

Entwicklung einer Bildungsplattform für Quantenkryptografie

Studienarbeit

im Studiengang Informatik

an der DHBW Ravensburg
Campus Friedrichshafen

von

Tim Bader, Daniel Erhard, Xena Letters

18.07.2022

Bearbeitungszeitraum: 6 Monate
Name, Matrikelnummer, Kurs: Bader 7322851 TIM-19
Erhard 1757926 TIM-19
Letters 3176202 TIM-19
Gutachter der Dualen Hochschule: Prof. Dr. Jürgen Schneider

Selbständigkeitserklärung

gemäß Ziffer 1.1.13 der Anlage 1 zu §§ 3, 4 und 5 der Studien- und Prüfungsordnung für die Bachelorstudiengänge im Studienbereich Technik der Dualen Hochschule Baden-Württemberg vom 29.09.2017 in der Fassung vom 27.07.2020.

Ich versichere hiermit, dass ich meine Studienarbeit mit dem Thema

Entwicklung einer Bildungsplattform für Quantenkryptografie

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Des Weiteren bestätige ich hiermit, dass die Arbeit unbefristet aufbewahrt werden darf.

Geislingen, den 17. 07.2022

Ort, Datum



Tim Bader - 7322851

Wolfratshausen, den 17.07.2022

Ort, Datum



Daniel Erhard - 1757926

Weingarten, den 17.07.2022

Ort, Datum



Xena Letters - 3176202

Abstract

Die Quantenkryptografie basiert auf einem komplexen Themenfeld bestehend aus mathematischen Gleichungen sowie den Gesetzen der Quantenmechanik. Um diese Inhalte der studentischen Zielgruppe näher zu bringen, wird im Rahmen dieser Arbeit eine Bildungsplattform für Quantenkryptografie entwickelt.

Diese soll die Grundlagen der Quantenkryptografie kapitelweise aufschlüsseln und diese mithilfe verschiedener Medienelemente anschaulich darstellen. Zu den Medienelementen gehören neben Bildern und Videos auch Aufgaben, kleinere Anwendungen und Simulationen. Die Auswahl basiert auf den Ergebnissen einer Anforderungsanalyse und auf den theoretischen Grundlagen des menschlichen Lernens.

Die Bildungsplattform wird im Rahmen einer Webanwendung mit dem Frontend Framework React entwickelt. Für spezielle Funktionalitäten werden zusätzliche Bibliotheken von Drittanbietern verwendet.

Die Inhalte der Bildungsplattform können dynamisch durch LaTeX-Dateien hinzugefügt werden. In den LaTeX-Dateien können auch zusätzliche Script- und HTML-Dateien mit eingebunden werden.

Ein einheitliches Designkonzept sorgt für eine abgerundete User Experience und einen angenehmen Gesamteindruck.

Inhaltsverzeichnis

Abbildungsverzeichnis	VI
Tabellenverzeichnis	IX
1 Einleitung	1
1.1 Problemstellung und Zielsetzung	1
1.2 Motivation	1
1.3 Aufbau der Arbeit	2
2 Grundlagen	3
2.1 Quantenmechanik	3
2.2 Quantum Computing	5
2.2.1 Quantum Bit	5
2.2.2 Quantengatter	9
2.2.3 Quantenschaltung	15
2.2.4 Quanten-Fouriertransformation	16
2.2.5 Quantum Phase Estimation	19
2.3 Algorithmen der Quantenkryptografie	23
2.3.1 BB84 Quantenschlüsselaustausch	23
2.3.2 Shor Algorithmus	26
2.4 Lerntheorie	31
2.4.1 Lernen und Wissen	31
2.4.2 Lernprozess im Gehirn	31
2.4.3 Unterscheidung von Lerntypen	32
2.4.4 Lernstiltypologie nach Kolb	33
2.4.5 Lernstrategien	35
2.4.6 Lernmotivation	36
3 Anforderungsanalyse	39
3.1 Bestimmung von System und Systemkontext	39
3.1.1 Definition des Systems	39
3.1.2 Erfassung des Systemkontexts	39
3.1.3 Bestimmung der Systemgrenze	40
3.2 Konkurrenzanalyse	41
3.3 Analyse der Stakeholder	42
3.4 Ermittlung der Anforderungen	43
3.4.1 Brainstorming	44
3.4.2 Konkurrenz	45

3.4.3	Befragungen	45
3.5	Anforderungsliste	51
4	Anwendungsentwicklung	53
4.1	Architekturmuster: Model-View-Controller (MVC)	53
4.2	Technologieentscheidung	55
4.3	Drittanbieter Bibliotheken	57
4.4	Umsetzung des LaTeX-Parsers	57
4.5	Visuelle Gestaltung der Oberfläche	58
4.5.1	Farbschema	59
4.5.2	Seitenaufbau und Komponenten	59
4.6	Lernelemente	63
4.6.1	Grafiken und Videos	63
4.6.2	Simulationen	63
4.6.3	Übungen	66
4.7	Administration	66
4.7.1	Lokales Setup	66
4.7.2	Erweiterbarkeit	68
5	Diskussion & Reflexion	70
5.1	Evaluation der Ergebnisse	70
5.2	Gewonnene Erkenntnisse	70
6	Fazit & Ausblick	72
6.1	Ergebnisse	72
6.2	Entwicklungsmöglichkeiten	72
A	Anhang	74
A.1	Interview	74
A.2	Umfrageformular	77
A.3	Anforderungsliste	81
A.4	Icons	83
	Literatur	84

Abbildungsverzeichnis

2.1 Eine Bloch-Kugel eines Qubits im Zustand $ +\rangle$, die mit dem Qiskit SDK erstellt wurde.	7
2.2 Visualisierung einer HZH Gatterfolge auf ein Qubit mit dem Startzustand $ 0\rangle$. Nach Anwendung der Gatter befindet sich das Qubit im Zustand 1 - es wurde ein X -Gatter bzw. eine NOT Operation durchgeführt. (ANIS u. a., 2021, Vgl. Textbook 'Single Qubit Gates' - Chapter 4)	11
2.3 Controlled NOT-Gatter	12
2.4 Anwendung des CNOT-Gatters auf den Qubit Zustand $ -\rangle$	12
2.5 Beispiel Implementation eines Quantum AND-Gatters aus zwei CH-Gatter und einem CZ-Gatter	13
2.6 Controlled-U-Gatter mit n Ziel Qubits	14
2.7 Beispiel: Algorithmus der Quanten-Teleportation (ANIS u. a., 2021, Textbook 'Quantum Circuits' - Chapter 3)	15
2.8 Beispielhafte Darstellung einer Quanten-Fouriertransformation mit vier Qubits und $x_{dez} \in \{0, 1, 2, \dots\}$, $\max(x_{dez}) = 15$. (ANIS u. a., 2021, Vgl. Textbook 'Quantum Fourier Transform' - Chapter 2)	17
2.9 Quanten-Fouriertransformationsschaltkreis mit n Qubits	18
2.10 Grundlegende Idee der Quantum Phase Estimation	20
2.11 Quantum Phase Estimation Subroutine mit t Messungssqubits (ANIS u. a., 2021, Textbook 'Quantum Phase Estimation' - Chapter 1)	21
2.12 Beispiel einer Quantum Phase Estimation mit unbekannter Phase $\theta = \frac{1}{3}$ und 5 Messungssqubits (ANIS u. a., 2021, Textbook 'Quantum Phase Estimation' - Chapter 3)	22
2.13 Wahrscheinlichkeitstabelle des Beispiels in Abb. 2.12 nach 4096 Messungen (ANIS u. a., 2021, Textbook 'Quantum Phase Estimation' - Chapter 3)	22
2.14 Beispiel einer Schlüsselgenerierung nach dem BB84 Protokoll. Die Schlüssel müssen anschließend noch bruchteilhaft miteinander verglichen werden, um sie auf Korrektheit zu überprüfen.	24
2.15 Beispiel eines Man-in-the-Middle Angriffs durch Eve während der Schlüsselgenerierung nach dem BB84 Protokoll. Bei der anschließenden Überprüfung auf Korrektheit der Schlüssel fällt auf, dass etwas falsch gelaufen ist.	25
2.16 Beispiel der periodischen Funktion $f(x) = a^x \bmod n$ aus Shor's Algorithmus mit $a = 3$, $n = 35$ und der Ordnung $r = 12$. (ANIS u. a., 2021, Textbook 'Shor's Algorithm' - Chapter 1)	26
2.17 Schaltung einer Shor Algorithmus Implementation (nach der Qiskit Qubit Ordering Convention)(ANIS u. a., 2021, Textbook 'Shor's Algorithm' - Chapter 2)	29

2.18	Beispiel des Shor Algorithmus mit 8 Zählerqubits, $n = 15$ und $a = 7$ (ANIS u. a., 2021, Textbook 'Shor's Algorithm' - Chapter 3)	30
2.19	Durchschnittliches Messergebnis von Abbildung 2.18 (links) und als Vergleich die periodische Funktion $f(x) = 7^x \bmod 15$ (rechts) (ANIS u. a., 2021, Vgl. Textbook 'Shor's Algorithm' - Chapter 3)	30
2.20	Lernen und Wissen (Groß und Bastian, 2017, S. 108, Abb. 7)	31
2.21	Lernzyklus nach Kolb (Alonso u. a., 2017, S. 22, Abb. 3)	34
2.22	Systematisierung von Lernstrategien (Alonso u. a., 2017, S. 24, Abb. 4) . .	35
2.23	Konzentrationsleistung (Reinhaus, 2011, S. 52)	37
3.1	Modellierung des Systemkontexts	40
3.2	Diese Stakeholdermatrix veranschaulicht den Einfluss in Relation zum Interesse von Stakeholdern des Projekts.	42
3.3	Mindmap der Nicht-Anforderungen aus der Sichtweise des Projektteams . .	44
3.4	Mindmap der Anforderungen aus der Sichtweise des Projektteams	45
3.5	Semester der Befragten	46
3.6	Unter Welchen Bedingungen lernen die Befragten optimal	47
3.7	Vorwissen in den Bereichen klassische und quantentechnische Kryptografie	49
3.8	Genauigkeit der behandelten Themen	50
3.9	Lernkanäle	51
4.1	MVC: Beziehungen der drei Hauptkomponenten (Smith, 2022)	53
4.2	Planung der Anwendung mittels einer MVC-Architektur	54
4.3	Meistgenutzte Web-Frameworks unter Entwicklern weltweit, ab 2021 (Stack Overflow, 2021)	56
4.4	Farbschema	59
4.5	Abbildung der Standardkomponenten	60
4.6	Abbildung des Endpoints für den Hilfschat	60
4.7	Abbildung des Chatfensters	61
4.8	Hintergrundbild	61
4.9	Icon für das Kapitel Quantencomputing	62
4.10	Simulation einer Blochsphäre	63
4.11	Deutsch-Jozsa Algorithmus Schaltung	64
4.12	Schlüsselgenerierung BB84 Simulation	65
4.13	Schlüsselgenerierung BB84 Simulation mit Angreifer	65
4.14	Beispielübung	66
4.15	Beispielübung innerhalb der Kapitelsseite	66
4.16	Inhalt der Datei page.json	68
A.1	Anforderungen Teil 1	81
A.2	Anforderungen Teil 2	82

A.3 Kapitel-Icons	83
-------------------	----

Tabellenverzeichnis

3.1 Konkurrenzanalyse	41
4.1 Übersicht an Befehlen für <i>latex_page.tex</i>	69

1 Einleitung

Die Welt der Quanten fasziniert die Wissenschaft seit über hunderten von Jahren. Der Wellen-Teilchen Dualismus scheint für den durchschnittlichen Menschen kaum verständlich. Trotz alledem werden Quantentechniken bereits heute angewandt.

Der Trend entwickelt sich immer weiter in Richtung Quantencomputer, wobei sie bereits in ihren ersten Formen existieren.

Im Jahr 2021 gab IBM bekannt, dass bereits die Entwicklung eines Quantenprozessors mit dem Namen Eagle mit 127 Qubits gelungen sei. Für das Jahr 2023 plant die Firma bereits die Entwicklung eines Quantenprozessors mit knapp 1000 Qubits. (Bolkart, 2022) Diese Entwicklungen schaffen neue Möglichkeiten in allen Bereichen des Lebens. Zum ersten Mal in der Geschichte wird die Vorstellung eines Computers mit unendlicher Rechenleistung wirklich greifbar.

Ebenfalls in der Kryptographie gibt es einige Algorithmen, die auf der Theorie der Quanten beleuchten. Darunter zählt zum einen das BB84-Protokoll oder der Shor-Algorithmus. Um die faszinierende Welt der Quanten den Studierenden in Deutschland näher zu bringen, wird in dieser Studienarbeit eine Bildungsplattform der Quantenkryptographie entwickelt werden. Hierdurch soll den Studierenden das Thema spielend leicht näher gebracht werden.

1.1 Problemstellung und Zielsetzung

Die Quantenkryptografie basiert auf komplexen und theoretischen Konzepten. Die Einarbeitung erfordert dabei einen hohen Aufwand, sowie Fachkenntnisse im Bereich Quantenmechanik und kryptografischen Verfahren. Um diese Thematik für Studenten im Sinne der Weiterbildung zugänglich zu machen, wird in dieser Arbeit eine Bildungsapplikation als Webanwendung für Quantenkryptografie erstellt. Dabei soll diese ohne tiefergehende Vorkenntnisse die Funktion der Protokolle BB84 und den Shor-Algorithmus behandeln. Hierdurch soll erreicht werden, dass ein Einstieg in Quanteninformatik geschaffen wird.

1.2 Motivation

Die Motivation ist wie bereits erwähnt, einen einfachen Einstieg in die Welt der Quanten zu schaffen. Dabei sollen Studierende motiviert werden, sich näher mit der Thematik zu befassen. Die Bildungsplattform stellt dabei den ersten Schritt in der beeindruckenden Reise durch die Welt der Quanten dar. Ebenfalls soll die Bildungsplattform durch das erhöhte Interesse zu weiteren Entwicklungen in der Quanteninformatik führen, da sich hierdurch mehr Personen mit der Thematik beschäftigen.

1.3 Aufbau der Arbeit

Die Arbeit gliedert sich in sechs Kapitel. Beginnend mit der Einleitung werden in den darauffolgenden Kapiteln mittels Literaturrecherche Grundlagen zu den Themen Quantenmechanik und -kryptografie sowie der Lerntheorie dargelegt. Basierend auf diesen Informationen wird die Anforderungsanalyse durchgeführt, die maßgeblich für die Anwendungsentwicklung ist. Im Kapitel fünf erfolgt die Diskussion der erarbeiteten Ergebnisse. Zuletzt wird ein Fazit gezogen und ein Ausblick auf potenziell weiterführende Arbeiten und Tätigkeiten gegeben.

2 Grundlagen

Die hier beschriebenen Grundlagen bauen auf Grundkenntnissen über Mathematik, speziell lineare Algebra, Physik und Informatik auf und sind für das Verständnis vieler Kapitel Voraussetzung.

Das Kapitel Grundlagen untergliedert sich in drei Bereiche. Zu Beginn werden die theoretischen Aspekte der Quantenmechanik erläutert und grundlegende Prinzipien vorgestellt. Darauf aufbauend folgt ein Kapitel über Quantum Computing, in dem die Funktionsweisen von Qubits bis hin zu komplexen Quantenalgorithmen erklärt werden. Letzten Endes werden verschiedene Lerntheorien beleuchtet, um die im Anschluss zu entwickelnde Bildungsapplikation möglichst lerneffizient zu gestalten.

2.1 Quantenmechanik

Um Quanten und ihre Axiome zu verstehen, wird im Folgenden eine Einführung in die Eigenschaften und die Annahmen der Quantenmechanik gegeben. „Ausgangspunkt für die Entwicklung einer Theorie der Quantenmechanik waren Beobachtungen, die mit herkömmlichen Theorien nicht erkläbar sind“ (Brands, 2011, S. 9). Der Fokus früherer physikalischen Theorien lag auf makroskopischen Körpern. Diese versagen jedoch, wenn kleinere Dimensionen erforscht werden. Der Gegenstand der Betrachtung der Quantenmechanik ist das Verhalten kleinstter Teilchen wie Photonen und Elektronen. (Brands, 2011, vgl. S. 9)

Der bedeutsamste Unterschied zwischen der Quantentheorie und der klassischen Physik ist das Unschärfeprinzip. Dies besagt, dass verschiedene Eigenschaft eines quantenmechanischen Teilchens nur einzeln messbar sind. Somit sind verschiedene Kombinationen von Eigenschaften wie Ort oder Geschwindigkeit eines Teilchens nicht einzeln messbar. Ebenfalls beeinflusst eine Messung das gemessene System, wodurch eine Zustandsänderung des Systems folgt. Hierdurch darf nicht gemessen werden, wenn das System seinen aktuellen Zustand beibehalten soll. Soll ein Teilchen beispielsweise an einem bestimmten Ort gemessen werden, so kann es sich etwa dort befinden (JA-Zustand) oder nicht (NEIN-Zustand). Vor der Messung befindet sich das Teilchen in einem JA-NEIN-Zustand, also in einem Überlagerungszustand von JA und NEIN. Erst nach der Messung kann festgestellt werden, an welchem Ort sich das gemessene Teilchen wirklich befindet. (Brands, 2011, vgl. S.17-18)

Ein quantenmechanisches System wird mittels der Wellenfunktion $\psi(q, t)$ beschrieben. Diese umfasst den dualen Charakter von Elementarteilchen als Teilchen oder Welle. Ebenfalls gibt sie Auskunft über Ort, Zustand und zeitlicher Entwicklung eines Elementarteilchens. Auf eine mathematische Formulierung wird an dieser Stelle verzichtet, kann jedoch

im Anhang eingesehen werden. (Brands, 2011, vgl. S.19-20)

Dabei sind unitäre Räume, auch Hilbert-Raum genannt, die Basis der mathematischen Quanten. Daraus resultiert, dass Messungen an Quanten wie oben erwähnt nur bestimmte Werte liefern, welche im mathematischen Sinn durch Eigenwerte und -vektoren der Matrizen repräsentiert werden, was in späteren Kapiteln genauer ausgeführt wird. Weiterhin gilt das Axiom der Superposition, welches einer Linearkombination, die alle möglichen Zustände des Quantums darstellt, entspricht. Die beschreibt den oben genannten JA-NEIN-Zustand mathematisch.(ANIS u. a., 2021, Textbook 'Quantum States and Qubits' - Chapter 1) (Brands, 2011, vgl. S.22)

Besteht ein System aus mehreren voneinander unabhängigen Teilchen, werden diese jeweils durch eine eigene Wellenfunktion beschrieben. Das Produkt dieser Wellenfunktionen ergibt den Gesamtzustand. (Brands, 2011, vgl. S.22)

Eine Unterscheidung zwischen verschiedenen Systemen erfolgt durch die Kategorisierung in reine und gemischte Systeme., „Wird in einem Experiment ein bestimmter Wert reproduzierbar gemessen, so wird das System durch eine bestimmte Wellenfunktion beschrieben. Systeme mit dieser Eigenschaft nennt man reine Systeme“(Brands, 2011, S.23). Werden die Messbedingungen verändert, sodass nicht immer ein gleicher Wert gemessen wird, sondern verschiedene aus einem Spektrum an Messwerten, nennt sich dies gemischtes System. Die Wellenfunktion wird hierbei als eine Linearkombination von Eigenfunktionen beschrieben. Es wird davon ausgegangen, dass die Messgröße nur bestimmte Messwerte annehmen kann. Der dabei entstehenden Erwartungswert kann dabei unterschiedlich interpretiert werden : (Brands, 2011, vgl. S.23)

- als Wahrscheinlichkeit einer Einzelmessung
- als Mittelwert von gemessenen Einzelwerten
- als Messwert einer mittleren Messung von vielen unabhängigen Systemen

Ein weiteres wichtiges Prinzip der Praxis ist das Dekohärenzprinzip. Wird ein Quantenversuch beispielsweise mit einzelnen Atomen durchgeführt, wechselwirken diese miteinander und führen zu Zustandsänderungen bei den anderen Atomen. Die Dekoheränz beschreibt dieses auseinanderfallen des Systems. Ein Vakuum schafft hierbei Abhilfe. Das erhalten eines quantenmechanischen Systems ist trotz dieser Möglichkeit nur über einen kurzen Zeitraum möglich, bevor zu viele Zustandsänderungen stattgefunden haben. Experimente sind hierdurch schwer durchzuführen und kaum skalierbar.(Brands, 2011, vgl. S.25)

Als letztes soll der Begriff Wirkung und Verschränkung näher erläutert werden. „Wird ein quantenmechanisches System in einem bestimmten Eigenfunktions-/Eigenwertraum [...] beschrieben, so sorgt eine Wirkung für den Übergang in [...] [Anm. des Verf.: einen anderen] Zustand, transformiert also die Mischfaktoren der Eigenfaktoren“(Brands, 2011, S.26). Es werden im Gegensatz zu einer Messung keine Informationen offenbart, wodurch dieser Vorgang reversibel ist. Eine Messung dagegen ist irreversibel. Die Verschränkung

dagegen beschreibt ein System, welches durch eine Gesamtwellenfunktion beschrieben wird. Die Messungen ihrer Eigenwerte ist somit nicht unabhängig voneinander. „Einfache Wirkungen sind bei solchen Systemen global, obwohl sie nur lokal erzeugt werden können[...], lokale Messungen haben globale Aussagekraft, d.h. sie legen die Ergebnisse entfernter Messungen fest“ (Brands, 2011, S.27). (Brands, 2011, vgl. S.26-27)

2.2 Quantum Computing

In klassischen Computersystemen werden einzelne Einheiten, die entweder AN oder AUS sein können, als Bit bezeichnet. Bits befinden sich durch elektrische Ladung entweder in dem Zustand 1 oder 0. Wenige Bits können zusammen mit logischen Gattern bereits einfache Berechnungen durchführen, was bei einer höheren Skalierung und komplexeren Schaltkreisen letztendlich zu den heutigen Informationsverarbeitungssystemen führt.

Quantum Computing baut auf einer ähnlichen Grundlage wie die klassischen Computersysteme auf, doch verwendet anstelle von herkömmlichen Bits *Quantum Bits*, die auf den Prinzipien der Quantenmechanik basieren. Durch Phänomene wie die der *Superposition* und des *Quantenverschränkung* können Schaltkreise nach einer anderen Logik entwickelt werden, die bei korrekter Anwendung oftmals enorme Vorteile gegenüber den klassischen Systemen vorweisen. (Nielsen und Chuang, 2001, Vgl. S. 4-5)

In den folgenden Untersektionen wird die Funktionsweise von Quantensystemen und wie sie dadurch Vorteile erzielen erläutert.

2.2.1 Quantum Bit

Ein klassisches Bit ist wie ein Quantum Bit (kurz: Qubit) ein Teil eines physikalischen Systems. Physikalische Qubits können auf verschiedene Weisen realisiert werden, beispielsweise durch ein zwei-Level-Atom oder Elektronenspins (Steane, 1998, Vgl. S. 22). In dieser Arbeit werden Qubits und alle weiteren Quantenkomponenten ausschließlich mathematisch interpretiert, um die Theoriegrundlagen hardwareunabhängig betrachten zu können. Ebenso befinden sich beide Bitarten nach dem Messen entweder in dem Zustand 1 oder 0. Klassische Bits können nur diese Zustände annehmen, sowohl vor dem Messen als auch danach, während Qubits vor dem Messen die Zustände $|0\rangle$ und $|1\rangle$ als orthonormale Basis für die Bildung von Linearkombinationen verwenden können.

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Linearkombinationen aus $|0\rangle$ und $|1\rangle$ werden auch als *Superposition* bezeichnet. Hierfür wird der Quanten-Zustand eines Qubits als ein komplexer zweidimensionaler Vektorraum betrachtet. Solche Zustände werden wie in der Quantenmechanik mit der *bra-ket* Notation,

also ' $\langle bra |$ ' für Zeilenvektoren und ' $|ket \rangle$ ' für Spaltenvektoren, geschrieben.

$$\begin{aligned} \text{Zustandsvektor} &= |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \\ \alpha, \beta &\in \mathbb{C} \end{aligned} \tag{1}$$

Dies ermöglicht häufig keine genaue Untersuchung des Quanten-Zustands, also von den Amplituden α und β . Während klassische Bits zu jeder Zeit überprüft werden können, in welchem Zustand sie sich befinden, ist bei Qubits eine genaue Überprüfung schwierig, da eine Messung ihren Quanten Zustand kollabieren lässt. „Wenn ein Qubit gemessen wird, resultiert dies entweder in dem Ergebnis 0 mit der Wahrscheinlichkeit $|\alpha|^2$, oder in dem Ergebnis 1 mit der Wahrscheinlichkeit $|\beta|^2$. Natürlich ist $|\alpha|^2 + |\beta|^2 = 1$, da sich die Wahrscheinlichkeiten zu eins summieren müssen.“ (Nielsen und Chuang, 2001, S. 13)

Das bedeutet, dass die Wahrscheinlichkeit einer Messung des Qubits ψ in dem Zustand x resultiert,

$$p(|x\rangle) = |\langle x|\psi\rangle| \tag{2}$$

ist. So hat ein Qubit mit dem Zustandsvektor $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ eine 50% Chance, nach dem Messen in den Zustand $|0\rangle$ zu zerfallen und somit den Wert 0 zurückzugeben, da

$$\begin{aligned} \langle 0|+ \rangle &= \frac{1}{\sqrt{2}}\langle 0|0 \rangle + \frac{1}{\sqrt{2}}\langle 0|1 \rangle \\ \langle 0|+ \rangle &= \frac{1}{\sqrt{2}} \cdot 1 + \frac{1}{\sqrt{2}} \cdot 0 \\ \langle 0|+ \rangle &= \frac{1}{\sqrt{2}} \end{aligned}$$

$$|\langle 0|+ \rangle|^2 = \frac{1}{2},$$

oder kurz gesagt, weil $|\frac{1}{\sqrt{2}}|^2 = 0.5$ ist. Die Wahrscheinlichkeit für eine Messung des Werts 1 und dem folgenden Zerfall in den Zustand $|1\rangle$ liegt bei $|+\rangle$ ebenfalls bei 50%.

Visualisierung eines Qubit Zustands

Der Zustand eines Qubits kann auch geometrisch repräsentiert werden. Durch die Einführung einer Messung des relativen Phasenunterschieds zwischen $|0\rangle$ und $|1\rangle$ wird *Formel 1*

wie folgt erweitert und α und β auf rationale Zahlen beschränkt:

$$|q\rangle = \alpha |0\rangle + e^{i\phi} \beta |1\rangle \quad (3)$$

$$\alpha, \beta, \phi \in \mathbb{R}.$$

Wendet man zusätzlich die trigonometrische Identität $\sin^2 x + \cos^2 x = 1$ auf den normalisierten Qubit Zustand $|\alpha|^2 + |\beta|^2 = 1$ an, so können Alpha und Beta auch als $\alpha = \cos \frac{\theta}{2}$ und $\beta = \sin \frac{\theta}{2}$ beschrieben werden. Dies ermöglicht die Visualisierung eines Qubit Zustands als Punkt auf einer dreidimensionalen Sphäre durch die Variablen θ und ψ :

$$|q\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \quad (4)$$

$$\theta, \psi \in \mathbb{R}.$$

Diese Sphäre wird *Bloch-Kugel* genannt. Sie beschreibt den Zustand eines einzelnen Qubits und wird oft für die Visualisierung der Auswirkungen, die bestimmte Operationen auf ein Qubit haben, verwendet.

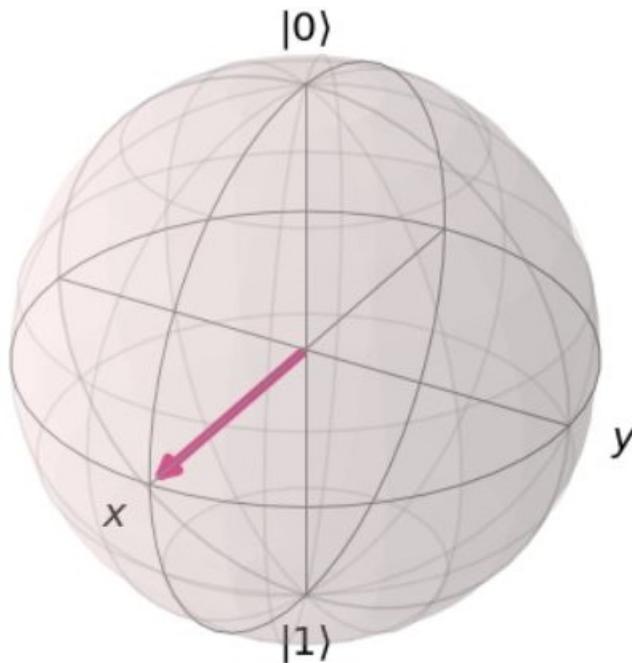


Abb. 2.1: Eine Bloch-Kugel eines Qubits im Zustand $|+\rangle$, die mit dem Qiskit SDK erstellt wurde.

Theoretisch lassen sich durch die unendlich große Anzahl an Punkten auf der Oberfläche der Kugel auch unendlich viele Quantenzustände bilden. „Diese Schlussfolgerung ist aber irreführend [...], da die Messung eines Qubits dessen Zustand ändert, indem es aus seiner Superposition von $|0\rangle$ und $|1\rangle$ in den spezifischen Zustand kollabiert, der mit dem Messergebnis übereinstimmt. Wenn zum Beispiel die Messung von $|+\rangle$ den Wert 0 ergibt, dann wird der Zustand des Qubits nach der Messung $|0\rangle$ sein. Warum kommt es zu dieser Art

von Zusammenbruch? Das weiß keiner.“ (Nielsen und Chuang, 2001, S. 15) Dieses Problem wird in den Hintergrund gerückt, indem Qubits so selten wie nur möglich gemessen werden. Denn auch wenn die versteckten Quantum Informationen eines Qubits nicht wirklich messbar sind, ist es möglich, sich diese Informationen zunutze zu machen. Das Verständnis jener Quanteninformationen schafft die Grundlage für Quantum Computing.

