Langzeitsichere Kryptografie II

IT-Entscheidungen für Quantensicherheit – Zukunftsmusik oder akuter Handlungsbedarf?

Selbst unter Kryptografen ist noch nicht klar, welche Post-Quanten-Algorithmen die heutigen klassischen Algorithmen ersetzen werden. Trotzdem können IT-Entscheider in Unternehmen schon jetzt einiges tun, um der Bedrohung durch Quantencomputer entgegenzutreten.

Von Marie-Luise Groh und Georg Nestmann, Chemnitz

Betrachtet man den aktuellen Fortschritt im Bereich des Quantencomputing und die Anstrengungen, die weltweit in diesem Gebiet gebündelt werden, so steht außer Frage, dass die Kryptografie, wie wir sie kennen, vor einem Umbruch steht. Wann der Tag sein wird? Nicht morgen und nächstes Jahr wohl auch nicht. Doch selbst wenn es erst in 10 Jahren so weit ist, müssen sich IT-Entscheider schon heute diesem Szenario stellen!

So dauert zum Beispiel die Entwicklung eines neuen Autos durchschnittlich vier Jahre, der Wagen soll acht Jahre lang verkauft und dann noch mindestens acht Jahre sicher gefahren werden. Noch drängender ist die Lage für Unternehmen, die sich der Verschlüsselung sensibler und langlebiger Daten verschrieben haben. Vorausschauende Angreifer können schon heute Chiffrate sammeln – in froher Erwartung des Tages, an dem der Klartext einsehbar sein wird, weil etwa der geheime Teil eines Diffie-Hellman-Schlüsselaustauschs dann nicht mehr ganz so geheim ist. Und das betrifft längst nicht nur die Transport-Layer-Security (TLS) als Kernbaustein der gesicherten Kommunikation im Netz.

Doch wie lautet die Folgerung? Jetzt schon her mit den Post-Quanten-Algorithmen?! Wenn es nur so einfach wäre ...

Post-Quanten-Algorithmen

Seit absehbar ist, wie real und nah die Bedrohung durch Quantencomputer für die Informationssicherheit ist, hat die Suche nach alternativen Verschlüsselungs- und Singnaturalgorithmen einen enormen Schub erlebt. Maßgeblich dafür verantwortlich ist die US-amerikanische Standardisierungsbehörde National Institute of Standards and Technology (NIST), die im November 2016 einen Aufruf zur Suche nach Algorithmen veröffentlicht hat, die vom Quantencomputing bedrohte Verfahren ersetzen sollen. Ähnlich dem Auswahlverfahren, das im Jahr 2000 den heute breit genutzten symmetrischen Verschlüsselungsalgorithmus AES hervorgebracht hat, ist der Standardisierungsprozess als Wettbewerb organisiert (siehe Kasten auf S. 62) – Ergebnisse werden jedoch frühestens Anfang 2022 erwartet, wenn dessen 3. Runde abgeschlossen sein wird.

Auch Bestrebungen von anderen Seiten laufen: Das Europäische Institut für Telekommunikationsnormen (ETSI) erarbeitet Anforderungen an Post-Quanten-Verfahren aus praktischer Sicht, etwa um sie in derzeitige Protokolle zu integrieren (vgl. www.etsi.org/technologies/quantum-safe-cryptography). Das Projekt PQCrypto bietet ein Forum für Kryptografen, um den Forschungsstand zu diskutieren und neue Ansätze zu präsentieren, unter anderem mit regelmäßigen Konferenzen. Fast alle Finalisten der 3. Runde des NIST-Wettbewerbs wurden durch Mitglieder von PQCrypto eingereicht oder mitentwickelt.

Obwohl das Feld der aussichtsreichen Algorithmen-Kandidaten mittlerweile überschaubar ist (siehe Kasten), befindet sich die Internetgemeinschaft im Wartemodus: Eine Prognose ist schwierig, unter anderem da NIST aus den gitterbasierten Verfahren für digitale Signaturen und Schlüsseleinigung wohl erst einmal nur eines auswählen wird. Solange die Ergebnisse der 3. Runde ausstehen, dürften sich auch Software-Unternehmen zurückhalten – es könnte schließlich sein, dass sich im Laufe der aktuellen Kryptanalyse doch noch Angriffsszenarien auf den gerade favorisierten Algorithmus offenbaren.

