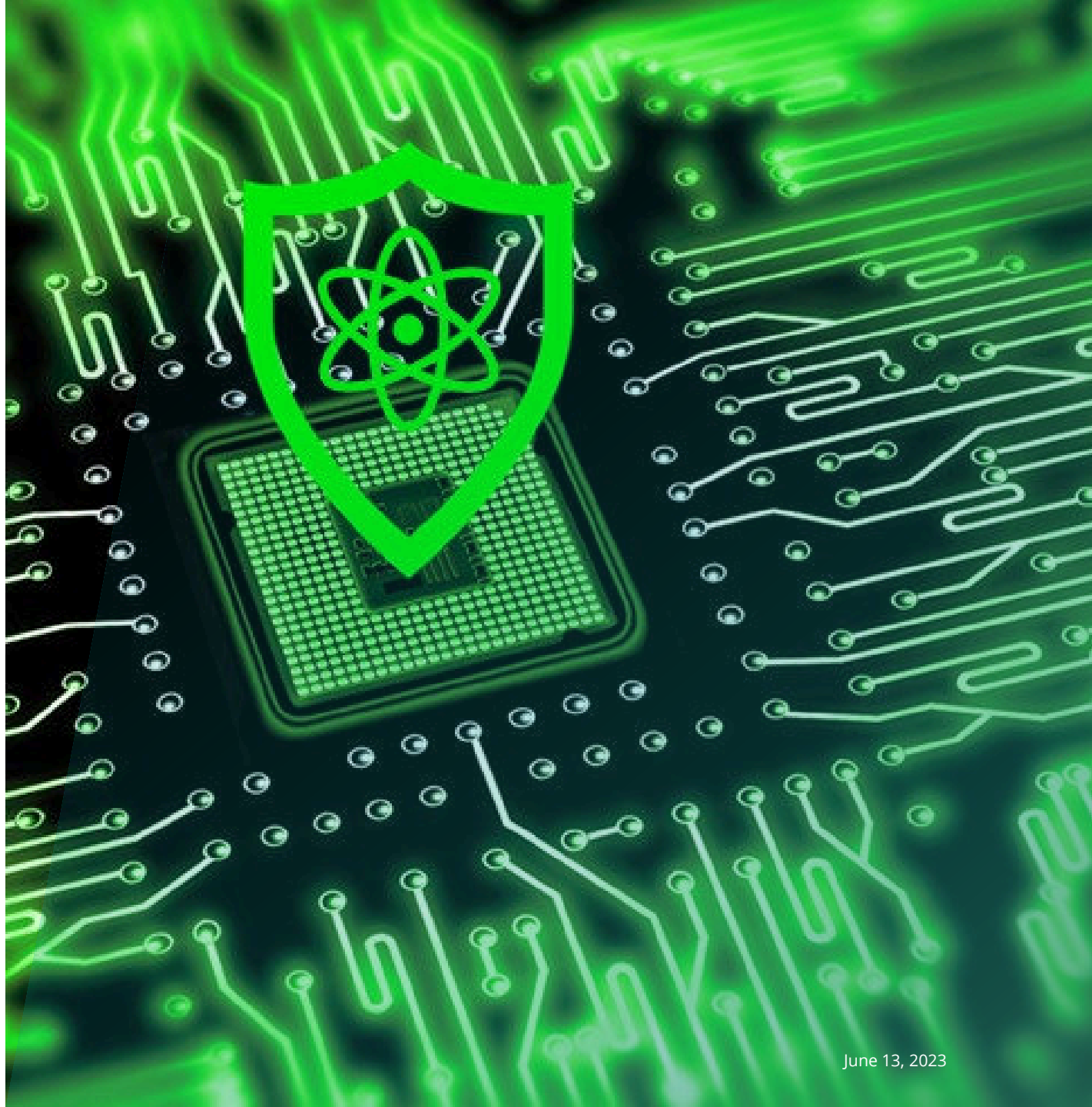
Requirements*	Boundary Values			
	V2V Communication	Feature Activation	Secure Time Distribution	Session-based Secure Channel
Latency	< 10 ms	< 5 s	< 1 s	< 1s : 10 ms
# Execution per lifetime	unlimited	unlimited	unlimited	unlimited
Size of processed data	< 1 MB	< 1MB	< 1 KB	< 1KB : > 1GB
# Key pairs	< 1000	< 10	< 10	< 1000
Life time of signature	< 1 day	< 1 years	< 1 day	< 1 year
RAM	< 1 MB	< 256 KB	< 1 MB	< 1 MB
Storage	< 32 MB	< 4 MB	< 32 MB	< 32 MB