Zusammenspiel mehrerer Qubits

Jedes Qubit besitzt zwei komplexe Amplituden α und β . Um den gemeinsamen Zustand von zwei Qubits zu beschreiben, werden folglich vier komplexe Amplituden benötigt. Diese werden in einem 4D-Vektor zusammengefasst:

$$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \quad (5)$$

Die Regeln für die Messung und Normalisierung verändern sich dabei nicht:

$$p(|00\rangle) = |\langle 00|\alpha\rangle|^2 = |\alpha_{00}|^2,$$

da

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

Bei zwei getrennten Qubits werden beide Qubit Zustände durch ein Tensorprodukt zusammengefasst:

$$|a\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}, \quad |b\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

$$|ba\rangle = |b\rangle \otimes |a\rangle = \begin{bmatrix} b_0 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \\ b_1 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{bmatrix} \quad (6)$$

Diese Zusammenfassung der Zustände mittels des Tensorprodukts lässt sich auf eine beliebige Anzahl an Qubits anwenden. Hierbei gilt allerdings: „Wenn wir n Qubits haben, müssen wir den Überblick über 2^n komplexe Amplituden behalten. Wie wir sehen kön-

nen, wächst die Größe der Vektoren exponentiell mit der Anzahl der Qubits. Dies ist der Grund, warum Quantencomputer mit einer großen Anzahl von Qubits so schwer zu simulieren sind. Ein moderner Laptop kann problemlos einen allgemeinen Quantenzustand von etwa 20 Qubits simulieren, aber die Simulation von 100 Qubits ist zu schwierig für die größten Supercomputer.“ (ANIS u. a., 2021, Textbook 'Multiple Qubits and Entangled States' - Chapter 1)

verschränkte Zustände

Befindet sich ein einzelnes Qubit in einer Superposition, so zerfällt diese nach einer Messung in die Zustände $|0\rangle$ oder $|1\rangle$. Wenn das Qubit aber Teil eines Systems $|s\rangle$ aus mehreren Qubits ist, wie zum Beispiel bei dem *Bell-Zustand*, dann hat die Messung von Qubit *A* eine direkte Auswirkung auf den Zustand von Qubit *B* und lässt dessen Superposition ebenfalls zerfallen.

$$|s\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (7)$$

Dieser zwei-Qubit-Zustand *Bell-Zustand* befindet sich in einer Superposition und kann nach einer Messung ausschließlich in $|00\rangle$ oder $|11\rangle$ zerfallen. Wird nur ein Qubit des *Bell-Zustand* gemessen, ist direkt erkennbar, in welchen Zustand sich das andere Qubit befinden muss. Erhält man nach der Messung von Qubit *A* zum Beispiel den Wert 1, so verändert sich der gemeinsame Zustand zu $|s\rangle = |11\rangle$.

Hierbei ist es egal, wie physisch weit entfernt Qubit *A* von Qubit *B* ist, da sie *verschränkt* sind. Dieses Phänomen wird auch als *Quantum Nonlocality* bezeichnet.

2.2.2 Quantengatter

In der klassischen Informationstechnik werden logische Schaltungen mithilfe verschiedener *Gatter* realisiert. Ein *Gatter* setzt boolsche Funktionen um, die binäre Eingangssignale zu einem binären Ausgangssignal verarbeiten.

Das Prinzip von Quantengattern ist dasselbe. Häufig sind die inneren Funktionen aber deutlich komplexer, um Gebrauch von den Möglichkeiten der Quantenmechanik zu machen.

Single Qubit Gatter

Um den Zustand eines einzelnen Qubits zu ändern, ohne dessen potenzielle Superposition zu zerstören, können *Single Qubit Gatter* auf das Qubit angewandt werden. Beispielhaft

dafür sind die *Pauli Gatter* X, Y, und Z mit den Funktionen (Matrizen):

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (8)$$

Diese Single Qubit Gatter führen Rotationen mit dem Wert π um die jeweilige Achse der Bloch-Kugel durch. Liegt die Basis eines Qubits beispielsweise auf der Z-Achse mit den Eigenzuständen $|0\rangle$ und $|1\rangle$, was standardmäßig der Fall ist, so hat ein *X-Gatter* dieselbe Wirkung wie ein *NOT-Gatter* in der Digitaltechnik:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Eine weitere häufig verwendete Basis ist die X-Basis, deren Eigenzustände $|+\rangle$ und $|-\rangle$ sind. Ein Umschwung von der Z-Basis auf die X-Basis kann durch das *Hadamard-Gatter* erreicht werden.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (9)$$

Die Anwendung des *Hadarmad-Gatter* auf $|0\rangle$ oder $|1\rangle$ resultiert in einer Superposition:

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \end{aligned}$$

Die Anwendung eines Hadarmad Gatter auf ein Qubit mit dem Zustand $|z\rangle$ kann dank der Euler'schen Identität auch generalisiert geschrieben werden:

$$\begin{aligned} e^{xi} &= \cos(x) + i\sin(x) \xrightarrow{x=\pi} e^{\pi i} = -1 \\ H|z\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{2\pi iz}{2}}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi iz}|1\rangle). \end{aligned}$$

Qubit Gatter können hintereinander ausgeführt werden, um bestimmte logische Operationen durchzuführen. So kann die Wirkung eines *X-Gatters* beispielsweise auch durch zwei *Hadamard Gatter* und ein *Z-Gatter* erzielt werden:

$$HZH = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$

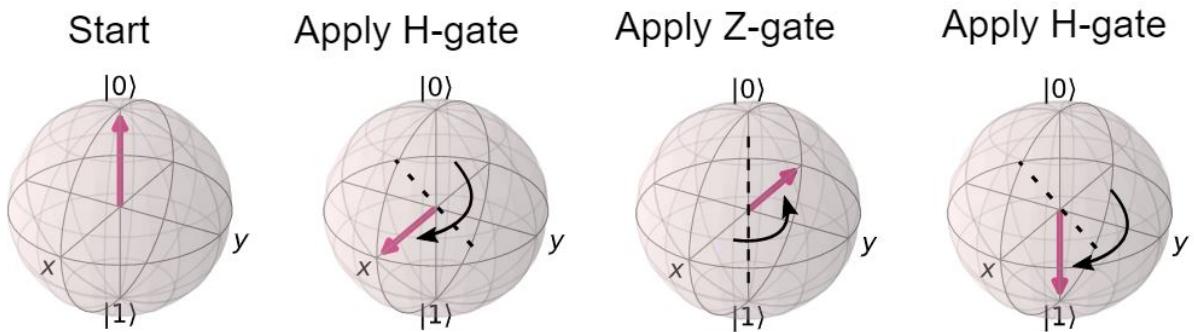


Abb. 2.2: Visualisierung einer *HZH* Gatterfolge auf ein Qubit mit dem Startzustand $|0\rangle$. Nach Anwendung der Gatter befindet sich das Qubit im Zustand 1 - es wurde ein *X-Gatter* bzw. eine *NOT* Operation durchgeführt. (ANIS u. a., 2021, Vgl. Textbook 'Single Qubit Gates' - Chapter 4)

Theoretisch existieren unendlich viele *Single Qubit Gatter*. Dabei werden die Rotationen häufig auch parametrisiert. Die einzige Bedingung für ein valides Quantum Gatter ist *Unitarität*. Eine Quantum Gatter U muss also reversibel sein. Für U bedeutet das, dass $U^\dagger U = I$, also adjunkte Matrix U^\dagger mal Matrix U gleich Einheitsmatrix I ist.

Ein arbiträres (willkürliches) Single Qubit Gatter U kann durch eine endliche Anzahl an Qubit Gatter realisiert werden:

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix}, \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \quad (10)$$

$$\alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

„Die zweite Matrix [ist] nur eine gewöhnliche Drehung. Es stellt sich heraus, dass die erste und die letzte Matrix auch als Drehungen in einer anderen Ebene verstanden werden können. Diese Zerlegung kann verwendet werden, um ein genaues Rezept für die Ausführung eines beliebigen Quantenlogik-Gatters auf ein einzelnes Qubit zu erhalten.“ (Nielsen und Chuang, 2001, S. 20)

Multiple Qubit Gatter

Obwohl es unendlich viele verschiedene Single Qubit Gatter gibt, sind die Grenzen an Möglichkeiten sehr eingeschränkt. Multiple Qubit Gatter verschaffen Abhilfe, indem komplexere Funktionen mit mehreren Qubits gleichzeitig durchgeführt werden.

Auch für Multiple Qubit Gatter gilt die Regel, dass die Gatter unitär sein müssen. Das bedeutet, dass klassische *XOR*- oder *NAND-Gatter* in der Welt des Quantum Computings nicht existieren und aufwändig aus anderen Gatter-Kombinationen kreiert werden müssen, da diese in ihrer Natur nicht reversibel sind und dadurch Informationen verloren gehen.

Ein wichtiges Multiple Qubit Gatter ist das *Controlled NOT-Gatter*. Aus *CNOT-Gatter* und Single Qubit Gatter kann jedes beliebige Multiple Quantum Gatter erstellt werden. (Nielsen und Chuang, 2001, Vgl. S.22)

Ein CNOT-Gatter besteht aus zwei Qubits: dem Kontroll- und dem Ziel-Qubit. Ist das Kontroll-Qubit im Zustand $|1\rangle$, so wird ein *X-Gatter* auf das Ziel-Qubit ausgeführt. Ist das Kontroll-Qubit $|0\rangle$, so verändert sich nichts.

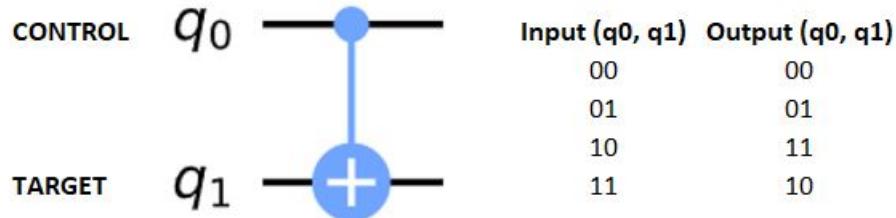


Abb. 2.3: Controlled NOT-Gatter

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad CNOT |\alpha\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} = \begin{bmatrix} \alpha_{00} \\ \alpha_{11} \\ \alpha_{10} \\ \alpha_{01} \end{bmatrix} \quad (11)$$

Gleichung 11 zeigt, dass das CNOT-Gatter die Zustände $|01\rangle$ und $|11\rangle$ vertauscht. Befindet sich das Kontroll-Qubit vor Anwendung des CNOT-Gatters in einer Superposition, entsteht der in Kapitel 2.2.1 erwähnte Bell-Zustand und die Qubits werden verschränkt:

$$|0\rangle \otimes |+\rangle = |0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle),$$

$$CNOT |0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Befinden sich sowohl Kontroll- als auch Ziel-Qubit in einer Superposition wie $|-\rangle$, erstellt durch direkt davor angewendete H-Gatter, so ist das Phänomen des *Phase-Kickbacks* zu erkennen:

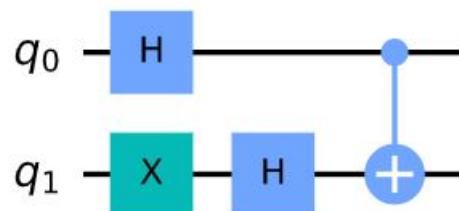


Abb. 2.4: Anwendung des CNOT-Gatters auf den Qubit Zustand $|-\rangle$

$$\begin{aligned} |-\rangle &= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) \\ CNOT\,|-\rangle &= \frac{1}{2}(|00\rangle + |11\rangle - |10\rangle - |01\rangle) = |--\rangle, \end{aligned}$$

$|+\rangle$ = Kontroll, $|-\rangle$ = Ziel.

„Das ist interessant, weil [das CNOT-Gatter] den Zustand des Kontroll-Qubits beeinflusst, während der Zustand des Ziel-Qubits unverändert bleibt. [...] Kickback bedeutet, dass der durch ein Gatter zu einem Qubit hinzugefügte Eigenwert durch eine controlled-Operation in ein anderes Qubit ‘zurückgekickt’ wird.“ (ANIS u. a., 2021, Textbook ‘Phase Kick-back’ - Chapter 1 & 2) Dieser Effekt betrifft auch andere Controlled-Gatter.

Um die Funktion eines klassischen *AND-Gatter* zu implementieren, können verschiedene Gatter-Kombinationen verwendet werden. Als Beispiel können zwei Controlled-H-Gatter und ein Controlled-Z-Gatter verwendet werden. Das CZ-Gatter wird aus einem CNOT-Gatter und zwei weiteren H-Gattern gebildet. Die CH-Gatter werden auf eine ähnliche Weise gebildet, jedoch werden anstelle von H-Gattern jeweils Rotationen um $\frac{\pi}{4}$ und $-\frac{\pi}{4}$ um die Y-Achse verwendet.

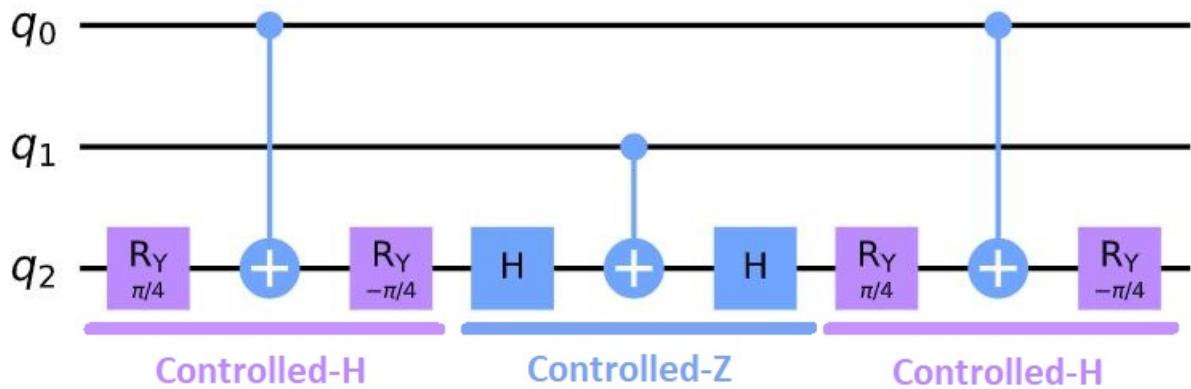


Abb. 2.5: Beispiel Implementation eines Quantum AND-Gatters aus zwei CH-Gatter und einem CZ-Gatter

Dieses AND-Gatter benötigt zwei Kontroll-Qubits q_0 und q_1 sowie ein Ziel-Qubit q_2 . Bei $|00\rangle$ verändert sich der Zustand von q_2 nicht, während unter $|11\rangle$ die Gatterfolge $HZH = X$, also eine NOT-Operation, auf q_2 durchgeführt wird. Die Zustände $|01\rangle$ und $|10\rangle$ erzeugen entweder eine zunächst irrelevante relative Phase durch alleinige Ausführung des CZ-Gatter auf q_2 oder gleichen sich gegenseitig aus.

Als abstrakte Betrachtung für Quantengatter wird die Variable U verwendet, welche eine beliebige unitäre Matrix repräsentiert. Durch eine Erweiterung des CNOT-Gatter kann aus dem U -Gatter ein *Controlled-U-Gatter* entstehen, das genau ein Kontroll-Qubit und n Ziel-Qubits besitzt. Wenn das Kontroll-Qubit im Zustand $|0\rangle$ ist, passiert nichts. Wenn dieses sich aber im Zustand $|1\rangle$ befindet, so wird auf alle n Ziel-Qubits das U -Gatter angewendet.

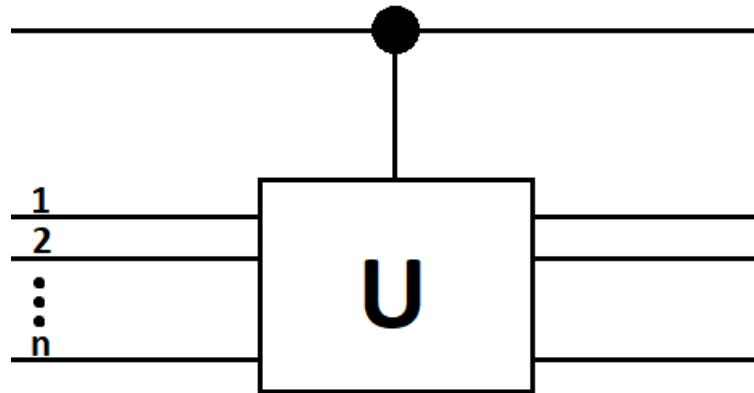


Abb. 2.6: Controlled-U-Gatter mit n Ziel Qubits

Mit dieser Denkweise kann beispielsweise auch das CNOT-Gatter beschrieben werden:
 $U = X$ und $n = 1$. (Nielsen und Chuang, 2001, Vgl. S.23)

2.2.3 Quantenschaltung

Eine Quantenschaltung ist ein Ausführungsplan von verschiedenen Operationen auf ein oder mehrere Qubits. Dieser Plan besteht aus Qubits, die jeweils eine horizontale Leitung mit verschiedenen Gattern haben, und wird von links nach rechts gelesen.

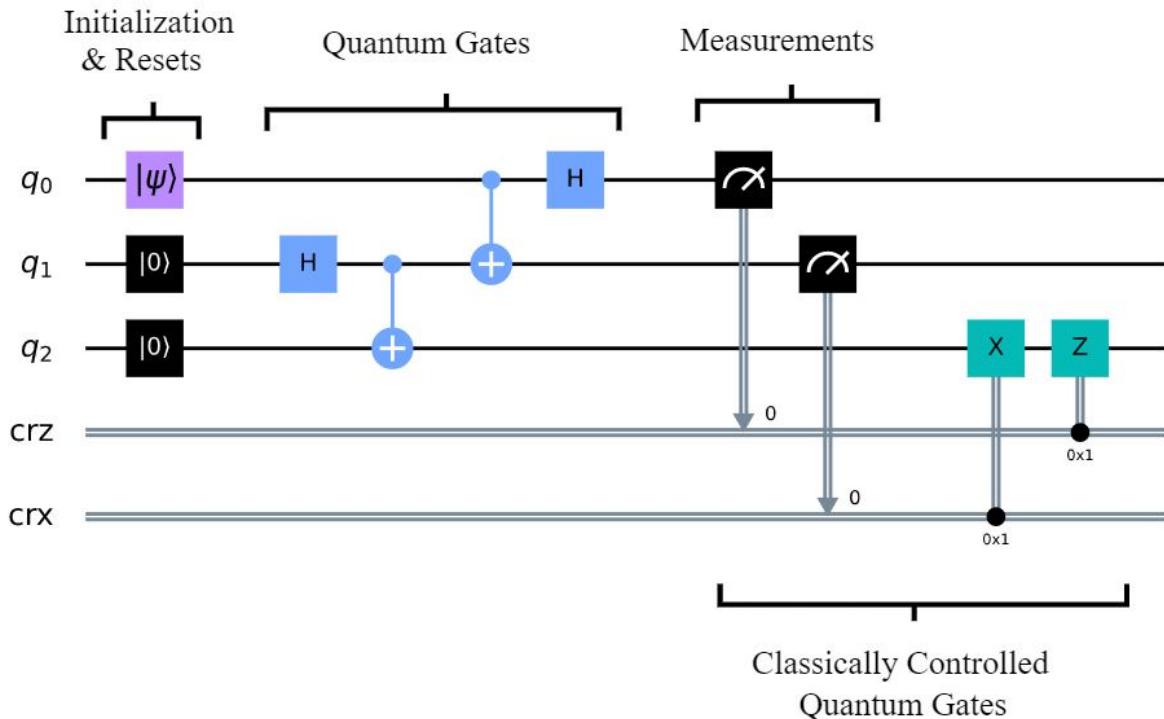


Abb. 2.7: Beispiel: Algorithmus der Quanten-Teleportation (ANIS u. a., 2021, Textbook 'Quantum Circuits' - Chapter 3)

Eine Quantenschaltung besteht i.d.R. aus vier verschiedenen Phasen. Die erste ist die der Initiierung, wo sich Qubits zu Beginn der Ausführung entweder standardmäßig im Zustand $| 0 \rangle$, oder nach expliziter Kennzeichnung auch in einem anderen Zustand, befinden. Danach folgen Quantengatter, welche die Zustände der Anfangsqubits manipulieren. Anschließend werden die manipulierten Qubits gemessen und das Ergebnis als klassische Bits gespeichert. Abschließend werden unter Umständen noch von den Messergebnissen abhängige Gatter ausgeführt. (ANIS u. a., 2021, Vgl. Textbook 'Quantum Circuits' - Chapter 3)

Anzumerken ist, dass Quantenschaltung keine Schleifen besitzen und ausschließlich reversible bzw. unitäre Operationen durchführen.

2.2.4 Quanten-Fouriertransformation

Ist ein mathematisches Problem nur schwer lösbar, kann es einfacher sein, das Problem zu einem anderen Problem zu transformieren, dessen Lösung bereits bekannt ist. Die Quanten-Fouriertransformation (QFT) übernimmt genau diese Rolle und ist ein wichtiger Baustein für andere Quantenalgorithmen, wie beispielsweise der Phasenschätzungs- und somit auch des Shor Algorithmus.

Grundlegend wird eine klassische diskrete Fouriertransformation auf quantenmechanische Amplituden von Wellenfunktionen durchgeführt. Die diskrete Fouriertransformation wird auf einen Vektor $(x_0, x_1, \dots, x_{N-1})$ mit N als Parameter angewandt und resultiert in einem transformierten Vektor $(y_0, y_1, \dots, y_{N-1})$. (Nielsen und Chuang, 2001, Vgl. S. 217)

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp\left(\frac{2\pi i j k}{N}\right) \quad (12)$$

Die Quanten-Fouriertransformation ist nahezu identisch. Die Transformation wird auf der orthonormalen Basis $|0\rangle, \dots, |N-1\rangle$ durchgeführt und resultiert in den von $|x\rangle$ transformierten Amplituden $|\tilde{x}\rangle$ in einer Superposition:

$$|\tilde{x}\rangle = QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(\frac{2\pi i x y}{N}\right) |y\rangle \quad (13)$$

$$N = 2^n, \quad n = \text{Anzahl der Qubits}, \quad |y\rangle = \text{Zustand mit Binärwert von } y.$$

Die QFT transformiert Qubits zwischen der Z-Basis und der Fourier-Basis, die eine Variation der X-Basis ist. Ein Zustand der Fourier-Basis wird mit einer Tilde \sim geschrieben. Um die Binärität der Qubits zu berücksichtigen, muss die obige Formel vor der Anwendung ausgeschrieben werden:

$$\begin{aligned} |\tilde{x}\rangle &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^n \exp\left(xy_k \cdot \frac{2\pi i}{2^k}\right) |y_1, y_2, \dots, y_n\rangle \\ |\tilde{x}\rangle &= \frac{1}{\sqrt{N}} \left(|0\rangle + \exp(x \cdot \frac{2\pi i}{2^1}) |1\rangle \right) \otimes \left(|0\rangle + \exp(x \cdot \frac{2\pi i}{2^2}) |1\rangle \right) \otimes \dots \otimes \left(|0\rangle + \exp(x \cdot \frac{2\pi i}{2^n}) |1\rangle \right). \end{aligned}$$

Somit sieht die Formel für beispielsweise einen drei Qubit Zustand mit $x = |6_{dez}\rangle \xrightarrow{\text{Binär}} x = |110_b\rangle$ wie folgt aus:

$$\begin{aligned} |\tilde{6}\rangle &= \frac{1}{\sqrt{8}} \sum_{y=0}^7 \prod_{k=1}^3 \exp\left(6y_k \cdot \frac{2\pi i}{2^k}\right) |y_1, y_2, y_3\rangle \\ |\tilde{6}\rangle &= \frac{1}{\sqrt{8}} \left(|0\rangle + \exp\left(6 \cdot \frac{2\pi i}{2}\right) |1\rangle \right) \otimes \left(|0\rangle + \exp\left(6 \cdot \frac{2\pi i}{4}\right) |1\rangle \right) \otimes \left(|0\rangle + \exp\left(6 \cdot \frac{2\pi i}{8}\right) |1\rangle \right). \end{aligned}$$

Durch das Beispiel wird deutlich, dass jedes Qubit von der Z-Basis in die X-Basis transformiert wird und auch eine Rotation um die Z-Achse durchführt. Die Rotationen werden jeweils x_{dez} Mal wiederholt. Die Größe der ursprünglichen Rotation des Qubit Zustands ist abhängig von seiner Position in der Reihenfolge x_b .

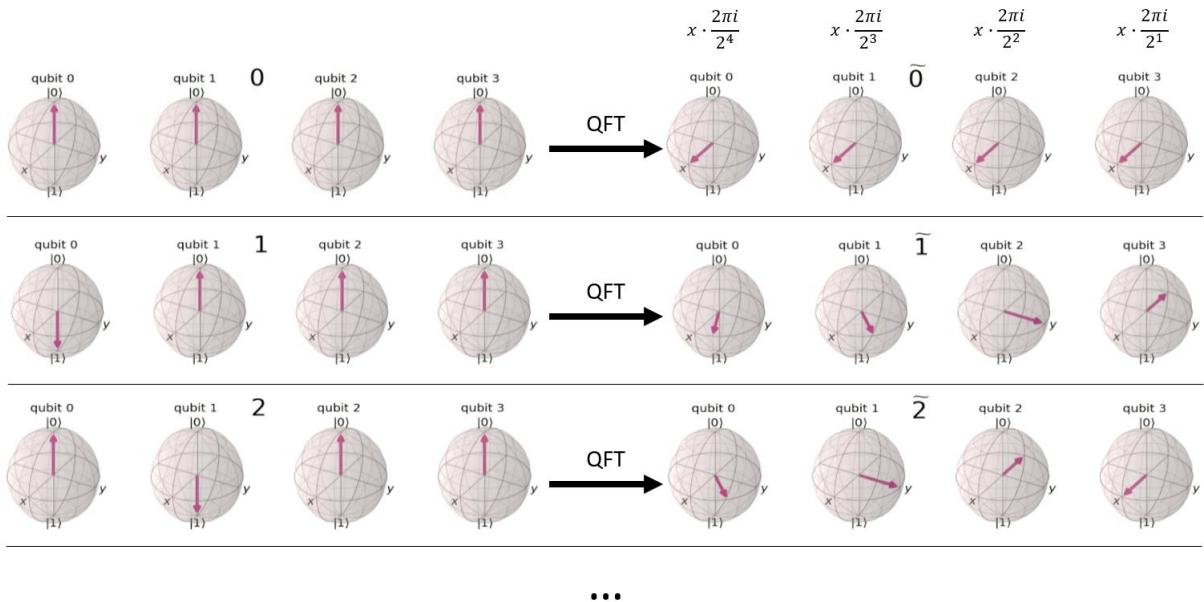


Abb. 2.8: Beispielhafte Darstellung einer Quanten-Fouriertransformation mit vier Qubits und $x_{dez} \in \{0, 1, 2, \dots\}$, $\max(x_{dez}) = 15$. (ANIS u. a., 2021, Vgl. Textbook 'Quantum Fourier Transform' - Chapter 2)

Um die QFT in der realen Welt anzuwenden, muss die vorherige Formel zu einer Quantenschaltung umgebaut werden. Hierfür werden zwei verschiedene Gatter verwendet: H-Gatter und Controlled-UROT-Gatter.

Ein CROT-Gatter ist parametrisiert und besteht aus einem UROT-Gatter (Unitary Rotation Gate):

$$CROT_k = \begin{bmatrix} I & 0 \\ 0 & UROT_k \end{bmatrix}, \quad UROT_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{bmatrix}. \quad (14)$$

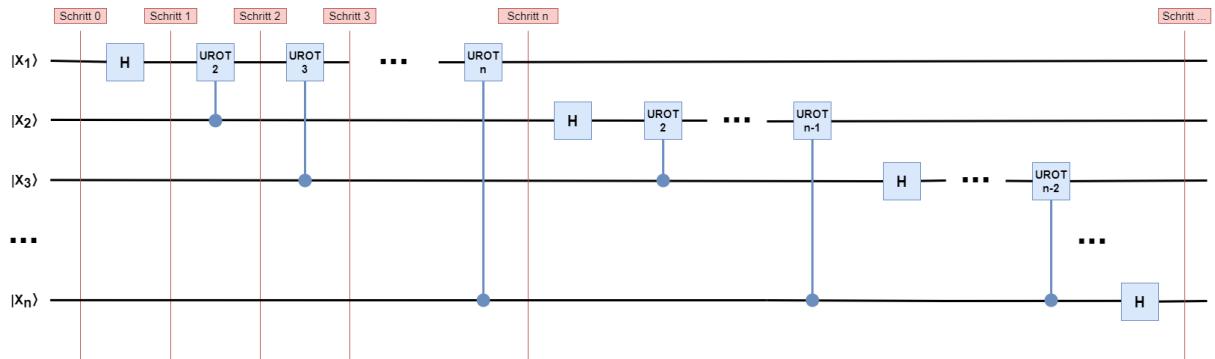


Abb. 2.9: Quanten-Fouriertransformationsschaltkreis mit n Qubits

Die Anzahl an Gatter pro Leitung nimmt linear mit der Rangfolge ab. Somit befinden sich auf der ersten Leitung n Gatter und auf der letzten nur noch eins.

