HAW HAMBURG

BACHELOR THESIS
Deniese Kotthoff

Post-Quantum-Kryptografie: Eine vergleichende Analyse neuer kryptografischer Verfahren und deren Anwendung

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Deniese Kotthoff

Post-Quantum-Kryptografie: Eine vergleichende Analyse neuer kryptografischer Verfahren und deren Anwendung

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Olaf Zukunft

Eingereicht am: 04. Januar 2024

Deniese Kotthoff

Thema der Arbeit

Post-Quantum-Kryptografie: Eine vergleichende Analyse neuer kryptografischer Verfahren und deren Anwendung

Stichworte

Post-Quantum-Kryptografie, Analyse, Sicherheit, kryptografische Verfahren, Anwendung kryptographischer Verfahren, Quantencomputer

Kurzzusammenfassung

In dieser Bachelorarbeit wird die Post-Quantum-Kryptografie untersucht, ein Forschungsfeld, das durch die potenzielle Bedrohung herkömmlicher Kryptosysteme durch Quantencomputer an Bedeutung gewinnt. Der Fokus liegt auf der vergleichenden Analyse neuer kryptografischer Verfahren, die darauf abzielen, die Sicherheitslücken zu schließen, die durch die Fortschritte in der Quanteninformatik entstehen könnten. Diese Arbeit bietet einen umfassenden Überblick über verschiedene Post-Quantum-Kryptografie Methoden, einschließlich gitter-basierter, hash-basierter, multivariater und code-basierter Kryptografie. Jedes Verfahren wird hinsichtlich seiner theoretischen Grundlagen, Sicherheitsmerkmale und potenziellen Anwendungsbereiche untersucht. Darüber hinaus werden die Herausforderungen und Vorteile dieser Verfahren im Vergleich zu herkömmlichen kryptografischen Ansätzen diskutiert. Ein besonderer Schwerpunkt liegt auf der Analyse der Praktikabilität dieser Verfahren für reale Anwendungen, einschließlich der Bewertung ihrer Implementierungseffizienz und der Widerstandsfähigkeit gegenüber verschiedenen Angriffstypen. Die Arbeit zielt darauf ab, ein tieferes Verständnis der Post-Quantum-Kryptografie zu vermitteln und ihre Rolle in der zukünftigen Umgebung der Informationssicherheit zu beleuchten. Abschließend werden Empfehlungen für die Wahl des geeignetsten Post-Quantum-Kryptografieverfahrens gegeben.

Deniese Kotthoff

Title of Thesis

Post-Quantum Cryptography: A Comparative Analysis of New Cryptographic Techniques and Their Applications

Keywords

Post-Quantum Cryptography, Analysis, Security, Cryptographic Techniques, Application of Cryptographic Techniques, Quantum Computing

Abstract

In this bachelor thesis, post-quantum cryptography is explored, a field of research gaining significance due to the potential threat quantum computers pose to conventional cryptosystems. The focus is on a comparative analysis of new cryptographic methods aimed at addressing security gaps that could arise from advances in quantum informatics. This work provides a comprehensive overview of various post-quantum cryptography methods, including lattice-based, hash-based, multivariate, and code-based cryptography. Each method is examined in terms of its theoretical foundations, security features, and potential application areas. Additionally, the challenges and advantages of these methods compared to traditional cryptographic approaches are discussed. Special emphasis is placed on analyzing the practicality of these methods for real-world applications, including assessing their implementation efficiency and resilience against various types of attacks. The thesis aims to convey a deeper understanding of post-quantum cryptography and illuminate its role in the future landscape of information security. Finally, recommendations are given for selecting the most suitable post-quantum cryptographic method.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Post-Quantum-Kryptografie (PQK), oft als quantenresistente Kryptografie bezeichnet, bildet einen Forschungszweig innerhalb der Kryptografie, der sich der Entwicklung von kryptografischen Systemen widmet, welche sowohl vor Angriffen durch Quantencomputer als auch klassische Computer sicher sind. Diese Systeme sind darauf ausgelegt, nahtlos mit existierenden Kommunikationsprotokollen und Netzwerken zu interagieren [2]. Im Unterschied zur Quantenkryptografie, die Quantenphänomene für die Sicherheit und Erkennung von Abhörversuchen einsetzt, können PQ-Kryptografieverfahren auf konventioneller Hardware implementiert werden [3].

Die Sicherheit digitaler Infrastrukturen basiert heute wesentlich auf der Public-Key-Kryptografie, die sich auf die angenommene Rechenkomplexität bestimmter mathematischer Probleme stützen. Zu diesen Problemen gehören das Faktorisierungsproblem (FP) und das Diskrete Logarithmusproblem (DLP). Jedoch könnten die Fortschritte in der Entwicklung von Quantencomputern, insbesondere durch die Einführung effizienter Algorithmen wie den von Peter Shor entwickelten, diese Verfahren bedrohen. Shor's Algorithmus ist in der Lage, große Zahlen effizient zu faktorisieren und das Diskrete Logarithmusproblem zu lösen. Diese Fähigkeit stellt eine signifikante Bedrohung für die Sicherheit von Public-Key-Systemen dar. In Kapitel 3.1 wird detaillierter auf Shor's Algorithmus und seine potenziellen Auswirkungen auf die heutige Kryptografie eingegangen [4].

Vor diesem Hintergrund strebt die PQK nach Methoden, die auch durch die Fähigkeiten von Quantencomputern schwer zu entschlüsseln sind. Zu den führenden Ansätzen zählen dabei die code-basierte, die gitter-basierte und die hash-basierte Kryptografie [4]. Aktuelle Standardisierungsinitiativen, insbesondere das PQK Project des National Institute of Standards and Technology (NIST), fokussieren darauf, eine Auswahl an Verfahren zu standardisieren, deren Sicherheit auf einer Vielzahl von mathematischen Problemen basiert [4].

1.1 Hintergrund, Motivation und Forschungsfragen

Die Entwicklung von Quantencomputern birgt ein signifikantes Potenzial, stellt jedoch gleichzeitig erhebliche Herausforderungen dar, insbesondere im Bereich der Kryptografie. Vor diesem Hintergrund zielt die vorliegende Arbeit darauf ab, die Implikationen von Quantencomputertechnologie auf die Sicherheit gegenwärtiger kryptografischer Verschlüsselungssysteme zu erforschen. Es werden Verfahren der PQK identifiziert, die potenziell in der Zukunft implementiert werden könnten, und eine eingehende Bewertung dieser Verfahren in Bezug auf ihre Sicherheit, Effizienz und Praktikabilität wird durchgeführt. Die zentralen Forschungsfragen sind:

1. *Inwiefern bedrohen Quantencomputer die Integrität und Vertraulichkeit bestehender kryptografischer Verschlüsselungssysteme?*
2. *Welche PQK-Verfahren, einschließlich code-, gitter-, hash- und multivariater Ansätze, bieten sich als zukunftsfähige Lösungen zur Sicherstellung der Datenübertragungssicherheit an, und welche charakteristischen Eigenschaften weisen sie auf?*
3. *Wie unterscheiden sich ausgewählte PQK-Verfahren in Bezug auf Sicherheit, Effizienz und Anwendbarkeit im Vergleich zu traditionellen Verfahren?*

1.2 Zielsetzung und Methodik

Das primäre Ziel dieser Arbeit ist es, ein tiefgehendes Verständnis für die Auswirkungen von Quantencomputern auf die bestehende Kryptografie zu entwickeln und die Eignung verschiedener PQ-Kryptografieansätze für die Sicherung zukünftiger Datenübertragungen zu bewerten. Die methodische Vorgehensweise der Arbeit umfasst dabei die folgenden Schlüsselaspekte:

Literaturrecherche: Ziel ist eine tiefgreifende Analyse bestehender Forschungsergebnisse und Publikationen im Bereich Quantencomputing und PQK, um ein umfassendes Bild des derzeitigen Forschungsstandes zu erhalten.

Bewertungskriterien: Die Entwicklung von Kriterien zur Bewertung der Sicherheit, Effizienz und Anwendbarkeit von PQ-Kryptosystemen. Diese Kriterien werden verwendet, um die verschiedenen Ansätze objektiv zu vergleichen und ihre Eignung für zukünftige Anwendungen zu beurteilen.

Analyse bestehender Systeme: Eine detaillierte Analyse traditioneller kryptografischer Systeme und ihrer Anfälligkeit gegenüber Quantencomputer-Angriffen. Dies umfasst eine Untersuchung der grundlegenden Schwächen herkömmlicher Verschlüsselungstechniken im Kontext von Quantenrechenleistung.

Vergleich von PQ-Verfahren: Eine detaillierte und vergleichende Untersuchung verschiedener Ansätze in der PQK, unter Berücksichtigung ihrer theoretischen Fundamente.

Synthese und Schlussfolgerungen: Eine Zusammenführung der gesammelten Informationen und Erkenntnisse, um umfassende Antworten auf die Forschungsfragen zu geben und Empfehlungen für zukünftige Entwicklungen in der Kryptografie zu formulieren.

Durch diesen strukturierten Ansatz strebt die Arbeit an, die Aspekte der PQK zu beleuchten und einen wertvollen Beitrag zum Verständnis dieses sich schnell entwickelnden Forschungsfeldes zu leisten.

1.3 Struktur der Arbeit

Die Bachelorarbeit ist folgendermaßen gegliedert:

Kapitel 2: Grundlagen bildet die Grundlage für das Verständnis der Funktionsweise von Quantencomputern und der Prinzipien der Kryptografie, einschließlich der PQK.

Kapitel 3: Quanten-Algorithmen in der Kryptografie behandelt spezifische Algorithmen wie Shor's und Grover's Algorithmus, die die Sicherheit traditioneller kryptografischer Systeme bedrohen könnten.

Kapitel 4: Post-Quanten Kryptosysteme untersucht die verschiedenen Kategorien von PQ-Kryptosystemen und analysiert ausgewählte Ansätze im Detail.

Kapitel 5: Standardisierung von Post-Quantum-Kryptografie konzentriert sich auf den Standardisierungsprozess durch Organisationen wie das NIST und diskutiert die Bedeutung dieser Standards.

Kapitel 6: Analyse von Post-Quantum-Kryptografie Ansätzen geht direkt auf die zweite und dritte Forschungsfrage ein, indem es die Sicherheit, Effizienz und Anwendbarkeit verschiedener PQ-Kryptografieansätze bewertet und vergleicht.

Kapitel 7: Schlussfolgerung fasst die wichtigsten Ergebnisse zusammen und bietet einen Ausblick auf zukünftige Forschungsrichtungen im Bereich der PQK.

Diese Struktur erlaubt es, die Forschungsfragen systematisch zu adressieren und bietet einen umfassenden Überblick über das Feld der PQK im Kontext der aufkommenden Quantencomputertechnologie.

2 Grundlagen

Der Grundlagenteil dieser Arbeit legt den soliden Boden für das Verständnis von Quantencomputern, kryptografischen Grundprinzipien und der evolutionären PQK. In einer Ära, in der die Leistungsfähigkeit von Quantencomputern stetig zunimmt, wird die Sicherheit herkömmlicher kryptografischer Systeme zunehmend in Frage gestellt. Daher ist es von entscheidender Bedeutung, die Grundlagen zu verstehen, um innovative Lösungen für die Sicherheitsherausforderungen der Zukunft zu entwickeln.

Quantencomputer: Eine Revolution in der Rechenleistung Die erste Stufe unseres Fundaments führt uns in die Welt der Quantencomputer ein. Hierbei werden die grundlegenden Prinzipien der Quantenmechanik, die für das Verständnis von Quantencomputern unerlässlich sind, erläutert. Wir werden die Konzepte von Qubits, Superposition und Verschränkung erkunden, die die Basis für die beeindruckende Rechenleistung von Quantencomputern bilden. Die Fähigkeit von Quantencomputern, komplexe mathematische Operationen viel schneller durchzuführen als klassische Computer, macht es möglich, Berechnungen durchzuführen, die sonst unermesslich lange dauern würden [1].

Grundlagen der Kryptografie: Schutz in der Digitalen Welt Mit einem fundierten Verständnis der Quantenwelt werden wir uns dann den Grundlagen der Kryptografie zuwenden. Kryptografie bildet die Grundlage für die Sicherheit digitaler Kommunikation und Datenspeicherung. Hier werden klassische Verschlüsselungsverfahren, Hashfunktionen und digitale Signaturen beleuchtet, um die Prinzipien zu verstehen, die es zu schützen gilt [1].

Post-Quantum-Kryptografie: Eine Notwendigkeit in der Quantenära Im letzten Abschnitt dieses Teils werden wir den Übergang zur PQK vollziehen. Wir werden untersuchen, warum die herkömmliche Kryptografie durch Quantencomputer gefährdet ist und wie PQK als Antwort auf diese Bedrohung entstanden ist. Ein Überblick über die vielversprechendsten Ansätze und Algorithmen wird dabei helfen, die Vielschichtigkeit dieser neuen Ära der Kryptografie zu verstehen. [1].

Durch diesen Grundlagenteil wird der Leser optimal auf die weiteren Abschnitte vorbereitet, die detaillierte Einblicke in die Funktionsweise von Quantencomputern, die Prinzipien von Shor und Grover, post-quanten Kryptosysteme sowie die aktuelle Standardisierung und Bewertung bieten.

2.1 Funktionsweise eines Quantencomputers

Die Arbeitsweise eines Quantencomputers basiert auf einem innovativen Paradigma, das sich fundamental von der Funktionsweise herkömmlicher Computer unterscheidet. Während herkömmliche Computer Berechnungen auf der Grundlage der Gesetze der klassischen Physik durchführen, nutzt ein Quantencomputer die Prinzipien der Quantenphysik. Dies führt zu grundlegenden Unterschieden in der Art und Weise, wie Informationen gespeichert und verarbeitet werden. Drei herausragende Merkmale kennzeichnen einen Quantencomputer im Vergleich zu einem herkömmlichen Computer: Superposition, Verschränkung und der sogenannte Beobachtereffekt. Im Folgenden werden diese drei Konzepte näher erläutert. [5].

In einem herkömmlichen Computer erfolgt die Speicherung von Informationen in Form von Bits, während in einem Quantencomputer Informationen in Quantenbits, auch als Qubits bekannt, abgelegt werden. Der wesentliche Unterschied zwischen einem Bit und einem Qubit besteht darin, dass ein Bit entweder den Wert Eins (wie in Abbildung 2.1) oder Null enthält [5].

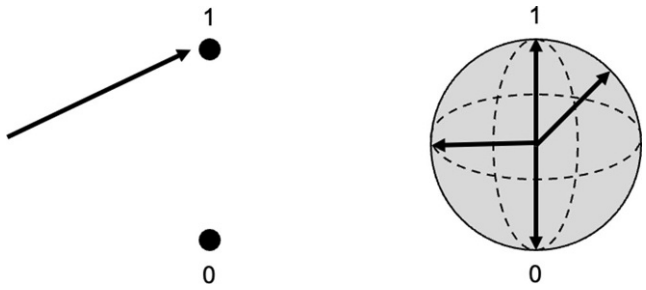

Abbildung 2.1: Bit- und Qubit-Darstellung (Barenkamp, 2022, S. 2)

Im Gegensatz dazu hat ein Qubit, wie ebenfalls in Abbildung 2.1 dargestellt, die bemerkenswerte Eigenschaft, gleichzeitig beide Zustände anzunehmen. Dies bedeutet, dass es sowohl den Zustand Eins als auch den Zustand Null zur gleichen Zeit enthalten kann.

Die Fähigkeit der Qubits zur Superposition ist von entscheidender Bedeutung und einer der Hauptgründe für die bemerkenswerte Rechenleistung von Quantencomputern. Diese Eigenschaft

ermöglicht es Quantencomputern, Berechnungen parallel durchzuführen, im Gegensatz zur aktuellen Computertechnologie, die sequenziell arbeitet. Dank dieser Eigenschaft können Quantencomputer bestimmte mathematische Herausforderungen erheblich schneller bewältigen als herkömmliche Computer, darunter die Faktorisierung von Primzahlen und das diskrete Logarithmenproblem, die in der Kryptografie von besonderer Bedeutung sind [5].

