QuantumRISC
Abschlussbericht

Version	1.0
Erstellungsdatum	19. Juni 2023
Partner	MTG AG
Fkz BMBF	16KIS1037

GEFÖRDERT VOM

Projektkoordination
Norman Lahr
Fraunhofer-Institut für Sichere Informationstechnologie
Advanced Cryptographic Engineering
Rheinstr. 75
D-64295 Darmstadt
Deutschland

Telefon +49 6151 869100
Fax +49 6151 869224
Mail norman.lahr@sit.fraunhofer.de

1 Übersicht

QuantumRISC ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Projekt. Das Ziel des Projekts ist, Post-Quanten-Kryptographie von der Theorie in die Anwendung zu bringen, wobei der Fokus auf eingebetteten Geräten liegt. Dies sind Systeme mit geringen Ressourcen, wie sie zum Beispiel in Steuergeräten in der Automobilbranche vorkommen, aber auch in Industrieanlagen oder in der Telekommunikation. Das Projekt beschäftigt sich mit der Forschung und Analyse von Post-Quanten-Algorithmen, so wie der Entwicklung von effizienten Implementierungen für eingebettete Geräte. Dabei werden sowohl Hardware Implementierungen als auch Software Implementierungen entwickelt.

MTG AG ist ein Partner dieses Projekts und beteiligt sich vorwiegend an den Arbeiten zu Software Implementierungen und der Integration von Post-Quanten-Algorithmen in kryptographischen Protokollen (z.B. X.509 und TLS).

Dieser Abschlussbericht beschreibt die Arbeiten von MTG AG im Projekt QuantumRISC für den gesamten Projektzeitraum, 01.09.2019 bis 31.12.2022. Der Bericht ist folgendermaßen strukturiert:

Kapitel 2 fasst die wichtigsten wissenschaftlichen-technischen Ergebnisse, welche in der Berichtsperiode erzielt wurden, zusammen.

Kapitel 3 nennt die Veröffentlichungen aus dem Berichtszeitraum.

Kapitel 4 bewertet die langfristigen und mittelfristigen Aussichten nach Projektabschluss.

2 Ergebnisse

Dieses Kapitel präsentiert die Arbeiten und fasst die Ergebnisse von MTG AG pro Arbeitspaket zusammen.

2.1 AP0: Technische Projektkoordination

Das AP0 beschäftigt sich mit der technischen Projektkoordination. MTG AG ist an Arbeitspaket 0 nicht beteiligt.

2.2 AP1: Definition von Anwendungsfällen und Anforderungen

Im AP1 werden Anforderungen an PQC-Verfahren aus der Industrie betrachtet. Zusätzlich wird der aktuelle Stand der Wissenschaft bezüglich PQC-Verfahren ermittelt. Darüber hinaus werden Hardware-Plattformen untersucht. Das AP1 hat drei Unterarbeitspakete. Im UAP1 werden Anwendungsfälle definiert und evaluiert. Das UAP2 behandelt die Anforderungen an PQC-Verfahren. Die Analyse der Anforderungen an die Hardware-Plattformen ist Gegenstand vom UAP3.

Im UAP1 haben wir die verschiedenen Anwendungsfälle insbesondere im Bereich PKI analysiert. Hauptsächlich wurden die Prozesse der Zertifizierung mit und ohne Schlüsselpaar-Erzeugung und die Sperrung von Zertifikaten mittels OCSP und Sperrlisten untersucht. Für die Zertifizierung ist auf den Besitznachweis eines privaten Schlüssels und die Prüfung der Qualität des öffentlichen Schlüssels zu achten.

Die PQC-Verfahren sind entweder als Key Encapsulation Mechanism (KEM) oder Signaturverfahren spezifiziert. Um den Besitznachweis eines Schlüssels von einem Signaturverfahren durchzuführen, reicht es aus, wenn der Schlüsselbesitzer eine Signatur erzeugt. Für asymmetrische Verschlüsselungsalgorithmen sind typische Ansätze, entweder einen Wert zu verschlüsseln und der CA zu präsentieren, oder das Zertifikat verschlüsselt an den Schlüsselbesitzer auszuliefern. Im ersten Fall erfolgt der Besitznachweis explizit, im zweiten Fall implizit. Diese Mechanismen sind nicht üblich und CAs müssen nachgerüstet werden, um solche Verfahren zu unterstützen. Weiterhin ist zu beachten, dass KEMs keine allgemeinen Verschlüsselungsalgorithmen sind und daher beispielsweise mit einer sogenannten KEM-DEM Konstruktion gearbeitet werden muss, um den Besitznachweis umzusetzen. Darüber hinaus existieren bisher keine Vorgaben bezüglich der Qualität eines Schlüssels für PQC-Verfahren.

Die nötigen Änderungen an den Richtlinien (Policies) einer PKI wurden ebenfalls betrachtet. Aspekete bezüglich der Interoperabilität von PQC-Verfahren im PKI Umfeld wurden behandelt. Die Existenz und Spezifizierung von Object Identifiers (OIDs) und eindeutigen Formaten für private und öffentliche Schlüssel sind notwendig. Im UAP2 wurden

Anforderungen für serverseiteige Komponenten aufgestellt. Im UAP3 wurden die Einschränkungen an Hardware-Plattformen und die Auswirkungen auf mögliche Implementierungen erforscht.