Jedes Qubit durchläuft zu Beginn ein H-Gatter, was denselben Effekt wie eine UROT-Gatter Rotation mit dem Parameter eins hat. Die Größe der UROT-Gatter Rotationen sind abhängig von den Gattern der bereits durchgeföhrten UROT-Gattern auf der jeweiligen Leitung. Das heißt, dass der UROT-Gatter Parameter k immer die Anzahl der bereits ausgeführten Gatter auf der jeweiligen Leitung plus eins ist.

Im folgenden Beispiel wird der Zustand eines QFT-Schaltkreises $|\psi\rangle$ mit drei Qubits in sechs Schritten Stück für Stück berechnet:

$$\begin{aligned}
 |\psi_1\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_1 \cdot \frac{2\pi}{2}) |1\rangle \right) \otimes |x_2\rangle \otimes |x_3\rangle \\
 |\psi_2\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_1 \cdot \frac{2\pi}{2} + x_2 \cdot \frac{2\pi}{4}) |1\rangle \right) \otimes |x_2\rangle \otimes |x_3\rangle \\
 |\psi_3\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_1 \cdot \frac{2\pi}{2} + x_2 \cdot \frac{2\pi}{4} + x_3 \cdot \frac{2\pi}{8}) |1\rangle \right) \otimes |x_2\rangle \otimes |x_3\rangle \\
 |\psi_4\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_1 \cdot \frac{2\pi}{2} + x_2 \cdot \frac{2\pi}{4} + x_3 \cdot \frac{2\pi}{8}) |1\rangle \right) \otimes \left(|0\rangle + \exp(x_2 \cdot \frac{2\pi}{2}) |1\rangle \right) \otimes |x_3\rangle \\
 |\psi_5\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_1 \cdot \frac{2\pi}{2} + x_2 \cdot \frac{2\pi}{4} + x_3 \cdot \frac{2\pi}{8}) |1\rangle \right) \otimes \\
 &\quad \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_2 \cdot \frac{2\pi}{2} + x_3 \cdot \frac{2\pi}{4}) |1\rangle \right) \otimes |x_3\rangle \\
 |\psi_6\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_1 \cdot \frac{2\pi}{2} + x_2 \cdot \frac{2\pi}{4} + x_3 \cdot \frac{2\pi}{8}) |1\rangle \right) \otimes \\
 &\quad \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_2 \cdot \frac{2\pi}{2} + x_3 \cdot \frac{2\pi}{4}) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp(x_3 \cdot \frac{2\pi}{2}) |1\rangle \right)
 \end{aligned}$$

2.2.5 Quantum Phase Estimation

Die Quantum Phase Estimation (QPE) ist eine sehr wichtige Subroutine in Quantum Computing. Sie ermöglicht die Bestimmung von Phasen verschiedener Qubits und ist ein wichtiger Bestandteil des Shor Algorithmus.

Wenn ein unitärer Operator U , also eine unitäre Matrix, einen Eigenvektor $|\psi\rangle$ mit dem Eigenwert $\exp(2\pi i\theta)$ besitzt und der Wert θ unbekannt ist, dann kann dieser mit der Quantum Phase Estimation Routine bestimmt werden.

Einschub: Eigenwerte sind die Skalierungsfaktoren von Eigenvektoren. Eigenvektoren sind auch als Nullvektoren bekannt und bilden eine orthonormale Basis. Das bedeutet, dass die Eigenvektoren orthogonal zueinander stehen. Bei einer unitären Matrix haben die Eigenwerte die Form $\exp(i\theta)$ und sind auf 1 normiert. So skaliert beispielsweise ein Operator U (unitäre Matrix) den Zustand $|\psi\rangle$ mit einer Konstante λ :

$$U|\psi\rangle = \lambda|\psi\rangle, \quad \lambda \in \mathbb{C}$$

Hier ist $|\psi\rangle$ ein *Eigenzustand / Eigenket / Eigenvektor* von U und die Konstante λ ein *Eigenwert* von U . Die Menge an Eigenwerten $\{\lambda\}$ ist das *Spektrum* von U .

„Ein Eigenwert hat nicht nur etwas mit einem Zustand allein zu tun, sondern mit einem Zustand und einem Operator. Der Eigenwert beschreibt also etwas über den Effekt eines Operators auf einen Zustand.“ (Steane, 2021)

Da $\exp(2\pi i\theta)$ eine globale Phase ist, kann θ nicht normal gemessen werden:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &\xrightarrow{\text{Messung}} 0: 0.5, 1: 0.5 \\ \exp\left(\frac{i\pi}{2}\right)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &\xrightarrow{\text{Messung}} 0: \left|\exp\left(\frac{i\pi}{2}\right)\frac{1}{\sqrt{2}}\right| = 0.5, 1: ... = 0.5. \end{aligned}$$

Wenn die globale Phase $\exp(2\pi i\theta)$ durch einen unitären Operator U hinzugefügt wurde, also $U|\psi\rangle = \exp(2\pi i\theta)|\psi\rangle$, dann kann die globale Phase aber durch Quantum Phase Estimation angenähert werden. (Asfaw und Qiskit, Vgl. Min. 15) Es wird davon ausgegangen, dass diese Operation U nicht vollständig bekannt ist, weshalb sie in diesem Fall auch als *Black Box* oder *Oracle* bezeichnet wird.

Um diese grundlegende Idee umzusetzen, wird ein Messungsqubit in dem Zustand $|0\rangle$ initialisiert und durch ein H-Gatter in eine Superposition versetzt. Nun kann mittels eines Controlled-U-Gatter die unbekannte Phase von $|\psi\rangle$ auf das Messungsqubit durch den zuvor erwähnten *Phase Kickback* Effekt übertragen werden, weshalb im letzten Schritt ein weiteres H-Gatter auf das Messungsqubit angewendet wird.

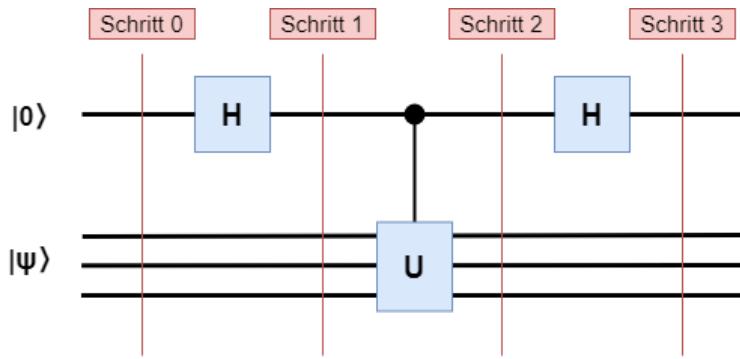


Abb. 2.10: Grundlegende Idee der Quantum Phase Estimation

Die übertragene und umgewandelte Phase von $|\psi\rangle$ auf das Messungssqubit kann nun gemessen werden. Dafür muss die Schaltung und somit auch die anschließende Messung des Messungssqubits sehr oft wiederholt werden, und die Wahrscheinlichkeiten des Erhalts von 0 und 1 zu beobachten, wodurch sich die Phase annähernd berechnen lässt.

Durch eine genaue Betrachtung des Quantenschaltungszustands nach jedem Schritt wird dieser Vorgang anschaulicher:

$$\text{Schritt 0: } |0\rangle |\psi\rangle$$

$$\text{Schritt 1: } \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle |\psi\rangle + |1\rangle |\psi\rangle)$$

$$\text{Schritt 2: } \frac{1}{\sqrt{2}} (|0\rangle |\psi\rangle + |1\rangle \exp(i\theta_\psi) |\psi\rangle)$$

$$\begin{aligned} \text{Schritt 3: } & \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |\psi\rangle + \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \exp(i\theta_\psi) |\psi\rangle \right) \\ &= \frac{1}{2} \left[(1 + \exp(i\theta_\psi)) |0\rangle + (1 - \exp(i\theta_\psi)) |1\rangle \right]. \end{aligned}$$

Wie aus dem Ergebnis aus Schritt 3 die Phase geschlussfolgert werden kann, wird in einem Beispiel deutlich. Die Wahrscheinlichkeiten, die Werte 0 oder 1 zu messen, sind wie folgt:

$$\begin{aligned} P(0) &= \left| \frac{1}{2} (1 + \exp(i\theta_\psi)) \right|^2 \\ P(1) &= \left| \frac{1}{2} (1 - \exp(i\theta_\psi)) \right|^2. \end{aligned} \tag{15}$$

Wird der Schaltkreis nun sehr oft ausgeführt und die Ergebnistabelle des Messungssqubits ergibt langfristig beispielhaft $P(0) = 99.24\%$ und $P(1) = 0.76\%$, so können diese angenäherten Wahrscheinlichkeiten in Formel 15 eingesetzt werden, um die Phase $\theta_\psi = 10^\circ$ zu berechnen. (Asfaw und Qiskit, Vgl. Min. 18-23)

Dieser Vorgang ist ohne großen Aufwand durch die ständige Wiederholung sehr ungenau. Mit mehreren Messungssqubits kann eine höhere Genauigkeit mit weniger Wiederholungen erzielt werden. Hierfür muss die Quantenschaltung erweitert und angepasst werden.

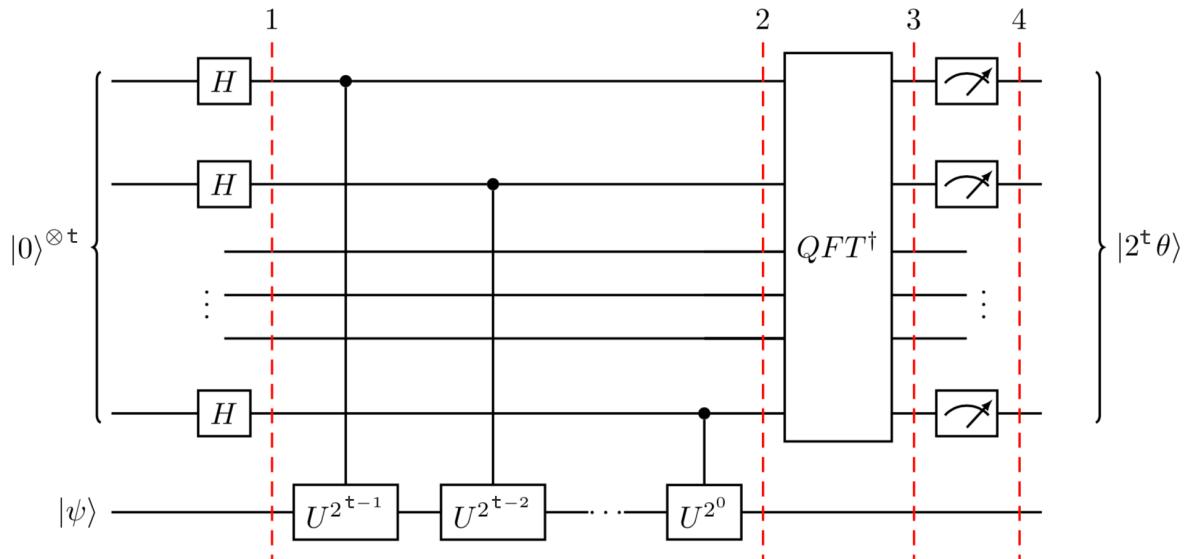


Abb. 2.11: Quantum Phase Estimation Subroutine mit t Messungsquibits (ANIS u. a., 2021, Textbook 'Quantum Phase Estimation' - Chapter 1)

Eine schrittweise Berechnung des Schaltungszustands verdeutlicht die Funktionsweise:

$$\text{Schritt 0: } |0\rangle^{\otimes t} |\psi\rangle$$

$$\text{Schritt 1: } \left(\frac{1}{\sqrt{2}}\right)^t \left(|0\rangle + |1\rangle\right)^{\otimes t} |\psi\rangle$$

$$\text{Einschub: } U^{2^x} |\psi\rangle = U^{2^{x-1}} U |\psi\rangle = U^{2^{x-1}} \exp(i\theta_\psi) |\psi\rangle = U^{2^{x-2}} \exp(i\theta_\psi) \exp(i\theta_\psi) |\psi\rangle$$

$$\begin{aligned} \text{Schritt 2: } & \left(\frac{1}{\sqrt{2}}\right)^t \left(|0\rangle + \exp(i\theta_\psi 2^{t-1}) |1\rangle\right) \otimes \left(|0\rangle + \exp(i\theta_\psi 2^{t-2}) |1\rangle\right) \dots \\ & \dots \otimes \left(|0\rangle + \exp(i\theta_\psi 2^{t-t}) |1\rangle\right) |\psi\rangle \end{aligned}$$

Der Schaltungszustand nach Schritt zwei ähnelt stark dem einer QFT.

$$\text{Einschub: } QFT |x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + \exp(x \cdot \frac{2\pi i}{2^1}) |1\rangle\right) \otimes \dots \otimes \left(|0\rangle + \exp(x \cdot \frac{2\pi i}{2^n}) |1\rangle\right)$$

Der einzige Unterschied ist die Phase θ_ψ der QPE, da die QFT $2\pi \frac{\theta_\psi}{2^n}$ als Phase verwendet. Folglich wird in Schritt zwei eine QFT mit einer anderen Phase durchgeführt. (Asfaw und Qiskit, Vgl. Min. 33)

Das ist der Grund, weshalb auf die Messungsquibits am Ende des Schaltkreises noch eine inversive QFT angewandt wird. Dadurch kann die unbekannte Phase von ψ , die auf die Messungsquibits in QFT Form übertragen wird, als $|2^t \theta_\psi\rangle$ gemessen werden. Dies hat zufolge, dass die Phase θ_ψ mit 2^t multipliziert und somit die Genauigkeit abhängig von t erhöht wird.

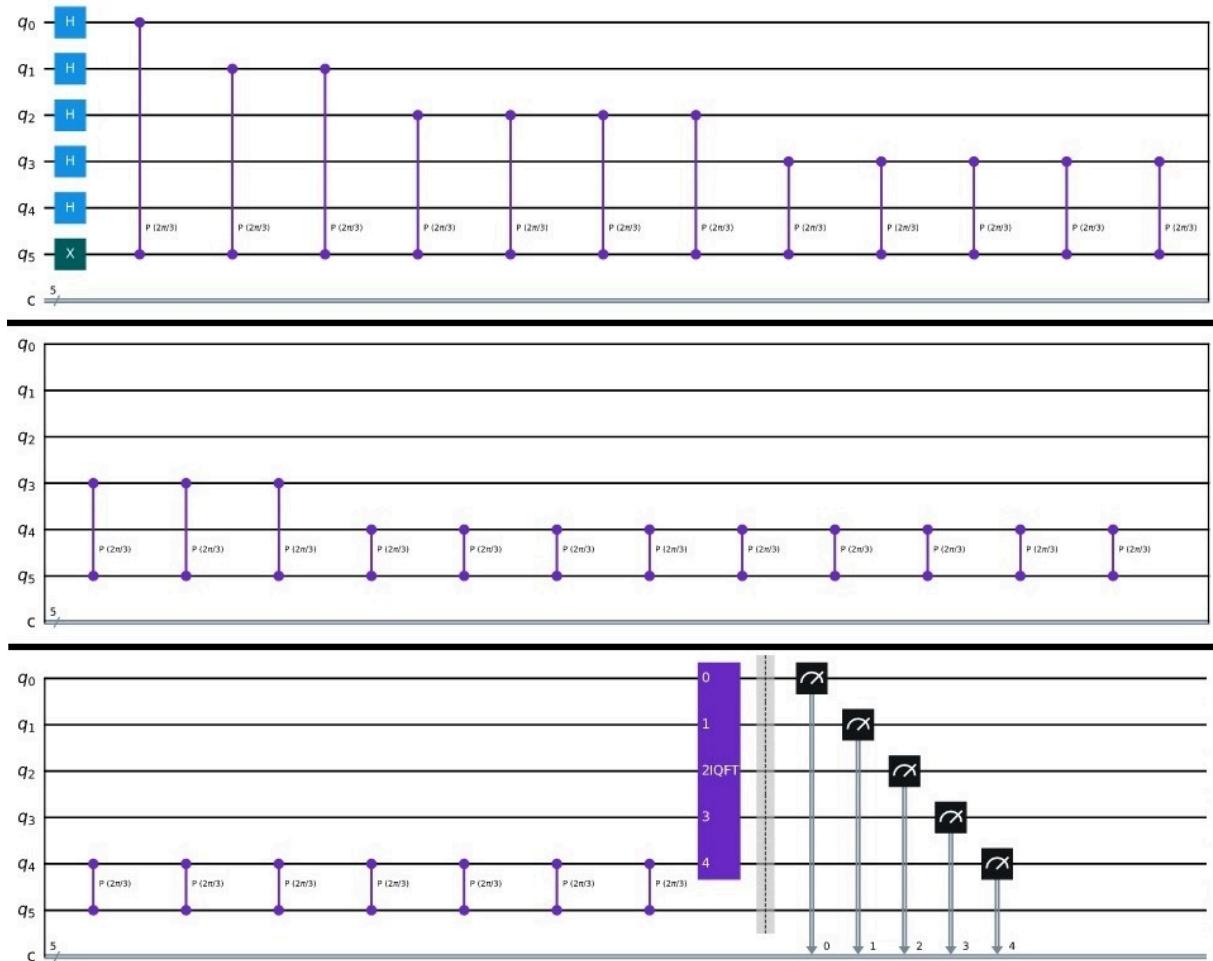


Abb. 2.12: Beispiel einer Quantum Phase Estimation mit unbekannter Phase $\theta = \frac{1}{3}$ und 5 Messungsqubits (ANIS u. a., 2021, Textbook 'Quantum Phase Estimation' - Chapter 3)

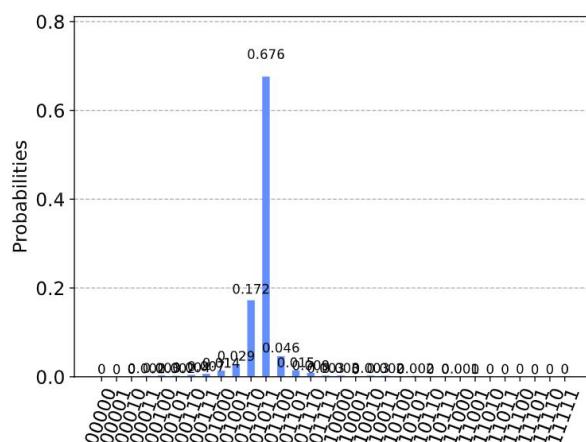


Abb. 2.13: Wahrscheinlichkeitstabelle des Beispiels in Abb. 2.12 nach 4096 Messungen (ANIS u. a., 2021, Textbook 'Quantum Phase Estimation' - Chapter 3)

Aus der Messung des Beispiels geht hervor, dass die zwei häufigsten Ergebnisse $01011_b = 11_{dez}$ und $01010_b = 10_{dez}$ sind. Umgerechnet bedeutet das, dass $\theta \approx \frac{11}{2^5} = 0.344$ oder $\theta \approx \frac{10}{2^5} = 0.313$ ähnelt, was geringe Abweichungen von der echten Phase $\theta = 0.334$ sind.

2.3 Algorithmen der Quantenkryptografie

Die ungewöhnlichen Eigenschaften von Quantum Computing bieten vor allem für kryptografische Zwecke viele neue Möglichkeiten, Algorithmen zu erstellen. Zwei Algorithmen dieser Art sind der *BB84 Quantenschlüsselaustausch* und der *Shor Algorithmus*.

2.3.1 BB84 Quantenschlüsselaustausch

Alice und Bob möchten über eine weite Distanz sicher miteinander kommunizieren. Da die meisten Kommunikationskanäle öffentlich sind, wie beispielsweise das Internet, und somit jede Person mitlesen kann, müssen die Nachrichten mit einem Schlüssel verschlüsselt werden. Wenn Alice und Bob aber keine Schlüssel im Voraus ausgetauscht haben, ist es problematisch, diese Schlüssel sicher über eine ferne Distanz zu übertragen, um überhaupt erst eine sichere Kommunikation aufzubauen. Eine dritte Person Eve könnte diesen Schlüssel bei der Übertragung also heimlich abfangen und kopieren, wodurch die Verschlüsselung von Alice und Bob nicht mehr sicher wäre.

Das *BB84 Protokoll*, auch bekannt als Quantenschlüsselaustausch, beschreibt ein sicheres Verfahren der Schlüsselgenerierung. Es verwendet die Eigenschaften der Quantenverschränkungen und Superpositionen von Qubits um Sicherheit zu garantieren.

Um Qubits versenden zu können, kann das Prinzip von klassischen physikalischen Kanälen angewandt werden. Bei einer Telefonleitung werden elektronische Signale durch die Leitung versendet, die die Nachricht bzw. Bits darstellen. Bei einem Quantenkommunikationskanal kann die Leitung beispielsweise aus einem Glasfaserkabel bestehen, durch das einzelne Photonen gesendet werden. Photonen können polarisiert werden, wodurch sie einen von zwei Zuständen annehmen können, und somit ein Qubit darstellen. (ANIS u. a., 2021, Vgl. Textbook 'Quantum Key Distribution' - Chapter 1)

Das Protokoll zur Generierung des Schlüssels kann in mehrere Schritte aufgeteilt werden:

1. Alice erstellt eine Liste aus Qubits mit der Länge n . Die Qubits sind sich standardmäßig in der z-Basis und haben zufällig die Zustände $|0\rangle$ oder $|1\rangle$.
2. Alice erstellt eine zweite Liste, diesmal aus den Qubit Basen x und z, die ebenfalls n lang ist. Die Basen werden zufällig gewählt.
3. Alice wendet die Basenliste nun auf die erste Liste an. Jedes Qubit aus Liste eins bleibt entweder in der z-Basis, oder wird in die x-Basis transformiert. Am Ende hat Alice eine neue Liste aus Qubits in den möglichen Zuständen $|0\rangle, |1\rangle, |+\rangle$ und $|-\rangle$.
4. Alice sendet die neue Liste an Bob. Liste eins und zwei hält sie vorerst noch geheim.
5. Bob erhält die Liste von Alice und erstellt selbst eine Liste aus zufälligen x- und z-Basen der Länge n .
6. Bob verwendet seine Basenliste, um die Qubits aus Alice's Liste nach der jeweiligen Basis zu messen. Die Messergebnisse hält er geheim.

7. Bob und Alice veröffentlichen ihre Basenlisten.
8. Wenn Bob ein Qubit in derselben Basis gemessen hat, in der Alice dieses vorbereitet hat, wird das Qubit Teil des Schlüssels. Hierfür übernimmt Alice für jede übereinstimmende Basis ein Qubit aus ihrer ersten Liste mit dem jeweiligen Basenindex, während Bob dasselbe mit seinen Messergebnissen macht. Am Ende haben Alice und Bob denselben Schlüssel.
9. Ist der Schlüssel zu kurz, wird das Protokoll wiederholt.
10. Alice und Bob veröffentlichen einen kleinen Teil ihres Schlüssels und vergleichen diesen, um potenzielle Übertragungsfehler auszuschließen.

(Shor und Preskill, 2000, Vgl. S.4), (ANIS u. a., 2021, Vgl. Textbook 'Quantum Key Distribution' - Chapter 2)

In den folgenden Beispielen wird deutlich, wie ein Schlüssel durch das BB84 Protokoll generiert wird. Im zweiten Beispiel wird auch das Szenario eines *Man-in-the-Middle* Angriffs erläutert.

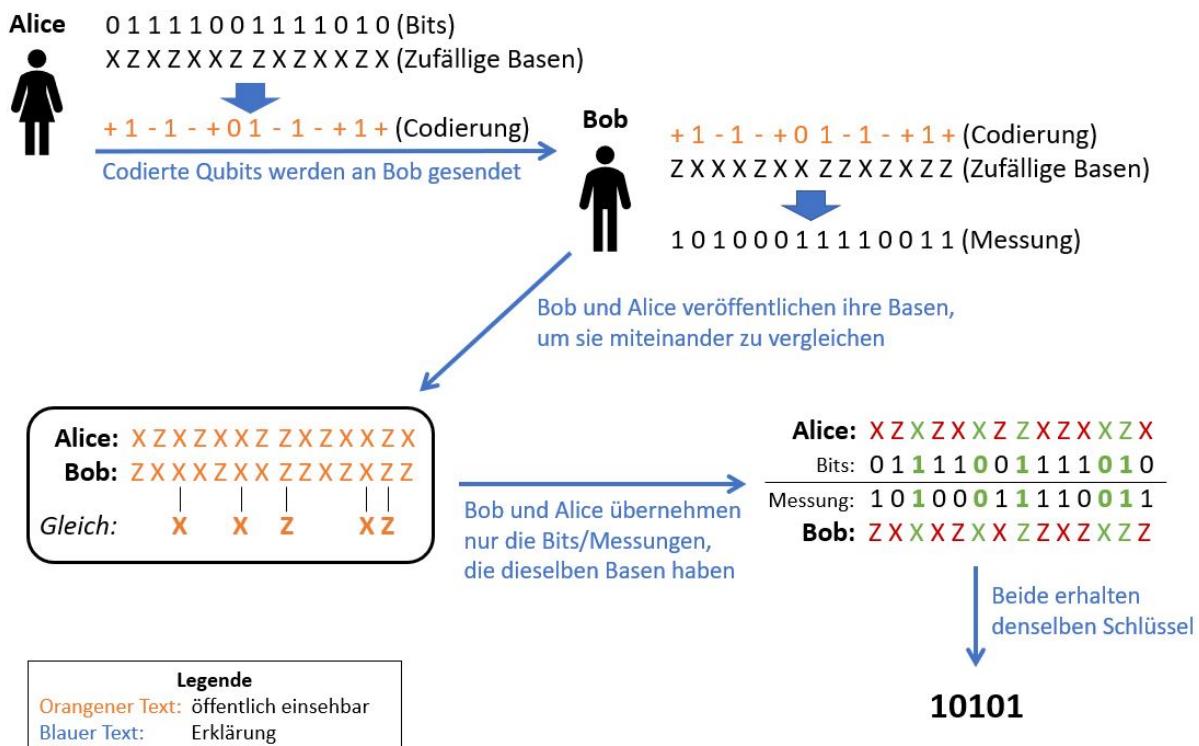


Abb. 2.14: Beispiel einer Schlüsselgenerierung nach dem BB84 Protokoll. Die Schlüssel müssen anschließend noch bruchteilsweise miteinander verglichen werden, um sie auf Korrektheit zu überprüfen.

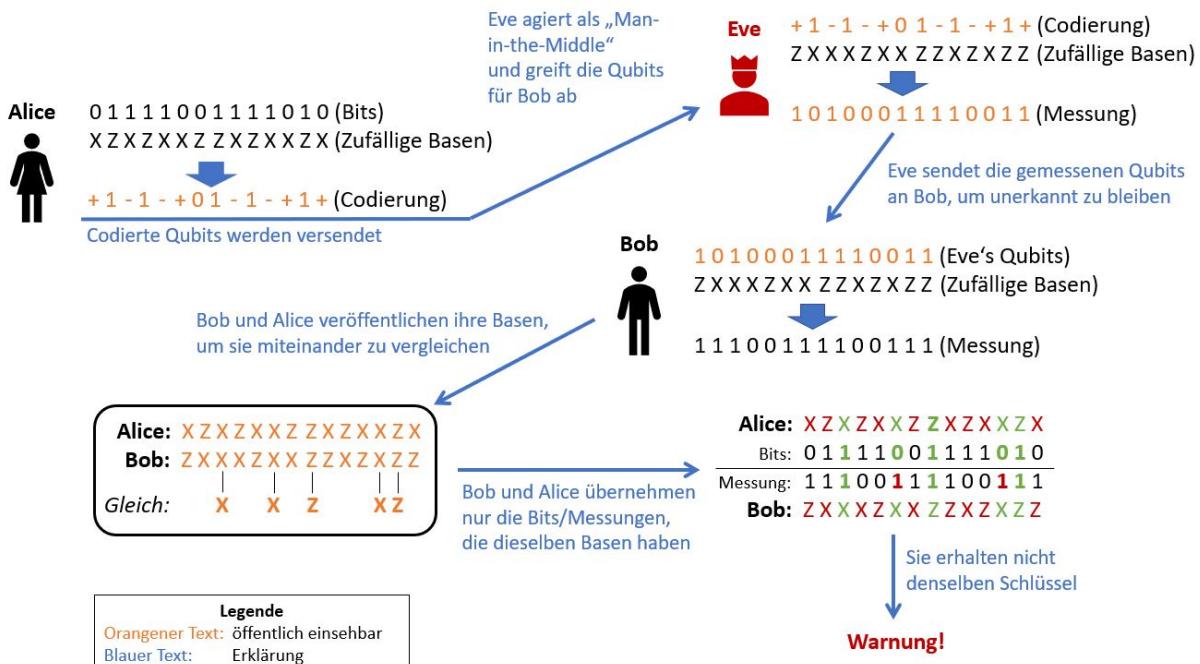


Abb. 2.15: Beispiel eines Man-in-the-Middle Angriffs durch Eve während der Schlüsselgenerierung nach dem BB84 Protokoll. Bei der anschließenden Überprüfung auf Korrektheit der Schlüssel fällt auf, dass etwas falsch gelaufen ist.

Im zweiten Beispiel fängt eine dritte Person *Eve* die codierten Qubits von Alice heimlich ab und misst diese. Dabei zerstört Eve die Superposition mancher Qubits und verfälscht dadurch die ursprüngliche Qubit-Nachricht von Alice. Eve sendet die bereits gemessenen Qubits nun an Bob, um keinen Verdacht zu schöpfen, dass eine weitere Person die Nachrichten mitliest.

