Das Post-Quantum-Kalkül

Die Informationstechnik steht an der Schwelle zum Quantenzeitalter. Für die Cybersicherheit künftiger Fahrzeuge und ihrer vernetzten Systeme ist das keine gute Nachricht, denn die heutigen Securitymechanismen werden sich per Quantencomputer aushebeln lassen. Etas arbeitet an Benchmarks für quantensichere Automotive-Security-Verfahren.

VERFASST VON

Aaron Rathweg, M. Sc.
ist Security Engineer
bei Etas in Bochum.

Abdelrahman Osman, M. Sc.
ist Security Engineer
bei Etas in Berlin.

Andreas Fleig, M. Sc.
ist Security Consultant
bei Etas in Berlin.

Markus Herbst, M. Sc.
ist Security Consultant
bei Etas in München.

Heute entwickelte Fahrzeuge werden auch in 15 bis 20 Jahren noch auf der Straße sein. Bis dahin sind erste Quantencomputer vermutlich Wirklichkeit. Die derzeit für die Absicherung von Fahrzeugen und in deren IT-Ökosystem verwendeten klassischen kryptografischen Verfahren würden allerdings gezielten Angriffen durch Cyberkriminelle mit derartigen Rechnern kaum standhalten: Asymmetrische Algorithmen wie RSA und Elliptic Curve Cryptography (ECC) beruhen auf der Primfaktorzerlegung beziehungsweise dem Problem des diskreten Logarithmus. Beides ist für einen Quantenrechner mit ausreichend Rechenleistung in überschaubarer Zeit lösbar. Auch für die heute verwendeten symmetrischen Verfahren wäre bei einer Attacke aus dem Quantenrechner per Grover-Algorithmus die Schutzwirkung theoretisch halbiert.

Diese Situation vor Augen, startete das US-amerikanische National Institute for Standards and Technology (NIST) 2016 einen Auswahl- und Standardisierungsprozess für Post-Quantum-sichere Signaturverfahren und sogenannte Key Encapsulation Mechanisms (KEM, Schlüsselkapselungsverfahren). Aktuell befinden sich vier quantensichere Algorithmen in Standardisierung: Crystals-Kyber als KEM für den Schlüsselaustausch sowie Crystals-Dilithium, Falcon und Sphincs+ als Signaturalgorithmen zum Nachweis von Authentizität und Integrität digitaler Daten. In weiteren Auswahlrunden plant die NIST zusätzliche KEM und Signaturverfahren zu standardisieren.

HOHE LEISTUNGSANFORDERUNGEN – BEGRENZTE RESSOURCEN

Im Vergleich zu klassischen kryptografischen Verfahren stellen diese vier Post-Quantum-Algorithmen deutlich höhere Anforderungen an Schlüsselgrößen und Performance. Damit stellt sich die Frage, wie sie in die Securityfunktionen der Fahrzeugsysteme integriert werden können, ohne deren begrenzte Ressourcen (etwa hinsichtlich RAM, Flash- und Rechenleistung) zu sprengen, **BILD 1**. Wie und mit welchen Post-Quantum-Verfahren der Übergang zu quantensicherer Kryptografie gelingt, hängt natürlich von den jeweiligen Anforderungen der für die Security relevanten Funktionen und vom Leistungsvermögen der ECUs ab, auf denen sie – parallel zu deren originären Aufgaben – ausgeführt werden. Daneben bestimmt der jeweilige Anwendungsfall, welche quantensicheren Verfahren im Einzelnen geeignet sind. Deutlich wird das an vier der aktuell gängigsten Use Cases für Automotive Cybersecurity [1]:

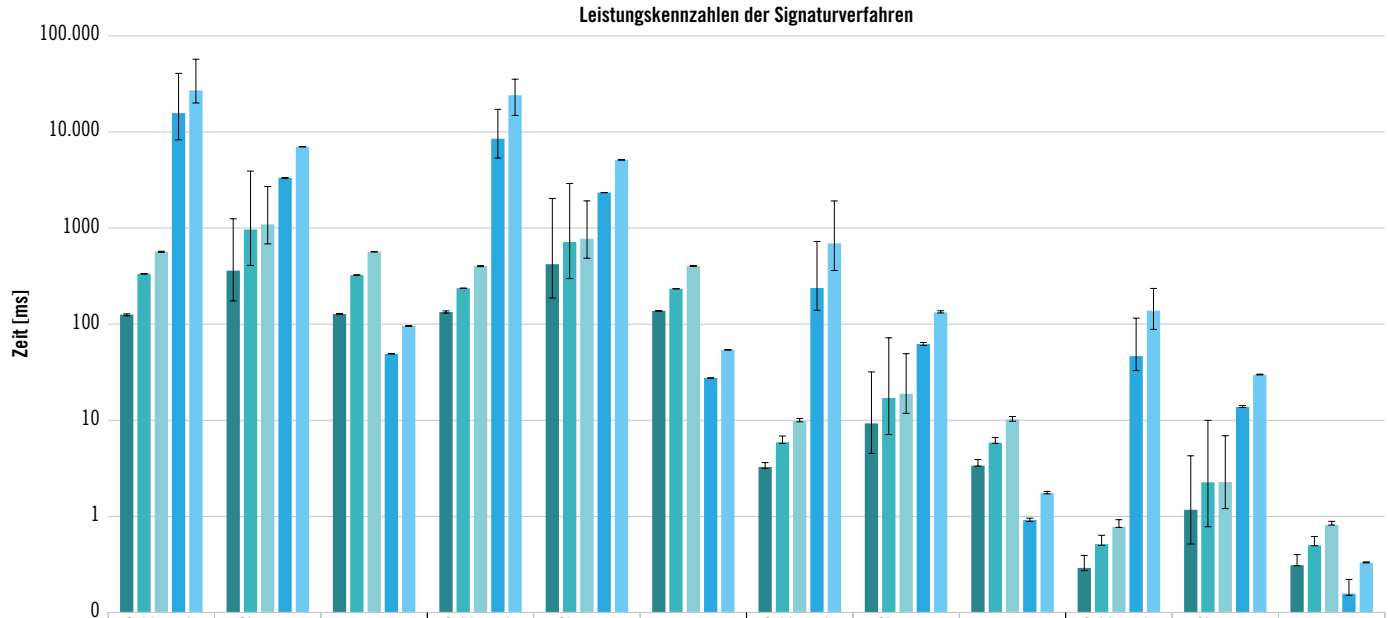
Key-Management-Systeme (KMS) verwalten das für sichere Onboard-Kommunikation und externe Kommunikation der Fahrzeuge notwendige kryptografische Schlüsselmaterial. Per KMS stellen die OEMs das Schlüsselmaterial ihren Fahrzeugflotten zur Verfügung. Typischerweise werden die kryptografischen Schlüssel dann im Fahrzeug an die einzelnen ECUs verteilt, und dort im Trusted Execution Environment (TEE) oder Hardware-Security-Modules (HSM) gespeichert. Eine Umstellung auf Post-Quantum-KMS brächte einige Herausforderungen mit sich, da das im Backend generierte quantensichere Schlüsselmaterial um ein Vielfaches größer wäre als bei den heute üblicherweise verwendeten asymmetrischen Schlüsseln, **BILD 1**. Die Übertragung ans Fahrzeug und das Einbringen in die Steuergeräte gelänge heute allenfalls mit neueren Versionen des ISO-TP-Standards (ISO 15765-2), der Containergrößen bis zu $(2^{32}-1)$ Bytes nutzt. Zugleich würde der RAM-Verbrauch der ECUs ansteigen, da das Schlüsselmaterial gepuffert wird, bevor es im TEE oder HSM sicher gespeichert wird. RAM- und Flash-Ressourcen von TEE oder HSM müssten angepasst und die Krypto-Libraries der ECUs um Post-Quantum-Verfahren erweitert werden.