Zurzeit ist das Angebot an einsatzbereiter Post-Quanten-Software jedenfalls überschaubar. Infolgedessen sind auch Anwendungsbeispiele und Antworten auf typische Fragen bei der Nutzung rar gesät – von Langzeittests und Bugfixes, die erst durch die Anwendung in breiter Masse kommen, ganz zu schweigen.

Komplexer Umstieg

Selbst wenn man zu den wenigen gehört, welche die Implementierung kryptografischer Software

beherrschen und dies sogar beruflich tun, ist Post-Quanten-Kryptografie ein steiniges Feld. Während man dem Prinzip eines Diffie-Hellman-Schlüsselaustauschs oder einer RSA-Verschlüsselung noch mit grundlegender Zahlentheorie beikommt, sucht man Post-Quanten-Mathematik wie gitterbasierte Kryptografie oder gar supersinguläre Kurven in vielen Mathemaktikstudiengängen vergeblich. Einige Teilgebiete der Post-Quanten-Kryptografie sind schlichtweg so neu oder wenig erforscht, dass sie noch längst nicht zum Standardrepertoire eines Mathematikers gehören.

Und auch wenn man sich an den Einreichungen der Algorithmen des NIST-Wettbewerbs orientiert, die alle auf der Website inklusive Quellcode verlinkt sind, mag einige Zeit vergehen, bis die mathematischen Hintergründe und die (teilweise rudimentär dokumentierten) Referenzimplementierungen einen Fahrplan zur eigenen Software ermöglichen. Zudem lauern dann noch immer Tücken bei der Implementierung und ungeahnte Seitenkanalangriffe, die sich erst im Laufe der Zeit und mit zunehmender Zahl praktischer Umsetzungen offenbaren werden.

Dieses Problem zeigte sich bereits bei der letzten großen Neuerung kryptografischer Standards – dem beginnenden Einsatz elliptischer Kurven Anfang der 2000er-Jahre: So stellten renommierte Forscher aus diesem Fachgebiet im Nachhinein fest, dass einige der durch Standards empfohlenen Kurventypen zwar auf dem Papier sicher, jedoch bei der Implementierung besonders fehleranfällig waren. Folglich hatten viele Programmierer mit Timing-Attacken oder dem Durchsickern geheimer Daten zu kämpfen, wenn ein Angreifer spezielle Eingaben für die Algorithmen vorgeben konnte.

Welcher der „richtige" Post-Quanten-Algorithmus ist, hängt zudem stark vom Anwendungsfall ab. Forscher der Universität Singapur haben 14 heutige Einsatzgebiete für digitale Signaturen untersucht, um herauszufinden, wie gut sich die finalen Signaturalgorithmen des NIST-Wettbewerbs darin schlagen würden [1]. Zu den Anwendungen gehören unter anderem das E-Mail-Signaturverfahren S/MIME, EMV-Chips, welche die Sicherheit von Kreditkarten gewährleisten, oder die Authentifizierung im Internet durch FIDO-Verfahren (Fast IDentity Online). Da die Anwendungen auf verschiedensten Plattformen laufen und teils Bausteine in einem größeren Verfahren sind, ergeben sich vielfältige Einschränkungen an Laufzeit und Speicherplatz. So ist der Platz auf einem Kreditkartenchip eng begrenzt, wohingegen beim gegenseitigen Authentifizieren von Server und Client im TLS-Protokoll Schnelligkeit zählt.

Die Ergebnisse der Studie sind in einer „Machbarkeits-Matrix" zusammengefasst (siehe Tab. 1). Die Forscher haben die Eignung mit maximal 12 Punkten bewertet – der Höchstwert gibt an, dass der Algorithmus die Anforderung einer Anwendung vollständig erfüllt. Je kleiner der Wert, desto weniger geeignet ist der Post-Quanten-Algorithmus für die entsprechende Applikation. In Tabelle 1 werden Werte von 11 und 12 Punkten als sehr gut (++) dargestellt, 8–10 Punkte als gut, 6–7 Punkte als befriedigend (o) und 5 oder weniger Punkte als schlecht (-).

