Anwendbarkeit quantencomputerresistenter kryptografischer Verfahren

Schlussbericht Teil II – Teilvorhaben der Technischen Universität München

Autoren:	Patrick Karl, Dr. Tim Fritzmann, Prof. Dr. Georg Sigl

Vorhabenbezeichnung:	Aquorypt
Förderkennzeichen:	16KIS1017K
Laufzeit des Vorhabens:	01. September 2019 bis 28. Februar 2023

Inhaltsverzeichnis

1. Kurzdarstellung des Projekts

Quantencomputer mit großer Rechenleistung werden in der Lage sein, alle gängigen kryptografischen Verfahren für digitale Signaturen und zum Schlüsselaustausch zu brechen. Es existieren bereits erste quantencomputerresistente kryptografische Verfahren. Diese Verfahren zählen zur Kategorie Post-Quanten-Kryptografie. Allerdings müssen die neuartigen Verfahren noch weiter optimiert werden und in die relevanten Anwendungen integriert werden, bevor leistungsstarke Quantencomputer zur Verfügung stehen und zur Gefahr für die IT-Sicherheit werden. Das Projekt Aquorypt untersucht daher die Anwendung und praktische Umsetzung von quantencomputerresistenten kryptografischen Verfahren in zwei wichtigen Bereichen, die besonders auf langfristige Sicherheit angewiesen sind: Eingebettete Systeme in der industriellen Automatisierung und Chipkarten-basierte Sicherheitsanwendungen. Eingebettete Systeme im Industriebereich haben hohe Echtzeitanforderungen und erfordern Migrationskonzepte bis in die Hardware. Mit hochsicheren Chipkarten werden außerdem Systeme analysiert, welche extreme Kostenanforderungen haben und einen geringen Stromverbrauch voraussetzen.

1.1 Aufgabenstellung

Der Fokus der Technischen Universität München in diesem Projekt liegt vor allem bei der Weiterentwicklung und Auswahl geeigneter Algorithmen, bei der effizienten Realisierung in Hardware und Software und bei der Härtung dieser Verfahren gegen Seitenkanalangriffe. Durch die Erforschung von effizienten Hardware- und Softwarelösungen sollen die Post-Quanten-Kryptografie Verfahren für die Integration in die Applikationen vorbereitet werden. Die im Projekt entwickelten Koprozessoren und Hardwarebeschleuniger sollen den Hauptprozessor bei rechenintensiven kryptografischen Aufgaben unterstützen, um die Gesamteffizienz des Systems zu steigern. Ein solcher Ansatz ist besonders wichtig für kleine Prozessoren, die ansonsten Latenz-, Durchsatz- oder Energieanforderungen nicht erfüllen könnten. Aber auch leistungsstarke Prozessoren oder Rechenzentren können von einer Beschleunigung profitieren.

1.2 Voraussetzungen unter denen das Vorhaben durchgeführt wurde

Public-Key-Kryptografie bildet die Grundlage für den Aufbau einer gesicherten Kommunikation zwischen mehreren Parteien oder Geräten. Allerdings werden Quantencomputer mit einer großen Rechenleistung in der Lage sein alle herkömmlichen kryptografischen Public-Key Verfahren wie das Rivest–Shamir–Adleman (RSA)-Kryptosystem oder Elliptische Kurven Kryptosystem (ECC) zu brechen. Diese Verfahren beruhen auf mathematischen Problemen wie der Faktorisierung von großen Zahlen und der Lösung des diskreten Logarithmus. Durch Shor's Quantenalgorithmus [Sho94] können diese Probleme in polynomialer Laufzeit gelöst werden. Erste Arbeiten entwickelten bereits quantencomputerresistente kryptografische Verfahren, welche eingesetzt werden können, um Sicherheit auch im Zeitalter von leistungsstarken Quantencomputern gewährleisten zu können. Diese Algorithmen sind nicht durch bekannte Quantenalgorithmen, wie Shor's oder auch Grover's Algorithmus [Gro96], gefährdet. Die Integration dieser Verfahren in den verschiedenen Industrieapplikationen und Alltagsgegenständen, ist allerdings noch weitestgehend unerforscht. Um eine langfristige Sicherheit gewährleisten zu können, müssen bereits jetzt Migrationskonzepte und Strategien zur Realisierung von Post-Quanten-Kryptografie erstellt werden.
Insbesondere eingebettete Systeme in der industriellen Automatisierung und im Chipkarten-Bereich erfordern eine langfristige Sicherheit und kryptografische Realisierungen, welche auch gegen Angriffe ausgehend von Quantencomputern resistent sind. Die Optimierungsziele für industrielle Anlagen und Chipkarten sind dabei durchaus verschieden. Anlagen im Industriebereich benötigen oftmals eine hohe Performanz und benötigen ein hohes Maß an Flexibilität. Chipkarten haben besonders hohe Sicherheitsanforderungen und müssen gegen zahlreiche Angriffe geschützt werden. Außerdem stehen im Chipkartenbereich nur eine geringe Anzahl an Ressourcen zur Verfügung. Post-Quanten-Kryptografie in solche Geräte zu integrieren ist deshalb besonders herausfordernd.
Unabhängig von der Entwicklung von quantencomputerresistenten Verfahren hat die Forschung und Industrie erkannt, dass Entwicklung von frei verfügbaren Prozessoren immer wichtiger für kryptografische Anwendungen wird. Der Open-Source Charakter fördert die Entwicklung und Forschung von effizienten Gesamtsystemen. Besonders Prozessoren im Bereich der Kryptografie benötigen tiefe Kenntnisse der Architektur, um möglichst viele Sicherheitslücken schließen zu können. RISC-V, eine offene Befehlssatzarchitektur, ist dabei eine der vielversprechendsten Open-Source Initiativen. Die RISC-V-Initiative wurde 2010 von der University of California, Berkley gestartet und ist mittlerweile zu einer großen Non-Profit-Organisation herangewachsen. Die RISC-V Befehlssatzarchitektur basiert auf den Konzepten des Reduced Instruction Set Computer (RISC). Unzählige RISC-V Projekte sind in den letzten Jahren gestartet und werden bereits in die ersten Anwendungen gebracht. RISC-V ist besonders relevant für eingebettete Systeme und äußerst gut geeignet für die Entwicklung von Post-Quanten-Kryptografie Prozessoren.

1.3 Planung und Ablauf des Vorhabens

Das Verbundprojekt Aquorypt wurde von seinen Partnern ursprünglich auf drei Jahre geplant. Die Arbeiten waren dabei auf die sieben Teilprojekte aufgeteilt:

- AP1: Bewertung und Auswahl existierender quantencomputerresistenter Verfahren,
- AP2: Anpassung und Weiterentwicklung quantencomputerresistenter Verfahren,
- AP3: Hardware-Beschleuniger,
- AP4: Implementierung in Hard- und Software,
- AP5: Sicherheitsuntersuchungen und Angriffsresilienz,
- AP6: „Krypto-Agilität“ und Migrationspfade,
- AP7: Koordination und Steuerung.

Im Arbeitspaket 6 „Krypto-Agilität“ und Migrationspfade hat sich die Technische Universität nicht beteiligt.

