Verwendungsnachweis
Sachbericht
Teil I
„Kurzbericht“

Verbundvorhaben:
PQC-Technologien für den Datenschutz in der medizinischen Versorgung in Deutschland – PQC4MED

Teilvorhaben:
Sicherheitsmodelle und kryptographische Funktionalitäten für PQC Technologien

Verwendungsnachweis Sachbericht Teil I „Kurzbericht“

Förderkennzeichen: 16KIS1043
Laufzeit des Vorhabens: 01.11.2019 bis 31.01.2023

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Zuwendungsgeber:

Bundesministerium für Bildung und Forschung

Zuwendungsempfänger:

Karlsruher Institut für Technologie (KIT)

Institut für Informationssicherheit und Verlässlichkeit (KASTEL)

[(ehemals) Institut für Theoretische Informatik (ITI)]

KASTEL

Karlsruhe, 26.04.2023

Im Folgenden wird „KASTEL“ für die Arbeitsgruppe Kryptographie und Sicherheit unter der Leitung von Herrn Prof. Jörn Müller-Quade verwendet. Seit dem 01.01.2021 gehört die Arbeitsgruppe zu KASTEL -- Institut für Informationssicherheit und Verlässlichkeit.

1 Aufgabenstellung:

Das Projektziel von PQC4MED war es, eine Update-Infrastruktur zu erforschen, modellieren und in einem Demonstrator zu präsentieren, welche die Grundlage schafft Medizintechnikgeräte auf die Verwendung von zukünftigen quanten-resistenten kryptographischen Algorithmen – auch bekannt als Post-Quanten Kryptographie – zu aktualisieren. Die Aufgabenstellung des Einzelvorhabens im Rahmen von PQC4MED war für KASTEL, die Update-Infrastruktur zu modellieren und die Forschung hin zu ihrer beweisbaren Sicherheit voranzutreiben.

2 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

KASTEL kann am Institut auf Vorarbeiten und Wissensgrundlagen im Allgemeinen zur formalen Modellierung von Protokollen sowie deren Sicherheitsanalyse zurückgreifen. Im Speziellen gibt es auch Vorarbeiten zur Modellierung von Langfristiger Sicherheit im Setting von Universeller Komponierbarkeit [1]. Die kryptographische Forschung befasste sich bisher nur wenig mit Krypto-Agilität im Sinne des Ersetzens kryptografischer Verfahren. Einige Arbeiten gibt es zu „updatable Encryption“, bei denen aber nur das sichere Austauschen eines Schlüssels betrachtet wird. Neuere Arbeiten befassen sich mit Familien von Protokollen, innerhalb derer Updates möglich sind. Arbeiten zu Updates eines Systems auf Verfahren, die zum Zeitpunkt des Systemdesigns unbekannt sind, sind nicht bekannt. [2] beschäftigt sich mit der Frage, unter welchen Voraussetzungen derselbe Schlüssel für verschiedene Instanziierungen einer Primitive ohne Sicherheitsverlust wiederverwendet werden kann. Der eigentliche Update-Prozess wird dabei jedoch nicht betrachtet.

3 Planung und Ablauf der Vorhabensbeschreibung

Zu Beginn des Projekts hat KASTEL die interne Dokumentations- und Kommunikationsinfrastruktur aufgesetzt. Im Laufe des Projekts wurde der gegengleich alternierende Termin für die Präsentation projektrelevanter Thematiken wie zum Beispiel neue Forschungsfortschritte, Einblicke in vorhandene Strukturen der Projektpartner und Standardisierungen im Medizinbereich genutzt. Darüber hinaus, zur Vertiefung und zur Gewinnung eins besseren Verständnisses der NIST PQC Kandidaten, wurden intern die einzelnen Verfahren präsentiert. KASTEL hat die Vorstellung von FrodoKEM übernommen. Zur Modellierung der Update-Infrastruktur hat sich eine Kleingruppe regelmäßig getroffen. Die einzelnen Updateprozeduren wurden konzeptionell erarbeitet und mit dem Konsortium in mehreren Feedbackschleifen weiterentwickelt. Ein Demonstrator wurde gemeinsam mit den Projektpartnern konzeptionell entworfen. Das Kick-Off-Meeting am05.11.2019 fand noch in Präsenz bei WIBU in Karlsruhe statt, sodass sich die meisten der Projektmitarbeitende zu Beginn des Projektes persönlich sehen konnten. Die darauffolgenden Konsolidierungstreffen (16.11.2020, 03.12.2021) fanden virtuell statt. Das Meilensteintreffen vom 26.-28.07.2022 an der Universität zu Lübeck war ein großer Erfolg, da die Zusammenarbeit durch Präsenz der meisten Projektmitarbeitenden gestärkt wurde und über schnelle Gespräche in Kleingruppen Missverständnisse aufgedeckt und behoben werden konnten.

4 Die wesentlichen Ergebnisse:

4.1 Modellierung Update-Infrastruktur

Ein erstes Projektergebnis ist, dass die Reihenfolge der zu aktualisierenden Komponenten bestimmt wurde um die Abhängigkeiten zwischen den Komponten darzustellen. Nur bei Einhaltung

dieser Reihenfolg, ist die Funktionalität des Systems gesichert Ein zweites Projektergebnis ist, dass selbst bei einem „atomaren“ Update von einem alten zu einem neuen Zustand ein Zwischenzustand für jede Komponente entsteht: Am Anfang befinden sich alle Komponenten in dem Zustand in dem sie nur klassische Kryptographie verstehen. Im Zwischenzustand sind die Komponenten in der Lage sowohl via klassischer und Post-Quanten Kryptographie im System zu kommunizieren. Der Zielzustand von einem quanten-resistenten Gesamtsystem ist erreicht, wenn alle Komponenten nur noch die zuvor definierte PQC verwenden. Die Auswirkung von unterschiedlichen Komponentenzustände wird weiter im Folgeprojekt „Sec4IoMT“ erforscht. Ein drittes Projektergebnis ist, dass bevor die „kryptographischen Updates“ stattfinden können, sprich dem Austausch von neu-generierten Schlüsselmaterial, etc., muss es passende Format-Updates geben, welche die passenden Algorithmen bereitstellen. Ein viertes Projektergebnis ist, dass ein Hauptaugenmerk auf Übertragung der potentiell zu schützenden kryptographischen Materialen über sichere Kommunikationskanäle gelegt wird.