Bei der Nutzung von zwei Bits in konventionellen Computern lassen sich vier Zustände darstellen, die die Zahlen von Null bis Drei repräsentieren: [0,0] steht für Null, [0,1] für Eins, [1,0] für Zwei und [1,1] für Drei. Jede Bitkombination entspricht eindeutig einer bestimmten Zahl [5].

Qubits in Quantencomputern haben die Fähigkeit, theoretisch unendlich viele Zustände gleichzeitig anzunehmen. Diese Eigenschaft ermöglicht es Qubits, simultan eine Vielzahl von Zahlen zu repräsentieren. Selbst wenn ein Qubit lediglich die Zustände Null und Eins annimmt, ergibt sich bereits ein bedeutender Vorteil gegenüber einem klassischen Bit [5].

In Quantencomputern führt jedes zusätzliche Qubit zu einer Verdoppelung der gleichzeitig darstellbaren Zustände, was eine exponentielle Steigerung der Rechenkapazität bewirkt [5].

n der heutigen Verschlüsselungstechnologie werden sogenannte Einwegfunktionen verwendet. Diese mathematischen Funktionen können zwar schnell berechnet werden, aber ihre Umkehrung erfordert erheblichen Rechenaufwand. Zu diesen Funktionen gehören die Multiplikation von Primzahlen und die Berechnung bestimmter Exponentialfunktionen. Die Multiplikation von vier Primzahlen, wie zum Beispiel
$2 \times 3 \times 5 \times 7 = 210$, bereitet einem herkömmlichen Computer keine Schwierigkeiten und kann schnell durchgeführt werden. Im Gegensatz dazu verursacht die Bestimmung der Primfaktoren der Zahl 210 erheblich mehr Rechenaufwand und folglich auch einen erhöhten Zeitaufwand [5].

An dieser Stelle offenbaren Quantencomputer ihre bemerkenswerte Leistungsfähigkeit. Sie sind dazu in der Lage, die in Verschlüsselungsverfahren verwendeten Einwegfunktionen in deutlich kürzerer Zeit umzukehren und somit herkömmliche Verschlüsselungsverfahren zu durchbrechen. Während die Umkehrung einer Primzahlmultiplikation, auch als Primfaktorzerlegung bekannt, oder die Lösung einer Exponentialfunktion, wie der diskrete Logarithmus, mithilfe eines herkömmlichen Computers mehrere Millionen Jahre in Anspruch nehmen würde, kann ein Quantencomputer diese Aufgaben in nur wenigen Minuten bewältigen [5].

Zusätzlich zur Superposition verfügen Quanten auch über die Eigenschaft der Quantenverschränkung, die auf den Grundsätzen der Quantenphysik beruht. Diese Charakteristik der Qubits gewährt dem Quantencomputer einen weiteren Vorteil in Bezug auf die Rechengeschwindigkeit im

Vergleich zu klassischen Computern. Wenn Qubits miteinander quantenverschränkt sind, bedeutet dies, dass sie in gewisser Weise miteinander verknüpft sind [5](siehe Abbildung 2.2).

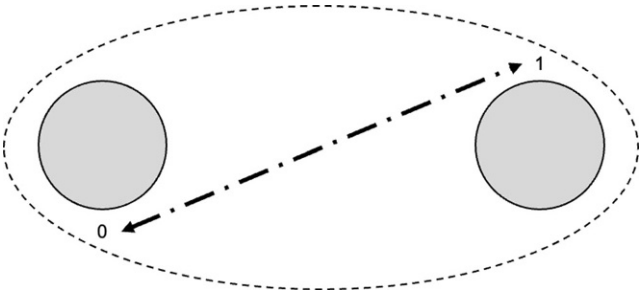

Abbildung 2.2: Verschränkung (Barenkamp, 2022, S. 3)

Die Veränderung des Zustands eines Qubits, beispielsweise auf 1, bewirkt gleichzeitig die Änderung des Zustands des anderen mit diesem Qubit quantenverschränkten Qubits auf 0. Dieser Prozess erfolgt ohne zeitliche Verzögerung Anders formuliert ermöglicht das Messen eines Qubits unverzüglich die Bestimmung des Zustands des anderen verschränkten Qubits. Diese Eigenschaft ermöglicht es, Berechnungen in einem Quantencomputer mit Überlichtgeschwindigkeit durchzuführen, was mit einem konventionellen Computer nicht realisierbar ist [5].

Die dritte außergewöhnliche Eigenschaft von Quantencomputern wird als der Beobachtereffekt bezeichnet. Wenn ein Qubit beispielsweise als Lichtphoton übertragen wird, zeigt es die auffällige Eigenschaft, dass es im Falle einer Messung oder Beobachtung seines Zustandes einen der beiden Zustände, Null oder Eins, annimmt. Dies bedeutet, dass es in einen der beiden Zustände „kollabiert“, die es gleichzeitig repräsentiert. Daher hat der Beobachter durch die Durchführung einer Messung einen direkten Einfluss auf den Zustand der Qubits und somit auf das Ergebnis des Experiments [5] (siehe Abbildung 2.3).

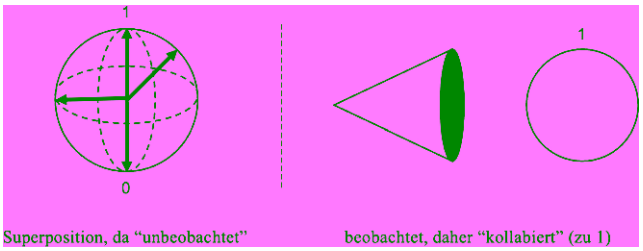

Abbildung 2.3: Qubit unbeobachtet vs. beobachtet (Barenkamp, 2022, S. 3)

Die oben beschriebene Eigenschaft der Qubits hat zwar keine direkte Auswirkung auf die Rechengeschwindigkeit von Quantencomputern, jedoch beeinflusst sie wesentlich die zukünftigen Potenziale und innovativen Ansätze in der Kryptografie. Dabei wird der Umstand genutzt, dass

ein unerwünschtes Abgreifen von Informationen durch eine dritte Partei genau dem Beobachtereffekt entspricht. Sobald während der Kommunikation zwischen zwei Endpunkten ein Mitschnitt dieser (verschlüsselten) Informationen erfolgt, kollabieren die Qubits, und sie erreichen den Empfänger nicht in der erwarteten Art und Weise [5].

2.2 Grundlagen der Kryptografie

Kryptografie ist die Wissenschaft, Nachrichten mithilfe von Mathematik zu verschleiern. Die Nachricht wird unter Verwendung eines kryptografischen Verschlüsselungsalgorithmus getarnt, um den Inhalt der Nachricht zu verbergen. Die getarnten Daten werden auch als Chiffretext bezeichnet. Die Nachricht wird als Klartext bezeichnet. Der Chiffretext kann mithilfe von Entschlüsselungsalgorithmen wieder in die Nachricht umgewandelt werden. Die Umsetzung einer kryptografischen Technik wird als Kryptosystem bezeichnet. Kryptoanalyse ist die Wissenschaft, Kryptosysteme zu analysieren und zu brechen, die als sicher gelten [6].

Bei der Initiierung einer Verbindung zu einer Website, die durch das Protokoll `https` gekennzeichnet ist, implementiert der Computer des Benutzers das *Transport Layer Security* (TLS) Protokoll, um eine gesicherte Verbindung mit dem entsprechenden Webserver zu etablieren. Laut Bernstein und Lange (2017) implementiert TLS eine Vielzahl von kryptografischen Verfahren, um mehrere Sicherheitsziele zu erreichen. Erstens wird durch diese Verfahren die Vertraulichkeit der übertragenen Daten sichergestellt, indem verhindert wird, dass Dritte die Inhalte der Kommunikation entschlüsseln können. Zweitens gewährleistet TLS die Integrität der übertragenen Daten, indem es sicherstellt, dass jegliche Modifikationen der Nachrichten während der Übertragung erkannt werden können. Drittens stellt TLS die Authentizität der Kommunikation sicher, indem es die Möglichkeit ausschließt, dass sich Dritte als eine der beteiligten Parteien ausgeben. [7]

Im Kontext der symmetrischen Kryptografie, wie sie von Alice und Bob genutzt wird, besteht der Schlüsselunterschied in der Verwendung eines gemeinsamen geheimen Wertes, des sogenannten *Schlüssels*. Mit diesem Schlüssel führen sie symmetrische kryptografische Operationen durch, die sowohl für die Verschlüsselung als auch für die Entschlüsselung der Nachrichten erforderlich sind. Eine wesentliche Frage, die in diesem Zusammenhang oft aufkommt, ist die Methode, mittels derer beide Parteien in den Besitz desselben geheimen Schlüssels gelangen, ein Problem, das in späteren Diskussionen näher betrachtet wird [7].

In der betrachteten Kommunikationssituation besitzt Alice eine Nachricht m, bestehend aus Daten wie einer Webseite oder einer Datei, die sie an Bob übermitteln möchte. Sowohl Alice als auch Bob sind im Besitz eines gemeinsamen symmetrischen Verschlüsselungsschlüssels k_{enc}. Alice nutzt einen „symmetrischen Verschlüsselungsalgorithmus“, der den Schlüssel k_{enc} einbezieht, um die Nachricht m zu verschlüsseln, wodurch ein Chiffretext c generiert wird. Dieser Chiffretext c wird anschließend über ein Netzwerk an Bob übertragen. Bei Empfang des Chiffretexts wendet Bob einen korrespondierenden symmetrischen Entschlüsselungsalgorithmus an, der ebenfalls den Schlüssel k_{enc} verwendet. Dieser Prozess rekonstruiert die ursprüngliche Nachricht m aus dem Chiffretext c [7].

Zur Gewährleistung der Authentizität der Nachricht integriert Alice zusätzlich einen *Message Authentication Code* (MAC), der unter Verwendung eines weiteren Schlüssels k_{auth} auf den Chiffretext c angewendet wird. Dieser Vorgang resultiert in einem Authentifizierungstag, welcher zusammen mit dem Chiffretext über das Netzwerk an Bob gesendet wird. Dieser Tag dient als Beweis dafür, dass Alice Zugang zu dem Schlüssel k_{auth} hat. Nach Erhalt dieses Tags führt Bob eine entsprechende Überprüfung durch, indem er denselben MAC-Algorithmus mit dem identischen Schlüssel k_{auth} anwendet, um die Authentizität der Nachricht zu verifizieren. [7].

Symmetrische Kryptografie, kennzeichnet sich durch die Verwendung eines einzigen Schlüssels für sowohl Verschlüsselungs- als auch Entschlüsselungsvorgänge. Dieses Verfahren beruht auf der Annahme, dass bei einer hinreichend langen und zufälligen Schlüsselauswahl die Durchführung von Brute-Force-Angriffen die Grenzen der gegenwärtig verfügbaren Rechenressourcen übersteigt. Die Effektivität symmetrischer Kryptografieschemata ist somit in hohem Maße abhängig von der Schlüssellänge und der Zufälligkeit des Schlüssels [6].

Ein zentrales Sicherheitsproblem in der Anwendung symmetrischer Kryptografie besteht in der Notwendigkeit, den Schlüssel sicher zwischen den kommunizierenden Parteien zu übermitteln. Da beide Parteien denselben Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln der Information verwenden, ist die vertrauliche und unverfälschte Übertragung dieses Schlüssels von Sender zu Empfänger von entscheidender Bedeutung. Die Herausforderung liegt darin, Methoden zu entwickeln und zu implementieren, die die Integrität und Geheimhaltung des Schlüssels während seiner Übermittlung gewährleisten, um die Gesamtsicherheit des Kryptografiesystems zu garantieren [6].

Im Rahmen der `https`-Kommunikation spielt die symmetrische Kryptografie eine entscheidende Rolle bei der Gewährleistung der Vertraulichkeit der Datenübertragung. Diese Technik verhindert, dass unbefugte Dritte die Inhalte der Nachrichten einsehen können. Darüber hinaus ist die Authentifizierung ein wesentlicher Bestandteil, der sowohl die Authentizität als auch die

Integrität der Nachrichten sichert. Sie verhindert effektiv, dass ein potenzieller Angreifer Nachrichten modifiziert oder unter falscher Identität Nachrichten in die Kommunikation einschleust. `https` unterstützt eine Vielzahl von symmetrischen Verschlüsselungsalgorithmen sowie Message Authentication Codes (MACs), von denen einige auf Hash-Funktionen basieren [7].

Hier betrachten wir nur Hash-Funktionen, die speziell dafür ausgelegt sind, bestimmte Berechnungen zu erschweren:

1. Das Auffinden eines Präbildes für einen gegebenen Wert z im Bild von h, d.h., eine Zeichenkette m zu identifizieren, so dass $h(m) = z$.

2. Für eine gegebene Zeichenkette m und $h(m)$ ein zweites Präbild zu finden, also eine Zeichenkette $m' \neq m$ mit $h(m) = h(m')$.

3. Das Auffinden einer Kollision, d.h., zwei unterschiedliche Zeichenketten $m \neq m'$ zu ermitteln, für die $h(m) = h(m')$ gilt [7].

Die bisherige Diskussion hat den Prozess, durch den Alice und Bob zu einem gemeinsamen symmetrischen Schlüssel gelangen, nicht thematisiert. Dieser Aspekt der `https`-Verbindung basiert auf der Public-Key-Kryptografie. In diesem System besitzt jede Partei zwei Schlüssel: einen öffentlichen und einen privaten. Der private Schlüssel bleibt ausschließlich dem Besitzer bekannt, während der öffentliche Schlüssel veröffentlicht werden kann. Unter Verwendung des öffentlichen Schlüssels von Alice kann jeder eine Nachricht verschlüsseln, die nur von Alice mit ihrem zugehörigen privaten Schlüssel entschlüsselt werden kann [7].

Im Rahmen der `https`-Protokollkommunikation agiert Alice als Webserver und Bob als Browser. In der Anfangsphase der Interaktion kontaktiert Bob Alice, um ihren öffentlichen Schlüssel anzufordern. Nach Erhalt dieses Schlüssels generiert Bob einen einmaligen symmetrischen Schlüssel, verschlüsselt ihn mit Alices öffentlichem Schlüssel und sendet ihn zurück an Alice. Für die nachfolgende Kommunikation wird dieser symmetrische Schlüssel für die Verschlüsselung und Authentifizierung verwendet, wie zuvor beschrieben. Alice entschlüsselt Bobs anfängliche Nachricht, um den gemeinsamen symmetrischen Schlüssel zu erlangen, und verwendet diesen für die wechselseitige Kommunikation [7].

Eine alternative Methode im `https`-Protokoll beinhaltet die Nutzung eines anderen Public-Key-Verfahrens, des sogenannten Schlüsselaustausches. Dieser Ansatz nutzt unterschiedliche mathematische Funktionen, ähnelt aber dem zuvor beschriebenen Verfahren. Anstatt dass Bob einen symmetrischen Schlüssel mit Alices öffentlichem Schlüssel verschlüsselt, leiten Bob und Alice

durch gemeinsame Berechnungen einen symmetrischen Schlüssel her. Die Authentizität und Gültigkeit der öffentlichen Schlüssel innerhalb des `https`-Protokolls wird durch das Herunterladen und Überprüfen von Zertifikaten durch den Browser gewährleistet [7].

In einem digitalen Signatursystem erzeugt Bob eine Signatur, indem er einen Signaturalgorithmus mit seinem privaten Signaturschlüssel auf eine Nachricht *m* anwendet. Jeder kann diese Signatur überprüfen, indem ein Verifizierungsalgorithmus mit Bobs öffentlichem Signaturschlüssel auf *m* angewendet wird. Typischerweise beinhalten diese Algorithmen die Anwendung einer Hash-Funktion auf die Nachricht, kombiniert mit weiteren mathematischen Operationen, die die Schlüssel involvieren [7].

