Bundesamt
für Sicherheit in der
Informationstechnik

Migration zu Post-Quanten-Kryptografie

Handlungsempfehlungen des BSI

Stand: August 2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-km21@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Hintergrund

Die Sicherheit digitaler Infrastrukturen beruht heute zu einem großen Teil auf Public-Key-Kryptografie, die sich selbst im Wesentlichen auf die angenommene Schwierigkeit zweier mathematischer Probleme stützt. Beispielsweise basiert das RSA-Verfahren auf der Tatsache, dass es im Allgemeinen schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen. Üblicherweise vereinbart man mit einem Public-Key-Verfahren („asymmetrisch“) kryptografische Schlüssel, um anschließend Nachrichten mit einem „symmetrischen“ Algorithmus (wie AES) zu verschlüsseln. Mit heutigen Mitteln sind die gängigen Public-Key-Verfahren nicht zu brechen. Dies gilt nicht mehr, wenn universelle Quantencomputer ausreichender Leistungsfähigkeit verfügbar sind.

Denn bereits 1994 wurde von Peter Shor ein Algorithmus vorgestellt, der die oben genannten mathematischen Probleme effizient lösen kann [1]. Allerdings lässt sich dieser Algorithmus nicht auf klassischen Computern realisieren, sondern nur auf damals noch rein hypothetischen Quantencomputern. Mit Entwicklung eines Quantencomputers, auf dem der Algorithmus von Shor für ausreichend große Eingabegrößen implementiert werden kann, würde somit der heutigen Public-Key-Kryptografie die Grundlage entzogen werden.

Symmetrische Verfahren sind durch Shors Algorithmus nicht gefährdet. Durch einen von Grover entwickelten Algorithmus zur Suche in unsortierten Datenbanken würde eine "Brute-Force"-Suche nach dem verwendeten Schlüssel asymptotisch deutlich beschleunigt werden [2], wenn dieser auf einem Quantencomputer realisiert werden würde. Die Verwendung von Schlüsseln mit einer Länge von 256 Bit ist aber ausreichend, um dieses Risiko auszuschließen – auch für Daten mit einem langfristigen Schutzbedarf.

Bisher ist noch kein Quantencomputer verfügbar, der zum Brechen kryptografischer Verfahren geeignet wäre. Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand bzw. der potentiellen zukünftigen Verfügbarkeit eines Quantencomputers zu erhalten, wurde vom BSI die Studie „Entwicklungsstand Quantencomputer“ in Auftrag gegeben [3]. Diese Studie haben Forscher der Universität des Saarlandes und der Florida Atlantic University durchgeführt.

Die Studie zeigt, dass aktuell eine enorme Anstrengung nötig wäre, um eine kryptografisch relevante Skalierung von Quantencomputer-Technologien vorzunehmen. Gleichzeitig aber wird deutlich, dass die Entwicklung durch starke Industrieakteure und große Forschungsprogramme an Fahrt gewonnen hat und dass weitere kommerzielle Anwendungen diese noch beschleunigen könnten.

Die Studie schätzt kurzfristige Entwicklungssprünge in Richtung kryptografisch relevanter Quantencomputer als eher unwahrscheinlich ein. Für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, ergibt sich dennoch akuter Handlungsbedarf. Hier besteht die Gefahr darin, dass Nachrichten zur Schlüsselaushandlung und die mit den ausgehandelten Schlüsseln verschlüsselten Daten auf Vorrat gesammelt und in der Zukunft mit Hilfe eines Quantencomputers entschlüsselt werden ("store now, decrypt later").

Signaturen zum Zwecke der Authentisierung dagegen haben in der Regel eine eher kurze Lebensdauer und müssen im Prinzip nur bis zum Zeitpunkt ihrer Prüfung sicher sein. Sollte ein Signaturverfahren in der Zukunft durch einen Quantencomputer gebrochen werden können, so sind die heutigen Signaturzertifikate vermutlich bereits abgelaufen. Nur bei sehr langen Gültigkeitszeiten für Signaturschlüssel ist Vorsicht geboten.

2 Post-Quanten-Kryptografie

In der kryptografischen Forschung entwickelte sich parallel zu den Fortschritten bei der Entwicklung von Quantentechnologien ein neues Arbeitsgebiet: die Post-Quanten-Kryptografie (engl. auch Quantum Safe Cryptography). Post-Quanten-Kryptografie beschäftigt sich mit der Entwicklung und Untersuchung von kryptografischen Verfahren, die auch mit Quantencomputern nicht gebrochen werden können. Diese Quantencomputer-resistenten Verfahren beruhen auf mathematischen Problemen, für deren Lösung heute weder effiziente klassische Algorithmen noch effiziente Quantenalgorithmen bekannt sind.