Vergleichen Bob und Alice am Ende Teile ihrer Schlüssel, fällt die Intervention eines Dritten direkt auf, da Bob trotz derselben Basen wie Alice teilweise andere Ergebnisse hat.

2.3.2 Shor Algorithmus

Kryptografische Systeme basieren heutzutage oft auf dem Prinzip des RSA-Algorithmus. Durch eine mathematische *Falltür* kann RSA nur in eine Richtung, in diesem Fall die Verschlüsselung, berechnet werden. Die andere Richtung ist die Entschlüsselung, deren Berechnung ohne Kenntnis des Schlüssels je nach Schlüsselgröße mit heutigen Supercomputern mehrere Menschenleben lang dauert.

Diese *Falltür* besteht grundlegend aus dem Faktorisieren des Produkts zweier großer Primzahlen. Die Berechnung der Faktoren dauert mit aktuell anwendbaren Algorithmen eine *superpolynome* Zeit lang. Shor's Algorithmus faktorisiert das Produkt von zwei Primzahlen in nur *polynomer* Zeit, was signifikant schneller ist und somit das Falltürprinzip von RSA in Frage stellt.

Einschub: Primzahlen sind natürliche Zahlen und nur durch sich selbst und 1 teilbar. Ein Beispiel für Primzahlen sind 3 oder 5. Das Gesetz der Primfaktorzerlegung besagt, dass jede natürliche Zahl, die keine Primzahl ist, sich als Produkt von mindestens zwei Primzahlen schreiben lässt. So lässt sich die natürliche Zahl 15, die keine Primzahl ist, beispielsweise auch als $3 \cdot 5$ schreiben.

Der Shor Algorithmus macht Gebrauch davon, ein Problem in ein anderes zu transformieren, dessen Lösung simpler ist. „Anstatt einen Quantencomputer-Algorithmus für die direkte Faktorisierung von n zu erstellen, verwenden wir einen Quantencomputer-Algorithmus zur Bestimmung der Ordnung eines Elements a in der multiplikativen Gruppe $(\text{mod } n)$, d.h. die kleinste ganze Zahl r , bei der $a^r \equiv 1 \pmod{n}$ ist. [Durch Miller] ist bekannt, dass die Faktorisierung mit Hilfe von Zufallszahlen auf die Suche nach der Reihenfolge eines Elements reduziert werden kann.“ (Shor, 1997, S. 15) (Miller, 1976, Vgl.) Das Faktorisierungsproblem wird also zu einem periodischen Problem transformiert.

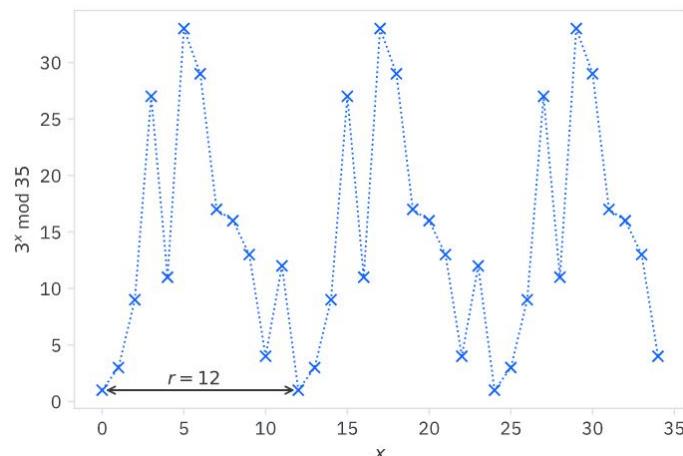


Abb. 2.16: Beispiel der periodischen Funktion $f(x) = a^x \pmod{n}$ aus Shor's Algorithmus mit $a = 3$, $n = 35$ und der Ordnung $r = 12$. (ANIS u.a., 2021, Textbook 'Shor's Algorithm' - Chapter 1)

Eine periodische Funktion mit Shor's genannten Bedingungen lässt sich mit den natürlichen Zahlen a , die eine Zufallszahl ist, und dem zu faktorisierenden Produkt n mit $a < n$ wie folgt definieren

$$f(x) = a^x \bmod n. \quad (16)$$

Diese periodische Funktion besitzt eine Ordnung r (Länge einer Periode), die für das Lösen des Faktorisierungsproblems benötigt wird und ist die kleinstmögliche natürliche Zahl für die gilt:

$$\begin{aligned} a^r \bmod n &= 1 \\ (a^r - 1) \bmod n &= 0. \end{aligned} \quad (17)$$

Nachdem die Ordnung r mithilfe des Quanten-Algorithmus berechnet wurde, folgt die Umformung des nun gelösten Periodenproblems zurück in ein Faktorisierungsproblem.

Falls r nicht gerade ist, muss eine andere zufällige Zahl a gewählt werden, da folgende Umformung sonst nicht möglich ist:

$$a^r - 1 = (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1). \quad (18)$$

Die Umformung wird mit der Erkenntnis aus dem zweiten Teil von Gleichung 17 durchgeführt, dass n ein Teiler von $a^r - 1$ sein muss. (ANIS u. a., 2021, Vgl. Textbook 'Shor's Algorithm' - Chapter 5) Es besteht die Wahrscheinlichkeit $P_{min} = 1 - \frac{1}{2^{k-1}}$ mit k als Anzahl der ungeraden Primfaktoren von n , dass der größte gemeinsame Teiler $\text{ggT}(a^{\frac{r}{2}} - 1; n)$ ein Faktor von n ist. (Shor, 1997, Vgl. S. 15-16) Der größte gemeinsame Teiler kann mithilfe des euklidischen Algorithmus effizient berechnet werden.

Der **Quanten-Algorithmus** zur Berechnung der Ordnung r verwendet *Quantum Phase Estimation* zusammen mit dem unitären Operator U . Die periodische Funktion aus Formel 16 wird wie folgt umgebaut:

$$U |y\rangle \equiv |ay \bmod n\rangle. \quad (19)$$

Jede Anwendung von U multipliziert den Zustand des Registers $|y\rangle$ mit $a \pmod n$. Beginnt $|y\rangle$ also im Zustand $|1\rangle$ wird nach r Anwendungen von U der Zustand $|1\rangle$ erneut erreicht. Die Anwendung des Prinzips aus Formel 19 auf das Beispiel aus Abbildung 2.17 mit $a = 3$, $n = 35$ und $r = 12$ veranschaulicht das:

$$U |1\rangle = |3\rangle, \quad U^2 |1\rangle = |9\rangle, \quad U^3 |1\rangle = |27\rangle \quad \dots \quad U^{r-1} |1\rangle = |12\rangle, \quad U^r |1\rangle = |1\rangle.$$

Hierbei ist im Vergleich mit Abbildung 2.17 die x-Achse die Anzahl an Anwendungen von U und die y-Achse der Zustand des Registers $|y\rangle$. (ANIS u. a., 2021, Vgl. Textbook 'Shor's Algorithm' - Chapter 2)

Um die Ordnung mithilfe von QPE zu messen, muss r als Phase vorhanden sein. Hierfür wird das Register $|y\rangle$ zunächst in die Superposition $|u_0\rangle$ gebracht, was ein valider Eigenzustand von U ist:

$$|u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |a^k \bmod n\rangle.$$

Das Beispiel mit $a = 3$, $n = 35$ und $r = 12$ sieht unter diesen Umständen wie folgt aus:

$$\begin{aligned} |u_0\rangle &= \frac{1}{\sqrt{12}} (|1\rangle + |3\rangle + |9\rangle \dots |4\rangle + |12\rangle) \\ U|u_0\rangle &= \frac{1}{\sqrt{12}} (|3\rangle + |9\rangle + |27\rangle \dots |12\rangle + |1\rangle) = |u_0\rangle. \end{aligned}$$

Dieser Eigenzustand hat einen Eigenwert von 1 und hat in diesem Kontext keine große Relevanz. „Ein interessanterer Eigenzustand könnte einer sein, bei dem die Phase für jeden dieser Zustände in der Berechnungsbasis [z-Basis] unterschiedlich ist.“ (ANIS u. a., 2021, Textbook 'Shor's Algorithm' - Chapter 2) Wenn die Phase des k -ten Zustands proportional zu k ist, resultiert dies in:

$$\begin{aligned} |u_1\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i k}{r}\right) |a^k \bmod n\rangle, \\ U|u_1\rangle &= \exp\left(-\frac{2\pi i}{r}\right) |u_1\rangle. \end{aligned}$$

Der Eigenwert beinhaltet in diesem Fall r , was für die Überprüfung der Gleichheit der Phasendifferenzen zwischen den Zuständen der Berechnungsbasis notwendig ist.

Wird dieses Prinzip weiter ausgenutzt, so kann eine weitere ganze Zahl s mit dieser Phasendifferenz multipliziert werden:

$$\begin{aligned} |u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) |a^k \bmod n\rangle, \\ U|u_s\rangle &= \exp\left(-\frac{2\pi i s}{r}\right) |u_s\rangle \end{aligned}$$

Mit dem Beispiel $a = 3$, $n = 35$ und $r = 12$ wird daraus also:

$$\begin{aligned} |u_s\rangle &= \frac{1}{\sqrt{12}} \left(\exp\left(-\frac{0 \cdot 2\pi i s}{12}\right) |1\rangle + \exp\left(-\frac{1 \cdot 2\pi i s}{12}\right) |3\rangle \dots \exp\left(-\frac{11 \cdot 2\pi i s}{12}\right) |12\rangle \right) \\ U|u_s\rangle &= \frac{1}{\sqrt{12}} \left(\exp\left(-\frac{0 \cdot 2\pi i s}{12}\right) |3\rangle + \exp\left(-\frac{1 \cdot 2\pi i s}{12}\right) |9\rangle \dots \exp\left(-\frac{11 \cdot 2\pi i s}{12}\right) |1\rangle \right) \\ U|u_s\rangle &= \exp\left(-\frac{2\pi i s}{12}\right) |u_s\rangle \end{aligned}$$

Dadurch entstehen singuläre Eigenzustände für jeden ganzzahligen Wert von s mit der Bedingung $0 \leq s \leq r-1$. Durch die Aufsummierung all dieser Eigenzustände werden durch die verschiedenen Phasen alle Zustände der Berechnungsbasis bis auf $|1\rangle$ aufgehoben:

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle .$$

Der Zustand $|1\rangle$ ist eine Überlagerung all dieser Eigenzustände. Die Phase des Zustands kann mit einer QPE gemessen werden:

$$\phi = \frac{s}{r}$$

In diesem Fall ist s eine zufällige ganze Zahl zwischen 0 und $r - 1$.

„Durch die Anwendung des Kettenbruch-Algorithmus, [also der Approximation durch einen Näherungsbruch], auf ϕ , kann r berechnet werden.“ (ANIS u. a., 2021, Vgl. Textbook 'Shor's Algorithm' - Chapter 2)

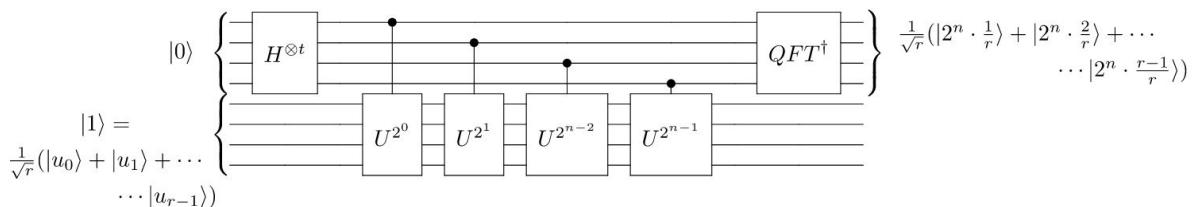


Abb. 2.17: Schaltung einer Shor Algorithmus Implementation (nach der Qiskit Qubit Ordering Convention)(ANIS u. a., 2021, Textbook 'Shor's Algorithm' - Chapter 2)

Die U-Gatter der QPE sind in diesem Fall die dynamischen Modulo Funktionen. Jedes U-Gatter führt wie in Formel 19 beschrieben eine kontrollierte Multiplikation auf die Phase von $|y\rangle$ mit dem Ergebnis von $a^{2^j} \bmod n$ durch, wobei j die Anzahl der bereits angewendeten U-Gatter ist. Mithilfe des *Repeated Squaring*-Algorithmus kann $a^{2^j} \bmod n$ effizient berechnet werden.

Soll zum **Beispiel** die Zahl $n = 15$ faktorisiert werden, die das Produkt der Primzahlen 3 und 5 ist, wird wie folgt vorgegangen:

1. Überprüfen, ob n eine gerade Zahl ist. Wenn ja, wird der Prozess beendet und Faktor 2 zurückgegeben. Da $n = 15$ ungerade ist, beginnt Schritt 2.
2. Es muss eine zufällige Zahl zwischen 1 und $n - 1 = 14$ ausgewählt werden. In diesem Beispiel wird zufällig $a = 7$ gewählt, was kein Faktor von n ist.

3. Mithilfe des Quanten-Algorithmus wird die Ordnung r von $7^r \bmod 15 = 1$ bestimmt.
 Wie in Abbildung 2.19 erkennbar ist, weisen zwei der vier Messergebnisse auf die korrekte Ordnung $r = 4$ hin:

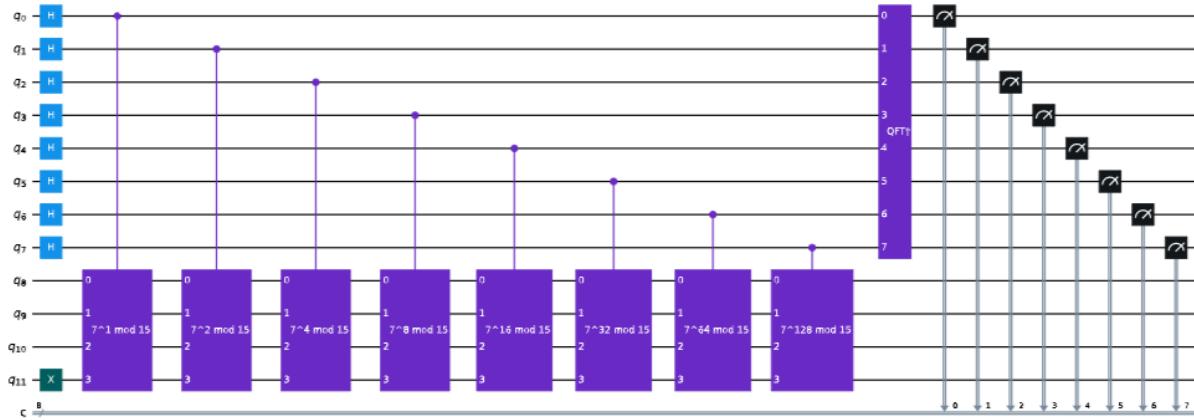


Abb. 2.18: Beispiel des Shor Algorithmus mit 8 Zählerqubits, $n = 15$ und $a = 7$ (ANIS u. a., 2021, Textbook 'Shor's Algorithm' - Chapter 3)

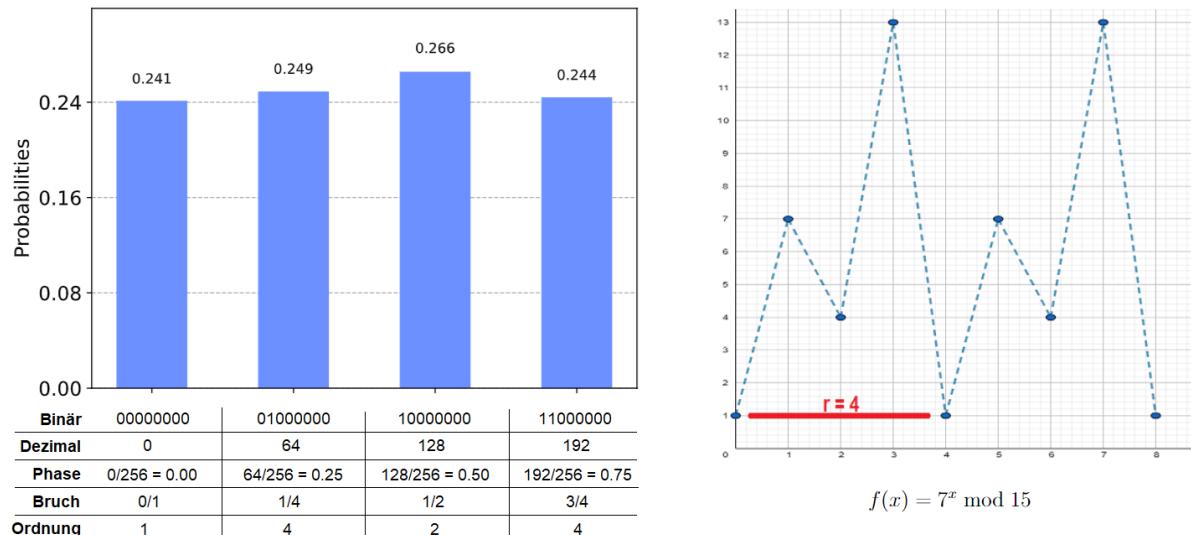


Abb. 2.19: Durchschnittliches Messergebnis von Abbildung 2.18 (links) und als Vergleich die periodische Funktion $f(x) = 7^x \bmod 15$ (rechts) (ANIS u. a., 2021, Vgl. Textbook 'Shor's Algorithm' - Chapter 3)

4. Anschließend folgt durch die Umformung in Formel 18 die Berechnung des ggTs $ggT\left(7^{\frac{4}{2}} - 1; 15\right) = 3$. Das Ergebnis ist korrekt, die Zahl 3 ist ein Faktor von $n = 15$.

2.4 Lerntheorie

Das folgende Kapitel beschreibt grundlegende Ansätze und Methoden des Lernens. Das Verständnis dieser Prinzipien ist für die erfolgreiche Vermittlung von Wissen essenziell.

2.4.1 Lernen und Wissen

„Lernen bedeutet, dass Menschen Fähigkeiten erwerben, um sich ihrer Umwelt anzupassen, sinnvoll zu handeln und ihre Umgebung, wenn nötig, zu verändern.“ (Groß und Bastian, 2017, S. 43) Der Lernprozess kann sowohl absichtlich und aktiv als auch beiläufig und passiv stattfinden. Es gibt viele verschiedene Arten von Lernaufgaben, dazu zählen beispielsweise Auswendiglernen, Zusammenhänge verstehen, Handlungsabläufe trainieren und soziale Erwartungen erfüllen. Trotz dieser Vielfalt finden bei allen Lernvorgängen ähnliche Veränderungen im Gehirn statt. (Reinhaus, 2011, S. 6 - 7)

Das Ergebnis des Lernprozesses ist Wissen, welches die Grundlage für weitere Lernprozesse bildet. „Wissen besteht aus der Gesamtheit aller Erfahrungen, Kenntnisse und Fähigkeiten eines Menschen.“ (Groß und Bastian, 2017, S. 110) Informationen sind nicht mit Wissen gleichzusetzen, da erst durch deren Wahrnehmung und die Verknüpfung mit bestehenden Erfahrungen neues Wissen entsteht. Der Lernprozess selbst ist für Außenstehende zunächst nicht zu beobachten, führt jedoch zu langfristigen Veränderungen des Wissens, welche sich beispielsweise bei der Bearbeitung von Aufgaben oder der Problemlösung zeigen können. (Groß und Bastian, 2017, S. 108 - 109)



Abb. 2.20: Lernen und Wissen (Groß und Bastian, 2017, S. 108, Abb. 7)

2.4.2 Lernprozess im Gehirn

Weil die Veränderungen im Gehirn die Grundlage für jegliches Lernen darstellen, ist das Verständnis des Prozesses essenziell für die Bildung von Lernstrategien. Jeder Lernvorgang beginnt mit der Wahrnehmung von Sinneseindrücken, wobei Reize als elektrischer Impuls von den Sinneszellen an das Gehirn weitergeleitet werden. Die Nervenzellen im Gehirn sind für die Verarbeitung der Informationen und das Einleiten der entsprechenden Reaktionen verantwortlich. Benachbarte Nervenzellen haben die Möglichkeit an ihren Kontaktstellen, welche als Synapsen bezeichnet werden, Informationen miteinander auszutauschen. Wenn dieselben Nervenzellen wiederholt genutzt werden, verdicken die Synapsen zwischen den beteiligten Nervenzellen. Handlungen die zu positiven Gefühlen geführt haben, werden

vom Gehirn bevorzugt wiederholt, wobei negative Gefühle vermieden werden. (Reinhaus, 2011, vgl. S. 7 - 12)

Da das Verdicken von bestehenden Synapsen und auch der Aufbau von neuen Nervenverbindungen den Körper Energie kosten, finden diese Prozesse nur für Informationen statt, die dem Gehirn wichtig erscheinen. Deshalb sind verschiedene Informationen unterschiedlich lange abrufbar. (Reinhaus, 2011, vgl. S. 7 - 12)

Es werden drei Gedächtnisebenen unterschieden: **Ultrakurzzeitgedächtnis** (sensorischer Speicher), **Kurzzeitgedächtnis** und **Langzeitgedächtnis**. (Reinhaus, 2011, vgl. S. 7 - 12)

Ins **Ultrakurzzeitgedächtnis** gelangen zunächst alle Informationen, da die Nervenzellen, die an der Verarbeitung eines Reizes beteiligt sind, bis zu 20 Sekunden lang elektrisch erregt bleiben. In dieser Zeit bleibt der Reiz in Erinnerung, allerdings wird er, falls keine Auseinandersetzung mit dem Reiz stattfindet, nach dieser Zeitspanne direkt wieder vergessen. Durch eine intensivere Auseinandersetzung mit einem Reiz werden an den Synapsen vorübergehend viele Botenstoffe ausgeschüttet, was bis zu einige Tage lang andauern kann. In dieser Zeitspanne bleibt der Eindruck in Erinnerung, befindet sich also im **Kurzzeitgedächtnis**. (Reinhaus, 2011, vgl. S. 7 - 12)

Damit ein Eindruck ins *Langzeitgedächtnis* gelangen kann, muss dieser für das Gehirn als sehr wichtiger erscheinen, beispielsweise durch das Auslösen von starken Emotionen. Ist dies der Fall, bilden die beteiligten Nervenzellen neue Verbindungen. Diese können, je nachdem wie oft sie genutzt werden, Wochen, Monate oder Jahre bestehen bleiben. Ungenutzte Verbindungen werden mit der Zeit auch wieder zurückgebildet. Dann geraten Lerninhalte auch wieder in Vergessenheit, können aber schnell wieder aufgefrischt werden, da die Verbindungen nicht vollständig abgebaut werden. (Reinhaus, 2011, vgl. S. 7 - 12) Es gelangen nur sehr wichtige Informationen bis in das Langzeitgedächtnis, dies geschieht vor allem wenn die Information hilfreich für die Erfüllung von Bedürfnissen und Erreichung von Zielen ist. (Reinhaus, 2011, vgl. S. 7 - 12)

2.4.3 Unterscheidung von Lerntypen

Jeder Mensch bevorzugt unterschiedliche Sinneskanäle um Informationen aufzunehmen. Es werden drei Lerntypen unterschieden. (Reinhaus, 2011, S. 27 - 31)

Der **visuelle Lerntyp** nimmt Informationen am besten über die Augen, also über genaueres betrachten von Texten, Grafiken, Tabellen, Zeichnungen, Bildern oder Videos. Neue Informationen werden bereits durch sorgfältiges Lesen und aufschreiben gelernt. Außerdem sind Schaubilder, Fotos, Mind Maps oder Tabellen sehr hilfreich. (Reinhaus, 2011, S. 27 - 31)

Der **auditive Lerntyp** lernt am besten über die Ohren, also durch aufmerksames zuhören. Hilfreich ist außerdem lautes Vorlesen von Texten und das Erklären und Diskutieren von

Inhalten mit anderen Personen. (Reinhaus, 2011, S. 27 - 31)

Der **haptische Lerntyp** profitiert von der zeitnahen praktischen Anwendung der Lerninhalte. Praktische Übungen, die bestenfalls Versuch und Irrtum nutzen, spielen eine wichtige Rolle. (Reinhaus, 2011, S. 27 - 31)

Auch wenn ein bestimmter Lerntyp bei einer Person besonders ausgeprägt ist, sollten dennoch auch die anderen Sinne beim Lernen eingesetzt werden. Durch diese Kombination kann die Lernleistung gesteigert werden, da mehrere Gehirnregionen an der Speicherung der Informationen beteiligt sind und diese somit länger im Gedächtnis bleiben. (Reinhaus, 2011, S. 27 - 31)

2.4.4 Lernstiltypologie nach Kolb

Der amerikanische Lerntheoretiker David A. Kolb unterteilt den Lernprozess in vier Stadien, die einen Kreislauf ergeben.

- Im Stadium der *konkreten Erfahrung* werden Reize aus der Umwelt aufgenommen.
- In der Phase der *reflektierende Beobachtung* wird der Lerngegenstand oder das Problem aus verschiedenen Perspektiven betrachtet.
- Innerhalb der *abstrakten Begriffsbildung* werden Erfahrungen und Beobachtungen durch logisches und analytisches Denken in ein Konzept integriert.
- Beim *aktiven Experimentieren* werden die Erkenntnisse praktisch erprobt, um neue Erfahrungen zu sammeln und den Lernkreislauf fortzusetzen.

Diese Phasen lassen sich in allen Lernprozessen wiederfinden, jedoch werden je nach Lerntyp manche Phasen stärker oder weniger stark genutzt. (Groß und Bastian, 2017, S. 58 - 59)

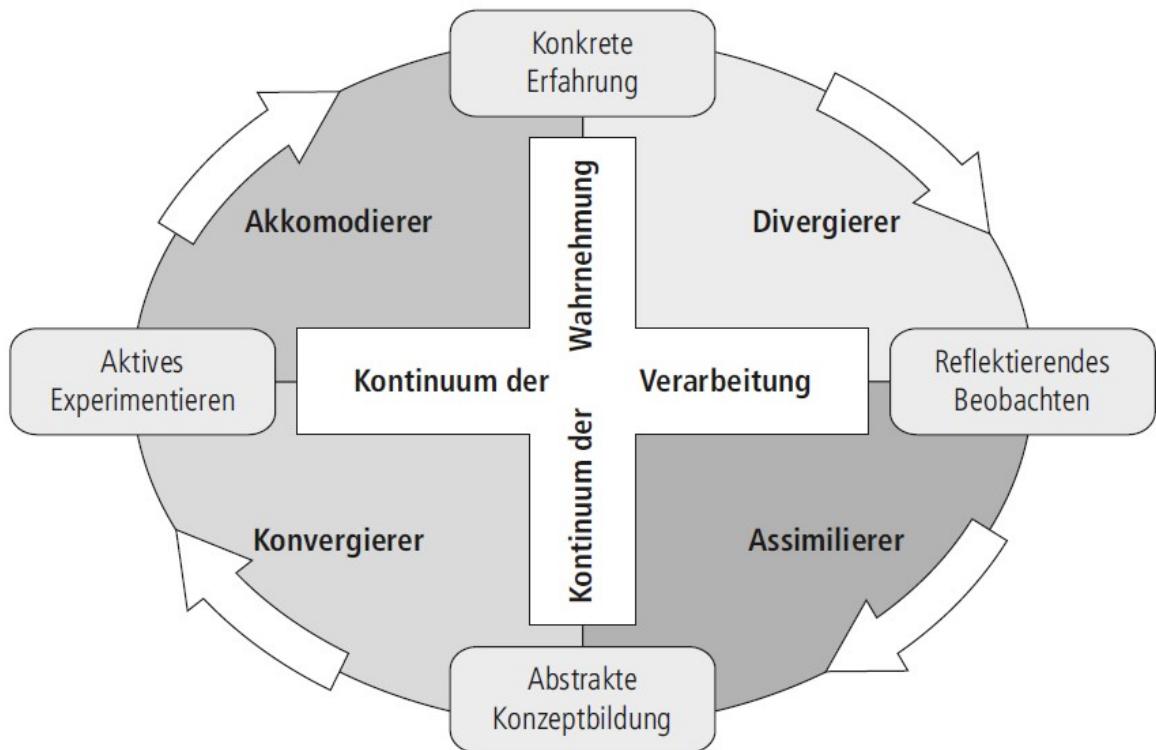


Abb. 2.21: Lernzyklus nach Kolb (Alonso u. a., 2017, S. 22, Abb. 3)

In Abbildung 2.21 ist der Lernzyklus nach Kolb zu sehen. Das Modell besteht aus zwei bipolaren Dimensionen. Die erste Dimension (Kontinuum der Wahrnehmung) zeigt wie Menschen Informationen wahrnehmen und sich aneignen. Dies kann entweder verstärkt durch konkrete Erfahrungen oder durch abstraktes Nachvollziehen geschehen. Die zweite Dimension (Kontinuum der Verarbeitung) zeigt die Art der Informationsverarbeitung, welche entweder verstärkt durch aktives Ausprobieren oder durch reflektiertes Beobachten entsteht. Daraus lassen sich vier Lerntypen ableiten, welche sich in den Quadranten des Modells befinden:

Für Menschen des Typs *Divergierer* (Kreative) steht das Fühlen und Wahrnehmen von konkreten Erfahrungen im Vordergrund. Sie neigen dazu eher zu beobachten, anstatt sofort zu handeln, treffen Entscheidungen eher intuitiv und legen Wert auf zwischenmenschliche Beziehungen. Perspektivwechsel fallen ihnen leicht, sie arbeiten gerne in Teams zusammen und sich offen für das Geben und Annehmen von Feedback.