4.2 Modellierung von Updatemechanismen und langfristiger Sicherheit

KASTEL hat in [3] erforscht inwiefern kryptographische Bausteine langfristige Sicherheitsgarantien bieten können. Dies sind Garantien, die erhalten bleiben, selbst wenn später kryptographische Annahmen gebrochen werden. Das ist sehr wichtig, da kryptographische Annahmen immer wieder gebrochen werden und insbesondere Quantencomputer viele häufig genutzte Annahmen brechen werden. Durch spezielle und neue Techniken ist es KASTEL gelungen zu zeigen, dass es möglich ist wichtige kryptographische Bausteine so zu konstruieren, dass wesentlich Sicherheitseigenschaften erhalten bleiben, selbst bestehende Annahmen (z.B. durch Quantencomputer) gebrochen werden. Im Rahmen einer Masterarbeit [4] hat KASTEL erforscht wie ein Updatemechanismus eines Common-Reference-Strings im UC-Framework aussieht.

4.3 Sichere Kommunikationskanäle

KASTEL hat eine Methode entwickelt, um sichere Kommunikationskanäle mit möglichst wenigen Voraussetzungen zu erstellen [5]. Sichere Kommunikationskanäle sind grundlegend für sehr viele Anwendungen, unter anderem für sichere Updateprozesse, da z.B. die Softwareupdates sicher übertragen werden müssen. Dabei ist es sinnvoll, den Ansatz von KASTEL zu verfolgen und so wenig Voraussetzungen wie möglich zu verwenden, da diese Konstruktionen dann weniger häufig von Angriffen betroffen sind. Des Weiteren hat KASTEL den obigen Ansatz weiterverfolgt und von Public-Key-Verschlüsselung auf „Key Encapsulation Mechanisms“ und hybride Verschlüsselung ausgeweitet [6]. Das erhöht weiter die Praktikabilität des von KASTEL konstruierten Verfahrens. Dies ist eine wichtige Verbesserung, da das NIST derzeit „Key Encapsulation Mechanisms“ standardisiert.

4.4 Krypto-Agilität

KASTEL hat den „State-of-the-Art“ Stand über Kryptoagilität mit in das Projekt einfließen lassen und sich mit den unterschiedlichen Definitionen auseinandergesetzt. Ergebnisse der Schaffung von Awarness hat KASTEL durch Vorträge und Poster dem Fachpublikum präsentiert und so in die Gesellschaft transportiert. Inhaltlich hat sich KASTEL auf den Definitionsbereich der Updatefähigkeit innerhalb der Kryptoagilität fokussiert.

5 Zusammenarbeit mit anderen Forschungseinrichtungen

KASTEL hat im Rahmen von Forschungsarbeiten mit Mitarbeitende vom Forschungszentrum Informatik, die im Projekt QuantumLeap forschen, kooperiert. Für die noch laufende Masterarbeit zum Thema „ Certificate Management for PQC IIoT“ gibt es Kooperation mit Dr. Sebastian Paul (FLOQI/Bosch). Während des Meilensteintreffens ist eine Forschungskooperation zwischen Projektmitarbeitende der Universität zu Lübeck und KASTEL zu „Subversion-resilienter Sicherheitsmodellierung“ entstanden und wird weiter vertieft.

6 Literaturverzeichnis

[1] J. Müller-Quade und D. Unruh, „Long-term security and universal composability," in *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007*, Amsterdam, The Netherlands, 2007.

[2] T. Acar, M. Belenky, M. Bellare und D. Cash, „Cryptographic agility and its relation to circular encryption," in *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques* , Monaco / French Riviera, 2010.

[3] R. Berger, B. Broadnax, M. Klooß, J. Mechler, J. Müller-Quade, A. Ottenhues und M. Raiber, „Composable Long-Term Security with Rewinding," *Cryptology ePrint Archive,* 2023.

[4] S. Eilebrecht, *Composable Definitions of Long-Term Security for Commitment Schemes and their Applications,* Karlsruhe Institute of Technology (KIT): Master thesis, 2021.

[5] W. Beskorovajnov, R. Gröll, J. Müller-Quade, A. Ottenhues und R. Schwerdt, „A new security notion for PKC in the standard model: weaker, simpler, and still realizing secure channels," in *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, 2022.

[6] R. Schwerdt, L. Benz, W. Beskorovajnov, S. Eilebrecht, J. Müller-Quade und A. Ottenhues, „Sender-binding Key Encapsulation," in *Cryptology ePrint Archive*, 2023.

Verwendungsnachweis Sachbericht
Teil II
„Eingehende Darstellung“

Verbundvorhaben:
PQC-Technologien für den Datenschutz in der medizinischen Versorgung in Deutschland – PQC4MED

Teilvorhaben:
Sicherheitsmodelle und kryptographische Funktionalitäten für PQC Technologien

Verwendungsnachweis Sachbericht Teil II „Eingehende Darstellung“

Förderkennzeichen: 16KIS1043
Laufzeit des Vorhabens: 01.11.2019 bis 31.01.2023

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Zuwendungsgeber:

Bundesministerium für Bildung und Forschung

Zuwendungsempfänger:

Karlsruher Institut für Technologie (KIT)

Institut für Informationssicherheit und Verlässlichkeit (KASTEL)

[(ehemals) Institut für Theoretische Informatik (ITI)]

KASTEL

Karlsruhe, 26.04.2023

Im Folgenden wird „KASTEL“ für die Arbeitsgruppe Kryptographie und Sicherheit unter der Leitung von Herrn Prof. Jörn Müller-Quade verwendet. Seit dem 01.01.2021 gehört die Arbeitsgruppe zu KASTEL -- Institut für Informationssicherheit und Verlässlichkeit.

1 Aufgabenstellung

Das Projektziel von PQC4MED war es, eine Update-Infrastruktur zu erforschen, modellieren und in einem Demonstrator zu präsentieren, welche die Grundlage schafft Medizintechnikgeräte auf die Verwendung von zukünftigen quanten-resistenten kryptographischen Algorithmen – auch bekannt als Post-Quanten Kryptographie – zu aktualisieren.

