Verbundschlussbericht

zum Gesamtvorhaben „QuantumLeap – Der Quantensprung für unsere Wirtschaft“

Aufgabenstellung

Die gegenwärtig stattfindenden Entwicklungen im Bereich der Quantencomputer könnten nach heutiger Einschätzung zu vielfältigen Konsequenzen führen, die für ein Unternehmen Kosten und Aufwände verursachen können. Es handelt sich dabei um Ereignisse, die unterschiedliche Risiken für Unternehmen mit sich bringen. Da niemand die Zukunft vorhersagen kann und alle Arbeiten rund um Quantencomputer derzeit Gegenstand laufender Forschung sind, können keine der Risiken mit einer gewissen Wahrscheinlichkeit vorhergesagt werden. Ein wichtiger Aspekt dieses Projekts war es, diese Risiken zu erforschen und Gegenmaßnahmen zu erproben. Die Bewertung der Eintrittswahrscheinlichkeit dieser Ereignisse, insbesondere in Bezug auf das Sicherheitsrisiko für kryptographische Verfahren durch die Verfügbarkeit eines Quantencomputers, erfordert stets Einzelfallbewertungen und ist im Allgemeinen nicht vollständig objektiv zu erfassen.

Die Ursache liegt in der Komplexität und Heterogenität realer IT-Systemumgebungen. Die Sicherheitsgarantien vieler sicherheitsrelevanter Anwendungen in solchen IT-Systemumgebungen beruhen auf den dort verwendeten kryptographischen Komponenten.

Die grundlegenden kryptographischen Bausteine werden als kryptographische Primitiven bezeichnet. Die Sicherheitsgarantie einer Primitiven beruht in den meisten Fällen auf mindestens einer Annahme. Die Annahmen können verschiedene Formen annehmen. Beispiele hierfür sind die Faktorisierungsannahme, die RSA-Annahme und die Schwierigkeiten bei der Berechnung eines diskreten Logarithmus in spezifischen mathematischen Strukturen. Diese Annahmen müssen jedoch nicht immer mathematischer Natur sein. Ein Beispiel dafür ist die Pseudozufälligkeit bei einer Hashfunktion oder einer symmetrischen Verschlüsselung. In diesem Fall sind eben die bisherigen mathematischen Annahmen der Faktorisierung und des diskreten Logarithmus von einem Quantencomputer betroffen. Seit 1994 ist aus der Arbeit „Algorithms for quantum computation: Discrete logarithms and factoring“ von Peter Shor bekannt, dass ein Quantencomputer diese mathematischen Probleme effizient berechnen kann. Sollten Quantencomputer im ausreichenden Reifegrad verfügbar sein, sind die Annahmen über die Schwierigkeit solcher Probleme nicht mehr gültig. Das ist das eingangs angesprochene Risiko, welches sicherheitstechnischer Natur ist.

Die deutsche Finanzwirtschaft ist ein Paradebeispiel für komplexe IT-Systemverbünde und Anwendungen, die extensiv auf sicheren kryptographischen Verfahren aufbauen, um die Sicherheit der Vorgänge zu garantieren. Zudem sind diese IT-Systemverbünde häufig systemrelevant und zählen damit im Sinne der KRITIS-Verordnung zu den kritischen Infrastrukturen in Deutschland.

Vor diesem Hintergrund ist die Aufgabenstellung des Projekts, die Anwendungs- und Systemlandschaft der deutschen Finanzwirtschaft auf die Bedrohung durch Quantencomputer zu untersuchen und Gegenmaßnahmen zu erarbeiten, um sich auf die möglichen Risiken vorzubereiten.

Planung und Ablauf des Vorhabens

Insgesamt hatte der Ablauf des Vorhabens keine nennenswerten Änderungen in der ursprünglichen Planung erfordert. Die einzigen Ausnahmen waren, dass ein Arbeitspaket schneller abgeschlossen werden konnte als ursprünglich angedacht. Auf der anderen Seite gab es leichte Verzögerungen wiederum bei einem anderen Arbeitspaket. Die Covid19 Pandemie hatte keinen gravierenden Einfluss auf den Ablauf des Projektes.

Die ursprüngliche Planung des Vorhabens sah folgendermaßen aus.

Geplante Dauer des Vorhabens: Aufgrund des hohen fachlichen Anspruchs der geplanten Forschungsarbeiten, sowie durch die systembedingte Komplexität der in der Finanzwirtschaft eingesetzten Prozesse und Systeme, war eine Projektlaufzeit von drei Jahren notwendig.

Die geplante Dauer des Vorhabens konnte abschließend auch eingehalten werden.

Die Geplante Struktur des Vorhabens: Die Arbeiten in Quantum Leap wurden in sechs Arbeitspaketen erbracht, die zu großen Teilen aufeinander aufbauten, aber jeweils einen eigenen inhaltlichen Schwerpunkt hatten.

Der Ablauf des Projektes folgte erfolgreich dieser Struktur.

AP1 -- Anforderungsanalyse: Zu Beginn des Projekts wurde eine Anforderungsanalyse der Systeme und Prozesse der Finanzwirtschaft durchgeführt. Ziel dieser Analyse war die Identifikation und umfassende Dokumentation von relevanten Prozessen, IT-Systemen und Hardwarekomponenten, mitsamt aller relevanten Parameter, die kryptographische Mechanismen verwenden, die von einem Angreifer mit Quantencomputern gebrochen werden konnten und somit potentiell einer Umstellung auf Verfahren der PQ-Kryptographie bedurften.

Dieses Arbeitspaket hat dem ursprünglich geplanten Lösungsweg gefolgt und konnte die geplanten Ergebnisse erreichen. Die Ergebnisse wurden in einer kondensierten Form auf der INFORMATIK2021 für die Öffentlichkeit frei zugänglich veröffentlicht[1].

AP2 – Sicherheitsanalyse: Auf Basis der vorangegangenen Anforderungsanalyse erfolgte anschließend eine Sicherheitsanalyse der identifizierten Protokolle und Komponenten. Ziel dieser Analyse war es, die tatsächliche Gefährdungslage fundiert zu ermitteln und geeignete Gegenmaßnahmen zu definieren.

Die erfolgte Sicherheitsanalyse konnte letztendlich wie geplant durchgeführt werden, sodass eine Übersicht der Gefährdungsgrundlage geschaffen worden war. Basierend darauf konnten auch Gegenmaßnahmen beschrieben werden in Form von kryptographischen Ersatzkandidaten aus dem aktuellen Stand der Technik der Post-Quanten Kryptographie, welche die bedrohten im Einsatz befindenden kryptographischen Verfahren ersetzen sollten. Hier konnte auch erfolgreich das Risiko abgewendet werden, dass die im Projekt ausgewählten Ersatzkandidaten letztendlich nicht standardisiert worden wären.

AP3&4 – Prototypenentwicklung in den Komponenten der IT-Infrastruktur und Eingeschränkter Hardware: Anschließend erfolgte die prototypische Implementierung von Komponenten der IT-Infrastruktur, bei der für geeignete Teile der IT-Infrastruktur die definierten Gegenmaßnahmen aus AP2 umgesetzt wurden. Entsprechend erfolgte auch eine prototypische Implementierung von Teilen der Firmware von Hardwarekomponenten.

Auch hier hat es keine gravierenden Änderungen gegeben. Eine Ausnahme stellt die prototypische Entwicklung der sicheren Firmware-Updates mithilfe der „Leigthon-Micali Sigantur“ (LMS) durch Reiner SCT und das FZI. Hier wurden die Arbeiten innerhalb weniger Monate abgeschlossen, sodass das FZI vor der ursprünglichen Planung mit dem Arbeitspaket der Evaluation anfangen konnte. Währenddessen waren die Arbeiten an prototypischen Implementierungen von Komponenten der IT-Infrastruktur durch Atruvia und FZI etwas aufwendiger, sodass sich der Arbeitsaufwand dadurch dennoch ausgeglichen hat.

[1] https://dl.gi.de/items/d029fbce-5c67-45ff-8c7a-a4f43a148de1

AP5 – Evaluationsarbeiten: Alle Implementierungen wurden anschließend hinsichtlich verschiedener Performance- und Sicherheitskriterien evaluiert.

Für Implementierungen auf eingeschränkter Hardware wurden Untersuchungen bezüglich der Seitenkanalresistenz angestellt. Dazu wurde vom FZI und SRC eine Recherche des akademischen Stands der Technik gemacht und die gravierendsten Seitenkanalangriffe aus der Literatur validiert um den Bedarf nach zusätzlichen Sicherheitsmaßnahmen in den Implementierungen von Verfahren der Post-Quanten Kryptographie auf eingeschränkter Hardware zu bestätigen. Auf der anderen Seite wurde in enger Zusammenarbeit zwischen Atruvia, Reiner SCT und dem FZI Performance-Evaluationen der selbst entwickelten Prototypen durchgeführt. Hierbei wurde zusätzlicher Forschungsbedarf und der Bedarf nach quantensicheren Programmierschnittstellen in den Browser-Technologien festgestellt.

