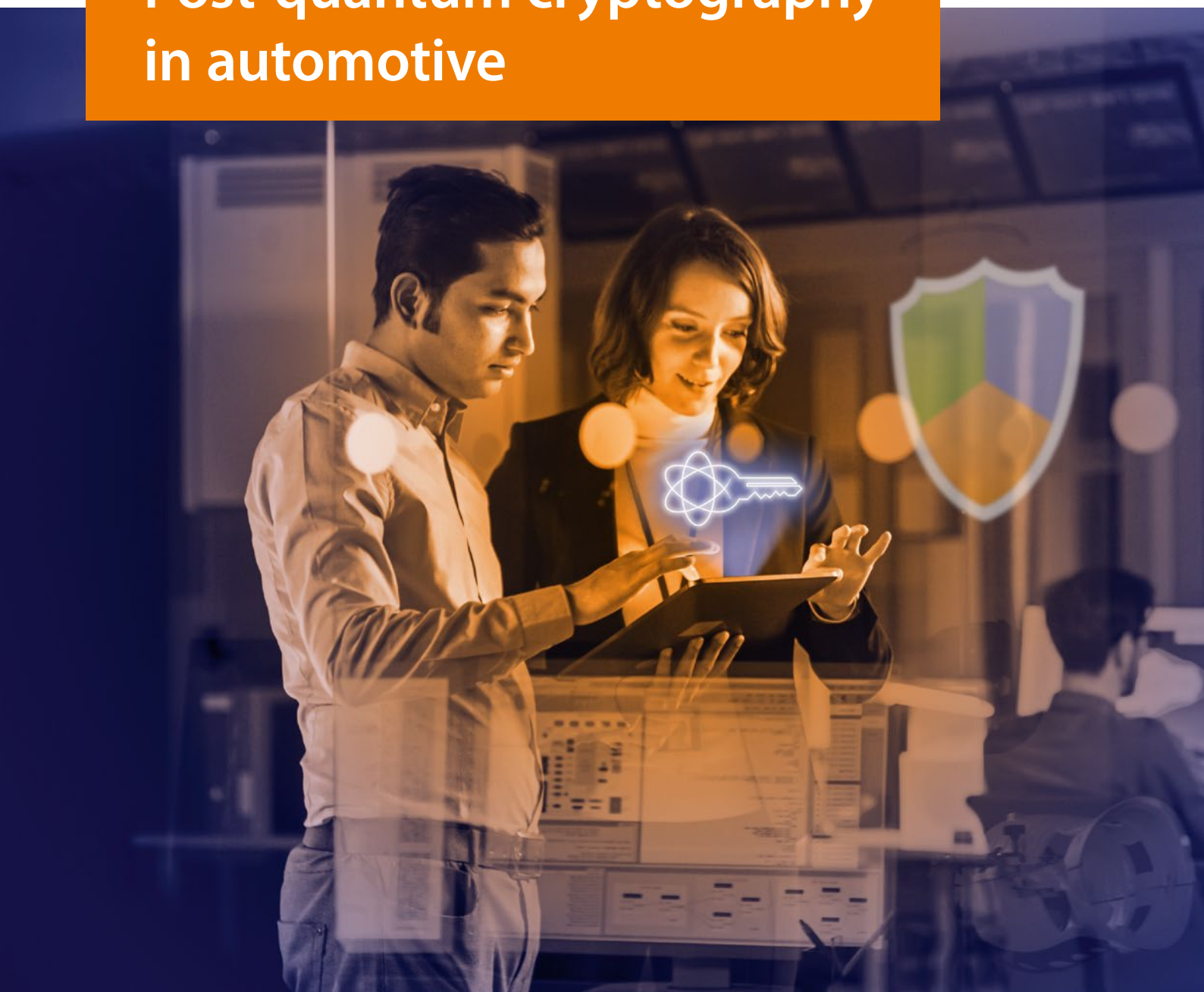
escrypt

SECURITY. TRUST. SUCCESS.