Die Forscher schließen, dass jeder der drei Finalisten des NIST für etwa die Hälfte der betrachteten Anwendungen ein geeigneter Kandidat wäre. Besonders auf dem Gebiet der Chipkarten bestehe jedoch noch Handlungsbedarf – dort sehen sie im Backup-Kandidaten Picnic das größte Potenzial. Es ist also zu erwarten, dass die Standardisierung eines einzelnen Algorithmus noch nicht der Startschuss für quantensichere Implementierungen auf allen Gebieten sein wird.

Tabelle 1: Einschätzung der Eignung von Post-Quanten-Algorithmen für verschiedene Einsatzzwecke (Basis: Tab. 4 in [1] – CC-BY)

	Finalist im NIST-Wettbewerb			Backup-Kandidat im NIST-Wettbewerb		
	Dilithium	**Falcon**	**Rainbow**	**GeMSS**	**Picnic**	**SPHINCS+**
3SKey	+	+	o	–	+	o
EMV-SDA	+	+	+	+	+	+
EMV-DDA	–	–	o	–	+	o
CA-Key	++	++	++	+	++	+
ICAO 9303	+	+	+	+	+	+
GSM eSIM	+	+	o	–	+	o
TLS-Server	++	+	++	+	+	+
TLS-Client	++	++	++	+	+	+
Bitcoin	++	++	++	o	+	o
FIDO	+	+	–	–	+	o
S/MIME	++	++	++	+	++	++
PDF-AES	++	++	++	+	++	+
PDF-QES	+	+	o	–	+	o
Code-Signing	++	++	++	+	++	+
Ø-Bewertung	10,21	9,85	9,29	6,78	9,71	8,28
Anz. ++	7	6	7	0	4	1
min. Bewertung	5	4	5	4	8	6

Erste Schritte laut BSI

Im August 2020 hat das BSI aktualisierte Handlungsempfehlungen veröffentlicht, um die Migration zur Post-Quanten-Kryptografie bereits einzuleiten, bevor die kryptografische Gemeinschaft sich auf die geeignetsten Post-Quanten-Algorithmen einigt und diese vom NIST standardisiert werden.

Kernpunkt der Empfehlung ist es, neu entwickelte Systeme auf eine flexible Wahl des Algorithmus vorzubereiten. Dies ist nicht nur nötig, weil noch aussteht, welcher Post-Quanten-Algorithmus den Platz welches klassischen Algorithmus einnehmen wird. Auch falls sich nach der Standardisierung und dem Einbau ins System noch Schwachstellen am ausgewählten Verfahren offenbaren, muss man es schnell durch ein anderes ersetzen können. Denn auch wenn die „Gewinner" des NIST-Wettbewerbs gewissenhaft und intensiv untersucht wurden, wird der weltweite Einbau eines neuen Algorithmus in kritische Systeme noch einmal zur Intensivierung der Suche nach Schwachstellen führen, selbstverständlich auch bei Hackern und Angreifern.

Als positiver Nebeneffekt eines flexiblen Systems ergibt sich, dass ein bisher verwendeter klassischer Algorithmus sich genauso durch einen anderen klassischen Algorithmus ersetzen lässt. Schließlich werden weiterhin neue Angriffe entwickelt, die ohne Quantencomputer auskommen, sodass klassische Verfahren auch vor deren Reife noch an Sicherheit verlieren können.

