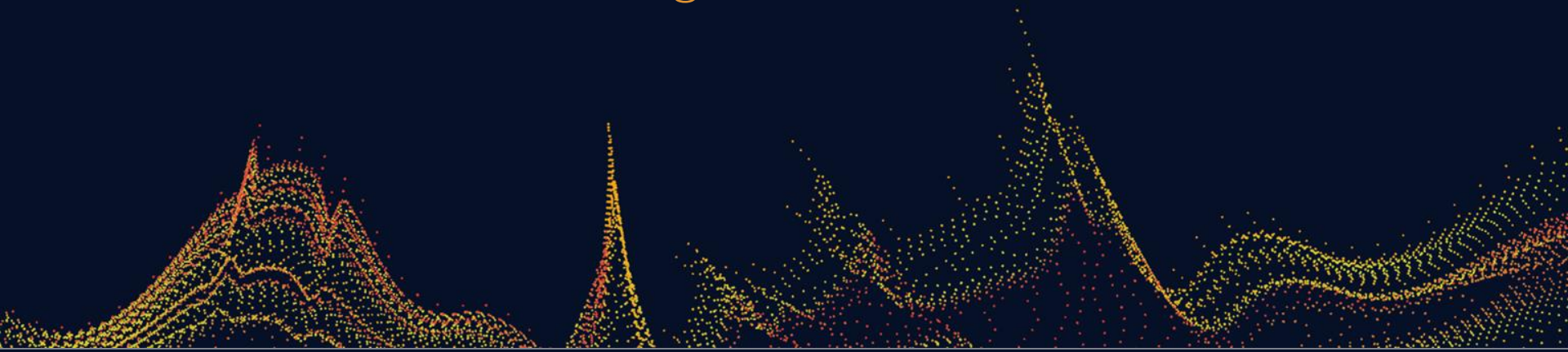
Dr. Axel Y. Poschmann.

