Whitepaper (work in progress): 2030 ist Nahe: Migration zu Quantencomputer-resistenten kryptographischen Verfahren

Version 0.8

Inhalt

1. Einleitung

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 (s. [1]).

Speziell im Zusammenhang mit Signaturen mit mittlerer Gültigkeitszeit der Zertifikate (3-5 Jahre) ist keine Hektik angebracht.

Für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, ergibt sich jedoch ggf. jetzt schon Handlungsbedarf (s. [1]). 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"). Auch bei sehr langen Gültigkeitszeiten für Signaturschlüssel ist Vorsicht geboten.

Ein Grossteil der heute auf breiter Basis eingesetzten asymmetrischen kryptographischen Verfahren kann nicht mehr als sicher betrachtet werden, sobald die Faktorisierung grosser Ganzzahlen (genauer sogenannter RSA-Moduln) und die Berechnung sogenannter diskreter Logarithmen effizient möglich ist. Peter Shor zeigte erstmals (s. [2]), dass beide Probleme asymptotisch effizient gelöst werden können, wenn ein hinreichend grosser und verlässlicher Quantencomputer verfügbar ist. Weitere Quantenalgorithmen von Grover oder Simon (s. [4] und [5]) haben zudem - obgleich nicht so drastische - Implikationen für die symmetrische Kryptografie, insbesondere auf deren Schlüssellängen und Betriebsarten.

Die amerikanische National Security Agency (NSA) hat daher bereits im August 2015 vor Quantencomputern gewarnt und die Migration zu Quantencomputer-resistenten Verfahren eingeleitet (s. [6]). Auch aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird Post-Quanten-Kryptografie langfristig zum Standard werden (s. [1]).

Dieses Whitepaper diskutiert die Migration bestehender Verfahren zu Quantencomputer-resistenten Verfahren. Grundlage dafür bilden die Ergebnisse der Quantum Safe Computing (QSC) Arbeitsgruppe von ETSI und insbesondere Überlegungen zu hybriden Ansätzen (s. [7]).

Das vorliegende Paper befasst sich mit Quantencomputer-resistenten asymmetrischen kryptographischen Verfahren (PQC-Verfahren). Es erhebt keinen Anspruch an Vollständigkeit. Es wird eine Auswahl von kryptographischen Verfahren aufgeführt, die in der akademischen Welt diskutiert werden, von derzeit aktiven Forschungsteams unterstützt werden, für reale Anwendungen praktikabel sein könnten und daher geeignete Kandidaten für die Prüfung durch verschiedene Standardisierungsorganisationen für die Standardisierung sind.

2. 2030: die Bedrohung

Das zugrundeliegende Prinzip, die bisher eingesetzten Public-Key-Verfahren wie z.B. RSA und ECDSA mit deutlich grösseren Schlüsseln als derzeit üblich in der Post-Quanten-Ära weiter zu verwenden, ist auf den ersten Blick naheliegend. Die Vorgehensweise, die Schlüsselgrössen von RSA und ECDSA zu erhöhen, um mit der ständig verbesserten Kryptoanalyse und neu entdeckten Angriffen fertig zu werden, hat zudem bereits Tradition (s. z.B. Entwicklung von SP 800-57 Teil 1 des NIST seit 2005 bis zur letzten Revision 4 [16] im Jahr 2016). Leider würde

dieses Prinzip im Zusammenhang mit Quantencomputern sehr schnell zu so grossen und unhandlichen und damit nicht mehr nutzbaren Schlüsselgrössen führen: Quantencomputer beruhen auf dem Konzept von Qubits (quantum bit), wobei jedes Qubit als Überlagerung (Superposition oder auch Kohärenz genannt) der Zustände 1 und 0 und allen, die dazwischen liegen, gleichzeitig existiert. Die Anzahl der Qubits, die auf einem Quantencomputer benötigt werden, um RSA zu brechen, wird auf 2n+3 [19] und 2n+2 [20] geschätzt, was bedeutet, dass ein Quantencomputer mit ca. 4.000 Qubits benötigt wird, um eine RSA-2048-Signatur zu brechen (weitere Optimierungen der Algorithmen sind zu erwarten, so dass die tatsächliche Zahl der benötigten Qubits voraussichtlich geringer sein wird). Der QFT-Algorithmus von Shor kann auch angepasst werden, um das Problem des diskreten Logarithmus zu lösen. Die Anzahl der Qubits, um ECDSA zu brechen, beträgt „ungefähr" 6n [8]. Das bedeutet, dass ein Quantencomputer mit ca.1.500 Qubits eine ECC-P256-Signatur brechen kann.