* Requirements for ECU

Source: QuantumRISC – WP1 Use Cases and Requirements

Security on ECU Level

- The aim is to prevent manipulaion or disruption of an ECU
- Example Use Cases on ECU level:
  - Secure software download
  - Secure diagnostic
  - Secure boot
  - Secure onboard communication



Security on ECU Level

Requirements*	Boundary Values			
	Secure Software Download	Secure Diagnostic	Secure Boot	Secure Onboard Communication
Latency	< 5s	< 5s	< 10 ms	< 10 ms
# Execution per lifetime	Limited	Unlimited	unlimited	Unlimited
Size of processed data	< 1KB : > 1GB	< 32B : > 1MB	< 1KB : > 1GB	< 1KB
# Key pairs	< 10	< 10	< 10	< 10
Life time of signature	> 5 years	> 5 years	> 5 years	> 5 years
RAM	< 32 KB	< 32 KB	< 256 KB	< 32 KB
Storage	< 2 MB	< 2 MB	< 4 MB	< 2 MB

* Requirements for ECU

Source: QuantumRISC – WP1 Use Cases and Requirements

Migration Challenges

Practical Challenges

- Large key and signature
- More bandwidth is required due to larger signature size
- *Kyber and Dilithium need both more memory, especially Dilithium has a* high RAM consumption
- PQC algorithms requiring lot of hashing – Hardware accelerated Keccak would speed-up the majority of schemes significantly
- No certified implementations (like FIPS 140-2 for HSM)

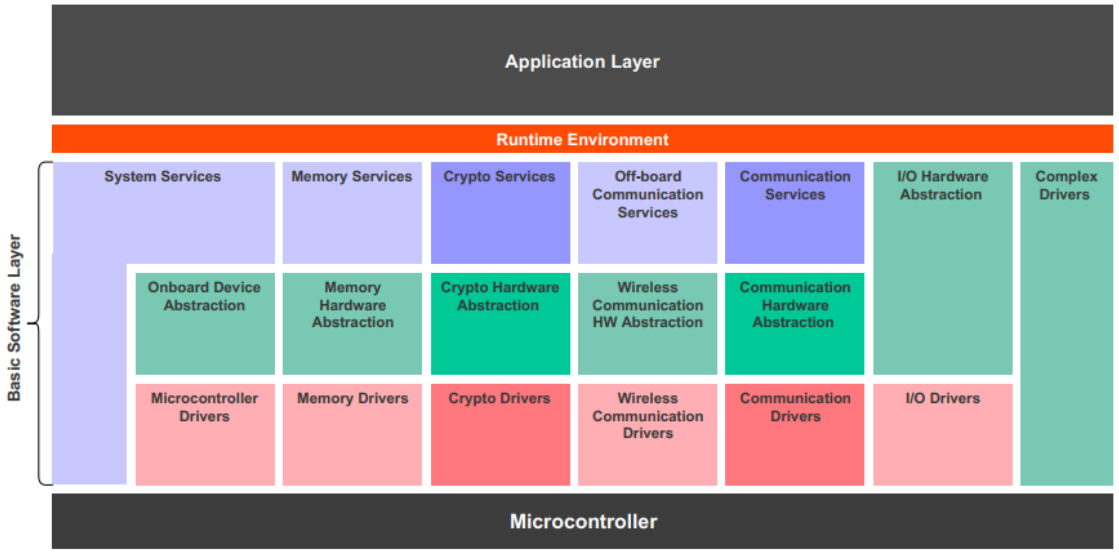
❖ ECUs shall have enough system resources to use PQC

Migration Challenges

AUTOSAR Compliance

- Fulfilling requirements:
  - Only one secondary primitive can be configured
  - Dilithium and Kyber have multiple secondary primitives, that is various hash algorithm.
- Missing specifications:
  - AUTOSAR does not specify how to handle KEMs (key encapsulation mechanism)

❖ Proposals are under discussion to support PQC migration in AUTOSAR



Migration Challenges

Production

- Longer flashing time due to larger keys or signatures
- Longer time for key generation
- Larger storage in Key distribution Manager (KDM)

Agenda

01 Motivation

02 Automotive Cybersecurity

03 PQC Migration Challenges

04 Demonstrator

05 Summary

Post-Quantum Demonstrator

What is the scope?