PQSHIELD

PQC and Automotive

Challenges and Solutions



Quantum Computers and Cryptography: A very quick primer

0 key
Crypto building blocks

- Hash functions
- TRNGs
- SHA2 + SHA3

Quantum safe

1 key
Symmetric Crypto

- Encryption
- Block ciphers
- Stream Ciphers
- AES

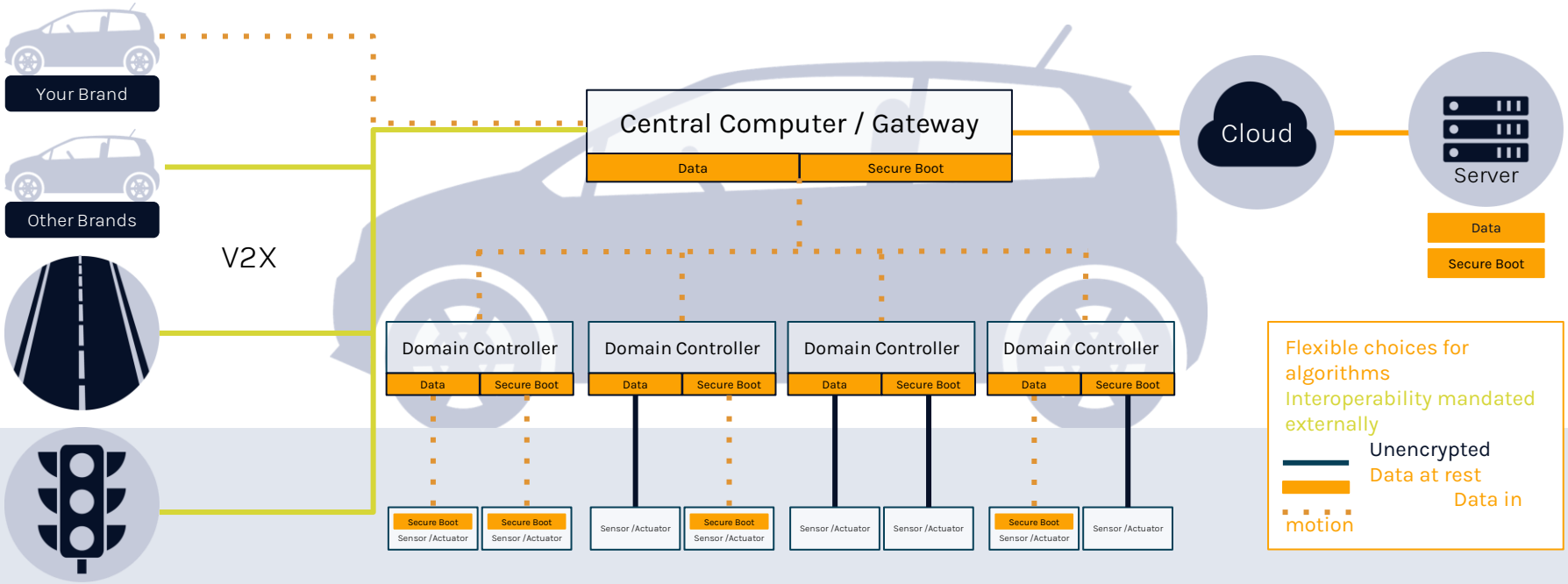
Quantum safe

2 keys
Asymmetric Crypto

- Key establishment
- Digital signature
- RSA and ECC
- DH and ECDH
- DSA and ECDSA

Quantum vulnerable

Where Is Your Crypto: Car E/E Architecture



Where Is Your Crypto: Root, Comms, Data

Root security of each computing device

- Secure boot
- Secure OTA updates
- Secure key management
- Requires dedicated hardware support and cannot be fixed later -> silicon vendors

Secure communications

- On-board, between devices
- To your company cloud servers
- V2X

Secure data storage

- Safety critical data
- Vendor confidential data and sensitive IP
- Car features configuration ->
- User Personally Identifiable Information (PII) -> risk of substantial financial damages

Overview of relevant algorithms : KEM and DSA

Key Encapsulation Methods

NIST

- **ML-KEM / Kyber (NIST Draft FIPS 203)**

Further KEMs

- FrodoKEM (to be ISO standardized)
- Classic McEliece (NIST KEM round 4)
- Bike or HQC (NIST KEM round 4)