Die *Assimilierer* (Planer, Forscher) kombinieren beim Lernen reflektiertes Beobachten mit einer abstrakten Begriffsbildung. Ihre Stärke liegt demnach in der Anwendung von Logik und theoretischen Modellen, wobei das Denken im Gegensatz zum Fühlen im Vordergrund steht. Sie haben die Fähigkeit zur Planung, Analyse und Strukturierung und sind an einer abstrakten Gestaltung von Ideen interessiert. Dabei lernen sie gerne alleine beispielsweise in Vorlesungen und legen Wert auf das Reflektieren des Gelernten.

Konvergierer (Spezialisten, Ingenieure) befassen sich wie Assimilierer ebenfalls mit Theo-

rien und abstrakten Modellen, legen aber Wert auf aktives Experimentieren, um ihre Ideen in die Praxis umzusetzen. Für das Lernen werden Simulationen bevorzugt, um Ideen auszuprobieren und praktische Anwendungen erproben zu können.

Akkomodierer (Macher) wenden gerne aktive Experimente an, konzentrieren sich gleichzeitig jedoch auf konkrete, praktische Erfahrungen, wobei ihnen menschliche Interaktion wichtig ist. Sie können sich schnell auf andere Menschen und Situationen einstellen und verlassen sich eher auf die Informationen von Mitmenschen als auf ihre eigene kognitive Analyse. Akkomodierer lernen gerne mit anderen zusammen, wobei ihnen die Umsetzung von Projekten Spaß macht. Außerdem setzen sie sich Ziele und probieren gerne unterschiedliche Vorgehensweisen aus. (Alonso u. a., 2017, S. 18 - 21)

2.4.5 Lernstrategien

Da jede Person eine andere Vorgehensweise beim Lernen nutzt, verfügt sie über eine Vielzahl an Strategien, die im Lernprozess jedoch meist unbewusst angewendet werden. Wie in Abbildung 2.22 zu sehen, wird zwischen kognitiven, metakognitiven und ressourcenbezogenen Lernstrategien unterschieden.

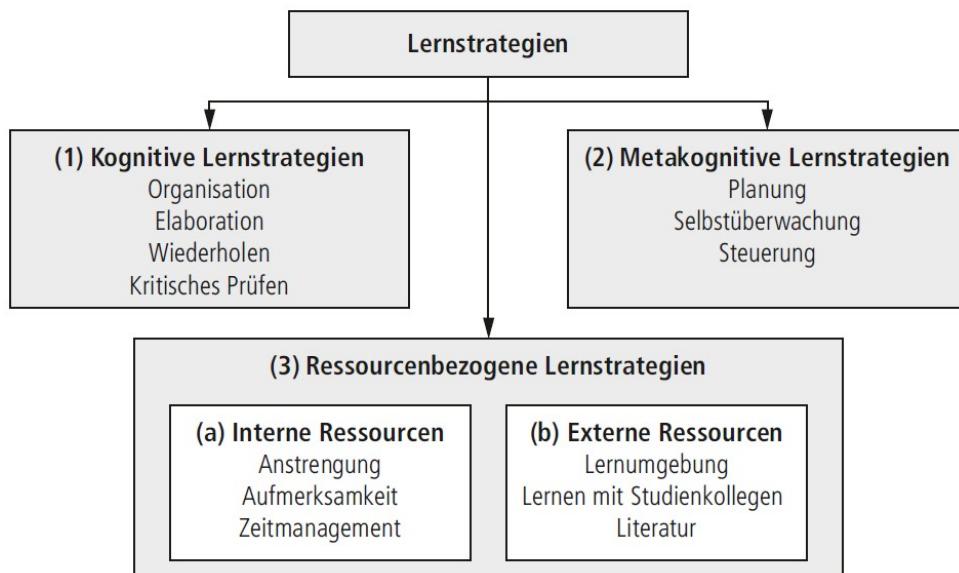


Abb. 2.22: Systematisierung von Lernstrategien (Alonso u. a., 2017, S. 24, Abb. 4)

Zu den *kognitive Lernstrategien* zählen Wiederholungsstrategien, Elaborationsstrategien und Organisationsstrategien. (Groß und Bastian, 2017, S. 56) „Kognitive Lernstrategien zielen darauf ab, durch die gedankliche Auseinandersetzung mit Inhalten einen Lernfortschritt zu erreichen.“ (Groß und Bastian, 2017, S. 60)

Metakognitive Strategien dienen zur Überwachung der eigenen Lernvorgänge, befinden sich demnach auf einer höheren Ebene, die auch Metaebene genannt wird.

Dazu gehören Methoden zur Selbstbeobachtung, Selbstregulation und Selbstbewertung. Zuerst muss das eigene Lernverhalten beobachtet werden, um ein besseres Bewusstsein für

die Abläufe zu entwickeln. Anschließend können gezielt Lernstrategien eingesetzt werden. Im letzten Schritt kann aktiv gegen ungewünschte Denkmuster vorgegangen werden und somit das Lernen umstrukturiert werden. (Groß und Bastian, 2017, S. 56)

Ressourcenbezogene Lernstrategien dienen dazu, die inneren und äußeren Ressourcen hinreichend zu nutzen und die Rahmenbedingungen des Lernens zu organisieren. Beispiele für innere Ressourcen sind Aufmerksamkeit, Willensstärke und Zeitmanagement. Äußere Ressourcen können Arbeitsplatz, Umgang mit Störungsquellen und zusätzliche Informationsquellen sein.

2.4.6 Lernmotivation

Motive und Motivation

Die Motivation wird als Ausgangspunkt des erfolgreichen Lernens bezeichnet. Der Begriff Motivation bezeichnet die Gesamtheit an einzelnen Beweggründen (Motive), die in einer Situation wirken. Die Wirkungskraft von Motiven wird bei der Betrachtung (Abbildung ?? der Bedürfnispyramide nach Maslow und des E-R-G Konzeptes von Alderfer deutlich. Laut Maslow bauen die menschlichen Bedürfnisse stufenweise aufeinander auf. Erst wenn die Grundbedürfnisse befriedigt sind, können Motive auf den anderen Stufen, wie Selbstverwirklichung und Anerkennung bearbeitet werden. Alderer unterscheidet in seiner E-R-G Theorie die drei Bedürfnisklassen Existenzbedürfnisse, Beziehungsbedürfnisse und Wachstumsbedürfnisse, welche ebenfalls aufeinander aufbauen und die Stufen der Bedürfnispyramide enthalten. Da es sich um theoretische Modelle handelt, können sich diese nicht eins zu eins auf die Wirklichkeit übertragen. Es können auch höhere Bedürfnisse befriedigt werden, ohne die darunter liegenden Stufen vorher bearbeitet zu haben, allerdings leidet dabei die Leistungsfähigkeit der Individuen darunter. Beispielsweise sinkt bei Schlafmangel die Aufmerksamkeit bei der Arbeit. (Groß und Bastian, 2017, S. 80 - 81)

Erkennen des Nutzens

Eine wichtige Grundlage für die Aufnahme von Informationen aus neuen Bereichen ist das Erkennen des Nutzens dieser Informationen für die lernende Person. Neugierde hilft, Aufmerksamkeit auf eine spezielle Information zu lenken. Deshalb ist es wichtig von Anfang an die Wichtigkeit und Relevanz einer Aufgabe oder eines Themas zu erkennen.

Verknüpfung mit Vorwissen

Ebenfalls hilfreich ist es, wenn neue Informationen mit bereits bestehendem Wissen verknüpft werden können, da so sehr leicht neue Verbindungen zwischen den Nervenzellen entstehen, was das Lernen erleichtert. Falls es sich ein völlig neues Gebiet handelt, ist es deshalb umso wichtiger, dass zunächst eine ausgiebige Auseinandersetzung mit den Grundlagen stattfindet, um im weiteren Verlauf auf diesen aufzubauen zu können. (Reinhäus, 2011, S. 13 - 16)

In der Psychologie wird zwischer *extrinsischer* und *intrinsischer* Motivation unterschie-

den. Die extrinsische Motivation ist von externen Faktoren bestimmt. Dazu zählen Anreize, wie gute Noten oder eine Gehaltserhöhung, aber auch die Vermeidung von negativen Folgen, wie das Wiederholen einer Prüfung bei nicht-bestehen. Intrinsische Motivation bedeutet, dass eine Tätigkeit aufgrund von inneren Beweggründen und aus Freude an der Sache selbst ausgeführt wird. Dazu gehört auch Spaß oder ein größeres Interesse an einer Sache zu haben, wie es oft bei Hobbys der Fall ist. Eine Belohnung oder Bestätigung von außen ist hierbei nicht notwendig.

Intrinsische und extrinsische Motive schließen sich nicht aus, sondern bestärken sich oft gegenseitig. Die Kombination beider Motivarten kann dazu beitragen ein Ziel schneller zu erreichen. Es gibt einige Methoden, um die Motivation zu wecken und aufrechtzuerhalten, welche zu den ressourcenbezogenen Lernstrategien zählen:

Pausen einlegen

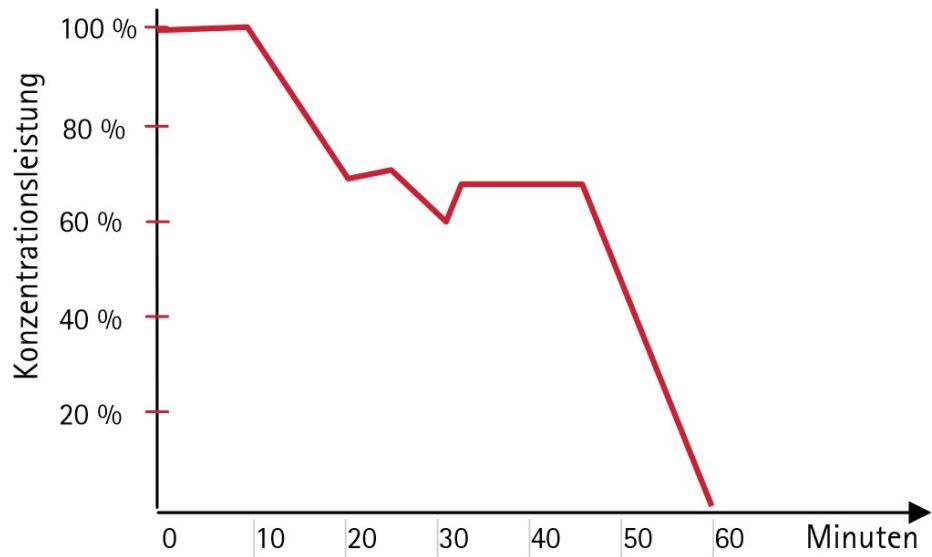


Abb. 2.23: Konzentrationsleistung (Reinhaus, 2011, S. 52)

Die Arbeit sollte ohne Stress und Zeitdruck begonnen werden, weshalb Pausen, Auszeiten und Ruhephasen wichtig sind. Ein erfülltes Privatleben schafft neue Motivation und einen Ausgleich zum Lernen. Groß und Bastian (2017)[S. 81 - 85] Um die Konzentrationsleistung aufrecht zu erhalten, sollten Pausen regelmäßig in bestimmten Abständen erfolgen. Wie in Abbildung 2.23 gezeigt, sinkt die Konzentrationsleistung im zeitlichen Verlauf ab. Deshalb ist bereits nach 15 Minuten eine kurze Pause sinnvoll, spätestens nach 60 Minuten ist eine längere Pause wichtig. Die Pausen können zur Aufnahme von Essen und Trinken oder auch zur Bewegung verwendet werden. Am Ende des Arbeitstags ist ein gezielter und langer Ausgleich, wie beispielsweise durch Sport denkbar. Der tageszeitliche Leistungsverlauf ist jedoch bei jedem Menschen unterschiedlich, da er von genetischen Faktoren abhängig ist. Das bedeutet, dass es Tageszeiten gibt, an denen die Leistungsfähigkeit höher ausfällt, bei

vielen Menschen ist dies gegen zehn Uhr morgens und gegen 18 Uhr. (Reinhaus, 2011, S. 50 - 53)

Lernziele setzen

Das Setzen von attraktiven und messbaren Lernzielen hilft dabei, das Durchhaltevermögen bei herausfordernden Aufgaben zu stärken. Ziele sind dann attraktiv, wenn die Erreichung einen hohen persönlichen Nutzen darstellt. Zusätzlich sollten Ziele so konkret wie möglich ausformuliert werden und messbar sein, damit Handlungen danach ausgerichtet werden können. Wichtig ist, dass Ziele realistisch sind. Dies anhand von kleinen Teilzielen erreicht werden, wodurch regelmäßige Erfolgserlebnisse entstehen. (Reinhaus, 2011, S. 34 - 38)

Belohnungen nutzen

„Damit Lernen mit Belohnungen verknüpft wird, sollten Sie sich unmittelbar nach einem Lernerfolg belohnen.“ (Reinhaus, 2011, S. 40)

Besonders wenn eine herausfordernde Aufgabe, die nicht direkt belohnt wird, ist es hilfreich zur Belohnung etwas zu tun, das Spaß macht. (Groß und Bastian, 2017, S. 84) Durch regelmäßige Belohnungen werden Lernaufgaben mit positiven Gefühlen verknüpft. Dies führt zu einer Steigerung der Motivation und auch der Merkleistung. Die Art und Größe der Belohnung sollte an den Umfang oder die Schwierigkeit der erledigten Aufgabe angepasst werden. (Reinhaus, 2011, vgl. S. 40)

3 Anforderungsanalyse

Um den Anforderungen aller am Projekt beteiligten Stakeholdern gerecht zu werden, wird eine Anforderungsanalyse aus bewährten Methodiken durchgeführt. Hierfür werden System, Kontext und Grenzen der Anwendung erörtert, um das Projektumfang zu definieren. Anschließend folgt eine *Konkurrenzanalyse*, in dem ähnliche *Produkte* analysiert werden. Nach der Vorarbeit wird mit dem eigentlichen Sammeln der Anforderungen begonnen, wofür aber zunächst die betroffenen Stakeholder definiert werden müssen. Anhand dieser werden mit verschiedenen Kreativitätstechniken die Anforderungen ermittelt und bearbeitet.

3.1 Bestimmung von System und Systemkontext

Die Bestimmung des Systems, dessen Grenzen und Kontextaspekte bilden die Grundlage der Anforderungsanalyse. Eine korrekte und vollständige Bestimmung ist deshalb wichtig, da ansonsten fehlerhafte Anforderungen entstehen können. (Pohl und Rupp, 2015, vgl. S. 13-14) Grundlegende Information zur Zielsetzung, welche bei der Definition des Systems zu beachten sind, befinden sich in Kapitel 1.1.

3.1.1 Definition des Systems

Es soll eine Bildungsplattform für Quantenkryptografie erstellt werden, welche Studierenden die Weiterbildung auf dem Gebiet ermöglichen soll. Um theoretische Konzepte, Protokolle und Algorithmen verständlich darzustellen, sollen diese visualisiert und simuliert werden. Die Applikation soll als Webanwendung umgesetzt werden, wobei der Aufbau und die inhaltliche Gestaltung auf wissenschaftlich fundierten Erkenntnissen auf den Gebieten der Quantenkryptografie und der Lerntheorie basieren soll.

3.1.2 Erfassung des Systemkontexts

Zur Bestimmung des Systemkontexts wird eine Annahme getroffen, wie das System in die Realität integriert wird. System- und Kontextgrenzen sind Teil des Systemkontexts, welcher alle Aspekte umfasst, die für die Anforderungen des geplanten Systems relevant sind, jedoch nicht im Rahmen der Entwicklung des Systems gestaltet werden. (Pohl und Rupp, 2015, vgl. S. 15)

Die Darstellung erfolgt innerhalb eines Kontextdiagramms (Abb. 3.1), welches das System, die Schnittstellen und die Umgebung zeigt. Das Diagramm ist auf den relevanten Teil der Systemumgebung beschränkt.

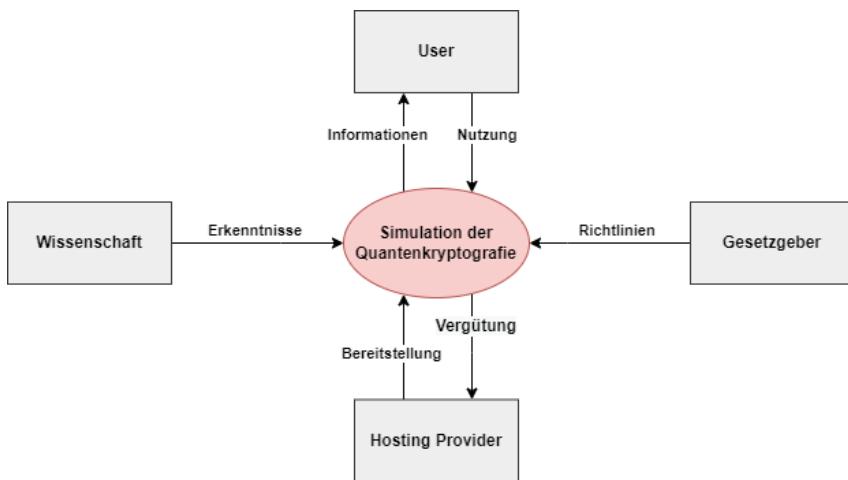


Abb. 3.1: Modellierung des Systemkontexts

3.1.3 Bestimmung der Systemgrenze

Die Systemgrenze definiert, welche Aspekte durch das geplante System abgedeckt werden und welche Aspekte Teil der Umgebung sind. Der Fokus der Anwendung auf der Vermittlung von Lehrinhalten und der Erweiterbarkeit der Inhalte. Eine Kommunikation zwischen der Anwendung und weiteren Systemen oder zwischen den Nutzenden ist nicht Teil des Systems. Die Anwendung soll in der Lage sein, Zustände lokal zu speichern, jedoch werden keine personenbezogenen Daten, wie beispielsweise das Nutzungsverhalten erfasst oder verarbeitet. Optionen zur Registrierung, Übersetzung oder der mobilen Nutzung sind ebenfalls nicht Teil des Systems. Die Bereitstellung der Webseite kann von einem Hosting Provider übernommen werden, welcher somit Teil der Umgebung ist.

Die Kontextabgrenzung dient zur Festlegung der Teile der Umgebung, die relevant sind, also eine Beziehung zum System haben und welche irrelevant sind. Dass es sich um eine bildungsorientierte und keine kommerzielle Anwendung handelt, ist bei der Einordnung der Aspekte zu beachten. Das geplante System basiert auf wissenschaftlichen Erkenntnissen, welche auf der Plattform dargestellt werden. Der User soll die Möglichkeit haben, die dargestellten Inhalte im Rahmen der Weiterbildung zu nutzen, weshalb diese auf die Zielgruppe abgestimmt werden sollten. Richtlinien und Gesetze müssen beachtet und eingehalten werden, sind jedoch nur teilweise, also hauptsächlich im Bereich des Datenschutzes relevant. Falls die Anwendung bei einem Hosting Anbieter bereitgestellt wird, müssen dessen Vertragsbedingungen eingehalten werden. Deshalb zählen Wissenschaft, User, Gesetzgeber und der Hostingprovider zu den für die Entwicklung relevanten Aspekten der Systemumgebung. Im Gegensatz dazu sind Aspekte wie Vertrieb oder Mitbewerber nicht relevant.

3.2 Konkurrenzanalyse

Die folgende Konkurrenzanalyse umfasst einen Vergleich verschiedener Produkte im gleichen Themenschwerpunkt wie die zu erstellende Bildungssoftware. Dabei wird mittels verschiedener Vergleichskriterien ein Überblick über diese Produkte geschaffen. Ziel ist eine Abgrenzung zur Konkurrenz, um mittels der Bildungsapplikation einen Mehrwert für Studierende zu generieren. Im Folgenden ist eine Tabelle mit zwei Produkten, die einen ähnlichen Funktionsumfang haben, gelistet.

	QuVis	Qiskit
Anbieter	The University of St Andrews	IBM
Funktionsumfang	BB84 Schlüsselgenerierung und Man-in-the-middle Angriff	Framework, Dokumentation, Simulation von Quantenschaltkreisen/-computern
Interaktivität	Ja, bitweise Nachverfolgen der Schritte	Ja, eigene Programmierung notwendig
Detailliertheit	Erklärungen, Grundlagen	Dokumentation, tiefgreifende Grundlagen und Erklärungen
Zielgruppe	Schüler und Studenten	Menschen aller Alters- und Berufsgruppen
Lernkanäle	Interaktion (visuell) und textuell	interaktiv (visuell) und textuell
Nutzererfahrung	Übersichtlich dargestellt, Erklärung der Schritte	hoher Durcharbeitungsaufwand, tiefgreifende Erklärungen in einfacher Formulierung
Kompatibilität	Webanwendung, plattformunabhängig	Webanwendung, für Framework Python benötigt oder innerhalb jupyter notebook framework auf der Webseite
Zugänglichkeit	nicht vollständiges Produkt, Webseite, kostenlos	kostenlos, einfache Installation
Zugang unter	(QuVis, 2015, vgl.)	(ANIS u. a., 2021, vgl.)

Tab. 3.1: Konkurrenzanalyse

Die zu entwickelnde Bildungsplattform soll Teile beider Produkte vereinen. Zum einen soll eine ausführliche Grundlageneinführung erfolgen, wie in Qiskit. Zum anderen sollen die Simulationen durch die Plattform bereit gestellt werden, wie bei QuVis. Ebenfalls wird die Anwendung in Form einer Webanwendung bereitgestellt.

3.3 Analyse der Stakeholder

Ausschlaggebend für das Ermitteln von Anforderungen ist das Definieren der Stakeholder, von denen die (Leistungs-)Anforderungen ausgehen. „Bleiben Stakeholder unberücksichtigt oder werden wichtige Stakeholder nicht identifiziert, hat dies signifikante negative Auswirkungen auf den gesamten Projektverlauf, da hierdurch Anforderungen nicht erkannt werden.“ (Pohl und Rupp, 2015, S. 22)

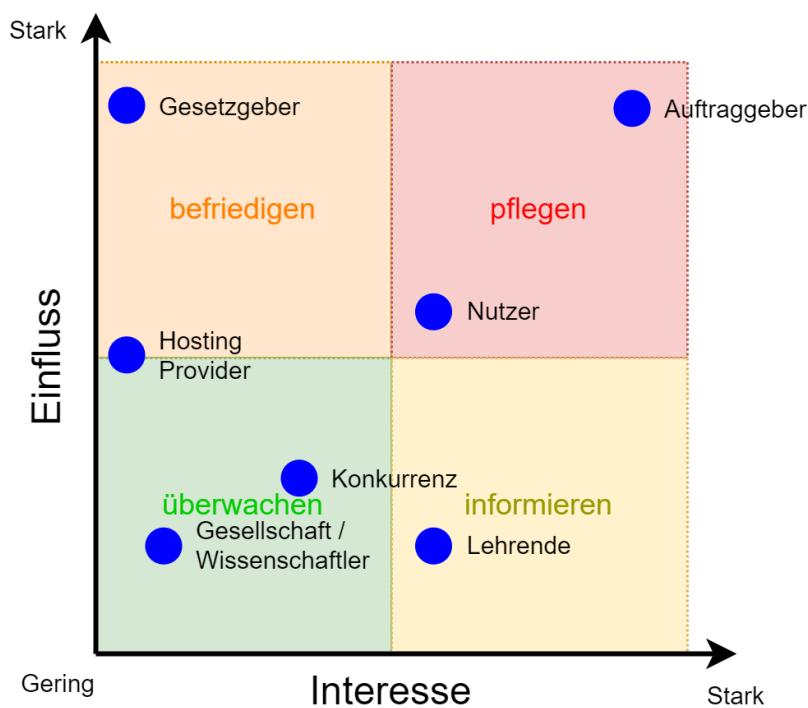


Abb. 3.2: Diese Stakeholdermatrix veranschaulicht den Einfluss in Relation zum Interesse von Stakeholdern des Projekts.

Alle sieben Stakeholder aus Abbildung 3.2 haben verschiedene Sichtweisen auf das Projekt. Die Einordnung beruht auf einer Einschätzung dieser Sichtweisen und dem potenziellen Einfluss auf den Erfolg des Projekts.

- Der **Auftraggeber** muss in die Zusammenarbeit mit eingebunden werden. Deshalb muss der Kontakt zu ihm stets gepflegt werden. Durch einen regelmäßigen Austausch im Sinne des agilen Arbeitens kann auf Änderungen schnell reagiert werden und Probleme können im Keim ersticken werden.
Ist der Auftraggeber mit der Arbeit nicht zufrieden, kann er das Projekt zu jeder Zeit abbrechen. Deshalb müssen seine Wünsche unbedingt berücksichtigt werden.
- Die **Nutzer** sind die zufriedenzustellende Zielgruppe. Das Projekt zielt darauf ab, jungen Studierenden aus niedrigen Semestern das Thema Quantum Computing näher zu bringen. Eine grobe Einordnung der Zielgruppe wären also Studierende im

Alter zwischen 18 und 25, die bereits mit einigen Grundlagen der Informatik vertraut sind und solide Grundkenntnisse der Mathematik besitzen.

Ohne Nutzer zu gewinnen und diese zu halten, scheitert das Projekt. Auf Ihre Anforderungen muss deshalb besonders geachtet werden.

3. Die **Lehrenden** sind Dozenten und Professoren an Hochschulen und Universitäten.
In diesem Kontext stellen sie die Bildungsplattform ihren Studierenden vor und leiten sie dazu an, mithilfe von dieser vorgegebene Lernziele zu erreichen. Deshalb ist es vorteilhaft, diese über das Projekt informiert zu halten.
Umso mehr den Lehrenden das Projekt gefällt, desto eher nutzen sie es für ihren Unterricht. Das Befriedigen ihrer Wünsche würde folglich zusätzliche Nutzerzahlen generieren.
4. Die **Konkurrenz** sollte stets überwacht werden, um zu verhindern, versehentlich eine Kopie eines bereits etablierten Produkts zu veröffentlichen. Außerdem können Ideen von Konkurrenzprodukten für das Projekt abgeleitet werden. Die Konkurrenz wird vermutlich ähnliche Schritte einleiten.
5. Die **Gesellschaft bzw. Wissenschaftler** sind ebenfalls ein relevanter Stakeholder, da die Bildungsplattform auf ihren Erkenntnissen beruht. Deshalb muss diese Stakeholdergruppe mit großem Respekt behandelt werden.
Außerdem dient das Projekt als Einstieg in die wissenschaftliche Welt des Quantum Computings, weshalb ein guter Ruf in der wissenschaftlichen Gesellschaft ebenso die Nutzerzahlen erhöhen würde. Deshalb sollten vereinzelte Anregungen dieser Stakeholdergruppe berücksichtigt werden.
6. Der **Gesetzgeber** hat kein ausgeprägtes Interesse an diesem Projekt, aber den Einfluss, es scheitern zu lassen. Deshalb müssen die wenigen Anforderungen des Gesetzgebers unbedingt beachtet werden, um ihn befriedigt zu halten.
7. Der **Hosting Provider** hat ähnlich wie der Gesetzgeber kein starkes Interesse an dem Projekt, hat aber signifikanten Einfluss auf die Erreichbarkeit der Bildungsplattform. Die Nutzungsbedingungen des Providers müssen deshalb mit den Anforderungen der anderen Stakeholdern abgeglichen werden. Auf der anderen Seite muss die Qualität des Providers auch den Anforderungen der Stakeholder gerecht werden, wie zum Beispiel einer hohen Uptime. Deshalb sollte dieser sowohl befriedigt, als auch überwacht werden.

3.4 Ermittlung der Anforderungen

Die Anforderungen des Projekts werden mit verschiedenen Methodiken ermittelt. Die Systemgrenzen weisen den Umfang der Anforderungen auf und die Interessen der Stakeholder dienen als Grundlage.

Für dieses individuelle Projekt werden Brainstorming von Anforderungen und Nicht-

Anforderungen, eine Analyse der Konkurrenz und Befragungen von Stakeholdern verwendet, um eine Sammlung aus verschiedenen Anforderungen zu erstellen.

Die Anforderungen werden nach dem Kano-Modell in **Basisfaktoren** (selbstverständliche Anforderungen, in Gesprächen unbenannt), **Leistungsfaktoren** (Hauptanforderungen, werden von Stakeholdern genannt) und **Begeisterungsfaktoren** (positive Zusätze, den Stakeholdern noch unbekannt) aufgeteilt. Das Kano-Modell beschreibt die Transformation von Begeisterungsfaktoren zu Basisfaktoren im Laufe der Zeit. Der Grund dafür ist die Gewohnheit an bestimmte Anforderungen. (Pohl und Rupp, 2015, Vgl. S. 25)

3.4.1 Brainstorming

Das Brainstorming der Anforderungen wird in zwei Schritten durchgeführt. Zunächst wird eine Mindmap mit den Anforderungen, die nicht umgesetzt werden sollen, erstellt. Dadurch entsteht in Kombination mit den Systemgrenzen ein klares Bild der Bildungsplattform und erleichtert das Finden realer Anforderungen. Diese realen Anforderungen werden anschließend mit einer zweiten Mindmap visualisiert.

Beide Mindmaps werden aus der Sichtweise des Projektteams erstellt und beruhen sowohl auf ihrer eigenen Vorstellung als auch auf den Informationen, die bis jetzt schon bekannt sind. Das bedeutet, dass die Inhalte der Mindmaps noch variabel sein können.