Das Konsortium hat den Bericht für das AP1 auf der Webseite veröffentlicht und auf der Mailing Liste vom NIST zum PQC Standardisierungsprozess darauf aufmerksam gemacht[1]. Das NIST hat mit einem positiven Feedback mit einer Mail an den Projektkoordinator auf diesen Report reagiert.

Zusammenfassung der Ergebnisse

- Anwendungsfälle insbesondere im Bereich PKI analysiert.
- Besitznachweis für private Schlüssel für KEM Zertifikate analysiert.
- Notwendige Änderungen an Policies analysiert.
- Veröffentlichung des AP1 Berichts auf der NIST Mailing Liste.

2.3 AP2: Auswahl und Verbesserung von PQC-Verfahren und Protokollen

Im AP2 werden PQC-Verfahren und Protokolle, welche die PQC-basierten Primitive benutzen, erforscht. Das AP2 hat sechs Unterarbeitspakete. Im UAP1 werden die PQC-Verfahren bezüglich deren Nutzung in eingebetteten Systemen analysiert und im UAP2 werden Protokolle untersucht. Im UAP3 und UAP4 werden Optimierungen bezüglich Performanz und Speicherbedarf erforscht. Das UAP5 betrachtet physikalische Angriffe, und UAP6 beschäftigt sich mit der Wahl der Parameter für die Zielplattformen und Anwendungen.

MTG AG hat sich, aufbauend auf der Analyse der PQC Verfahren in AP1, mit einigen PQC Verfahren intensiv auseinandergesetzt. Diese Verfahren beinhalten Classic McEliece, FrodoKEM, XMSS und SPHINCS$^+$. MTG AG ist interessiert an Dilithium bzw. Falcon, da beides sehr effiziente PQC Signaturverfahren sind. Das NIST strebte zum Zeitpunkt der Analyse an, eines davon als PQC Standard zu etablieren und nach Analysen von MTG AG eignen sich diese Kandidaten besonders, um aktuelle Signaturverfahren im PKI und TLS Bereich abzulösen. In der Zwischenzeit ist Dilithium und Falcon von NIST zur Standardisierung ausgewählt worden.

Weiter hat MTG AG das Classic McEliece Verfahren hinsichtlich der Speichernutzung optimiert und die Ergebnisse in einem Paper auf der CARDIS 2020 Konferenz veröffentlicht. Hier wurde das Augenmerk auf die Nutzung des Verfahrens auf eingebetteten Systemen gerichtet. Die bis über 1 MB großen öffentlichen Schlüssel stellen eingebettete Systeme die oft nur wenige hundert KB RAM oder weniger haben, vor eine Herausforderung. In der Veröffentlichung wurde gezeigt, wie Classic McEliece dennoch als Key Exchange Verfahren im TLS Protokoll auf einem Gerät mit 256 KB RAM eingesetzt werden kann. Dazu wurden die Algorithmen für die Encapsulation Operation und die Key Generation

[1] https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/3xnb93rDFbU/m/GWVaZztcBQAJ

Operation algorithmisch angepasst. Die Anpassungen machen es möglich, Classic McEliece sowohl als TLS Client, als auch als TLS Server mit den beschränkten Ressourcen ausführen zu können. Die Schlüssel können hierbei auch ephemeral erzeugt werden, so wie es z.B. in TLS 1.3 vorgesehen ist. Es ist also möglich, kurzlebige, direkt auf dem Gerät erzeugte Schlüsselpaare zu verwenden. Der Einsatz von Classic McEliece auf eingebetten Geräten mit wenig Speicher wurde bisher durch die großen Schlüssel als große Herausforderung angesehen. Classic McEliece wurde daher oft nicht berücksichtigt, wenn es um den Einsatz von Post-Quanten-Verfahren auf eingebetteten Systemen geht. Diese Arbeit leistet einen Beitrag dazu, dass Classic McEliece für solche Plattformen praktikabler wird.

Im Dezember 2019 hat das NIST einen Entwurf („Draft“) für das Dokument SP 800-208 mit dem Titel „Recommendation for Stateful Hash-Based Signature Schemes“ vorgestellt und um Feedback („public comments“) gebeten[2]. Bei Dokumenten der NIST SP (Special Publications) 800 Reihe handelt es sich um Guidelines, technische Spezifikationen, Empfehlungen und Referenzmaterial von NIST zum Thema Computer Security. In SP 800-208 wurde angestrebt, die beiden hashbasierten Signaturverfahren XMSS und LMS als vom NIST anerkannt („approved“) zu spezifizieren. Dadurch wird das Dokument FIPS 186 (Digital Signature Standard)[3] um diese Verfahren ergänzt, was in einigen Nutzungsszenarien eine Voraussetzung für die Verwendung ist. Zu diesem Draft hat das Konsortium Feedback erstellt und dem NIST gesendet[4]. Dabei hat MTG AG auf die Notwendigkeit von Object Identifiers (OID) hingewiesen, so dass die Algorithmen auch in der Praxis interoperabel eingesetzt werden können und ein explizites, eindeutiges ASN.1 Format vorgeschlagen, so dass die Keys interoperabel in kryptographischen Protokollen ausgetauscht werden können. Eines der Anliegen des Konsortiums war es, dass all diese Dinge in einem Dokument spezifiziert werden sollen, so dass der Einsatz von XMSS und LMS möglichst einfach ist und die Spezifikation nicht über viele verschiedene Standards verteilt ist.