Selbst wenn die ersten Post-Quanten-Algorithmen standardisiert sein werden, sollte der Umstieg auf diese schrittweise erfolgen. Die heute verwendeten klassischen Algorithmen blicken auf eine lange und intensive Kryptanalyse zurück. RSA beispielweise wurde 1977 veröffentlicht – doch auch Jahrzehnte später treten noch immer neue Angriffe auf RSA zutage (z. B. 2010 eine Hardware-Attacke auf RSA-Signaturen). Das Signaturverfahren Rainbow, einer der Finalisten der 3. Runde des NIST-Wettbewerbs, fußt dagegen auf einem Paper aus dem Jahr 2005. Um noch unentdeckte Schwachstellen der ersten Generation von Post-Quanten-Algorithmen auszugleichen, empfiehlt das BSI, neue Systeme (noch) nicht auf die alleinige Verwendung dieser Verfahren auszulegen. Stattdessen sollte man vorerst hybride Ansätze verfolgen – also eine Kombination aus klassischem und Post-Quanten-Algorithmus.

Hybridverfahren zur Schlüsselaushandlung

Eine hybride Schlüsselaushandlung (Schlüsseleinigung) könnte zum Beispiel so aussehen: Die Kommunikationspartner führen miteinander parallel ein klassisches Schlüsseleinigungsverfahren und ein Post-Quanten-KEM-Verfahren (Key-Encapsulation-Mechanism) durch – dabei werden immer nur öffentliche Informationen zwischen den Partnern übertragen. Im Ergebnis verfügen beide Kommunikationspartner über zwei geteilte Geheimnisse (Shared Secrets), wobei eines über ein klassisches Verfahren, etwa Diffie-Hellmann, und das zweite über ein Post-Quanten-Verfahren, zum Beipiel NTRUEncrypt, erzeugt wurde. Beide werden über eine Schlüsselableitungsfunktion (Key-Derivation-Function) zu einem hybriden geteilten Geheimnis verknüpft (vgl. Abb. 1), das dann je nach Anwendungsfall weiter verwendet wird.

Diesem Ansatz folgt zum Beispiel ein Vorschlag für eine quantensichere Version von TLS 1.3, der 2020 zur Diskussion veröffentlicht wurde (siehe https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/). In jedem Fall erhöht sich der Ressourcenbedarf bei beiden Kommunikationspartnern aufgrund des zusätzlichen Post-Quanten-KEM-Verfahrens und des zusätzlichen Aufrufs der Schlüsselableitungsfunktion – wie sehr, hängt vom eingesetzten Post-Quanten-Verfahren ab.

Heutige Optionen

Nicht überall muss auf das Ergebnis des NIST-Wettbewerbs gewartet werden. Für einige Anwendungsfälle lassen sich bereits heute quantensichere Algorithmen einsetzen:

Anders als die asymmetrischen Verfahren sind heute genutzte symmetrische Verschlüsselungsalgorithmen durch die Einführung von Quantencomputern wenig bedroht. Zwar haben Quantencomputer mit Grovers Algorithmus einen Angriffspunkt für symmetrische Algorithmen, doch hebeln sie diese nicht gänzlich aus. Um das heutige Sicherheitsniveau von 128 Bit für die Blockchiffre AES auch im Zeitalter von Quantencomputern zu erhalten, reicht es, die Schlüssellänge zu verdoppeln.

Teilweise Entwarnung gibt es auch für Hashfunktionen: Zwar sind diese ebenfalls durch Grovers Algorithmus bedroht, doch Hashfunktionen mit längerem Output, etwa SHA2-256 und SHA3-384, werden als quantensicher gehandelt, da selbst Grovers Algorithmus extrem viel Zeit brauchen würde, um sie zu brechen.