Digital Signature Algorithms

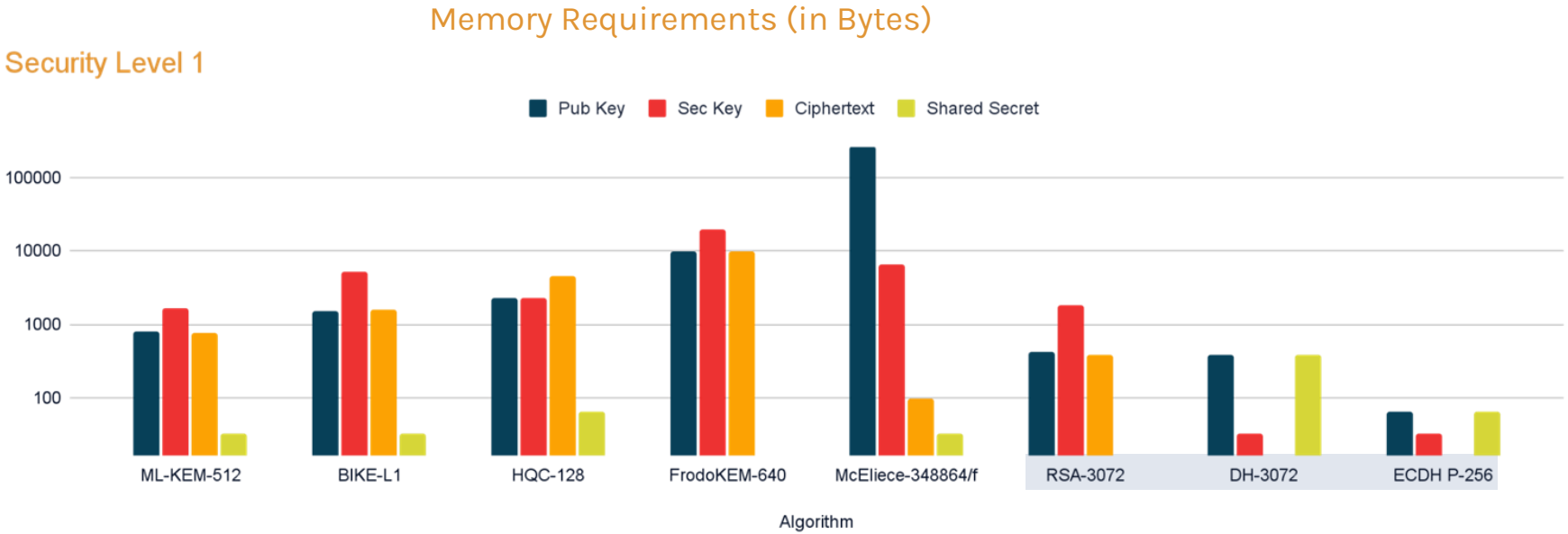
NIST

- **ML-DSA / Dilithium (NIST Draft FIPS 204)**
- **SBH-DSA / Sphincs+ (NIST Draft FIPS 205)**
- **FN-DSA / Falcon (NIST draft FIPS TBD)**

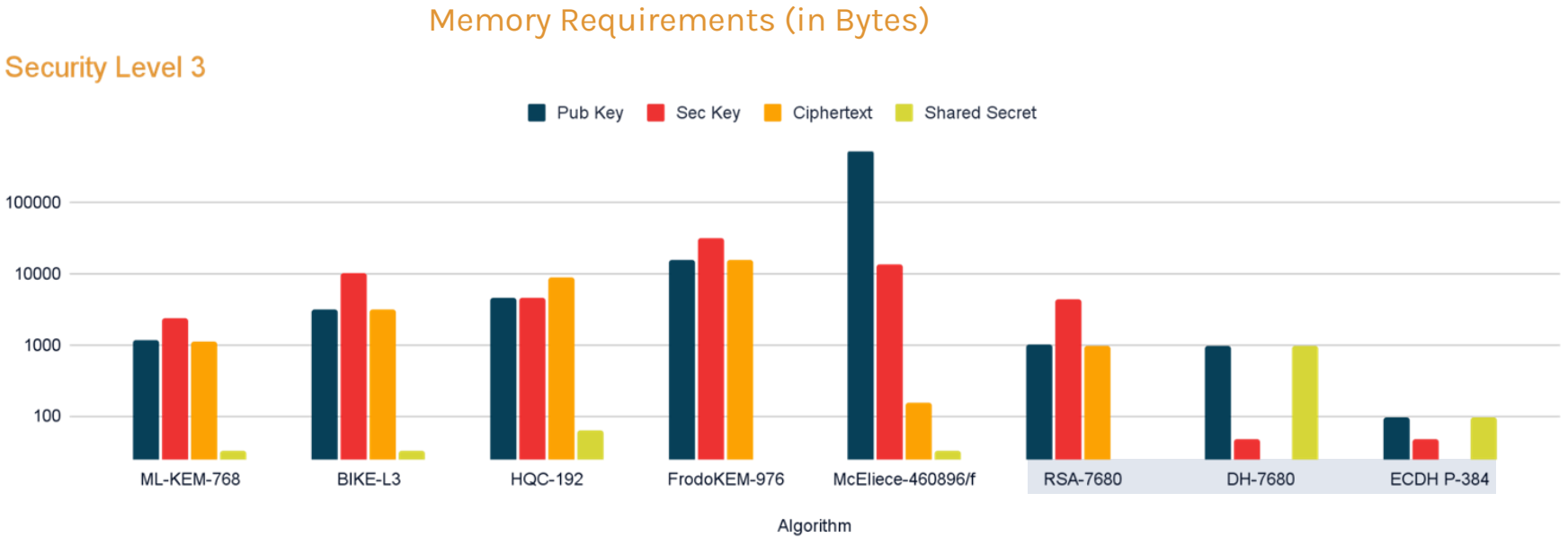
CNSA2.0

- LMS (NIST SP 800-208)
- XMSS (NIST SP 800-208)