1.4 Wissenschaftlicher und technischer Stand zu Beginn des Vorhabens

Das US-amerikanische „National Institute for Standards and Technology“ (NIST) hat einen Standardisierungsprozess in Gang gesetzt [Nat16], zu dem bis November 2017 Post-Quanten-Kryptografie Verfahren eingereicht werden konnten. Das Ziel dieses Prozesses besteht darin, mindestens ein Public-Key-Verschlüsselungsverfahren und ein Signaturverfahren zu standardisieren. Während für die erste Runde des Standardisierungswettbewerbs 69 Algorithmen ausgewählt wurden, blieben in der zweiten Runde noch 26 Einreichungen übrig. Im Juli 2020 wurde die dritte Runde dieses Wettbewerbs ausgeschrieben [AASA$^+$20]. Die verbleibenden Post-Quanten-Kryptografie Kandidaten wurden in zwei Kategorien eingeteilt: (i) Finalist, die Verschlüsselungs- und Signaturverfahren, welche teilweise für eine NIST-Standardisierung im Jahr 2022/2023 vorgesehen sind; und (ii) Ersatzkandidaten, die von NIST als vielversprechende Lösungen angesehen werden, aber noch eine Weiterentwicklung für eine mögliche zukünftige Standardisierung erfordern. Für die Kategorie Verschlüsselungsverfahren wurden vier Finalisten und fünf Ersatzkandidaten ausgewählt. Für die Kategorie Signaturen wurden drei Finalisten und drei Ersatzkandidaten ausgewählt. Trotz der erheblichen Fortschritte in der Entwicklung dieser Algorithmen ist die Forschung in diesem Bereich noch längst nicht abgeschlossen.

Neben dem NIST Standardisierungswettbewerb startete im Jahr 2018 auch die "Chinese Association for Cryptologic Research“ (CACR) einen eigenen Standardisierungsprozess. Dieser verfolgt eine ähnliche Zielsetzung wie der NIST Standardisierungswettbewerb [otPRC16].
Erste Arbeiten haben sich bereits mit der Implementierung von quantencomputerresistenter Kryptografie in eingebetteten Systemen beschäftigt. Die Autoren in [KRSS] haben zum Beispiel mehrere Verfahren auf einen beliebten ARM Mikrocontroller realisiert. In einer weiteren Arbeit wurde eine Implementierung vorgestellt, welche mit Hilfe eines RSA Koprozessors Post-Quanten-Kryptografie beschleunigt [AHH+19]. Erste Hardware-Implementierungen für Post-Quanten-Kryptografie wurden bereits für bekannte kryptografische Verfahren entwickelt. Beispielsweise wurden Hardwarebeschleuniger für das Kryptosystem NTRU und NewHope entwickelt [BFM+18, OG17]. Auch die RISC-V Security Arbeitsgruppe hat die Notwendigkeit einer Hardwarebeschleunigung für kryptografische Verfahren erkannt. Sie beabsichtigt Befehlssatzerweiterungen für alle gängigen symmetrischen und asymmetrischen kryptografischen Algorithmen zu entwickeln [OM20]. Neuere Arbeiten konzentrierten sich bereits auf kleine Befehlssatzerweiterungen für die weit verbreiteten symmetrischen Kryptosysteme AES [MNP+20] und ChaCha [MPP21]. Nicht nur traditionelle Kryptografie, sondern auch neuartige Kryptografie, wie Post-Quanten-Kryptografie, wird von der RISC-V Organisation berücksichtigt. Offizielle Lösungsansätze sind zum jetzigen Zeitpunkt allerdings noch nicht bekannt. Ein weiterer Schwerpunkt der RISC-V Security Arbeitsgruppe ist es, Lösungen zur Verhinderung von Mikroarchitekturangriffen auf Prozessor- und Befehlssatzebene zu finden [GGM+20, MPW21]. Um sicherheitsbezogene Mikroarchitekturprobleme anzugehen, wurden mehrere Initiativen für sichere RISC-V-Enklaven gestartet, z. B. Sanctum (Massachusetts Institute of Technology, Keystone und University of California, Berkeley), OpenTitan (Google), MultiZone (HexFive).

1.5 Bekannte Konstruktionen, Verfahren und Schutzrechte

Die Arbeiten in diesem Projekt verwenden kryptografische Algorithmen, welche im Rahmen des NIST Standardisierungsprozesses publiziert werden. Dabei wurden auch auf frei verfügbare Referenzimplementierungen und die dazugehörigen Spezifikationen der Post-Quanten-Kryptografie Verfahren zurückgegriffen. Diese wurden von NIST der Öffentlichkeit zur Verfügung gestellt [Nat].
Es ist davon auszugehen, dass es durch die verstärkten Forschungstätigkeiten und Standardisierungsinitiativen zu quantencomputersicherer Kryptografie zukünftig zur Anmeldung einer Vielzahl neuer Patente kommen wird. Wie im Falle von klassischer Kryptografie verschaffen dabei vor allem Verfahren zu effizienten und sicheren Implementierungen in Hard- und Software, als auch Techniken zur Reduktion von Schlüssel-, Signatur- und Geheimtextgrößen, einen entscheidenden Wettbewerbsvorteil. Es wurden zahlreiche

Patente in den letzten Jahren angemeldet, welche mit Post-Quanten-Kryptografie zusammenhängen. Die folgenden zwei Patente könnten allerdings einen besonders großen Einfluss auf Finalisten des Standardisierungsprozesses der NIST haben:

- Jintai Ding, „Cryptographic systems using pairing with errors“, US9246675B2.
- Kevin Yeo, Asra Ali, Tancrede Lepoint, Sarvar Patel, „Compression and oblivious expansion of RLWE ciphertexts“, WO2020226695A1.

Diese könnten möglicherweise auch einen Einfluss auf die kryptografischen Verfahren, welche in diesem Projekt betrachtet wurden, haben. In der allgemeinen Forschungsgemeinschaft werden diese Fälle aktuell genauer analysiert. Es ist derzeit noch unklar, ob diese Patente auf die NIST Kandidaten zutreffen oder nicht.

Bekanntmachung im Verlauf der Projekts. Um möglichen Lizenzproblemen vorzugreifen, hat die NIST eine Lizenzvereinbarung mit den entsprechenden Patentinhabern vereinbart, welche es erlauben, die zur Standardisierung ausgewählten Verfahren lizenzgebührenfrei entsprechend der standardisierten Spezifikation zu nutzen. Die Lizenzvereinbarung enthält folgende Patente:

- U.S. Pat. No. 9246675
- EP App. No. 11712927
- EP Pat. No. 2537284
- French Pat. App. No. 1051190
- French Pat. No. 2956541
- PCT App. No. PCT/FR2011/050336
- U.S. Pat. App. No. 13/579682
- U.S. Pat. No. 9094189

1.6 Fachliteratur und benutzte Informations- und Dokumentationsdienste

Ein Auszug der verwendeten Literatur ist diesem Dokument und ebenso den im Rahmen des Projekts entstandenen Veröffentlichungen beigefügt. Dabei wurden überwiegend Datenbanken der Forschungsverlage IEEE Xplore Digital Library, ACM Digital Library, Springer Link verwendet. Zusätzlich wurden diese durch freie Datenbanken, wie Cryptology ePrint Archive oder arXiv ergänzt.

1.7 Zusammenarbeit mit anderen Stellen

Im Projekt Aquorypt gab es über die gesamte Laufzeit eine intensive Zusammenarbeit der Partner. Die Technische Universität München hat hierbei regelmäßig an Telefonkonferenzen sowie Treffen der Partner teilgenommen. Die Ergebnisse wurden bereits während des Projekts in mehreren Konferenzen vorgestellt. Dabei wurden auch Veranstaltungen organisiert, um mit anderen Projekten zu diskutieren. Ein Beispiel war die Veranstaltung „Quo Vadis: Post-Quanten-Kryptografie?“ [Fra]. Bei dieser Veranstaltung haben insgesamt 70 Teilnehmer aus verschiedenen Sparten der Industrie und Wissenschaft teilgenommen. Ein starker wissenschaftlicher Austausch hat mit allen Projektpartnern stattgefunden. Insbesondere mit Infineon Technologies AG sind gemeinsame Masterarbeiten entstanden. Des Weiteren wurden gemeinsame Publikationen eingereicht.
Durch die enge Zusammenarbeit sind auch weitere Folgeprojekte entstanden. Ein Beispiel ist das Projekt PoQsiKom, bei welchen unter anderem wieder mit Siemens AG und dem Fraunhofer AISEC zusammengearbeitet wird.