2.3 Post-Quantum-Kryptografie

Die PQK ist ein Forschungsfeld innerhalb der Kryptografie, das sich auf die Entwicklung von Verschlüsselungsalgorithmen konzentriert, die selbst gegenüber Angreifern, die Zugang zu Quantencomputertechnologie haben, als sicher gelten. Die gängigen asymmetrischen Kryptografiealgorithmen, darunter RSA, ECC (Elliptische-Kurven-Kryptografie), DH (Diffie-Hellman) und DSA (Digital Signature Algorithm), sind anfällig für Angriffe mittels Quantencomputern. Diese Algorithmen basieren auf der Schwierigkeit der Primfaktorzerlegung oder des diskreten Logarithmusproblems, die jedoch durch den Einsatz des Shor-Algorithmus auf Quantencomputern effizient gelöst werden können. Diese zahlentheoretischen Probleme dienten Mathematikern und Kryptographen lange Zeit als Grundlage für die Sicherheit der asymmetrischen Algorithmen. Mit dem Aufkommen der Quantencomputertechnologie ist nun eine Neuorientierung erforderlich, um neue mathematische Probleme zu identifizieren, die einer Lösung durch Quantencomputer widerstehen können [6].

Symmetrische Verschlüsselungsalgorithmen und Hash-Funktionen werden im Vergleich zu asymmetrischen Algorithmen als relativ sicher angesehen, besonders unter Berücksichtigung potenzieller Angriffe mit Quantencomputern. Zwar bietet der Grover-Algorithmus auf Quantencomputern eine Beschleunigung potenzieller Angriffsstrategien gegen diese Algorithmen, jedoch lässt sich die Sicherheit der meisten symmetrischen Verschlüsselungsverfahren durch eine Verdoppelung der Schlüssellänge effektiv wiederherstellen. Diese Anpassung der Schlüssellänge wirkt der durch den Grover-Algorithmus erzielten quadratischen Beschleunigung entgegen und erhält damit die praktische Sicherheit der symmetrischen Kryptografie in einer von Quantencomputern dominierten Umgebung. [6].

Die derzeit verbreiteten asymmetrischen Kryptografiealgorithmen basieren auf mathematischen Problemstellungen, die laut [6] bisher nicht vollständig gelöst wurden. Ein wesentliches Sicherheitsrisiko dieser Algorithmen liegt in ihrer Anfälligkeit gegenüber Quantencomputern, die besonders effizient parallele Berechnungen durchführen können, die auf ein einzelnes Endergebnis abzielen. Durch die Nutzung der Superposition von Qubits ist es möglich, sämtliche erforderlichen Berechnungen eines asymmetrischen Algorithmus parallel durchzuführen und anschließend das Ergebnis zu messen. Um die inhärente Parallelitätsfähigkeit von Quantencomputern zu umgehen, könnten zukünftige Algorithmen entwickelt werden, die multiple, voneinander unabhängige Ergebnisse erfordern. Dieser Ansatz würde die Ausnutzung der vollen Parallelitätskapazität von Quantencomputern einschränken und könnte somit eine effektive Strategie zur Sicherung der asymmetrischen Kryptografie in einer zunehmend von Quantentechnologie dominierten Zukunft darstellen [6].

Aktuell werden die meisten Algorithmen im Bereich der PQK sechs verschiedenen Kategorien zugeordnet. Jede dieser Kategorien repräsentiert eine eigenständige Familie von mathematischen Problemen, deren Lösung auch für Quantencomputer als komplex gilt. Diese speziellen mathematischen Herausforderungen bilden die Basis für die Entwicklung der nächsten Generation von asymmetrischen Kryptografiealgorithmen. Im Jahr 2016 initiierte das NIST einen Standardisierungsprozess für PQK. Dieser Prozess zielt darauf ab, neue Schemata für digitale Signaturen und Public-Key-Verschlüsselung zu identifizieren und zu etablieren [6].

Post-Quantum-Kryptoalgorithmen werden einer gründlichen Sicherheitsanalyse unterzogen, um ihre Widerstandskraft gegenüber Quantenangriffen zu beurteilen. Diese Analyse berücksichtigt kritische Aspekte wie die Rechenkomplexität, die Beständigkeit gegenüber bekannten Angriffsmethoden und die Festlegung angemessener Schlüsselparameter, um ein erforderliches Sicherheitsniveau zu sichern [6].

Zusammenfassend kann festgestellt werden, dass die PQK sich mit der Untersuchung und Anwendung mathematischer Probleme und Strukturen befasst, die widerstandsfähig gegenüber den potenziellen Angriffen durch Quantencomputer sind. Ansätze wie gitter-basierte Kryptografie, code-basierte Kryptografie, multivariate Polynomkryptografie und hash-basierte Signaturen basieren auf theoretischen Annahmen bezüglich ihrer mathematischen Robustheit. Diese Annahmen sind darauf ausgerichtet, eine langfristige Sicherheit in einer Ära zu bieten, in der Quantencomputer eine bedeutende Rolle spielen. Diese mathematischen Prinzipien sind fundamental für die Entwicklung und Bewertung neuer kryptographischer Algorithmen und Protokolle in der post-quantencomputergestützten Zukunft [6].

2.3.1 Warum Post-Quantum-Kryptografie?

PQK ist von entscheidender Bedeutung, da sie auf die Herausforderungen reagiert, die sich durch den potenziellen Einsatz von Quantencomputern in der Zukunft ergeben. Die Notwendigkeit für PQK ergibt sich aus der Tatsache, dass Quantencomputer einige der grundlegenden mathematischen Probleme, auf denen viele aktuelle kryptografische Systeme basieren, erheblich schneller lösen könnten als herkömmliche Computer.

Ein Schlüsselaspekt dabei ist die Fähigkeit von Quantencomputern, Algorithmen zur Faktorisierung großer Zahlen oder zur Lösung des diskreten Logarithmusproblems in polynomialer Zeit zu bewältigen. Diese Probleme bilden die Grundlage für viele asymmetrische Verschlüsselungsalgorithmen.Wenn Quantencomputer diese Algorithmen mit Leichtigkeit überwinden können, werden herkömmliche Verschlüsselungsmethoden angreifbar und unsicher.

Bestimmte kryptografische Systeme, beispielsweise das RSA-Verfahren mit einem Schlüssel von 4000 Bits, sind konzipiert, um Widerstandsfähigkeit gegenüber Angriffen durch leistungsstarke klassische Computer zu bieten. Jedoch sind sie nicht darauf ausgelegt, Angriffen durch fortschrittliche Quantencomputer standzuhalten. Im Gegensatz dazu sind alternative kryptographische Methoden wie die McEliece-Verschlüsselung, die einen Schlüssel von vier Millionen Bits verwendet, sowohl gegen Angriffe durch hochleistungsfähige klassische Computer als auch gegen Angriffe durch leistungsstarke Quantencomputer resistent gestaltet. Diese unterschiedlichen Ansätze in der Kryptografie spiegeln die Notwendigkeit wider, Sicherheitsstrategien angesichts der sich entwickelnden Computertechnologien kontinuierlich anzupassen und weiterzuentwickeln [8].

Quantencomputer besitzen das Potenzial, bestimmte mathematische Herausforderungen, die als Grundlage vieler kryptographischer Systeme dienen, signifikant effizienter als konventionelle Computer zu lösen. Spezifisch könnten sie Aufgaben wie die Faktorisierung großer Zahlen oder das Lösen des diskreten Logarithmusproblems innerhalb polynomialer Zeit bewerkstelligen. Diese Fähigkeit resultiert aus der einzigartigen Quantenmechanik, die es Quantencomputern ermöglicht, komplexe Berechnungen durchzuführen, die für herkömmliche Computer unpraktikabel wären. Die Bewältigung solcher Probleme in polynomialer Zeit stellt eine wesentliche Abweichung von der aktuellen algorithmischen Landschaft dar, in der diese Aufgaben für klassische Computer nur in superpolynomialer oder exponentieller Zeit lösbar sind. Eine solche Entwicklung würde die Sicherheit bestehender Verschlüsselungsalgorithmen, die auf der rechnerischen Schwierigkeit dieser Probleme beruhen, untergraben und könnte weitreichende Auswirkungen auf die Informationssicherheit haben [8]. Ein Algorithmus, der in polynomialer Zeit arbeitet,

kann ein Problem in einer Zeit lösen, die proportional zu einer Potenz der Größe der Eingabedaten ist. Im Gegensatz zu exponentiellen Algorithmen, die mit der Eingabegröße exponentiell langsamer werden, skaliert ein polynomialer Algorithmus wesentlich besser mit zunehmender Problemgröße. Dies macht bestimmte Berechnungen, wie die Faktorisierung großer Zahlen, für Quantencomputer praktikabel, während sie für herkömmliche Computer äußerst zeitintensiv wären.

Laut [1, 9] ist die globale Gemeinschaft noch nicht für einen umfassenden Wechsel zur PQK bereit, was auf mehrere Faktoren zurückzuführen ist.

Erstens sind viele der Technologien im Bereich der PQK noch nicht ausreichend entwickelt. Dies umfasst sowohl die Effizienz der Algorithmen als auch ihre Integration in bestehende Infrastrukturen. Eine breite Implementierung dieser Technologien erfordert weiterführende Forschung und Entwicklung, um die Reife und Praktikabilität dieser Systeme sicherzustellen.

Zweitens besteht eine gewisse Unsicherheit über die Notwendigkeit der PQK. Während einige Experten die Entwicklung von leistungsfähigen Quantencomputern als unvermeidlich ansehen, wird dies von anderen als weniger dringliche oder sogar hypothetische Bedrohung betrachtet. Diese Unsicherheit erschwert die Einschätzung des tatsächlichen Bedarfs und der Dringlichkeit in der Entwicklung von PQ-Kryptografiesystemen.

Drittens birgt das Zögern oder die Verzögerung in der Forschung und Entwicklung von PQK das Risiko, kritische Zeit zu verlieren. Sollte sich herausstellen, dass Quantencomputer eine reale und unmittelbare Bedrohung für die Sicherheit bestehender kryptografischer Systeme darstellen, könnte der Mangel an Vorbereitung und fortgeschrittenen Sicherheitslösungen gravierende Folgen haben. Dies unterstreicht die Notwendigkeit, trotz der bestehenden Unsicherheiten, proaktiv in die Forschung und Entwicklung von PQK zu investieren, um potenzielle Risiken zu minimieren und die digitale Sicherheit langfristig zu gewährleisten.

2.3.2 Herausforderungen durch Quantencomputer

Wie können neue klassische Kryptosysteme entworfen werden, die auch in Gegenwart von Quantencomputern sicher bleiben? Solche Systeme wären von großer Bedeutung, da sie jetzt implementiert werden könnten, aber sicher bleiben würden, wenn Quantencomputer gebaut werden. Von den ursprünglich 69 Kandidaten wurden 25 bis 30 entweder vollständig gebrochen oder erheblich angegriffen [1]. Die Tabelle 2.1 zeigt den aktuellen Status einiger dieser Kryptosysteme.

Kryptosystem	Durch Quantenalgorithmen gebrochen?
RSA Public Key Verschlüsselung	Gebrochen
Diffie-Hellman Schlüsselaustausch	Gebrochen
Elliptische Kurvenkryptografie	Gebrochen
Buchmann-Williams Schlüsselaustausch	Gebrochen
Algebraisch Homomorph	Gebrochen
McEliece Public Key Verschlüsselung	Noch nicht gebrochen
NTRU Public Key Verschlüsselung	Noch nicht gebrochen
Gitter-basierte Public Key Verschlüsselung	Noch nicht gebrochen

Tabelle 2.1: Aktueller Stand der Sicherheit klassischer Kryptosysteme im Zusammenhang mit Quantencomputern [1].

2.3.3 Ziele und Prinzipien der Post-Quantum-Kryptografie

Ein zentrales Prinzip der PQK ist die Vielseitigkeit. Dies bedeutet, dass die entwickelten Algorithmen eine breite Palette von kryptografischen Anwendungen abdecken sollen. Dazu gehören digitale Signaturen, Verschlüsselungsverfahren und Schlüsselaustauschprotokolle. Diese Vielseitigkeit gewährleistet, dass PQK in einem breiten Spektrum von Anwendungsszenarien eingesetzt werden kann, um die digitale Sicherheit umfassend zu gewährleisten [10].

Ein weiteres entscheidendes Ziel der PQK ist die Interoperabilität. PQK-Algorithmen sollen reibungslos mit vorhandenen kryptografischen Standards interagieren können. Dies erleichtert die Integration der neuen Algorithmen in bestehende Systeme und Infrastrukturen, ohne die Notwendigkeit einer vollständigen Überarbeitung oder Ersetzung etablierter Protokolle [10].

Die Nachhaltigkeit der entwickelten Algorithmen ist ebenfalls von großer Bedeutung. Diese Algorithmen sollen langfristig sicher sein und den potenziellen Fortschritten in der Quantencomputertechnologie standhalten. Dies erfordert eine kontinuierliche Evaluierung und Anpassung der Algorithmen an die neuesten Erkenntnisse und Entwicklungen im Bereich der Quantencomputertechnologie [11].

Effizienz ist ein weiteres wesentliches Prinzip. PQK-Algorithmen sollen praktikabel und effizient in der Anwendung sein, um ihre breite Akzeptanz und Implementierung in verschiedenen Anwendungsgebieten zu ermöglichen. Dies bezieht sich sowohl auf die Rechenleistung als auch auf den Speicherbedarf der Algorithmen, um auch in ressourcenbeschränkten Umgebungen anwendbar zu sein [9].

Die Grundlage für die Entwicklung von PQK bildet die quantenresistente Mathematik. Es werden neue mathematische Konzepte und Ansätze erforscht und entwickelt, die gegenüber den speziel-

len Angriffsmethoden von Quantencomputern widerstandsfähig sind. Dies beinhaltet die Identifizierung und Nutzung von mathematischen Problemen, für die keine effizienten Quantenalgorithmen bekannt sind [11].

Diese Prinzipien und Ziele reflektieren das Bestreben der PQK, robuste Sicherheitslösungen für die kommende Ära der Quantencomputer zu bieten, die sowohl praktisch umsetzbar als auch langfristig sicher sind.

3 Quanten-Algorithmen in der Kryptografie

Die Entwicklung von Quantencomputern und die Einführung von Quantenalgorithmen wie Shor's und Grover's Algorithmus haben tiefgreifende Auswirkungen auf die heutige Kryptografie. Insbesondere stellt Shor's Algorithmus eine erhebliche Bedrohung für Public-Key-Verschlüsselungssysteme dar, die auf der Schwierigkeit der Faktorisierung des Produkts zweier großer Primzahlen, basieren. Diese Charakteristik ist zentral für die Sicherheit von Systemen wie RSA, einem grundlegenden Bestandteil der modernen asymmetrischen Kryptografie [12].

In diesem Kapitel werden Shor's und Grover's Algorithmen und ihre Auswirkungen auf die Kryptografie detailliert beleuchtet. Es wird erörtert, wie sich die Kryptografie an die durch Quanten-Algorithmen entstehenden Herausforderungen anpassen kann und welche Strategien für die Entwicklung sicherer Kryptosysteme in einer zukünftigen Welt, die stark von Quantencomputertechnologie beeinflusst ist, erforderlich sind.

3.1 Shor's Algorithmus

der effizient die Faktorisierung großer Zahlen ermöglicht. Diese Entwicklung hat weitreichende Konsequenzen für die Sicherheit von Verschlüsselungssystemen wie RSA, deren Sicherheitsannahmen auf der Unpraktikabilität der Faktorisierung großer Zahlen durch klassische Computer beruhen [13].

Die Fähigkeit, RSA und andere Public-Key-Verschlüsselungssysteme mittels Quantenalgorithmen effektiv zu kompromittieren, hat maßgeblich zur Förderung der Forschung in der PQK beigetragen. Infolgedessen konzentrieren sich laut [13] Forscher darauf, neue kryptografische Systeme zu entwickeln, die widerstandsfähig gegen Angriffe durch Quantencomputer sind. [13].