Secure Boot zielt darauf ab, die Integrität und Authentizität der Firmware und auszuführenden Software eines Fahrzeugsystems sicherzustellen. Hierbei wird deren Verifizierung beispielsweise mittels Public-Key-Kryptografie über eine Zertifikatskette hinweg validiert. Aufgrund der begrenzten Speicherkapazitäten der ECUs wird dabei zumeist statt der kompletten Zertifikatskette lediglich das letzte Zertifikat der Kette verfügbar gemacht. Selbst das wäre aufgrund der enormen Größe der Public Keys bei Post-Quantum-Verfahren kaum darstellbar. Eine mögliche Alternative wäre, lediglich den Public Key abzulegen und gegen einen authentisch gespeicherten Hashwert des Keys zu verifizieren. Um außerdem eine aus-

Algorithmus	Klassisches Securitylevel	Schlüsselgröße Public Key	Schlüsselgröße Private Key	Signaturgröße
Falcon 512	120	897	1281	666
Falcon 1024	277	1793	2305	1280
Crystals-Dilithium 2	121	1312	2544	2420
Crystals-Dilithium 3	176	1952	4016	3293
Crystals-Dilithium 5	253	2592	4880	4595
RSASSA-PSS 3072 bit	128	384	384	384
ECDSA mit P-256	128	32	32	64

Schlüssel- und Signaturgrößen in Bits

BILD 1 Die vom NIST standardisierten Post-Quantum-Signaturverfahren bringen deutlich größere Schlüssel- und Signaturgrößen mit sich als die heutige gebräuchlichen RSA- und ECDSA-Algorithmen [1] (© Etas)



	Schlüssel-generierung	Signatur **Renesas**	Verifizierung	Schlüssel-generierung	Signatur **Aurix TC3 75 LK**	Verifizierung	Schlüssel-generierung	Signatur **Raspberry Pi 2**	Verifizierung	Schlüssel-generierung	Signatur **Raspberry Pi 4**	Verifizierung
Dilithium 2	125,84	360,30	127,62	133,71	420,24	137,53	3,26	9,28	3,37	0,29	1,17	0,31
Dilithium 3	333,89	964,97	324,19	236,50	715,33	233,77	5,90	17,08	5,83	0,51	2,26	0,50
Dilithium 5	567,31	1093,92	564,01	401,62	774,43	403,24	9,81	18,91	10,20	0,78	2,27	0,81
Falcon 512	15.712,34	3324,37	49,14	8504,46	2338,48	27,47	238,28	62,11	0,92	46,46	13,74	0,16
Falcon 1024	27.094.31	7016,86	95,70	24.087,47	5121,28	54,01	694,45	132,82	1,75	138,26	29,75	0,33

BILD 2 Unter den PQ-Signaturalgorithmen scheint Crystals-Dilithium zwar generell die bessere Wahl zu sein; bei Anwendungsfällen reiner Signaturüberprüfung jedoch ist Falcon deutlich schneller [1] (© Etas)

reichend hohe Boot-Geschwindigkeit zu gewährleisten, bedarf die Ausführung von Post-Quantum-Verfahren einer Beschleunigung per Hardware(HW)-Algorithmen. OEMs und Halbleiterhersteller müssen die Zukunft hier gemeinsam planen. Von den bisher ausgewählten Post-Quantum-Algorithmen zeigt sich Falcon für Secure Boot derzeit als am besten geeignet. Im Vergleich zu Crystals-Dilithium hat er kleinere Signatur- und Public-Key-Größen und kann die Signatur unter geringerem Speicherbedarf schneller verifizieren.