2. Eingehende Darstellung

2.1 Erzielte Ergebnisse

Die erzielten Ergebnisse lassen sich in hauptsächlich vier Bereiche unterteilen: (a) Vorbereitungen, Auswahl und Analyse von Post-Quanten-Kryptografie Verfahren, (b) Betrachtung der Post-Quanten-Kryptografie Verfahren auf algorithmischer Ebene und Parametersatzoptimierungen, (c) Entwicklung von Hardware-Beschleunigern für Post-Quanten-Kryptografie und Integration der Beschleuniger in das Gesamtsystem, (d) Entwicklung von Seitenkanalgegenmaßnahmen, um die praktische Sicherheit des Gesamtdesigns zu erhöhen. Die Ergebnisse im Punkt (a) können hauptsächlich dem Arbeitspaket AP1 zugeordnet werden. Punkt (b) ist dem Arbeitspacket AP2 zuzuornden. Punkt (c) ist AP3 und AP4 zuzuordnen. Punkt (d) ist hauptsächlich AP5 zuzuordnen.

a. Bewertung und Auswahl der Post-Quanten-Kryptografie Verfahren

Post-Quanten-Kryptografie kann in gitterbasierte Kryptografie, codebasierte Kryptografie, hashbasierte Kryptografie, multivariate Kryptografie, und isogeniebasierte Kryptografie unterteilt werden. Nicht alle dieser Kategorien eignen sich gleichermaßen für die Implementierung von Verschlüsselungs- und Signaturverfahren in eigebetteten Geräten.

Auswahl der Kategorien. Eine erste Analyse hat ergeben, dass sich insbesondere gitterbasierte Kryptografie gut für ressourcenbeschränkte Geräte eignet. Die besonders hohe Flexibilität dieser Kategorie spiegelt sich auch im NIST Post-Quanten-Standardisierungsprozess wider. Unter den sieben Finalisten der dritten Runde, sind fünf Algorithmen (drei Verschlüsselungs- und zwei Signaturalgorithmen) der Kategorie gitterbasierte Kryptografie zuzuordnen. Gitterbasierte Kryptografie zeichnet sich durch eine gute Performanz und durch relative geringe Schlüssel- und Geheimtextgrößen aus. Codebasierte Kryptografie wiederum beruht teilweise auf sehr gut erforschten Verfahren, welche trotz großer Anstrengung nie wirklich gebrochen wurden. Ähnlich wie bei multivariater und hashbasierter Kryptografie eignet sich diese Klasse allerdings nur in speziellen Fällen für kleine ressourcenbeschränkte Geräte. Die äußerst großen Schlüsselgrößen sind oftmals ein Hindernis für die Einsetzbarkeit solcher Verfahren. Isogeniebasierte Kryptografie hat im Vergleich zu den anderen Verfahren die geringste Schlüssel- und Geheimtextgröße. Deshalb ist diese Kategorie interessant für eingebettete Geräte. Allerdings ist isogeniebasierte Kryptografie besonders langsam und erfordert

für einige Anwendungen eine extreme Beschleunigung. Die Technische Universität München hat sich nach dieser Analyse in diesem Projekt vor allem auf gitterbasierte und isogeniebasierte Kryptografie beschränkt.

Analyse einzelner Verfahren. Für eine erste Untersuchung der Performanz wurden vier gitterbasierte Verschlüsselungsalgorithmen auf den mittelmäßig leistungsstarken AURIX Mikrocontroller von der Infineon Technologies AG implementiert. Dieser Mikrocontroller ist für höchste Sicherheitsanforderungen ausgelegt und ist durch seine Architektur zum Beispiel auch für besonders kritische Operationen im Automobilbereich anwendbar. Die Untersuchungen umfassten die drei NIST-Post-Quanten-Kryptografie Finalisten Kyber, NTRU und Saber. Des Weiteren wurde der Algorithmus ThreeBears betrachtet. Obwohl ThreeBears nicht als Finalist eingestuft wurde, empfahl NIST weitere Untersuchungen in dieser Richtung aufgrund interessanter Sicherheits- und Leistungsmerkmale [AASA+20]. Unsere Analyse hat gezeigt, dass alle diese Algorithmen auf dem AURIX Mikrocontroller implementiert werden können. Unter den Finalisten lieferten besonders Kyber und Saber ein sehr gutes Ergebnis. Bei einer Frequenz von 300 MHz benötigt Kyber für den kleinsten Parametersatz nur 8.18 ms. NTRU ist aufgrund der aufwändigeren Schlüsselgenerierung langsamer als die Konkurrenten.
Die Ergebnisse dieser Analyse wurden in der Fachzeitschrift Microprocessors and Microsystems (MICPRO) von Elsevier publiziert [FVFS21].

Bekanntmachung im Verlauf der Projekts. Im Laufe des Projekts hat die NIST Kyber als Post-Quanten sicheres Schlüsselaustauschverfahren, sowie Dilithium, Falcon und SPHINCS+ für Post-Quanten sichere digitale Signaturen zur Standardisierung ausgewählt [Moo22].

b. Analyse der Parameterwahl von Post-Quanten-Kryptografie Verfahren

Die Fehlerrate, das Sicherheitslevel und Schlüssel/Geheimtextgröße von Post-Quanten-Kryptografie hängt von den gewählten Parametersatz der Algorithmen ab. Gitterbasierte Kryptografie enthält einen gewissen Fehlerterm, welcher in seltenen Fällen zu falschen Ergebnissen führt. Wird die Varianz (die Amplitude) dieses Fehlerterms erhöht, steigt allerdings das Sicherheitslevel des Systems. Die Erhöhung der Varianz führt zu einer Erhöhung der Verschiebung der Gitterpunkte und somit zu einen erhöhten Komplexität zur Lösung des kryptografischen Verfahrens. Eine Analyse ist daher notwendig, um eine geeignete Balance zwischen Fehlerrate und Sicherheitslevel zu finden.

Optimierung ThreeBears Algorithmus. Um die Fehlerrate eines gitterbasierten Algorithmus zu reduzieren aber gleichzeitig ein hohes Sicherheitslevel zu erreichen, können Fehlerkorrekturcodes eingesetzt werden. Das Post-Quanten-Kryptografie Verfahren ThreeBears enthält einen Fehlerkorrekturcode, welcher in der Lage ist, bis zu zwei

Bit-Fehler zu korrigieren. Unsere Analyse hat gezeigt, dass ein stärkerer Fehlerkorrekturcode, welcher bis zu sechs Bit-Fehler korrigieren kann, die Fehlerrate von 2^{-135} zu 2^{-153} reduzieren kann. Alternativ kann eine Erhöhung des Bit-Sicherheitslevels von 141 zu 144 erreicht werden. Das bedeutet, dass ein mathematischer Angriff auf das ThreeBears Kryptosystem acht Mal schwerer ist als zuvor. Der stärkere Fehlerkorrekturcode hat nur eine minimale Auswirkung auf die Gesamtausführungszeit. Um das System gegen Seitenkanalangriffe zu schützen, wurden zudem Sicherheitsmechanismen entworfen. Das beinhaltet eine konstante Ausführungszeit für den Fehlerkorrekturcode. Somit wird verhindert, dass ein Angreifer mit Hilfe der Ausführungszeit Informationen über geheime Elemente erlangen kann.
Die Ergebnisse dieser Analyse wurden auf der IEEE Konferenz „Euromicro Conference on Digital System Design (DSD)“ vorgestellt [FVS20].