Folgt man der Annahme des Neven'schen Gesetz [21] (dem Quantenäquivalent des Moore'schen Gesetzes) kann man schätzen, dass die Rechenleistung von Quantencomputern gegenüber klassischen Computern mit einer „doppelt exponentiellen Rate" zunimmt. Wenn wir in einem bestimmten Jahr mit 100 Qubits beginnen und die Qubits alle 18 Monate verdoppeln, werden wir 9 Jahre später wahrscheinlich Computer mit über 6000 Qubits haben und in 32 Jahren in der Lage sein, einen RSA-Schlüssel mit 1 Million Bit zu brechen. Post-Quanten-RSA (also RSA mit solch grossen Schlüssellängen) wurde von Bernstein [22] untersucht, der die technische Machbarkeit der Implementierung eines Terabit-Schlüssels unter Verwendung von 231 4096-Bit-Primzahlen als Faktoren zeigte. Bei diesen Schlüsselgrössen belief sich jede RSA-Operation auf Dutzende oder Hunderte von Stunden. In der Praxis kann ein solches System damit wohl ausgeschlossen werden.

Google LLC, IBM und andere haben bisher Maschinen mit etwa 50 oder mehr hochwertigen Qubits entwickelt (s. [51], [52]). IBM plant (noch schneller als das Neven'schen Gesetz erwarten lassen würde) weitere Quantencomputer, die im Jahr 2021 mit 127 Qubits, im Jahr 2022 mit 433 Qubits und im Jahr 2023 mit über 1000 Qubits arbeiten sollen ([52]).

Selbst bei etwas langsameren Entwicklungsgeschwindigkeit muss man ab dem Jahr 2030 damit rechnen, dass die o.g. 6000 Qubits erreicht werden.

Unterschiedlich sieht die Situation bzgl. symmetrischer Kryptoverfahren aus. Zwar sind Angriffe gegen symmetrische Kryptoverfahren mit Hilfe von Quantencomputern und Algorithmen von Grover oder Simon (s. [4] und [5]) effektiver als Angriffe mit herkömmlichen Computern, aber man geht derzeit davon aus, dass eine Verdoppelung der effektiven Schlüssellänge diesen Vorteil von Quantencomputern wieder aufhebt. Somit wäre z.B. AES256 gegenüber einem Quantencomputer etwa so sicher wie AES128 gegenüber herkömmlichen Computern.

Wenn man von der Verfügbarkeit ausreichend mächtiger Quantencomputer in naher Zukunft ausgeht, ist es naheliegend, diese nicht nur als Werkzeug zum Angriff gegen klassische Kryptoverfahren einzusetzen, sondern auch zu untersuchen, wie mit ihrer Hilfe Quantencomputer-resistente Kryptoverfahren realisiert werden könnten. Die Verwendung von Quantencomputern zur Durchführung bestimmter kryptographischer Operationen wird dabei Quantenkryptographie genannt. Entsprechende Operationen nutzen typischerweise die Quanteneigenschaften von Überlagerung, Interferenz und Verschränkung aus, die von klassischen Computern nicht reproduzierbar sind. Unter quantenverstärkter Sicherheit [25] versteht man dann die Erweiterung klassischer Nicht-Quantensysteme, die sich der Quantentechnologie bedienen oder durch sie ergänzt werden, um ihre Fähigkeit zu

verbessern, ihre Daten und Transaktionen gegen Gegner zu sichern, die möglicherweise voll quantenfähig sind.

Während die Quantenschlüsselverteilung (QKD) (s. [26], [27]) häufig mit (allgemeiner) Quantenkryptographie gleichgesetzt wird, basiert QKD auf dem Vernam-One-Time-Pad und ist daher eher nur für Schlüsselaustausch und Verschlüsselung geeignet.

