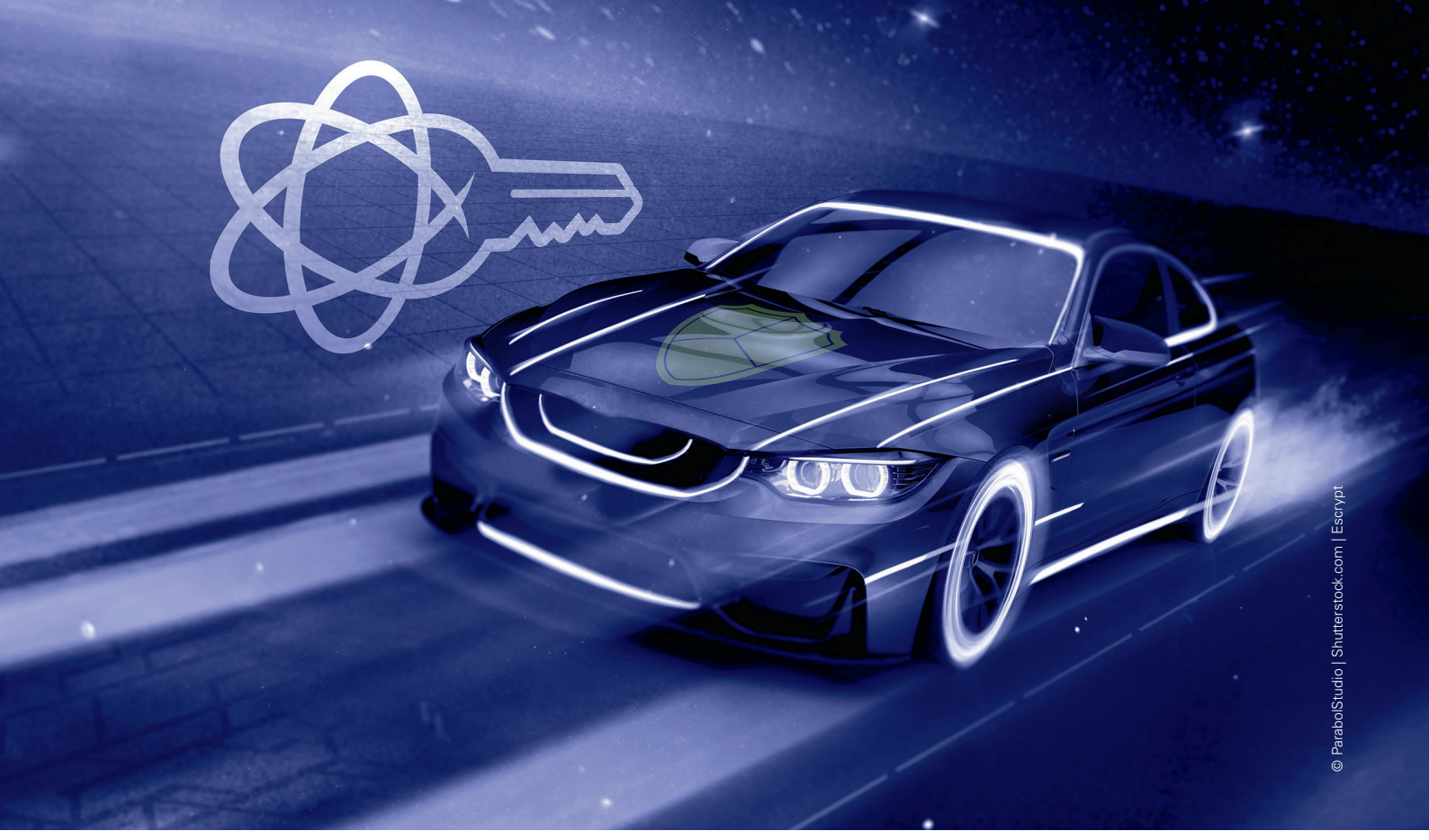

VERNETZTE FAHRZEUGE VOR CYBERANGRIFFEN SCHÜTZEN

Die **Post-Quantum**-Challenge

Quantencomputer gelten als nächste Revolution in der Informationstechnik. Noch sind die Rechnersysteme, die mithilfe von Quantentechnologie heutige Cybersecurity-Mechanismen spielend überwinden, nicht verfügbar. Doch jetzige Fahrzeuge sind mindestens 15 Jahre und länger auf der Straße. Wie lassen sich diese gegen mögliche künftigen Cyberattacken aus dem Quantencomputer wappnen? Den Anfang machen erste Post-Quantum Algorithmen in Automotive-spezifischen Krypto-Bibliotheken.

Die Absicherung von vernetzten Fahrzeugen und Fahrzeugsystemen gegen Cyberangriffe, Manipulation und unerlaubten Zugriff ist bekanntermaßen Grundvoraussetzung für ihre Funktions- und Verkehrssicherheit. Die vernetzte Mobilität der nahen Zukunft ist ohne Cybersecurity schlichtweg nicht denkbar. Neue Regularien und Standards wie die UN R155 oder die ISO/SAE 21434 sowie zunehmende Anstrengungen der Autohersteller hin zu Security by Design, wirksameren Security-Funktionen im Fahrzeug und kontinuierlichem Risikomanagement belegen das.