Whitepaper

Future challenges and possible solutions

Post-quantum cryptography in automotive



Digital signatures and certificates play a great role in securing the connected world, but the cryptographic algorithms they rely on will soon be in danger by quantum computers. Various alternative algorithms have been developed and are being scrutinized by the cryptographic community, all of which pose different challenges, regarding the required resources or the achieved security. In this presentation, we focus on the role of asymmetric cryptography for the IT security of automotive systems. We shortly present the status of post-quantum cryptography and discuss the challenges that future automotive systems face as well as possible solutions to these problems.

Table of contents

Public key cryptography and the threat of quantum computers

Digital Signatures using asymmetric cryptography are nowadays an inherent part of applications in the embedded systems and the automotive industry. Applications such as secure over-the-air updates (SOTA), Car-to-Car and Car-to-X communication and secure diagnostics are only some examples, which highlight the importance of establishing a secure communication channel and ensuring the messages are issued by a trusted sender (for example, the unit-manufacturer or a verified diagnostic tester) and have not been modified.

A typical way of binding the identities of the communicating entities to the corresponding public keys is by using digital certificates. These are issued by corresponding authorities, which are parts of a common Public Key Infrastructure (PKI). Car manufacturers (Original Equipment Manufacturers - OEMs) nowadays operate individual PKIs, with different entities responsible for multiple use cases (for example diagnostics, testing and production), which might depend on a common or distinct Root certification authorities, i.e. Root CA(s). Security in these cases depends upon the security of well-known algorithms, such as RSA, ECDSA and ECDH for signing and key generation. These in turn depend on hard mathematical problems, namely prime factorization and solving discrete logarithms on elliptic curves.

Developments in the field of quantum computing have however shown that there is an increasing need for revising the algorithms used for digital signatures and key establishment, while symmetric block algorithms are still considered secure. Indeed, Grover's algorithm (1996) [4] improves brute-force algorithms that check every possible key, providing a quadratic speedup. This means that for example a brute-force attack on AES-128 with a cost of at most 2128 AES-operations on a classical computing system can be finished with about 264AES-operations on a quantum computer.

Shor however provided an algorithm [6, 7], which solves integer factorization and discrete logarithms in polynomial time on a quantum computer. Although there is still a lot of progress to be made in the development of such computers, the time needed for finding suitable solutions and implementing them in fields like the automotive industry makes the transition to a quantum-world a very real and urgent matter. As per the often cited theorem of M. Mosca [5] : if the time needed for migrating to new solutions added to the time one product needs to be secure is greater than the time needed to compromise its security, then action has to be taken.

Post-quantum algorithms

The cryptographic community has already considered this and there are already various standardization activities taking place, most notably the NIST post-quantum algorithm competition. The quantum-secure algorithms submitted to the NIST competition fall into five categories, according to the problem they are based on:

- Hash based signature schemes: relying on the security of the chosen hash function.
- Isogeny based: relying on the difficult mathematical problem of finding isogenies between special elliptic curves (SIDH/SIKE).
- Lattice based: relying on the shortest vector problem and learning with errors problem.
- Code based: the security of such systems is based on the hardness of inverting a random linear code.
- Multivariate equations based: the security of these systems is based on the fact that solving multivariate quadratic systems of equations over finite fields is NP-hard.

As part of the NIST competition different algorithms will be chosen for signature generation and key establishment in the next couple of years. As recently as July 2020, this competition entered its third round [3], which includes seven "finalist"-algorithms, which will be considered for standardization in the next two years, and eight "alternate" algorithms, which may be standardized in the non-immediate future.