c. Hardwarebeschleuniger und Hardware/Software Co-Design

Die Integration von Post-Quanten-Kryptografie in elektronische Geräte ist eine anspruchsvolle Aufgabe. Post-Quanten-Kryptografie beruht auf neuen mathematischen Elementen, die auf Standardprozessoren meist nicht einfach zu realisieren sind. Speziell für kostengünstige und ressourcenbeschränkte Geräte, ist eine Hardwarebeschleunigung normalerweise erforderlich. Da der Standardisierungsprozess von Post-Quanten-Kryptografie noch nicht abgeschlossen ist, wird außerdem ein starker Fokus auf Flexibilität gelegt. Aber auch unabhängig von der Standardisierung, ist eine gewisse Flexibilität wichtig, um Produkte anpassungsfähig und agil zu halten. Um solchen Anforderungen gerecht zu werden, können Hardware/Software Co-Design Techniken für die Entwicklung komplexer und hochgradig kundenspezifischer Produkte verwendet werden. In diesem Zusammenhang wurden im Projekt Aquorypt Hardwarebeschleuniger und Systemlösungen für insgesamt vier gitterbasierte Verfahren (LAC, NewHope, Kyber, Saber) und ein isogenibasiertes Verfahren (SIKE) erforscht. Als Zielplattform wurde ein 32-Bit Mikroprozessor basierend auf einer RISC-V Architektur ausgewählt.

Designstrategie. Aufgrund des Open-Source Charakters hat RISC-V eine neue Ära in der Entwicklung von effizienten Koprozessoren eingeleitet. Durch die offene RISC-V Architektur ergeben sich neue Designmethoden, welche vorher nur wenige Chiphersteller verfolgen konnten. Da der gewählte Prozessor offen zur Verfügung steht, können Änderungen im Prozessorkern vorgenommen werden. Tiefe Einblicke in das System erlauben es, ein optimiertes Zusammenspiel zwischen Hauptprozessor und Koprozessor zu entwickeln. Darüber hinaus bietet RISC-V die Flexibilität, Befehlssatzerweiterungen vorzunehmen und anwendungsspezifische Hardwarebeschleuniger direkt in den Hauptprozessor zu integrieren. Solche Designansätze können kaum angewendet werden, wenn der Befehlssatz oder die Prozessorarchitektur nicht offen verfügbar sind. Anwendungen im Bereich Künstliche Intelligenz (KI) und Kryptografie profitieren besonders von maßgeschneiderter Hardwarebeschleunigung, da beide Bereiche rechenintensive Operationen beinhalten. Open-Source Initiativen wie RISC-V erlauben es Sicherheitslücken

zu identifizieren und zu schließen, da detaillierte Kenntnisse über die Mikroarchitektur und den Datenfluss des Prozessors offen verfügbar sind. Die Entwicklung sicherer Prozessoren und anwendungsspezifischer Beschleuniger wird aufgrund steigender Sicherheitsanforderungen und der zunehmenden Konnektivität zwischen Geräten immer wichtiger.
Im Projekt Aquorypt hat die Technische Universität München einen RISC-V basierten Mikrocontroller erweitert, um effizient und sicher Post-Quanten-Kryptografie umzusetzen. Das Grunddesign des verwendeten RISC-V Mikrocontrollers basiert auf der PULPino Plattform, welcher von den Designern frei zur Verfügung gestellt wurde [TZS+16]. Dieser Mikrocontroller wurde für eingebettete System entworfen, welche eine geringe Verlustleistung erfordern. Abbildung 2.1 zeigt die Mikroarchitektur des mit Post-Quanten-Kryptografie erweiterten RISC-V Prozessors. Die Hauptkomponenten des Prozessorkerns sind: ein Prefetch Buffer zum Speichern und Verarbeiten der Befehle, ein Befehlfsdecoder (Decode), zwei Registerbänke (GPR und FPR), eine Arithmetisch-logische Einheit (ALU), eine Multipliziereinheit (MULT) und eine Load/Store Einheit (LSU). Der Mikrocontroller enthält zudem mehrere Peripherieelemente: Universal Asynchronous Receiver / Transmitter (UART), Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I2C) und General Purpose Input/Output (GPIO). Der Prozessor wurde im Projekt um mehrere Koprozessoren und Beschleuniger erweitert. Diese Elemente sind mit PQ1–PQ3 gekennzeichnet.

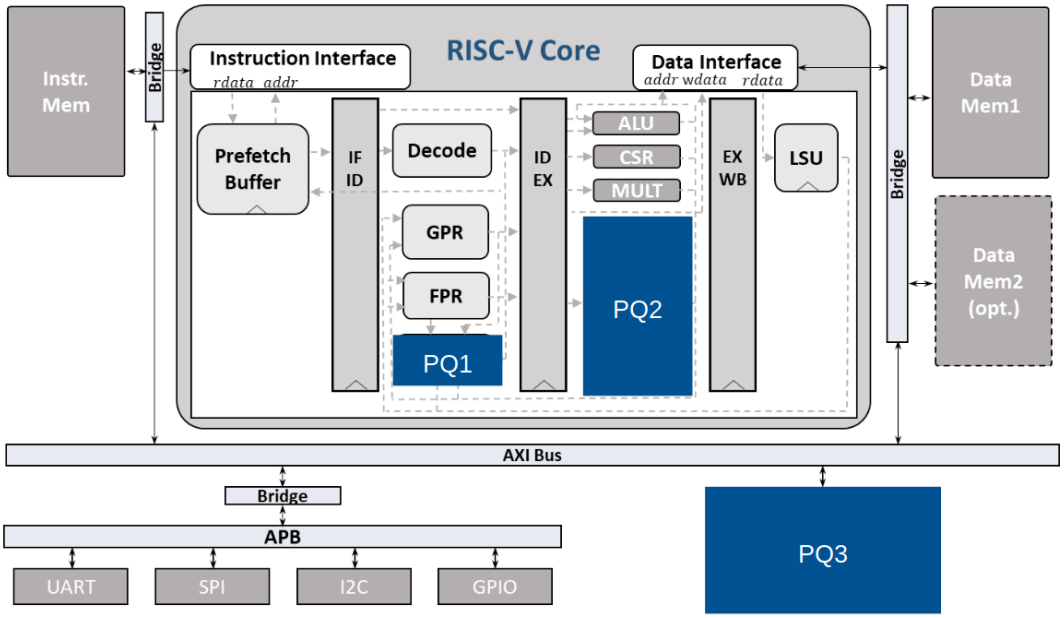

Abbildung 2.1: RISC-V Plattform mit Integration von Post-Quante-Kryptografie Beschleunigern

Kryptografiebeschleuniger können grundsätzlich in drei Kategorien eingeteilt werden:

- Hardwarelösungen für das komplette Kryptosystem. Diese sind oftmals sehr performant, haben allerdings eine schlechte Flexibilität und einen hohen Flächen-

verbrauch. Oft sind die extrem hohen Beschleunigungen, welcher dieser Ansatz bietet, gar nicht notwendig.

- Lose gekoppelte Beschleuniger (PQ3) werden durch einen Systembus, z.B. Advanced eXtensible Interface Bus (AXI), and den Hauptprozessor angebunden. Sie haben eine etwas höhere Flexibilität, da nur Teile in Hardware beschleunigt werden können. Die Kontrolllogik des Beschleunigers kann in Software umgesetzt werden.