Asymmetrische Kryptografie versus Quantenmechanik

Die Cybersicherheit im und um das Fahrzeug wird heute vornehmlich mithilfe digitaler Signaturen und Zertifikate gewährleistet. Diese werden mittels asymmetrischer Algorithmen erstellt, die dementsprechend heute in vielen eingebetteten Systemen im Fahrzeug zur Anwendung kommen. So werden zum Beispiel Over-the-air-Updates (OTA), V2X-Kommunikation und sichere Diagnoseschnittstellen per asymmetrischer Kryptografie vor unerlaubten Zugriff geschützt. Nicht minder wichtig, beispielsweise für die TLS-Kommunikation, ist die Public-Key-Verschlüsselung. Signatur und Schlüsselgenerierung erfolgen dabei über bekannte Algorithmen wie RSA, ECDSA und ECDH, die auf mathematische Problemstellungen, die Primfaktorzerlegung und die Lösung diskreter Logarithmen auf elliptischen Kurven, zurückgreifen. Diese kryptografischen Hürden sind für herkömmliche Computer mit vertretbarem Aufwand nicht zu überwinden (Bild 1).

Quantenalgorithmen indes sind heute bereits in der Lage diese klassischen asymmetrischen Algorithmen zu knacken. Die gute Nachricht: Noch fehlt es