Die Aufgabenstellung des Einzelvorhabens im Rahmen von PQC4MED war für KASTEL, die Update-Infrastruktur zu modellieren und die Forschung hin zu ihrer beweisbaren Sicherheit voranzutreiben. Der erste Arbeitsschritt bestand für KASTEL im Einarbeiten in verschiedene quanten-resistente Verfahren und Protokolle. Da post-quantum-sichere Verfahren noch nicht ausreichend verstanden sind, besteht die Gefahr, dass falsche Auswahlentscheidungen in Zukunft zu Sicherheitsproblemen führen können. KASTEL beschäftigt sich auch mit Fragen im Bereich quantencomputer-resistente Verfahren und ihre Sicherheitseigenschaften, insbesondere im Hinblick auf Sicherheitsmodelle und -begriffe.

Zeitgleich hat sich KASTEL direkt mit einem grundlegenden und wesentlichen Aspekt des Einzelvorhabens befasst: Die formale und beweisbar sichere Modellierung eines atomaren Update-Prozesses. Ohne formale Modelle kann keine wissenschaftlich fundierten Entscheidungen über die Sicherheit von Lösungen getroffen werden. Die entwickelten Protokolle sollen ihre Sicherheit behalten, auch wenn Annahmen im Nachhinein als falsch erkannt werden. Das Hauptaugenmerk des Projekts liegt jedoch auf der Entwicklung von Lösungen für eine einfache Migration zu Quantencomputer-resistenten Verfahren.

PQC4MED zielt darauf ab, durch die Entwicklung von Update-Infrastrukturen die Migrationsfähigkeit und Krypto-Agilität von PQC-Verfahren sicherzustellen, um auf die erwartete Umstellung auf PQC-Verfahren vorbereitet zu sein. KASTEL hat sich mit der Sicherheit des Update-Prozesses befasst und untersucht, wie Sicherheit von Protokollen modelliert werden kann, wenn Annahmen nicht mehr gelten. Langfristige, austauschbare kryptographische Lösungen sind notwendig, um eine überlebensfähige Infrastruktur im Gesundheitswesen zu gewährleisten.

2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Für das Projekt wurde eine neue wissenschaftliche Mitarbeiterin mit Promotionsabsicht, Frau Astrid Ottenhues, akquiriert. Sie hat das Projekt PQC4MED hauptverantwortlich inhaltlich für KASTEL betreut. Für die Forschungsarbeiten konnte sie mit Ihren Kolleginnen und Kollegen unter der Betreuung von Prof. Dr. Jörn Müller-Quade auf eine breite Wissensbasis aufbauen und gemeinsam relevante wissenschaftliche Ergebnisse erzielen.

Aufgrund von Corona-bedingten Ausfällen sowie der sich verspätenden Bekanntgabe der zu standardisierenden PQC-Algorithmen von dem NIST gab es die Notwendigkeit einer kostenneutralen Verlängerung der Projektlaufzeit. Durch (Corona-bedingte) Terminverschiebungen im Konsortium hat sich die fertige Modellierung sowie die dazugehörige beweisbare Sicherheitsanalyse verschoben, aber inhaltlich im Rahmen der Projektlaufzeit abgeschlossen.

3 Planung und Ablauf der Vorhabensbeschreibung

Zu Beginn des Projekts hat KASTEL die interne Dokumentationsinfrastruktur aufgesetzt, indem es eine Mailingliste und ein GIT bereitgestellt hat. Als Arbeitspaketleitung von AP 2 hat KASTEL darüber hinaus auch für die Zusammentragung der (Zwischen-)Ergebnisse und die Erstellung eines internen Deliverables ein Overleaf aufgesetzt, geteilt und gepflegt. Für den intensiveren Austausch hat KASTEL im Laufe des AP2 einen virtuellen BigBlueButton-Raum zur Verfügung gestellt, welcher dann für einstündige Konsolidierungstreffen alle zwei Wochen genutzt wurde. Dieser regelmäßige Austausch hat zu einem größeren Verständnis geführt, wie die einzelnen Projektpartner ihre Rollen für die Update-Infrastruktur einnehmen.

Im Laufe des Projekts wurde der gegengleich alternierende Termin für die Präsentation projektrelevanter Thematiken wie zum Beispiel neue Forschungsfortschritte, Einblicke in vorhandene Strukturen der Projektpartner und Standardisierungen im Medizinbereich genutzt. Darüber hinaus, zur Vertiefung und zur Gewinnung eins besseren Verständnisses der NIST PQC Kandidaten, wurden intern die einzelnen Verfahren präsentiert. KASTEL hat die Vorstellung von FrodoKEM übernommen.

Zur Modellierung der Update-Infrastruktur hat sich eine Kleingruppe bestehend aus Dr. Carmen Kempka (WIBU), Martin Böhning (CRS - als Unterauftragnehmer von Schölly) und Astrid Ottenhues (KASTEL) regelmäßig getroffen, um von der praxisnahen Realität des Updates zu einer formalen Modellierung zu kommen. Aus der anderen Richtung sind formale Kriterien aus der Sicherheitsanalyse in das Modell so eingeflossen, dass sie in der praxisnahen Realisierung des Demonstrators Anwendung fanden. Die einzelnen Updateprozeduren wurden konzeptionell erarbeitet und mit dem Konsortium in mehreren Feedbackschleifen weiterentwickelt. Letzteres fanden in den regulären TelKos sowie in dedizierten von KASTEL geführten virtuellen Workshops statt. KASTEL hat bei den Update-Prozessen einen Fokus auf Kryptoagilität gelegt, sowie auf die universelle Komponierbarkeit bei der formalen Modellierung des Update-Prozesses. Die inhaltlichen Ergebnisse der formalen Modellierung und Sicherheitsanalyse werden in Abschnitt 6.3.5 beschrieben.

Ein Demonstrator wurde gemeinsam mit den Projektpartnern konzeptionell entworfen. Dieser soll die Use-Cases aus AP 2.1 anschaulich darstellen. Hierfür wurde ein interner Workshop durchgeführt.

Das Kick-Off-Meeting am05.11.2019 fand noch in Präsenz bei WIBU in Karlsruhe statt, sodass sich die meisten der Projektmitarbeitende zu Beginn des Projektes persönlich sehen konnten. Die darauffolgenden Konsolidierungstreffen (16.11.2020, 03.12.2021) fanden virtuell statt. Das Meilensteintreffen vom 26.-28.07.2022 an der Universität zu Lübeck war ein großer Erfolg, da die Zusammenarbeit durch Präsenz der meisten Projektmitarbeitenden gestärkt wurde und über schnelle Gespräche in Kleingruppen Missverständnisse aufgedeckt und behoben werden konnten.