AP6 – Migrationskonzept und Standardisierungsvorbereitungen: Abschließend wurden die erarbeiteten Projektergebnisse für die Verwendung in Standardisierungsgremien aufgearbeitet und zu einem Migrationsleitfaden zusammengefasst.

Der finale Migrationsleitfaden wurde noch nicht veröffentlicht, obwohl seine Veröffentlichung durch Atruvia und das FZI für das Jahr 2024 fest eingeplant ist. Die Gründe hierfür sind aktuell folgende: Zum einen plant das NIST, im Jahr 2024 die endgültigen Standards für die neuen kryptographischen Verfahren herauszugeben, und zum anderen ist in der kryptographischen wissenschaftlichen Community eine Debatte über die Quantensicherheit vielversprechender kryptographischer Verfahren entstanden. Beide Ereignisse sollen abgewartet werden, um eine fundierte Meinung zu bilden, die in den finalen Migrationsleitfaden einfließen soll.

Zusammenfassend ist zu betonen, dass die Bearbeitung der einzelnen Arbeitspakete in enger gemeinschaftlicher Zusammenarbeit erfolgte, da nur wenige der vorgesehenen Arbeitsschritte thematisch isoliert betrachtet werden konnten. Vielmehr war die gemeinsame Expertise aller Projektpartner für die erfolgreiche Bearbeitung fast jeden Arbeitsschrittes notwendig.

Wissenschaftlicher und technischer Stand an den angeknüpft wurde

Zu Beginn des Projektes befand sich das NIST in der dritten Runde[2] der Standardisierung, in der noch 15 Verfahren zur Auswahl standen und von der wissenschaftlichen Community analysiert wurden. Dementsprechend war der akademische Stand der Technik zu dieser Zeit sehr heterogen, da sich die Forschung explorativ mit den zur Auswahl stehenden Verfahren auseinandersetzte.

Es wurden erste Anpassungsvorschläge für sicherheitsrelevante Protokolle im Bereich des sicheren Web-Surfens (HTTPS), VPN (OpenVPN) sowie die Anpassung aktueller Zertifikatsketten und der Public-Key-Infrastruktur (PKI) hin zu einem quantensicheren Zustand erarbeitet, wobei verschiedene Verfahren der Post-Quanten-Kryptographie zum Einsatz kamen.

Zu Beginn des Projektes wurde das Verfahren SIKE[3] als ein sicherer und vielversprechender Ersatz für klassische kryptographische Verfahren aus dem Bereich der Elliptischen-Kurven-Kryptographie betrachtet. Im Laufe des Projektes wurde jedoch von belgischen Wissenschaftlern eine vernichtende Arbeit veröffentlicht, die die Sicherheit dieses Verfahrens vollständig gebrochen hatte[4]. Die

[2] https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
[3] https://sike.org/
[4] https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf

Projektergebnisse und Arbeiten waren von dieser Arbeit nicht betroffen, da SIKE als ein weniger geeigneter Kandidat für die erarbeiteten Anwendungsfälle im Rahmen des Konsortiums identifiziert worden war.

Der Stand der Technik bei den Implementierungen von Verfahren der Post-Quanten-Kryptographie wies einen geringen Reifegrad auf und war noch stark explorativ. Im Laufe des Projektes wurden immer mehr Arbeiten veröffentlicht, die verschiedene Implementierungsstrategien für die im Projekt relevanten Verfahren erforschten. Diese Arbeiten sind im Laufe des Projekts auch in die Entscheidungsfindung bei der Sicherheitsanalyse eingeflossen. Aufgrund der Unzufriedenheit mit dem Stand der Technik der Implementierungen im Bereich der hash-basierten digitalen Signaturen wurde im Rahmen des Projektes eine Implementierung entwickelt, die über den Stand der Technik hinausgeht. Diese wird derzeit ebenfalls für eine Publikation vorbereitet.

Der Stand der Technik in Bezug auf die Implementierungssicherheit von Verfahren der Post-Quanten-Kryptographie, insbesondere im Bereich der Seitenkanalangriffe und ihrer Gegenmaßnahmen, bestand aus vereinzelten Arbeiten, die sich im Laufe des Projektes bis heute zu einem höheren Reifegrad weiterentwickelt haben. Leider hat sich bis heute kein einheitlicher Konsens über effiziente Gegenmaßnahmen im akademischen Stand der Technik gebildet.

Der Stand der Technik bezüglich der Kryptoagilität war zu Beginn des Projektes nahezu nicht vorhanden. Erst im Laufe des Projektes wurden mehrere Arbeiten veröffentlicht, die sich ausführlicher mit dieser Problematik befassten. Alle diese Arbeiten (ca. 30) wurden gesichtet und im Migrationsleitfaden zusammenfassend aufbereitet, damit sich die Lesende Person selbst eine Meinung bilden kann.

Zusammenarbeit mit anderen Stellen

Das FZI als Konsortialführer war im Projekt kontinuierlich auf die Zusammenarbeit mit Atruvia, Reiner SCT und SRC angewiesen.

Die Zusammenarbeit mit Atruvia erfolgte in Form von:

- Gemeinsamen bilateralen virtuellen Arbeitstreffen, um das fachliche Verständnis beider Seiten für die Inhalte zu stärken und zu vertiefen.
- Gemeinsamem Bearbeiten von Arbeitsdokumenten wie dem Migrationsleitfaden.
- Unterstützung bei der Recherche zu relevanten Standards im Bereich der deutschen Kreditwirtschaft.

Die Zusammenarbeit mit SRC erfolgte in Form von:

- Regelmäßigen virtuellen Austauschterminen zum aktuellen Fortschritt im Projekt bei der Seitenkanalanalyse von Implementierungen der Post-Quanten-Kryptographie.
- Gemeinsamem Bearbeiten von Arbeitsdokumenten wie einer Sammlung von Steckbriefen zu Seitenkanalangriffen und Gegenmaßnahmen.
- Gemeinsamem Durchführen von Seitenkanalangriffen aus der Literatur zu Validierungszwecken der veröffentlichten Angriffe.

Die Zusammenarbeit mit Reiner SCT erfolgte in Form gemeinsamer bilateraler virtueller Arbeitstreffen zum Diskutieren und Austauschen bezüglich des Fortschritts bei der Implementierung von Firmware-Signaturen und der Evaluationskriterien.

Der Austausch mit dem gesamten Konsortium fand über die gesamte Projektlaufzeit hinweg in Form regelmäßiger virtueller Austauschtermine, Workshops sowie von vom FZI geplanten Konsortial- und Meilensteintreffen statt, teilweise auch in Präsenz oder hybrid. Im Rahmen mehrerer Workshops versuchte das FZI, wissenschaftlich relevante Inhalte von hoher fachlicher Tiefe für die Industriepartner verständlich aufzubereiten, um das Verständnis für die Post-Quanten-Kryptographie und den relevanten Hintergrund zu fördern und zu diskutieren.

Zudem fand im Verlauf des Projekts auch eine Kommunikation mit dem Referat BSI über die Projektergebnisse statt.

Eingehende Darstellung: Ergebnisse

Im Folgenden sollen zusammengefasst die wichtigsten Projektergebnisse vorgestellt werden.

Arbeitspaket 1 – Anforderungsanalyse

Die Anforderungsanalyse ist ein unverzichtbarer Schritt in jedem Projekt, das die Migration zur Post-Quanten-Kryptographie zum Ziel hat. Dies liegt daran, dass die Anforderungen und die Inventarisierung (also die Identifikation der zum aktuellen Zeitpunkt eingesetzten kryptographischen Bausteine) eine notwendige Grundlage für alle weiteren Überlegungen bilden.

Das Vorgehen bestand aus einer Reihe konsortiumsweiter Workshops zur Erfassung und Diskussion der Anwendungs- und Standardlandschaft in der deutschen Kreditwirtschaft. Anschließend wurden vom FZI alle erfassten Anwendungen und Standards überprüft, und die relevanten Informationen aus den teilweise sehr umfangreichen Standards (ca. 800 Seiten) extrahiert. Es wurden mehrere Feedbackschleifen mit den Projektpartnern eingerichtet, um die extrahierten Informationen zu diskutieren und abzustimmen. Das Ergebnis war die folgende Zusammenfassung.

Geld Abhebe-Szenario / Point-of-Sale (PoS Kartenzahlungen)

Als Quelle wurden hier die Spezifikationen/Standards von der EMV-Contact[5] Reihe herangezogen. Die folgenden Details wurden aus der Quelle extrahiert:

- Welche Akteure und Systeme sind zum Funktionieren dieses Szenarios notwendig und an welchen sicherheitsrelevanten Protokollen nehmen diese teil?
- Welche sicherheitsrelevanten Protokolle kommen in der Anwendung zum Einsatz?

Als Akteure, sowie Soft- und Hardwaresysteme wurden identifiziert: Terminals, Herausgeber von Chipkarten, Zertifizierungsstellen für Chipkarten, Chipkarten und Besitzer von Chipkarten.