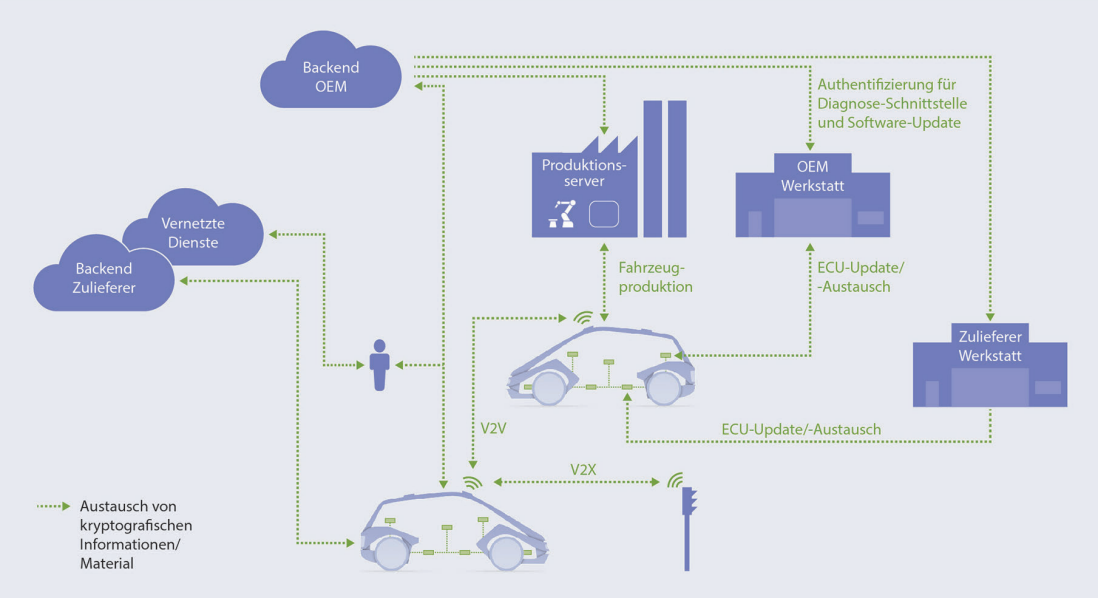

Bild 1: Fahrzeuge sind künftig vielfältig vernetzt. Digitale Signaturen und Zertifikate werden die Authentizität beim Datenaustausch in Zukunft auch quantensicher nachweisen müssen. © Escrypt

an kryptografisch relevanten Quantencomputern, die in der Praxis solche Operationen ausführen könnten. Tatsächlich sind die ersten funktionsfähigen Rechnersysteme, die auf Quantenmechanik beruhen, bislang nur unter extrem großem Aufwand und unter Laborbedingungen zu betreiben. Die Entwicklung jedoch ist vorgezeichnet: Die mit Qubits statt Bits arbeitenden Quantenrechner werden heutige Supercomputer in ihrer Rechenleistung für bestimmte Operationen exponentiell übertreffen. Realistische Annahmen gehen davon aus, dass sie in ca. 15 bis 20 Jahren verfügbar sind – unweigerlich auch für böswillige Angriffe auf IT-Systeme. Spätestens dann werden herkömmliche asymmetrische Algorithmen keine ausreichende Sicherheit mehr bieten können. Eine sichere Vergabe von Zertifikaten wird in dieser künftigen Post-Quantum-Ära nur mit neuen, Quantencomputer-resistenten Algorithmen zu gewährleisten sein (Bild 2).

Lange Fahrzeuglebensdauer erfordert Schutz

Fahrzeuge, die in den kommenden Jahren vom Band laufen, sind demnach von dieser Entwicklung bereits konkret betroffen. Lebensspannen von 15 Jahren oder mehr sind hier ja die Regel; bei batterieelektrischen Fahrzeugen rechnet man gar mit noch längeren Lebenszyklen. Damit stellt sich die Frage, welche Maßnahmen bereits heute bei der Entwicklung der Fahrzeugarchitektur zu berücksichtigen sind, um im Sinne eines lebenslangen Cyberschutzes und kontinuierlichen Risikomanagements sicherzustellen, dass die Fahrzeugsysteme auch im Post-Quantum-Zeitalter noch vor Angriffen und unerlaubtem Zugriff gefeit bleiben. Post-Quantum-Kryptografie (Post Quantum Cryptography, PQC) muss idealerweise heute schon konzeptionell in die Fahrzeugentwicklung mit einbezogen werden – entweder indem die Signatur- und Verschlüsselungsmechanismen und die Auswahl kryptografischer Algorithmen bereits quantensicher erfolgen, oder indem die Security-Funktionen so konzipiert und ausgelegt sind, dass sie jederzeit und in ausreichendem Maße auf Quantencomputer-Resistenz hin Upgrade-fähig sind.