Von den Forschern werden verschiedene Ansätze zur Realisierung von Post-Quanten-Kryptografie verfolgt. Kandidaten für solche Verfahren basieren beispielsweise auf der Schwierigkeit, allgemeine fehlerkorrigierende Codes effizient zu dekodieren ("codebasierte Verfahren") oder auf der Schwierigkeit von bestimmten Problemen in mathematischen Gittern ("gitterbasierte Verfahren").

In den letzten Jahren hat die Post-Quanten-Kryptografie erheblich an Bedeutung gewonnen: Die amerikanische National Security Agency (NSA) hat im August 2015 vor Quantencomputern gewarnt und die Migration zu Quantencomputer-resistenten Verfahren eingeleitet. Als Begründung hat die NSA Fortschritte in Physik und Technologie angegeben, die die Entwicklung eines kryptografisch relevanten Quantencomputers ermöglichen könnten. Konkrete Quantencomputer-resistente Verfahren hat die NSA dabei nicht benannt, sondern auf die künftigen Standards des National Institute for Standards and Technology (NIST) verwiesen.

Das NIST ist als US-amerikanische Behörde für Standardisierungsprozesse zuständig. Es hat unter anderem Wettbewerbe durchgeführt, die die weltweit anerkannten Algorithmen AES und SHA-3 hervorgebracht haben. Als Reaktion auf die Ankündigung der NSA hat NIST im November 2016 einen Prozess gestartet, an dessen Ende eine Auswahl von Quantencomputer-resistenten kryptografischen Verfahren zur Verfügung stehen soll[1]. Dieser Prozess wird aber frühestens 2022/23 abgeschlossen sein.

Eine Klasse von Verfahren, die nicht im NIST-Prozess betrachtet werden, sind zustandsbehaftete hashbasierte Signaturverfahren. Dies liegt daran, dass ihre Sicherheitseigenschaften sehr gut verstanden sind und sie bereits als ausgereiftes Quantencomputer-resistente Signaturverfahren gelten. Ein entscheidender Nachteil ist jedoch die Zustandsbehaftung der Verfahren, d.h. dass der Signaturersteller exakt nachhalten muss, welche Einmal-Signaturschlüssel bereits verwendet wurden. Zudem muss bereits bei der Erstellung des privaten Schlüssels die Anzahl der mit diesem Schlüssel erstellbaren Signaturen festgelegt werden. Die zustandsbehafteten hashbasierten Signaturverfahren LMS [4] und XMSS [5] wurden von der IETF bereits standardisiert. NIST hat Ende Dezember 2019 einen Draft für eine Special Publication veröffentlicht, der diese Standards übernimmt.

Die Aktivitäten des NIST zur Standardisierung von Post-Quanten-Kryptografie werden vom BSI begrüßt. Sie haben zu einer deutlichen Intensivierung der Forschung an Quantencomputer-resistenten Verfahren geführt. Das BSI arbeitet im Bereich Kryptografie international vernetzt. Insofern ist die Ankündigung der NSA und der Standardisierungsprozess von NIST auch für das BSI bedeutsam und die Entwicklung wird aufmerksam verfolgt.

1 Siehe https://csrc.nist.gov/Projects/Post-Quantum-Cryptography für weitere Informationen zu dem NIST-Prozess

3 Handlungsempfehlungen

Aus Sicht des BSI steht die Frage, "ob" oder "wann" es Quantencomputer geben wird, nicht mehr im Vordergrund. Post-Quanten-Kryptografie wird langfristig zum Standard werden. Abhängig vom Anwendungsfall sollte aber frühzeitig (und kontinuierlich - angepasst an die aktuellen Entwicklungen) im Rahmen eines maßvollen Risikomanagements abgewogen werden, ob und wann ein Umstieg auf Quantencomputer-resistente Verfahren erfolgen sollte. Hier sollen Maßnahmen aufgezeigt werden, wie eine Migration auf Post-Quanten-Kryptografie schon heute eingeleitet werden kann.

3.1 Kryptoagilität

Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor allem darauf geachtet werden, die kryptografischen Mechanismen möglichst flexibel zu gestalten, um auf alle denkbaren Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft Algorithmen, die nicht mehr das gewünschte Sicherheitsniveau garantieren, austauschen zu können („Kryptoagilität“). Dies gilt insbesondere aufgrund der Bedrohung durch Quantencomputer – aber nicht ausschließlich: Auch klassische Angriffe können sich weiterentwickeln und einstmals als sicher eingestufte Verschlüsselungsverfahren oder Schlüssellängen obsolet machen. Kryptoagilität sollte also – unabhängig von der Entwicklung von Quantencomputern – zum Designkriterium für neue Produkte werden.