Quantenforscher haben verschiedene quantendigitale Signaturverfahren eingeführt (s. [28] - [31]), die jedoch, da sie sich typischerweise auf QKD beziehen, besser als Datenauthentifizierungsschemata bezeichnet würden.

3. Verfahren

3.1. Übersicht zu PQC-Verfahren

Aufgrund obiger Betrachtungen in Abschnitt 1.2.2 scheiden klassische Kryptoverfahren wie RSA und ECDSA mit sehr grossen Schlüsseln (mittelfristig) aus, und können allenfalls für eine kurze Übergangsphase (d.h. maximal in den nächsten 9 Jahren) genutzt werden. Signaturen 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 bereits jetzt Vorsicht geboten.

Quantenerweiterte Verfahren spielen nach aktuellem Forschungsstand speziell für elektronische Signaturen (noch) keine Rolle.

Mittel -und langfristig sollte man sich also auf PQC-Verfahren konzentrieren.

Unter PQC-Verfahren verstehen wir in dieser Studie Kryptoverfahren (im speziellen asymmetrische Kryptoverfahren), die nach aktuellem Stand der Forschung möglicherweise ausreichende Sicherheit gegen Angriffe, die die Fähigkeiten und Eigenschaften von Quantencomputern nutzen, bieten können, also „Quantencomputer-resistent" sind. Dabei nutzen die Verfahren selbst zur Vorbereitung und Durchführung keine Unterstützung von Quantencomputern.

Die bisher in der Literatur und Forschung betrachteten Quantencomputer-resistenten asymmetrischen kryptographischen Verfahren lassen sich aktuell in fünf Familien basierend auf den den Sicherheitsannahmen zugrundeliegenden mathematischen Problemen einteilen[1]:

- Gitterbasierte Verfahren, bei denen die Sicherheit von der Schwierigkeit abhängt, ein kurzes oder nächstes Vektorproblem in einem Gitter zu lösen.
- Multivariate Primitive, bei denen die Sicherheit von der Schwierigkeit abhängt, ein System von multivariaten Polynomgleichungen zu lösen.
- Code-basierte Primitive, bei denen die Sicherheit von der Schwierigkeit abhängt, ein Dekodierungsproblem in einem linearen Code zu lösen.

[1] In diesem Text werden kryptographische Verfahren mit fortgeschritteneren Funktionen wie identitätsbasierter Verschlüsselung oder Gruppensignaturen nicht berücksichtigt.

- Hash-basierte Primitive, bei denen die Sicherheit von der Schwierigkeit abhängt, Kollisionen oder Urbilder in kryptographischen Hash-Funktionen zu finden.
- Isogenie-basierte Schlüsselprimitive, bei denen die Sicherheit davon abhängt, wie schwierig es ist, eine unbekannte Isogenie zwischen einem Paar übersingulärer elliptischer Kurven zu finden.

Es ist möglich, die Verfahren der Schlüsselherleitung und der Authentifizierung innerhalb jeder Familie weiter zu kategorisieren. Die Verfahren der Schlüsseleinrichtung sind meistens:

- Schlüsselvereinbarungs-Verfahren, bei denen zwei Parteien auf sichere Weise einen gemeinsamen symmetrischen Schlüssel aus Informationen erzeugen, die von beiden Parteien eingebracht werden, z.B. durch den Austausch von öffentlichen Schlüsseln untereinander; oder
- Schlüsseltransport-Verfahren, bei denen eine Partei einen symmetrischen Schlüssel erzeugt und diesen sicher mit einer zweiten Partei teilt, z.B. indem sie ihn mit dem öffentlichen Schlüssel verschlüsselt der zweiten Partei sendet.

In ähnlicher Weise sind auch die Authentifizierungsverfahren meist:

- Fiat-Shamir-Signaturverfahren (s. [11]), die aus interaktiven Protokollen zum Nachweis der Kenntnis aufgebaut sind; oder
- Hash and Sign Signatur-Verfahren, die aus Falltür-Einwegfunktionen aufgebaut sind.