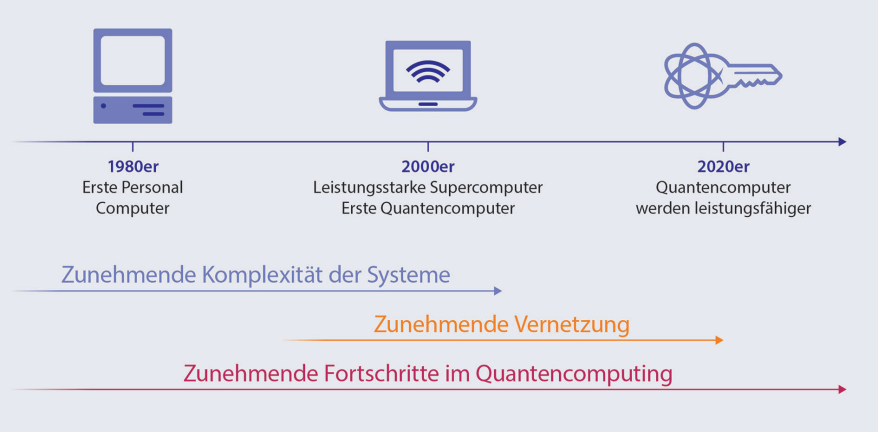

Bild 2: Die Entwicklung von Quantencomputer macht derzeit große Fortschritte. Die IT-Sicherheit in einer zunehmend vernetzten Welt stellt dies vor große Herausforderungen. © Escrypt

NIST-Ausschreibung für quantensichere Algorithmen

Als Richtschnur für die Auswahl geeigneter PQC können dafür die bereits vorliegenden Ergebnisse aus dem laufenden NIST-Post-Quantum-Projekt herangezogen werden. Das amerikanische National Institute of Standards and Technology (NIST) ruft seit einigen Jahren zur Einreichung geeigneter Public-Key-Verschlüsselungs- und Signaturverfahren auf. Infolgedessen gibt es mittlerweile erste Post-Quantum-reife kryptografische Algorithmen; bis Ende 2021 wird die Standardisierung einer ersten Auswahl solch quantensicherer Algorithmen durch das NIST erwartet. Dabei werden voraussichtlich mehrere Algorithmen für die unterschiedlichen Kategorien – Public-Key-Verschlüsselungsmechanismen, Key Encapsulation Mechanisms (KEM) und digitale Signatur – standardisiert.