- Eng gekoppelte Beschleuniger (PQ1/PQ2), welche direkt im Prozessorkern integriert sind. Diese benötigen tiefe Eingriffe in die Prozessorarchitektur. Sie können allerdings zu einer sehr hohen Flexibilität führen. Üblicherweise sind eng gekoppelte Beschleuniger in der Execute Stage integriert (PQ2). Um eine engere Bindung zu den Registerbänken zu realisieren, können diese aber auch in der Decode Stage instanziiert werden (PQ1).

Die Ergebnisse in diesem Projekt haben gezeigt, dass eng gekoppelte Beschleuniger sich besonders gut für Post-Quanten-Kryptografie Applikationen eignen. Diese zeichnen sich durch einen geringen Flächenverbrauch aus, da Systemressourcen effizient wiederverwendet werden können. In den folgenden Absätzen erfolgt eine genauere Analyse anhand von mehreren Beispielen, welche im Projekt von der Technischen Universität München untersucht wurden.

Hardware/Software Co-Design für LAC. LAC ist ein gitterbasiertes Public-Key-Verschlüsselungsverfahren, welches resistent gegen traditionelle und Quantenangriffe ist. Es zeichnet sich insbesondere durch kleine Schlüsselgrößen aus, da es einen Leistungsstarken Fehlerkorrekturcode verwendet. Im Projekt Aquorypt wurde ein effizientes und flexibles Hardware/Software Co-Design für LAC erforscht. Die ersten Messergebnisse haben gezeigt, dass die folgenden Operationen des Algorithmus rechenintensiv sind: die Erzeugung von zufälligen Ring-Polynomen, die Polynommultiplikation und die Fehlerkorrektur. Für diese Operationen wurden Hardwarebeschleuniger entwickelt. Zur Erzeugung von zufälligen Ring-Polynomen wurde ein Pseudo-Zufallszahlengenerator entworfen. Für die Beschleunigung der Polynommultiplikation hat sich herausgestellt, dass ein Design basierend auf einem Schieberegisteransatz besonders effizient für dieses Post-Quanten-Kryptografie Verfahren ist. Um den Flächenverbrauch der Beschleuniger gering zu halten, wurden algorithmische Maßnahmen erforscht, welche die großen Polynome in kleinere Subpolynome aufteilt. Letztendlich wurden maßgeschneiderte Beschleuniger für den Fehlerkorrekturcode von LAC entwickelt. Die Beschleuniger wurden anschließend in den RISC-V Prozessor integriert. Die Ergebnisse haben gezeigt, dass die vorgestellte Architektur die Laufzeit von LAC um einen Faktor von bis zu $14{,}42$ verbessert. Das Design, welches für ein Field Programmable Gate Array (FPGA) evaluiert wurde, erhöht den Ressourcenverbrauch um $32\,617$ LUTs (kombinatorische Logik), $11\,019$ Register und zwei DSP-Slices (Logik für Multiplizierer).

Die Ergebnisse wurden auf der „Design, Automation & Test in Europe Conference & Exhibition (DATE)“ vorgestellt [FSS20a].

Hardware/Software Co-Design für NewHope, Kyber und Saber. Für die Post-Quanten-Kryptografie Verfahren NewHope, Kyber und Saber wurden im Projekt mehrere leistungsstarke eng gekoppelte Beschleuniger erforscht. Auch diese Verfahren gehören zur Kategorie gitterbasierte Kryptografie. Die rechenintensiven Operationen sind ähnlich wie in LAC. Allerdings führten kleinere algorithmische Abweichungen, zu sehr großen Unterschieden im Gesamtdesign. Während LAC effizient mit einem Schieberegisteransatz beschleunigt wurde, verwenden beispielsweise NewHope und Kyber eine Transformation, um die Polynommultiplikation effizient zu realisieren. Diese Transformation, die Number Theoretic Transform (NTT), ähnelt der Fast Fourier Transform (FFT), welche in der Signalverarbeitung bekannt ist. Durch eine NTT Hardwarearchitektur können Polynome mit einer Komplexität von $\mathcal{O}(n \cdot log_2(n))$ multipliziert werden, während ein normaler Ansatz eine Komplexität von $\mathcal{O}(n^2)$ aufweist. Das kann zu einer erheblichen Beschleunigung für große Polynome führen. Die Forschungsergebnisse der Technischen Universität München haben gezeigt, dass sich die Hauptoperationen dieser Transformation gut für eine enge Prozessorkopplung eignen. Außerdem wurden Strategien entwickelt, um langsame Speicherzugriffe zu reduzieren. Für Saber ist die NTT aufgrund der Wahl des Parametersatzes nicht direkt anwendbar. Deswegen wurde für Saber ein eigener Beschleuniger entwickelt.
Um die Hardwarebeschleuniger anzusteuern, wurde der RISC-V Befehlssatz um 29 neue Instruktionen für gitterbasierte Kryptografie erweitert. Das finale Design wurde auf einem FPGA-Prototyp implementiert. Des Weiteren wurden Entwicklungen vorgenommen, um das Design zu einer anwendungsspezifischen integrierten Schaltung (ASIC) zu migrieren. Im Vergleich zu reinen Softwareimplementierungen auf RISC-V haben unsere Hardware/Software Co-Design Implementierungen einen Beschleunigungsfaktor von bis zu $11{,}4$ für NewHope, $9{,}6$ für Kyber und $2{,}7$ für Saber. Für das ASIC Design wurde der Energieverbrauch um Faktoren von bis zu $9{,}5$ für NewHope, $7{,}7$ für Kyber und $2{,}1$ für Saber reduziert. Die Zellenzahl (Anzahl der Logik-Gatter) des Prozessors erhöhte sich um den Faktor $1{,}6$ gegenüber dem ursprünglichen RISC-V-Design. Unter Berücksichtigung der erzielten Ergebnisse kann der erhöhte Ressourcenverbrauch als moderat angesehen werden.
Die Forschungserkenntnisse und Ergebnisse wurden auf der „IACR Transactions on Cryptographic Hardware and Embedded Systems“ vorgestellt [FSS20b].

SIKE. Das Post-Quanten-Kryptgrafie Verfahren Isogeny Key-Encapsulation (SIKE) hat durch die geringen Schlüssel- und Geheimtextgrößen viel Aufmerksamkeit auf sich gezogen. Allerdings beruht dieses Verfahren auf besonders rechenintensiver Arithmetik. Bestehende Implementierungen von SIKE konzentrieren sich entweder auf dedizierte Beschleuniger für FPGAs oder auf Softwareimplementierungen für ARM Mikrocontroller. Obwohl reine Hardwarebeschleuniger der vorherigen Arbeiten eine hohe Performanz

mit sich bringen, haben diese Ansätze den Nachteil eines großen Flächenverbrauchs und einer geringen Flexibilität. Auf der anderen Seite haben reine Softwareimplementierungen zwar eine hohe Flexibilität aber eine geringe Performanz. Deshalb wurden Hardware/Software Co-Design Methoden für SIKE analysiert. Um den Hauptprozessor bei der Berechnung von den rechenintensiven Finite-Field Operationen zu entlasten, wurden Hardwarebeschleuniger entworfen. Die Beschleunigung auf Systemebene wurde anschließend für zwei Mikrocontroller-Plattformen basierend auf ARM und RISC-V evaluiert. Das Ergebnis zeigt, dass unsere ARM Cortex-A9 Implementierung mit lose gekoppelten Finite-Field Beschleuniger verglichen mit reinen Softwareimplementierungen eine erhebliche Beschleunigung mit sich bringt. Um die aufwändige Buskommunikation zu verringern, wurde der Finite-Field-Beschleuniger außerdem direkt in einem RISC-V Prozessor integriert. Das vorgeschlagene Design erfordert $65\,500$ kilo Taktzyklen zum Ausführen von SIKEp434 auf einem ARM Cortex-A9 mit Finite-Field Beschleuniger. Durch die enge Prozessorkopplung mit dem RISC-V Core reduzierte sich die Zyklenanzahl sogar auf $36\,900$ kilo Taktzyklen.
Die Ergebnisse aus dieser Analyse wurden auf der „IEEE/ACM International Conference On Computer Aided Design (ICCAD)“ vorgestellt [RFS20]. Weitere Veröffentlichungen in diesem Bereich sind noch geplant [OFP$^+$].
Im Juli 2022 wurde ein Angriff auf das SIDH Verfahren bekannt auf welchem SIKE basiert [CD22]. Daher kann SIKE zukünftig nicht mehr als sichere Option für Post-Quanten Kryptografie betrachtet werden.