Sicherer Diagnosezugriff: Die Absicherung der Diagnoseschnittstelle des Fahrzeugs soll unberechtigtem Zugriff auf die ECUs vorbeugen. Gemäß des Unified-Diagnostic-Services(UDS)-Standards (ISO 14229-1) wird der Diagnosezugriff entweder mittels Challenge-Response-Ansatz oder per asymmetrischer Kryptografie gesichert. In letzterem Fall wird die Signatur der Zugriffsanforderung in der ECU per Public Key verifiziert. Auch hier erfordert Post-Quantum-Kryptografie ECU-seitig aufgrund der

größeren Schlüssel und Signatur deutlich mehr RAM und Speicherplatz. Zur Sicherung des Diagnosezugriffs erscheint daher Falcon im Vergleich zu Crystals-Dilithium wegen geringerer Schlüssellänge des Public Key und schnellerer Signaturprüfung als bessere Alternative.

Transport Layer Security (TLS) gilt heute als gängiges Securityprotokoll für die Absicherung der Online-End-to-End-Kommunikation zwischen Fahrzeug und Backend. Die Kommunikationspartner authentifizieren sich dabei durch Verifizierung ihrer Zertifikate während des digitalen Handshakes und tauschen dabei einen gemeinsamen symmetrischen Schlüssel für die Absicherung weiterer Kommunikation aus. Mit Post-Quantum-Kryptografie wächst die Größe der Nachricht beim TLS-Handshake erheblich. Auf ECU-Seite nähme der Speicherverbrauch deutlich zu. Zu große Nachrichten würden gar fragmentiert, was wiederum zum zeitlichen Overhead beim TLS-Handshake führt. Im Vergleich der Post-Quantum-Algorithmen ist Crystals-Dilithium hier gegenüber Falcon im Vorteil: Zwar liegt letzterer bei rein serverseitiger Authentifizierung leistungsmäßig vorn, ersterer jedoch erlaubt schnelleres Signieren und bessere Leistung auf der ECU.

BENCHMARKS FÜR HARDWAREPLATTFORMEN

ECUs im Fahrzeug verfügen heute über unterschiedlichste Leistungswerte. Das Infotainmentsystem verlangt nach ungleich mehr Speicherplatz und Rechengeschwindigkeit als etwa das Schließsystem. Dementsprechend sind die ECUs von einer Transition hin zu quantensicheren Verfahren in unterschiedlichem Maße betroffen. Etas und Volkswagen haben gemeinsam realitätsnahe Benchmarks für Post-Quantum-sichere Verfahren ermittelt [1]. Dabei wurden unter anderem die Signaturalgorithmen Crystals-Dilithium und Falcon gegenübergestellt und auf vier Mikrocontrollern mit unterschiedlicher, im Automotive-Umfeld gängiger Rechenleistung und Speicherkapazität getestet:

- Raspberry Pi 4 mit 1,5 GHz 64-Bit Quad-Core Cortex-A72 CPU, 4GB RAM
- Raspberry Pi 2 Model B V1.1 mit 900 MHz 32-Bit Quad-Core ARM Cortex-A7-CPU, 1 GB RAM
- Infineon Aurix Lite Kit V2 mit 300 MHz TriCore Aurix TC375, 992 KB RAM pro Core, 6 MB Flash
- Renesas R7F7015032 auf 20 MHz RH850/F1x-176pin Piggyback Board, 2 Cores mit je 192 KB Local RAM, 64 KB Global RAM, 6 MB Flash.

Sowohl Crystals-Dilithium als auch Falcon sind in mehreren Securitylevels verfügbar, gemessen an der Zahl der Operationen, die nötig sind, um die Verfahren zu knacken. Im Test wurden auf den genannten HW-Targets für beide Algorithmen jeweils über mehrere, in etwa vergleichbare Securitylevels hinweg folgende Leistungsparameter gemessen: Laufzeit in Millisekunden für eine spezifische Operation (Durchschnittswert aus 100 Iterationen) sowie Ressourcenverbrauch des Stacks (Stack Consumption) in Bytes bei Durchführung dieser Operation und Codegröße der kompilierten Binärdatei in Bytes. Darüber hinaus wurde für die Ermittlung der Benchmarks nach den ausführbaren Funktionen der Algorithmen unterschieden – für die verglichenen Signaturalgorithmen also nach Generierung des Schlüsselpaars, Signatur der Nachricht sowie deren Verifizierung.