MTG AG hat sich stetig weiter mit PQC Verfahren befasst, um auf dem aktuellen Stand zu bleiben. Da SPHINCS$^+$ für MTG AG ein sehr interessantes Signaturverfahren darstellt, wurden Optimierungen an diesem Verfahren betrachtet. Es wurde Potenzial in der Optimierung hinsichtlich des Speicherverbrauchs gesehen, wenn man analog zu den bereits erfolgten Arbeiten an Classic McEliece, ebenfalls das Streamen der Signatur in Betracht zieht. Dazu wurden die internen Details des Algorithmus im Detail analysiert, insbesondere mit einem Fokus auf den Speicherverbrauch. Dabei sind insbesondere die graphentheoretisch bereits optimierten Algorithmen zum Traversieren der Bäume von Relevanz gewesen. Aufbauend auf diesen Überlegungen wurde eine speichereffiziente streaming Implementierung (zugehörig zu AP3) erstellt und ein Paper dazu verfasst.

Zusammenfassung der Ergebnisse

- PQC-Signatur Verfahren analysiert. Stateless Signaturverfahren bieten unter gewissen Voraussetzungen ein angemessenen Trade-Off zwischen Sicherheit und Praktikabilität.

[2] https://csrc.nist.gov/publications/detail/sp/800-208/archive/2019-12-11
[3] https://csrc.nist.gov/publications/detail/fips/186/5/draft
[4] https://csrc.nist.gov/CSRC/media/Publications/sp/800-208/draft/documents/sp800-208-draft-comments-received.pdf, Seite 40

- Analyse von Erweiterungen von TLS um PQC-Verfahren zu unterstützen.
- Kommentare für den Draft von NIST bzgl. hashbasierten Signaturen eingereicht.
- Kryptosysteme analysiert, um den Fokus einzugrenzen. Ergebnis der Analyse hat ergeben: Classic McEliece, FrodoKEM, XMSS, SPHINCS$^+$, Dilithium.
- Classic McEliece: algorithmische Optimierungen bezüglich Speichernutzung auf eingebetten Geräten.
- Analyse von SPHINCS$^+$ bezüglich Speicherverbrauch auf algorithmischer Ebene.
- Speichereffizientes Streamen von SPHINCS$^+$ Signaturen.

2.4 AP3: Entwicklung von Software-Bibliotheken

Im AP3 wird die Umsetzung der Verfahren aus AP2 in Software untersucht, wobei das Augenmerk auf die Besonderheiten und die eingeschränkten Ressourcen von eingebetteten Geräten gelegt wird. Es gibt 6 Unterarbeitspakete. UAP1 befasst sich mit dem Thema "Mixed-PQ PKI", also dem Verwenden von unterschiedlichen PQC Algorithmen für verschiedene Aufgaben in der PKI. Im UAP2 wird erforscht, wie eine geeignete API für PQC aussehen kann, welche die besonderen Anforderungen von Verfahren (z.B. Statefulness), als auch die Hardwareanbindung (AP5), oder die Anforderungen im Embedded Bereich abdeckt. Das UAP3 erforscht die Implementierung von PQC Verfahren in Software. In UAP4 und UAP5 werden diese Implementierungen hinsichtlich Effizienz (Speicher, Laufzeit), als auch hinsichtlich Seitenkanalangriffen analysiert und gegebenenfalls optimiert bzw. gehärtet. Schließlich werden in UAP6 das TLS und das X.509 Protokoll betrachtet und es wird analysiert wie sich PQC Verfahren in diese Protokolle integrieren lassen.

Für das UAP3.1 wurde der aktuelle Forschungsstand analysiert, welcher sich noch in der Anfangsphase befindet. MTG AG hat sich auch mit dem FLOQI Projekt aus der gleichen Förderlinie zu dem Thema ausgetauscht, was in einem gemeinsamen wissenschaftlichen Papier mit QuantumRISC und FLOQI resultiert ist[5], wobei MTG AG hier unterstützend tätig war und Know-How bereitgestellt hat. Es gibt interessante Teilbereiche des Themas, welche aktiv in wissenschaftlichen Papieren, aber auch Standardisierungsgremien diskutiert werden, so zum Beispiel die Möglichkeit die zusätzlichen Kosten von Postquantum-Zertifikaten abzuschwächen, siehe z.B.[6]. Als Teil der Analyse wurden wissenschaftliche Papiere analysiert, die das Thema behandeln, z.B.[7,8].

Um die zu erstellende API zu entwickeln, wurden verschiedene APIs mit den Partnern im Konsortium diskutiert. Insbesondere wurde auch die von NIST gewählte API diskutiert, an die sich die Einreichungen in den NIST PQC Wettbewerb halten. MTG AG hat insbesondere eingebracht, dass entgegen der von NIST gewählten API, auch „Detached Signatures“ möglich sein müssen. Dies wurde nach Analyse vom X.509 Protokoll erkannt, für welches Detached Signatures benötigt werden. Der Beraterstab teilt diese Meinung.