3.2. Standardisierung

Um die Entwicklung neuer Quantencomputer-resistenter und praktisch nutzbarer Verfahren zu erleichtern, hat das National Institute of Standards and Technology (NIST) 2016 einen Standardisierungsprozess eingeleitet (s. [10]). In ihrer Ausschreibung forderte das NIST die Forscher auf, Verfahren einzureichen, die zu einem neuen Standard werden und somit die derzeitigen Verfahren, die anfällig für Angriffe von Quantencomputern sind, ersetzen können. Dieser Prozess steht Einreichern aus der ganzen Welt offen und folgt dem Geist früherer Wettbewerbe, die zur Standardisierung des weit verbreiteten Blockchiffrierungsstandards Advanced Encryption Standard (AES) oder des standardisierten Hash-Algorithmus SHA-3 (SHA, Secure Hash Algorithm) geführt haben. Der Umfang des PQC-Standardisierungsprozesses ist jedoch viel grösser als bei früheren Wettbewerben. Dies liegt daran, dass das NIST parallel Verfahren für Verschlüsselung mit öffentlichem Schlüssel und digitale Signaturverfahren fordert. Zudem ist der Lösungsraum für PQC-Verfahren viel breiter als für Blockchiffrierungen oder Hash-Funktionen. Daher kann das NIST die Regeln und Auswahlkriterien auf der Grundlage neuer Forschungsergebnisse ändern und wird höchstwahrscheinlich (einzelnen) keinen Gewinner auswählen. Darüber hinaus erklärte das NIST, dass das Verfahren nicht als Wettbewerb, sondern vielmehr als Bemühen der Gemeinschaft zu sehen sei, mehrere Algorithmen zu finden, die für eine zukünftige Verwendung geeignet sind.

Der NIST-Standardisierungsprozess für Post-Quantum-Kryptographie (PQC-Prozess des NIST) wird in die drei Runden durchgeführt. Von den 82 Einreichungen möglicher Kandidaten, die beim NIST eingingen, wurden 69 für Runde 1 zugelassen, die sowohl die Mindestannahmekriterien als auch die Einreichungsanforderungen erfüllten. Die erste Runde dauerte bis Januar 2019, in der die Kandidaten-Algorithmen auf der Grundlage ihrer Sicherheit, Leistung und anderer Merkmale bewertet wurden. Das NIST wählte 26 Algorithmen aus, die für weitere Analysen in die zweite Runde kamen. Nach einem

Evaluierungs- und Auswahlprozess auf Basis von öffentlichem Feedback und interner Überprüfung des NIST wurden diejenigen Verfahren identifiziert, die als Finalisten in die dritte Runde der Überprüfung einziehen (s. [24]):

Die Verschlüsselungs- und Schlüsselvereinbarungs- bzw. übertragungsverfahren der dritten Runde sind:

- Classic McEliece (s. [43]),
- CRYSTALS-KYBER (s. [44]),
- NTRU (s. [45], [46]) und
- SABER (s. [38]).

Die Finalisten der dritten Runde für digitale Signaturen sind:

- CRYSTALS-DILITHIUM (s. [40]),
- FALCON (s. [41]) und
- Rainbow (s. [42]).

Diese Finalisten werden am Ende der dritten Runde für die Standardisierung in Betracht gezogen. Darüber hinaus werden acht alternative Kandidaten-Algorithmen ebenfalls in die dritte Runde vorrücken: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic und SPHINCS+. Diese zusätzlichen Kandidaten werden noch für die Standardisierung in Betracht gezogen, obwohl dies am Ende der dritten Runde wahrscheinlich nicht mehr der Fall sein wird. Das NIST hofft (und betrachtet man die derzeitigen Veröffentlichungen im Bereich der Forschung, tut sie das zurecht), dass die Bekanntgabe dieser Finalisten und zusätzlichen Kandidaten dazu dient, die Aufmerksamkeit der kryptographischen Gemeinschaft während der nächsten Runde auf sich zu lenken.

Eine Besonderheit stellen sogenannte zustandsbehaftete hashbasierte Signaturen (stateful-hash-based signatures) dar, eine besondere Klasse von Signaturschemata mit bestimmten Einschränkungen, aus der sich derzeit die zwei Vertreter

- XMSS (eXtended Merkle Signature Scheme) [12] und
- LMS (Leighton-Micali Signatures) [13]

bei der Internet Engineering Task Force (IETF) und beim NIST in der Normung befinden, so dass Standards früher als beim o.g. PQC-Prozess des NIST erwartet werden können.