LAUFZEIT UND RESSOURCENVERBRAUCH

Im Vergleich zeigt Crystals-Dilithium gegenüber Falcon sowohl bei Schlüsselgenerierung als auch bei Signatur über alle Securitylevel und HW-Targets hinweg eine signifikant bessere Laufzeitperformance. Bei der Verifizierung hingegen ist letzterer klar im Vorteil. Für beide Signaturverfahren zeigt sich auf den leistungsstarken HW-Targets (Raspberry Pi 2 und Pi 4) unabhängig von der ausgeführten Funktion eine naturgemäß deutlich bessere Laufzeitperformance. Crystals-Dilithium scheint hier demnach im Allgemeinen die bessere Wahl zu sein. Bei Anwendungsfällen, die sich auf die Signaturüberprüfung beschränken (etwa sicherer Diagnosezugriff) ist Falcon allerdings die deutlich schnellere Alternative, **BILD 2**.

Er benötigt auch deutlich weniger Ressourcen auf dem Chip als Crystals-Dilithium und erweist sich insbesondere bei der Verifizierung der Signaturen um ein Vielfaches effizienter. Bei Schlüsselgenerierung und Signaturerstellung oder Verifizierung erfordert Falcon einen 2,6-, 1,5-, beziehungsweise 10,5-fach geringeren Speicherverbrauch als Crystals-Dilithium, **BILD 3**.

USE-CASE-ABHÄNGIGE OPTIMIERUNG DER CODEGRÖSSE

Konträr zum Ressourcenverbrauch hat Falcon einen um den Faktor 4,2 höheren Speicherbedarf als Crystals-Dilithium. Grund dafür ist die Vielzahl vorberechneter Werte, die er in sogenannten Lookup Tables im Speicher hinterlegt. Allerdings relativiert sich dieser Unterschied für Anwendungsfälle, bei denen auf der ECU lediglich eine Signaturverifikation benötigt wird. Wird der Code für Schlüssel-

Algorithmus	Schlüsselgenerierung	Signatur	Verifizierung
Falcon 512	18.261	42.181	4770
Falcon 1024	36.829	82.511	8873
Crystals-Dilithium 2	38.509	51.783	36.385
Crystals-Dilithium 3	61.071	79.825	57.976
Crystals-Dilithium 5	97.937	122.573	92.718

Speicherverbrauch in Bytes

BILD 3 Bei Schlüsselgenerierung, Signaturerstellung beziehungsweise Verifizierung erfordert Falcon einen wesentlich geringeren Speicherverbrauch als Crystals-Dilithium [1] (© Etas)