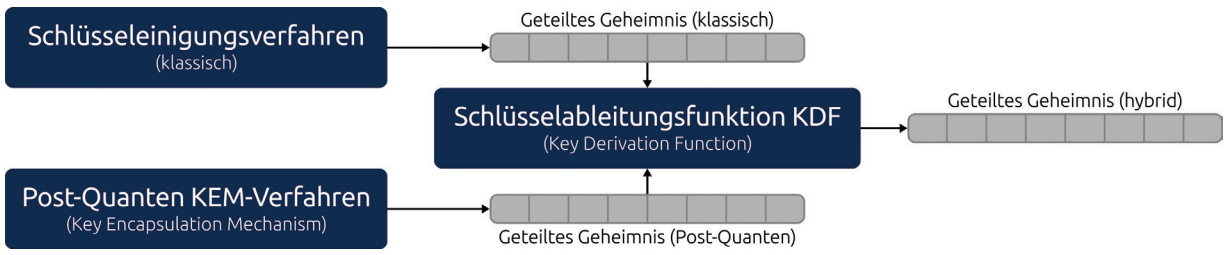

Abbildung 1: Hybride Schlüsseleinigung

Der Standardisierungsprozess des NIST

Ziel der „Post Quantum Cryptography Standardization“ ist die Standardisierung von Algorithmen für Public-Key-Encryption, die sowohl sicher gegen Angriffe durch Quantencomputer als auch gegen herkömmliche Angriffe sind. Gesucht werden sowohl Schlüsseleinigungsverfahren als auch Verfahren zur Erzeugung digitaler Signaturen.

Hierzu wurde bereits im Dezember 2016 ein Wettbewerb ausgeschrieben, der in mehrere Runden gegliedert ist – mindestens drei, vielleicht auch vier. In der ersten Runde reichten Teilnehmer ihre Kandidatenalgorithmen inklusive einer Dokumentation, mathematischer Hintergründe und Referenzimplementierungen ein. Diese sind auf der Website des NIST verlinkt und downloadbar (https://csrc.nist.gov/projects/post-quantum-cryptography). Neben der Analyse durch ein NIST-Expertenteam lebt der Wettbewerb von Hinweisen und Kryptanalyse der mathematischen Öffentlichkeit – die Auswahl der Kandidaten für die nächste Runde erfolgt jedoch durch das NIST.

Das Hauptbewertungskriterium ist die Sicherheit, die anhand von Definitionen gemessen wird, die das NIST vorgegeben hat. Für einen Algorithmus werden außerdem Parametersätze verlangt, durch welche sich die Sicherheit adaptieren lässt – von Kategorie 1 (minimal notwendige Sicherheit) bis 5 (maximal). Zweitwichtigstes Kriterium sind „Kosten“ und Performance des Algorithmus: Das umfasst die Berechnungszeit sowie die Länge von Schlüsseln, Chiffretexten oder Signaturen sowie die notwendigen Ressourcen zur Implementierung (RAM, Anzahl der Logikgatter). Weitere Kriterien sind etwa die Frage, wie einfach ein Algorithmus in bestehende Protokolle wie TLS oder SSH einzubauen ist und welche Randbedingungen bei der Lizenzierung zu beachten sind.

Eingangs hatten sich 69 Kandidaten aus verschiedensten mathematischen Richtungen qualifiziert. In der dritten Runde, die aktuell läuft, liegt ein besonderes Augenmerk auf der Performance in Internetprotokollen und auf der Sicherheit gegen Seitenkanalangriffe – weiterhin steht fortwährend die Suche nach Sicherheitslücken im Fokus. Derzeit sind noch sieben Kandidaten im Rennen (vier Schlüsseleinigungsverfahren und drei Signatur-Algorithmen). Das NIST erwartet, dass die ersten Algorithmen aus dem Pool dieser Finalisten sowie acht Backup-Algorithmen – möglicherweise nach einer vierten Runde – Anfang 2022 bereit für eine Standardisierung sein werden.

Die Bandbreite der vertretenen mathematischen Richtungen hat sich in der dritten Runde stark verengt: Unter den Schlüsseleinigungsverfahren sind drei Verfahren gitterbasiert (Crystals-Kyber, NTRU und SABER) – mit hoher Wahrscheinlichkeit wird davon eines standardisiert. Das vierte Verfahren „Classic McEliece“ basiert auf einem fehlerkorrigierenden Code. Aufgrund extrem großer Schlüssel ist es für den generellen Gebrauch in Internetprotokollen wohl nicht geeignet, kann aber wegen besonders kurzer Chiffretexte in ausgewählten Anwendungen von Vorteil sein.

Auch bei den Finalisten der Signaturverfahren erwartet das NIST, einen der beiden gitterbasierten Algorithmen Crystals-Dilithium oder FALCON zu standardisieren. Das dritte Verfahren „Rainbow“ ist der multivariaten Kryptografie zuzuordnen und dürfte aufgrund sehr großer Schlüssel wiederum nicht einfach in bestehende Protokolle integrierbar sein – für Anwendungen, die selten den öffentlichen Schlüssel austauschen müssen, ist es jedoch vielversprechend.