[5] https://eprint.iacr.org/2021/1447
[6] https://www.ietf.org/id/draft-kampanakis-tls-scas-latest-01.html
[7] https://eprint.iacr.org/2020/071
[8] https://eprint.iacr.org/2019/1276

Insgesamt ist im Konsortium eine API entwickelt worden, die den Besonderheiten bei der Entwicklung von Software für eingebetteten Systemen Rechnung trägt, sowie auch die flexible Nutzung auf herkömmlichen Systemen bedenkt. Ein Augenmerk ist zudem auf die sichere Nutzung der API gelegt worden, so dass es für den Anwender der API möglichst einfach ist, Programmierfehler zu vermeiden bzw. die Auswirkungen bezüglich der Sicherheit von etwaigen Fehlern zu minimieren. Hierbei hat MTG AG mit Erfahrung zur sicheren Implementierung von zustandsbehafteten Signaturverfahren beigetragen. Für die Kollaboration mit den Partnern befindet sich der Code in einem vom Fraunhofer SIT gehosteten Gitlab-Repository, so dass dezentral an der Implementierung entwickelt werden kann, aber die Zusammenarbeit dennoch an einer zentralen Stelle zusammenläuft.

MTG AG hat die Referenzimplementierung des Classic McEliece Verfahren hinsichtlich der Speicheranforderungen optimiert. Dies stellt die Implementierungsarbeit zu den im AP2 beschriebenen Optimierungen dar. Die Key Pair Generation, so wie die Encapsulation Operation wurden hierbei deutlich effizienter bezüglich der Menge des benötigten Arbeitsspeichers umgesetzt, was auf algorithmischen Überlegungen und implementierungstechnischen Details basiert. Hierbei wurde insbesondere das „Streaming“ vom öffentlichen Schlüssel in den Vordergrund gerückt, also eine Implementierung entwickelt, die den öffentlichen Schlüssel verarbeitet, ohne ihn in Gänze abspeichern zu müssen. Weiterhin wurde darauf geachtet, dass die neuen Codebestandteile effizient sind. Dabei wurden keine gerätespezifischen Optimierungen, zum Beispiel auf Assemblerebene, betrachtet, sondern allgemeine Optimierungen für 32-bit Plattformen der zugrundeliegenden Algorithmen.

MTG AG hat die Referenzimplementierung des SPHINCS$^+$ Verfahrens hinsichtlich der Speicheranforderungen optimiert. Hierzu wurde, ähnlich zu der bereits erfolgten Optimierung für Classic McEliece, ein Ansatz zum Streamen der Signatur verfolgt. Nach eingehender Analyse des SPHINCS$^+$ Verfahrens wurde festgestellt, dass im Grunde keine Notwendigkeit besteht, die bis zu 49 Kilobyte großen Signaturen auf dem Gerät zu speichern. Dies gilt sowohl für den Vorgang des Signierens, als auch für den Vorgang des Verifizierens der Signatur. Es wurde eine Implementierung entwickelt, welche eine Streaming API für SPHINCS$^+$ umsetzt, so wie zahlreiche Modifikationen umsetzt, um dabei effizient bezüglich der Speichernutzung zu sein. Dabei verbrauchen die SPHINCS$^+$ Operationen (Key Gen, Sign, Verify) maximal ungefähr 3 Kilobyte, bei den meisten Parametersätzen und Operationen jedoch deutlich weniger. Die Praxistauglichkeit wurde anhand einer Integration in den TPM 2.0 Standard und einer entsprechenden Implementierung demonstriert.

Weiter hat MTG AG sich in der Literatur und in Gesprächen mit den Partnern mit gängigen Seitenkanalangriffen und Fehlerangriffen, so wie Gegenmaßnahmen, auseinandergesetzt. Dies umfasst beispielsweise Timing-Angriffe, so wie Simple und Differential Power Analysis. In allen Codebestandteilen, die von MTG AG entwickelt wurden, wie die Implementierung der speicheroptimierten Algorithmen für das Classic McEliece Verfahren, wurde darauf geachtet, dass diese als Constant-Time Code implementiert sind, um Timing-Angriffe abzuwehren. Diese Gegenmaßnahmen haben eine besonders hohe Priorität, denn Timing-Angriffe können oft auch von entfernten Angreifen ohne physischen Zugang zu den Systemen durchgeführt werden. Die Entwicklung von Constant-Time Code ist zeitaufwendig, da eine effiziente Umsetzung erfordert, dass im Einzelfall entschieden werden muss, wie die zeitliche Korrelation der Ausführung des Codes und geheimer Daten

mit möglichst wenig zusätzlichem Rechenaufwand aufgelöst werden kann. Zusätzlich leidet die Lesbarkeit und Wartbarkeit des Codes, denn beispielsweise darf das Verzweigen (if-then-else, Schleifenbedingungen, ...) nicht explizit von geheimen Daten abhängen und erfordert oft, dass die Logik der Verzweigung implizit durch geschicktes Einsetzen von Bitweisen Operatoren nachgestellt wird.