4 Vergleich zur ursprünglichen Vorhabensbeschreibung

Ein Fokus hat sich auf die Thematik „sichere Kommunikationskanäle“ verlagert: Bei der Modellierung der Update-Infrastruktur hat sich frühzeitig herausgestellt, dass wir folgende Annahme aufstellen: die Kommunikationskanäle über die wir die Update-Informationen verschicken müssen sicher sein.

KASTEL hat verstärkt einen Fokus auf das „Awareness Schaffen“ für Krypto-Agilität über einen einmaligen Wechsel zu festen PQC-Algorithmen hin zu flexiblen Update-Infrastrukturen gelegt, welche unter bestimmten Voraussetzungen nach dem Austausch der Algorithmen ein ähnliches Sicherheitsniveau wie vor dem Austausch erhalten. Bei den Industriepartnern ist während der Projektlaufzeit das Bewusstsein für die erhöhte Komplexität der Implementierung einer agilen Update-Infrastruktur gewachsten und auch die hohe Relevanz von kryptoagilen Updateprozessen merklich gestiegen.

Im Allgemeinen lässt sich festhalten, dass ein zusätzliches und gleichzeitig grundlegendes Ziel von PQC4MED darin erreicht wurde, dass eine Sensibilisierung für eine Bestandsanalyse zu updatefähigen Systemen zu Beginn geschaffen wurde. Wenn folgende Fragen geklärt sind, kann darauf aufgebaut werden, eine geeignete kryptoagile Update-Infrastruktur zu quanten-resistente kryptographischen Algorithmen zu modellieren und demonstrieren: Wo wird welche Kryptographie verwendet? Wer hat welche Berechtigungen? Was passiert bei einem Austausch von einer bestimmten kryptographischen Komponente?

5 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

KASTEL kann am Institut auf Vorarbeiten und Wissensgrundlagen im Allgemeinen zur formalen Modellierung von Protokollen sowie deren Sicherheitsanalyse zurückgreifen. Im Speziellen gibt es auch Vorarbeiten zur Modellierung von Langfristiger Sicherheit im Setting von Universeller Komponierbarkeit [1].

Im Bereich medizinischer Anwendungen sind KASTEL keinerlei Vorarbeiten im Bereich QC-resistenter Kryptographie bekannt. Die kryptographische Forschung befasst sich bisher nur wenig mit Krypto-Agilität im Sinne des Ersetzens kryptografischer Verfahren. Einige Arbeiten gibt es zu „updatable Encryption“, bei denen aber nur das sichere Austauschen eines Schlüssels betrachtet wird. Neuere Arbeiten befassen sich mit Familien von Protokollen, innerhalb derer Updates möglich sind. Arbeiten zu Updates eines Systems auf Verfahren, die zum Zeitpunkt des Systemdesigns unbekannt sind, sind nicht bekannt. Hier ergibt sich jedoch eine Schwachstelle, da das Ändern kryptografischer Verfahren ein verlockender Angriffspunkt ist. Ein Angreifer, dem es gelingt, ein unsicheres Verfahren über den Update-Prozess zu verteilen, kann Zugriff auf zahllose schutzbedürftige Endgeräte erlangen. Hier ist es also nötig, diesen Angriffspunkt zu schützen, z.B. durch das Verteilen von Vertrauen, so dass ein Angreifer mehrere Organisationen gleichzeitig kompromittieren muss.
[2] beschäftigt sich mit der Frage, unter welchen Voraussetzungen derselbe Schlüssel für verschiedene Instanziierungen einer Primitive ohne Sicherheitsverlust wiederverwendet werden kann. Der eigentliche Update-Prozess wird dabei jedoch nicht betrachtet.

6 Die wesentlichen Ergebnisse

In den folgenden Abschnitten werden die Hauptergebnisse seitens KASTEL für das Einzelvorhaben von PQC4MED präsentiert. Eine grobe Zuordnung zu den APs wurde vorgenommen, jedoch wurden inhaltliche Ergebnisse zusammen präsentiert um das Verständnis und den Lesefluss zu erleichtern.

6.1 AP 2: Anforderungsanalyse (9 PM)

Die Anforderungsanalyse wurde termingerecht abgeschlossen. Innerhalb des Konsortiums wurden Use-Cases definiert, die am Beispiel von endoskopischen Bildgebungssystem die Verwendung von Kryptographie im laufenden Betrieb und das sichere Update von kryptographischen Verfahren in deren Secure Element untersucht. Aus der Bedrohungsanalyse sowie Standardisierungsempfehlungen von dem NIST und dem BSI hat das Konsortium Anforderungen an mögliche PQC Algorithmen definiert. In einem internen Deliverable wurden die Ergebnisse der einzelnen Projektpartner sowie der gemeinsamen Diskussion im Konsortium dokumentiert und für die weiteren APs vorbereitet. Für den „State-of-the-Art“ in der Wissenschaft der Kryptoagilität hat KASTEL dem Konsortium zusätzliche Informationen bereitgestellt um die Anforderungen an PQC Algorithmen zu extrahieren.

6.2 AP 3: PQC Verfahren und Einbettung (6 PM)

Die Auswahl der PQC Verfahren ist abgeschlossen, deren Einbettung und Sicherheitsarchitektur ist inhaltlich abgeschlossen und die Ergebnisse wurden in einem internen Deliverable dokumentiert. Das Konsortium hat mit Kyber [3] und FrodoKEM [4] zwei gitterbasierte KEMs ausgewählt. Als Signaturverfahren wurden Picnic [5] und LMS gewählt.

6.3 AP 4: Entwicklung generischer PQC-Hardware und Implementierung von Updatemechanismen

KASTEL erarbeitet Modellierungen der konzeptionell-beschriebenen Updateprozeduren aus AP 3. Der Fokus wurde im Konsortium auf die Modellierung der atomaren Updates der einzelnen Komponenten sowie deren Abhängigkeit gelegt, für letzteren Aspekt erforscht KASTEL den Begriff der universell komponierbaren Updatemechanismen.

6.3.1 Post-Quanten Kryptographie und Quanten-Sicherheit

Für und bei der regelmäßigen Durchführung des Seminars „Post-Quantum Cryptography“ hat KASTEL grundlegendes Wissen über die verschiedenen PQC-Algorithmen erlangt und je nach Forschungsfortschritt in der Community auch aktualisieren und weitergeben können.