3.2 Hashbasierte Signaturverfahren für Firmware-Updates

Wie in Abschnitt 2 beschrieben, haben zustandbehaftete hashbasierte Signaturverfahren gewisse Nachteile. So können mit ihnen nur eine im Vorhinein begrenzte Anzahl von Signaturen geleistet werden. Sie eignen sich aber insbesondere für die Signatur von Firmware-Updates, da hierfür nur eine geringe Zahl von Signaturen erforderlich ist. Der Einsatz von zustandsbehafteten hashbasierten Signaturverfahren wird schon seit Längerem vom BSI empfohlen - beispielsweise in den Technischen Richtlinien TR-02102 [6] und TR-03140 [7]. Sie liefern einen wichtigen Beitrag in Richtung Kryptoagilität.

3.3 Schlüssellängen für symmetrische Verschlüsselung

Wie bereits erwähnt, sind symmetrische Verschlüsselungsalgorithmen wesentlich weniger durch die Entwicklung von Quantencomputern bedroht als asymmetrische Verfahren. Bei Verwendung von Schlüsseln mit einer Länge von 128 Bit (oder weniger) sind potentiell allerdings Quantencomputer-Angriffe mit dem Suchalgorithmus von Grover möglich. Insbesondere, wenn es auf einen langfristigen Schutz von Daten ankommt, sollte daher bei Neuentwicklungen, bei denen ein symmetrischer Verschlüsselungs-algorithmus implementiert werden soll, eine Schlüssellänge von 256 Bit vorgesehen werden.

3.4 Kurzfristige Schutzmaßnahmen

Üblicherweise wird asymmetrische Kryptografie benötigt, um ein gemeinsames Geheimnis zwischen den Kommunikationspartnern auszutauschen, aus dem dann symmetrische Sitzungsschlüssel abgeleitet werden. Als kurzfristige Schutzmaßnahme gegen Angriffe mit Quantencomputern kann für die Schlüsselableitung zusätzlich ein vorverteilter symmetrischer Langzeitschlüssel verwendet werden. Ebenso ist es möglich, einen asymmetrischen Schlüsselaustausch mit Hilfe eines vorverteilten Geheimnisses

symmetrisch zu verschlüsseln. In beiden Fällen muss jeweils natürlich das Problem der Verteilung der symmetrischen Langzeitschlüssel gelöst werden.

Für Kryptografie auf elliptischen Kurven bringt die Verwendung von geheim gehaltenen Kurvenparametern einen gewissen Schutz gegen Angriffe mit Quantencomputern. Dabei ist zu beachten, dass sich die Kurvenparameter bei Kenntnis von drei Punkten auf der Kurve berechnen lassen. Es müssen also Maßnahmen (z. B. Punktkompression) getroffen werden, um die Kurvenparameter zu schützen. Zudem muss sichergestellt sein, dass die verwendeten Kurven kryptografisch geeignet sind. Details hierzu finden sich in [8].

3.5 Hybride Lösungen

Die Quantencomputer-resistenten Verfahren, die zurzeit standardisiert werden, sind noch nicht so gut erforscht wie die „klassischen“ Verfahren (RSA und ECC). Dies gilt insbesondere mit Hinblick auf Schwächen, die sich größtenteils erst in der Anwendung zeigen wie typische Implementierungsfehler, mögliche Seitenkanalangriffe, usw. Das BSI empfiehlt daher, Post-Quanten-Kryptografie möglichst nicht isoliert einzusetzen, sondern nur „hybrid“, d.h. in Kombination mit klassischen Algorithmen. Bei einem hybriden Schlüsselaustausch müssen dafür beispielsweise die beiden ausgehandelten Geheimnisse mittels einer geeigneten Schlüsselableitungsfunktion zu einem Sitzungsschlüssel kombiniert werden. Im Hochsicherheitsbereich wird vom BSI der Einsatz von hybriden Lösungen gefordert.

3.6 Anpassung von kryptografischen Protokollen

Der Umstieg auf Quantencomputer-resistente Verfahren, insbesondere der Einsatz von hybriden Lösungen, erfordert Anpassungen in den heute verwendeten kryptografischen Protokollen. Für die Protokolle Transport Layer Security (TLS) und Internet Key Exchange (IKEv2) gibt es bereits Ansätze dafür, siehe [9] und [10]. Diese Anpassungen erfolgen unabhängig von der konkreten Auswahl von Quantencomputer-resistenten Verfahren.