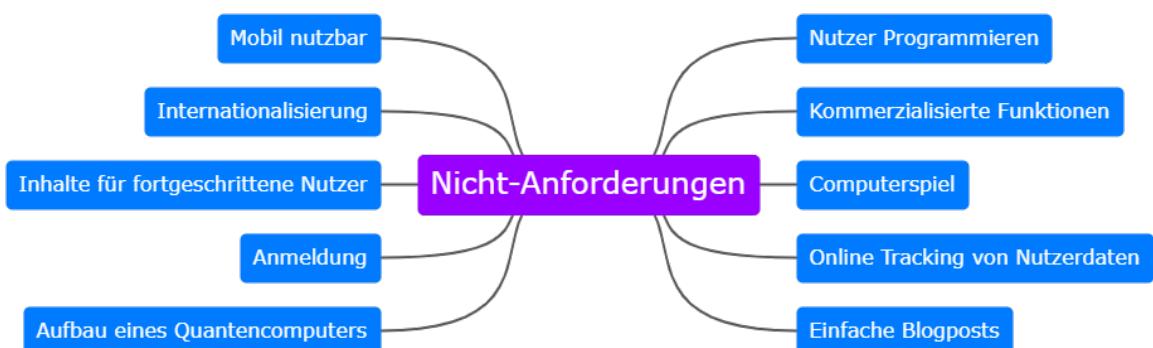


Abb. 3.3: Mindmap der Nicht-Anforderungen aus der Sichtweise des Projektteams

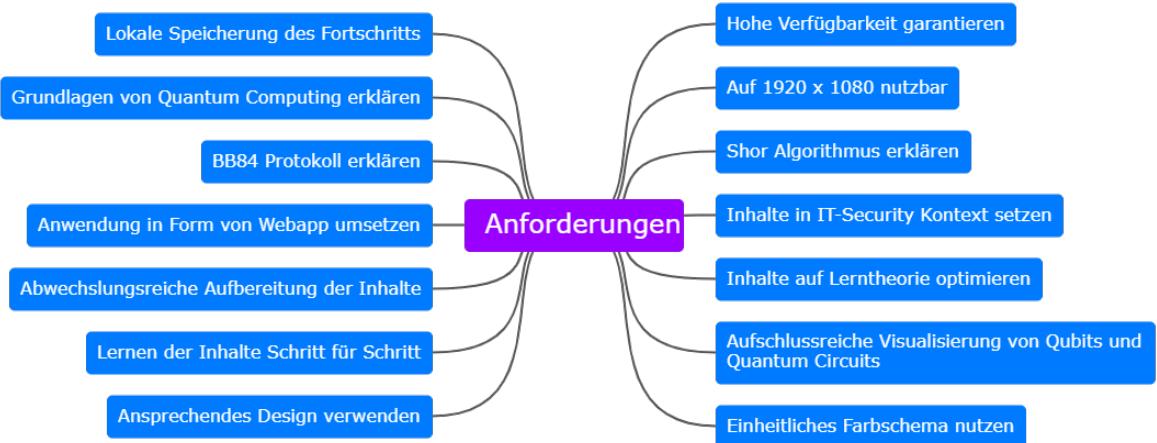


Abb. 3.4: Mindmap der Anforderungen aus der Sichtweise des Projektteams

3.4.2 Konkurrenz

Innerhalb der Konkurrenzanalyse wurden die Konkurrenzprodukte QuVis und Qiskit betrachtet. Hieraus lässt sich ebenfalls auf Funktionen schließen, die zum einen übernommen werden sollen und zum anderen die Abgrenzung zur Konkurrenz definieren.

Die Plattform sollte für eine große Menge an Anwendern zur Verfügung stehen. Dies ermöglichen die betrachteten Produkte in einer Webanwendung. Beide Produkte ermöglichen eine Interaktivität mit den Simulationen, wodurch motorische Lerntypen angesprochen werden können. Ebenfalls bieten die Produkte eine visuelle und textuelle Beschreibung des Lerninhaltes. Hierdurch werden ebenfalls visuelle Lerntypen angesprochen. Diese Vielzahl an Lernkanälen soll ebenfalls durch die Bildungsplattform gewährleistet werden. Ebenfalls soll wie bei Qiskit eine einheitliche Übersicht über die Lerninhalte bereitgestellt werden.

3.4.3 Befragungen

Mithilfe der Befragung von Stakeholdern können konkrete Leistungsfaktoren erörtert werden. In Gesprächen lässt sich dabei häufig auch einige nicht erwähnte Basis- und Begeisterungsfaktoren rückschließen.

Es werden die Stakeholder aus dem *pflegen*-Quadranten der Stakeholder Matrix aus Abbildung 3.2, also der *Auftraggeber* und die *Nutzer*, befragt, da diese am meisten Relevanz für das Projekt haben.

Die Befragung des Auftraggebers erfolgt in einem direkten Gespräch in Form eines Interviews. So können unklare Fragen auf Seite des Projektteams schnell geklärt werden. Der Auftraggeber kann im Anschluss noch zusätzlichen Input liefern, falls Punkte unerwähnt blieben. Die aus dem Interview resultierenden Anforderungen werden direkt in die Anforderungsliste übernommen. Das Interview ist in Anhang A.1 einsehbar.

Da die Stakeholdergruppe *Nutzer* deutlich größer ist als *Auftraggeber*, sind direkte Interviews sehr zeitaufwändig. Deshalb wird ein Umfrageformular erstellt, das Anhaltspunkte auf den Nutzer selbst, die Inhalte der Lernplattform und konkrete Anforderungen aufnimmt. Dieses Formular kann schnell an die Nutzer versandt und von diesen ausgefüllt werden.

Bei der Erstellung der Umfrage muss darauf geachtet werden, dass diese nicht zu lang oder zu aufwändig ist und der Nutzer dadurch nicht die Geduld verliert. Durch die Verwendung von Multiple Choice Fragen und die Sparsamkeit von Textfeldern kann dem entgegen gesteuert werden. Allerdings werden dadurch die erhaltenen Informationen verringert und es besteht die Gefahr, dass nicht alle relevanten Punkte vom Projektteam abgedeckt werden.

Die Umfrageergebnisse werden zunächst ausgewertet, bevor diese in die Anforderungsliste übernommen werden können. Das verwendete Umfrageformular ist in Anhang A.2 einsehbar, die genauen Ergebnisse werden im Folgenden evaluiert. .

Ergebnisse

In der Umfrage wurden 525 Studierende aus allen Semestern befragt. Davon studierten 99,4 % an einer Hochschule und 0,6% an einer Universität. Die prozentuale Zuordnung der Anzahl der Studierenden zu den Semestern ist in Abbildung 3.5 zu sehen.

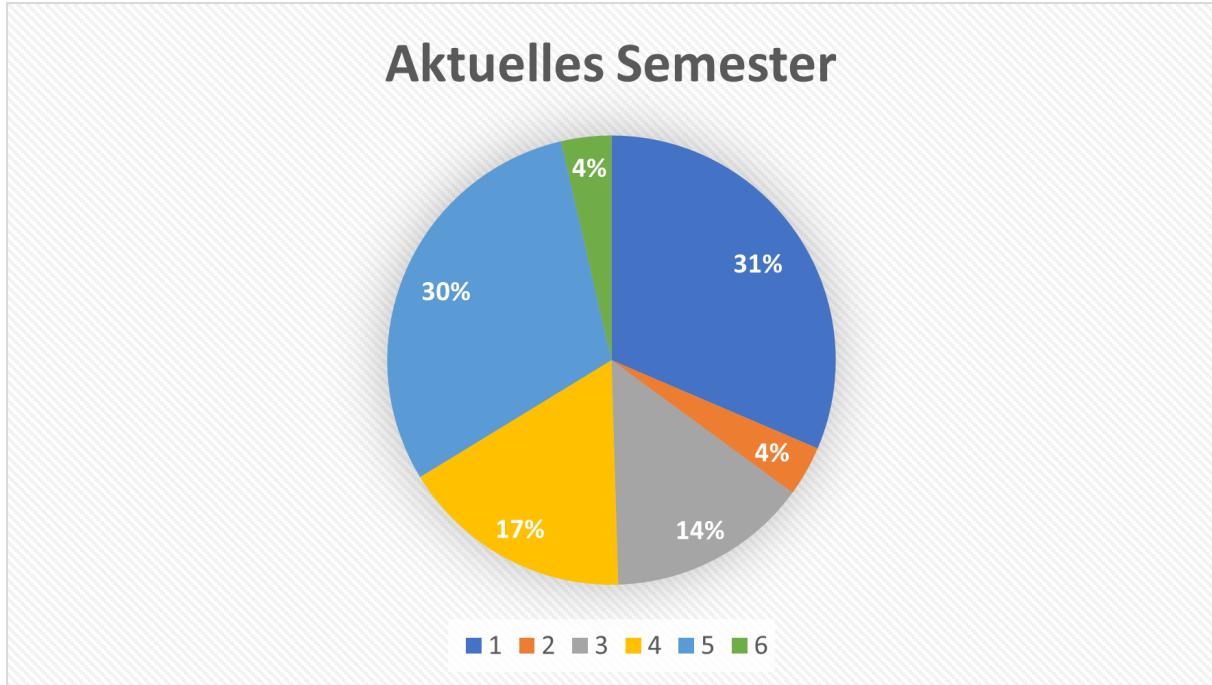


Abb. 3.5: Semester der Befragten

Die höchste Beteiligung an der Umfrage entstammt dem ersten (31,5%) und dem fünften (30,1%) Semester.

Zunächst wurden Fragen im Bereich der Lerntheorie gestellt. Dabei erfolgte eine Selbst-einschätzung der Befragten in einen oder mehrere definierte Personentypen. Dabei identifizierten sich die Befragten hauptsächlich mit den nachfolgenden Personas:

- Der/Die Kreative - Das Fühlen und Wahrnehmen von konkreten Erfahrungen steht im Vordergrund. (147 Befragte, 28%)
- Forscher*in - Die Stärke liegt in der Anwendung von Logik und theoretischen Modellen. (132 Befragte, 25,1%)
- Ingenieur*in - Arbeitet auch mit Modellen, legt aber mehr Wert auf aktives Experimentieren. (207 Befragte, 39,4%)
- Macher*in - Führt Experimente durch und legt gleichzeitig Wert auf praktische Erfahrungen. (203 Befragte, 38,7%)

Um die Anforderungen dieser Gruppen zu bedienen, sollten zum einen grafische Darstellungen und eine Erlebnispädagogik zum Einsatz kommen. Zum anderen sollten die dargestellten Modelle interaktiv sein und gelernte Inhalte zu bekanntem verknüpfen. Vor allem die Möglichkeit, gelerntes Wissen aktiv anzuwenden, um die verschiedenen Ergebnisse bei unterschiedlichen Rahmenbedingungen sollten gewährleistet werden.

Im Folgenden erfolgte eine Einschätzung zu ihren individuellen Rahmenbedingungen für erfolgreiches Lernen. Die Ergebnisse sind in Abbildung 3.6 zu erkennen.

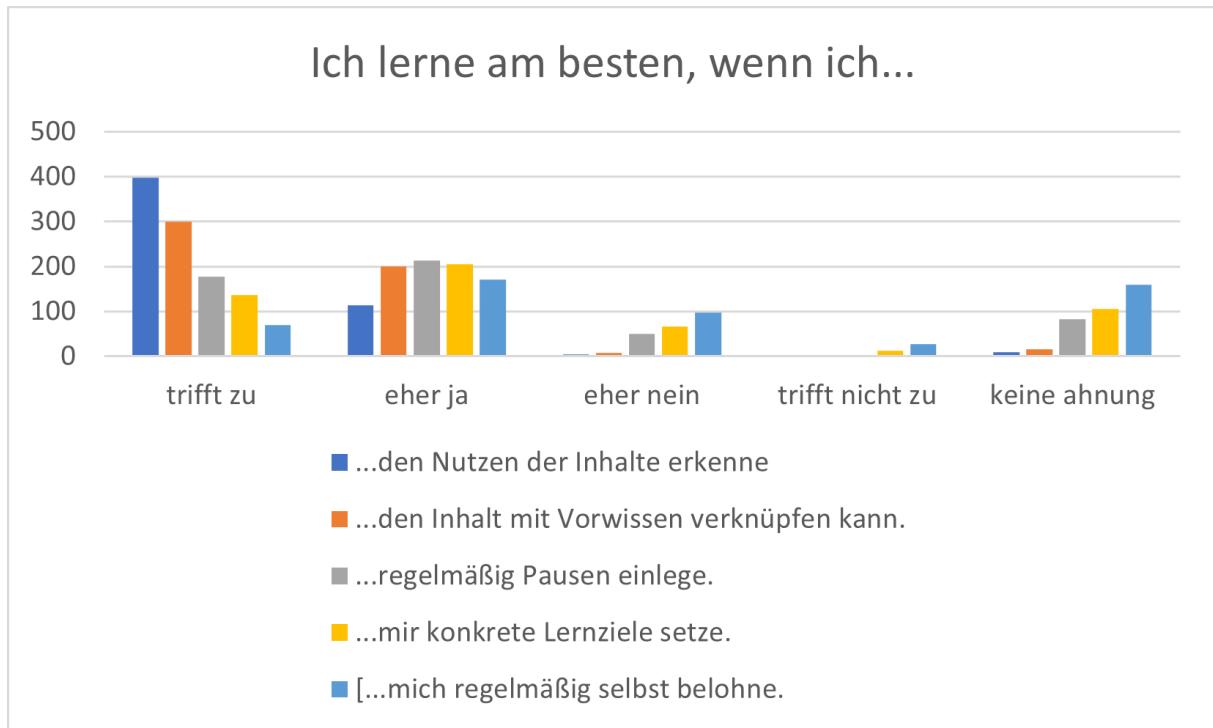


Abb. 3.6: Unter Welchen Bedingungen lernen die Befragten optimal

Dabei gaben 397 Befragte (75,6%) an, ihnen sei es wichtig, den Nutzen der Inhalte zu erkennen. 114 Befragte (21,7%) gaben eher ja als Antwort. Hierdurch spiegelt sich die

Relevanz für die Erklärung vom Zusammenhängen und Bezügen zur Praxis innerhalb der Bildungsplattform wieder.

Dies spiegelt sich ebenfalls in der Auswahlmöglichkeit, den Inhalt mit Vorwissen verknüpfen zu können, wieder. 300 Befragte (57,1%) gaben dies als zutreffend und 200 (38,1%) mit eher ja an.

178 Befragte (33,9%) wünschen sich regelmäßige Pausen für ein erfolgreiches Lernen, 213 (40,5%) beantworteten diese Frage mit eher ja. Um dies zu ermöglichen, sollten die Lerneinheiten kompakt und zeitlich begrenzt sein. Hierdurch können die Lektionen abgearbeitet werden und im darauffolgenden eine Pause eingelegt werden. Ebenfalls kann ein Hinweis innerhalb der Plattform über das Einlegen von Pausen eingebaut werden.

Im weiteren Verlauf wurde die Relevanz von gesetzten Lernzielen abgefragt. Dabei sagten 202 (38,4%) aus, dass diese eher hilfreich sind. Bei Belohnungen kristallisierte sich heraus, dass einige der Studierenden diese positiv bewerteten, jedoch ebenso viele dieses nicht beurteilen konnten.

Darauffolgend wurde das Interesse an den Themengebieten und das Vorwissen mittels einer Zahlenskala abgefragt. Dabei steht 1 für ein geringes Vorwissen oder Interesse und 5 bzw. 10 für ein hohes Interesse und Vorwissen.

Auf die Frage Wie sehr interessierst Du dich für Quantentechnik, insbesondere Quantenkryptografie? zeigt sich eine absteigende Verteilung des Interesse. Nur 2,5 % der Befragten gaben ein hohes Interesse an der Thematik an, 14,9% bewerteten ihr Interesse mit 4 von 5. Dies zeigt die Spezialisierung des Themas im Bereich Physik und Informatik auf. Durch gezielte Demonstrationen und Werbung könnte das Interesse an der Thematik gesteigert werden.

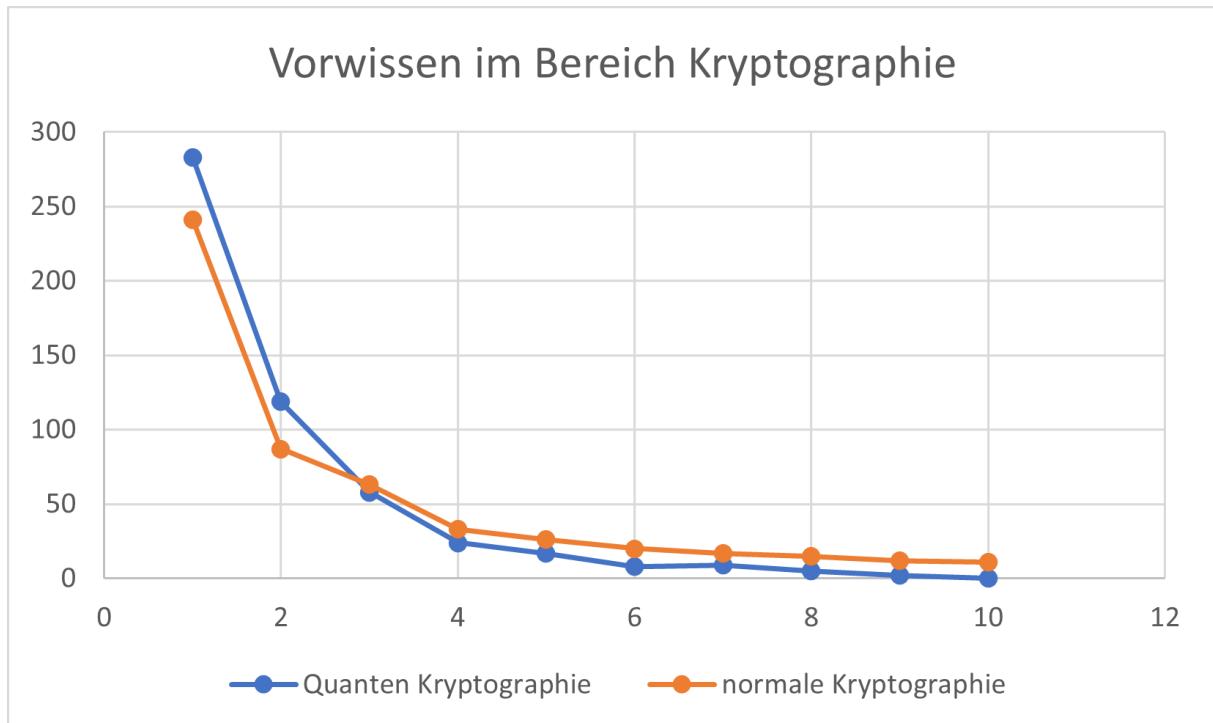


Abb. 3.7: Vorwissen in den Bereichen klassische und quantentechnische Kryptografie

Ebenfalls gaben 87,6% der Befragten ein geringes Vorwissen im Bereich von Quanten Computing an, was in Abbildung 3.7 im Vergleich zur klassischen Kryptografie dargestellt ist. Die Bildungsplattform sollte deshalb sowohl komplexe Verfahren, als auch die Grundlagen behandeln. Im Vergleich zu der klassischen Kryptografie ist das Vorwissen ähnlich. Ebenfalls dieses Themenspektrum ist den Befragten nur im geringen Maße, jedoch etwas mehr, bekannt.

In der anschließenden Frage sollte die gewünschte Tiefe der zu behandelten Themen eingeordnet werden. Hierbei hab es drei Auswahlmöglichkeiten, welche in der Abbildung 3.8 zu sehen sind.

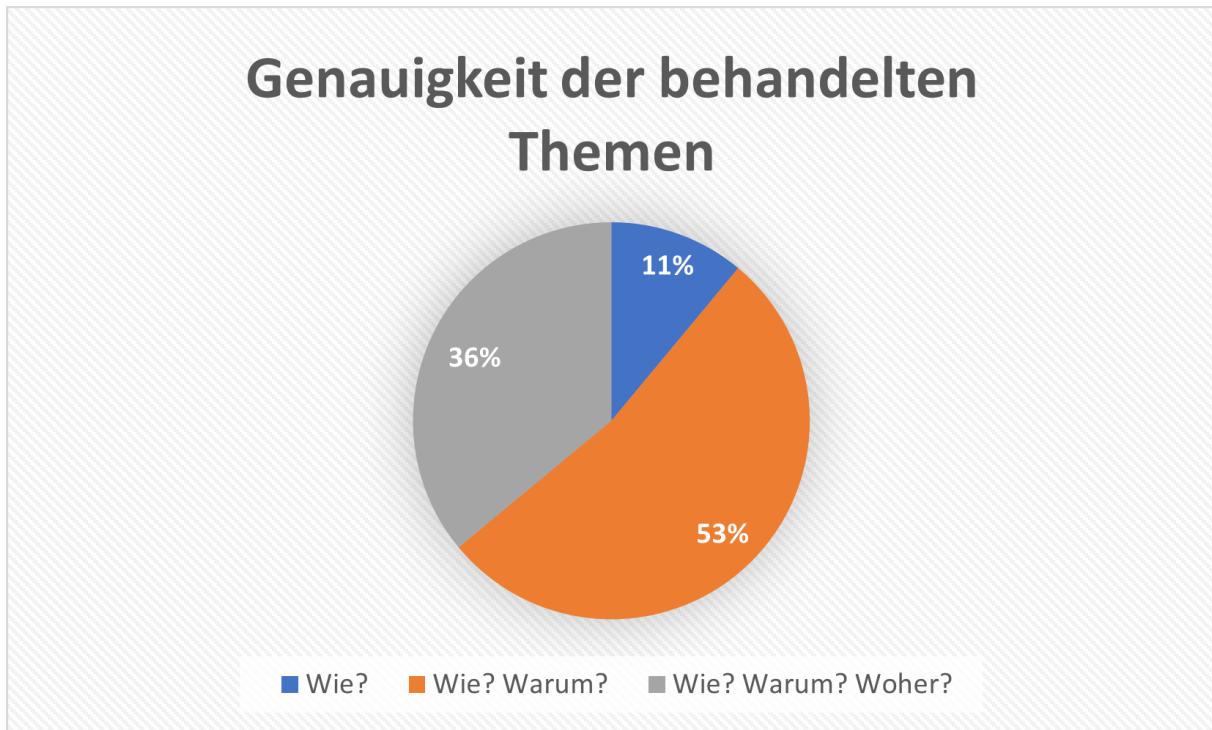


Abb. 3.8: Genauigkeit der behandelten Themen

53% der Befragten wünschen sich Erläuterungen zur Funktion und deren Aufbau. Hierauf sollte in der Bildungsplattform der Hauptfokus der Inhalte gelegt werden. 36% wünschen sich außerdem eine Herleitung der Inhalte, weshalb dies in Form eines ergänzenden Abschnittes ebenfalls erläutert werden sollte.

Zu der Frage, ob sich die Studierenden Übungen innerhalb der Bildungsplattform wünschen, zeigte sich ein klares Meinungsbild, welches sich für diese aussprach. Nur 2 % waren gegen die Einführung von Übungen, wogegen sich 25,7 % für Übungen am Ende der Lektion aussprachen und 70,5 % sich ebenfalls Übungen innerhalb der Lektionen wünschten.

Als weiteres Element sollten die gewünschten Lernkanäle ermittelt werden. Dabei ordneten die Studierenden textuelle, grafische, animierte, auditive, videografische, simulierte und interaktiv simulierte Designelemente in die Kategorien sehr hilfreich, hilfreich, eher nicht hilfreich und unentschlossen ein.

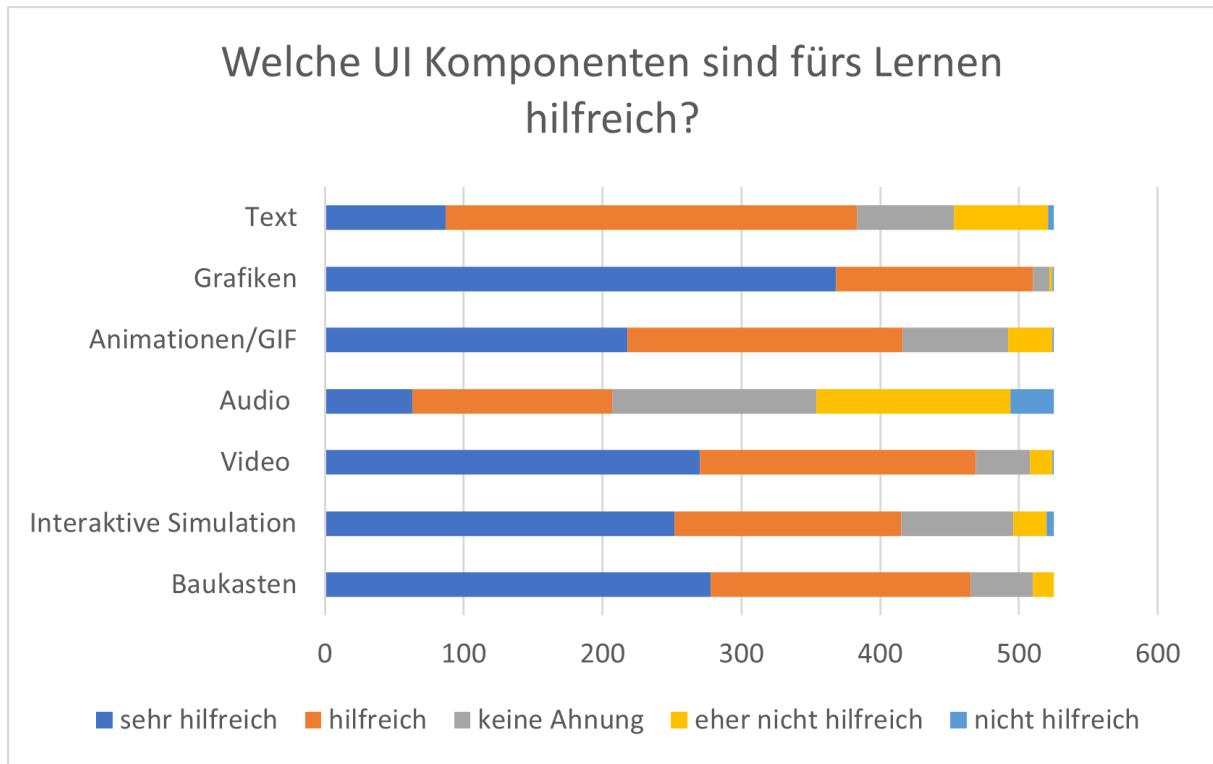


Abb. 3.9: Lernkanäle

Abbildung 3.9 zeigt die Ergebnisse dieser Frage. So wurden Grafiken von den Studierenden als hilfreichstes Element gewertet, gefolgt von interaktiven Simulationen und Videos. Audiodateien wurden als am wenigsten hilfreich gewertet, weswegen dies innerhalb der Bildungsplattform weggelassen wird.

Zuletzt sollten die Studierenden die Leistung ihres Computers oder Laptops zwischen 1 für schlecht und 5 für sehr gut einordnen. 50% schätzen ihren Computer für gut bis sehr gut ein, 20% für mittel und 30 % schätzen ihren Computer im unteren drittel ein. Da jedoch die Leistung vorwiegend im mittleren und guten Bereich eingeordnet wird, ist davon auszugehen, dass die Webapplikation auf fast allen Computern der Studierenden unterstützt wird.

3.5 Anforderungsliste

Die Anforderungsliste ist eine systematisch dargestellte Sammlung aller Anforderungen an das Projekt und ist in Anhang A.4 einsehbar. Während der Durchführung des Projekts muss diese stets aktuell gehalten werden, um nachträgliche Anforderungen oder Veränderungen zu berücksichtigen.

Die Liste wird der Einfachheit halber mit Microsoft Office 365's *Excel* erstellt und verwaltet, da diese Anwendung genug Flexibilität mit sich bringt und keine Einarbeitung seitens des Projektteams benötigt.

In der Anforderungsliste setzt sich jede Anforderungen aus den grundlegenden Metadaten **ID**, **Name**, **Kurzbeschreibung**, **Begründung**, **Datum letzter Änderung**, **Autor** und den in Kapitel 3.4 beschriebenen **Anforderungsfaktoren** zusammen. Weitere komplexe Attribute, die in der Anforderungsliste enthalten sind, werden hier erläutert:

- Die **Volatilität** sagt auf einer Skala von 1 bis 10 aus, wie variabel die Anforderung im jetzigen Stand noch ist.
- Die **Dringlichkeit** gibt auf einer Skala von 1 bis 10 an, wie zeitnah eine bestimmte Anforderung umgesetzt werden muss.
- Das **Stakeholder-Interesse** beschreibt die Wichtigkeit der Anforderung für die Stakeholder auf einer Skala von 1 bis 10.
- Die **Priorität** einer Anforderung besteht aus dem Mittelwert der Dringlichkeit, der Stakeholder-Interesse und der invertierten Volatilität.
- Die **Klasse** dient zur Klassifizierung der Anforderung, um diese z.B. einem Designer oder Programmierer zuzuweisen.
- Das **Risiko** bestimmt die Wichtigkeit der sorgfältigen Arbeit. Ist ein Risiko hoch, so kann dies bei einem Fehler in der Umsetzung der Anforderung große Auswirkungen auf die Stakeholder haben.
- Der **Aufwand** beschreibt die geschätzte Umsetzungszeit der Anforderung auf einer Skala von 1 bis 10 und wird vom Projektteam vorgegeben.

4 Anwendungsentwicklung

In diesem Kapitel wird die Durchführung des Projektes, also die Entwicklung der Anwendung beschrieben. Dabei wird auf die Architektur, die verwendeten Bibliotheken, die visuelle Gestaltung und Administration genauer eingegangen.

4.1 Architekturmuster: Model-View-Controller (MVC)

Das Model-View-Controller Architekturmuster (abgekürzt MVC) teilt eine Anwendung in drei Komponentengruppen auf. In Modelle (Models), Ansichten (Views) und Controller (Controllers).