Der Vorteil, den statusbehaftete Hash-basierte Signaturen gegenüber zustandslosen Hash-basierten Signaturen haben, ist die relativ kleinere Signaturgrösse. Auf der anderen Seite muss der Unterzeichner bei statusbehafteten Hash-basierten Signaturen die Schlüsselverwendung oder den „Status" so verfolgen, dass alle Schlüssel einmalig verwendet werden. Wie von NIST und den eingegangenen öffentlichen Kommentaren erkannt [14], können Stateful-Hash-basierte Signaturen in Anwendungen bereitgestellt werden, in denen die Signaturerstellung mit Hilfe des privaten Schlüssels nicht häufig ausgeführt wird, während die Überprüfung der Signatur mit Hilfe des öffentlichen Schlüssels häufiger erfolgen kann. Die genannten Anwendungsfälle betreffen die Codesignatur und die Ausstellung von PKI-Stammzertifikaten von Zertifizierungsstellen.

An der PQC-Normung sind im Weiteren auch die Normungsorganisationen ETSI und ISO mit eigenen Arbeitsgruppen beteiligt. Derzeit sieht es jedoch so aus, als würden sich ETSI und ISO bei der anfänglichen Auswahl von Verfahren auf das NIST stützen.

Ferner werden derzeit in mehreren europäischen Forschungsprojekten, z.B. PROMETHEUS (http://www.h2020prometheus.eu/) und FutureTPM (https://futuretpm.eu/), die Effizienz, Sicherheit und Praktikabilität von Quantencomputer-resistenten Verfahren untersucht. Schliesslich wurden auf nationaler Ebene kürzlich mehrere PQC-bezogene öffentlich geförderte Projekte (Aquorypt, QuaSiModO, QuantumRISC, PQC4MED, FLOQI, SIKRIN-KRYPTOV und KBLS) nach einer Ausschreibung des Bundesministeriums für Bildung und Forschung gestartet (s. [9]).

Zurzeit zieht jedoch der PQC-Prozess des NIST die grösste Aufmerksamkeit auf sich. Man darf annehmen, dass die Verfahren, die nun in Runde 3 untersucht werden, auch Einfluss auf die übrigen genannten Standardisierungsbemühungen und Untersuchungen haben werden. Tatsächlich erscheint es zum jetzigen Zeitpunkt eher unwahrscheinlich, dass im Rahmen der (internationalen) Standardisierung weitere grundsätzlich neue, noch nicht im PQC-Prozess des NIST betrachtete Verfahren auftauchen werden. 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 (s. [1]).

4. Migration

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 (s. [1]).

Speziell im Zusammenhang mit Signaturen mit mittlerer Gültigkeitszeit der Zertifikate (3-5 Jahre) ist keine Hektik angebracht (PAPER).

Für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, ergibt sich jedoch ggf. jetzt schon Handlungsbedarf (s. [1]). 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"). Auch bei sehr langen Gültigkeitszeiten für Signaturschlüssel ist Vorsicht geboten.

Es muss also bereits jetzt diskutiert werden, wie eine Migration auf Post-Quanten-Kryptografie für Hersteller und Anwender zu einem vollständig quantensicheren kryptographischen Zustand (Fully Quantum Safe Cryptographic State, FQSCS) schon heute eingeleitet werden kann.

Ein Migrationsrahmen und der Migrationsplan, der ihn dokumentiert, wird in [7] beschrieben und umfasst wie bei jeder Art von Migration die folgenden drei Stufen:

1) Inventarisierung.
2) Vorbereitung des Migrationsplans.
3) Ausführung der Migration.

Ziel der Migration ist der Weg vom nicht-Quanten-sicheren kryptographischer Zustand - dem „Anfangszustand", in dem kryptographische Werte klassische, nicht-Quanten-resistente

Kryptographie verwenden, zu einem vollständig quantensicheren kryptographischen Zustand (Fully Quantum Safe Cryptographic State, FQSCS) - den angestrebte „Endzustand" des Systems, in dem alle kryptographischen Werte Quanten-resistente Kryptographie verwenden.