In the process of identifying suitable algorithms for all the relevant use cases in the automotive industry, there are different problems that have to be taken into consideration. One of them is related to resource constraints: many of the proposed schemes that are considered secure produce very large signatures or require very large key pairs, that would be not suited to be used in resource-constrained ECUs (electronic control units), which possess a limited amount of secure memory and computation resources. Especially for use cases with strict timing requirements (for example Car-to-Car communication), the selection of post-quantum algorithms is a challenge. See for example Table 1 some key sizes recommended for four algorithms that were considered in the second round of the NIST competition.

Future challenges for the automotive industry

Many different issues need to be considered even after suitable quantum-secure algorithms are chosen:

- Enable a smooth transition from current systems to quantum-secure ones. For critical use cases, like online firmware updates, many ECUs in the field should be able to establish a secure connection to the OEM Backend, without big interruptions.
- Cryptographic agility: ensure flexibility on the choice of algorithms, use case or security-level specific. The integrity of algorithm selection needs to be in turn ensured (protection against downgrade attacks), while in field updates of the used algorithms and parameters, e.g. the key lengths of the symmetric keys used, would ideally be made possible in the near future.
- Address performance restrictions by taking advantage of or extending hardware acceleration solutions.
- Reconsider and redesign the used protocols (for example, quantum cryptography adjusted TLS). The communication protocols used should for example be able to handle larger certificates and keys (for example for diagnosis).
- Restructure the respective PKIs and focus on lightweight certificates for embedded systems. Special care to ensure a smooth migration to the new PKIs needs to be taken.
- Redesign of key and certificate management, to account for the transition period.
- Develop suitable hardware security solutions.

Signature Scheme	Private key	Public key	Signature
qTesla p-III(lattice)	12.39 KB	38.43 KB	5.66 KB
Crystals Dilithium (lattice)	3.86 KB	1.76 KB	3.37 KB
SPHINCS+ - SHA192 (hash-based)	96 B	48 B	17.06 KB
GeMSS192 (multivariate)	24 B	1.24 MB	51 B

Table 1. Example key sizes for some NIST round 2 PQ-signatures schemes, security greater than or equivalent to 174 bits

Ensuring a smooth transition to the post-quantum world

We would now like to focus on some ideas regarding the preparation needed for the post-quantum transition, from the point of view of ECU-development. As discussed before, use cases that use asymmetric cryptography are the most critical and one can assume that the symmetric keys currently in use are secure enough (merely doubling the key-length would suffice for block algorithms like AES).

First, one can assume the ECU has a unique identification and possesses ECU-specific asymmetric keys. Those can either be injected during the production or can be generated inside the ECU by using a secret known to the ECU and the Backend of the OEM or Tier 1. Handling those secrets of course requires a centralized key management and ideally the use a hardware security module (e.g. a HSM or a TPM) as a trust anchor. These symmetric keys, present in all ECUs could be used to established a secure connection to the OEM Backend, while in the field. This communication path can then be used for a secure firmware update, which could even update the cryptographic libraries used by the ECUs, even in the worst case of asymmetric cryptography being already broken.

In this scenario, the OEM would be required to trigger certificate revocation, so that old broken certificates are not used for unauthorized firmware updates. A connection with pre-shared keys can be established with the Backend. Then an emergency firmware-update or an update of the crypto-library firmware should be triggered. Of course, this requires the possibility of such firmware updates and the existence of already prepared alternative solutions. If an attacker that can already forge the OEM Root signature uses it to perform firmware updates, before the OEM certificate has been revoked, this could lead to a catastrophic scenario for the OEM.

A way to prevent this scenario is "crypto agility by design": that is, if the OEMs already start preparing for a transition long before the asymmetric algorithms in use can be broken. As a first step, OEMs can take advantage of the centralized architecture (domain or zone-based architecture) that is prevalent nowadays and focus on making the connected and less resource-constraint Gateway ECU(s) "quantum-enabled" as a first step. This would ease the constraints posed by the high computational resources needed by most of the post-quantum algorithms, with respect to RSA and elliptic curve cryptography. Enabling the use of post-quantum algorithms in these gateway ECUs is an important first step towards securing the whole architecture.