Shor's Algorithmus kombiniert zwei unterschiedliche Quantenverfahren, die sowohl das Problem der Primfaktorzerlegung als auch das diskrete Logarithmusproblem lösen können, auf denen die Sicherheit heutiger Kryptosysteme basiert. Während klassische Methoden für diese Probleme

exponentielle Laufzeiten benötigen, entwickelte Shor Algorithmen, die auf Wahrscheinlichkeitsprinzipien basieren und in polynomieller Zeit operieren. Er erreichte dies durch den Einsatz der Quanten-Fourier-Transformation für die Ermittlung von Periodizitäten, ein Schlüsselelement, das es ermöglicht, die Struktur der zu faktorisierenden Zahl effizient zu enthüllen [6].

Obwohl Shor's Algorithmus auf Wahrscheinlichkeitsprinzipien basiert und nicht garantiert, dass eine Zahl beim ersten Versuch faktorisiert wird, steigt die Erfolgswahrscheinlichkeit, einen Faktor zu finden, mit jeder Wiederholung des Algorithmus [6].

Im verbreiteten RSA Public-Key-System besteht der öffentliche Schlüssel aus einem Produkt $N = pq$ zweier geheimer Primzahlen p und q. Die Sicherheit von RSA beruht auf der Herausforderung, die Primfaktoren p, q der Zahl N zu ermitteln. 1994 präsentierte Shor einen effizienten Quantenalgorithmus, der in der Lage ist, die Primfaktorzerlegung jeder positiven ganzen Zahl N schnell durchzuführen [7].

Laut [7] wurden in der Forschung erhebliche Anstrengungen unternommen, um die spezifischen Anforderungen von Shor's Algorithmus zu analysieren und zu optimieren, besonders hinsichtlich der Quantenressourcen wie Qubits und der Anzahl der benötigten Qubit-Operationen. Ein spezielles Design von Shor's Algorithmus erfordert $O(n^3 \log n)$ Operationen unter Verwendung von $2n + 3$ Qubits für Zahlen $N = pq$, die in n Bits dargestellt werden können. Interessanterweise besteht die Möglichkeit, die Anzahl der Operationen zu verringern, was allerdings zu einem erhöhten Bedarf an Qubits führt [7].

Shor's Algorithmus nutzt die Prinzipien der Quantenmechanik, um eine effiziente Faktorisierung großer Zahlen zu ermöglichen. Der Kern des Algorithmus besteht darin, eine interne Bewertung einer periodischen Funktion innerhalb einer Superposition aller möglichen Eingaben eines definierten Bereichs zu implementieren. Mathematisch wird die zugrunde liegende Funktion als $e^{a \cdot x} \mod N$ definiert, wobei a eine zufällige, mit N teilerfremde ganze Zahl ist.

Der Algorithmus folgt einem mehrstufigen Prozess:

1. Zuerst wird eine Quantensuperposition aller möglichen Eingabewerte erstellt.
2. Anschließend wird eine Quanten-Fourier-Transformation angewandt, um eine Näherungssuperposition der Perioden dieser Funktion zu erzeugen.
3. Nach der Anwendung der Quanten-Fourier-Transformation wird die resultierende Superposition gemessen, um zufällig eine Periode der Funktion zu identifizieren.

Shor's Algorithmus nutzt eine Schlüsseleigenschaft von Zahlen, die keine Primzahlpotenz sind, aus. Eine Primzahlpotenz ist eine Zahl, die als Potenz einer Primzahl ausgedrückt werden kann, wie z.B. 2^3 oder 5^2. Im Gegensatz dazu haben Zahlen, die keine Primzahlpotenz sind, mehr als einen Faktor (außer 1 und sich selbst). Der Algorithmus ist in der Lage, die Periodizität einer quantenmechanischen Superposition zu nutzen, um diese zusätzlichen Faktoren effizient zu identifizieren. Daher kann, wenn N keine Primzahlpotenz ist, die Identifikation einer zufälligen Periode mit hoher Wahrscheinlichkeit einen Faktor von N aufdecken. Dies macht Shor's Algorithmus besonders mächtig für die Faktorisierung großer Zahlen und stellt eine signifikante Bedrohung für viele derzeitige Verschlüsselungsmethoden dar, die auf dem Problem der Faktorisierung großer Zahlen basieren [7].

Diese Algorithmen erfordern bei Anwendung auf weit verbreitete öffentliche Schlüsselgrößen für RSA und ECC Milliarden von Operationen auf Tausenden von logischen Qubits. Fehlertolerante Angriffe könnten Billionen von Operationen auf Millionen von physischen Qubits erfordern. Obwohl bisher keine Hindernisse für das erfolgreiche Skalieren zu diesen Größen identifiziert wurden, ist es ratsam, sich gegen die Möglichkeit zu verteidigen, dass solche Angriffe erfolgreich sein könnten [7].

Angesichts der rasanten Entwicklungen im Bereich der Quantencomputertechnologie ist es wahrscheinlich, dass Shor's Algorithmus in Zukunft eine noch größere Rolle in der Kryptografie spielen wird. Die Forschung konzentriert sich darauf, sowohl die Technologie der Quantencomputer als auch die kryptografischen Techniken weiterzuentwickeln, um die Sicherheit in der Ära der Quantencomputer zu gewährleisten [7].

3.2 Grover's Algorithmus

Es handelt sich bei Grover's Algorithmus um einen quantenmechanischen Suchalgorithmus, der in einer unsortierten Datenbank in $O(\sqrt{n})$ sucht, eine signifikante Verbesserung gegenüber dem $O(n)$-Problem bei klassischen Computern [6]. Dieser Algorithmus ist probabilistisch, was bedeutet, dass er mehrmals wiederholt werden kann, um die Wahrscheinlichkeit eines erfolgreichen Suchergebnisses zu erhöhen [14, 7].

Jede Grover-Iteration beinhaltet eine Suche, und durch wiederholte Iterationen lässt sich die Wahrscheinlichkeit, das gesuchte Element in einer Datenbank zu finden, erhöhen. Darüber hinaus kann Grover's Algorithmus auch für andere Aufgaben eingesetzt werden, wie zum Beispiel um den Mittelwert und Median von Daten zu bestimmen, den inversen Wert einer Funktion zu

finden und andere. Diese Anwendungen machen ihn zu einem wertvollen Werkzeug für quantenmechanische Kryptanalytiker, um kryptografische Algorithmen zu knacken oder Schlüssel in symmetrischen Kryptosystemen zu suchen [15, 6].

Viele kryptografische Systeme sind potenziell von Grover's Algorithmus betroffen, der 1996 eingeführt wurde [16]. Dieser Algorithmus bildet auch die Grundlage für zahlreiche, wenn auch nicht alle, positive Anwendungen, die für Quantencomputer identifiziert wurden.

Ursprünglich beschrieb Grover seinen Algorithmus als die Suche in einer ungeordneten Datenbank der Größe N mit N quantenmechanischen Abfragen. Eine genauere Betrachtung zeigt jedoch, dass es besser ist, Grover's Algorithmus als eine Methode zur Suche nach Lösungen x für die Gleichung $f(x) = 0$ zu beschreiben. Wenn etwa jede N-te Eingabe eine Lösung darstellt, findet Grover's Algorithmus eine solche Lösung mit nur etwa $\sqrt{N}$ quantenmechanischen Auswertungen von f [14]. Wenn f schnell durch eine kleine Schaltung ausgewertet werden kann, sind die notwendigen Qubit-Operationen relativ gering. Dies ist oft der Fall bei Funktionen f, die in der Kryptografie verwendet werden [15].

Ein konkretes Beispiel ist der 'Advanced Encryption Standard' (AES), ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus. Angenommen, ein Benutzer hat bekannte 128-Bit-Klartexte '7' und '8' mit einem geheimen 128-Bit-AES-Schlüssel k verschlüsselt, was zu einem 256-Bit-Chiffretext $c = (AES_k(7), AES_k(8))$ führt. Die Funktion $f(x) = (AES_x(7), AES_x(8)) - c$ kann schnell (etwa 20.000 Bit-Operationen) von einer kleinen Schaltung ausgewertet werden. Grover's Algorithmus ist dann in der Lage, mit etwa 264 quantenmechanischen Auswertungen von f eine Lösung zu finden, die sehr wahrscheinlich dem Schlüssel k entspricht [15].

Die Effizienzsteigerung von Grover von N auf $\sqrt{N}$ ist beachtlich, aber nicht so disruptiv wie die Beschleunigung, die durch Shor's Algorithmus für Probleme wie die Primzahlfaktorisierung erreicht wird [16]. Zudem müssen die quantenmechanischen Auswertungen von Grover sequenziell erfolgen, wodurch die Gesamteffizienz begrenzt wird [14]. Um dieses Problem zu quantifizieren, definieren wir T als die Anzahl der seriellen Auswertungen, die in einer gegebenen Zeit durchgeführt werden können. Wenn beispielsweise f in einer Nanosekunde ausgewertet werden kann und ein Jahr für die Berechnung zur Verfügung steht, ist $T \approx 2^{55}$. Ist N größer als T, kann Grover's Algorithmus nicht weniger als N/T Auswertungen nutzen, die auf N/T^2 parallele Quantenprozessoren verteilt sind [7].

Dies stellt zwar eine Verbesserung gegenüber präquantenmechanischen Techniken dar, aber die Kosten von Qubit-Operationen könnten diese Effizienzsteigerung zunichte machen, was den Nut-

zen von Grover's Algorithmus einschränkt, selbst wenn skalierbare Quantencomputer realisiert und Shor's Algorithmus erfolgreich implementiert werden [15].

Andererseits, wenn Qubit-Operationen klein genug und schnell genug sind, könnte Grover's Algorithmus viele kryptografische Systeme bedrohen, die auf eine Sicherheit von 2^{128} ausgelegt sind, wie z. B. 128-Bit-AES-Schlüssel. In solchen Fällen empfehlen wir den Wechsel zu 256-Bit-AES-Schlüsseln, da die zusätzlichen Kosten in der Regel gering sind. 'Informationstheoretische' MACs wie GMAC und Poly1305 sind bereits ohne Modifikationen gegen Quantenangriffe sicher, da ihre Sicherheitsanalyse von einem Angreifer mit unbegrenzter Rechenkapazität ausgeht [16].

4 Post-Quanten Kryptosysteme

In diesem Kapitel wird die Bedrohung für klassische Kryptografie durch Quantencomputer beleuchtet. Diese sind in der Lage, traditionelle kryptografische Algorithmen zu gefährden. Dies erfordert die Entwicklung von quantenresistenten Kryptosystemen.

Zu den wichtigsten Kategorien der PQK gehören:

- Gitter-basierte Kryptografie
- Code-basierte Kryptografie
- Hash-basierte digitale Signaturen
- Multivariate Kryptografie

In Anbetracht der fortschreitenden Entwicklung von Quantencomputern, und deren Auswirkungen auf die Kryptografie, stellt sich die dringende Frage nach der Zukunftsfähigkeit bestehender kryptografischer Verfahren. Die fortschrittlichen Fähigkeiten von Quantencomputern könnten zu einer potenziellen Obsoleszenz etablierter Public-Key-Algorithmen führen. Diese Algorithmen, die bisher den Standard in der Kryptografie darstellen, sind besonders anfällig gegenüber Quantencomputern, da sie Probleme in einer Weise lösen können, für die klassische Computer exponentiell lange benötigen würden [7].

In diesem Kontext wird die Entwicklung von kryptographischen Systemen, die den neuen Sicherheitsanforderungen der Quantencomputertechnologie gerecht werden, entscheidend. Die PQK zielt darauf ab, Lösungen zu entwickeln, die sowohl benutzerfreundlich als auch flexibel sind und gleichzeitig das Vertrauen in ihre Sicherheit aufrechterhalten. Der Fokus zukünftiger Forschungen liegt dabei auf der Weiterentwicklung dieser Kryptosysteme und ihrer Vorbereitung für den breiten Einsatz [7].

Die Notwendigkeit für ein Umdenken in der Kryptografie betont die Bedeutung von alternativen Systemen, die sowohl gegen klassische als auch gegen Quantencomputer resistent sind. Diese neuen Ansätze, die sich in der Entwicklung befinden, sind entscheidend, um die Sicherheit in der

Ära der Quantenüberlegenheit zu gewährleisten. Ihre erfolgreiche Implementierung wird nicht nur die Fortsetzung sicherer digitaler Kommunikation ermöglichen, sondern auch einen wichtigen Schritt in der Anpassung unserer Sicherheitstechnologien an das Zeitalter der Quantencomputertechnologie darstellen [8].

Das NIST hat Initiativen zur Entwicklung quantensicherer Algorithmen gestartet. Diese umfassen die Bewertung von Algorithmen aus aller Welt, um Standards für die Ära der Quantencomputer zu etablieren. Es werden die Auswirkungen von Quantencomputern auf aktuelle kryptographische Algorithmen sowie verschiedene Algorithmen der PQK, die sich als resistent gegen Angriffe durch Quantencomputer erwiesen haben, untersucht. Zudem wird ein Überblick über vielversprechende Kandidaten für den NIST-Standard gegeben und zukünftige Forschungsrichtungen im Bereich der PQK aufgezeigt [6].

4.1 Kategorien von Post-Quantum-Kryptosystemen

Die Landschaft der PQK ist reich an Vielfalt, geprägt von innovativen Ansätzen, um den Herausforderungen leistungsstarker Quantencomputer zu begegnen. In dieser Sektion werden verschiedene Kategorien von PQ-Kryptosystemen beleuchtet, wobei jede Kategorie einzigartige Prinzipien und Methoden verkörpert.

Im bevorstehenden Kapitel 6 werde ich eine detaillierte Analyse der Ansätze in der PQK durchführen. Hierbei werde ich mich auf die Konstruktion, die Funktionsweise und die Sicherheitsanalyse dieser Ansätze konzentrieren. Dieser Abschnitt des Textes wird es ermöglichen, ein umfassendes Verständnis für PQK zu entwickeln und die Bedeutung dieser Technologien zu betonen.

Gitter-basierte Kryptosysteme

Gitter-basierte Kryptografie, ein führender Ansatz in der PKQ, unterscheidet sich von herkömmlichen Kryptosystemen durch ihre Grundlage auf Worst-Case-Problemen, speziell mathematischen Gitterproblemen. Ihre Sicherheit beruht auf der Annahme, dass es keine effizienten klassischen oder Quantenalgorithmen gibt, die diese Gitterprobleme lösen können. Die außergewöhnliche Sicherheit von Gitterkryptosystemen wird durch ihre Worst-Case-Härte untermauert, was bedeutet, dass die Schwierigkeit, ein solches System zu brechen, mathematisch gleichbedeutend ist mit der Herausforderung, harte Gitterprobleme wie das Shortest Vector Problem (SVP), das

Closest Vector Problem (CVP) und Learning With Errors (LWE) zu lösen. Ihre dominante Position in der PQK-Landschaft wird durch die Aufnahme von zwei Standards aus diesem Ansatz in die PQK-Standards unterstrichen [6, 17].

Code-basierte Kryptosysteme

Die Sicherheit der code-basierten Kryptografie basiert auf der Schwierigkeit der Dekodierung von zufälligen linearen Codes, die zur NP-vollständigen Klasse gehören [17]. Prominente Beispiele sind das McEliece- und das Niederreiter-Kryptosystem [18, 19], die auf der Herausforderung basieren, den korrekten Code aus vielen Möglichkeiten zu identifizieren, was eine erhebliche Schwierigkeit für Angreifer darstellt. Diese Systeme nutzen fehlerkorrigierende Codes, um die Zuverlässigkeit von Kommunikationssystemen zu verbessern, indem sie Daten für die Fehlerkorrektur während der Übertragung integrieren. Ihr Hauptvorteil ist die Resistenz gegen Quantenangriffe, was sie zu starken Kandidaten für die PQK macht. Eine aktuelle Herausforderung ist jedoch die Größe der Schlüssel [20], weshalb Forschungen darauf abzielen, die Effizienz und Praktikabilität dieser Kryptosysteme zu verbessern.