Die identifizierten sicherheitsrelevanten Protokolle sind:

- Authentifikation des Kartenbesitzers: Generierung der PIN (DIN/TS 16591[6]), Verschlüsselte Übertragung der PIN (ISO 9564[7])
- Übertragung von Autorisierungsnachrichten (ISO 8583[8])
- Das sichere Abheben des Bargelds: Kontaktbehaftete/Kontaktlose Kommunikation mit dem Terminal (EMV-SDA/DDA/CDA (offline/online))
- Bezahlen an einem PoS-Gerät: EMV-CDA/DDA (online)

[5] https://www.emvco.com/emv-technologies/contact/
[6] Extern nicht vefügbar
[7] https://www.iso.org/standard/68669.html
[8] https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:en

Online Banking

Als Quelle wurden hier die folgenden Spezifikationen/Standards herangezogen:

- Financial Transaction Services (FinTS[9])
- Electronic Banking Internet Communication Standard (EBICS[10])
- Access to Account (XS2A[11])

Die folgenden Details wurden aus der Quelle extrahiert:

- Welche Akteure und Systeme sind zum Funktionieren dieses Szenarios notwendig und an welchen sicherheitsrelevanten Protokollen nehmen diese teil?
- Welche sicherheitsrelevanten Protokolle kommen in der Anwendung zum Einsatz?

Als Akteure, sowie Soft- und Hardwaresysteme wurden identifiziert: Browser-Clients, Intermediäre, Smartphones, Sicherheitsmedien (z.B. Chipkarten oder andere personalisierte Security-Gerätschaften), Chipkartenleser, Rechenzentren von Kreditinstituten, Middleware, Benutzer (Kunden, Herausgeber von Signaturkarten, Herausgeber von Aufträgen/Geschäftsvorfällen), Back-End Administratoren.

Die identifizierten sicherheitsrelevanten Protokolle sind:

- Authentifikation der Benutzer im Back-End via Passwort oder nPA.
- Multi-Faktor Authentifikation von Benutzern.
- Autorisierung von Dritten zum Zugriff auf Konten-/Account-informationen (XS2A)
- Autorisierung und Vertraulichkeit von Geschäftsvorfällen/Aufträgen von Kunden zum Kreditinstitut (FinTS über PIN/TAN oder HBCI; EBICS)
- Transportverschlüsselung (TLS[12])

Inventarisierung der Kryptographischen Komponenten in der Landschaft der Sicherheitsrelevanten Protokolle

Alle bisher genannten sicherheitsrelevanten Protokolle wurden gesichtet und die eingesetzten kryptographischen Komponenten wurden extrahiert.

Die Kategorien an eingesetzten kryptographischen Verfahren und die aktuell empfohlenen Implementierungen sind:

- Pseudozufallszahlengeneratoren (PRNG)
- Schlüsselableitungsfunktionen (KDF)
- Digitale Signaturen: PKCS#1 RSA[13] (EMSA-PSS, EMSA-PKCS1-v1_5)
- (Hybride) Public-Key Verschlüsselung: PKCS#1 RSA (RSA-OAEP)
- Symmetrische Verschlüsselung: AES-CBC
- Hashfunktionen: SHA1&2
- Message Authentication Codes (MACs): AES-CBC-MAC

Die Schutzziele, Protokollbeschreibungen, Schlüsselgrößen und viele weitere Implementierungsdetails wurden ebenfalls erfasst in Form von Sequenzdiagrammen und Dokumentation, aber hier aus Platzgründen nicht aufgeführt.

---

[9] https://www.hbci-zka.de/spec/4_1.htm
[10] https://www.ebics.de/de/ebics-standard
[11] https://www.berlin-group.org/nextgenpsd2-downloads
[12] https://tools.ietf.org/html/rfc8446
[13] https://tools.ietf.org/html/rfc8017

Arbeitspaket 2 – Sicherheitsanalyse der eingesetzten Bausteine und Protokolle

Die Inventarisierten kryptographischen Verfahren wurden in diesem Arbeitspaket auf ihre Bedrohungslage durch Quantencomputer hin analysiert.

Analyse der Bedrohung durch Quantencomputer:

- Pseudozufallszahlengeneratoren (PRNG)
- Schlüsselableitungsfunktionen (KDF)
- Digitale Signaturen: PKCS#1 RSA[14] (EMSA-PSS, EMSA-PKCS1-v1_5)
- (Hybride) Public-Key Verschlüsselung: PKCS#1 RSA (RSA-OAEP)
- Symmetrische Verschlüsselung: AES-CBC
- Hashfunktionen: SHA1&2
- Message Authentication Codes (MACs): AES-CBC-MAC

In Grau markiert: Im Laufe des Projekts wurde nur eine unzureichende Menge an Informationen zu den eingesetzten PRNGs (Pseudozufallszahlengeneratoren) und KDFs (Schlüsselableitungsfunktionen) gesammelt, sodass keine abschließende Meinung gebildet werden konnte. Die Hintergründe hierfür liegen darin, dass Informationen zu diesen Arten von Verfahren in der Regel nicht öffentlich zugänglich sind.

In Rot markiert: Die digitalen Signaturen sowie die Implementierungen der Public-Key-Verschlüsselung in der deutschen Kreditwirtschaft haben einen klaren Schwerpunkt auf dem RSA-Verfahren, das auf dem Faktorisierungsproblem basiert. "Shor's Algorithmus" für Quantencomputer stellt daher eine reale Bedrohung dar, und es besteht dringender Handlungsbedarf für den Beginn einer Migration dieser Verfahren.

In Orange markiert: Das sind tatsächlich Verfahren aus der Kategorie der symmetrischen Kryptographie, die nur durch den "Grover's Algorithmus" betroffen sind. In der Theorie führt dieser Algorithmus dazu, dass die Schlüssellängen verdoppelt werden müssen, zum Beispiel erfordert ein Wechsel von AES-128 auf AES-256. Der akademische Stand der Technik sowie das BSI sind sich jedoch einig, dass dieser theoretische Algorithmus in der Praxis des Quantencomputings eine Reihe zusätzlicher Hürden zu bewältigen hat im Vergleich zum "Shor's Algorithmus".

Schlussendlich wurde als Ergebnis des Arbeitspakets 2 beschlossen, dass die Hauptpriorisierung auf den digitalen Signaturen und der Public-Key-Verschlüsselung liegt. Daraufhin haben wir begonnen, die Verfahren der Post-Quanten-Kryptographie zu sichten und ihre Eignung als Ersatzkandidaten zu analysieren.

Die betrachteten Verfahren der quantensicheren Public-Key Verschlüsselung sind: Kyber, Lightsaber, FrodoKEM, Alle NTRU Varianten, SIKE[15], BIKE, HQC.

Die betrachteten Verfahren der quantensicheren Digitalen Signaturen sind: Dilithium, Falcon, SPHINCS, LMS.

Zur Bewertung der Eignung dieser Verfahren wurden die folgenden Anforderungen erhoben.

- **Anforderung an den Langzeitspeicher** war 100kB für Signaturen und Verschlüsselung. Daher fielen raus: BIKE, ntru, ntruprime. Bei den digitalen Signaturen wurde Dilithium, Sphincs und LMS präferiert.

[14] https://tools.ietf.org/html/rfc8017

[15] Zum Zeitpunkt der Analyse war SIKE noch in der Auswahlliste des NIST

- **Anforderung an die RAM:** Für die Eignungsbeurteilung sollte die Minimalfunktion der relevanten Algorithmen zum Einsatz kommen. Kyber, Lightsaber, SIKE wurden präferiert. FrodoKEM und HQC waren aufgrund des hohen Bedarfes an dieser Stelle ausgeschlossen.
- **Ausführungszeiten**: Kyber und LightSaber haben hier die Führung bei den Verschlüsselungsverfahren gehabt. Dilithium und Falcon waren in der Führung bei den digitalen Signaturen.
- **Bandbreitenbedarf**: Es hat sich ein ähnliches Bild wie bei den Ausführungszeiten ergeben.

Fazit zur quantensicheren digitalen Signaturen: Zum Zeitpunkt der Analyse scheinte Dilithium das flexibelste Verfahren zu sein wegen den unterschiedlichen Implementierungsstrategien im Hinblick auf minimalen RAM-Verbrauch oder Ausführungszeiten. LMS ist zwar zustandsbehaftet, viel langsamer und hat eine fast doppelt so große Signatur wie Dilithium, aber die sonstigen Anforderungen sind im besseren Maße erfüllt. Falcon wurde vor allem mit dem Fokus auf eine effiziente Verifikation entwickelt, was jedoch zu erheblichen Effizienzeinbußen beim Signieren führt. Für den Anwendungsfall der Firmware-Signaturen wurde LMS gewählt.

Fazit zur quantensicheren Public-Key Verschlüsselung: Am Ende übrig gebliebene Verfahren sind Kyber-512 und Lightsaber, die von den Anforderungen her nahezu gleichauf sind. Da Kyber auf derselben Arithmetik wie Dilithium aufbaut, wurde letztendlich auch Kyber als Ersatzkandidat bestimmt.