Das Modell kann unabhängig von der grafischen Darstellung (View) erstellt und getestet werden, da es weder von der View noch vom Controller abhängig ist. Jedoch sind View und Controller abhängig vom Modell. In der MVC-Anwendung ist das **Modell** für die Darstellung des Status und der Vorgänge bzw. der Geschäftslogik zuständig. Der **Controller** übernimmt die Verarbeitung der Benutzerinteraktionen. Der Controller ist der Einstiegspunkt des MVC-Musters. Er ist verantwortlich für die Auswahl des genutzten Modells und der genutzten View und kontrolliert somit wie die App auf eine bestimmte Anfrage reagiert. Die **Ansicht** dient zur Darstellung von Inhalten in Form einer Benutzeroberfläche. Dabei soll in der Ansicht so wenig Logik wie möglich enthalten sein bzw. sich nur auf die Darstellung von Inhalt beziehen.

Die Beziehungen zwischen den drei Komponenten sind in Abbildung 4.2 dargestellt.

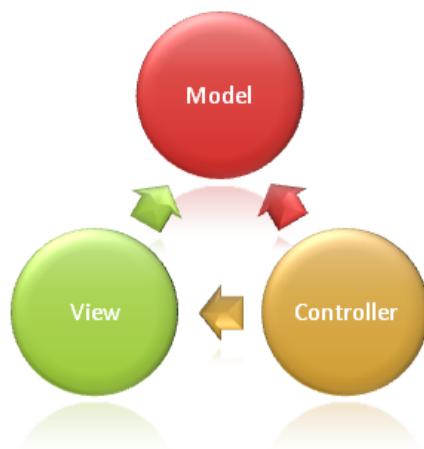


Abb. 4.1: MVC: Beziehungen der drei Hauptkomponenten (Smith, 2022)

Durch die Verteilung und Abgrenzung der Aufgaben auf die Hauptkomponenten wird die Skalierung der Anwendung erleichtert, da es leichter ist, ein Element zu entwickeln und zu testen, dass sich nur auf eine einzelne Aufgabe beschränkt und keine zusätzlichen Abhängigkeiten aufweist. (Smith, 2022, vgl.)

Da die Bildungsplattform eine Single Page Application mit flachen Seitenhierarchien ohne Backend ist, eignet sich die simple MVC Architektur besonders für die Anwendung.

Das Model besteht aus zwei Teilen: den Cookies und dem Content. Die Cookies sind ausschließlich funktional und speichern die Nutzereinstellungen und den Fortschritt. Hierfür wird der Local Storage des aktuellen Webbrowsers verwendet. Die Seiteninhalte hingegen werden von LaTeX (.tex) Dateien und weiteren Medienelementen definiert.

Als Schnittstelle zwischen Anwendung und der beiden Models werden zwei separate Controller verwendet. Updates beim Fortschritt oder den Einstellungen werden ebenfalls von weiteren Controllern verwaltet, genauso wie der Hilfe-Chat.

Die View stellt vordefinierte statische Seiten dar, sowie dynamische Elemente. Das Intro-Tutorial, die Landing Page, der Hilfe-Chat und die Einstellungen sind bis auf wenige funktionale Elemente unveränderbar in ihrer Darstellung. Dynamisch hingegen ist die Kapitelübersicht, die je nach Anzahl an Kapitelordnern die verschiedenen Kapitel anzeigt. Ebenso wird durch die Farbe des Kapitel-Icons visualisiert, ob das Kapitel bereits abgeschlossen wurde. Die Kapitelordner beinhalten eine LaTeX-Datei, eine beschreibende JSON-Datei, zwei Icons und zusätzliche Medienelemente wie Videos, Bilder, Skript Elemente oder Schaltkreise, die von verschiedenen Controller geladen werden. In der View befinden sich hierfür vordefinierte JSX-Komponenten Blueprints für die Umsetzung der Medienelemente.

Die finale MVC-Architektur ist in Abbildung 4.2 einsehbar.

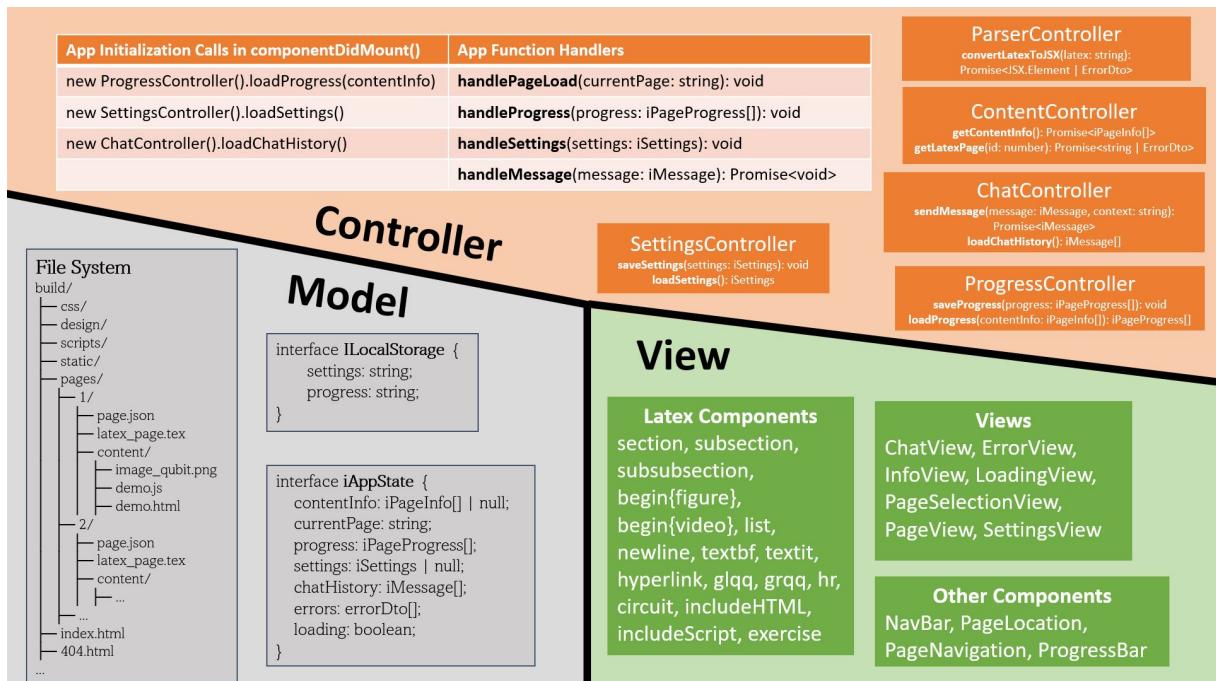


Abb. 4.2: Planung der Anwendung mittels einer MVC-Architektur

4.2 Technologieentscheidung

Die Technologieentscheidung basiert auf der Einhaltung aller technischen Anforderungen und der generellen Machbarkeit. Wichtig ist dabei, dass sich die empfohlene Technologie im Gesamtsystem integrieren lässt, also kompatibel ist.

Die Anforderungen beschreiben eine Webanwendung, die auch ohne aktive Internetverbindung auf Desktop-PCs lokal ausgeführt werden kann. Unterstützung für die aktuellen Versionen des Browsers Chrome unter den Betriebssystemen Windows und Linux muss gegeben sein. Eine Umsetzung der Anwendung als Single Page Application erfüllt diese Anforderungen und bietet eine bessere Nutzerfreundlichkeit als herkömmliche Webanwendungen, die nicht als Single Page Applications konzipiert wurden.

Single Page Applications sind Webanwendungen, die aus einer einzelnen HTML-Seite (meist index.html) bestehen. Diese wird vom Browser geladen, wobei Code ausgeführt wird, wodurch Teile der Webseite mit neuen Daten vom Webserver dynamisch aktualisiert werden können. Während des gesamten Prozesses wird die Website nicht neu geladen und leitet nicht auf andere Webseiten weiter. Durch schnellere Übergänge kommt die Webseite einer nativen Anwendung möglichst nahe. (Krause, 2021, vgl. S. 6) Die HTML 5 API bietet eine wesentliche Grundlage für die Web-Entwicklung. Alle bestehenden Frameworks und Bibliotheken bauen darauf auf. Vorteile bei der Verwendung von Web-Frameworks sind unter anderem eine vereinfachte oder reduzierte Ansicht (View), ein eleganteren API-Stil oder sogar robusterer Code dank zusätzlicher Fehlerbehandlung. (Krause, 2021, vgl. S. 7) Web-Frameworks werden eingesetzt, um einfache Tätigkeiten innerhalb der Entwicklung zu automatisieren und damit den gesamten Prozess der Erstellung der Webseite zu vereinfachen.

Um ein passendes Web-Framework auszuwählen, müssen zunächst die auf dem Markt vorhandenen und genutzten Bibliotheken betrachtet werden. Eine Umfrage zu den meistgenutzten Web-Frameworks unter Entwicklern weltweit ab 2021 ist zu folgendem Ergebnis gekommen:

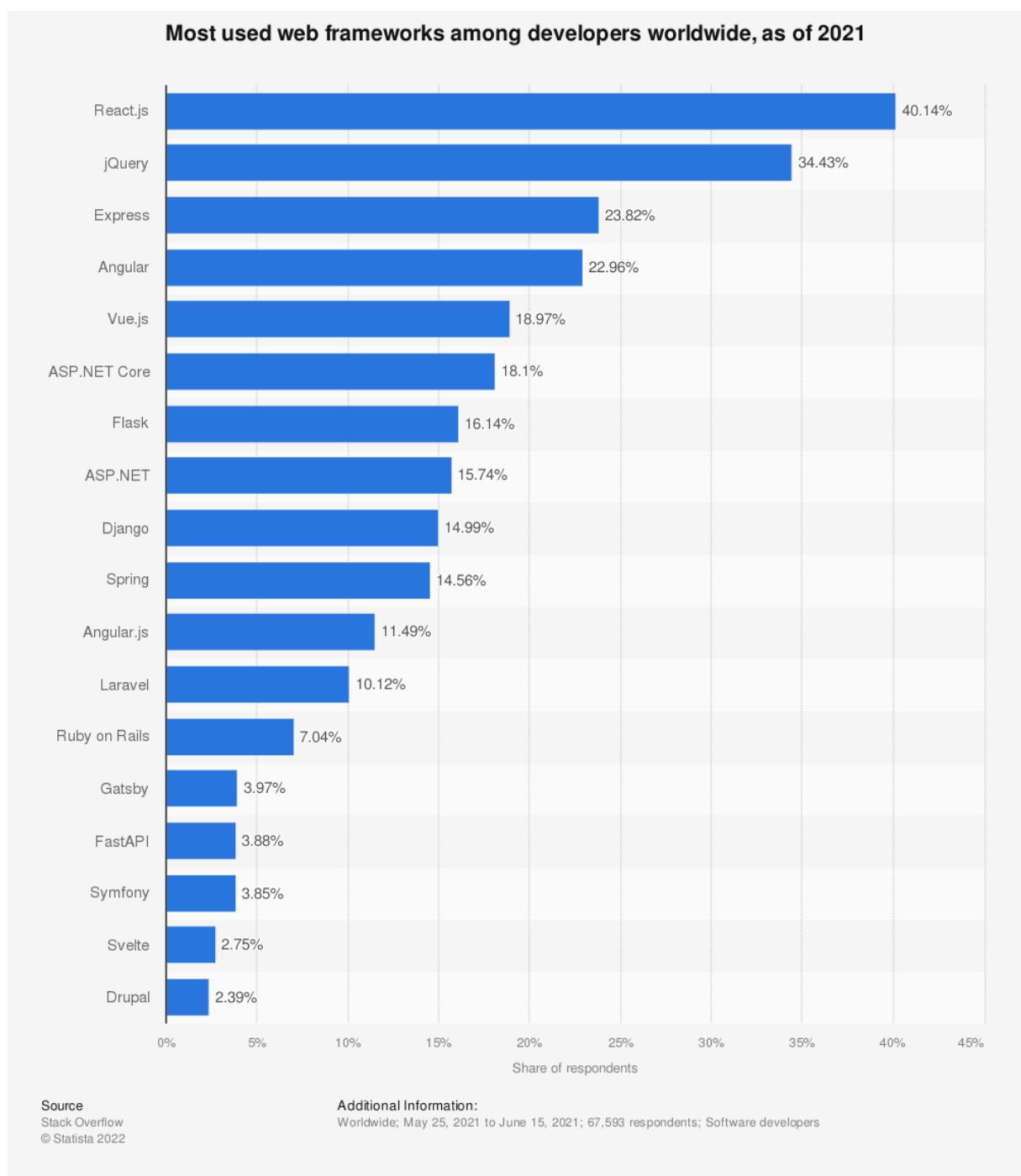


Abb. 4.3: Meistgenutzte Web-Frameworks unter Entwicklern weltweit, ab 2021 (Stack Overflow, 2021)

React.js wird ab 2021 das meistgenutzte Web-Framework unter Softwareentwicklern weltweit sein. Es gab 40,14 Prozent der Befragten an, React.js zu verwenden, während 34,43 Prozent jQuery nutzten. Weitere häufig genutzte Frameworks sind Express, Angular, AngularJS, Vue.js und ASP.NET Core. (Stack Overflow, 2021)

Für die Umsetzung des Projektes kommt die von Facebook entwickelte Bibliothek React.js zum Einsatz, da sie aus den folgenden Gründen gut geeignet ist:

React.js ist im Gegensatz zu Angular oder Vue.js keine Frontend Gesamtlösung, sondern

eine leichtgewichtige Bibliothek zum Rendern grafischer Oberflächen. Somit ist React.js nur ein Teil der Webanwendung und wird deshalb mit weiteren Modulen kombiniert. Dadurch lässt sich die Bibliothek entkoppeln und kann in Zukunft bei Bedarf auch ausgetauscht werden. Ein weiterer Vorteil ist die enge Integration von JavaScript, dadurch kommt kein proprietärer Programmcode, sondern bereits etablierte Standards zum Einsatz. Veröffentlicht wird die Softwarebibliothek unter der MIT-Lizenz, wodurch die Wiederverwendung sowohl für Open-Source (frei verwendbarer Quelltext) als auch für Closed-Source Projekte (nicht frei verwendbarer Quelltext) gestattet ist. (Roden, 2020)

Außerdem ist React.js im Vergleich zu Vue.js und Angular das flexibelste Framework mit nur wenig Vorgaben. Das Framework kann den Anforderungen entsprechend mit weiteren Bibliotheken erweitert werden. Dadurch wird vermieden, dass viel ungenutzter Code in die finale Anwendung integriert wird.

Unabhängig von dem ausgewählten Framework wird zusätzlich aufgrund der mangelhaften Wartbarkeit von JavaScript die TypeScript Erweiterung verwendet. Dadurch ist eine erhöhte Vorbeugung von Fehlern gegeben, beispielsweise durch sauberen Code und besseres Linting mithilfe der IDE.

4.3 Drittanbieter Bibliotheken

Für die bestmögliche Umsetzung der Anforderungen werden im Rahmen der Programmierung einige Bibliotheken der React.js Anwendung hinzugefügt. So wird der Fokus bei der Anwendungsentwicklung auf das Ergebnis gelegt, da viele Grundlagen nicht zusätzlich noch implementiert werden müssen.

- **React Router** erweitert das React-Framework mit einem Frontend Routing System, um im Rahmen einer Single Page Application dem Nutzer dennoch das Gefühl mehrerer Seiten zu ermöglichen.
- **Bootstrap** wird als Unterstützung für die Umsetzung des Designs verwendet. Hierbei werden sowohl die CSS-Datei importiert, als auch das *react-bootstrap* Packet.
- **Three.js** dient als 3D-Engine für interaktives Simulieren verschiedener Lerninhalte.
- **MathJax** unterstützt den Controller bei der Konvertierung der mit LaTeX definierten mathematischen Elemente zu HTML.
- **Quantum.js** dient als Engine für das Berechnen für Quantenschaltungen und bietet zusätzlich interaktive Visualisierungen.

4.4 Umsetzung des LaTeX-Parsers

Ein zentrales Feature der Anwendung ist das einfache Integrieren neuer Inhalte. Durch das Hinzufügen einer LaTeX-Datei können neue Kapitel ohne Programmieren individuell erstellt werden. Um dies zu ermöglichen, muss die Anwendung über einen Parser verfügen,

der die LaTeX-Blaupause in eine Webseite bestehend aus HTML-Elementen konvertiert. Diese Aufgabe übernimmt der Parser Controller. Das Parsing wird in vier Schritte aufgeteilt:

1. **Fetching:** Der Controller lädt die *page.tex* Datei über die JavaScript *fetch()* Methode. Anschließend wird der Seiteninhalt dem zweiten Schritt als ein einzelner String übergeben.
2. **Sweeping:** Der String wird Stück für Stück von Anfang bis Ende nach LaTeX-Elementen durchsucht. Die Elemente haben eine bestimmte Anfangs- und Endnotation und sind im Controller definiert.

Wenn ein Element gefunden wird, wird dieses zu einem für React renderbaren JSX-Element konvertiert und auf ein Element-Array gepusht. Dabei wird der Inhalt des Elements auf dieselbe Weise nach Subelementen untersucht, wie beispielsweise der Überschrift eines Bildes. Enthält ein Element ein Skript, so wird dieses registriert.

3. **Mapping:** Das Element-Array wird zu einem großen JSX-Element zusammengefügt. Hierbei werden String-Elemente in MathJax Tags umhüllt. Es wird davon ausgegangen, dass String-Elemente entweder Fließtext oder Gleichungen sind, die beide mathematische Elemente enthalten können.

Da das Rendern von mathematischen Elementen über MathJax viel Rechenleistung benötigt, wird jeder MathJax Tag mit einer Lade-Callback Methode versehen. Die Callback Methode zählt einen globalen Lade-Counter hoch. Entspricht der Wert des Lade-Counters der Anzahl aller MathJax Elementen, signalisiert dies, dass alle mathematischen Elemente geladen sind.

4. **Loading:** Das finale JSX-Element wird an die PageView Komponente übergeben, die das Anzeigen der verschiedenen Seiten verwaltet.

Die PageView Komponente zeigt während des Ladevorgangs einen Lade-Spinner und einen kurzen Text an. Sobald der Lade-Counter aus Schritt drei der Anzahl der mathematischen Elemente entspricht und die Seite somit geladen ist, wird das JSX Element gerendert und der Lade-Spinner demontiert.

4.5 Visuelle Gestaltung der Oberfläche

Innerhalb dieses Kapitels wird das gewählte Designkonzept näher beschrieben. Dabei wird zum einen auf die Komponenten eingegangen, zum anderen wird das Farbschema erläutert. Hierfür wurden grundlegende Designprinzipien angewandt.

4.5.1 Farbschema

Um ein Design zu erstellen wird zunächst eine Farbpalette definiert, welche in Abbildung 4.4 dargestellt wird.

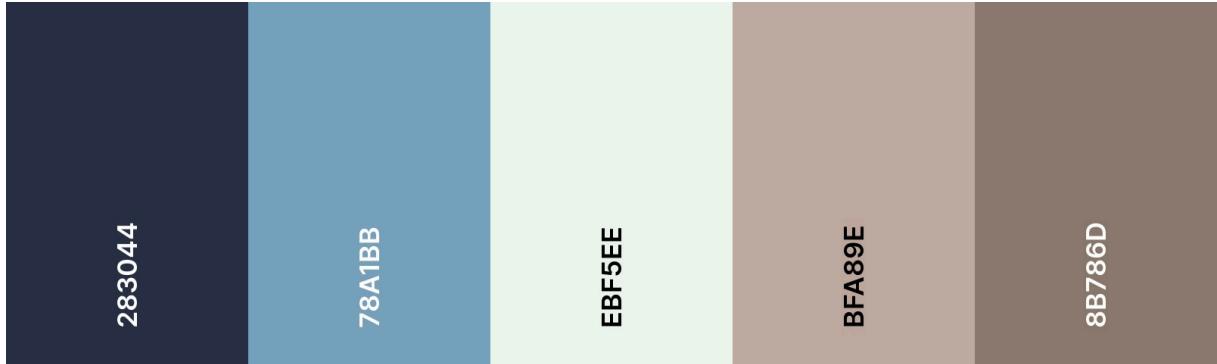


Abb. 4.4: Farbschema

Auf dem Bild sind zum einen die Farben sowie die zugehörigen Hex-Werte dargestellt. Das Design besteht aus zwei Braun- und zwei Blautönen. Ebenfalls wird ein Weißton verwendet. Dabei lassen sich die Farben mit der Farbbedeutung weiter erläutern.

Die Farbe blau wird in den europäischen Ländern vor allem mit Zuverlässigkeit, Technik und Weisheit verbunden, wohingegen weiß für Vertrauen und Modernität steht. Unter der Farbe braun wird ebenfalls mit Zuverlässigkeit verbunden, sowie mit einer Bodenständigkeit und Ruhe.

Die Farbe blau steht in dieser Anwendung vor allem für die technischen Inhalte, die vermittelt werden und das Wissen, welches erlangt wird. Der Weißton hingegen porträtiert die Modernität der Applikation und soll Vertrauen in die Applikation stärken. Braun steht hingegen für die Ruhe beim Lernen.

Gesamtheitlich soll das Design schlicht und wenig ablenkend gestaltet werden. Hierdurch werden die Lernenden nicht abgelenkt, wodurch eine angenehme Lernatmosphäre geschaffen wird. Ebenfalls können sich die Lernenden hierdurch auf das Wichtigste, die Inhalte, konzentrieren.

4.5.2 Seitenaufbau und Komponenten

Der Seitenaufbau setzt sich aus verschiedenen Komponenten zusammen. Drei wesentliche Bestandteile, die sich ebenfalls auf jeder Unterseite wiederfinden, sind die Navigationsleiste, die Fortschrittsanzeige und der Hilfe-Chat. In Abbildung 4.5 sind diese Komponenten zu sehen.



Abb. 4.5: Abbildung der Standardkomponenten

Dabei umfasst die Navigationsleiste mehrere Inhalte. Zum einen wird das Logo der Bildungsplattform links in Kombination mit dem Namen dargestellt. Weiterhin folgt darauf ein Drop-Down Menü, welches eine Kapitelübersicht bietet. Hierdurch kann der Nutzer zwischen den Inhalten wechseln. Rechts kann durch Icons zum einen zu einer Hilfe Seite mit Bedienungsanweisung und zu den Einstellungen navigiert werden. Die Navigationsleiste wird mit einem dunklen Blauton aus der bestehenden Farbpalette eingefärbt. Hierdurch hebt sich von der sonst hellen Seite ab, wirkt jedoch nicht ablenkend auf den Nutzer, da sie sonst schlicht gestaltet ist.

Die Fortschrittsanzeige wird im selben Blauton der Farbpalette eingefärbt. Sie befindet sich wahlweise rechts unter der Navigationsleiste oder unter dem Inhalt eines Kapitels. Hierdurch kann der Nutzende durchgehend seinen Fortschritt überwachen.

Der Hilfschat kann eingesehen werden, wenn der Nutzende einen gültigen OpenAI API Key innerhalb der Einstellungen eingibt. Er wird bei jeder Kapitelseite in der rechten unteren Ecke der Seite angezeigt. Abbildung 4.6 stellt das Feld zum Öffnen des Chats dar.



Abb. 4.6: Abbildung des Endpoints für den Hilfschat

Durch die hellblaue Farbe hebt sich der Chat vom weißen Hintergrund ab und kann somit leicht entdeckt werden. Wird der Button gedrückt, öffnet sich ein Chatfenster in dem der Nutzende seine Fragen stellen kann. Diese werden im Folgenden von der künstlichen Intelligenz beantwortet. Abbildung 4.7 zeigt das Chatfenster.

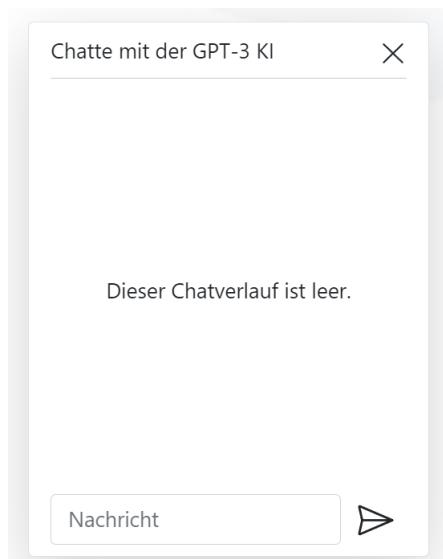


Abb. 4.7: Abbildung des Chatfensters

Der Chat erinnert dabei an einen typischen Messenger. Der Nutzende kann in das Textfeld seine Nachricht eingeben und mittels des Pfeil-Icons die Nachricht absenden. Das Design ist dabei in Weiß gewählt, während die eigenen Chat-Nachrichten in blau dargestellt sind. Die Chatnachrichten der künstlichen Intelligenz grau eingefärbt sind. Hierdurch entsteht eine klare Abhebung der Nachrichten, wodurch der Nutzende die eigenen Nachrichten von den anderen unterscheiden kann.

Für den Hintergrund wurde ein unauffälliges Design gewählt. Es kann in Abbildung 4.8 eingesehen werden.



Abb. 4.8: Hintergrundbild

Ziel war es, einen Hintergrund zu erstellen, der zum einen das Thema Quanten repräsentiert, zum anderen den Nutzer jedoch nicht beim Lernen ablenkt. Dabei wurde das Design als zwei Atome in der Orbitalmodelldarstellung. Diese wurden in einem Grauton eingefärbt und die Sättigung und sowie die Durchsichtigkeit reduziert.

Die Themen werden in der Übersicht mit Hilfe von Icons dargestellt. Es wurde diese Form des Designs gewählt, da Icons den Benutzenden bereits vom Smartphone oder Tablet bekannt ist. Durch den Wiedererkennungseffekt soll die Bedienung für die Zielgruppe intuitiv möglich sein.

Um schnell zu erfassen, ob ein Kapitel abgeschlossen ist, wird zwischen zwei Icontypen unterschieden. Zum einen wird ein braunes Design, zum anderen ein blaues Design zur Verfügung gestellt. Das braune Design steht hierbei für nicht abgeschlossene Lktionen, während das Blaue für abgeschlossene steht. Hierdurch kann der Nutzende auf den ersten Blick die noch zu bearbeitenden Inhalte erkennen.

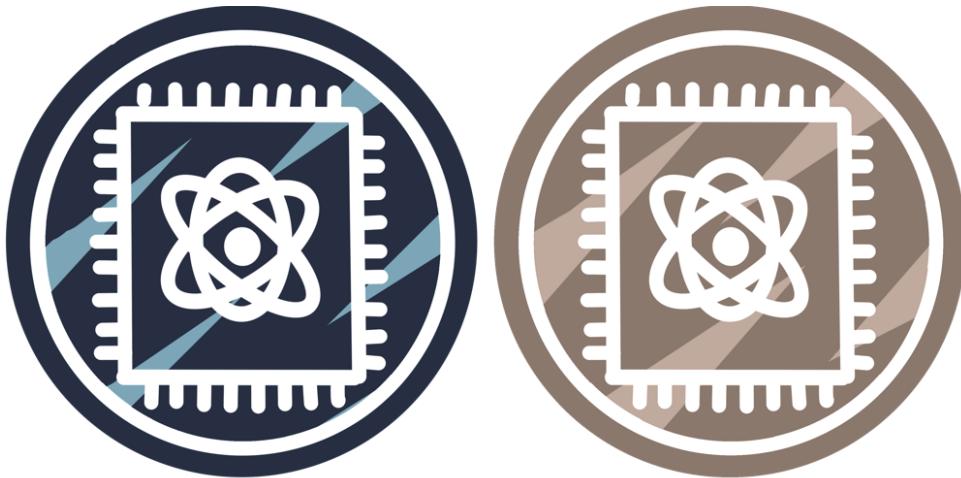


Abb. 4.9: Icon für das Kapitel Quantencomputing

Abbildung 4.9 stellt beispielhaft das fertige Icondesign für das Kapitel Quantencomputing dar. Alle übrigen Icondesigns können dem Anhang A.4 entnommen werden.

Um dem Nutzer den Inhalt leichter verständlich zu machen, welcher sich hinter dem jeweiligen Icon befindet, wird unter dem Icon die Überschrift des Kapitels ergänzt. durch das Prinzip der Nähe kann der Nutzer die jeweilige Überschrift dem entsprechenden Icon zuordnen.

Ebenfalls wird für jedes bereits bestehende Kapitel ein eigenes Icon erstellt. Werden neue Kapitel hinzugefügt, kann entweder ein neues Icon erstellt werden oder es wird ein vorgefertigtes Default-Icon geladen.

4.6 Lernelemente

Unter dem Kapitel Lernelemente werden die verschiedenen Kreativelemente betrachtet, die den Lernerfolg sicherstellen.

4.6.1 Grafiken und Videos

Bilder und Videos werden mit dem Latex-Parser, welcher in Kapitel 4.4 beschrieben wurde, eingebunden. Hierfür muss ein Bild oder ein Video in den jeweiligen Content-Ordner eingefügt und mit Latex eingebunden werden.

Dies bietet die Möglichkeit der Visualisierung und der Einbindung von anderen Wissensquellen, welche nicht zwangsläufig selbst erstellt wurden.

4.6.2 Simulationen

Ein weiteres Lernelement sind die Simulationselemente. Diese werden im Folgenden vorgestellt.