Hash-basierte Kryptosysteme

Hash-basierte Kryptografie, ein wichtiger Bestandteil der PQK, basiert auf der Sicherheit symmetrischer kryptografischer Hashfunktionen. Ein bekanntes Beispiel ist Merkles Hash-Baum-Signatursystem, das auf sicheren Hashfunktionen für einmalige Signaturen aufbaut [21]. Im Rahmen der PQK beschränkt sich der hash-basierte Ansatz auf Signaturkonstruktionen, mit prominenten Beispielen wie das SPHINCS+, der einzigen erfolgreichen nicht-gitter-basierten Standardisierung des NIST-PQK-Wettbewerbs [17]. Die Sicherheit dieser Signatur beruht auf der Schwierigkeit, eine entsprechende Eingabe für einen gegebenen Hash-Ausgabestring zu finden, wie bei Lamports Einmalsignaturen [7].

Multivariate Kryptosysteme

Multivariate Kryptosysteme sind eine wichtige Klasse in der PQK, die mehrdimensionale Polynome, insbesondere quadratische Gleichungen, für
Verschlüsselungs- und Authentifizierungsfunktionen nutzen. Sie basieren auf der mathematischen Herausforderung, spezifische Gleichungssysteme über endlichen Körpern zu lösen [22].

Die Signaturen in multivariate Systemen basieren auf Polynomen, die auf quadratischen Gleichungen ohne quadratische Terme aufbauen, was sie zu einer effektiven Alternative in der PQK macht. Ihre Struktur stellt hohe Sicherheitsstandards sicher und bleibt praktikabel [7]. Diese Kategorien geben einen Einblick in die Vielfalt der PQ-Kryptosysteme, die jeweils auf spezifischen mathematischen Grundlagen und Sicherheitsmodellen basieren, entscheidend für die Auswahl und Implementierung geeigneter Kryptosysteme in einer zunehmend quantenbedrohten Welt.

Zusammenfassung

Die folgende Auflistung bietet eine detaillierte Übersicht über die Implementierungseigenschaften verschiedener Schemata in der asymmetrischen PQK. Sie unterstreicht die Vielfalt und Unterschiedlichkeit in den Bereichen Signaturfähigkeit, Verschlüsselungskapazität, Schlüsselgrößen, Datentypen, Kernoperationen und kryptografische Reife der einzelnen Schemata. Diese Diversität in den technischen Spezifikationen und Reifegraden der Schemata macht die Forschung und Entwicklung in der PQK zu einem komplexen Bereich [10].

Hash-basierte Kryptosysteme:
Signatur: Ja – unterstützt digitale Signaturen
Verschlüsselung: Nein – nicht für Verschlüsselungszwecke geeignet
Schlüsselgröße: 20 Bytes
Daten Typen: Hash-Ausgaben
Kernoperationen: Hashing
Kryptografische Reife: Hoch – weit entwickelt und als sicher angesehen

Multivariate Kryptosysteme:
Signatur: Ja – kann für digitale Signaturen verwendet werden
Verschlüsselung: Nein – nicht für Verschlüsselungszwecke geeignet
Schlüsselgröße: 10k Bytes
Daten Typen: GF(2m), Lösung linearer Gleichungssysteme (LSE)
Kernoperationen: Matrixmultiplikation
Kryptografische Reife: Niedrig bis mittel – noch in Entwicklung oder nicht vollständig etabliert

Gitter-basierte Kryptosysteme:
Signatur: Vielleicht – unsicher oder abhängig von der spezifischen Implementierung

Verschlüsselung: Ja – geeignet für Verschlüsselungszwecke
Schlüsselgröße: <0.1k Bytes
Daten Typen: GF(2m) Matrixmultiplikation
Kernoperationen: Nicht spezifiziert
Kryptografische Reife: Mittel – in einem mittleren Entwicklungsstadium

Code-basierte Kryptosysteme:
Signatur: Teuer – digitale Signaturen sind möglich, aber mit hohem Aufwand verbunden
Verschlüsselung: Ja – geeignet für Verschlüsselungszwecke
Schlüsselgröße: 100k Bytes
Daten Typen: GF(2m) Matrixmultiplikation, Decodierung
Kernoperationen: Nicht spezifiziert
Kryptografische Reife: Hoch, jedoch mit Vorsicht zu behandeln – weit entwickelt, aber es gibt möglicherweise Bedenken oder Einschränkungen

5 Standardisierung von Post-Quantum-Kryptografie

Dieses Kapitel widmet sich der Untersuchung des Standardisierungsprozesses von PQK durch das National Institute of Standards and Technology (NIST). Wir werden die Phasen dieses Prozesses, die Auswahl von Algorithmen und deren Bewertung sowie die Bedeutung dieses Schrittes für die Informationssicherheit näher beleuchten.

5.1 NISTPQK-Standardisierungsprozess

Im Prozess der PQK-Standardisierung des NIST werden öffentliche Schlüssel-Kryptografiealgorithmen durch einen wettbewerbsähnlichen öffentlichen Prozess ausgewählt. Die neuen Standards für öffentliche Schlüsselkryptografie sollen zusätzliche Algorithmen für digitale Signaturen, öffentliche Schlüsselverschlüsselung und Schlüssel-Etablierungsverfahren umfassen, die die bestehenden Standards ergänzen [23].

Im Dezember 2016 initiierte das NIST einen Prozess zur Standardisierung von PQK. Dieser Prozess fokussierte auf die Entwicklung kryptografischer Algorithmen, die sowohl gegen klassische als auch gegen Quantencomputer sicher sind. Zu den betrachteten Kategorien gehören PKE-Schemata (Public-Key-Encryption-Schemata) und KEMs (Key Encapsulation Mechanisms), sowie digitale Signaturen. PKE-Schemata sind Algorithmen für die öffentliche Schlüsselverschlüsselung, während KEMs Mechanismen zur sicheren Schlüsselübertragung sind. In jeder Phase des PQK-Wettbewerbs veröffentlichte NIST Berichte, die die ausgewählten Verfahren analysierten und die Gründe für ihre Auswahl erläuterten [24].

Laut [17] weisen Prognosen darauf hin, dass gängige Algorithmen wie RSA bis zum Jahr 2030 durch Quantencomputer gefährdet sein könnten. Dieser Standardisierungsprozess repräsentiert die bedeutendste gemeinschaftliche Anstrengung in der Entwicklung und Bewertung von Algorithmen für quantensichere Kryptografie. In mehreren Runden, begleitet von entsprechenden

Konferenzen, erfolgt die Eliminierung einiger Algorithmen und die vertiefte Untersuchung anderer [17].

Für den NISTPQK-Wettbewerb wurden in der ersten Runde 26 der 69 eingereichten Algorithmen ausgewählt, basierend auf Kriterien wie Sicherheit, Kosten und Leistung sowie Algorithmus- und Implementierungsmerkmale. Nach Runde 2 hat das NIST 15 Algorithmen ausgewählt, die auf verschiedenen schwer zu lösenden Problemen basieren, um die Sicherheit zu gewährleisten [6].

Im Bericht über die dritte Runde des Standardisierungsprozesses werden diese 15 Kandidaten-Algorithmen bewertet, basierend auf öffentlichem Feedback und interner Überprüfung. Für die Standardisierung ausgewählt wurden der öffentliche Schlüssel-Verschlüsselungs- und Schlüssel-Etablierungsalgorithmus CRYSTALS-KYBER sowie die digitalen Signaturverfahren CRYSTALS-Dilithium, FALCON und SPHINCS+. NIST empfiehlt CRYSTALS-Dilithium als primären Algorithmus zur Implementierung. Zusätzlich werden vier alternative Kandidaten für Schlüssel-Etablierungsverfahren in die vierte Runde der Bewertung vorrücken: BIKE, Classic McEliece, HQC und SIKE. Diese Kandidaten werden weiterhin für eine zukünftige Standardisierung in Betracht gezogen. Die Finalisten wurden aufgrund ihrer Vielseitigkeit und der Aussicht auf baldige Standardisierung nach Abschluss der dritten Runde ausgewählt. Die alternativen Kandidaten galten als mögliche zukünftige Standardisierungsoptionen, eventuell nach weiteren Evaluierungsrunden. Einige dieser Alternativen, obwohl leistungsschwächer, könnten aufgrund hoher Sicherheitsüberzeugung ausgewählt werden, während andere noch zusätzliche Analysen erfordern. Des Weiteren wurden einige Alternativen aufgrund des Wunsches nach Diversität in zukünftigen Standards oder aufgrund ihres Verbesserungspotenzials ausgewählt. NIST plant außerdem einen neuen Aufruf für Vorschläge für öffentliche Schlüsseldigital-Signaturalgorithmen, um sein Signatur-Portfolio zu erweitern und zu diversifizieren [23].

Das öffentliche Interesse an dieser Initiative wuchs, da große Quantencomputer eine reale Möglichkeit darstellen [24]. Die neuesten Fortschritte in der Quanteninformatik, wie die Entwicklung eines 53-Qubit-
Quantencomputers durch Google, haben die Debatte über die Sicherheit aktueller Public-Key-Algorithmen und digitaler Signaturen verändert. Obwohl dieser Quantencomputer noch nicht ausreichend leistungsfähig ist, um Public-Key-Kryptografie zu gefährden, hat er laut [6] die Frage von „ob“ sie gebrochen werden können, zu „wann“ sie gebrochen werden können, verändert [6].

5.2 Bedeutung von Standards des NIST in der Kryptografie

In diesem Kontext werden die formalen Konzepte und Anforderungen präsentiert, die von Standardisierungsgremien festgelegt wurden. Insbesondere umfassen die Standardisierungsbemühungen des NIST klar definierte Metriken für drei wesentliche Aspekte: Sicherheit, Implementierungskosten und algorithmische Eigenschaften. Andere Standardisierungsorganisationen und -projekte legen überwiegend anwendungsspezifische Kriterien oder Vorschriften anstelle von Metriken fest [17].

Sicherheit: Das Hauptkriterium für die Bewertung von Post-Quantum-Kryptosystemen ist das erreichte Sicherheitsniveau. Das NIST hat fünf Sicherheitsstufen definiert, die auf symmetrischen kryptographischen Primitiven basieren:

- **Stufe Eins** entspricht dem Brechen von AES-128. AES steht für Advanced Encryption Standard, und die Zahl 128 gibt die Schlüssellänge in Bit an. AES-128 ist bekannt für seine Sicherheit und Effizienz in der Verschlüsselung.
- **Stufe Zwei** beinhaltet das Auffinden einer Kollision bei einer 256-Bit-Hash-Funktion. Eine Kollision in einer Hash-Funktion tritt auf, wenn zwei unterschiedliche Eingaben denselben Hash-Wert ergeben.
- **Stufe Drei** umfasst das Brechen von AES-192, einer stärkeren Variante des AES mit einer Schlüssellänge von 192 Bit.
- **Stufe Vier** bezieht sich auf das Auffinden einer Kollision bei SHA-384. SHA-384 steht für Secure Hash Algorithm 384 und ist Teil der SHA-2-Familie von Hash-Funktionen.
- **Stufe Fünf** umfasst eine Schlüsselsuche bei AES-256, der stärksten Variante des AES mit einer Schlüssellänge von 256 Bit.

Diese Sicherheitsstufen des NIST definieren die Stärke der Kryptografie in Bezug auf die Schwierigkeit, verschiedene etablierte Verschlüsselungs- und Hash-Methoden zu kompromittieren. Der Fokus des NIST-Wettbewerbs liegt auf den ersten drei Stufen, jedoch wird auch die Einreichung für Stufe fünf ermutigt. Zusätzlich sind Sicherheitseigenschaften wie Vorwärts-/Rückwärtssicherheit, Rückwärtskompatibilität und Widerstand gegen Angriffe wie Seitenkanal- und Mehrschlüsselangriffe von Bedeutung. Sowohl das Random Oracle Model (ROM) als auch das Quantum Random Oracle Model (QROM) spielen eine Rolle, wobei das QROM Quantengegnern und -operationen Rechnung trägt. PKE/KEM und Signaturschemata müssen bestimmte Sicherheitsstandards erfüllen [17].

Kosten, Leistung & Implementierung: Die Kosten umfassen Faktoren wie die Größe von Schlüsseln, Chiffretexten und Signaturen sowie Speicher- und Codegrößenbeschränkungen. Die Leistungsbewertung berücksichtigt Rechenkosten, Kommunikationsintensität und Entschlüsselungsfehlerraten, unter Berücksichtigung von Plattform, Softwareeffektivität und Hardwareanforderungen. Die Schlüsselgenerierung ist besonders wichtig und muss in verschiedenen Systemaspekten berücksichtigt werden. Bei PQ-Kryptosystemen ist die Begrenzung der Nachrichtenanzahl pro Schlüssel zu beachten, was besondere Herausforderungen für IoT-Geräte darstellen kann. IoT-Geräte sind vernetzte Geräte des „Internet of Things“, die Daten sammeln, austauschen und verarbeiten. Bei der Bewertung von Post-Quantum-Kryptografiealgorithmen spielen Kosten- und Leistungsfaktoren eine entscheidende Rolle, insbesondere in Bezug auf die Begrenzungen von IoT-Geräten. Dies umfasst die Berücksichtigung der Schlüsselgröße, Rechenkosten, Kommunikationsanforderungen und die Schlüsselgenerierung, um die Effizienz und Sicherheit dieser Geräte in einer post-quanten Ära sicherzustellen. [17].

Angriffssicherheit: Seitenkanalangriffe nutzen Implementierungsschwächen, um sensible Daten zu extrahieren. Sie beinhalten die Beobachtung interner Schaltkreise und das Sammeln und Analysieren durchgesickerter Informationen. Verschiedene Methoden wie Akustik, Zeitmessung, Energieanalyse und elektromagnetische Emissionen werden angewendet [17].

Vielfalt und Vielseitigkeit: Die Auswahl von Kandidaten für die Standardisierung berücksichtigt Diversitäts- und Vielseitigkeitsmetriken, um eine breite Sicherheitsabdeckung zu gewährleisten. Diese Metriken berücksichtigen Variationen in mathematischer Komplexität und Sicherheitsannahmen sowie die Integration verschiedener kryptographischer Primitive [17].

Exotische Merkmale und Einfachheit: Standardisierungsgremien beachten auch die Unterstützung für exotische Merkmale wie Blind-/Gruppen-/Ringsignaturen, FHE, MPC, SS usw. Einfachheit und Einzigartigkeit in Design und Annahmen sind ebenfalls wichtige, wenn auch implizite, Kriterien. Blinde Signaturen ermöglichen das Signieren von Nachrichten, ohne den Inhalt zu kennen. Gruppen- und Ringsignaturen gewährleisten Anonymität bei der Signierung. Fully Homomorphic Encryption (FEH) ermöglicht die Berechnung auf verschlüsselten Daten. Multi-Party Computation (MPC) erlaubt sichere kooperative Berechnungen. Secret Sharing (SS) teilt Geheimnisse in Teile, um ihre Sicherheit zu gewährleisten [17].

6 Analyse von Post-Quantum-Kryptografie Ansätzen

Im Kontext der PQK ist der Übergang und die Migration von klassischen kryptographischen Systemen zu PQK-Algorithmen von großer Bedeutung. Die Entwicklung von Quantencomputern stellt eine erhebliche Bedrohung für herkömmliche Public-Key-Kryptografie dar, da sie weit verbreitete, klassiche Algorithmen gefährden können. Um dieser Herausforderung zu begegnen, hat das Gebiet der PQK erhebliches Wachstum erlebt, was zur Entwicklung einer vielfältigen Palette von Algorithmen geführt hat, die voraussichtlich quantenresistente Eigenschaften aufweisen. Dieses Kapitel wird eine vergleichende Analyse von code-basierten, gitter-basierten, hash-basierten und multivariaten kryptographischen Systemen durchführen, um ihre Stärken, Schwächen und Eignung in der PQ-Ära zu untersuchen.