Weiterhin wurde für XMSS eine Implementierung für ein Hardware Security Modul (HSM) der Firma Utimaco implementiert. XMSS ist ein hashbasiertes und zustandsbehaftetes Verfahren, welches bereits standardisiert ist. Konkret hat MTG AG ein Software Modul erstellt, welches die Funktionalität von XMSS bereitstellt und in das HSM integriert. Die Schlüssel werden vom HSM verwaltet und können so vor unerlaubtem Zugriff geschützt werden. Im Gegensatz zu rein softwarebasierten Lösungen können so einige der Probleme gelöst werden, welche sich aus dem Einsatz von zustandsbehafteten Verfahren ergeben. So ist der Besitz des privaten Schlüssels und damit auch der Zustand des privaten Schlüssels eindeutig festgelegt und kann nicht z.B. unbewusst und unbemerkt durch das Klonen einer VM, oder durch inkonsistente Caches und Ähnliches beeinträchtigt werden. Zunächst wurde die Implementierung mit dem Simulator von Utimaco entwickelt und getestet. Um die Implementierung praxisnah evaluieren zu können, wurde ein Utimaco HSM on-premise geliehen und das Modul darauf aufgebracht. Probleme die sich nicht im Simulator gezeigt haben, wurden gelöst und durch geeignete Tests wurde sichergestellt, dass die Implementierung auf der Hardware korrekt arbeitet. Weiterhin wurde die Performanz auf der realen HSM Hardware evaluiert.

Um geeignete Softwarebibliotheken für das TLS und X.509 Protokoll zu finden, auf denen aufgebaut werden kann und PQC integriert werden kann, hat sich MTG AG einen Überblick über die derzeit existierenden kryptographischen Bibliotheken geschaffen. Dabei wurden die Bibliotheken liboqs (OpenSSL Integration), mbedTLS, WolfSSL und fleaTLS in Betracht gezogen und auf die Anforderungen hin untersucht.

Im Rahmen der zu entwickelnden kryptographischen API welche AP3 und AP4 betrifft, hat MTG AG eigene Erfahrungen mit inkrementellen APIs und dem Streamen von kryptographischen Objekten einfließen lassen und mit dem Konsortium diskutiert. Diese Punkte wurden mitunter in den entsprechenden Meetings zur API besprochen.

Zusammenfassung der Ergebnisse

- Existierende APIs analysiert und eine PQC-geeignete C-API mit den Partnern erarbeitet.
- Weitere Erkenntnisse und Erfahrungen bezüglich der praktischen Verwendbarkeit von zustandsbehafteten Signaturverfahren.
- Implementierung von Speicheroptimierungen für das Classic McEliece Verfahren.
- Gegenmaßnahmen für Timing Seitenkanalangriffe implementiert.
- Auswahl und Analyse von Open Source Bibliotheken für X.509 und TLS.
- SPHINCS$^+$ Paper: Speichereffizientes Streamen auf eingebetteten Geräten und TPMs.
- XMSS Implementierung als Utimaco HSM Modul.

- Kollaboration mit FLOQI bezüglich des Themas Mixed-PQ PKI.

2.5 AP4: Entwicklung von Hardware-Beschleunigern

MTG AG beteiligt sich nicht direkt an diesem Arbeitspaket.

2.6 AP5: Software-Hardware Co-Design; Integration von HW mit SW

Im AP5 wird untersucht, wie sich die Ergebnisse aus AP3 und AP4 zusammenführen lassen. Es wird ein Software-Hardware Co-Design angestrebt. In UAP1 werden agile Schnittstellen erforscht, so dass die konkrete Implementierung, z.B. in Software oder Hardware, für die Anwendungsschicht transparent ist. UAP2 beschäftigt sich mit transparenten Low-Level Schnittstellen, so dass Hardwareimplementierungen ohne plattformspezifische Details in Software angesprochen werden können. Schließlich untersucht UAP3 die Integration dieser Schnittstellen in Software-Bibliotheken.

MTG AG hat eine für eingebettete Geräte adaptierte Version von Classic McEliece entwickelt. Dazu wurden speichereffiziente Algorithmen in den anderen Arbeitspaketen entwickelt und umgesetzt. Auf der Zielplattform, einem ARM Cortex-M4 Board wurden die getrennten RAM Sections berücksichtigt, um den zur Verfügung stehenden Speicher effizient ausnutzen zu können.

Zusammen mit den Projektpartnern beim Fraunhofer SIT wurde eine Streaming Implementierung für SPHINCS$^+$ in einem hardwarenahen Aufbau entwickelt. Dazu wurde ein Raspberry Pi als TPM mit einem ARM Cortex-M4 Entwicklerboard über SPI zusammengeschlossen. Die TPM Implementierung wurde so angepasst, dass sie inkrementell weitere Signaturdaten anfragt, welche dann in der Streaming Implementierung auf dem Entwicklerboard generiert werden. Es wurden die Laufzeiten und der Speicherverbrauch für verschiedene SPHINCS$^+$ Parametersätze in einem Paper festgehalten, sowohl für das gesamte Setup, als auch als reine Software Implementierung.

Ein Ziel dieses Arbeitspakets ist es, eine einheitliche kryptographische API zu entwickeln, welche flexibel in dem Sinne ist, dass sowohl zur Laufzeit (dynamisch), als auch zur Kompilierzeit (statisch) Algorithmen ausgewählt werden können, so wie verschiedene Implementierungen (Software oder Hardware) angesteuert und ausgetauscht werden können. Hierbei hat MTG AG die Partner unterstützt, insbesondere bei der Berücksichtigung von zustandsbehafteten Verfahren. Beispielsweise sehen gängige kryptographische APIs einen const Qualifier für die Secret Key Inputs vor. Dies verhindert die Nutzung zustandsbehafteter Verfahren über die generische API, da der Zustand im Secret Key angepasst werden muss – in der Regel wird dort ein Index gespeichert und hochgezählt.