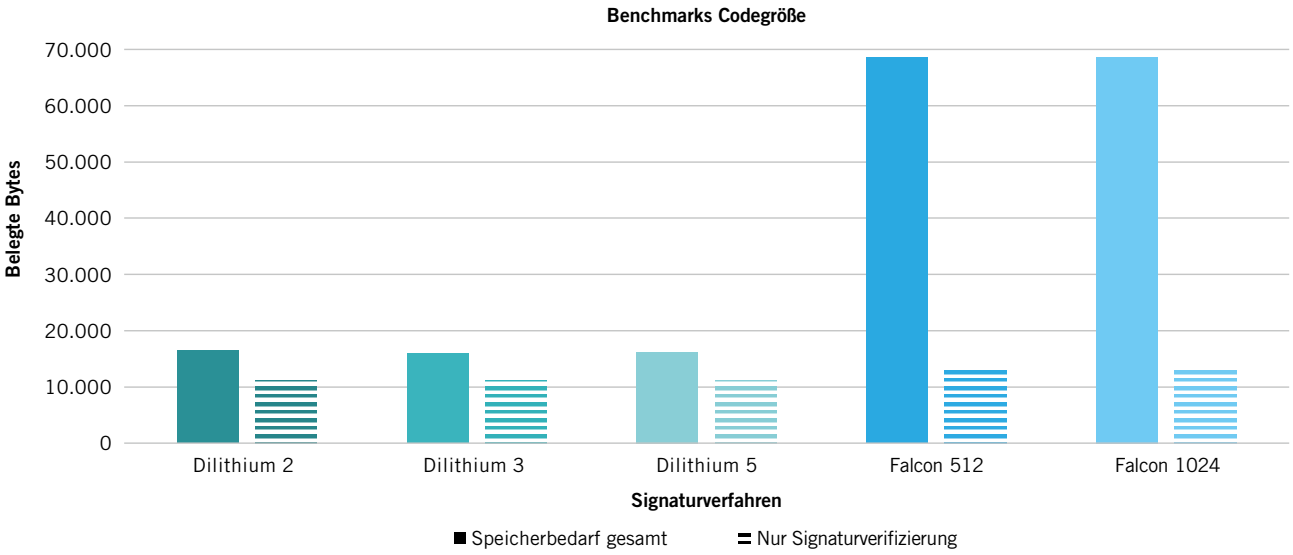


BILD 4 Codegrößen der Post-Quantum-Verfahren über die verschiedenen Sicherheitsstufen hinweg – nur zur Signaturüberprüfung eingesetzt, verringert sich der Speicherbedarf von Falcon drastisch [1] (© Etas)

und Signaturgenerierung entsprechend entfernt, verringert sich unter Falcon der Speicherbedarf viermal mehr als bei Crystals-Dilithium. Wird also einzig die Signaturverifizierung benötigt, liegen beide Verfahren bei der Codegröße nahezu gleichauf, und sein hierbei geringerer operativer Ressourcenverbrauch gereicht Falcon insgesamt zum Vorteil, **BILD 4**.

EINZELFALLBETRACHTUNG NÖTIG

Die Wahl des jeweils richtigen quantensicheren Verfahrens bedarf, wie anhand der Benchmarkwerte für die verglichenen Signaturalgorithmen gezeigt, einer differenzierten Einzelfallbetrachtung. Welches Post-Quantum-Verfahren jeweils am besten geeignet ist, hängt ab vom gewünschten Securitylevel, von der HW-Performance der ECU und des verwendeten Chips sowie insbesondere auch vom jeweiligen Anwendungsfall mit seinen nötigen ausführbaren Securityfunktionen. OEMs und Zulieferer bewegen sich hier letztlich in einem Entscheidungsraum zwischen Risikoabwägung, (HW-)Kosten und systemischen Anforderungen beziehungsweise Notwendigkeiten, werden aber an Post-Quantum-Kryptografie nicht vorbeikommen. Bei der langen Lebensspanne von Fahrzeugen bedarf es frühzeitig einer zukunftsgewandten Definition der Securityziele, eines Proof-of-Concept für die securityrelevanten Automotive Use Cases und gegebenenfalls entsprechender Post-Quantum-fähiger Hardware im Fahrzeug. So viel jedenfalls steht fest: Ist der erste Quantencomputer erst einmal verfügbar, ist es zu spät.

LITERATURHINWEIS

[1] Rathweg, A.; Osman, A.; Fleig, A.; Katsigianni, E.; Tschache, A.: Impacts of post-quantum cryptography on automotive security. In: 11th escar USA 2023, Plymouth, Michigan (Detroit): The World's Leading Automotive Cyber Security Conference. A case study, 2024. Online: https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/docId/10394, aufgerufen: 3. Mai 2024