Absehbar ist, dass es nicht den *einen* Post-Quanten-Algorithmus geben wird, der alle Probleme löst. Stattdessen liegen die Stärken verschiedener Verfahren in verschiedenen Bereichen: Einer ist besonders schnell, der andere hat kurze Schlüssel, noch ein anderer basiert auf einem schon gut studierten Problem und gilt daher als besonders sicher. Ray A. Perlner und David A. Cooper hatten bereits 2009 in [5] einen Vergleich von benötigter Rechenzeit, Schlüssellängen und Nachrichtengrößen ausgewählter Post-Quanten-Algorithmen mit klassischen Verfahren erstellt.

Der gitterbasierte Algorithmus NTRU hat ähnlich kurze Schlüssel wie klassische Algorithmen und dabei auch sehr gute Performance. Classic McEliece besticht zwar mit kurzen Signaturen, hat jedoch den Nachteil extrem großer Schlüssel. Würde man Classic McEliece für TLS-Zertifikate der heutigen Art benutzen, die den Public Key des Eigentümers enthalten, wären diese mehrere Megabyte groß. Bei zustandsbasierten Signaturverfahren wie Lamport/Merkle und seiner bereits standardisierten Weiterentwicklung XMSS ist die Anzahl der Signaturen pro Schlüssel begrenzt. Dennoch bieten sich diese Algorithmen für spezielle Anwendungen wie das Signieren von Firmwareupdates an.

Daher plant das NIST, mehrere Algorithmen für verschiedene Anwendungsfälle zu standardisieren – beginnend mit denen, die am ausgereiftesten erscheinen. Zudem will das NIST Algorithmen aus unterschiedlichen mathematischen Gebieten auswählen, damit nicht ein einzelner neuer Angriffserfolg in einem Teilgebiet alle neu standardisierten Verfahren mit einem Mal bedroht.

Auf der Quantenresistenz von Hashfunktionen fußen darüber hinaus verschiedene Post-Quanten-Algorithmen, zum Beispiel die zustandsbehafteten hashbasierten Signaturverfahren LMS (Leighton-Micali Hash-Based Signatures) und XMSS (eXtended Merkle Signature Scheme) – beide wurden von der Internet Engineering Task Force (IETF) bereits standardisiert [3,4]. Zwar lässt sich bei diesen Verfahren ein öffentlicher Schlüssel nur für eine begrenzte Anzahl von Signaturen verwenden, doch ist das für bestimmte Anwendungsfälle völlig ausreichend.

Entscheidungshilfe für die Zukunft

Der noch nicht abgeschlossene wissenschaftliche Prozess ist der Grund für eine heute sehr anspruchsvolle Situation für IT-Entscheider. Die Gefahr, dass Investitionen in Eigen- oder Auftragsentwicklungen für quantensichere Verschlüsselung letztlich an der finalen Einschätzung der Wissenschaft und dem zukünftigen Standard vorbei getätigt werden, hält viele IT-Entscheider von Investitionen in Post-Quanten-Entwicklungen ab. Doch zunehmend drängt die Zeit: Gerade bei Produkten mit langen Lebenszyklen können Entscheidungen, die heute falsch getroffen werden, sich maßgeblich auf die nächsten 10 oder sogar 20 Jahre auswirken.

Gesichert scheint die Erkenntnis, dass es kein Standard-Verfahren für alle Anwendungsfälle geben wird – wie das zum Beispiel im Bereich der symmetrischen Verschlüsselung mit dem AES der Fall ist. Je nach Anwendungsszenario (Embedded-Kommunikation, Browser, E-Mail-Verschlüsselung) unterscheiden sich die verfügbaren Ressourcen so stark, dass man verschiedene Algorithmen brauchen wird, um die unterschiedlichen Gegebenheiten zu erfüllen. Davon ausgehend, lässt sich für manche Anwendungen das Feld der geeigneten Algorithmen aber bereits einschränken.