Für die Implementierung von XMSS auf einem Hardware Security Modul (HSM) von Utimaco hat die MTG AG die proprietäre CXI Schnittstelle für das HSM analysiert. Die XMSS Implementierung wurde an diese Schnittstelle angepasst und weiter wurden vom HSM bereitgestellte Funktionalitäten eingebunden, wie beispielsweise die intern bereitgestellten Implementierungen für Hashfunktionen. Eine entsprechende externe Komponente kann dann über die CXI Schnittstelle XMSS Keys auf dem HSM nutzen und erhält somit

erweiterte Sicherheitsgarantien des HSM. Insbesondere die Aufbewahrung des zustandsbehafteten Schlüssels im HSM stellt sicher, dass ein Schlüssel und sein Zustand nicht kopiert, gecached, oder anderweitig vervielfältigt werden können, womit die Verwaltung des Zustands vereinfacht wird und das mehrfache Verwenden des selben Zustands effektiv verhindert wird.

Zusammenfassung der Ergebnisse

- Classic McEliece Implementierung auf Cortex M4 Board mit hardwarespezifischen Anpassungen.
- Prototypische TPM Implementierung welche das Streamen von SPHINCS$^+$ Signaturen umsetzt.
- Unterstützung von zustandsbehafteten Kryptosystemen in der agilen API.
- XMSS Modul für Utimaco HSM entwickelt.

2.7 AP6: Evaluation, Integration in Anwendungsfälle und Demonstrator

Gemeinsam mit den Partnern haben wir den Architekturentwurf erarbeitet.

Im Jour-Fixe im Juni 2021 hat MTG AG den anderen Partnern einen kurzen Workshop zu Utimaco HSMs gegeben. Dies ist als Vorbereitung auf eine geplante Integration im Demonstrator geschehen.

Durch einen Top Down Ansatz wurden die Anwendungsfälle identifiziert die im Demonstrator integriert und demonstriert werden. Dazu wurde auf die Ergebnisse aus AP1 zurückgegriffen. Aufbauend auf diesen Anwendungsfällen haben sich die Partner im Konsortium erarbeitet, wie die technische Umsetzung im Rahmen des AP6 erfolgt.

Zusammenfassung der Ergebnisse

- Anwendungsfälle für den Demonstrator identifiziert.
- Architekturentwurf zum Demonstrator erarbeitet.
- Unterstützung beim Erarbeiten des Demonstrator Designs.

2.8 Sonstiges

MTG AG hat den zum im Jahr 2020 veröffentlichten Paper über eine speichereffiziente Classic McEliece Implementierung für eingebettete Systeme auf Nachfrage[9] entsprechenden Source Code auf Github veröffentlicht[10].

[9] https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/PHn7rjmZdfs/m/ZYAUIye4CQAJ

[10] https://github.com/MTG-AG/streamingCME

Weiterhin gab es im Bezug darauf ein Gespräch mit Hanno Becker von ARM, welcher Interesse an einer Integration in mbedTLS geäußert hat. Dabei sind die Gesprächspartner dabei verblieben, dass es vorerst keine konkreten Bemühungen geben wird, aber dennoch interessante Aspekte für mögliche zukünftige (zusammen-)Arbeiten gefunden wurden.

Mit Teilnehmern von dem auch vom BMBF geförderten Projekt QuaSiModO gab es bezogen darauf auch regen projektübergreifenden Informationsaustausch. MTG AG hat im Zuge dessen Hilfestellungen geboten und viele Fragen der Gegenseite klären können. Weiter hat MTG AG Kontakt zu anderen Partnern aus dem Konsortium hergestellt, um sich mit dem auf beiden Seiten bestehenden Interesse bezüglich Hardwarebeschleuniger austauschen zu können.

Außerdem gab es mehrfachen Austausch mit dem Forscherteam um Hwajeong Seo, einem Professor an der Hansung University in Südkorea, welcher auf den Ergebnissen der Arbeit aufbauen wollte.

Weiterhin hat MTG AG den Source Code zum im Jahr 2021 veröffentlichten Paper über SPHINCS$^+$ auf Github veröffentlicht[11]. Es findet sich eine prototypische TPM und ARM Cortex-M4 Implementierung für eine Streaming Variante des Verfahrens.

[11] `https://github.com/QuantumRISC/mbedSPHINCSplusArtifact`

3 Veröffentlichungen

Die folgenden Aufzählungen geben die Veröffentlichungen an, die im Rahmen des QuantumRISC Projekts entstanden sind und an denen MTG AG beteiligt war:

Technische Berichte:

- QuantumRISC Projekt. (2020) Work Package 1, Deliverables 1.1 to 1.3: Use Cases and Requirements – Industrial Use Cases and Requirements for the Deployment of Post-Quantum Cryptography. https://www.quantumrisc.de/results/quantumrisc-wp1-report.pdf
- QuantumRISC Projekt. (2023) Work Package 2, Deliverable 2.1: Analysis and Optimization of PQC Schemes. https://www.quantumrisc.de/results/quantumrisc-wp2-report.pdf
- QuantumRISC Projekt. (2023) Work Package 3, Deliverables 3.1 and 3.2: Development of Software Libraries – Software Implementation Approaches for Post-quantum Cryptography on Embedded Systems. https://www.quantumrisc.de/results/quantumrisc-wp3-report.pdf
- Der Bericht zum Arbeitspaket 5. Dieser wird erst nach diesem Abschlussbericht veröffentlicht.
- Der Bericht zum Arbeitspaket 6. Dieser wird erst nach diesem Abschlussbericht veröffentlicht.