Im Bereich der symmetrischen Kryptografie bieten Quantencomputer neue kryptoanalytische Möglichkeiten. Die Auswirkungen sind jedoch weniger dramatisch als bei asymmetrischer Kryptografie. Eine Erhöhung der Schlüssellänge auf 256 Bit scheint derzeit eine wirksame Gegenmaßnahme zu sein. Weitere Quantenangriffe auf symmetrische Verfahren sind bekannt, die dabei verwendeten Angriffsmodelle sind jedoch laut dem BSI in aktuellen Implementierungen oft nicht realistisch. [25].

6.1 Analyse ausgewählter Ansätze

Nach der umfassenden Betrachtung der Grundlagen des Quantencomputings und der Kryptografie sowie der spezifischen Herausforderungen der PQK, konzentriert sich die vorliegende Analyse auf die detaillierte Untersuchung konkreter Ansätze in diesem zukunftsweisenden Bereich.

Herausforderungen der PQK:

1. **Effizienzsteigerung:** Die Notwendigkeit, die Leistungsfähigkeit post-quanten sicherer Systeme zu erhöhen, ist entscheidend, um sie für anspruchsvolle Anwendungen geeignet zu machen [26].

2. **Vertrauensaufbau:** Umfassende kryptanalytische Prüfungen neuer Systeme sind unabdingbar, um ein hohes Maß an Vertrauen in ihre Sicherheit zu gewährleisten [27].

3. **Benutzerfreundlichkeit:** Die Entwicklung von sicheren und zugleich benutzerfreundlichen Standards und Implementierungen stellt eine zentrale Herausforderung dar [28].

Die Analyse fokussiert sich auf Kryptosysteme, die sich als widerstandsfähig gegenüber den potenziellen Bedrohungen durch leistungsstarke Quantencomputer erwiesen haben, einschließlich gitter-basierter Systeme, hash-basierter Verfahren, code-basierter Ansätze und multivariater polynomialer Systeme. Diese Systeme bringen jeweils eigene Stärken und mathematische Grundlagen mit sich.

Es werden nicht nur die spezifischen Sicherheitsmerkmale und mathematischen Grundlagen dieser ausgewählten Ansätze beleuchtet, sondern auch Aspekte wie Leistungsfähigkeit, Skalierbarkeit und Implementierungskomplexität berücksichtigt.

Das Ziel der Analyse ist es, ein tiefgreifendes Verständnis für die Vorzüge und Herausforderungen dieser Post-Quanten-Kryptosysteme zu schaffen. In einer Welt, die durch die rasante Entwicklung der Quantentechnologie geprägt ist, stellt die Bewertung und Implementierung robuster PQK eine entscheidende Aufgabe dar.

6.1.1 Gitter-basierte Kryptosysteme

Gitter-basierte Kryptosysteme nutzen die anspruchsvolle mathematische Gittertheorie und sind besonders für ihre Sicherheit bekannt, die auf Worst-Case-Szenarien beruht. Dies unterscheidet sie von vielen anderen Kryptosystemen, die auf Durchschnittsfallproblemen basieren. In Worst-Case-Szenarien berücksichtigen gitter-basierte Systeme die schwierigsten möglichen Fälle – Situationen, die die maximale Rechenleistung erfordern, um eine Lösung zu finden. Diese Eigenschaft macht sie besonders widerstandsfähig gegenüber Angriffen, da die Sicherheit nicht nur auf den typischerweise erwarteten, sondern auch auf den schwierigsten denkbaren Fällen basiert. Dieser Ansatz stellt einen wichtigen Fortschritt in der PQK dar, da er eine hohe Sicherheit gegenüber den potenziellen Gefahren durch leistungsstarke Quantencomputer bietet [6].

Ein Gitter in der Kryptografie wird als ein hochdimensionales Raster von Punkten beschrieben, wobei jeder Punkt durch einen Vektor repräsentiert wird. Die Sicherheit von gitter-basierten Systemen basiert auf der Schwierigkeit, bestimmte mathematische Probleme in diesen hochdimensionalen Räumen zu lösen. Zu diesen Problemen zählen unter anderem das Shortest Vector Problem (SVP), das Closest Vector Problem (CVP) und Short Integer Solution (SIS). Diese Herausforderungen sind in niedrigeren Dimensionen relativ einfach zu bewältigen, nehmen jedoch in der höheren Dimensionalität, die für die Kryptografie erforderlich ist, an Komplexität zu [6, 7].

Die Analyse dieser spezifischen Probleme und ihrer Rolle in der Kryptografie ist zentral für das Verständnis der Sicherheitsmechanismen von gitter-basierten Systemen. Die folgende Erläuterung bietet einen tieferen Einblick in diese Schlüsselprobleme:

- **Das Problem des kurzen Vektors (Shortest Vector Problem, SVP):** Gegeben ist eine Basis für ein Gitter L. Das Ziel ist, einen Gitterpunkt in L zu finden, der so nah wie möglich am Ursprung liegt und nicht der Nullvektor ist. Dieses Problem ist zentral in der gitter-basierten Kryptografie, da die Schwierigkeit, den kürzesten, nicht-trivialen Vektor in einem Gitter zu finden, die Sicherheit vieler gitter-basierter kryptografischer Schemata bildet [6].
- **Das Problem der kurzen Basis (Short Basis Problem, SBP):** Gegeben ist eine lange Basis für ein Gitter L. Das Ziel ist, eine kürzere Basis für denselben Gitterraum L zu finden. Dieses Problem ist wichtig für die Konstruktion und Analyse von Gittern in kryptografischen Anwendungen, da eine kürzere Basis oft effizientere Berechnungen und verbesserte Sicherheitseigenschaften ermöglicht [6].
- **Das Problem des nächsten Vektors (Closest Vector Problem, CVP):** Gegeben ist eine Basis für ein Gitter L und ein Punkt P im Gitterraum. Das Ziel ist, den dem Punkt P am nächsten liegenden Gitterpunkt zu finden. Dieses Problem spielt eine Schlüsselrolle in der gitter-basierten Kryptografie und dient als Grundlage für bestimmte kryptografische Primitive, da es oft schwierig ist, den nächsten Punkt in einem hochdimensionalen Gitter zu bestimmen [6].
- **Das Problem der kurzen ganzzahligen Lösung (Short Integer Solution, SIS):** Gegeben ist eine Matrix A mit m Vektoren der Dimension n und eine positive ganze Zahl q. Das Ziel ist, einen Vektor y mit kleinen ganzzahligen Einträgen zu finden, sodass $Ay = 0 \mod q$ ist. Dieses Problem wird in einigen gitter-basierten kryptografischen Konstruktionen verwendet und ist besonders relevant, da es schwierig ist, solche Lösungen in hochdimensionalen Räumen zu finden, was zur Sicherheit dieser Systeme beiträgt [6].

Fundamentale Aspekte der Gittertheorie

In der Kryptografie bilden Gitterstrukturen die Basis für diverse asymmetrische Kryptosysteme, die insbesondere in der PQK eine entscheidende Rolle spielen. Das SVP ist zentral für die Sicherheit dieser Systeme. Dieses Problem ist als NP-schwer eingestuft, was bedeutet, dass es zu den komplexesten Herausforderungen in der Klasse der NP-Probleme gehört, für die bis heute keine effiziente Lösungsmethode bekannt ist, die in polynomieller Zeit operiert. Diese hohe Komplexität stellt sowohl für klassische Rechner als auch für Quantencomputer ein bedeutendes Hindernis dar, welches nicht praktikabel schnell gelöst werden kann [29].

Konstruktion, Funktionsweise und Sicherheitsanalyse von gitter-basierten Kryptosystemen

Gitter-basierte Kryptosysteme sind eine innovative Klasse von Verschlüsselungsalgorithmen, die die mathematische Theorie der Gitter nutzen, um asymmetrische Verschlüsselungsalgorithmen zu entwickeln, die insbesondere gegen Quantenangriffe widerstandsfähig sind [30]. Die Konstruktion dieser Systeme basiert auf der Erzeugung komplexer Gitterstrukturen in einem n-dimensionalen Raum, einem abstrakten Raum mit n unabhängigen Dimensionen, was die Komplexität und damit die Sicherheit erhöht [31].

In diesen Kryptosystemen basiert die Erzeugung von Schlüsselpaaren auf der Nutzung von Gitterstrukturen. Der Prozess umfasst die Erstellung eines öffentlichen Schlüssels durch Kodierung eines spezifisch ausgewählten Punktes innerhalb des Gitters, bekannt als „trapdoor“-Mechanismus oder im Deutschen als „Falle“ bezeichnet. Die Entschlüsselung der mittels des öffentlichen Schlüssels verschlüsselten Nachrichten erfordert das Lösen einer komplexen mathematischen Aufgabe, die eng mit den Eigenschaften der Gitterstruktur verknüpft ist. Diese Aufgabe stellt selbst für Quantencomputer eine beträchtliche Herausforderung dar [32].

Die Sicherheitsanalyse dieser Kryptosysteme fokussiert sich auf die Schwierigkeit für einen Angreifer, dieses mathematische Problem zu lösen, das für die Entschlüsselung des verschlüsselten Textes erforderlich ist [33]. Der „Gitterproblem-Bitsecurity-Parameter“ ist ein Maß für die Sicherheit und gibt die Anzahl der Bits des geheimen Schlüssels an, die ein Angreifer benötigt, um das zugrundeliegende mathematische Problem zu lösen [34]

Gitter-basierte Kryptosysteme zeichnen sich durch starke Sicherheitsnachweise und effiziente Implementierungen aus. Ihre Kompatibilität mit aktuellen Verschlüsselungsstandards macht sie

zu einer attraktiven Alternative zu traditionellen kryptografischen Verfahren. Ihre Resistenz gegenüber Quantencomputer-Angriffen macht sie zu vielversprechenden Kandidaten für die Herausforderungen der PQK [33, 35].

Bei der Bewertung von gitter-basierten Kryptosystemen sind Faktoren wie Sicherheitsnachweise, Effizienz, Schlüsselgröße und Robustheit gegenüber Angriffen zu berücksichtigen. Diese Systeme erfüllen die meisten dieser Kriterien und stellen vielversprechende Optionen für zukünftige Sicherheitsprotokolle dar [35].

6.1.2 Code-basierte Kryptosysteme

Code-basierte Kryptografie, die auf der Theorie fehlerkorrigierender Codes beruht, spielt eine wesentliche Rolle in der Kommunikationstechnologie zur Korrektur von Übertragungsfehlern und ist seit über vier Jahrzehnten Gegenstand intensiver Forschung. Diese Kryptosysteme erhöhen die Sicherheit, indem sie Nachrichten in Fehlerkorrekturcodes umwandeln und dabei bewusst Fehler einführen [10].

Ein exemplarisches Kryptosystem dieser Art ist der McEliece-Algorithmus, der auf linearen Fehlerkorrekturcodes basiert. Bei diesem Ansatz verwendet der Empfänger einen effizienten Fehlerkorrekturcode als privaten Schlüssel, der mit zwei Blindmatrizen kombiniert wird, um einen öffentlichen, weniger effizienten Code zu erzeugen. Diese Blindmatrizen dienen dazu, die Verschlüsselung zu verschleiern und die Sicherheit zu erhöhen. Die Verschlüsselung einer Nachricht mit dem öffentlichen Schlüssel und die anschließende Einführung von Fehlern erzeugen den Geheimtext, der mit dem privaten Schlüssel entschlüsselt wird [10].

Der McEliece-Algorithmus, der 1978 eingeführt wurde, hat sich als widerstandsfähig gegenüber signifikanten Schwächen erwiesen. Ein Nachteil ist die Größe des öffentlichen Schlüssels, die erheblich größer als bei gängigen asymmetrischen Verfahren wie RSA ist. Im NIST-Wettbewerb basieren 21 der 69 vorgeschlagenen Algorithmen auf code-basierter Kryptografie [6].

Die code-basierte Kryptografie ist effizient in Verschlüsselung und Entschlüsselung, bedingt durch die Verwendung von Matrix-Vektor-Multiplikation, einem Prozess, bei dem ein Vektor mit einer Matrix multipliziert wird, um einen neuen Vektor zu erzeugen. Sie gilt als sehr sicher, sofern die Parameter sorgfältig ausgewählt werden. Trotz großer Schlüsselgrößen wird sie als zuverlässige Alternative zu traditionellen Verfahren betrachtet, besonders in Anbetracht der Tatsache, dass zukünftige Technologien den Umgang mit längeren Schlüsseln erleichtern könnten [10].

Code-basierte Kryptosysteme wenden Prinzipien der Coding-Theorie an, um robuste asymmetrische Verschlüsselungsverfahren zu entwickeln, die besonders für die Post-Quanten-Ära geeignet sind. Ein zentraler Aspekt dieser Kryptosysteme ist die Umwandlung von Nachrichten in Codewörter, die auf komplexen algebraischen Strukturen, wie Fehlerkorrekturcodes, basieren. Ein prominentes Beispiel hierfür ist das McEliece-Kryptosystem, welches Goppa-Codes verwendet. Diese Codes sind spezielle Arten von Fehlerkorrekturcodes, deren Decodierung als schwieriges Problem bekannt ist, und tragen damit maßgeblich zur Sicherheit des McEliece-Kryptosystems bei [10].

Eine Herausforderung bei der Implementierung von code-basierten Kryptosystemen ist die Notwendigkeit größerer Schlüsselgrößen im Vergleich zu herkömmlichen Verfahren wie RSA oder ECC. Die Forschung in diesem Bereich zielt darauf ab, ihre Effektivität und praktische Anwendbarkeit kontinuierlich zu verbessern, was diese Kryptosysteme zu vielversprechenden Kandidaten für zukünftige Sicherheitsprotokolle macht [6].

Grundlagen der Fehlerkorrekturcodes

Fehlerkorrekturcodes sind spezielle Algorithmen, die in der Datenübertragung und Datenspeicherung eingesetzt werden, um die Integrität von Daten zu gewährleisten. Sie ermöglichen die Erkennung und Korrektur von Fehlern, die während der Übertragung oder Speicherung auftreten können [10, 17].

Die essentielle Funktionsweise von Fehlerkorrekturcodes basiert auf der Implementierung zusätzlicher Redundanz in die zu übertragenden Daten. Diese Redundanz wird in Form von zusätzlichen Bits realisiert, bekannt als Paritätsbits, die gemeinsam mit den Originaldaten übermittelt werden. Die Integration dieser Paritätsbits ermöglicht es, Unregelmäßigkeiten innerhalb der Datenstruktur zu identifizieren und zu korrigieren, was essentiell für die Gewährleistung der Datenintegrität während der Übertragung ist [7].

Es existieren verschiedene Typen von Fehlerkorrekturcodes, die je nach Anforderung der Übertragungsumgebung eingesetzt werden. Hamming-Codes beispielsweise sind in der Lage, einen einzelnen Bitfehler zu erkennen und zu korrigieren, während Reed-Solomon-Codes mehrere Fehler gleichzeitig korrigieren können. Bose-Chaudhuri-Hocquenghem (BCH)-Codes sind eine weitere Klasse von Fehlerkorrekturcodes, die sowohl für die Erkennung als auch für die Korrektur von einzelnen sowie multiplen Fehlern innerhalb einer Datenübertragung konzipiert sind. Diese Codes zeichnen sich durch ihre Fähigkeit aus, sogenannte Burst-Fehler effizient zu korrigieren, bei denen mehrere, sequenziell aufeinanderfolgende Bits fehlerhaft sein können. Die BCH-Codes

basieren auf komplexen algebraischen Strukturen und ermöglichen es, durch sorgfältig konstruierte Polynome eine hohe Fehlerkorrekturkapazität zu erreichen, was sie besonders für Anwendungen geeignet macht, in denen eine hohe Zuverlässigkeit der Datenübertragung erforderlich ist [17].