Arbeitspaket 3 – Prototypische Implementierung von Komponenten der IT-Infrastruktur

Im Arbeitspaket 3 wurde eine prototypische Implementierung im Kontext des Online-Bankings vorgenommen. Durch die Analyse hat sich gezeigt, dass additiv zur Transportverschlüsselung eine Verschlüsselung von sensitiven Informationen (Login-Credentials) auf Anwendungsebene stattfindet. Hierfür wird aktuell eine asymmetrische Verschlüsselung mittels RSA genutzt. Diese Verschlüsselung ist nicht PQ-sicher und muss in den Folgejahren angepasst werden. Im Projekt wurde dies prototypisch bereits durchgeführt.

Insgesamt ist die prototypische Umsetzung gelungen und das bisherige Verfahren konnte durch PQ-sichere Verfahren getauscht werden. Bei dieser Implementierung wurden verschiedene Herausforderungen deutlich:

- Zum einen sind PQC-Algorithmen / –Verfahren keine sog. „Drop-In Replacements“, d.h. ein Tausch der Verfahren bedarf in Teilen auch eines Umbaus der Anwendung. So auch in diesem Fall, da mit den neuen PQC-Verfahren nur Schlüssel zwischen Kommunikationspartner sicher ausgetauscht werden können und keine direkte Verschlüsselung möglich ist. Daher wurde die Anwendung auf ein zweistufiges Verfahren erweitert. Zum Schlüsselaustausch wird Kyber verwendet. Anschließend erfolgt dann eine Verschlüsselung der Credentials mittels AES.
- Zum anderen hat sich gezeigt, dass die zum Zeitpunkt des Prototypen vorliegenden Software-Bibliotheken nicht out-of-the-box einsetzbar waren. Es wurde die Crystal Kyber Implementierung[16] genutzt. Zum Implementierungszeitpunkt war die Typescript-Implementation von Steven Fisher die beste Alternative für Javascript, was seitens Online-Banking benötigt war. Diese NPM-Packages konnten nur mit Workarounds für eine Browser-Anwendung gangbar gemacht werden und wären auch für den Praxiseinsatz zu groß. Insofern hat sich insgesamt gezeigt, dass eine PQ-sichere Implementierung bereits jetzt gelingen kann, aber dazu auch Änderungen in der eingesetzten Anwendung – hier Online

[16] https://pq-crystals.org/kyber/software.shtml

Banking – notwendig werden können als auch die Standard-Software-Bibliotheken noch weiterentwickelt werden sollten, um einen effiziente PQC-Migration zu erleichtern.

Arbeitspaket 4 – Prototypische Implementierung auf Hardwarekomponenten

Im Zuge der Anforderungsanalyse wurde festgestellt, dass ein bedeutender Anwendungsfall asymmetrischer Kryptographie die Sicherung von Firmwareupdates auf den verwendeten Geräten ist. Die zugrundeliegende Hardware, wie beispielsweise Kartenlesegeräte, betreibt Software, die für die Bereitstellung von Funktionalitäten erforderlich ist und als Firmware bezeichnet wird. Änderungen an dieser Funktionalität können notwendig werden, sei es aufgrund von erweiterten Funktionen seitens der Hersteller oder aufgrund geänderter Vorschriften. Auch die Entdeckung von Sicherheitslücken in der Firmware erfordert eine Aktualisierung. Daher ist es von entscheidender Bedeutung, sicherzustellen, dass die Firmware der verwendeten Geräte aktualisiert werden kann. Dabei besteht das Risiko, dass Angreifer versuchen, bösartige Updates einzuschleusen, die beispielsweise Hintertüren enthalten. Aus diesem Grund ist es unerlässlich, bei der Installation von Firmwareupdates sicherzustellen, dass diese tatsächlich vom Hersteller stammen. Hierbei kommen kryptographische Signaturverfahren zum Einsatz. Bei der Analyse hat sich gezeigt, dass das Signaturverfahren LMS für diesen Anwendungsfall geeignet ist.

Das LMS-Signaturverfahren wurde erfolgreich auf Kartenlesegeräten von ReinerSCT implementiert. Aufgrund der begrenzten Speicherkapazität dieser Geräte wurde eine speichersparende Variante des LMS-Verfahrens entwickelt. Dabei wird ausgenutzt, dass bei der Verifikation von LMS-Signaturen nur ein Teil der Signatur im Speicher geladen werden muss. Anschließend kann ein Zwischenwert berechnet, der vorherige Teil gelöscht und der nächste Teil der Signatur geladen werden. Somit ist nicht die gesamte Signatur gleichzeitig im Speicher erforderlich. Diese Berechnungsmethode wird als Streaming bezeichnet.

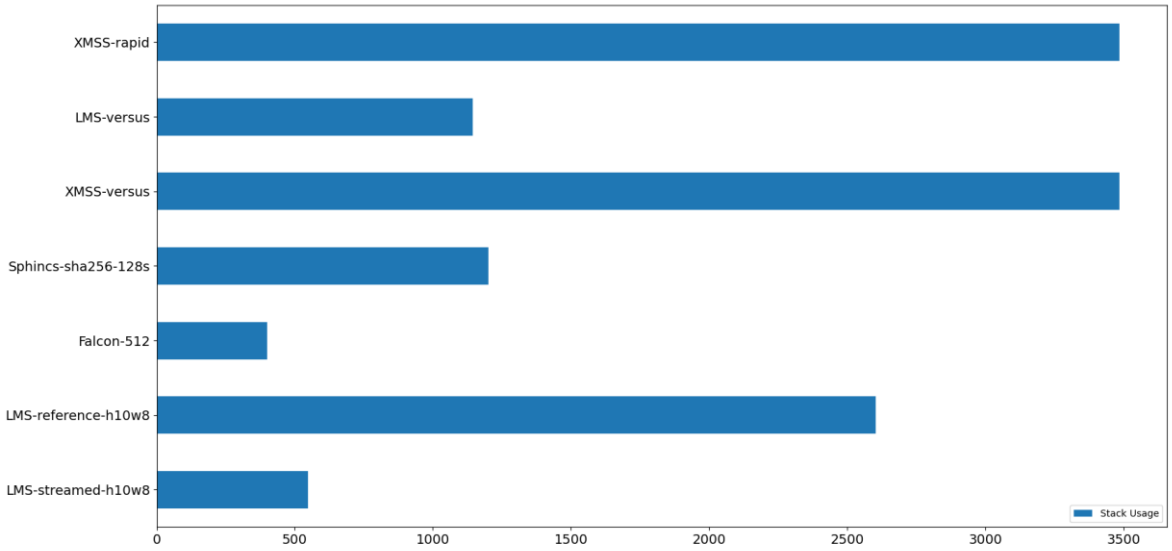
Arbeitspaket 5 – Evaluation der Implementierung

Die Implementierungen aus den Arbeitspaketen 4&5 mussten abschließend in Form einer Evaluation validiert werden.

Leighton-Micali Signatur (LMS)

Für LMS und den Anwendungsfall der Firmware-Signaturen waren Seitenkanäle nicht relevant, da es nur auf die Implementierung der Verifikation der Signatur ankommt. Der Hintergrund ist, dass für die Verifikation einer Signatur keine Geheimnisse verarbeitet werden und damit Seitenkanalangriffe, die darauf ausgelegt sind geheime Informationen über Seitenkanäle wie z.B. Stromverbrauch, zu extrahieren, keine Rolle spielen. Am relevantesten für die Evaluation waren die Performance-Indikatoren für die Implementierung von LMS und der Vergleich zum aktuellen Stand der Technik.

Das Zielsetzung der eigenen Implementierung war den RAM-Verbrauch tiefer zu senken als es im Stand der Technik zum Zeitpunkt des Projektes der Fall war. Wie die Grafik unten zeigt wurde dies erreicht.



Das vom Konsortium entwickelte Verfahren heißt in der Grafik „**LMS-streamed-h0-w8**“ weist in der Evaluation um mehrere Faktoren geringeren Verbrauch des RAMs auf als es bei anderen Verfahren aus dem Stand der Technik der Fall ist. Für eine wissenschaftliche Publikation werden die Ergebnisse noch entsprechend aufbereitet.

CRYSTALS-Dilithium

Im Vergleich zu LMS ist der Stand der Technik bei der effizienten Implementierung von Dilithium wesentlich fortgeschrittener. Zu diesem Zeitpunkt sind Implementierungen verfügbar, die auch für den Anwendungsfall der Kartenechtheitsprüfungen beim Abheben von Bargeld geeignet sind. Daher bestand kein Bedarf, eine eigene Implementierung von Dilithium zu erstellen. Ein weiterer Unterschied besteht darin, dass im Anwendungsfall der Kartenechtheitsprüfung Seitenkanalangriffe eine wichtige Rolle spielen. Dies liegt daran, dass in diesem Anwendungsfall die Signaturoperation im Vordergrund steht. Während dieser Operation werden in der Chipkarte geheime Informationen verarbeitet, die über mögliche Seitenkanäle extrahiert werden könnten. Daher ist es notwendig, dass ein kryptographisches Verfahren in diesem Anwendungsfall resistent gegen Seitenkanalangriffe ist. Aus diesem Grund haben sich das FZI und SRC in enger Zusammenarbeit der Analyse der Seitenkanäle bei Dilithium gewidmet.