Veröffentlichungen auf Konferenzen:

- Roth J., Karatsiolis E., Krämer J. (2021) Classic McEliece Implementation with Low Memory Footprint. In: Liardet PY., Mentens N. (eds) Smart Card Research and Advanced Applications. CARDIS 2020. Lecture Notes in Computer Science, vol 12609. Springer, Cham. https://doi.org/10.1007/978-3-030-68487-7_3. 19th International Conference, CARDIS 2020.
- Ruben Niederhagen and Johannes Roth and Julian Wälde (2021), Streaming SPHINCS+ for Embedded Devices using the Example of TPMs. In: Cryptology ePrint Archive, Report 2021/1072. https://ia.cr/2021/1072. 13th International Conference on Cryptology AfricaCrypt 2022.

Beteiligungen an anderen Arbeiten:

- Sebastian Paul and Yulia Kuzovkova and Norman Lahr and Ruben Niederhagen (2021), Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3. In: Cryptology ePrint Archive, Report 2021/1447 https://ia.cr/2021/1447

  Hierbei war die MTG AG intensiv an Diskussionen zu dem Thema beteiligt und hat ihr Know-How zur Verfügung gestellt. Jedoch wurde übereinstimmend festgestellt, dass es im weiteren Verlauf nicht weiter der Beteiligung von MTG AG bedarf, um das Projekt erfolgreich durchzuführen. Daraufhin hat MTG AG den eigenen Beitrag als nicht groß genug für eine Co-Autorenschaft erachtet.

4 Verwertungsabsichten

Die MTG AG konnte Know-How im Bereich Post-Quantum-Kryptographie sammeln. Weiterhin konnte Know-How für speichereffiziente und sichere Implementierungen von kryptographischen Verfahren, so wie Detailwissen über verschiedene kryptographische Algorithmen erworben werden. Gleichzeitig konnte sich die MTG AG einen umfassenden Überblick über die aktuelle Forschung und Standardisierung in verschiedenen Gremien (IETF, NIST, BSI) verschaffen. Dies umfasst unter anderem die Themenkomplexe TLS, X.509 Zertifikate und weitere Protokolle, Seitenkanalangriffe und Constant-Time Implementierungen, Schlüsselformate, so wie die generelle Fragestellung um die Kombination von verschiedenen (klassischen und post-quanten) Verfahren in der Praxis.

Die Ergebnisse, so wie die gesammelte Erfahrung und das Know-How, das im Rahmen des QuantumRISC Projektes gesammelt wurde, helfen MTG AG sowohl bei der Integration von PQC Algorithmen in die eigenen Produkte, als auch bei Folgeprojekten.

Die MTG AG ist Partner im QuantID Projekt, welches ebenfalls vom BMBF gefördert wird und Ende des Jahres 2022 begonnen hat. Im QuantID Projekt geht es um digitale Identitäten, bzw., quantensichere Autorisierung und Authentifizierung mithilfe eines QNRGs. Die Ergebnisse des QuantumRISC Projekts können direkt in das QuantID Projekt einfließen, beispielsweise, um Zertifikate für die quantensichere Authentifizierung mittels Post-Quantum-Kryptographie bereitzustellen.

Wir erwarten, dass nach dem Abschluss des Standardisierungsverfahren von NIST viele Firmen und Organisationen, welche noch klassischen Verfahren einsetzen, ihre Lösungen um Post-Quanten-Verfahren erweitern oder umstellen werden. Da ergibt sich Bedarf an Beratung insbesondere in der Migrationsphase. Auch die eingesetzten Produkte müssen entsprechend angepasst werden. Daraus ergeben sich neue Geschäftsfelder, welche die MTG AG durch die im Projekt gewonnen Erfahrungen, einfacher und zuverlässig anschließen kann.

QuantumRISC
Kurzbericht

Version	1.0
Erstellungsdatum	19. Juni 2023
Partner	MTG AG
Fkz BMBF	16KIS1037

GEFÖRDERT VOM

Projektkoordination
Norman Lahr
Fraunhofer-Institut für Sichere Informationstechnologie
Advanced Cryptographic Engineering
Rheinstr. 75
D-64295 Darmstadt
Deutschland

Telefon +49 6151 869100
Fax +49 6151 869224
Mail norman.lahr@sit.fraunhofer.de

1 Kurzbericht

QuantumRISC ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Projekt. Das Ziel des Projekts ist, Post-Quanten-Kryptographie von der Theorie in die Anwendung zu bringen, wobei der Fokus auf eingebetteten Geräten liegt. Dies sind Systeme mit geringen Ressourcen, wie sie zum Beispiel in Steuergeräten in der Automobilbranche vorkommen, aber auch in Industrieanlagen oder in der Telekommunikation. Das Projekt beschäftigt sich mit der Forschung und Analyse von Post-Quanten-Algorithmen, so wie der Entwicklung von effizienten Implementierungen für eingebettete Geräte. Dabei werden sowohl Hardware Implementierungen als auch Software Implementierungen entwickelt.