Als Forschungsprojekt zur Einarbeitung in die Thematik „gitterbasierter Protokolle“ hat KASTEL Verfahren für „Black Box Accumulation“ erforscht [6]. Das wichtigste Ergebnis hierbei war, dass KASTEL es geschafft hat „Black Box Accumulation“ auf Basis von Gittern zu konstruieren, weshalb diese Konstruktion sicher gegen Angreifer mit Zugriff auf Quantencomputer ist.

KASTEL hat im Rahmen einer Masterarbeit die Konstruktion von „Oblivious Pseudorandom Functions“ (OPRFs) mit Hilfe von „Garbled Circuits“ erforscht [7]. OPRFs werden z.B. für sichere Authentifizierung verwendet [8]. Sichere und zuverlässige Authentifizierung ist wesentlich für sichere und robuste Updateprozesse. Der Vorteil der Verwendung von „Garbled Circuits“ ist, dass diese auf symmetrischer Kryptographie basieren und daher auch gegen Angreifer mit Zugriff auf Quantencomputer noch sicher sein werden. Fortführend plant KASTEL eine erweiterte Version des genannten Forschungsergebnisses zu publizieren.

Durch das Seminar „Quantum Information Theory“ hat KASTEL sein Grundlagenwissen im Bereich der Quantenkryptographie gestärkt. KASTEL hat im Rahmen von zwei Masterarbeiten erforscht, welche Schwachstellen durch Superpositions-Angriffe für zukünftige Verfahren entstehen [9, 10].

6.3.2 Sichere Kommunikationskanäle

KASTEL hat eine Methode entwickelt, um sichere Kommunikationskanäle mit möglichst wenigen Voraussetzungen zu erstellen [11]. Sichere Kommunikationskanäle sind grundlegend für sehr viele Anwendungen, unter anderem für sichere Updateprozesse, da z.B. die Softwareupdates sicher übertragen werden müssen. Dabei ist es sinnvoll, den Ansatz von KASTEL zu verfolgen und so wenig Voraussetzungen wie möglich zu verwenden, da diese Konstruktionen dann weniger häufig von Angriffen betroffen sind.

Des Weiteren hat KASTEL den obigen Ansatz weiterverfolgt und von Public-Key-Verschlüsselung auf „Key Encapsulation Mechanisms“ und hybride Verschlüsselung ausgeweitet [12]. Das erhöht weiter die Praktikabilität des von KASTEL konstruierten Verfahrens. Dies ist eine wichtige Verbesserung, da das NIST derzeit „Key Encapsulation Mechanisms“ standardisiert.

6.3.3 Krypto-Agilität

KASTEL hat den „State-of-the-Art“ Stand über Kryptoagilität mit in das Projekt einfließen lassen und sich mit den unterschiedlichen Definitionen auseinandergesetzt. Ergebnisse der Schaffung von Awarness hat KASTEL wie in Abschnitt 10 beschrieben durch Vorträge und Poster dem Fachpublikum präsentiert und so in die Gesellschaft transportiert. Inhaltlich hat sich KASTEL auf den Definitionsbereich der Updatefähigkeit innerhalb der Kryptoagilität fokussiert.

6.3.4 Modellierung von Updatemechanismen und langfristiger Sicherheit

KASTEL hat in [13] erforscht inwiefern kryptographische Bausteine langfristige Sicherheitsgarantien bieten können. Dies sind Garantien, die erhalten bleiben, selbst wenn später kryptographische Annahmen gebrochen werden. Das ist sehr wichtig, da kryptographische Annahmen immer wieder gebrochen werden und insbesondere Quantencomputer viele häufig genutzte Annahmen brechen werden. Durch spezielle und neue Techniken ist es KASTEL gelungen zu zeigen, dass es möglich ist wichtige kryptographische Bausteine so zu konstruieren, dass wesentlich Sicherheitseigenschaften erhalten bleiben, selbst bestehende Annahmen (z.B. durch Quantencomputer) gebrochen werden. Aktuell und weiterführend forscht KASTEL an einer Modellierung für ein universell komponierbares langfristig sicheres Updaten im Random-Oracle-Modell sowie die generische Modellierung von langfristig sicheren Updates im UC-Framework [14]. Im Rahmen einer Masterarbeit [15] hat KASTEL erforscht wie ein Updatemechanismus eines Common-Reference-Strings im UC-Framework aussieht.

Im Rahmen einer Masterarbeit in Betreuungskooperation mit Dr. Sebastian Paul aus dem Projekt FLOQI wird das Zertifikatsmanagement von Bosch für das Update auf PQC-Algorithmen im IIoT-Bereich untersucht. Diese Arbeit soll Anfang Mai 2023 abgeschlossen sein.

6.3.5 Modellierung Update-Infrastruktur

Die Modellierung der Update-Infrastruktur fand inhaltlich hauptsächlich in der Arbeitsgruppe bestehend aus Dr. Carmen Kempka (WIBU), Martin Böhning (CRS) und Astrid Ottenhues (KASTEL) statt. Die Haupterkenntnisse dieses Prozesses werden im Folgenden beschrieben. Erst wurde sich gegenseitig auf den aktuellen Stand gebracht, welcher für die Modellierung relevant ist, da sehr verschiedenen Sichtweisen auf die Problematik schauen. Zu Beginn wurden alle Komponenten extrahiert, welche mit kryptographischem Material arbeiten. Diese Komponenten wurden dann in Abhängigkeit gebracht.

Ein erstes Projektergebnis ist, dass die Reihenfolge der zu aktualisierenden Komponenten bestimmt wurde um die Abhängigkeiten zwischen den Komponten darzustellen. Nur wenn diese Reihenfolge eingehalten wird, ist gesichert, dass das System weiterhin sicher funktioniert.

Ein zweites Projektergebnis ist, dass selbst bei einem „atomaren“ Update von einem alten zu einem neuen Zustand ein Zwischenzustand für jede Komponente entsteht: Am Anfang befinden sich alle Komponenten in dem Zustand in dem sie nur klassische Kryptographie verstehen. Im Zwischenzustand sind die Komponenten in der Lage sowohl via klassischer und Post-Quanten Kryptographie im System mit allen Komponenten zu kommunizieren. Der Zielzustand von einem quanten-resistenten Gesamtsystem ist erreicht, wenn alle Komponenten nur noch die zuvor definierte Post-Quanten Kryptographie verwenden. Innerhalb eines Systems kann es sein, dass unterschiedliche Komponten sich in unterschiedlichen Zuständen befinden. Diese Auswirkung wird weiter im Folgeprojekt „Sec4IoMT“ erforscht.