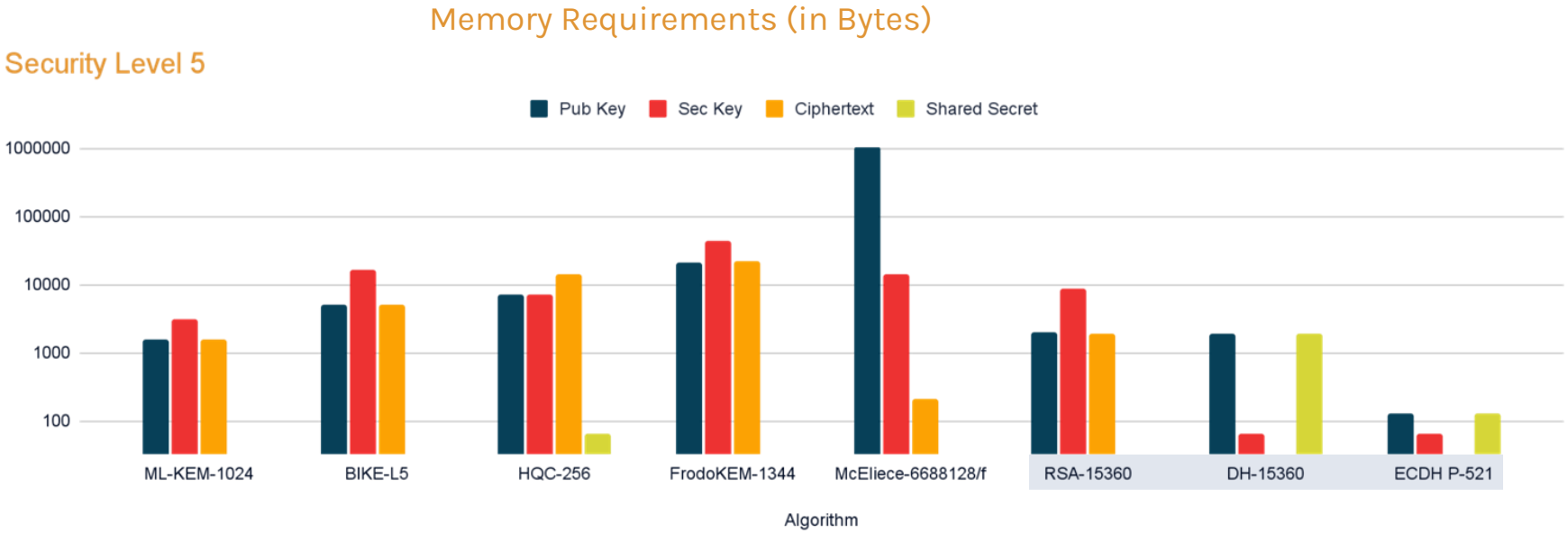
Comparison of key parameters: KEMs



Comparison of key parameters: KEMs



Comparison of key parameters: KEMs

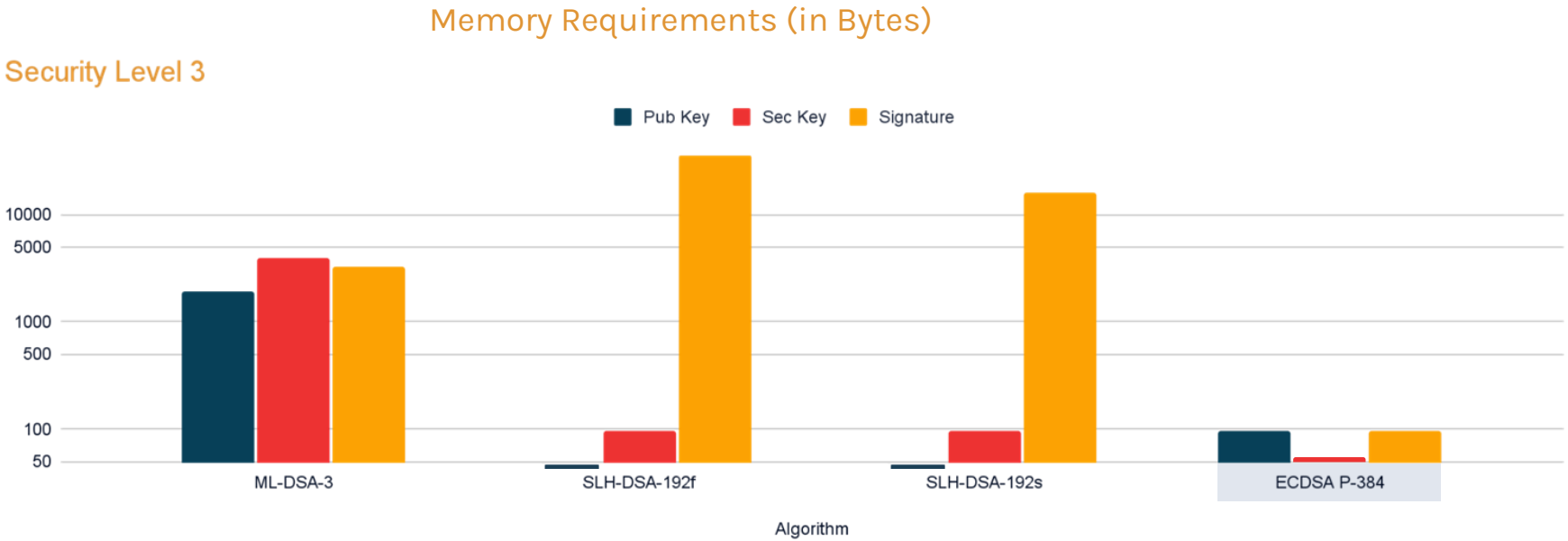


Comparison of key parameters: DSAs

Memory Requirements (in Bytes)