MTG AG ist ein Partner dieses Projekts und beteiligt sich vorwiegend an den Arbeiten zu Software Implementierungen und der Integration von Post-Quanten-Algorithmen in kryptographischen Protokollen (z.B. X.509 und TLS).

Im Projekt wurden Anforderungen an PQC-Verfahren aus der Industrie betrachtet. Zusätzlich wurde der aktuelle Stand der Wissenschaft bezüglich PQC-Verfahren ermittelt. Darüber hinaus wurden Hardware-Plattformen untersucht. MTG AG hat die Anwendungsfälle insbesondere im Bereich PKI analysiert und untersucht, wie Datenformate in X.509 Zertifikaten umgesetzt werden können, oder welche Änderungen an Richtlinien (Policies) ebenfalls nötig wären. MTG AG hat den Bericht zum ersten Arbeitspaket zusammen mit den Partnern auf internationalen Gremien veröffentlicht.

Zusätzlich wurden PQC-Verfahren und Protokolle, welche die PQC-basierten Primitive benutzen, erforscht. Wir haben PQC-Signaturverfahren analysiert, darunter auch zustandsbehaftete Verfahren (stateful schemes), und anschließend eine enge Auswahl an Verfahren getroffen, welche mit Priorität im weiteren Projektverlauf betrachtet wurden. Dabei hat die MTG AG insbesondere die beiden Verfahren Classic McEliece und SPHINCS$^+$ auf algorithmischer Ebene betrachtet, um sie für bestimmte Einsatzzwecke im Umfeld eingebetteter Systeme hinsichtlich ihres Speicherverbrauchs zu optimieren, der bei diesen Verfahren aus den großen öffentlichen Schlüsseln, beziehungsweise, Signaturen, hervorgeht.

Die Umsetzung der PQC-Verfahren in Software wurde untersucht, wobei das Augenmerk auf die Besonderheiten und die eingeschränkten Ressourcen von eingebetteten Geräten gelegt wurde. Dazu hat die MTG AG zuerst den (damals) aktuellen Stand von existierenden Implementierungen in Softwarebibliotheken analysiert. Die MTG AG hat verschiedene Implementierungen von PQC-Verfahren entwickelt und Härtungsmaßnahmen umgesetzt. Zusätzlich haben wir PQC-Verfahren im TLS-Protokoll integriert und Experimente durchgeführt. Teile dieser Implementierungen sind als Open-Source Projekte veröffentlicht worden. Weiter wurde für das TLS 1.3 Protokoll untersucht, wie sich verschiedene Signaturalgorithmen innerhalb einer Zertifikatskette auf die Performanz im TLS Handshake auswirken, wofür ein automatisierter Testaufbau auf Basis des OpenSSL Forks des Open Quantum Safe Projekts erstellt wurde.

Außerdem wurden Aspekte von Software-Hardware Co-Design betrachtet. In diesem

Bereich haben wir die Schnittstellen der Zielplattformen untersucht und unsere Softwareimplementierungen entsprechend angepasst und in Hardware, sowohl für eingebettete- als auch für Servergeräte, integriert. Im Rahmen der SPHINCS$^+$ Optimierungen hinsichtlich des Speicherbedarfs für Signaturen hat MTG AG mit den Partnern vom Fraunhofer SIT einen Prototyp für das Streamen von Signaturen im TPM 2.0 Protokoll entwickelt.

Darüber hinaus wurden Anwendungsfälle identifiziert, welche in einem Demonstrator integriert und demonstriert werden. Der Architekturentwurf zum Demonstrator wurde erarbeitet.

Unsere wissenschaftlichen Ergebnisse haben wir auf internationalen Konferenzen veröffentlicht. Die Veröffentlichungen waren gemeinsame Arbeiten mit anderen Partnern des QuantumRISC Projekts. Zusätzlich wurden Ergebnisse aus der Entwicklung als Open-Source Projekte veröffentlicht.

Die MTG AG konnte Know-How im Bereich Post-Quantum-Kryptographie sammeln. Weiterhin konnte Know-How für speichereffiziente und sichere Implementierungen von kryptographischen Verfahren, so wie Detailwissen über verschiedene kryptographische Algorithmen erworben werden. Gleichzeitig konnte sich die MTG AG einen umfassenden Überblick über die aktuelle Forschung und Standardisierung in verschiedenen Gremien (IETF, NIST, BSI) verschaffen.

Die Ergebnisse, so wie die gesammelte Erfahrung und das Know-How, das im Rahmen des QuantumRISC Projektes gesammelt wurde, hilft MTG AG sowohl bei der Integration von PQC Algorithmen in die eigenen Produkte, als auch bei Folgeprojekten.

Wir erwarten, dass nach dem Abschluss des Standardisierungsverfahren von NIST viele Firmen und Organisationen, welche noch klassischen Verfahren einsetzen, ihre Lösungen um Post-Quanten-Verfahren erweitern oder umstellen werden. Da ergibt sich Bedarf an Beratung insbesondere in der Migrationsphase. Auch die eingesetzten Produkte müssen entsprechend angepasst werden. Daraus ergeben sich neue Geschäftsfelder, welche die MTG AG durch die im Projekt gewonnen Erfahrungen, einfacher und zuverlässig anschließen kann.