Für die Zwischenschritte werden dazu in [1] folgende Massnahmen aufgezeigt:

- Kryptoagilität
  Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor 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 der Bundesdruckerei GmbH werden.
- Hashbasierte Signaturverfahren für Firmware-Updates
  Zustandsbehaftete hashbasierte Signaturverfahren haben 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 oder Code Signing, da hierfür z.B. nur eine geringe Zahl von Signaturen erforderlich ist. Der Einsatz von zustandsbehafteten hashbasierten Signaturverfahren wird schon seit Längerem vom BSI empfohlen (s. [48], [49]).
- Schlüssellängen für symmetrische Verschlüsselung
  Auch wenn der Fokus dieses Textes auf asymmetrischen Verfahren liegt und symmetrische Verschlüsselungsalgorithmen wesentlich weniger durch die Entwicklung von Quantencomputern bedroht sind als asymmetrische Verfahren, sollte bei Schlüsseltransportverfahren etc. doch beachtet werden, dass bei Verwendung von Schlüsseln mit einer Länge von 128 Bit (oder weniger) Quantencomputer-Angriffe mit dem Suchalgorithmus von Grover möglich sind. 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.
- 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.
- 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.

- 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 z.B. [47]]. Diese Anpassungen erfolgen unabhängig von der konkreten Auswahl von Quantencomputer-resistenten Verfahren.
- Quantencomputerresistente Signaturverfahren
  Zurzeit gibt es aufgrund des Ressourcenbedarfs bestehender PQC Verfahren für einzelne Anwendungen, die auf der Nutzung von Smartcards oder anderen Devices beruhen, keine befriedigende Alternative zu RSA oder EC. Es kann jedoch erwartet werden, dass diese Verfahren weiterentwickelt und optimiert werden. Diese Entwicklungen sollten von Herstellern unterstützt und begleitet werden.
- Quantencomputerresistente Schlüsseleinigung
  Der Handlungsbedarf bei Schlüsseleinigungsverfahren ist deutlich grösser als bei Signaturverfahren. Für eine Schlüsseleinigung sind das gitterbasierte Verfahren FrodoKEM [50] und das codebasierte Verfahren Classic McEliece [10] 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 Technischen Richtlinie zu Algorithmen und Schlüssellängen [49] die beiden genannten Verfahren als grundsätzlich geeignet (in einer hybriden Lösung).

Literatur

[1] Migration zu Post-Quanten-Kryptografie, Handlungsempfehlungen des BSI, August 2020

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM review, vol. 41, no. 2, pp. 303–332, 1999

[3] Teik Guan Tan und Jianying Zhou, "A Survey of Digital Signing in the Post Quantum Era", Cryptology ePrint Archive

[4] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Physical review letters, vol. 79, no. 2, p. 325, 1997.

[5] Simon, D.R. (1994), "On the power of quantum computation", Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on: 116–123, retrieved 2011-06-06

[6] Information Assurance by the NSA, Commercial National Security Algorithm Suite, August 2015, www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

[7] Migration strategies and recommendations to Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)

[8] D. J. Bernstein, "Comparing proofs of security for lattice-based encryption", Second PQC Standardization Conference, https://cr.yp.to/papers/latticeproofs-20190719.pdf

[9] Förderung von Forschungsvorhaben zum Thema „Post-Quanten-Kryptografie" im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020". Bundesanzeiger vom 22.08.2018

[10] "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms", 81 Federal Register 92787 (December 20, 2016), pp. 92787-92788. https://federalregister.gov/d/2016-30615

[11] Amos Fiat, Adi Shamir: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Andrew M. Odlyzko (Hrsg.): Advances in Cryptology – CRYPTO' 86 (= Lecture notes in computer science. Band 263). Springer, Berlin / Heidelberg 1987, ISBN 3-540-18047-8, S. 186–194.

[12] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle signature scheme," Available Online: https://tools.ietf.org/html/rfc8391, 2018 [last accessed: September 2020].

[13] F. T. Leighton and S. Micali, "Large provably fast and secure digital signature schemes based on secure hash functions," 1995, uS Patent 5,432,852.