Insgesamt spielen Fehlerkorrekturcodes eine entscheidende Rolle in der digitalen Kommunikation. Sie stellen sicher, dass Daten trotz potenzieller Fehlerquellen zuverlässig übertragen und gespeichert werden können und bilden damit eine essentielle Komponente moderner Kommunikationstechnologien [10].

Konstruktion, Funktionsweise und Sicherheitsanalyse des McEliece-Verschlüsselungsalgorithmus

Die Sicherheit der code-basierten Kryptografie, speziell des McEliece-Verschlüsselungsalgorithmus, basiert auf der Komplexität des Decodierens von Goppa-Codes, einer speziellen Art von fehlerkorrigierenden Codes. Die Ununterscheidbarkeit dieser Codes von zufälligen linearen Codes bildet das Kernstück ihrer Sicherheit. [7].

Eingeführt wurde der McEliece-Verschlüsselungsalgorithmus 1978 von Robert McEliece, Bei der Verschlüsselung mittels Goppa-Codes, wird das Codewort mit einer zufälligen invertierbaren Matrix, bekannt als Permutationsmatrix, multipliziert, um den Geheimtext zu erzeugen. Der private Schlüssel, bestehend aus dem Goppa-Code und der Permutationsmatrix, ermöglicht die Entschlüsselung durch Invertierung dieser Matrix [7].

Obwohl der öffentliche Schlüssel bekannt ist, bleibt das Entschlüsseln eine Herausforderung, da die Rekonstruktion des geheimen Schlüssels aufgrund der komplexen Struktur dieser Goppa-Codes und der Permutationsmatrix äußerst schwierig ist. Die Sicherheitsanalyse des McEliece-Verfahrens zeigt, dass selbst mit fortgeschrittenen Quantencomputern das Decoding von Goppa-Codes eine beträchtliche Herausforderung darstellt [10].

Das McEliece-Verfahren gilt daher als eines der vielversprechendsten post-quantum Kryptosysteme. Es wird von der NIST für die Standardisierung in der PQK empfohlen. Trotz seiner starken Sicherheitsmerkmale sind die großen Schlüsselgrößen und der hohe Rechenaufwand Herausforderungen, die die Anwendung in einigen Szenarien einschränken können [7, 17].

Im Folgenden werden die Kriterien von Codes-basierten Verschlüsselungsmethoden genauer untersucht:

1. **Sicherheit:** Die Sicherheit von code-basierten Verschlüsselungsmethoden beruht auf der Schwierigkeit, den Code zu dekodieren, der durch das Verschlüsselungsverfahren generiert wurde. Die Sicherheitsanalyse solcher Verfahren umfasst die Berechnung der Entropie des Schlüsselraums, die Bewertung der Schlüsselgröße und die Bestimmung der Komplexität des Dekodierungsproblems. Es ist wichtig sicherzustellen, dass das Dekodierungsproblem auch für zukünftige Quantencomputer schwierig bleibt [36].

2. **Effizienz:** Die Effizienz von code-basierten Verschlüsselungsmethoden hängt von der Komplexität des Kodierungs- und Dekodierungsprozesses ab. Es ist wichtig, Verfahren mit geringem Ressourcenverbrauch zu entwickeln, um sie in praktischen Anwendungen einsetzen zu können [36].

3. **Schlüsselgröße:** Die Schlüsselgröße ist ein wichtiger Faktor bei der Sicherheit von code-basierten Verschlüsselungsmethoden. Ein langer Schlüssel erhöht die Sicherheit, kann aber auch die Effizienz beeinträchtigen. Daher ist es wichtig, die richtige Balance zwischen Sicherheit und Effizienz zu finden [7].

4. **Flexibilität:** Code-basierte Verschlüsselungsmethoden müssen flexibel sein, um verschiedene Anwendungsfälle zu unterstützen. Sie sollten in der Lage sein, sowohl für symmetrische als auch für asymmetrische Verschlüsselung eingesetzt zu werden. Zudem sollte es möglich sein, den verwendeten Code zu ändern, um der Entwicklung von zukünftigen Angriffen entgegenzuwirken [7].

Insgesamt sind code-basierte Verschlüsselungsmethoden vielversprechende Kandidaten für die PQK, da sie eine hohe Sicherheit und Effizienz bieten. Die Entwicklung von Verfahren mit ausgewogener Sicherheit und Effizienz ist jedoch eine große Herausforderung und erfordert eine sorgfältige Abwägung der genannten Kriterien [7].

6.1.3 Hash-basierte Kryptosysteme

Hash-basierte digitale Signaturschemata bieten eine sichere Alternative zu herkömmlichen asymmetrischen Algorithmen wie RSA. Sie basieren auf der Vorbildwiderstandsfähigkeit und Kollisionssicherheit von Hashfunktionen, was sie besonders robust gegenüber Quantencomputer-Angriffen macht. Diese Eigenschaften machen hash-basierte Schemata ideal für Anwendungen, die hohe Sicherheitsanforderungen haben, wie beispielsweise sichere digitale Kommunikation und Authentifizierung [10].

Die Vorbildwiderstandsfähigkeit einer Hashfunktion H bedeutet, dass es für eine gegebene Ausgabe y von H schwierig ist, irgendeine Eingabe x zu finden, für die $y = H(x)$ gilt. Diese Eigenschaft ist entscheidend, um zu verhindern, dass jemand, der den Hashwert kennt, die ursprüngliche Nachricht rekonstruieren kann. Schwache Kollisionssicherheit impliziert, dass es für eine beliebige Nachricht m_1 anspruchsvoll ist, eine andere Nachricht m_2 zu finden, so dass $H(m_1) = H(m_2)$. Dies stellt sicher, dass es nicht möglich ist, zwei unterschiedliche Nachrichten zu erstellen, die denselben Hashwert ergeben, was bei der Integritätssicherung von Daten wichtig ist. Starke Kollisionssicherheit erfordert, zwei unterschiedliche Nachrichten m_1 und m_2 zu finden, die denselben Hashwert ergeben. Diese Eigenschaft ist aufgrund des Geburtstagsparadoxons wichtiger, da sie die allgemeine Widerstandsfähigkeit der Hashfunktion gegen jegliche Art von Kollisionsangriffen erhöht [10].

Leslie Lamport führte 1979 das hash-basierte digitale Signaturschema ein, das grundlegend für die Verwendung von Hashfunktionen zur digitalen Signaturerstellung ist. Winternitz entwickelte daraufhin ein effizienteres Einmal-Signaturschema, das insbesondere durch kleinere Schlüssel- und Signaturgrößen überzeugt. Ralph Merkle erweiterte diese Konzepte weiter zu einem Merkle-Signaturschema, das Winternitz' Ansatz mit binären Bäumen kombiniert, um eine effektive und flexible Signaturerstellung zu ermöglichen. SPHINCS+, ein fortschrittliches hash-basiertes Signaturschema, integriert das „Forest of Random Subsets"-Signaturschema (FORS). FORS verwendet eine Sammlung von Hash-Bäumen zur effizienten Schlüsselverwaltung und kombiniert dies mit Winternitz' Einmal-Signaturmethode, um die Sicherheit und Effizienz weiter zu verbessern [6, 10]. Hash-basierte Schemata, einschließlich SPHINCS+, sind wichtige Kandidaten, da sie robust gegenüber potenziellen Angriffen durch Quantencomputer sind [10].

Diese Schemata sind jedoch nicht ohne Herausforderungen. Sie neigen dazu, größere Schlüssel- und Signaturgrößen zu haben und erfordern eine sorgfältige Abwägung zwischen Sicherheit, Leistung und Speicheranforderungen. Trotz dieser technischen Herausforderungen bieten hash-basierte Signaturschemata, insbesondere in einer zunehmend digitalisierten Welt, eine vielversprechende Lösung für die Zukunft der Datensicherheit [10].

Grundlagen der Hash-Funktionen

Kollisionssichere Hashfunktionen sind essentiell in der Kryptografie, da sie eine lange Nachricht effizient auf einen kurzen Hash-Wert abbilden. Ziel ist es, Kollisionen zu verhindern, also zwei unterschiedliche Eingaben, die denselben Hash-Wert erzeugen [7].

Eine innovative Entwicklung in diesem Bereich sind gitter-basierte Hashfunktionen. Sie bieten starke Sicherheitsnachweise, die auf der Komplexität von Gitterproblemen basieren und sind besonders widerstandsfähig gegen Quantenangriffe. Diese gitter-basierten Konstruktionen ermöglichen eine sichere Komprimierung von Nachrichten und haben breite Anwendungen in der Kryptografie. Ihre Erforschung und Entwicklung tragen dazu bei, robuste Post-Quantum-Kryptosysteme zu schaffen [7].

Hash-Funktionen sind mathematische Algorithmen, die eine beliebige Eingabe in einen festen Hash-Wert transformieren. Sie sind deterministisch, d.h., sie liefern für dieselbe Eingabe stets denselben Hash-Wert. Eine Schlüsseleigenschaft ist die Unveränderlichkeit: Selbst kleinste Änderungen in der Eingabe führen zu einem deutlich anderen Hash-Wert. Diese Eigenschaft macht Hash-Funktionen ideal für die Datenintegritätsprüfung und Authentifizierung [7].

In diesem Kontext wird die Sicherheit von Hash-Funktionen durch die Verwendung eines „Salt“ verstärkt. Ein „Salt“ ist eine zufällige Datenreihe, die zu jedem Eingabewert, wie einem Passwort, vor der Hash-Berechnung hinzugefügt wird. Dieser Schritt erhöht die Einzigartigkeit jedes Hash-Werts und macht es deutlich schwieriger, die ursprünglichen Daten durch z.B. Brute-Force-Angriffe zu entschlüsseln. Durch „Salting “ wird die Wahrscheinlichkeit von Kollisionen, also identischen Hash-Werten für unterschiedliche Eingaben, reduziert. Dies ist besonders wichtig, da eine entdeckte Kollision die Sicherheit des gesamten Systems, das die Hash-Funktion nutzt, gefährden kann. Daher ist neben dem „Salting“ auch die regelmäßige Aktualisierung und Verwendung sicherer Hash-Funktionen für die Aufrechterhaltung der Systemsicherheit entscheidend.[7].

Konstruktion, Funktionsweise und Sicherheitsanalyse von hash-basierten Signaturen

Digitale Signaturen sind entscheidend für die Sicherheit von Daten, da sie Authentizität, Integrität und Nicht-Abstreitbarkeit gewährleisten. Die Nicht-Abstreitbarkeit bedeutet, dass der Absender einer signierten Nachricht nicht leugnen kann, diese gesendet zu haben, was für rechtliche und vertragliche Zwecke essentiell ist [7].

Hash-basierte Signaturen gelten heute als vielversprechende Alternative in der PQK [7]. Sie gehören zur Familie der asymmetrischen Kryptosysteme und garantieren durch die Verwendung von Hash-Funktionen die Integrität und Authentizität digitaler Daten. Ihre Funktionsweise und Sicherheit basiert auf der Schwierigkeit, Kollisionen in Hash-Funktionen zu finden, wodurch sie vor Angriffen geschützt sind [17]. Diese Signaturen nutzen asymmetrische Schlüssel, wobei der private Schlüssel für die Erzeugung und der öffentliche Schlüssel für die Verifikation der Signatur verwendet wird [7]. Der Prozess beginnt damit, dass der Sender eine Nachricht erstellt und deren

Hash-Wert generiert. Der Hash-Wert wird mit dem privaten Schlüssel signiert, was die digitale Signatur ergibt. Der Empfänger nutzt den öffentlichen Schlüssel des Senders, um die Signatur zu überprüfen und damit die Authentizität der Nachricht zu bestätigen [17].

Ralph Merkle entwickelte hash-basierte Signaturschemata, die auf Einmalsignaturen basieren. Einmalige Signaturen sind grundlegend, erfordern jedoch für jedes Dokument ein neues Schlüsselpaar. Merkles Ansatz nutzt Hash-Bäume, um viele einmalige Verifikationsschlüssel auf einen öffentlichen Schlüssel zu reduzieren [7].

6.1.4 Multivariate-polynom-Kryptosysteme

Multivariate Public-Key-Kryptografie (MPKC) basiert auf der Anwendung multivariater quadratischer Polynomabbildungen. Der öffentliche Schlüssel in solchen Systemen besteht aus einer Sammlung dieser Polynome, deren Sicherheit sich von der Schwierigkeit ableitet, ein System quadratischer Gleichungen zu lösen, und nicht von komplexen mathematischen Annahmen wie bei klassischen Kryptosystemen [7].

Im Gegensatz zu Verfahren, die auf der Faktorisierung von Primzahlen oder dem diskreten Logarithmus beruhen, liegt der Fokus bei MPKCs auf der Komplexität der Lösung dieser Polynomsysteme. Die Konstruktion solcher Systeme beinhaltet die Auswahl von Polynomgleichungen mit hohen Graden und zahlreichen Variablen. Für die Verschlüsselung wird eine Nachricht in eine Zahlenfolge transformiert und in das Polynomsystem eingesetzt, während die Entschlüsselung das Lösen dieses Systems erfordert [10, 17].

Grundlagen der Polynomarithmetik

Polynomarithmetik beschäftigt sich mit arithmetischen Operationen auf Polynomen, mathematischen Ausdrücken, die aus Summen von Potenzen einer Variablen bestehen, multipliziert mit Koeffizienten. Ein Beispiel für ein Polynom ist $P(x) = 3x^3 + 2x^2 - x + 1$, das in der Variablen x ausgedrückt wird [7].

Die Grundoperationen umfassen Addition, Subtraktion, Multiplikation und Division. Bei Addition und Subtraktion werden die Koeffizienten entsprechender Potenzen zusammengefasst. Die Multiplikation erfordert das Verteilen jedes Terms eines Polynoms über jeden Term des anderen, gefolgt von der Addition der Koeffizienten. Die Division von Polynomen zielt darauf ab, einen Quotienten und Rest zu ermitteln, indem ein Polynom durch ein anderes geteilt wird [7, 6].

Konstruktion, Funktionsweise und Sicherheitsanalyse von multivariaten-polynom-Kryptosystemen

Die Konstruktion von MPKCs involviert die Generierung von Polynomen mit mehreren Variablen als öffentliche Schlüssel und zugehörige Matrizen partieller Ableitungen als private Schlüssel. Die Verschlüsselung nutzt das Polynom, um Gleichungen zu erstellen, deren Lösung die ursprüngliche Nachricht offenbart, während die Entschlüsselung durch Lösen dieser Gleichungen mit dem privaten Schlüssel erfolgt [10, 17].

Zusätzlich werden in der MPKC-Konstruktion Modifikatoren angewendet, um die Widerstandsfähigkeit gegen bestimmte konstruktionsbasierte Kryptanalysemethoden zu erhöhen und gleichzeitig die Effizienz zu verbessern. Diese Modifikatoren beinhalten die Hinzufügung von Zufallsgleichungen, das Entfernen öffentlicher Gleichungen, Änderungen im Eingaberaum, die Hinzufügung von Variablen, die Einbeziehung zufälliger Summanden und die Integration einer nichtlinearen Komponente in die Konstruktion [17].

Die Sicherheit von MPKCs basiert auf der NP-Schwere beim Lösen komplexer Polynomgleichungen, wobei die Polynomauswahl entscheidend für die Resistenz gegen Angriffe ist. MPKCs bieten potenzielle Sicherheit gegen Quantencomputerangriffe und sind vielseitig einsetzbar. Herausforderungen umfassen die Generierung zufälliger Zahlen für die Schlüsselerstellung und die Anfälligkeit bestimmter Polynomtypen für Angriffe. Trotz der NP-Schwere zeigt die Multivariate-Kryptografie Schwächen bei der Entdeckung des geheimen Schlüssels und der Wiederherstellung von Klartext aus Kryptotext. Dennoch sind MPKCs besonders resistent gegen Brute-Force-Angriffe, da keine effizienten Lösungsalgorithmen existieren [10, 17].