FrodoKEM: Das Post-Quanten-Kryptografie Verfahren FrodoKEM beruht auf besonders konservativen Sicherheitsannahmen, wodurch es besonders viel Vertrauen in die Sicherheit weckt. Andererseits entsteht durch den konservativen Designansatz ein hoher Rechenaufwand, weshalb Hardwarebeschleunigung hier essentiel für die praktikabilität ist. Durch die Integration von eng gekoppelten Hardwarebeschleunigern der intensivsten Rechenoperationen kann daher die Anzahl der Taktzyklen um einen Faktor von 7 bis 8 reduziert werden, bei einem relativ geringem Kostenfaktor von $1{,}4$.
Die Ergebnisse wurden auf dem "25th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)"präsentiert [KFS21].

Realisierung eines ASICs in 22nm Technologie Verschiedene Hardwarebeschleuniger unterschiedlicher Kategorien (gitter- und isogeniebasiert) wurden im Laufe des Projekts entwickelt und in eine RISC-V Platform integriert. Das entstandene Design beinhaltet verschiedene eng gekoppelte Hardwarebeschleuniger für die gitterbasierten Verfahren SABER und Kyber. Um die Performanz weiter zu verbessern wurden lose gekoppelte Beschleuniger für das isogeniebasierte Verfahren SIKE integriert. Zudem wurde ein lose gekoppelter Hardwarebeschleuniger für das codebasierte Verfahren HQC integriert, welcher im Rahmen des Projekts SIKRIN-KRYPTOV von der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau entwickelt wurde. Diese Platform wurde schließlich in einer 22nm Technologie von Globalfoundries gefertigt

weist eine Fläche von $2{,}5mm \times 1{,}25mm$ auf. Die Anzahl der Taktzyklen reduziert sich durch die Hardwarebeschleunigung abhängig vom ausgewählten Algorithmus und Sicherheitslevel um einen Faktor von bis zu 12, während sich gleichzeitig auch der Energieverbrauch um einen Faktor von 7 bis 13 abhängig von Algorithmus und Sicherheitslevel reduziert. Tests haben ergeben, dass die gefertigten Chips mit einer Frequenz von bis zu 500MHz korrekt funktionieren und alle ausgewählten Post-Quanten Verfahren wie gewünscht beschleunigen. Zudem wurde der gefertigte Chip im Rahmen des Projekts SIKRIN-KRYPTOV verwertet indem eine Sicherheitsanalyse des HQC Hardwarebeschleunigers durchgeführt wurde.
Der entstandene ASIC wurde auf dem Workshop "Topics in hArdware SEcurity and RISC-V (TASER)"(Leuven, 18. September 2022) vorgestellt[1].

Integration der Forschungserkenntnisse in einen Demonstrator Die konzeptionelle Anwendung der im Projekt gesammelten Ergebnisse wurde in Form eines Demonstrators im Industrie 4.0 Kontext umgesetzt. Hierfür wurde eine Post-Quanten sichere TLS1.3 Verbindung mittels der Softwarebibliothek WolfSSL zwischen einem Host-PC und einem symbolischen Industriegerät aufgebaut. Dieses Industriegerät bestand aus einem Roboterarm welcher mit einem Steuergerät auf FPGA-basis verbunden ist. Als Post-Quantum sicheres Schlüsselaustauschverfahren wurde Kyber gewählt. Auf der Seite des Host-PCs wurden alle Operationen von Kyber auf einer zu Demonstrationszwecken vom Projektpartner Infineon zur Verfügung gestellten Smartcard ausgeführt. Auf Seiten des Industriesteuergeräts wurden alle entsprechenden quantensicheren Operationen auf dem im Projekt gefertigten ASIC ausgeführt. Dadurch werden alle sicherheitskritischen Funktionen zum Schlüsselaustausch auf dedizierten Sicherheitskomponenten gekapselt. Nach erfolgtem Schlüsselaustausch können klassische, symmetrische Algorithmen wie AES mit entsprechender Schlüssellänge verwendet werden, um eine sichere Kommunikation zwischen Host-PC und Industriegerät zu gewährleisten.

d. Seitenkanaluntersuchungen und Beschleuniger

Auch wenn kryptografische Verfahren mathematisch sicher sind, können Seitenkanalangriffe deren Implementierung angreifen. Das führt zu einem großen Problem in der angewandten Kryptografie. Während die Kryptoanalyse und Sicherheitsbewertung von Post-Quanten-Kryptografie bereits relativ weit fortgeschritten ist, ist ein zunehmender Forschungsaufwand in der Absicherung von kryptografischen Implementierungen notwendig. Seitenkanalangriffe gewinnen aus physikalischen Größen wie dem Stromverbrauch oder der Ausführungszeit Informationen, um Rückschlüsse auf Geheimnisse ziehen zu können.

Absicherung von Kyber und Saber gegen Seitenkanalattacken. Im Projekt hat die Technische Universität München kritische Operationen untersucht, welche an-

[1] https://homes.esat.kuleuven.be/ bgierlic/taser/taser.html

fällig für Seitenkanalangriffe sind. Diese Operationen wurden anschließend gehärtet. Zum Einsatz kam eine bekannte und effiziente Gegenmaßnahme, welche sich Maskierung nennt [CJRR99]. Diese Methode versucht durch Randomisierung die Korrelation zwischen der Verlustleistung und den zu verarbeitenden Daten zu brechen. Im Projekt Aquorypt wurden maskierte Hardware/Software Co-Designs für die NIST Post-Quanten-Kryptografie Finalisten Kyber und Saber entwickelt. Es wurden neuartige maskierte Hardwarebeschleuniger präsentiert. Dabei wurden Seitenkanaleffekte durch Glitches analysiert und behoben. Ein verbesserter generischer Ring-Arithmetik Beschleuniger führte zudem dazu, dass sowohl Kyber als auch Saber noch schneller ausgeführt werden. Durch die Integration der Gegenmaßnahmen verlangsamt sich die Ausführungszeit trotzdem um Faktor $4{,}48$ für Kyber und $2{,}60$ für Saber. Die hohen Kosten solcher Gegenmaßnahmen verdeutlicht noch einmal die Wichtigkeit von Hardwarebeschleunigern. Ohne eine Beschleunigung wäre die Ausführungszeit für viele Applikationen nicht mehr tolerierbar.
Die Ergebnisse dieser Analyse wurden auf der „IACR Transactions on Cryptographic Hardware and Embedded Systems“ vorgestellt [FVBBR+21].