[14] L. Marks and E. Clendening, "Stateful hash-based signatures, "Available Online: https://csrc.nist.gov/CSRC/media/Projects/statefulhash- based-signatures/documents/stateful-HBS-misuse-resistancepublic- comments-April2019.pdf, 2019 [last accessed: September 2020].

[15] P. Wallden and E. Kashefi, "Cyber security in the quantum era", Commun. ACM, vol. 62, no. 4, p. 120, 2019.

[16] E. Barker, "SP 800-57 part 1 rev. 4 recommendation for key management part 1: General," NIST special publication, vol. 800, p. 57, 2016.

[19] Y. Takahashi and N. Kunihiro, "A quantum circuit for shor's factoring algorithm using 2n+2 qubits," Quantum Information & Computation, vol. 6, no. 2, pp. 184–192, 2006.

[20] S. Beauregard, "Circuit for shor's algorithm using 2n+3 qubits," arXiv preprint quant-ph/0205095, 2002.

[21] K. Hartnett, "A new law to describe quantum computing's rise?" Available Online: https://www.quantamagazine.org/does-nevens-lawdescribe-quantum-computings-rise-20190618/, 2019 [last accessed: September 2020].

[22] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, "Post-quantum RSA," in International Workshop on Post-Quantum Cryptography. Springer, 2017, pp. 311–329.

cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology, 2019.

[24] NISTIR 8309, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process", Available Online:https://csrc.nist.gov/publications/detail/nistir/8309/final

[25] P. Wallden and E. Kashefi, "Cyber security in the quantum era", Commun. ACM, vol. 62, no. 4, p. 120, 2019.

[26] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci., vol. 560, no. 12, pp. 7–11, 2014.

[27] A. K. Ekert, "Quantum cryptography based on bell's theorem", Physical review letters, vol. 67, no. 6, p. 661, 1991.

[28] D. Gottesman and I. Chuang, "Quantum digital signatures," arXiv preprint quant-ph/0105032, 2001.

[30] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," Nature communications, vol. 3, p. 1174, 2012.

[31] W. Li, R. Shi, and Y. Guo, "Blind quantum signature with blind quantum computation," International Journal of Theoretical Physics, vol. 56, no. 4, pp. 1108–1115, 2017.

[38] "Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM", Available Online: https://eprint.iacr.org/2018/230.pdf, 2018 [last accessed: September 2020].

[40] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and D. Stehle, "Crystals- dilithium: A lattice-based digital signature scheme", IACR Cryptology ePrint Archive , 2017, https://eprint.iacr.org/2017/633

[41] Fouque, P-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., and Z. Zhang, "Falcon: Fast-Fourier lattice- based compact signatures over NTRU", IACR Cryptology ePrint Archive , 2018, https://falcon-sign.info/

[42] Ding, J. and D. Schmidt, "Rainbow, a New Multivariable Polynomial Signature Scheme", 2005, https://link.springer.com/chapter/10.1007/11496137_12

[43] McEliece R (1978) A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report, DSN PR 42-44. NASA. Available at https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF

[44] CRYSTALS-Kyber (version 2.0) – Submission to round 2 of the NIST post-quantum project. Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé.

Specification document (part of the submission package). Available at https://pq-crystals.org/kyber/data/kyber-specification-round2.pdf [last accessed: September 2020].

[45] Institute of Electrical and Electronics Engineers (2009) IEEE Standard 1363.1-2008 - Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices (IEEE, Piscataway, New Jersey, United States). https://doi.org/10.1109/IEEESTD.2009.4800404

[46] American National Standards Institute (2010) ANSI X9.98-2010 -Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry (ANSI, New York City, United States). Available at https://webstore.ansi.org/standards/ascx9/ansix9982010r2017

[47] Draft IETF draft-whyte-qsh-tls13-01: "Quantum-safe hybrid (QSH) ciphersuite for Transport Layer Security (TLS) version 1.3 (draft RFC)", 20 September 2015.

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

[49] 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.

[50] 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.

[51] Arute, F., Arya, K., Babbush, R. et al.: Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5

[52] Gambetta, J.: „IBM's Roadmap For Scaling Quantum Technolog, IBM Research", IBM Research Blog, https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/, [last accessed: November 2020].