Ein bekanntes Beispiel für MPKCs ist das Rainbow-Kryptosystem, basierend auf der Schwierigkeit, ein System von Polynomgleichungen zu lösen. Trotz ihrer vielversprechenden Eigenschaften sind MPKCs anfällig für algebraische Angriffe und erfordern im Vergleich zu anderen Kryptosystemen höhere Rechenleistungen [7].

Multivariate-polynom-Kryptosysteme müssen verschiedene Sicherheitskriterien erfüllen:

1. **Resistenz gegen Polynomgleichungsangriffe:** Die Sicherheit beruht auf der Komplexität der Polynomgleichungen. Die Herausforderung für Angreifer liegt im Lösen dieser Systeme zur Extraktion des privaten Schlüssels [17, 10].
2. **Anzahl der Variablen und Gleichungen:** Systeme mit mehr Variablen und Gleichungen sind sicherer, da sie die Analyse für Angreifer erschweren [17, 10].

3. **Schlüssellänge:** Die Länge des privaten Schlüssels ist entscheidend. Längere Schlüssel erhöhen die Lösungskomplexität des Gleichungssystems [17, 10].

4. **Effizienz:** Die praktische Anwendbarkeit von MPKCs hängt von ihrer Effizienz ab. Herausforderungen bestehen in höherer Rechenzeit und Speicherbedarf [17, 10].

MPKCs sind vielversprechend für die PQK, jedoch sind Herausforderungen wie Effizienz und Schlüssellänge Gegenstand laufender Forschung zur Verbesserung ihrer praktischen Anwendbarkeit.

7 Schlussfolgerung

Die vorliegende Arbeit hat umfassend untersucht, wie die Entwicklung von Quantencomputern und die Einführung von Quantenalgorithmen, insbesondere Shor's und Grover's Algorithmus, die Landschaft der heutigen Kryptografie beeinflussen. Insbesondere stellt Shor's Algorithmus eine ernsthafte Bedrohung für Public-Key-Verschlüsselungssysteme dar, da er die Faktorisierung großer Primzahlen effizient ermöglicht – eine Grundlage für die Sicherheit von Systemen wie RSA. Diese Arbeit reflektiert die wesentlichen Erkenntnisse und Herausforderungen, die sich aus der Entwicklung und dem Einsatz von Quantencomputern ergeben, und betrachtet die Rolle und Zukunft der PQK im Kontext der modernen Kryptografie.

7.1 Auswirkungen von Quantencomputern auf die Kryptografie

Die Entwicklung von Quantencomputern und die Einführung von Quantenalgorithmen, insbesondere Shor's und Grover's Algorithmus, haben tiefgreifende Auswirkungen auf die heutige Kryptografie. Shor's Algorithmus stellt eine erhebliche Bedrohung für Public-Key-Verschlüsselungssysteme dar, die auf der Faktorisierung großer Primzahlen basieren, wie es bei RSA der Fall ist.

7.2 Prinzipien und Ziele der Post-Quantum-Kryptografie

Die PQK zielt darauf ab, eine Vielzahl kryptografischer Anwendungen zu unterstützen, darunter digitale Signaturen, Verschlüsselungsverfahren und Schlüsselaustauschprotokolle. Ein entscheidendes Ziel ist die Interoperabilität der PQK-Algorithmen mit vorhandenen kryptografischen Standards, um deren Integration in bestehende Systeme zu erleichtern. Die Algorithmen sollen langfristig sicher bleiben und sowohl in Bezug auf Rechenleistung als auch auf Speicherbedarf praktikabel sein.

7.3 Sicherheitsanalyse von Post-Quantum-Kryptoalgorithmen

Post-Quantum-Kryptoalgorithmen werden einer gründlichen Sicherheitsanalyse unterzogen, um ihre Widerstandskraft gegenüber Quantenangriffen zu beurteilen. Die Analyse berücksichtigt kritische Aspekte wie Rechenkomplexität, Beständigkeit gegen Angriffe und angemessene Schlüsselparameter.

7.4 Forschungs- und Entwicklungsbedarf in der PQK

Trotz der bestehenden Unsicherheiten über die Notwendigkeit und Dringlichkeit der PQK, besteht ein dringender Bedarf an weiterführender Forschung und Entwicklung, um die Reife und Praktikabilität von PQK-Systemen zu sichern.

7.5 Empfehlungen des BSI für Maßnahmen

BSI betrachtet die Existenz von Quantencomputern als eine zukünftige Gewissheit und empfiehlt, sich auf die Einführung von PQK vorzubereiten. Es wird geraten, je nach Anwendungsszenario, frühzeitig und fortlaufend im Kontext eines angemessenen Risikomanagements zu bewerten, ob und wann ein Umstieg auf quantencomputerresistente Algorithmen sinnvoll ist. Im Folgenden werden einige spezifische Empfehlungen des BSI präsentiert [37]:

7.6 Empfehlungen des BSI für Maßnahmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erkennt die Entwicklung von Quantencomputern als eine unvermeidliche zukünftige Realität an und empfiehlt eine proaktive Vorbereitung auf die Implementierung von Post-Quantum-Kryptografie. Es wird dazu geraten, abhängig vom jeweiligen Anwendungskontext und im Rahmen eines angemessenen Risikomanagements, frühzeitig die Notwendigkeit und den Zeitpunkt eines Übergangs zu quantencomputerresistenten Algorithmen zu bewerten. Nachstehend sind einige spezifische Empfehlungen des BSI dargestellt [37]:

- **Kryptoagilität:** Für die Entwicklung neuer sowie die Wartung bestehender Systeme ist es essentiell, kryptografische Prozesse flexibel zu gestalten. Dies ermöglicht eine schnelle Anpassung an neue Entwicklungen und Standards und erleichtert den Ersatz veralteter Algorithmen. Diese Agilität ist sowohl im Hinblick auf die Bedrohung durch Quantencomputer als auch zur Abwehr fortschreitender konventioneller Angriffe von Bedeutung [37].

- **Hash-basierte Signaturen für Firmware-Updates:** Für die Signierung von Firmware-Updates empfiehlt das BSI den Einsatz von zustandsbasierten, hash-basierten Signaturalgorithmen, die eine limitierte Anzahl von Signaturen ermöglichen. Diese Signaturmethode wird in den Empfehlungen des BSI schon lange favorisiert und trägt signifikant zur Förderung der Kryptoagilität bei [37].

- **Schlüssellängen für symmetrische Algorithmen:** Symmetrische Verschlüsselungsalgorithmen sind im Vergleich zu asymmetrischen Algorithmen weniger anfällig für Quantencomputerangriffe. Bei symmetrischen Schlüsseln mit einer Länge von 128 Bit oder weniger könnten Angriffe durch Quantencomputer jedoch erfolgreich sein. Für einen langfristigen Schutz wird die Verwendung von Schlüssellängen von 256 Bit empfohlen [37].

- **Kurzfristige Schutzmaßnahmen:** Als temporärer Schutz gegen Angriffe durch Quantencomputer können vorverteilte symmetrische Langzeitschlüssel genutzt werden. Diese Strategie erfordert individuelle Lösungen für die Schlüsselverteilung [37].

- **Hybride Lösungen:** Das BSI empfiehlt den Einsatz von quantencomputerresistenten Algorithmen in Kombination mit klassischen Algorithmen, insbesondere für Anwendungen, die ein hohes Maß an Sicherheit erfordern. Diese hybriden Lösungen bieten eine zusätzliche Sicherheitsebene, da die quantencomputerresistenten Algorithmen noch nicht so umfassend erforscht sind wie die klassischen [37].

- **Anpassung kryptografischer Protokolle:** Die Umstellung auf quantencomputersichere Algorithmen, insbesondere die Nutzung von Hybridlösungen, erfordert Modifikationen in bestehenden kryptografischen Protokollen [37].

- **Quantencomputersichere Schlüsselvereinbarung:** Das BSI empfiehlt spezifische Algorithmen für eine sichere Schlüsselvereinbarung unter der Berücksichtigung von Quantencomputern und hält an der Empfehlung für FrodoKEM fest, trotz gewisser Einschränkungen. Es wird erwartet, dass diese Empfehlungen aktualisiert werden, sobald vom NIST neue Algorithmen standardisiert werden [37].

Diese Empfehlungen des BSI reflektieren das Bestreben, sich proaktiv auf die Herausforderungen durch Quantencomputer vorzubereiten und dabei sowohl aktuelle als auch zukünftige Sicherheitsrisiken zu berücksichtigen [37].

7.7 Zukünftige Forschungsrichtungen und globale Herausforderungen

In der zukünftigen Forschungsausrichtung der Post-Quantum-Kryptografie werden verschiedene Schlüsselbereiche fokussiert, um den mit der Einführung von Quantencomputern verbundenen Herausforderungen zu begegnen. Ein Hauptaugenmerk liegt auf der Weiterentwicklung und Optimierung von PQK-Algorithmen, um deren Robustheit gegenüber Angriffen durch Quantencomputer zu gewährleisten, wobei ein ausgewogenes Verhältnis zwischen Sicherheit und Effizienz angestrebt wird. In diesem Kontext ist auch die Standardisierung dieser Algorithmen von großer Bedeutung. Die Kooperation mit Institutionen wie dem NIST zur Standardisierung von PQK-Algorithmen ist essenziell, um deren Interoperabilität, Zuverlässigkeit und allgemeine Akzeptanz zu erhöhen [38, 25].

Ein weiterer bedeutender Forschungsbereich ist die Kryptoagilität, die darauf abzielt, Systeme so zu gestalten, dass sie flexibel auf den Wechsel kryptografischer Algorithmen reagieren können. Dies umfasst die Herausforderung, PQK-Algorithmen nahtlos in bestehende Systeme und Infrastrukturen einzubinden. Umfassende Sicherheitsanalysen der Algorithmen sind zudem von Bedeutung, um deren Widerstandsfähigkeit gegenüber einer Vielzahl von Angriffen zu verstehen und entsprechende Gegenstrategien zu entwickeln [37, 25].

Des Weiteren gewinnen praktische Anwendungen und Implementierungen von PQK an Bedeutung, wobei der Fokus auf der Umsetzbarkeit von PQK in verschiedenen technologischen und industriellen Bereichen liegt [25].

Zum Abschluss werden langfristige Perspektiven und Herausforderungen in der PQK-Forschung beleuchtet, einschließlich der Anpassung an die sich kontinuierlich entwickelnde Quantencomputertechnologie und der Entwicklung zukunftssicherer kryptografischer Lösungen. Diese vielfältigen Forschungsrichtungen gewährleisten, dass PQK nicht nur den aktuellen, sondern auch zukünftigen Sicherheitsanforderungen entspricht und einen integralen Bestandteil der Cybersicherheitsstrategie darstellt [3, 25].

Literaturverzeichnis

[1] Philip Ball. Keeping secrets in a quantum world. *Nature*, 2022. https://www.nature.com/articles/d41586-022-02833-8.

[2] National Institute of Standards and Technology. Post-quantum cryptography, 2023. Zugriff: Dezember 2023.

[3] Bundesamt für Sicherheit in der Informationstechnik. Post-quanten-kryptografie, 2023. Zugriff: Dezember 2023.

[4] Bundesamt für Sicherheit in der Informationstechnik. Bsi - post-quanten-kryptografie, 2023. Zugriff: Dezember 2023.

[5] Marco Barenkamp. Steal now decrypt later: Post-quantum-kryptografie und ki. *Informatik Spektrum*, 45:349–355, 2022.

[6] Ritik Bavdekar, Eashan Jayant Chopde, Ashutosh Bhatia, Kamlesh Tiwari, Sandeep Joshua Daniel, and Atul. Post quantum cryptography: Techniques challenges standardization and directions for future research, Feb 2022.

[7] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549, 2017.

[8] Daniel J. Bernstein. Introduction to post-quantum cryptography, 2023. Kapitel in "Post-Quantum Cryptography".

[9] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography*. Springer, 2009.

[10] Stefan Heyse. *Post-Quantum Cryptography*. PhD thesis, Bochum University, 2013.

[11] National Institute of Standards and Technology. Post-quantum cryptography standardization project. https://csrc.nist.gov/projects/post-quantum-cryptography.

[12] Mateusz D. Zych Audun Jøsang Vasileios Mavroeidis, Kamer Vishi. The impact of quantum computing on present cryptography. *ar5iv*, 2020. https://ar5iv.org/html/1804.00200.

[13] Edward Gerjuoy. Shor's factoring algorithm and modern cryptography. an illustration of the capabilities inherent in quantum computers. *American Journal of Physics*, 73(6):521–540, 2005.

[14] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998.

[15] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[16] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 1997.

[17] Saleh Darzi, Kasra Ahmadi, Saeed Aghapour, Attila Altay Yavuz, and Mehran Mozaffari Kermani. Envisioning the future of cyber security in post-quantum era: A survey on pq standardization applications challenges and opportunities. *ACM Computing Surveys*, 2023.

[18] Daniel J. Bernstein. A code-based public-key encryption system. In *Post-Quantum Cryptography*, page 8. Springer, 2023.

[19] Niederreiter cryptosystems using quasi-cyclic codes that resist quantum fourier sampling. *ar5iv*, 1911. https://ar5iv.org/abs/1911.00661.

[20] Smaller keys for code-based cryptography: Mceliece cryptosystems with convolutional encoders. *ar5iv*, 2104. https://ar5iv.org/abs/2104.06809.

[21] Daniel J. Bernstein. Hash-based public-key signature system. In *Post-Quantum Cryptography*, page 7. Springer, 2023.

[22] Daniel J. Bernstein. A multivariate-quadratic public-key signature system. In *Post-Quantum Cryptography*, page 9. Springer, 2023.

[23] National Institute of Standards and Technology. Nist interagency report 8413, update 1. Technical report, National Institute of Standards and Technology, 2023.

[24] Post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed: 2024-01-01.

[25] Bundesamt für Sicherheit in der Informationstechnik. Entwicklungsstand von quantencomputern, 2023.

[26] Daniel J. Bernstein. Efficiency, confidence and usability in post-quantum cryptography. In *Post-Quantum Cryptography*, pages 12–13. Springer, 2023.

[27] Daniel J. Bernstein. Building confidence in post-quantum cryptography. In *Post-Quantum Cryptography*, page 13. Springer, 2023.

[28] Daniel J. Bernstein. Usability in post-quantum cryptography. In *Post-Quantum Cryptography*, page 13. Springer, 2023.

[29] G. Birkhoff. *Lattice Theory*. Amer. Math. Soc., Providence, RI, 3 edition, 1967.

[30] H. A. Priestly and B. A. Davey. *Introduction to Lattices and Order*. Cambridge University Press, Cambridge, England, 1990.

[31] Miklós Ajtai. Generating hard instances of lattice problems. *Complexity of computations and proofs*, 13:1–32, 1996.

[32] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[33] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. A fast, secure and simple encryption scheme. *International Workshop on Public Key Cryptography*, pages 267–288, 1998.

[34] Craig Gentry. Fully homomorphic encryption using ideal lattices. *STOC*, 9:169–178, 2009.

[35] G. Grätzer. *Lattice Theory: First Concepts and Distributive Lattices; General Lattice Theory*. W. H. Freeman; Birkhäuser, San Francisco, CA; Boston, MA, 2 edition, 1971; 1998.

[36] Daniel J. Bernstein. Grover vs. mceliece. https://eprint.iacr.org/2010/313, 2010.

[37] Bundesamt für Sicherheit in der Informationstechnik (BSI). Migration to post quantum cryptography: Recommendations for action, May 2021. Englische Übersetzung.

[38] NIST. Nist announces first four quantum-resistant cryptographic algorithms. 2023.

Erklärung zur selbstständigen Bearbeitung

Hiermit versichere ich, Deniese Kotthoff, Matrikel-Nr. 2385708, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort | Datum | Unterschrift im Original