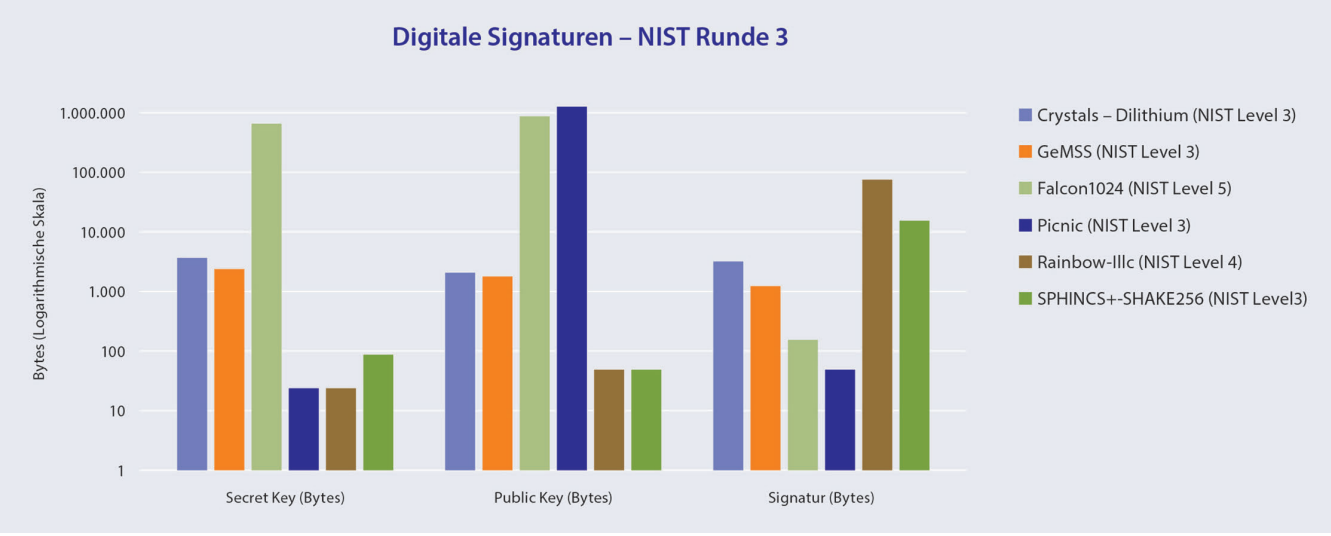

Bild 3: Die ausgewählten Algorithmen des NIST-Wettbewerbs weisen große Unterschiede bei Schlüssel- und Signaturgrößen auf. Für Automotive-Anwendungen sind nicht alle gleich gut geeignet. © Escrypt

Die Wahl der geeigneten verfügbaren Algorithmen für die Implementierung Post-Quantum-resistenter Cybersecurity orientiert sich dann an folgenden Fragestellungen:

- Wie muss die Struktur der Security-Funktionen angepasst werden, um die neuen Algorithmen mit einbeziehen zu können?
- Welcher Hardware-Erfordernisse bedarf es dafür in Zukunft?
- Wie wird eine Public-Key-Infrastruktur (PKI) mit quantensicheren Algorithmen aussehen?

Quantensichere Algorithmen für Automotive Krypto-Bibliothek

Auf dieser Basis hat Escrypt im Rahmen des Projektes Full-Lifecycle-Post-Quantum (FLOQI-PKI, Info-Box) die aus der NIST-Ausschreibung hervorgegangenen quantensicheren Algorithmen im Hinblick auf ihre Eignung für den Automotive-spezifischen Einsatz evaluiert. Die erste Wahl fiel dabei auf zwei gitterbasierten Algorithmen:

- CRYSTALS-Dilithium als Signaturalgorithmus und
- CRYSTALS-Kyber als KEM.

Beide Algorithmen finden sich auch in der finalen Auswahlrunde der NIST-Verfahrens. Ausgewählt als gute Kandidaten für die Anwendungsfälle im Automobilbereich wurden sie insbesondere aufgrund ihrer Leistung und ihres konstanten Ressourcenverbrauchs (Bild 3).

Um diese beiden Post-Quantum-Algorithmen heute schon für die Automotive-Anwendungen verfügbar zu machen, hat Escrypt sie jüngst in seine Automotive-spezifische Krypto-Bibliothek implementiert. Solch eine kryptografische Bibliothek ist Kernkomponente der Cybersicherheit im Fahrzeug. Sie stellt die nötigen kryptografischen Algorithmen, Formate und Verschlüsselungsprotokolle für die meisten Security-Anwendungen bereit. So greift beispielsweise die digitale Signaturverifikation, etwa für Flash-Lösungen oder die Aktivierung von Secure Boot, auf eine Krypto-Bibliothek zurück. Automotive Crypto Libraries sind außerdem auf die speziellen Anwendungen und Anforderungen des Fahrzeugs und seiner Infrastruktur hin entwickelt. Das bedeutet, dass die Algorithmen gemäß ASPICE Level 2 und ISO 262662 (bis ASIL D) implementiert werden, wobei die begrenzten Ressourcen und erforderliche Leistung der eingebetteten Systeme Fahrzeug besondere Berücksichtigung finden.

INFO

FLOQI: Forschungsprojekt für Post-Quantum-Security

Das vom Bundesministerium für Bildung und Forschung förderten Forschungsvorhaben FLOQI zielt auf die Entwicklung einer Quantencomputer-widerständigen Public-Key-Infrastruktur, die in einer künftigen Post-Quantum-Ära über ihren gesamten Lebenszyklus hinweg die sichere Vergabe von Zertifikaten gewährleistet. Die Technische Universität Berlin, das Fraunhofer AISEC, BMW, Bosch, Nixdorf, Escrypt und andere setzen dabei Post-Quantum-Verfahren auf unterschiedlichen Plattformen um und erproben deren Einsatz – insbesondere auch für die Automobilbranche. Die Ergebnisse sollen dann in internationale Standards einfließen.