Verbesserung der Effizienz von Seitenkanalangriffen auf Kyber In vielen gitterbasierten Verfahren werden polynommultiplikationen mittels der sogenannten Number Theoretic Transform (NTT) durchgeführt um die Berechnung signifikant zu beschleunigen. In vorherigen Arbeiten wurde bereits gezeigt, dass die Multiplikation mit den geheimen Schlüsselpolynomen mittels Seitenkanalangriffen attackiert werden kann. Hierfür wurden jedoch relativ starke Angreifermodelle vorausgesetzt. Im Rahmen des Projekts hat die Technische Universität München unter anderem untersucht, wie solche Angreifermodelle vereinfacht werden können und somit die Effizienz dieser Angriffe verbessert werden kann. Mittels speziell konstruierten Ciphertexten und unter Verwendung sogenannter Belief Propagation (BP) Algorithmen, welche häufig im Bereich des maschinellen Lernens verwendet werden, konnte die Rauschtoleranz und somit die Effizienz des Angriffs verbessert werden.
Diese Arbeiten wurden unter anderem mit dem Projektpartner Fraunhofer AISEC durchgeführt und auf der „IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021“ veröffentlicht [HHP+21].

2.2 Nutzen und Verwertbarkeit der Ergebnisse entsprechend des Verwertungsplans

Die Ergebnisse fließen in den Lehrbetrieb an der Technischen Universität München ein. Insbesondere wurden und werden Ergebnisse aus dem Bereich sichere und effiziente Hardwareimplementierung von kryptografischen Verfahren in den Lehrveranstaltungen „Projektpraktikum Krypto-Implementierung“ und „Circuit Design for Security“ verwendet. Zudem wurden die Erkenntnisse des ASIC Designs genutzt um das „Projekt-

praktikum Krypto-Implementierung“ zur Lehrveranstaltung „Praktikum ASIC Design von Hardwarebeschleunigern für RISC-V“ weiter zu entwickeln. Die Erkenntnisse im Bereich Post-Quanten-Kryptografie fließen außerdem in die Vorlesung „Quantum Computers + Quantum Secure Communications“ mit ein. Außerdem werden die Ergebnisse aus dem Projekt in der „Ringvorlesung Sicherheit in der Informationstechnik“ verwendet. Die Ergebnisse dienen außerdem als Basis für weitere Forschungskooperationen. Zum Beispiel spielt das Thema Post-Quanten-Kryptografie in den Projekten PoQsiKom und 6G-life eine große Rolle. Zudem werden die Erfahrungen mit RISC-V Prozessoren im Projekt PoQsiKom verwertet.

2.3 Während des Vorhabens bekanntgewordene Fortschritte auf dem Gebiet des Vorhabens bei anderer Stelle

Wie oben bereits erwähnt ist der NIST Standardisierungsprozess zur Post-Quanten Kryptografie weiter fortgeschritten und erste Algorithmen wurden zur Standardisierung ausgewählt [Moo22]. Zudem wurde jedoch angekündigt, dass es eine zusätzliche Runde zur Evaluierung alternativer Kandidaten geben wird. Zusätzlich rief die NIST explizit zur Einreichung neuer Signaturverfahren im Rahmen der nächsten Runde auf[2]. Die Arbeiten im Projekt Aquorypt können als Beitrag zur Evaluierung der Sicherheit als auch Implementierungseffizienz der verschiedenen Verfahren gesehen werden. Es sind keine Fortschritte auf dem Gebiet des Vorhabens bekannt geworden, die das Projekt gefährdet haben. Zeitgleiche Forschungsarbeiten wie unter anderem [AEL+20] und [BGR+21] wurden in die Arbeiten aufgenommen und erweitert.

[2] https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals

Aquorypt Puplikationen der TUM

[FSS20a] Tim Fritzmann, Georg Sigl, and Johanna Sepúlveda. Extending the RISC-V instruction set for hardware acceleration of the post-quantum scheme LAC. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1420–1425. IEEE, 2020.

[FSS20b] Tim Fritzmann, Georg Sigl, and Johanna Sepúlveda. RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(4):239–280, Aug. 2020.

[FVBBR+21] Tim Fritzmann, Michiel Van Beirendonck, Debapriya Basu Roy, Patrick Karl, Thomas Schamberger, Ingrid Verbauwhede, and Georg Sigl. Masked accelerators and instruction set extensions for post-quantum cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(1):414–460, Nov. 2021.

[FVFS21] Tim Fritzmann, Jonas Vith, Daniel Flórez, and Johanna Sepúlveda. Post-quantum cryptography for automotive systems. *Microprocessors and Microsystems*, 87(November 2021):1–8, Nov. 2021.

[FVS20] Tim Fritzmann, Jonas Vith, and Johanna Sepúlveda. Strengthening post-quantum security for automotive systems. In *23rd Euromicro Conference on Digital System Design (DSD)*, pages 570–576. IEEE, 2020.

[HHP+21] Mike Hamburg, Julius Hermelink, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. Chosen ciphertext k-trace attacks on masked CCA2 secure kyber. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(4):88–113, 2021.

[KFS21] Patrick Karl, Tim Fritzmann, and Georg Sigl. Hardware accelerated FrodoKEM on RISC-V. In *International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*. IEEE, 2021.

[RFS20] Debapriya Basu Roy, Tim Fritzmann, and Georg Sigl. Efficient hardware/software co-design for post-quantum crypto algorithm SIKE on ARM

and RISC-V based microcontrollers. In *IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, pages 1–9. IEEE/ACM, 2020.

Aquorypt Geplante Puplikationen der TUM

[OFP+] Felix Oberhansl, Tim Fritzmann, Thomas Pöppelmann, Debapriya Basu Roy, and Georg Sigl. Uniform instruction set extensions for multiplications in contemporary and post-quantum cryptography. In *Journal of Cryptographic Engineering*. Springer-Verlag. Submitted (no acceptance decision yet).

Literaturverzeichnis

[AASA+20] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the NIST post-quantum cryptography standardization process. *US Department of Commerce, NIST*, 2020.

[AEL+20] Erdem Alkim, Hülya Evkan, Norman Lahr, Ruben Niederhagen, and Richard Petri. Isa extensions for finite field arithmetic. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 219–242, 2020.

[AHH+19] Martin R. Albrecht, Christian Hanser, Andrea Höller, Thomas Pöppelmann, Fernando Virdia, and Andreas Wallner. Implementing rlwe-based schemes using an RSA co-processor. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(1):169–208, 2019.

[BFM+18] Konstantin Braun, Tim Fritzmann, Georg Maringer, Thomas Schamberger, and Johanna Sepúlveda. Secure and compact full ntru hardware implementation. In *2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, pages 89–94. IEEE, 2018.

[BGR+21] Joppe W Bos, Marc Gourjon, Joost Renes, Tobias Schneider, and Christine van Vredendaal. Masking kyber: First-and higher-order implementations. *IACR Cryptol. ePrint Arch.*, 2021:483, 2021.

[CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. Cryptology ePrint Archive, Paper 2022/975, 2022. `https://eprint.iacr.org/2022/975`.

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In *Annual International Cryptology Conference*, pages 398–412. Springer, 1999.

[Fra] Fraunhofer AISEC. Quo Vadis: Post-Quanten-Kryptografie? `https://eveeno.com/quovadispqk`.

[GGM+20] Si Gao, Johann Großschädl, Ben Marshall, Dan Page, Thinh Pham, and Francesco Regazzoni. An instruction set extension to support software-based masking. Cryptology ePrint Archive, Report 2020/773, 2020. https://ia.cr/2020/773.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *28th annual ACM Symposium on Theory of Computing*, pages 212–219. Association for Computing Machinery, 1996.