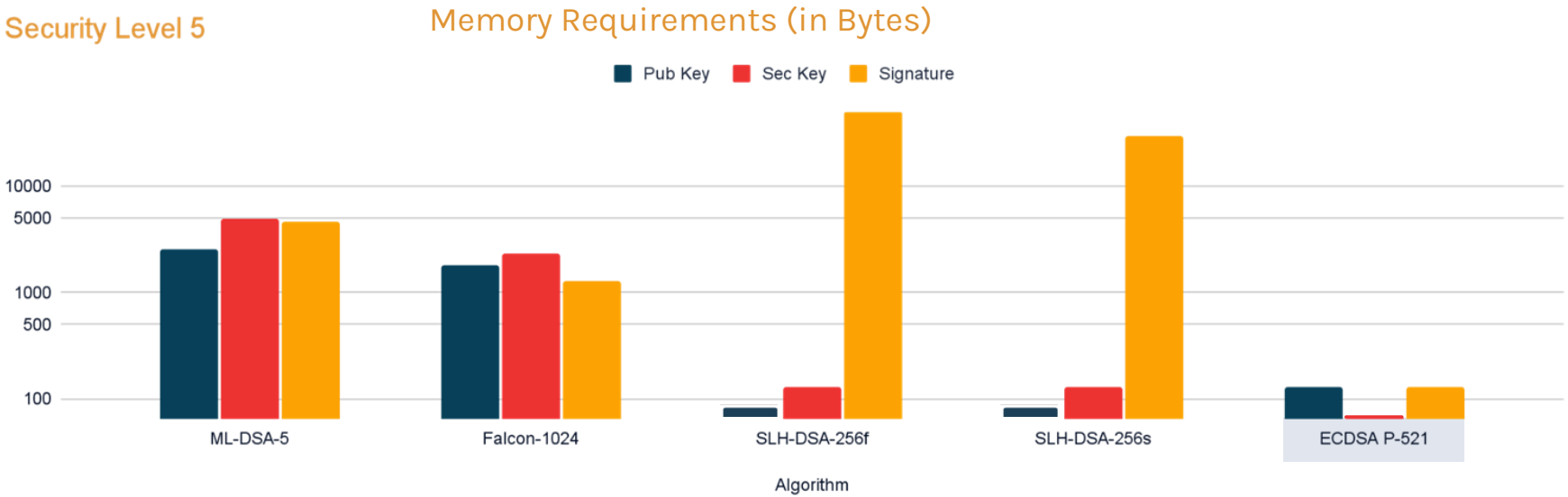
Security Level 1 & 2

Comparison of key parameters: DSAs



Comparison of key parameters: DSAs

Security Level 5



Protectability: Side-Channel

Algorithm	Grade (5= best)	Argument
ML-KEM	2	Many different non-linear operations require many masking gadgets. Powerful chosen ciphertext attacks (decryption failure / plaintext checking oracle) apply to all lattice based KEMs using FO-transform.
FrodoKEM	2	Power of 2 modulus facilitates masking, but masking large matrices requires more resources. Slightly fewer non-linear operations than ML-KEM (no CT compression).
McEliece	3	Seems to resist better to DF-oracle style CCA than lattice based KEMs
ML-DSA	3	Long term secrets are easy to protect, ephemeral secrets involve more complicated operations. Cost of masking could be reduced by using non-deterministic randomness.
FN-DSA	1	Contains floating point operations vulnerable to SCA.
SLH-DSA	5	Due to the structure of HBS, very few SCA attack paths exist.
LMS / XMSS	5	Similar to SLH-DSA, but with a limited number of traces available.

Protectability: Fault Attack

Algorithm	Grade (5= best)	Argument
ML-KEM	3	Chosen ciphertext attacks (decryption failure checking oracle) using fault injection during re-encryption.
FrodoKEM	2	Vulnerable to the same CC attacks as ML-KEM, but recomputation countermeasures are more expensive.
McEliece	3	Better resistance against CCA, but more complicated decoding increases attack surface.
ML-DSA	3	Protection against loop-abort attacks required. Full signature recomputation has relatively low performance cost due to rejection sampling.
FN-DSA	?	?
SLH-DSA	1	FA forcing multiple uses of WOTS scheme.
LMS / XMSS	1	Similar to SLH-DSA but with a limited number of faults.

Decision Criteria: Algorithm Selection

Costs

Hardware, software, bandwidth, management

Compatibility

- **Car internal** communication: Freedom of choice within the capabilities of the components
- Communication with **own servers** and own cars: Freedom of choice, low hanging fruit
- Communication with **other cars and road infrastructure**: Compliance with standards
- If hardware has already been selected: Compatibility with selected hardware

Regulations and Standards

- May **vary** between countries / markets
- May **change** over time

Urgency and criticality

- **Risk analysis**: What could happen when data is changed or leaked?