- Definition of common Automotive Use-cases
- Development of a custom library targeting embedded ECUs containing post-quantum algorithms
- Implementation of the Use-cases in a server-client architecture
- Benchmarking and identification of requirements

What are our use-cases?

- ECU Software Update
- Secure Vehicle Diagnostics
- Secure Channel Establishment

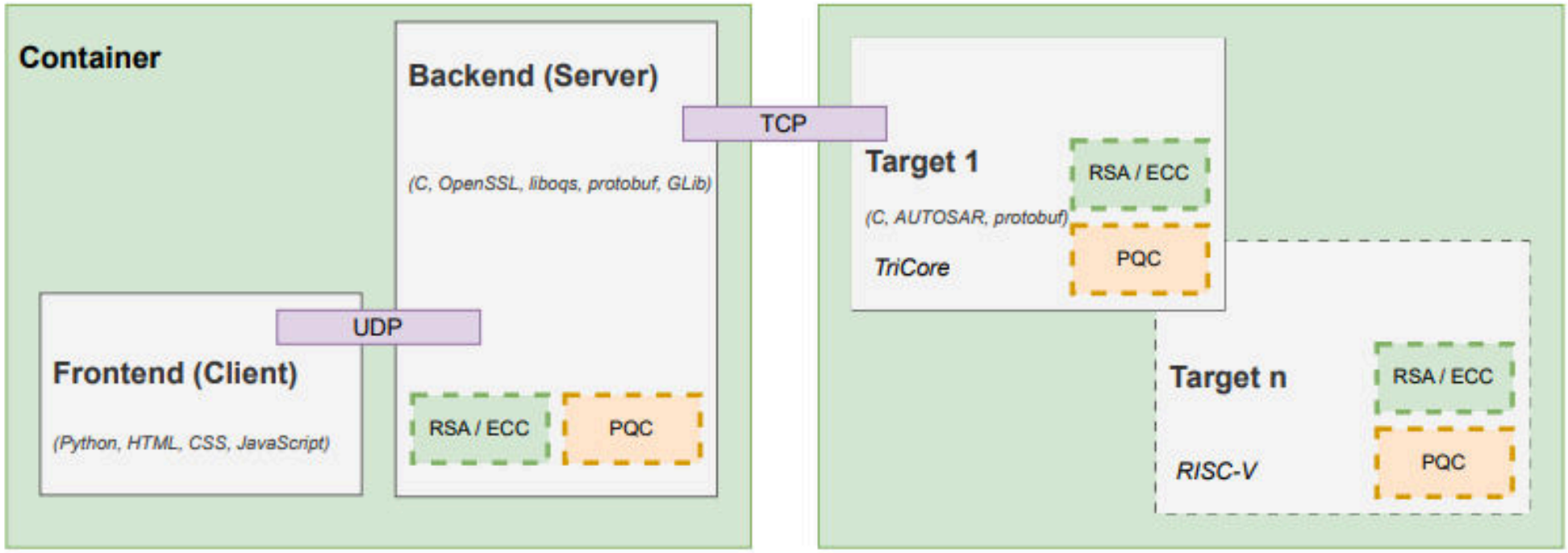
What did we do?

- Implemented the Use-cases in an End-to-End demonstrator
- Developed an AUTOSAR Classic library containing custom implementations of Kyber and Dilithium
- Integrated the library on a 32-bit AURIX™ TriCore™ microcontroller TC38x from Infineon
- Implemented a scalable backend using libOQS

This research work has been partly funded by the German Federal Ministry of Education and Research under the project “QuantumRISC”