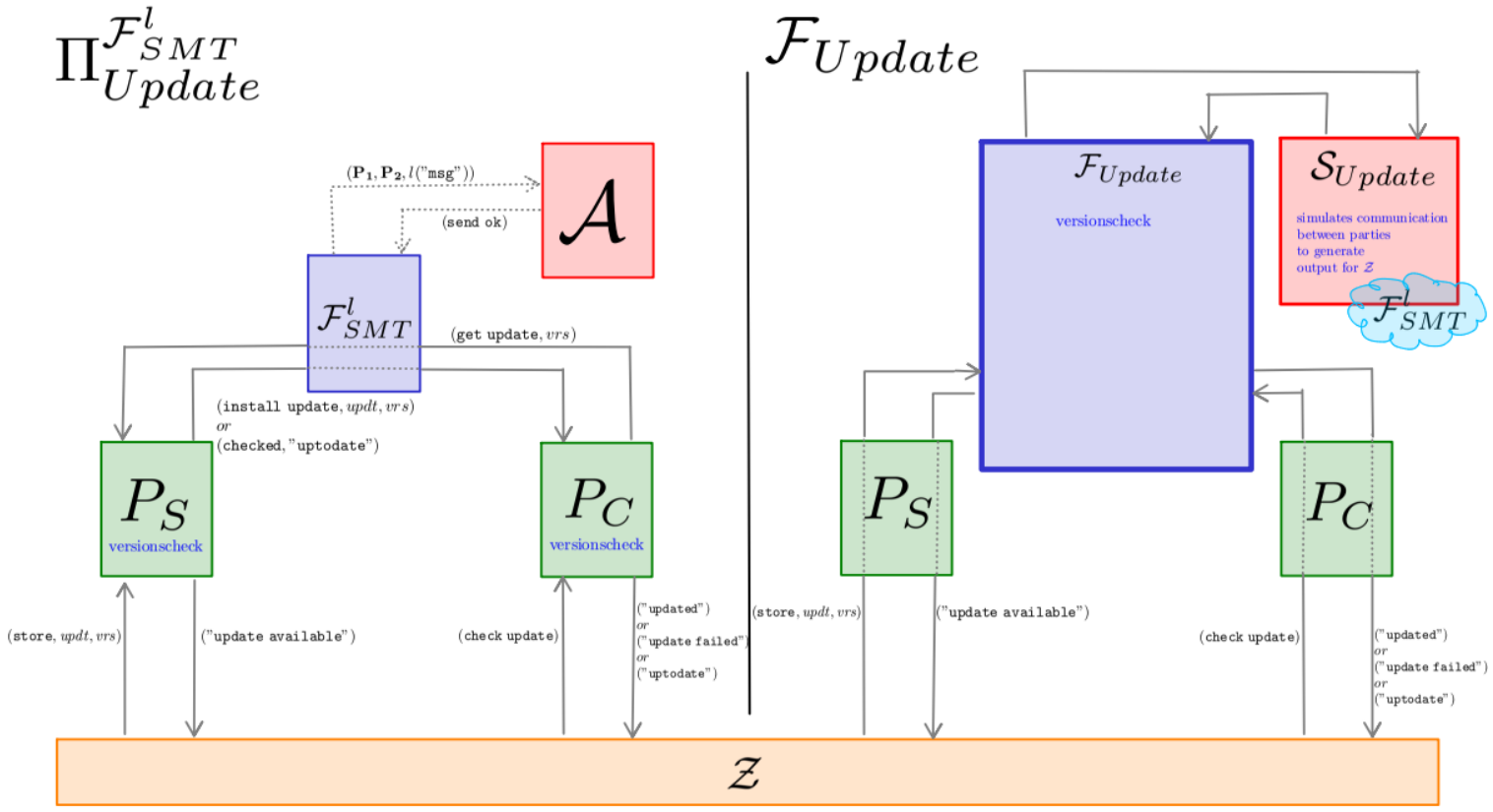
Ein drittes Projektergebnis ist, dass bevor die „kryptographischen Updates“ stattfinden können, sprich dem Austausch von neu-generierten Schlüsselmaterial, der Aufbau von neuen Kommunikationskanäle, und dergleichen, muss es passende „Format-Updates“ geben, welche die passenden Algorithmen in den einzelnen Komponenten bereitstellen.

Ein viertes Projektergebnis ist, dass ein Hauptaugenmerk auf Übertragung der potentiell zu schützenden kryptographischen Materialen über sichere Kommunikationskanäle gelegt wird.

Für viele diese Projektergebnisse konnte KASTEL aus den zuvor genannten Forschungsergebnissen nennenswerte Fortschritte erzielen und diese im Projekt mit einfließen lassen.

Formalisierung der Update-Prozedur im UC-Framework

Eine Updateprozedur ist der Prozess von einem aktuellen Zustand zu einem neuen – als besser angenommenen – Zustand. Für diesen Übergang geben wir ein Protokoll $\pi_{Update}^{F_{SMT}^{l}}$ zwischen einem Nutzer P_c und einem Server P_s an. Im Protokoll ist die Kommunikation über einen sicheren Kanal via der idealen Funktionalität für „secure message transfer“ F_{SMT}^{l} realisiert. Mit der Angabe eines Simulators, welcher einen idealen Angreifer im UC-Framework darstellt, zeigen wir, dass das Protokoll die ideale Funktionalität für Updates F_{Update} realisiert. Die formalen Beschreibungen der einzelnen Komponenten sind im projektinternen Deliverable zu AP 4 festgehalten. Folgend zeigen wir für ein übersichtliches Verständnis die graphische Darstellung der Sicherheitsanalyse und die Formalisierung der Update-Prozedur im UC-Framework:



6.4 AP 8: Evaluierung (7 PM)

KASTEL hat die Modellierung auf ihre Modularisierung überprüft und dabei die einzelnen schrittweisen Vorgehensweisen zur Erstellung einer Update-Prozedur mit herauskristallisiert. Anschließend wurde das Modell formalisiert. Für diese Formalisierung wurde eine Sicherheitsanalyse durchgeführt, welche zeigt, dass das angegebene Update-Protokoll die genannte ideale Funktionalität für Updates im UC-Framework sicher realisiert. KASTEL hat auf die Sicherheit von den Kommunikationskanäle hingewiesen, sodass diese im Demonstrator eine erhöhte Relevanz bekommen haben. Dazu zeigt KASTEL, wie langfristige Sicherheit modelliert werden kann.