- There is no **safety** without security
- A **crypto agile** design allows later crypto upgrades
- **Boot security** requires dedicated hardware support and cannot be fixed later
- **SCA resistance**

Conclusion: Challenges and light ahead

Security, including resistance against quantum computers, will affect costs, but

- Considering it and designing it in from the very beginning has the lowest total costs
- Having to bolt it on later will be more expensive, whilst typically less secure
- With today's highly computerized cars, security breaches can also break safety
- Major security incidents and/or product recalls have the highest costs
- A proper risk analysis will make the business case
- **Only asymmetric crypto needs to be updated**

Timing: No reason to panic, but also no time to waste

- The Q-Day, when quantum computers will break today's crypto, is expected in 5…15 year from now
- Cars have a long lifetime, in Germany typically 14 to 26 (!) years*
- New cars designed today will probably become threatened by quantum computer attacks later in their lifecycle
- New cars should be designed at least crypto agile, better already quantum safe

*Source: https://de.statista.com/statistik/daten/studie/316498/umfrage/lebensdauer-von-autos-deutschland/

Conclusion: Challenges and light ahead

Standards and legislations

- Standards and legislation are still in development
- Different jurisdictions desire different algorithms (US, EU, CN)
- The requirement for PQC will come, the standardization is on the way, the NIST PQC Draft standard is here
- Crypto agility will allow ongoing compliance

Legacy support

- For some time, classic crypto will still be required for legacy compatibility
- The industry offers classic + PQC crypto libraries

The time to start working on the transition to PQC is NOW

- Start a risk analysis, including the CFO and CISO, to create a business case and get an appropriate budget
- Get experience on how to transition to PQC, best with PoCs
- A massive push should go towards silicon vendors to include PQC crypto in new devices ASAP. But don't just wait on them.

Dr. Axel Y. Poschmann
axel.poschmann@pqshield.com
www.linkedin.com/in/dr-axel-york-poschmann
X @stylenerd

PQSHIELD

Thank you for your attention!

Dr. Axel Y. Poschmann

axel.poschmann@pqshield.com | www.linkedin.com/in/dr-axel-york-poschmann | X @stylenerd