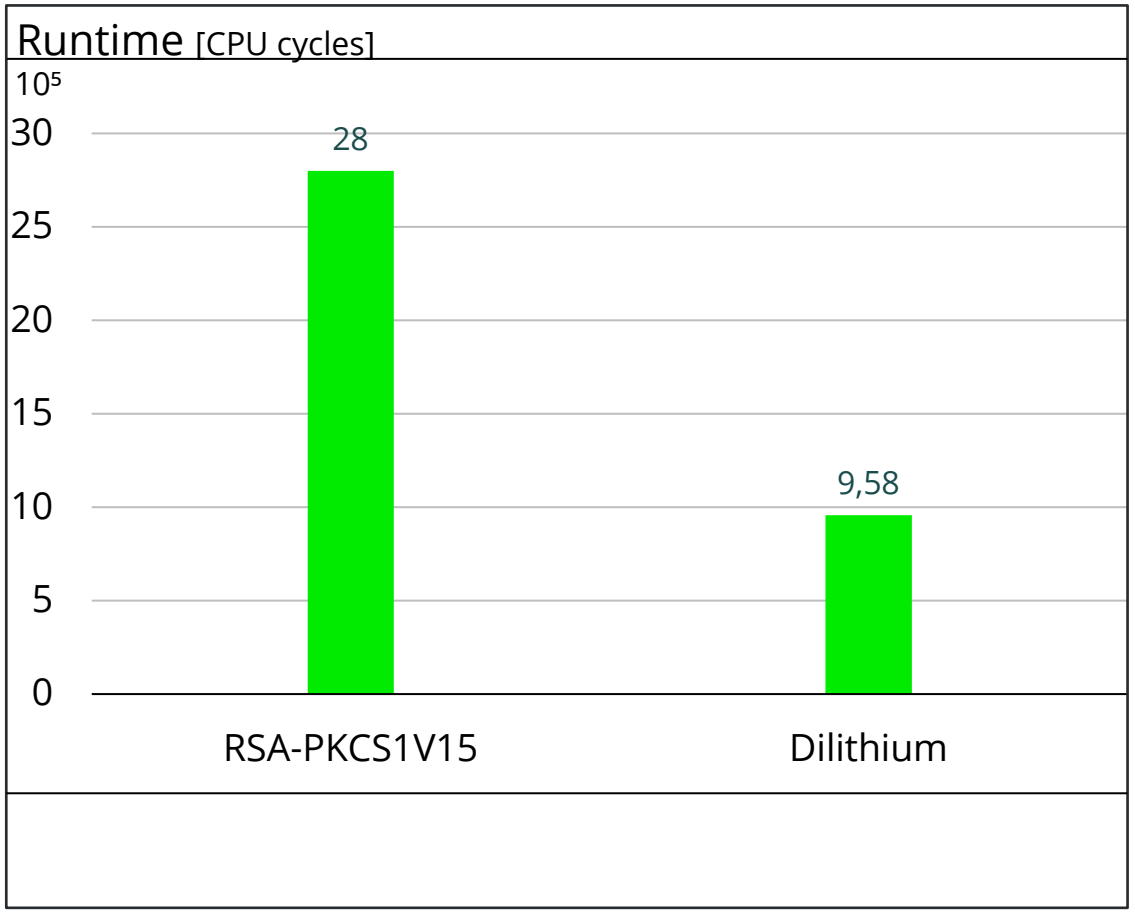
Post-Quantum Demonstrator

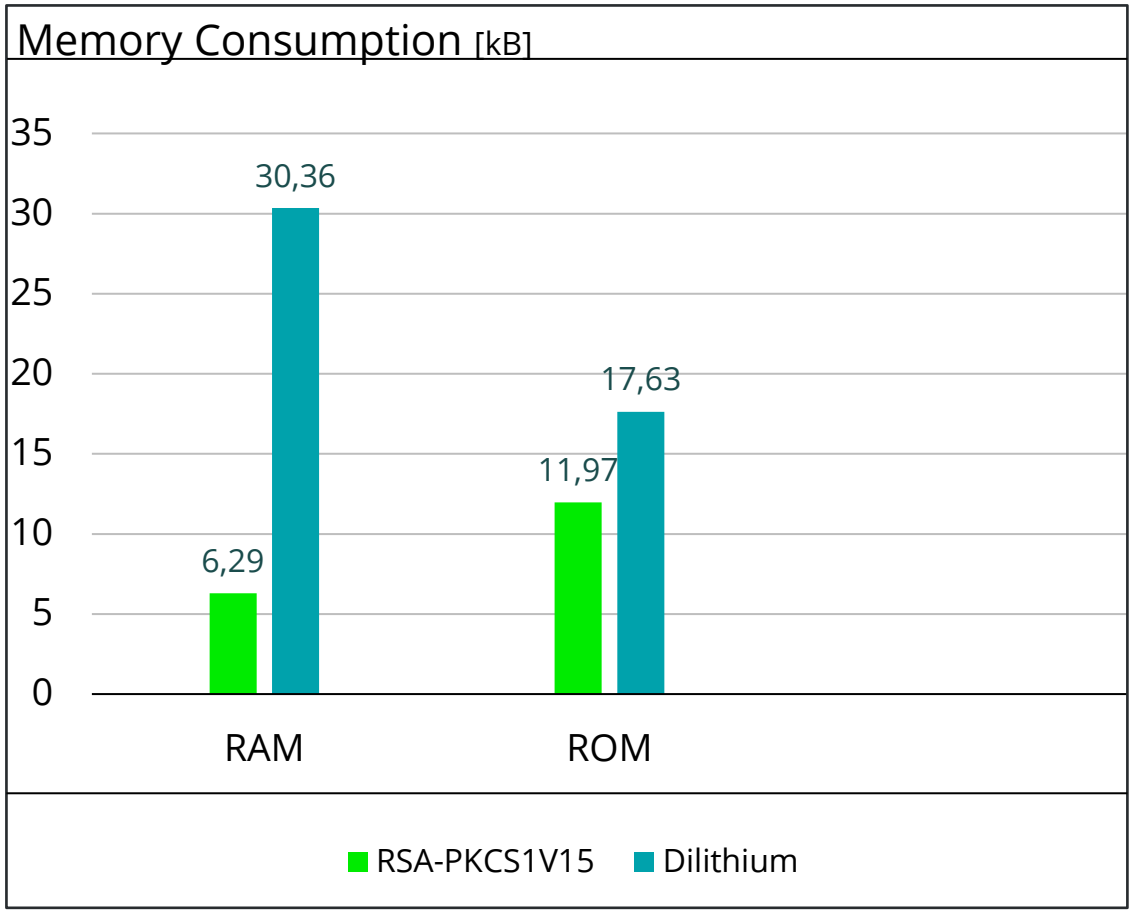
Architecture



Results

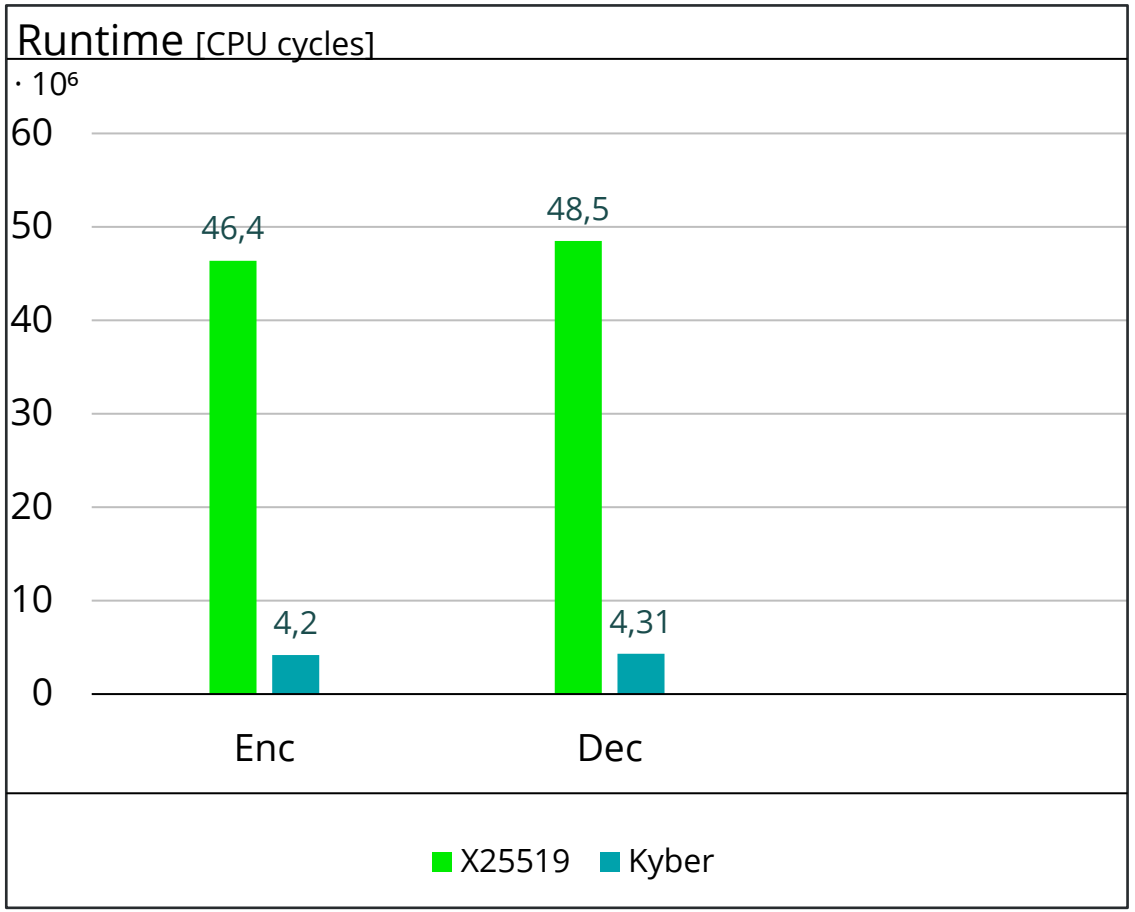
Signature Verification

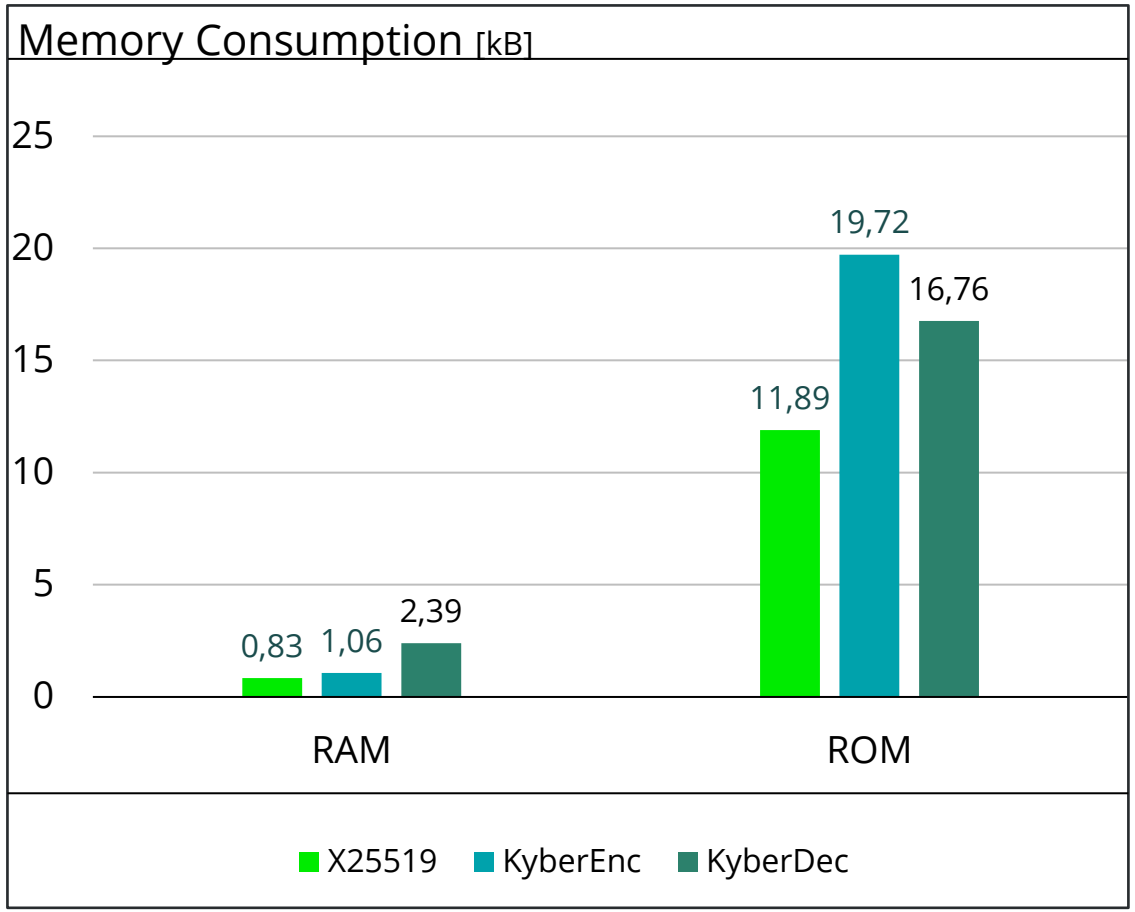




Results

Key Exchange / KEM



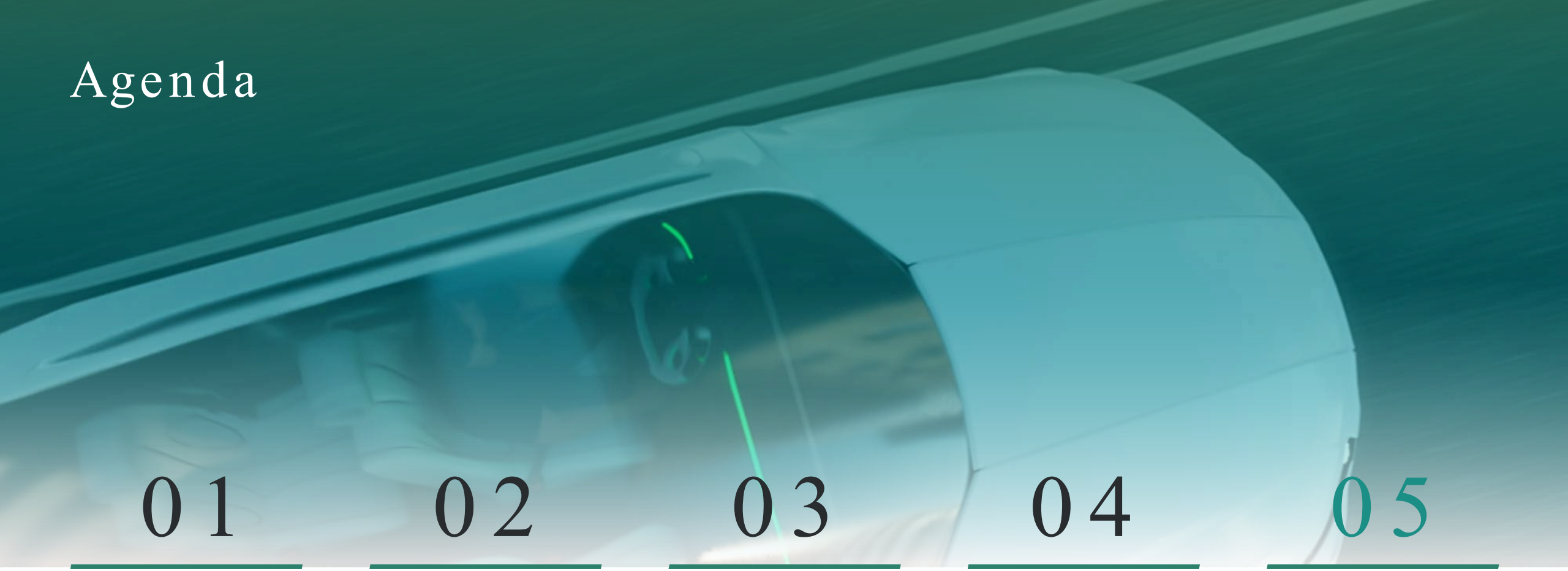


Enc/Dec refers to Encapsulation and Decapsulation case of Kyber, for X25519 it means CalcPubValue and CalcSecret.

Post-Quantum Demonstrator

The numbers shown in this video are preliminary – we are still implementing some improvements and are aware of some inconsistencies we are investigating.

Agenda



01 Motivation

02 Automotive Cybersecurity

03 PQC Migration Challenges

04 Demonstrator

05 **Summary**

Summary

- The migration to PQC is not straightforward since no “one-size-fits-all” solution exists
- Crypto-Agility in the Automotive world is not that easy to achieve due to e.g., processes, hardware constraints, performance and security considerations
- Depending on the use-case, PQC algorithms can be faster than pre-quantum ones while they tend to require more hardware resources (ROM & RAM)
- There is still a risk to go for a full-migration to PQC
  - Hybrid solutions are preferrable

Contact Details

Ayoub Mars

Senior Expert Cybersecurity
Elektrobit Automotive GmbH

ayoub.mars@elektrobit.com

Maurice Heymann

Security & Privacy Researcher
Continental Automotive GmbH

maurice.heymann@continental-corporation.com