6.5 AP 9: Vorbereitung und Standardisierung der Ergebnisse (2 PM)

Die im Abschnitt 6.3.5 beschriebenen Projektergebnisse sind zum Teil generischer Natur und werden im Rahmen weitere Projekt- und Forschungsarbeiten seitens KASTEL berücksichtigt. Durch die geplante Veröffentlichung aus der Formalisierung werden die Ergebnisse zur Formalisierung und im Allgemeinen zu Update-Prozeduren einem Peer-Review unterzogen und der Öffentlichkeit zur Verfügung gestellt.

Wie in Abschnitt 10 beschrieben, hat KASTEL durch Vorträge und Postersession Awarness für kryptoagile Update-Prozeduren geschaffen und plant dies auch weiterhin zu tun.

Das im Rahmen von PQC4MED generierte Erklärvideo wird KASTEL bei seinen Ausstellungen nutzen um die Projektergebnisse zu präsentieren und zeitgleich auf die steigende Gefahr von Quantencomputer-basierten Angriffen im Medizinsektor aufmerksam zu machen.

7 Zusammenarbeit mit anderen Forschungseinrichtungen

KASTEL hat im Rahmen von Forschungsarbeiten mit Mitarbeitende vom FZI, Forschungszentrum Informatik, die im Projekt QuantumLeap forschen, kooperiert. Bei diesen Forschungsarbeiten und darüber hinaus sind Synergieeffekte der beiden Projekte genutzt worden. Für die noch laufende Masterarbeit zum Thema „ Certificate Management for PQC IIoT“ gibt es Kooperation zwischen Dr. Sebastian Paul von Bosch im Rahmen des Projektes FLOQI und KASTEL.

Während des Meilensteintreffens in Lübeck im Sommer 2022 ist eine Forschungskooperation zwischen Projektmitarbeitende der Universität zu Lübeck und KASTEL zu „Subversion-resilienter Sicherheitsmodellierung“ entstanden und wird weiter vertieft. Es ist aufgefallen, dass der Schutz gegen den Austausch eines manipulierten Codes essenziell ist, um die Update-Prozedur sicher durchführen zu können.

8 Die wichtigsten Positionen des zahlenmäßigen Nachweises

Für das Projekt wurde eine wissenschaftliche Mitarbeiterin mit Promotionsabsicht akquiriert, die das Projekt hauptsächlich inhaltlich betreut hat. Für die Arbeit in diesem Projekt wurden für diese Mitarbeiterin zum größten Teil die Personalmittel, sowie zusätzlich Sachmittel und Reisemittel, verwendet.

Dienstreisen wurden von der aus Projektmitteln bezahlten Mitarbeiterin, den am Projekt beteiligten Professor und den mit Projektaufgaben betrauten, aber nicht aus dem Projekt finanzierten Mitarbeitenden durch-

geführt. Sie dienten zur Diskussion von projektbezogenen Fragestellungen mit externen Fachleuten, zur Vorstellung von Projektergebnissen, zu projektbezogenen Forschungsfragen mit Projektpartner*innen sowie zu projektinternen Abstimmungen.

9 Die Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die Notwendigkeit der geleisteten Arbeit ergibt sich aus der Wichtigkeit der Forschungsthemen und den mit ihrer Bearbeitung verbundenen hohen wissenschaftlichen Risiken. Zu Beginn des Projektes gab es zu der Thematik der Krypto-Agilität in der IT-Sicherheitsbranche hauptsächlich die Aufforderung zu mehr Forschung und erste, definitorische Ansätze sowie eine Einordnung der Thematik. Selbst zum Ende der Projektlaufzeit gibt es zwar viele weitere und unterschiedliche Definitionen für Krypto-Agilität aus der Forschungscommunity der Kryptographie, jedoch ist noch kein einheitlicher Konsens gefunden. KASTEL bringt mit der Sichtweise der „updatefähigen“ Modellierung dieses Forschungsfeld grundlegend voran. Zusätzlich hat sich der Fokus auf eine formale Modellierung samt Sicherheitsanalyse im Projekt seitens KASTEL bewährt, da so eine Update-Infrastruktur für ein atomares Update von aktuellen kryptographischen Verfahren zu potentiell quanten-resistente Verfahren gezeigt werden konnte. Dieses wird nun in einem Folgeprojekt, das von einem Konsortium getragen wird, das sich mit dem des Projektes PQC4MED stark überschneidet, weiter vertieft und generalisiert wird. Die letzten Punkte unterstreichen auch die Angemessenheit der geleisteten Projektarbeiten.

10 Die Verwertbarkeit der Ergebnisse

Während der Projektlaufzeit gab es einen direkten Austausch zwischen den Seminaren „Post-Quantum Cryptography“ und „Quantum Information Theory“. Wissensgrundlagen zu PQC-Algorithmen und zu Quantenkryptographie wurden im Projekt genutzt und umgekehrt sind neue Forschungserkenntnisse zurück in die Seminare geflossen. Die in Abschnitt 12 gelistete Publikationen fließen in mehrere Promotionsarbeiten von Doktorandinnen und Doktoranden bei KASTEL ein. Mehrere Fragestellungen haben sich aus dem Projekt für erfolgreich abgeschlossene und noch offene Masterarbeiten ergeben.

Beim „Women in Security and Cryptography Workshop“ (21.-23.09.2021) hat Astrid Ottenhues einen Lightnight Talk zum Thema „Cryptoagility“ präsentiert. Auch für die Ausgabe des Workshops vom 27.-29.06.2023 hat sich Astrid Ottenhues erfolgreich um eine Teilnahme beworben und plant einen Beitrag zur Sicherheitsmodellierung von updatefähigen Protokollen.

Beim Workshop „Post-Quanten Kryptographie in der Praxis“ der INFORMATIK2021 am 28.09.2021 hat Astrid Ottenhues mit dem Vortrag „PQC4MED: Cryptoagility in Medical Technology“ den Stand der Forschung sowie des Projektes präsentiert. Einen ähnlichen Vortrag mit vertiefender Forschungsfrage hat Sie beim Workshop „Young Research in Cryptography“ (01.-03.03.2023) gegeben. Im Rahmen der „Nationalen Konferenz IT-Sicherheitsforschung 2023“ (13.-15.03.2023) konnte Astrid Ottenhues mit Ihrem Poster zum Thema Kryptoagilität erfolgreich während der Postersession „Austausch vor Ort mit der Community“ präsentieren.