Es konnten die folgenden Ergebnisse erreicht werden:

- Literaturrecherche zu möglichen Angriffsszenarien für Seitenkanalanalysen und Gegenmaßnahmen für Dilithium. Dieses Thema entwickelt sich im Moment sehr stark, insbesondere nach der Nominierung der Standardisierungskandidaten. Ausgehend davon wurde ein Angriffsszenario für praktische Tests sowie mögliche Gegenmaßnahmen zur Erprobung ausgesucht.
- Durchführung von Seitenkanalanalysen einer Dilithium-Implementierung auf Cortex M4 Chip. Die Hardwareplattform wurde durch den NIST Wettbewerb für die Messung der Performance auf Plattformen mit beschränkten Ressourcen vorgegeben und erleichtert den Zugang zu bereits vorhandenen Implementierungen. Das ausgewählte Angriffsszenario für die Testdurchführung wurde sehr nah an der klassischen DPA gewählt wie sie z.B. auch auf AES als symmetrischen Verfahren angewendet werden kann und zielt auf die Berechnung von modularen Multiplikationen. Im Unterschied zum klassischen Angriff steigert sich die Anzahl und der Hypothesenraum für die Schlüsselbestandteile. Üblich sind Hypothesen über einen Raum von 8 Bit also 256

Möglichkeiten, bei AES werden davon nur 16 Komponenten benötigt. Bei Dilithium musste ein Hypothesenraum von 23 Bit, also ungefähr 8 Millionen Möglichkeit für 256 Komponenten durchsucht werden, was die Durchführbarkeit des Angriffes signifikant erschwert. Dafür konnte eine Optimierung des Angriffs gefunden werden, welche gut handhabbar ist.

- Parallel dazu wurde ein anderes Angriffsszenario untersucht, bei der die Berechnung einer SHA-3 Hashfunktion analysiert wurde. Hier spielt die Speicherplatz-Optimierung der Implementierung von Dilithium dem Angreifer in die Hände und der Angriff ist leichter umzusetzen, falls durchführbar. Insgesamt gibt es in der vorhandenen Literatur noch weitere Angriffsszenarien, welche je nach Art der Implementierung anwendbar sind. Die beiden betrachteten Analysen stellen eine repräsentative Auswahl dar.
- Weiterführend wurden auch erste Versuche mit möglichen Gegenmaßnahmen unternommen. Eine frei verfügbare gehärtete Implementierung erwies sich dabei als nicht geschützt für das von uns untersuchte Angriffsszenario. Daher wurde eine eigene Implementierung mittels eines Shuffling der 256 verschiedenen Werte untersucht. Diese erwies sich als gehärtet gegen das analysierte Angriffsszenario. Damit ist die Frage der Seitenkanalresistenz aber noch nicht abschließend geklärt. Das Shuffling erschwert nur den Angriff, macht ihn aber nicht unmöglich. Daher muss dies Gegenmaßnahme durch weitere unterstützt werden. Daneben gibt es wie angedeutet mehrere unterschiedliche Angriffsmöglichkeiten, welche alle jeweils durch separate Gegenmaßnahmen abgesichert werden müssen. Schließlich gibt es neben den Seitenkanalangriffen auch die Klasse der Fehlereinstreuungsangriffe, die nicht nur die Implementierung bei der Berechnung abhören, sondern auch versuchen diese beispielsweise durch Glitches in der Stromversorgung oder durch elektromagnetische Einstrahlung zu stören und die Auswirkung davon auswerten.
- Ein weiteres Fazit ist, dass die ausgewählte Hardwareplattform ungeeignet ist um eine Seitenkanalresistenz umzusetzen, da diese bereits leicht zu erkennende Seitenkanalinformationen einem Angreifer zur Verfügung stellt. Als alternative Hardwareplattformen würden sich FPGAs anbieten, womit das Seitenkanalverhalten spezieller Hardware simulieren ließe.
- Insgesamt konnte ein gutes Verständnis aufgebaut werden, welche Angriffe möglich sind und wie diesen begegnet werden kann. Damit kann dieses Wissen im nächsten Schritt in die Arbeit von SRC als Prüfstelle einfließen.

Arbeitspaket 6 – Migrationskonzept und Standardisierungsvorbereitung

Alle Erfahrungen und Lessons Learned aus dem Projekt sowie der ursprünglichen Planung wurden ausführlich im Konsortium diskutiert und in Form eines Migrationsleitfadens zusammengefasst, um Unternehmen bei der Orientierung in diesem Thema zu unterstützen. Leider gestaltet sich die Veröffentlichung des Migrationsleitfadens schwieriger als gedacht und wurde bisher noch nicht durchgeführt. Ein wichtiger Grund hierfür ist, dass das Konsortium noch abwartet, bis das NIST die endgültigen Standards offiziell bekannt gibt. Derzeit existieren diese nur in Form von sogenannten Entwürfen (Drafts), die sich glücklicherweise mit den im Projekt ausgewählten Verfahren decken.

Der Migrationsleitfaden behandelt die folgenden Themengebiete.

Allgemeiner Teil – Empfehlungen Weltweit

Das Ziel dieses Kapitels ist es, die Leserinnen und Leser über den weltweiten aktuellen Stand der Migration zur Post-Quanten-Kryptographie zu informieren und wichtige Konzepte verständlich und prägnant zu umreißen. Um dieses Ziel zu erreichen, wurden alle derzeit öffentlich zugänglichen Empfehlungen von Behörden und Institutionen weltweit gesichtet und hinsichtlich ihrer Aussagen

über Handlungsempfehlungen zur Migration zusammengefasst. Insgesamt sind es Stand heute 26 Leitfäden und Empfehlungen. Als Beispiel wird in diesem Bericht die Auswertung der Empfehlungen des BSI dargelegt, wie es im Abschlussbericht geplant ist einzureichen.

Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Das BSI fungiert in Deutschland als kompetenter Ansprechpartner für Wirtschaft, Wissenschaft, Gesellschaft sowie für die Bürgerinnen und Bürger in allen Fragen der Informationssicherheit. In diesem Rahmen formuliert das BSI Empfehlungen zu sicheren kryptografischen Verfahren, einschließlich der Empfehlungen zur Post-Quanten-Kryptographie und den Risiken von Quantencomputern. Die Befugnisse des BSI wurden in der Vergangenheit mehrfach erweitert, und die sicherheitstechnischen Empfehlungen des BSI wurden ebenfalls mehrfach aktualisiert. Daher ist anzunehmen, dass die hier dargelegte Zusammenfassung der Empfehlungen des BSI zum Thema Post-Quanten-Kryptografie nur eine Momentaufnahme ist und fortlaufend weiterentwickelt wird.

Das BSI führt eine übersichtliche Auflistung[17] über seine Auseinandersetzung mit dem Thema der Quantentechnologien und quantensicheren Kryptografie, wobei die Post-Quanten-Kryptographie eine wichtige Rolle einnimmt[18].

Innerhalb dieser Auflistung finden sich mehrere Dokumente, die das Thema der Post-Quanten-Kryptografie näher beleuchten.

Migration zu Post-Quanten-Kryptografie: Handlungsempfehlungen des BSI

Das BSI schreibt dazu das Folgende in ihrem aktuellen Leitfaden "Kryptografie quantensicher gestalten: Grundlagen, Entwicklungen, Empfehlungen"

> "Das BSI hat im März 2020 die Handlungsempfehlungen „Migration zu Post-Quanten-Kryptografie“ veröffentlicht [BSI_PQ_Info], die sehr positiv aufgenommen wurden und zu vielen Rückfragen und Anmerkungen geführt haben. Diese Handlungsempfehlungen sind allerdings sehr knapp gehalten und inzwischen nicht mehr auf dem aktuellsten Stand."

Dieses Dokument umfasst nur 9 Seiten und dessen Kernaussagen werden viel ausführlicher im aktuellen Leitfaden angegangen, sodass wir allen Interessierenden zum Thema Migration, Post-Quanten-Kryptographie und Handlungsempfehlungen empfehlen stattdessen den aktuellen Leitfaden "Kryptografie quantensicher gestalten: Grundlagen, Entwicklungen, Empfehlungen" zu lesen.

Kryptografie quantensicher gestalten: Grundlagen, Entwicklungen, Empfehlungen

Der Leitfaden des BSI verfolgt in vielen Punkten ähnliche Ziele wie unser Migrationsleitfaden. Insbesondere legt das BSI in seinem Leitfaden einen großen Wert auf die Erklärung der Grundlagen der Post-Quanten-Kryptographie und der Quantencomputer. Alle Interessierten finden dort eine ausführliche Auseinandersetzung mit diesen Grundlagen. Es sei auch erwähnt, dass das BSI sich in diesem Leitfaden wieder auf die Arbeitshypothese für den Hochsicherheitsbereich aus den Antworten auf die kleinen Anfragen BT-Drs-19/25208 und BT-Drs-19/26340 bezieht, wonach Anfang der 2030er-Jahre kryptographisch relevante Quantencomputer zur Verfügung stehen werden.