PQ-Security in der Praxis evaluieren

Mit einer derartigen PQC-fähigen Krypto-Bibliothek können Automobilhersteller und -zulieferer einen ersten entscheidenden Schritt hin zu einer Post-Quantum-resistenten Cybersicherheit ihrer Fahrzeuge und Fahrzeugkomponenten vollziehen. Sie können auf diese Weise bereits heute damit beginnen, Post-Quantum-Algorithmen auf ihren Zielsystemen zu evaluieren und im Zuge eines Proof-of-Concept ermitteln, wie diese sich in der angewandten Praxis verhalten und welche Anforderungen die Post-Quantum-Kryptografie an die Hardware stellt.

Gerade weil dieses Entwicklungsfeld noch neu ist und zum Teil anderen mathematischen Theorien folgt als die bisher verwendeten kryptografischen Algorithmen, ist es wichtig, Qualität und Wirksamkeit der Implementierung zu verifizieren – und zwar über die etablierten Entwicklungsprozesse hinaus. Nur

so lässt sich beispielsweise herausfinden, ob die Zielsysteme mit ihren implementierten quantensicheren Algorithmen in der angewandten Praxis auch Seitenkanalangriffen standhalten. Security-Anbieter, Forschung und Anwender im Automotive-Bereich werden hier über die kommenden Jahre laufend gegenseitigen Erfahrungsaustausch pflegen müssen, um die Qualität der PQC für Automotive Anwendungsfälle weiter zu verbessern.

Quantenresistente Hardware-Security-Module

Die Post-Quantum-Ära hat gerade erst begonnen. Mit ihr wird die Absicherung vernetzter Fahrzeuge und Flotten gegen Cyberattacken neu verhandelt. Die Industrie muss sich zügig die notwendigen Grundlagen erarbeiten und neue Fahrzeugarchitekturen und -systeme auf zukünftige Quantensicherheit hin auslegen. Mit der um die ersten quantensicheren Algorithmen Dilithium und Kyber erweiterten Krypto-Bibliothek können Automobilhersteller und Zulieferer den Fahrzeugsystemen heute schon erste Teile der notwendigen Automotive-Security-DNA dafür mitgeben – und diese dann gemäß jeweils aktueller Erkenntnisse und Best-Practices um weitere Post-Quantum-Algorithmen erweitern.

Vor allem jedoch ist damit der Weg geebnet hin zu einer erweiterten Quantencomputer-widerständigen Absicherung des Fahrzeugs. Denn in der Folge lassen sich so auch die Security-Funktionen im Hardware-Security-Modul (HSM) auf den Mikrocontrollern und -prozessoren der künftigen ECUs, DCUs und Vehicle Computer quantensicher ausführen. Voraussetzung auf der HSM-Hardware-Seite sind leistungsstarke Acceleratoren. So machen zum Beispiel Hashing-Algorithmen (SHA3 oder auch SHA2–256) bis zu 80 Prozent des Rechenbedarfs der asymmetrischen PQC-Verfahren aus. Aber auch ein leistungsstarker AES-256 für die symmetrische Kryptografie wird zum absoluten Muss-Kriterium im Post-Quantum-Zeitalter. Folgerichtig braucht es einen leistungsfähigen Security-Stack auf dem HSM, der die entsprechenden Hardware-Acceleratoren unterstützt und sie in sicherheitsrelevante Funktionen und Protokolle integriert, die dann der Applikations-Software zur Verfügung gestellt werden. Solchermaßen mit Post-Quantum-fähigem HSM bestückte Mikrocontroller und Mikroprozessoren werden die notwenige Cybersicherheit für das Fahrzeug bis in die Ära der Quantencomputer hinein gewährleisten können. ■ (eck)

www.escrypt.com

Dr. Efstathia Katsigianni arbeitet als Security Consultant Post Quantum Cryptography bei Escrypt in Berlin. © Escrypt

Dipl.-Math. **Sandra Weigl** ist Product Manager Crypto Library bei Escrypt in Stuttgart. © Escrypt