Das Ergebnis einer atomaren Update-Infrastruktur für eingebettete Medizingeräte aus diesem Projekt wird im Folgeprojekt „Sec4IoMT“ vertieft und auf mehrere vernetzte Medizingeräte erweitert. Im Rahmen dieses Projekts wird auch die aufgekommene Fragestellung von einer Subversion-resilienter Sicherheitsanalyse im Framework der universellen Komponierbarkeit als Forschungsprojekt zwischen den Projektpartnern KASTEL und Universität zu Lübeck intensiviert.

Um auch in der Gesellschaft ein Bewusstsein zu schaffen, hat KASTEL Erfahrung mit einem Kurzvideo zum Quantencomputer-basierte und Post-Quanten-Kryptographie gesammelt und unterstützte das Konsortium bei der Planung zur Erstellung eines Erklärvideos für PQC4MED. Das von macio fertiggestellte Video plant

KASTEL im Rahmen von Veranstaltungen für die Öffentlichkeit wie zum Beispiel dem „Tag der offenen Tür“ des KIT einzusetzen.

11 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

- Das NIST hat 2022 folgende PQC-Algorithmen standardisiert: Kyber als KEM-Algorithmus und für Digitale Signaturalgorithmen wurden DILITHIUM, Falcon und SPHINCS+ standardisiert. https://csrc.nist.gov/Projects/post-quantum-cryptography
- Das NIST hat im Oktober 2020 die Empfehlung für Stateful Hash-based Signatur Verfahren herausgegeben: https://csrc.nist.gov/publications/detail/sp/800-208/final
- Das BSI hat im August 2020 Handlungsempfehlungen zur PQC-Migration herausgegeben: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf
- Es gab Fortschritte im Bereich der Quantencomputer, z.B. kündigte IBM an, bis 2023 einen Quantencomputer mit 1121 Qubits zu bauen: https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/
- Das BSI hat im Dezember 2021 den Leitfaden „Kryptografie quantensicher gestalten“ herausgegeben, damit ihre Handlungsempfehlungen aktualisiert und damit auch einen weiteren Fokus auf die Kryptoagilität gesetzt: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf
- Das NIST hat 2022 eine neue Auschreibung für Digitale PQC Signaturalgorithmen ausgeschrieben: https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals

12 Die erfolgten oder geplanten Veröffentlichungen des Ergebnisses

Veröffentlichungen aus KASTEL:

[11] W. Beskorovajnov, R. Gröll, J. Müller-Quade, A. Ottenhues und R. Schwerdt, „A new security notion for PKC in the standard model: weaker, simpler, and still realizing secure channels,“ in *Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, 2022.

[12] R. Schwerdt, L. Benz, W. Beskorovajnov, S. Eilebrecht, J. Müller-Quade und A. Ottenhues, „Sender-binding Key Encapsulation,“ in *Cryptology ePrint Archive*, 2023.

[13] R. Berger, B. Broadnax, M. Klooß, J. Mechler, J. Müller-Quade, A. Ottenhues und M. Raiber, „Composable Long-Term Security with Rewinding,“ *Cryptology ePrint Archive,* 2023.

Abgeschlossene und unter KIT-Open veröffentlichte Studien- und Masterarbeiten:

[6] S. H. Faller, P. Baumer, M. Klooß, A. Koch, A. Ottenhues und M. Raiber, „Black-Box Accumulation Based on Lattices,“ in *Cryptography and Coding: 18th IMA International Conference, IMACC 2021, Virtual Event, December 14–15, 2021, Proceedings 18*, 2021.

[7] S. Faller, *Oblivious Pseudo-Random Functions via Garbled Circuits,* Karlsruhe Institute of Technology (KIT): Master thesis, 2022.

[9] F. Hägele, *Estimating the Cost of Superposition Attacks on Lightweight Cryptography on Fault-Tolerant Quantum Systems,* Karlsruhe Institute of Technology (KIT): Master thesis, 2021.

[10] J. Nguyen, *Provably Quantum-secure Message Authentication Code,* Karlsruher Institut für Technologie (KIT): Master thesis, 2022.

[15] S. Eilebrecht, *Composable Definitions of Long-Term Security for Commitment Schemes and their Applications,* Karlsruhe Institute of Technology (KIT): Master thesis, 2021.

Zeitnah geplante projektbezogenen Veröffentlichungen aus KASTEL:

Im Bereich des Forschungsfeld zur Modellierung von langfristiger Sicherheit im UC-Framework plant KASTEL weiter Veröffentlichungen. Aufbauend auf dem Ergebnis von [2] wird es einen generischeren Ansatz und eine Modellierung des Updatings im Random Oracle Modell geben. Des Weiteren sind schon erweiterte Ergebnisse, welche zeitnah veröffentlicht werden, von KASTEL erforscht worden, welche auf den Masterarbeiten X und Y aufbauen. Darüber hinaus wird nach Fertigstellung die Masterarbeit „Certificate Management for PQC IIoT“ in der KIT Bibliothek veröffentlicht.

13 Literaturverzeichnis

[1] J. Müller-Quade und D. Unruh, „Long-term security and universal composability,“ in *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007*, Amsterdam, The Netherlands, 2007.

[2] T. Acar, M. Belenky, M. Bellare und D. Cash, „Cryptographic agility and its relation to circular encryption,“ in *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques* , Monaco / French Riviera, 2010.

[3] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, ... und D. Stehlé, „CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM,“ in *European Symposium on Security and Privacy*, 2018.

[4] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, ... und D. Stebila, „Frodo: Take off the ring! practical, quantum-secure key exchange from LWE,“ in *ACM SIGSAC conference on computer and communications security*, 2016.

[5] M. e. a. Chase, „The picnic signature scheme,“ in *The ePrint Archive*, 2020.

[8] S. Jarecki, H. Krawczyk und J. Xu, „OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks,“ in *Advances in Cryptology--EUROCRYPT 2018*, Tel Aviv, Israel, 2018.

[14] R. Canetti, „Universally composable security: A new paradigm for cryptographic protocols,“ in *42nd IEEE Symposium on Foundations of Computer Science*, 2001.