---

[17] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html

[18] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie/post-quanten-kryptografie_node.html

Zuerst beschreibt der Leitfaden den Hintergrund für den Bedarf an Post-Quanten-Kryptografie. Auf jedes Grundlagenthema des Quantencomputings wird knapp eingegangen, um den Lesenden zu erklären, wie ein Quantencomputer funktioniert, was Quantenalgorithmen sind und wie sie die gegenwärtigen kryptographischen Verfahren bedrohen, sowie welche Entwicklungen noch durchlaufen werden müssen, um zu einem für die Kryptographie relevanten Quantencomputer zu gelangen.

Beim Thema der Post-Quanten-Kryptographie erklärt das BSI knapp die heterogenen Grundlagen dieser Verfahren, ohne allzu tief in die Mathematik einzusteigen. Dazu gehören die Grundlagen der codebasierten, gitterbasierten und hashbasierten kryptographischen Verfahren. Anschließend gibt das BSI einen Überblick über die weltweit stattfindenden Standardisierungsbestrebungen und die neuen Verfahren für Schlüsseltransport und digitale Signaturen. Die Bemühungen des BSI werden ebenfalls in diesen Überblick eingegliedert. Im Anschluss an die einfachsten Bausteine der Post-Quanten-Kryptographie widmet sich der Leitfaden komplexeren Anwendungen dieser, den kryptographischen Protokollen, dazu zählen das IKEv2[19], TLS[20] und die X.509-Zertifikate[21].

Für Interessierte an der Quantum Key Distribution (QKD) bietet der Leitfaden eine differenzierte Betrachtung dieses Themas und weist auf die Vorteile und Schwierigkeiten dieser Technik hin.

Allgemeiner Teil – Post-Quanten Kryptographie

In diesem Kapitel werden kurz die Grundlagen von Post-Quanten Kryptographie umrissen und Steckbriefe zu allen relevanten Verfahren aufgeführt. Als Beispiel soll hier das vom BSI vorgeschlagene Verfahren FrodoKEM dienen. Insgesamt sind aktuell 8 Verfahren auf diese Art beschrieben. Den Unternehmen soll dies als Übersicht zur Entscheidungsfindung dienen.

FrodoKEM ist ein gitterbasiertes Verfahren. Das Verfahren wurde im Jahr 2016 eingeführt und beim Wettbewerb des NIST eingereicht[22]. Das BSI hat im Jahr 2019 dieses Verfahren in ihre Empfehlungen aufgenommen.[23] Im Jahr 2022 ist dieses Verfahren in der Runde 3 des NIST-Wettbwerbs ausgeschieden. Die Gründe für das Ausscheiden sind im Status-Bericht des NIST angegeben.[24] Der wichtigste Grund ist wohl die vergleichsweise schlechte Performance des Verfahrens. Im April 2023 hat die ISO/IEC JTC 1/SC 27/WG 2 zugestimmt, mit der Standardisierung von FrodoKEM als genehmigtem Mechanismus in einer Überarbeitung von ISO/IEC 18033-2, Verschlüsselungsalgorithmen — Teil 2: Asymmetrische Chiffren, voranzuschreiten.[25]

Leitfäden, die dieses Verfahren explizit empfehlen:

- BSI TR-02102-1[26]

[19] https://www.rfc-editor.org/rfc/rfc7296.txt
[20] https://www.rfc-editor.org/rfc/rfc7296.txt
[21] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02103/tr-02103.html
[22] https://eprint.iacr.org/2016/659 , https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions
[23] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html
[24] https://csrc.nist.gov/pubs/ir/8413/upd1/final
[25] https://frodokem.org/files/FrodoKEM-standard_proposal-20230314.pdf
[26] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

- Kryptografie quantensicher gestalten[27]

Aktueller Reifegrad

Verfügbarkeit: Der Code und die Spezifikation zum Verfahren ist auf der eigenen Homepage zusammengefasst.[28]

FrodoKEM ist aktuell in den folgenden Bibliotheken zu finden:

- Botan 3.0[29][30]
- PQCrypto[31]
- BouncyCastle[32]

Performance: Die größte Schwierigkeit des Verfahrens liegt in der Größe des Schlüsselmaterials und des Chiffrats. Die Größen des geheimen Schlüssels liegen je nach Sicherheitsgrad in der Spanne 19-43 kByte.[33]

Grundlagensicherheit: Die kryptographische Grundlage des (unstrukturierten) LWE-Problems ist in der kryptographischen Forschung im Vergleich zu den weiteren ring- oder modulbasierten Varianten von LWE ausführlich untersucht worden.

Risiken und Handlungsbedarf

In diesem Kapitel wird eingehend erläutert, dass die aktuell laufenden Vorgänge um Quantencomputer nach heutiger Einschätzung zu mannigfaltigen Konsequenzen führen können, die für ein Unternehmen Kosten und Aufwände verursachen können. Es geht dabei um Ereignisse, die unterschiedliche Risiken für die Unternehmen bergen. Da niemand die Zukunft vorhersagen kann und alle Arbeiten um Quantencomputer Gegenstand laufender Forschung sind können keine der Risiken mit einer gewissen Wahrscheinlichkeit versehen werden. Die Bewertung der Eintrittswahrscheinlichkeit dieser Ereignisse sind dabei immer Einzelfallbewertungen und sind im Allgemeinen nicht vollständig objektiv zu erfassen.

Insgesamt werden in diesem Kapitel 3 Kategorien von Risiken beschrieben, die Unternehmen begegnen können bei der Evaluation der Bedrohung durch Quantencomputer: Sicherheitsrelevante Risiken, Regulatorische Risiken, Wettbewerbliche Risiken.

Für jede Kategorie an Risiken ist eine erläuternde Beschreibung hinzugefügt, damit Lesende den Hintergrund und die Konsequenzen eindeutig nachvollziehen können. Damit die Risiken nicht zu abstrakt sind, werden spezifische Arten von Technologien beschrieben, die diesen Risiken unterliegen. Zudem wird die Art von Handlungsbedarf beschrieben, die notwendig ist um Maßnahmen zu ergreifen, die die entsprechenden Risiken minimieren. Am Ende jeder Kategorie wird eingehend darauf eingegangen, wie die Eintrittswahrscheinlichkeit der entsprechenden Risiken zu bewerten ist. In der Regel wird darauf hingewiesen, dass keine eindeutigen Wahrscheinlichkeiten

---

[27] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
[28] https://frodokem.org/
[29] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html
[30] https://github.com/randombit/botan
[31] https://github.com/microsoft/PQCrypto-LWEKE
[32] https://www.bouncycastle.org/specifications.html
[33] https://openquantumsafe.org/liboqs/algorithms/kem/frodokem.html

angegeben werden können, aber es hinreichend Quellen gibt um zumindest qualitative Aussagen über die Bedrohung treffen zu können.

Kryptoagilität

In diesem Kapitel gehen wir auf den aktuellen Stand der Wissenschaft und Technik um die Begriffsdefinition des Konzepts der "Kryptoagilität" ein. Dieser ist in der Tat weit von einer einheitlichen und wohldefinierten Definition entfernt. Aktuell findet in der Industrie und Wissenschaft eine rege Debatte statt, welche Kernaussagen das Konzept umfasst. Aus unserer Sicht ist kein Ende der Debatte in Sicht, da der Begriff überraschend vielschichtig ist. Im Folgenden sollen wissenschaftliche Arbeiten und ihre Kernaussagen zu der Begriffsdefinition des Konzepts der Kryptoagilität vorgestellt werden um eine Übersicht über die aktuelle Debatte zu verschaffen. Es ist anzumerken, dass die meisten der hier aufgeführten Arbeiten den MSDN-Artikel von Bryan Sullivan[34] zitieren und dessen Verständnis von Kryptoagilität aufnehmen.

Insgesamt haben wir im Zuge unserer Recherche 40 Arbeiten sichten können, die nach unserem besten Wissen und Gewissen den Stand der Technik ausmachen. Aus diesen Arbeiten konnten wir 16 verschiedene Begriffsbeschreibungen/-definitionen extrahieren, die wir kurz und bündig im Leitfaden vorstellen.

Wir haben uns im Konsortium entschieden keine eigene Definition zu erfinden, da wir gerade keinen Weg sehen dieses Konzept objektiv sauber definieren zu können. Das beste Indiz aktuell ist, dass es zum aktuellen Zeitpunkt 16 verschiedene Definition existieren und unsere Definition sich sicherlich davon unterscheiden wird.