Sicher ist auch: Eine tragfähige kryptografische Software-Komponente für die nächsten 20 Jahre hängt weniger am einzelnen Algorithmus als viel mehr an einem belastbaren Unterbau, der zukünftige Updates ermöglicht. So sollten sich Betriebsparameter der verwendeten Verfahren an gestiegene Sicherheitsanforderungen anpassen oder ganze Algorithmen bausteinartig durch andere ersetzen lassen. Wer diese Anforderung schon bei heute geplanten Investitionen formuliert, kann auch in 10 Jahren ein produktiv laufendes System an die dann herrschende Bedrohungslage anpassen.

Es bleibt die Frage, wann es notwendig wird, zu handeln. Auch das lässt sich nur schwer allgemeingültig beantworten: In Unternehmen, in denen eine Produktgeneration zum Beispiel 1 Jahr entwickelt, 3 Jahre lang verkauft und das Produkt im Schnitt 3 Jahre lang genutzt wird, kommt die heutige Entwicklung der nächsten Produktgeneration sicherlich noch ohne Quantensicherheit aus. Bei langlebigen Industriegütern (zum Beispiel Automobile, Züge, vernetzte Produktionsanlagen) kommt man selbst bei pessimistischen Schätzungen der Verfügbarkeit von Quantencomputern erst in 20 Jahren schon heute zu der Erkenntnis, handeln zu müssen.

Auf das Ergebnis des NIST-Wettbewerbs zu warten, klingt zwar verlockend, birgt aber Risiken. Denn ob tatsächlich 2022 ein finales Ergebnis bekannt gegeben werden kann, für welche Anwendungsfälle es passt und ob es sich im Praxiseinsatz bewähren wird, all das ist derzeit völlig offen. Dass aber für jede heutige IT-Lösung ein sicherer und flexibler Update-Mechanismus für den verwendeten Algorithmen-Stack gebraucht wird, ist bereits heute völlig klar. Wer in dieser Situation also entsprechend investiert, investiert zweifelsfrei in die Zukunft. ■

Marie-Luise Groh ist Krypto-Entwicklerin, Georg Nestmann ist Geschäftsführer der comcrypto GmbH.

Literatur

[1] Teik Guan Tan, Pawel Szalachowski, Jianying Zhou, SoK: Challenges of Post-Quantum Digital Signing in Real-world Applications, in: Cryptology ePrint Archive, Report 2019/1374, November 2019, https://eprint.iacr.org/2019/1374

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), Migration zu Post-Quanten-Kryptografie, Handlungsempfehlungen des BSI, August 2020, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html

[3] D. McGrew, M. Curcio, S. Fluhrer, Leighton-Micali Hash-Based Signatures (LMS), RFC 8554, April 2019, https://tools.ietf.org/html/rfc8554

[4] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, A. Mohaisen, XMSS: eXtended Merkle Signature Scheme, RFC 8391, Mai 2018, https://tools.ietf.org/html/rfc8391

[5] Ray A. Perlner, David A. Cooper, Quantum Resistant Public Key Cryptography: A Survey, in: IDtrust 2009, Proceedings of the 8th Symposium on Identity and Trust on the Internet, April 2009, online verfügbar auf https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901595

Need to know für CISO & Co

- <kes> liefert strategisches Wissen für Security-Verantwortliche
- <kes> informiert redaktionell unabhängig zu Management und Technik der Informations-Sicherheit
- <kes> enthält das amtliche Organ des Bundesamts für Sicherheit in der Informationsverarbeitung – BSI-Forum
- <kes> kostet im Jahr weniger als zwei Beraterstunden

<kes>
Die Zeitschrift für Informations-Sicherheit

Für 139 € jährlich (inkl. MwSt. und Versandkosten) erhalten Sie alle zwei Monate eine gedruckte Ausgabe und für bis zu fünf Mitarbeiter am belieferten Standort Online-Zugriff auf alle aktuellen Beiträge sowie das <kes>-Archiv.

Online bestellen: datakontext.com/kes
oder per Mail: abo@kes.de

DATAKONTEXT