3.7 Quantencomputerresistente Schlüsseleinigung

Der Handlungsbedarf bei Schlüsseleinigungsverfahren ist – wie eingangs bereits erwähnt – deutlich größer als bei Signaturverfahren. Für eine Schlüsseleinigung sind das gitterbasierte Verfahren FrodoKEM [11] und das codebasierte Verfahren Classic McEliece [12] die aus Sicht des BSI konservativste Wahl. Da der Schutz langfristiger Geheimnisse ein zeitnahes Handeln notwendig machen kann, hat sich das BSI Ende 2019 entschieden, nicht auf die Entscheidung von NIST zu warten und empfiehlt in der aktuellen Version der Technischen Richtlinie zu Algorithmen und Schlüssellängen [6] die beiden genannten Verfahren als grundsätzlich geeignet (in einer hybriden Lösung).

Mitte Juli 2020 wurden von NIST die Kandidaten für die dritte Runde des Standardisierungsprozess bekannt gegeben. Während Classic McEliece eines von den vier verbleibenden Schlüsseleinigungsverfahren ist, ist FrodoKEM von NIST auf die Liste mit den alternativen Verfahren gesetzt worden, siehe [13]. Neben Classic McEliece sind noch drei gitterbasierte Schlüsseleinigungsverfahren (CRYSTALS-Kyber, NTRU, SABER) in der dritten Runde dabei. NIST begründet die Entscheidung, FrodoKEM nur als alternatives Verfahren zu betrachten, mit der gegenüber den anderen gitterbasierten Verfahren schlechteren Perfomance. Diese ist dadurch bedingt, dass die anderen Verfahren auf Problemen in Gittern beruhen, die eine zusätzliche Struktur besitzen. Die zusätzliche Struktur bietet den Vorteil, dass die entsprechenden Verfahren effizienter sind und kleinere Schlüssel benötigen. Sie führt aber auch dazu, dass von Seiten des BSI noch nicht das

gleiche Vertrauen in die Sicherheit dieser Verfahren besteht. Auch NIST sieht eine potentielle Gefahr, dass neue Angriffe auf gitterbasierte Verfahren, die auf Problemen in „strukturierten“ Gittern beruhen, entwickelt werden könnten und sieht FrodoKEM als „conservative backup“, vgl. [13].

Aus den genannten Gründen hält das BSI an der Empfehlung für FrodoKEM fest, auch wenn FrodoKEM für spezielle Anwendungsfälle eher ungeeignet sein könnte. Die Empfehlungen in der Technischen Richtlinie werden voraussichtlich um weitere Verfahren ergänzt werden, wenn diese von NIST standardisiert wurden.

Literaturverzeichnis

[1] Shor, Peter: "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantencomputer", SIAM Journal on Computing, 1484-1509, 1997.

[2] Grover, L.: "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, , 1996.

[3] Bundesamt für Sicherheit in der Informationstechnik: "Entwicklungsstand Quantencomputer", https://www.bsi.bund.de/qcstudie, 2018.

[4] D. McGrew, M. Curcio, S. Fluhrer: "Leighton-Micali Hash-Based Signatures", RFC 8554, , 2019.

[5] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, A. Mohaisen: "XMSS: Extended hash-based signatures", RFC 8391, , 2018.

[6] Bundesamt für Sicherheit in der Informationstechnik: "TR-02102: Kryptografische Verfahren: Empfehlungen und Schlüssellängen", in der aktuellen Version auf den BSI-Webseiten verfügbar.

[7] Bundesamt für Sicherheit in der Informationstechnik: "TR-03140: Conformity assessment according to the satellite data security act (TR-SatDSiG)", in der aktuellen Version auf den BSI-Webseiten verfügbar.

[8] M. Lochter, J. Merkle: " Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, 2010 .

[9] D. Stebila, S. Fluhrer, S. Gueron: "Hybrid key exchange in TLS 1.3", Internet-Draft, https://tools.ietf.org/html/draft-stebila-tls-hybrid-design-03, 2020.

[10] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, V. Smyslov: "Multiple Key Exchanges in IKEv2", Internet-Draft, https://tools.ietf.org/html/draft-ietf-ipsecme-ikev2-multiple-ke-01, 2020.

[11] E. Alkim, J. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila: "FrodoKEM: Learning With Errors Key Encapsulation", Einreichung zum NIST-Prozess, https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[12] D. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen,E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, W. Wang: "Classic McEliece", Einreichung zum NIST-Prozess, https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[13] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone: "NISTIR 8309: Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process", https://doi.org/10.6028/NIST.IR.8309, 2020.