Handlungsempfehlungen

Zum Abschluss des Projekts haben wir uns die Frage gestellt, was Unternehmen bereits jetzt umsetzen können, um mit der Migration zur Post-Quanten-Kryptographie zu beginnen. Idealerweise sollten solche Handlungsempfehlungen eine sehr niedrige Einstiegshürde haben. Aus unserer Sicht sind die folgenden Maßnahmen zum gegenwärtigen Zeitpunkt auch ohne zusätzliches Fachpersonal in den Unternehmen umsetzbar.

Inventarisierung

Das ETSI und das BSI empfehlen als ersten Schritt für einen Migrationsplan hinzu Post-Quanten-Kryptografie eine Inventarisierung der eingesetzten kryptografischen Verfahren. (Quelle ETSI und BSI einfügen) Vorteilhaft ist eine regelmäßige Aktualisierung der Inventarisierungsliste, so kann bei einer geplanten Migration schnell abgeleitet werden, welche Maßnahmen umzusetzen sind. Idealerweise enthält die Software Bill of Materials eines Produktes bereits die eingesetzten kryptographischen Verfahren, so könnten die Inventarisierungsliste automatisch generiert werden.

Für die Inventarisierungsliste sollen als erstes die Produkte, die kryptographische Verfahren einsetzen, identifiziert werden. Folgende Grundparameter sollen dabei berücksichtigt werden.

- Ansprechpartner für das Produkt
- Use Case des Produktes
- End of Life (EoL) Datum der Produkte
- Hersteller der Produkte
- Abhängigkeiten zu anderen Produkten
- Vertragliche Verpflichtungen

[34] https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/august/cryptographic-agility

Der Ursprung der Produkte kann in Standard, Eigenentwicklung, proprietär und Fremdbezug unterteilt werden.

- Standardprodukte: Es werden kryptografische Standards gemäß ISO oder RFCs etc. eingesetzt, welche durch Dritte bzw. den Markt wie z.B. TLS bereitgestellt werden. Diese Produkte müssen aktuell gehalten werden.
- Eigenentwicklung: Es werden kryptografische Standards in eigenen Entwicklungen verwendet. Die Integration neuer, aktualisierter Verfahren erfolgt in Eigenregie.
- proprietär: Es sind komplett eigene Entwicklungen umgesetzt worden.
- Fremdbezug: Es wurden Produktlösungen eingekauft. Diese Produkte müssen aktuell gehalten werden

Solche Maßnahmen können bereits jetzt in den Unternehmen ergriffen werden ohne auf Fachkräfte zu warten, die sich mit der Migration und Post-Quanten Kryptographie auskennen.

Einkaufsprozesse

Folgendes wird in diesem Kapitel ausgeführt. Das Ziel ist es, frühzeitig PQ-Sicherheit bei Hersteller, Lieferanten und Dienstleistern einzufordern, insbesondere bei langlebigen und spezialisierten Produkten, wenn diese Hardware, Software oder IT-Services bereitstellen.

Für Standard-Services / -Hardware / -Software ist dies weniger wichtig, denn als für spezialisierte Lösungen. So kann man beispielsweise bei Notebooks, Smartphones oder Standard-Software wie Web-Browsern unterstellten werden, dass diese rechtzeitig PQ-sicher sein werden. Die Austausch- und Updatezyklen sind dabei so kurz, dass es keiner expliziten Berücksichtigung bedarf. Bei spezialisierter Hard- und Software kann hingegen der Fall anders gelagert sein. So weist eine Auszahleinheit eines Geldautomaten mehrere Merkmale auf, die dafür sprechen frühzeitig eine PQ-Sicherheit beim Hersteller einzufordern. Eine solche Auszahleinheit verfügt in der Regel über einen Mikrocontroller mit limitierten Hardware-Ressourcen, die Signatur der Firmware der Auszahleinheit ist essentiell für den Schutz des Geldes im Geldautomaten und die Laufzeit mit mehreren Jahren solcher Geräte ist in der Regel sehr lange.

Stellt ein Hersteller, Lieferant oder Dienstleister Hardware, Software oder IT-Services bereit, sollte folgendes im Ausschreibungsprozess abgefragt werden.

Im Migrationsleitfaden wurde daher ein Standardtext für Ausschreibungen formuliert. Dieser besteht zum einen aus einem allgemeinen Fragebogen, um zu prüfen ob und wie tief sich der Lieferant mit dem Thema auseinandersetzt. Zum anderen folgen spezifische Anforderungen, um mittel-/langfristig eine Quantensicherheit sicherzustellen.

Hybride Gestaltung von Kryptographischen Komponenten

Der aktuelle Stand der Technik bezüglich der Empfehlungen für kryptografische Komponenten im europäischen Wirtschaftsraum besagt, dass es nicht nur empfohlen wird, einen „klassischen“ kryptografischen Algorithmus einfach durch einen quantensicheren zu ersetzen, sondern vielmehr die bestehende Sicherung durch Hinzufügen eines quantensicheren Algorithmus zu ergänzen. Es ist ebenfalls anzunehmen, dass in Zukunft kryptografische Algorithmen immer öfter im Tandem empfohlen und verwendet werden. Daher kann bereits jetzt damit begonnen werden, zu überlegen, inwieweit eine hybride Nutzung von kryptografischen Algorithmen in aktuellen Produktlinien möglich ist. Hierfür ist vorerst kein Fachwissen über Migration und Post-Quanten-Kryptographie erforderlich, da auf abstraktem Niveau die hybride Kombination mit vorhandenem Fachwissen planbar ist, indem zwei klassische Verfahren zusammengeführt werden.

Sobald Fachwissen über Post-Quanten-Kryptographie im Unternehmen verfügbar ist, müssen lediglich die bisherigen Überlegungen entsprechend angewendet werden.

Paradigmenwechsel in der Handhabung der kryptographischen Komponenten

Ein häufiges Argument von Unternehmen, die sich ungern mit dieser Thematik auseinandersetzen möchten, ist, dass sie bei aktuellen Produktentwicklungen mit deutlich dringlicheren Sicherheitsproblemen zu kämpfen haben. Daraufhin hört man oft die Frage, warum man sich jetzt schon mit Risiken wie Quantencomputern befassen und Ressourcen dafür bereitstellen soll, obwohl die Eintrittswahrscheinlichkeit oder der Zeitpunkt dafür höchst unklar sind. Aktuelle Schätzungen geben eine Spanne von 5 bis 30 Jahren an.

In diesem Kapitel wird exemplarisch aufgezeigt, dass diese Denkweise oder Paradigma äußerst kontraproduktiv und irreführend ist. Unsere Antwort darauf ist, dass die Migration nicht durch einzelne große Investitionen bewältigt werden muss. Vielmehr geht es darum, eine Denkweise zu etablieren, bei der die Risiken durch Quantencomputer zumindest bei allen neuen Entwicklungen oder Produktkonzepten mit kryptografischen Komponenten berücksichtigt werden. Auf diese Weise können die Investitionen aufgeteilt werden, sodass sich die Kosten langfristig amortisieren.

Fazit des Migrationsleitfadens

Am Ende wird ein Fazit gezogen wo die deutsche Industrie weltweit im Kontext der Migration zur Post-Quanten Kryptographie und der Absicherung gegen Quantencomputer steht. Was insgesamt noch zu tun ist und wie jedes Unternehmen dazu beitragen kann.

Notwendigkeit und Angemessenheit der geleisteten Arbeit

Der gegenwärtige Gesamteindruck in der Industrie legt nahe, dass die meisten Unternehmen derzeit die Marktsituation abwarten. Sie lassen bewusst anderen Unternehmen den Vortritt, um erste Erfahrungen mit der Migration zu sammeln. Der Hintergrund hierfür ist, dass Migrationsprojekte derzeit noch zahlreiche Herausforderungen mit sich bringen, die dazu führen können, dass Investitionen in vielen Fällen scheitern. Misserfolge bei der Migration können schwerwiegende Konsequenzen haben, da im schlimmsten Fall die Sicherheit auf der untersten Ebene beeinträchtigt sein könnte.

Aus diesem Grund waren die Arbeiten in diesem Projekt von entscheidender Bedeutung. Unternehmen können auf unseren Erfahrungen aufbauen und ihre eigenen Pläne zur Migration entsprechend anpassen. Alle unseren Erfahrungen und Empfehlungen sind im Migrationsleitfaden zusammengefasst und werden zeitnah veröffentlicht.

Als Beispiel lassen sich die folgenden Arbeiten aus dem Projekt aufführen. Im Laufe des Projektes wurde der Fokus auf die mögliche Nutzung von PQ-Verfahren bei kartengestützter Autorisierung verschoben. Hier gibt es den Aspekt der Implementierungssicherheit, also Resistenz gegen Seitenkanal- und Fehlereinstreuungsangriffen zu berück-sichtigen. Es wurde vor allem die Seitenkanalanalyse für ein Verfahren, Dilithium oder auch ML-DSA nach dem ersten Draft zum NIST Standard FIPS 204, durchgeführt und Überlegungen zu Gegenmaßnahmen angestellt. Insbesondere ist daraus die Empfehlung abzuleiten, dass dieses Verfahren, trotz Performance-technischer Eignung, nicht in Seitenkanalanfälligen Szenarien eingesetzt werden kann.