In the case of a smooth transition, OEMs can use the still valid classic certificates to force secure online firmware updates to these ECUs, which would make them post-quantum "enabled". The development of cryptographic libraries and solutions that can support this kind of updates would make this step much easier. One possibility to be considered in this case is including some already well-understood and standardized post-quantum alternatives in the next generations of cryptographic libraries (see for example XMSS [2], [1]). Redesigning the used digital certificates and the respective PKIs, as well as planning for and reserving the necessary resources (RAM/ROM consumption, key and certificate sizes) at an early design phase of the ECUs, are both also of great importance.

What would happen however with ECUs not suitable to handle post-quantum algorithms at all? The OEM PKI could handle this by issuing different certificates in parallel (classical and post-quantum), with only the new ECUs being able to handle the PQ Signatures. Older ECUs could use the classical certificates either while they are still valid and be forced to only get updates in a controlled repair-shop environment, once classical certificates get revoked.

Another solution for this "transition phase" would be a hybrid PKI, issuing certificates for all ECUs. Every end-entity can then choose to verify the classical or post-quantum signatures according to their capabilities. Non post-quantum enabled ECUs should not however pose a threat for the whole architecture. In order to ensure this, additional security measures are needed to be implemented on the vehicle network, for example domain isolation, Intrusion Detection (and Prevention) Systems ID(P)S should be considered already in an early stage of architectural design.

Conclusion

In conclusion, the technological transformation originating from the eve of quantum computers poses a variety of challenges and risks for the automotive industry. Tackling these challenges requires a lot of preparation and careful ECU-design decisions by the OEMs. ESCRYPT is already working on all these challenges and engages in the development of a quantum computer-resistant public key infrastructure (PKI) as part of the research project FLOQI, which is funded by the German Federal Ministry of Education and Research.

The goals of the FLOQI project include the specification of a PKI supporting both classical and quantum-computer-resistant algorithms and the choice of signature and key agreement algorithms suitable for use-cases in the automotive industry, the financial sector, e-governance and Industry 4.0.

To guide customers though future quantum challenges, ESCRYPT offers post-quantum consulting as an expert consulting service. ESCRYPT supports its customers to fully understand the challenge, identify action items, and develop quantum-secure systems. The service encompasses workshops, management trainings, analyses, the design of migration and transition solutions and guidance on roadmaps and specific tasks, depending on the needs of each customer. With the product CycurLIB ESCRYPT is already offering a cryptographic library which features post-quantum secure algorithms.

References

[1] Andreas Huelsing et al. XMSS: eXtended Merkle Signature Scheme. RFC 8391, May 2018.

[2] David A. Cooper et al. Recommendation for stateful hash-based signature schemes. Technical report, October 2020.

[3] Dustin Moody et al. Status report on the second round of the NIST post-quantum cryptography standardization process. Technical report, July 2020.

[4] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, pages 212 – 219, New York, NY, USA, 1996. Association for Computing Machinery.

[5] Michele Mosca. Cybersecurity in an era with quantum computers. IEEE Security & Privacy, 16:38–41, 2018.

[6] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, SFCS '94, pages 124 – 134, USA, 1994. IEEE Computer Society.

[7] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5):1484 – 1509, October 1997.

Contact

Dr. Efstathia Katsigianni
Security Consultant
Efstathia.Katsigianni@escrypt.com
Telephone +49 30 40369-1958

ESCRYPT GmbH
Wittener Straße 45
44789 Bochum, Germany
Telephone +49 234 43870-200
info@escrypt.com

www.escrypt.com

Dr. Alexandre Berthold
Expert (technical and organizational information privacy)*

Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow
poststelle@lda-brandenburg.de

www.lda.brandenburg.de

* The opinion expressed here by the author is independent of the state commissioner or department.

Status: 01/2021