[KRSS] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. PQM4: Post-quantum crypto library for the ARM Cortex-M4. https://github.com/mupq/pqm4.

[MNP+20] Ben Marshall, G. Richard Newell, Dan Page, Markku-Juhani O. Saarinen, and Claire Wolf. The design of scalar AES instruction set extensions for RISC-V. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(1):109–136, Dec. 2020.

[Moo22] Dustin Moody. Status report on the third round of the NIST post-quantum cryptography standardization process. Technical report, 2022.

[MPP21] Ben Marshall, Daniel Page, and Thinh Hung Pham. A lightweight ISE for ChaCha on RISC-V. In *IEEE 32nd International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pages 25–32. IEEE, 2021.

[MPW21] Ben Marshall, Dan Page, and James Webb. Miracle: Micro-architectural leakage evaluation. Cryptology ePrint Archive, Report 2021/261, 2021. https://ia.cr/2021/261.

[Nat] National Institute of Standards and Technology. Post-Quantum Cryptography - Round 3 Submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[Nat16] National Institute of Standards and Technology. Announcing request for nominations for public-key post-quantum cryptographic algorithms, 2016. https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms.

[OG17] Tobias Oder and Tim Güneysu. Implementing the newhope-simple key exchange on low-cost fpgas. In *International Conference on Cryptology and Information Security in Latin America*, pages 128–142. Springer, 2017.

[OM20] Jeffrey Osier-Mixon. RISC-V: An open approach to system security, 2020. Accessed December 18, 2021: https://riscv.org/blog/2020/03/risc-v-an-open-approach-to-system-security/.

[otPRC16] The Central People's Government of the People's Republic China. Outline of the national medium and long term program for science and technology development, 2016. `http://www.gov.cn/jrzg/2006-02/09/content_183787.htm`.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994.

[TZS+16] Andreas Traber, Florian Zaruba, Sven Stucki, Antonio Pullini, Germain Haugou, Eric Flamand, Frank K. Gurkaynak, and Luca Benini. PULPino: A small single-core RISC-V SoC. In *3rd RISCV Workshop*, 2016.

Kurzbericht zum Projekt Aquorypt

Autoren: Patrick Karl, Dr. Tim Fritzmann, Prof. Dr. Georg Sigl, Technische Universität München

Hintergrund des Projekts

Quantencomputer mit großer Rechenleistung werden in der Lage sein, alle gängigen kryptografischen Verfahren für digitale Signaturen und zum Schlüsselaustausch zu brechen. Es existieren bereits erste quantencomputerresistente kryptografische Verfahren. Diese Verfahren zählen zur Kategorie Post-Quanten-Kryptografie. Allerdings müssen die neuartigen Verfahren noch weiter optimiert werden und in die relevanten Anwendungen integriert werden, bevor leistungsstarke Quantencomputer zur Verfügung stehen und zur Gefahr für die IT-Sicherheit werden. Das Projekt Aquorypt (16KIS1017K) untersucht daher die Anwendung und praktische Umsetzung von quantencomputerresistenten kryptografischen Verfahren in zwei wichtigen Bereichen, die besonders auf langfristige Sicherheit angewiesen sind: Eingebettete Systeme in der industriellen Automatisierung und Chipkarten-basierte Sicherheitsanwendungen. Eingebettete Systeme im Industriebereich haben hohe Echtzeitanforderungen und erfordern Migrationskonzepte bis in die Hardware. Mit hochsicheren Chipkarten werden außerdem Systeme analysiert, welche extreme Kostenanforderungen haben und einen geringen Stromverbrauch voraussetzen.

Ziele

Der Fokus der Technischen Universität München in diesem Projekt liegt vor allem auf der Weiterentwicklung und Auswahl geeigneter Algorithmen, auf der effizienten Realisierung in Hardware und Software und auf der Härtung dieser Verfahren gegen Seitenkanalangriffe. Diese Angriffe nutzen physikalische Effekte wie zum Beispiel den Stromverbrauch, um Rückschlüsse auf den geheimen Schlüssel zu ziehen. Durch die Erforschung von effizienten Hardware- und Softwarelösungen sollen die Post-Quanten-Kryptografie Verfahren für die Integration in die Applikationen vorbereitet werden. Die im Projekt entwickelten Koprozessoren und Hardwarebeschleuniger sollen den Hauptprozessor bei rechenintensiven kryptografischen Aufgaben unterstützen, um die Gesamteffizienz des Systems zu steigern. Ein solcher Ansatz ist besonders wichtig für kleine Prozessoren, die ansonsten Latenz-, Durchsatz- oder Energieanforderungen nicht erfüllen könnten. Aber auch leistungsstarke Prozessoren oder Rechenzentren können von einer Beschleunigung profitieren.

Ergebnisse

Der Forschungsschwerpunkt des Lehrstuhls für Sicherheit in der Informationstechnik der TUM im Verbundprojekt Aquorypt lag in der Erforschung und Entwicklung von effizienten Hardwarebeschleunigern für Post-Quanten sichere Kryptografieverfahren. Dabei wurden verschiedene Kandidaten des NIST Standardisierungsprojektes analysiert und entsprechend deren Anwendbarkeit für eingebettete Systeme evaluiert. Hierbei hat sich ergeben, dass besonders gitterbasierte Verfahren aufgrund ihrer Ressourceneffizienz geeignet sind. Neben

Parameteroptimierungen hat sich die TUM damit beschäftigt, Hardwarebeschleuniger in eine quelloffene RISC-V Prozessorarchitektur zu integrieren, um durch das HW/SW Codesign einerseits die Performanz der Verfahren zu verbessern und gleichzeitig den Energieverbrauch zu senken. Dies wurde für verschiedene Verfahren durchgeführt und damit ein Beitrag hinsichtlich der Implementierungseffizienz zum Standardisierungsprozess geleistet. Um die Beschleuniger zusätzlich gegen Seitenkanalangriffe abzusichern, wurden Maskierungsverfahren in Hardware implementiert. Letztlich wurde die entstandene RISC-V Plattform mit ausgewählten Beschleuniger in einem ASIC Tapeout auf 22nm Technologie umgesetzt. Durch entsprechende Tests konnte die Funktionalität der gefertigten Chips erfolgreich überprüft werden und beispielhaft in einem Demonstrator integriert werden.

Nutzen und Verwertbarkeit der Ergebnisse

Die Ergebnisse fließen in den Lehrbetrieb an der Technischen Universität München ein. Insbesondere wurden und werden Ergebnisse aus dem Bereich sichere und effiziente Hardwareimplementierung von kryptografischen Verfahren in den Lehrveranstaltungen „Projektpraktikum Krypto-Implementierung“ und „Circuit Design for Security“ verwendet. Zudem wurden die Erkenntnisse des ASIC Designs genutzt um das „Projektpraktikum Krypto-Implementierung“ zur Lehrveranstaltung „Praktikum ASIC Design von Hardwarebeschleunigern für RISC-V“ weiter zu entwickeln. Die Erkenntnisse im Bereich Post-Quanten-Kryptografie fließen außerdem in die Vorlesung „Quantum Computers + Quantum Secure Communications“ mit ein. Außerdem werden die Ergebnisse aus dem Projekt in der „Ringvorlesung Sicherheit in der Informationstechnik“ verwendet.

Ferner dienen die Ergebnisse als Basis für weitere Forschungskooperationen. Zum Beispiel spielt das Thema Post-Quanten Kryptografie in den Projekten PoQsiKom (13I40V010B) und 6G-life (16KISK002) eine große Rolle. Zudem werden die Erfahrungen mit RISC-V Prozessoren im Projekt PoQsiKom verwertet.