Derzeit sind keine Aktivitäten im kreditwirtschaftlichen Bereich bekannt, die bereits Anwendungen auf der Basis von PQ-Verfahren vorsehen. Insofern kann das ursprünglich geplante Verwertungsziel der Erstellung von Spezifikationsentwürfen nicht unmittelbar umgesetzt werden. Dies ist nicht nur auf eine später als ursprünglich geplante Festlegung und auch derzeit noch nicht vollständig abgeschlossene Standardisierung von PQ-resistenten Algorithmen zurückzuführen, sondern u. a.

auch darauf, dass die bestehenden Anwendungen auf Basis der klassischen Kryptoverfahren bislang nicht durch die zur Verfügung stehenden Quantencomputer gefährdet sind.

Dennoch wird in der Kreditwirtschaft eine Migration zu PQ-Verfahren weiterhin stringent verfolgt.

Die von SRC erzielten Ergebnisse im Projekt Quantum Leap sind für den in der Kreditwirtschaft – aber selbstverständlich auch in anderen Bereichen kritischer Infrastrukturen – auch künftig weiterhin notwendigen Aspekt des Nachweises von sicheren Implementierungen von PQ-Standards und -Spezifikationen sehr wertvoll, wie in dem nachfolgenden Abschnitt weiter ausgeführt wird.

Voraussichtlicher Nutzen und Verwertbarkeit, sowie Fortschritte bei anderen Stellen

Es sind folgende Verwertungen seitens des FZI vorgesehen:

- Bei jeder Gelegenheit soll ein Nachfolgeprojekt in Form eines öffentlich geförderten Projekts eingereicht werden.
- Die aufgebauten Kompetenzen vom FZI im Bereich der sicheren Entwicklung von post-quanten kryptographischen Komponenten und deren Seitenkanalresistenzen, sollen weiter vertieft werden. Auch hier sollen zusätzliche Projektskizzen bei der nächsten Gelegenheit eingereicht werden.
- Die Ergebnisse sollen der Industrie frei zugänglich gemacht werden, um sicherzustellen, dass das FZI seinen Auftrag erfüllt.[35]

Es sind folgende Verwertungen seitens der SRC vorgesehen:

- Von einem Forscherteam der Universität Luxemburg wurde (Improved Gadgets for the High-Order Masking of Dilithium) beschrieben, welche Gegenmaßnahmen zur Vermeidung von Seitenkanälen ergriffen werden sollten. Eine Implementierung hiervon steht mittlerweile als OpenSource in Github zur Verfügung. Für diese Implementierung wäre eine SCA mit den Kenntnissen des QuantumLeaps-Projektes durchzuführen und damit weiterzuentwickeln.
- Weiterer Ausbau einer Testinfrastruktur für SCA von PQC-Implementierungen.
- Analyse weiterer PQ-Algorithmen (neben Crystals Dilithium) hinsichtlich SCA (also z. B. KYBER, SPHINCS+).
- Möglicher Beitrag zu einem Seitenkanalleitfaden des BSI. Diese sind gerade aktualisiert worden als Teil der AIS 46, die für CC Evaluierung kryptographischer Implementierungen relevant ist. Diese behandeln traditionelle asymmetrische Algorithmen RSA, DSA, DH und ECC sowie die Anwendung von KI Methoden. Angedacht ist seitens des BSI, sich in einem Nachfolgeprojekt den PQ Algorithmen zu widmen. Diese Art der Verwertung kann nicht von SRC alleine entscheiden werden. SRC wird aber hierzu mit den Entscheidern beim BSI in Verbindung treten und zu dieser Erweiterung der AIS46 raten.

Es sind folgende Verwertungen seitens der Atruvia AG (ehemals Fiducia & GAD IT AG) vorgesehen:

- Awareness zum Thema PQC. Auf Basis der Ergebnisse des Forschungsprojektes QuantumLeap konnte und wird Entscheidungsträgern wie Bankvorständen in der der genossenschaftlichen Finanzgruppe die Handlungsnotwendigkeit nähergebracht

- Eine Migration zu PQ-sicheren Verfahren in den nächsten 10 Jahren wird nun in der genossenschaftlichen Finanzgruppe verfolgt. Der erarbeitete Migrationsplan wird hierzu als Grundlage dienen

[35] https://www.fzi.de/das-fzi/auftrag/

- Das Projekt hat gezeigt, dass kein ausreichender Handlungsdruck auf Hersteller- und Lieferantenseite gegeben ist, dies wird nun in den Einkaufsprozessen berücksichtigt.
- Beiträge zu kreditwirtschaftlichen Gremien / Verbänden wie der Deutschen Kreditwirtschaft (DK).

Letztendlich konnten leider nicht alle angestrebten Verwertungsziele erreicht werden. Derzeit sind keine Aktivitäten im kreditwirtschaftlichen Bereich bekannt, die bereits Anwendungen auf der Basis von PQ-Verfahren vorsehen. Insofern kann das ursprünglich geplante Verwertungsziel der Erstellung von Spezifikationsentwürfen nicht unmittelbar umgesetzt werden. Dies ist nicht nur auf eine später als ursprünglich geplante Festlegung und auch derzeit noch nicht vollständig abgeschlossene Standardisierung von PQ-resistenten Algorithmen zurückzuführen, sondern u. a. auch darauf, dass die bestehenden Anwendungen auf Basis der klassischen Kryptoverfahren bislang nicht durch die zur Verfügung stehenden Quantencomputer gefährdet sind.

Dennoch wird in der Kreditwirtschaft eine Migration zu PQ-Verfahren weiterhin stringent verfolgt.

Auch war es nicht möglich ein Nachfolgerprojekt für Quantum Leap zu beantragen. Trotz einer passenden Ausschreibung[36] durch das Ministerium für Bildung und Forschung (BMBF) wurde die eingereichte Skizze nicht angenommen.

Erfolgte und Geplante Veröffentlichungen

Vorträge zu Seitenkanalanalysen auf Dilithium:

- auf dem ID:Smart Workshop der Fraunhofer Gesellschaft am 22.2.2024.
- Bereits erfolgt ist eine Präsentation innerhalb des EMVCo-Labmeetings am 07.11.2023. EMVCo ist ein Verbund von Kreditkartenfirmen, welche international die Standards festlegen, welche im Moment auch in Deutschland bei kartengestützten Autorisierungen verwendet werden.

Weitere Vorträge zu den Ergebnissen aus dem Projekt:

- Ein weiterer Vortrag wurde am 28.11.23 beim ‚ECC Brainpool' einem vom BSI organisierten Workshops zu neuen kryptographischen Themen von SRC und dem FZI gehalten.
- Bei PQC-Workshop der deutschen Kreditwirtschaft am 22.04.2024 wurden von Atruvia die geplanten Inhalte des Migrationsleitfadens vorgestellt.

Der Migrationsleitfaden soll zeitnah publiziert werden. Außerdem ist es eingeplant die Implementierung der Leighton-Micali-Signatur (LMS) zu publizieren. Zudem wurde das FZI vom BSI aufmerksam gemacht, dass das BSI ebenfalls vor hat einen Migrationsleitfaden zu erarbeiten und wir wurden eingeladen uns diesbezüglich auszutauschen.

[36] https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2022/12/2022-12-30-Bekanntmachung-PostQuantenKryptografie.html

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht

3. Titel

Verbundschlussbericht
zum Gesamtvorhaben „QuantumLeap – Der Quantensprung für unsere Wirtschaft“

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens
Wasilij Beskorovajnov, Dirk Feldhusen, Jochen Dinger	31.10.2023
	6. Veröffentlichungsdatum
	7. Form der Publikation

8. Durchführende Institution(en) (Name, Adresse)	9. Ber. Nr. Durchführende Institution
FZI Forschungszentrum Informatik Haid-und-Neu-Str. 10-14, 76131, Karlsruhe	10. Förderkennzeichen 01MT20007A
	11. Seitenzahl 19

12. Fördernde Institution (Name, Adresse)	13. Literaturangaben
Bundesministerium für Wirtschaft und Klimaschutz (BMWK) 53107 Bonn	14. Tabellen
	15. Abbildungen

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

19. Schlagwörter

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) Report

3. title

Verbundschlussbericht
zum Gesamtvorhaben „QuantumLeap – Der Quantensprung für unsere Wirtschaft“

4. author(s) (family name, first name(s)) Wasilij Beskorovajnov, Dirk Feldhusen, Jochen Dinger	5. end of project 31.10.2023
	6. publication date
	7. form of publication
8. performing organization(s) (name, address) FZI Forschungszentrum Informatik Haid-und-Neu-Str. 10-14, 76131, Karlsruhe	9. originator’s report no.
	10. reference no. 01MT20007A
	11. no. of pages 19
12. sponsoring agency (name, address) Bundesministerium für Wirtschaft und Klimaschutz (BMWK) 53107 Bonn	13. no. of references
	14. no. of tables
	15. no. of figures

16. supplementary notes

17. presented at (title, place, date)

18. abstract

19. keywords

20. publisher	21. price