Bloch-Kugel Simulation

Die Simulation der Bloch-Kugel erfolgt mittels Three.js im 3D-Raum. Der Nutzer kann diese aus jedem Winkel betrachten, wobei sein Blick immer zentral auf die Bloch-Kugel gerichtet ist. Abbildung 4.10 zeigt die Simulation innerhalb der Anwendung.

Visualisierung eines Qubit Zustands

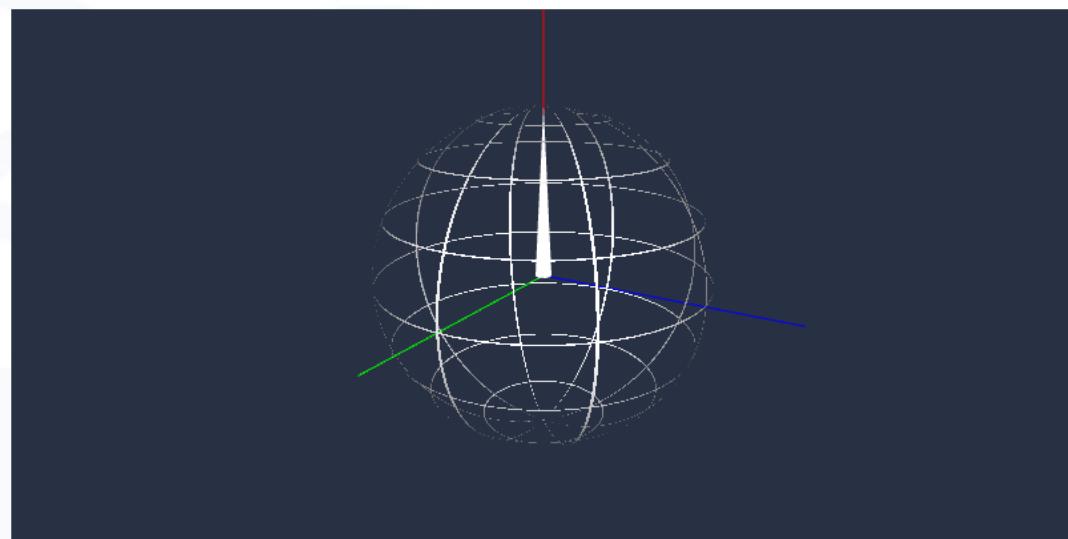


Abb. 4.10: Simulation einer Blochsphäre

Der Nutzende kann durch verschiedene Buttons, die ebenfalls in der Darstellung gezeigt sind, den Zustand des Qubits mittels verschiedener Quantengatter verändern und erhält hierzu eine visuelle Simulation. Diese Gatter sind die X,Y,Z und das $X^{1/2}$ Gatter.

Quantenschaltungen

Die Quantenschaltungen werden im Rahmen eines LaTeX-Elements mithilfe der Q.js Bibliothek realisiert. Für das selbstständige Definieren einer Quantenschaltung wird eine Skriptdatei benötigt, die in der LaTeX-Seite referenziert wird.

Innerhalb der Skriptdatei kann die Schaltung mit einem bestimmten Syntax aufgebaut werden. Für den Deutsch-Josza Algorithmus sieht der Inhalt der Skriptdatei wie folgt aus:

```
var circuit1 = Q'
    H-I-X0-I—I-H
    H—I—I—X0—I-H
    X-H-X1-X1-H-X'
```

Die Quantenschaltung wird als interaktives Element gerendert. In der LaTeX Datei kann festgelegt werden, ob der Nutzer die Schaltung verändern kann oder ob diese statisch bleibt.

Neben der Quantenschaltung werden die Messergebnisse der aktuellen Schaltung in Form eines Balkendiagramms dargestellt. Die Messergebnisse reagieren dynamisch auf Veränderungen der Quantenschaltung.

Beispiel: Deutsch-Jozsa Algorithmus

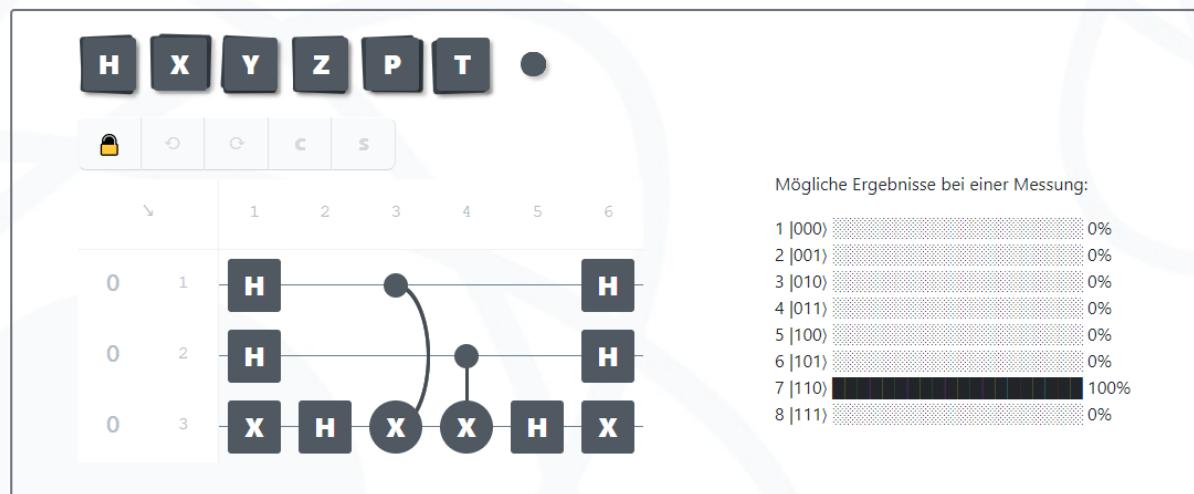


Abb. 4.11: Deutsch-Jozsa Algorithmus Schaltung

BB84-Protokoll

Die Simulation des BB84 Protokolls basiert auf einer interaktiven Demo mit Eingaben durch den Benutzer. Hierbei werden zwei Versionen bereitgestellt. Eine mit und eine ohne

Angreifer. Die Simulation wurde mit HTML und JavaScript umgesetzt.

Der Nutzer gibt die zu sendenden Bits und die von Alice gewählten Basen ein. Hieraus ergeben sich Alice Qubits. Daraufhin können die von Bob gewählten Basen eingegeben. Im unteren Teil der Simulation wird dargestellt, welche Basen von Alice und Bob dieselben waren, woraus sich der Schlüssel ergibt. Dabei kann der Nutzende die Basen und die Bits beliebig anpassen. Abbildung 4.12 zeigt die Errechnung des gemeinsamen Schlüssels zur Kommunikation innerhalb der Simulation.

	Alice's Basen	Bob's Basen	
5.	XZXZXXZZXZXXZ	ZZXZXXZXXZXZXX	
6.	Alice's Basen: X Z X Z X X Z Z X Z X X Z X Bob's Basen: Z Z X Z X X Z X X Z Z X X Z X Index: 1 2 3 4 5 6 7 8 9 10 11 12 13 14	X	Alice's Basen: X Z X Z X X Z Z X Z X X Z X Bob's Basen: Z Z X Z X X Z X X Z X Z X X Z X Index: 1 2 3 4 5 6 7 8 9 10 11 12 13 14
7.	Index: 2 3 4 5 6 7 9 10 11 14 Alice's Input: 0 1 1 1 1 0 0 1 1 1 1 0 1 0 Schlüssel: 1 1 1 1 0 0 1 1 1 1 0	X	Index: 2 3 4 5 6 7 9 10 11 14 Bob's Messung: 1 1 1 1 1 0 0 0 1 1 1 1 0 0 Schlüssel: 1 1 1 1 0 0 1 1 1 1 0

Abb. 4.12: Schlüsselgenerierung BB84 Simulation

Die Simulation mit einem Angreifer gleicht der ohne Angreifer, jedoch wird diese durch die frei wählbaren Basen von Eve ergänzt. Die Kommunikationspartner erkennen den Angriff im Basenvergleich, was ebenfalls grafisch dargestellt wird. Dies kann in Abbildung 4.13 eingesehen werden.

	Alice's Basen	Bob's Basen	
7.	XZXZXXZZXZXX	XXXXZXXZZZXZ	
8.	Alice's Basen: X Z X Z X X Z Z X Z X X Bob's Basen: Z X X X Z X X Z Z X Z X Index: 1 2 3 4 5 6 7 8 9 10 11 12	X	Alice's Basen: X Z X Z X X Z Z X Z X X Bob's Basen: Z X X X Z X X Z Z X Z X Index: 1 2 3 4 5 6 7 8 9 10 11 12
9.	Index: 3 6 8 12 Alice's Input: 0 1 1 1 1 0 0 1 1 1 1 0 Schlüssel: 1 0 1 0	X	Index: 3 6 8 12 Bob's Messung: 0 0 0 0 1 1 1 1 0 1 1 Schlüssel: 0 1 1 1

Abb. 4.13: Schlüsselgenerierung BB84 Simulation mit Angreifer

4.6.3 Übungen

Die Bildungsplattform bietet ebenfalls die Möglichkeit, Multiple Choice Übungen in ein Kapitel einzubinden. Abbildung 4.14 zeigt eine dieser Übungen aus der Bildungsplattform.

Frage: Bieten Quantencomputer immer Vorteile gegenüber klassischen Computersystemen?

- 1) Quantencomputer sind prinzipiell schneller als klassische Computersysteme.
- 2) Nein, Quantencomputer können gar nicht schneller als die heutigen Rechensysteme sein.
- 3) Das ist vom jeweiligen Anwendungsgebiet abhängig.

Abb. 4.14: Beispielübung

Wird dabei die falsche Antwort geklickt, wird der Text der Antwort rot gefärbt. Ist die Lösung richtig, wird dieser grün eingefärbt. So hat der Nutzende die Möglichkeit, seine Antwort nochmals zu überlegen und kann Verständnisprobleme nochmals speziell bearbeiten. Die Übungen können beliebig in die Latex-Seite eingebunden werden.

Abbildung 4.15 zeigt die Implementierung einer Aufgabe innerhalb der LaTeX-Datei mit dem Befehl `\exercise`.

```
\exercise[type=multipleChoice]{
    \question{Frage: Bieten Quantencomputer immer Vorteile gegenüber klassischen Computersystemen? }
    \possibleAnswers{
        \item 1) Quantencomputer sind prinzipiell schneller als klassische Computersysteme.
        \item 2) Nein, Quantencomputer können gar nicht schneller als die heutigen Rechensysteme sein.
        \item 3) Das ist vom jeweiligen Anwendungsgebiet abhängig.
    }
    \result{3}
```

Abb. 4.15: Beispielübung innerhalb der Kapitelsseite

4.7 Administration

Das Kapitel Administration umfasst die grundlegende lokale Installation der Anwendung. Ein weiteres Thema ist die Bearbeitung und das Hinzufügen von Inhalten auf der Plattform.

4.7.1 Lokales Setup

Im Folgenden wird beschrieben, wie die Webanwendung lokal installiert werden kann. Für die Weiterentwicklung ist die Nutzung des Entwicklungsservers (siehe Schritt 2) zu empfehlen. Für die Benutzung an sich kann der lokale Webserver XAMPP genutzt werden (siehe Schritt 3).

Schritt 1: Download des Webservers:

Für die lokale Nutzung wird der Apache Webserver von XAMPP¹ empfohlen. Bei der

¹XAMPP-Webseite: <https://www.apachefriends.org/de/download.html>

portablen Version von XAMPP ist keine Installation erforderlich. In diesem Fall muss das heruntergeladene Verzeichnis lediglich entpackt werden. Dabei muss auf die korrekte Wahl des Betriebssystems geachtet werden.

Der Quellcode und aktuelle Releases der Anwendung sind auf GitHub verfügbar.

Schritt 2: (optional) Anwendung selbst bauen:

Die Anwendung kann auch selbst kompiliert und lokal getestet werden. Diese Option ist insbesondere für Entwickler gedacht. Für diesen optionalen Schritt muss Node.js auf dem System installiert sein. Zunächst wird das Repository geklont und die Abhängigkeiten installiert.

```
git clone https://github.com/BaderTim/education-platform-for-quantum-cryptography.git  
cd education-platform-for-quantum-cryptography/webapp/  
npm install
```

Danach kann der Entwicklungserver lokal gestartet werden. Der Build wird mit dem Befehl `npm run build` gestartet. Die Dateien befinden sich nach Abschluss im Ordner `build`.

```
npm start  
npm run build
```

Schritt 3: Anwendung auf lokalem Webserver starten:

Microsoft Windows:

Falls der Build-Ordner heruntergeladen wurde, muss dieser ggf. entpackt werden. Der Inhalt des Build-Ordners muss dann in das XAMPP-Verzeichnis `xampp-portable-XXXXXX` kopiert werden. Bestehende Dateien im Verzeichnis sollten vorher gelöscht werden. Nun wird der Apache Webserver gestartet. Dies geschieht über das Skript `apache_start.bat`. Zum Beenden von Apache bzw. XAMPP muss das Skript `xampp_stop.exe` verwendet werden. Der aktuelle Status kann über das XAMPP-Dashboard `xampp-control.exe` überprüft werden. Die Anwendung kann dann im Browser lokal unter `http://localhost:80` aufgerufen werden.

Ubuntu:

Die folgenden Schritte basieren auf der Anleitung von `ubuntuusers`.²

Befehle zum Ausführen der Installation:

```
chmod 755 xampp-linux-VERSION-installer.run  
sudo ./xampp-linux-VERSION-installer.run
```

Falls der Build-Ordner heruntergeladen wurde, muss dieser ggf. entpackt werden. Der Inhalt des Build-Ordners muss dann in das XAMPP-Verzeichnis `/opt/lampp/htdocs/` kopiert werden. Bestehende Dateien im Verzeichnis sollten vorher gelöscht werden.

²XAMPP-ubuntuusers.de: <https://wiki.ubuntuusers.de/XAMPP/>

```
sudo /opt/lampp/lampp start
```

4.7.2 Erweiterbarkeit

Eine wesentliche Anforderung an die Plattform ist die Definition der Kapitel durch austauschbare Dateien, damit Inhalt und Formatierung geändert werden können, ohne in den Programmcode einzugreifen. Umgesetzt wird diese Funktionalität durch einen Parser, der den in der Datei gespeicherten Text einliest und die dort enthaltenen Befehle in die entsprechende Formatierung zur Anzeige auf der Webseite umwandelt. Die Kapitel werden automatisch anhand der IDs eingelesen und auf der Startseite angezeigt. Das Erstellen eines neuen Kapitel erfordert wenige, einfache Schritte.

Anlegen eines neuen Kapitels

Zunächst muss die Ordner- und Dateistruktur für das Kapitel wie folgt angelegt werden:

1. neuen Ordner (Seiten-ID als Ordnername) erstellen im Verzeichnis *public/pages/*
2. Unterordner *content* erstellen
3. Datei erstellen: *latex_page.tex*
4. Datei erstellen: *page.json*

Aufbau und Inhalt der Datei *page.json*:

Für den Schlüssel *id* wird die ID der Seite als Wert eingetragen. Diese muss fortlaufend und eindeutig sein. Für *title* wird der Seitentitel eingetragen.

In Abbildung 4.16 ist ein Beispiel für ein Kapitel mit der ID „1“ und dem Titel „Hallo Welt“ enthalten.

```
{  
  "id": 1,  
  "title": "Hallo Welt!"  
}
```

Abb. 4.16: Inhalt der Datei *page.json*

Aufbau und Inhalt der Datei *latex_page.tex*:

Innerhalb der *latex_page.tex* können die folgenden Befehle verwendet werden:

Beschreibung	Befehl
kursiver Text	<code>\textit{kursiv}</code>
fetter Text	<code>\textbf{fett}</code>
Überschrift 1	<code>\section{Überschrift}</code>
Überschrift 2	<code>\subsection{Überschrift}</code>
Überschrift 3	<code>\subsubsection{Überschrift}</code>
Horizontale Linie	<code>\hr</code>
Anführungszeichen	<code>\glqq Das ist ein Zitat\grqq</code>
Absatz einfügen	<code>\newline</code>
Link einfügen	<code>\hyperlink[url=https://www.dhbw.de/]{Webseite}</code>
Liste einfügen	<code>\list{\item erstens \item zweitens}</code>
Bild einfügen (.jpg/.png)	<code>\includegraphics[width=42]{content/DATEINAME.XYZ}</code>
Video einfügen (.mp4)	<code>\includegraphics[width=84]{content/DATEINAME.XYZ}</code>
Bildunterschrift	<code>\caption{Quantum Fourier Transformation Circuit}</code>
mathematische Formel	<code>\begin{equation}\begin{gathered} 1 + 1 = 2 \end{gathered}\end{equation}</code>

Tab. 4.1: Übersicht an Befehlen für *latex_page.tex*

Die Verwendung von weiteren Funktionen und Modulen wird auf der Infoseite innerhalb der Anwendung genau beschrieben.

5 Diskussion & Reflexion

Im Folgenden werden die Ergebnisse betrachtet und auf ihren Erfüllungsgrad der Anforderungen überprüft.

5.1 Evaluation der Ergebnisse

Die Inhalte der Bildungsplattform wurden auf Basis einer umfangreichen Literaturrecherche erstellt. Hierdurch wird die Qualität der Daten sichergestellt. Die Befragten interessierten sich für die Erklärung der Inhalte sowie die Erläuterung der Funktionsweise. Dies wurde innerhalb der Plattform erfüllt. Dabei umfassen die Inhalte sowohl Grundlagen zu Quanten, als auch dem Quantencomputing sowie dem BB84-Protokoll und dem Shor-Algorithmus.

Die Befragungen und das Brainstorming stellten die Basis für die Anforderungsanalyse dar. Hierdurch wird ein Bezug zu den Wünschen und Erwartungen der Stakeholder hergestellt. Diese spielten eine maßgebliche Rolle während der Entwicklung der Bildungsplattform. Hierdurch wird die Zufriedenheit der Stakeholder sichergestellt.

Die Anforderungen wurden dabei zu 95% erfüllt. Eine der Anforderungen wurden jedoch nicht umgesetzt. Der Nutzer die Applikation nicht personalisieren. Die restlichen Anforderungen wurden vollständig erfüllt.

Durch verschiedene Elemente wie interaktive Simulationen, Text, Grafiken, Videos und Aufgaben können visuelle, auditive und haptische Lerntypen angesprochen werden. Durch das ausschließliche Aufbauen auf mathematischen Grundlagen ermöglicht es den Nutzenden leicht in die Applikation einzusteigen. Hierdurch können diese auf bekanntem Vorwissen aufbauen und dieses miteinander verknüpfen.

5.2 Gewonnene Erkenntnisse

Innerhalb der Reflexion werden verschiedene Probleme, welche im Laufe der Arbeit aufgetreten sind, betrachtet und Maßnahmen für die Zukunft definiert, wie diese vermieden werden können.

Zum einen wurde im Verlauf der Arbeit der Titel, sowie die Grundidee verändert. Dabei ergaben sich verschiedene Anforderungen, welche durch ihre Masse schlussendlich nicht vollständig erfüllt wurden. Ebenfalls stellte der große Zeitraum ein Hindernis dar, da regelmäßige Absprachen mit dem Auftraggeber sich schwierig gestalteten. In Zukunft bedarf es einer besseren Projekt- sowie Meilensteinplanung.

Weiterhin wurden zu viele Kann-Anforderungen vom Projektteam definiert, wobei der Fokus auf die Kernelemente verloren ging. Diese lassen sich jedoch zukünftig ergänzen.

Hierbei muss in Zukunft ein Versionierungsplan erstellt werden, wobei der Release der einzelnen Funktionen genau definiert wird.

6 Fazit & Ausblick

Im folgenden Kapitel werden die Ergebnisse zusammengefasst und aufgezeigt, welche Themen für eine mögliche Weiterentwicklung relevant sind.

6.1 Ergebnisse

Im Rahmen der Studienarbeit wurde eine Plattform entwickelt, die wesentliche Inhalte aus dem Gebiet der Quantenkryptografie für verschiedene Lerntypen anschaulich und interaktiv darstellt. Diese basiert auf dem Framework React und ist eine reine Frontend-entwicklung, welche Cookies zum Speichern des Fortschritts verwendet.

Es ist die Möglichkeit gegeben, die Kapitelinhalte zu erweitern und dabei die verfügbaren interaktiven Module individuell einzusetzen. Durch die Befragung der Zielgruppe und der Abstimmung mit den Stakeholdern ist es gelungen eine performante Anwendung zu entwerfen, die durch die Vielzahl an Funktionen einen guten Einstieg in die Thematik bietet. Aufgrund der Komplexität der Themen war es nicht möglich Simulationen und Visualisierungen für alle Themenbereiche zu entwickeln. In diesen Fällen wurde auf andere effektive Lernelemente, wie beispielsweise Grafiken und Videos zurückgegriffen.

Durch eins schlichtes und modernes Design bietet die Applikation eine gute und strukturierte Lernumgebung. Mittels des Icondesigns, welches von Smartphones inspiriert ist, findet sich der Nutzende leicht in den Kapiteln zurecht.

Schlussendlich kann ein OpenAi Key in den Einstellungen eingegeben werden. Die künstliche Intelligenz kann mittels des Chats angeschrieben werden und beantwortet inhaltliche Fragen.

6.2 Entwicklungsmöglichkeiten

Es gibt verschiedene Bereiche, die für die Weiterentwicklung des Projekts eine Rolle spielen. Um die technische Entwicklung effizienter zu gestalten, sollte eine Teststrategie entwickelt werden, die auch Unit-Tests umfasst. Ebenfalls können Individualisierungsmöglichkeiten ergänzt werden.

Im Hinblick auf die Übungsaufgaben ist es denkbar, diese sowohl inhaltlich als auch technisch zu erweitern. Dazu gehört auch die Speicherung und Auswertung der Antworten analog zur bereits implementierten Speicherung des Fortschritts. Weiterhin können Tests eingefügt werden, bei denen der Nutzende sein Wissen kapitelübergreifend überprüfen kann.

Auch ist es denkbar, weitere Simulationen oder Inhalte einzuführen, sodass noch mehr Lerninhalt vermittelt werden kann.

Eine weitere Funktionalität könnte ein Tagesstreak sein, also das Zählen der Tage, an denen gelernt wurde. Hierdurch können die Nutzer motiviert werden, regelmäßig Inhalte zu

erarbeiten. Zuletzt kann ein Lernlevel beziehungsweise eine Erfahrungspunktesammlung ergänzt werden, die den Nutzer durch Belohnungen bei Levelaufstieg motivieren.

A Anhang

A.1 Interview

Interview mit Auftraggeber Prof. Dr. Jürgen Schneider

Thema: Entwicklung einer Bildungsplattform für Quantenkryptografie

Inhalt

F1: Auf welche inhaltlichen Themen legen Sie besonders großen Wert?

A1:

Der Schwerpunkt soll auf Kryptografie liegen, es soll Quantencomputing visualisiert und Quantenbits sichtbar gemacht werden. Die Zielgruppe besteht aus Studenten.

F2: Wie tiefgründig sollen die Themen behandelt werden?

A2:

Verständlichkeit muss gegeben sein, es müssen keine quantentheoretischen Gleichungen gelöst werden, aber die Komplexität soll verständlich gemacht werden.

Es ist ausreichend Grundprinzipien zu zeigen, es muss nicht selbst entworfen bzw. gerechnet werden. Zusätzlich soll deutlich werden, was Einsatzszenarien für Quantenkryptografie sind und warum diese verwendet wird.

F3: Sollen Grundlagen mit aufgegriffen werden? Wenn ja, welche und in welchem Ausmaß?

A3:

Mathematische Grundlagen, die keinen direkten Zusammenhang zum Thema haben, sollen nicht wiederholt werden. Der Fokus soll auf Quantenbits und Quantenalgorithmen liegen.

F4: Sollen Übungen eingebaut werden? Wenn ja, wann und in welchem Stil?

A4:

Der Fokus soll auf der Demonstration liegen, Entschlüsselung und Verschlüsselung simulieren und lebhaft machen, Zeitgefühl soll geschaffen werden. Verständnisfragen und Übungen können zur Ergänzung verwendet werden.

Technische Umsetzung

F5: Was eine Art von Anwendung soll die Bildungsplattform werden?

A5:

(Lokale) Webanwendung

F6: Wie performant soll die Anwendung werden?

A6:

Die Anwendung soll Ladezeiten von einer Sekunde pro Ladevorgang nicht überschreiten.

F7: Auf welchen Geräten soll die Anwendung ausführbar sein?

A7:

Auf Desktop Computern, bzw. auch auf virtuellen Maschinen unter Linux.

F8: Wie stellen Sie sich die technische Umsetzung vor? Was sind Ihre Ansprüche an das Design der Anwendung?

A8:

Für die technische Umsetzung gibt es keine konkrete Vorgabe, es wird Wert auf Eigenständigkeit und Eigenleistung gelegt. Das React.js Framework oder ein vergleichbares wäre geeignet.

Für das Design des Userinterface ist die grafische Bedienbarkeit und eine flüssige Performance wichtig.

Sonstiges

F10: Würden Sie als lehrender Professor die Anwendung in Ihren Vorlesungen verwenden? Wenn ja, wie und unter welchen Umständen?

A10:

Ja, wenn die Anforderungen erfüllt wurden, um das Thema innerhalb von Vorlesungen transparent und anschaulich zu vermitteln.

F11: Was wären absolute No-Gos für Sie?

A11:

Schlechte Stabilität oder geringe Performance der Anwendung.

F12: Haben Sie sonstige Anmerkungen oder konkrete Anforderungen, die bis jetzt unerwähnt geblieben sind?

A12:

Frühzeitige Tests eines Prototyps im Informatik Labor. Möglichkeiten zur Personalisierung: Schriftgröße, Zoom, nutzbar trotz unterschiedlicher Bildschirmgrößen

A.2 Umfrageformular

Umfrage zu einer Lernplattform über Quantum Kryptografie

Hey Du!

Unser Team bestehend aus Xena Letters, Daniel Erhard und Tim Bader ist auf Deine Meinung angewiesen! Wir entwickeln eine Bildungsplattform zum Thema Quantum Kryptografie und würden gerne Deine kurze Einschätzungen zu den folgenden Fragen haben, es wird auch gar kein Vorwissen benötigt.

* Erforderlich

1. Wo studierst Du? *

Markieren Sie nur ein Oval.

- An einer Hochschule
 An einer Universität

2. In welchem Semester befindest Du dich aktuell? *

Markieren Sie nur ein Oval.

- 1
 2
 3
 4
 5
 6

3. Welchen Studiengang belegst Du? *

Theorie des Lernens

4. Wie würdest Du Dich selbst einschätzen? *

Wählen Sie alle zutreffenden Antworten aus.

- Der/Die Kreative - Das Fühlen und Wahrnehmen von konkreten Erfahrungen steht im Vordergrund.
 Forscher*in - Die Stärke liegt in der Anwendung von Logik und theoretischen Modellen.
 Ingenieur*in - Arbeitet auch mit Modellen, legt aber mehr Wert auf aktives Experimentieren.
 Macher*in - Führt Experimente durch und legt gleichzeitig Wert auf praktische Erfahrungen.

Sonstiges:

5. Unter welchen Umständen lernst Du besser? Bei welchen eher weniger? *

Ich lerne besser, wenn ich....

Markieren Sie nur ein Oval pro Zeile.

	Trifft zu	Eher ja	Weiß nicht	Eher nein	Trifft nicht zu
...den Nutzen der Inhalte erkenne.	<input type="checkbox"/>				
...den Inhalt mit Vorwissen verknüpfen kann.	<input type="checkbox"/>				
...regelmäßig Pausen einlege.	<input type="checkbox"/>				
...mir konkrete Lernziele setze.	<input type="checkbox"/>				
...mich regelmäßig selbst belohne.	<input type="checkbox"/>				

6. *Markieren Sie nur ein Oval.* Option 1

Inhalt

7. Wie sehr interessierst Du dich für Quantentechnik, insbesondere Quantenkryptografie? *

Markieren Sie nur ein Oval.

1 2 3 4 5

gar nicht sehr stark

8. Wie viel Vorwissen hast Du im Bereich des Quantum Computings bzw. der Quantenkryptografie? *

Markieren Sie nur ein Oval.

1 2 3 4 5 6 7 8 9 10

keine Ahnung ich weiß wie der Shor Algorithmus funktioniert

9. Wie viel Vorwissen hast Du im Bereich der klassischen Kryptografie? *

Markieren Sie nur ein Oval.

1 2 3 4 5 6 7 8 9 10

keine Ahnung ich weiß wie RSA, PGP und asymmetrische Verschlüsselung funktioniert

10. Wie tiefgründig sollen die Themen behandelt werden? *

Markieren Sie nur ein Oval. Die Funktion von Inhalten erklären (Wie?) Funktion von Inhalten und deren Aufbau erklären (Wie? Warum?) Funktion von Inhalten, deren Aufbau und wie diese hergeleitet wurde erklären (Wie? Warum? Woher?)

11. Sind kurze Übungen eine gute Idee? *

Markieren Sie nur ein Oval.

- Nein
- Ja, aber nur am Ende eines Kapitels
- Ja, auch gerne zwischendurch

Anforderungen

12. Welche Design Elemente könntest Du Dir zum Erlernen komplexer Themen als hilfreich erachten? *

Markieren Sie nur ein Oval pro Zeile.

	sehr hilfreich	hilfreich	weiß nicht	eher nicht	gar nicht
Textuelle Beschreibung des Themas	<input type="radio"/>				
Grafiken, die Themen oder Abläufe darstellen	<input type="radio"/>				
GIF/Animation zur Darstellung eines Prozessablaufs	<input type="radio"/>				
Audio / Erläuterungen / Vorlesen von Text	<input type="radio"/>				
Erklärvideos	<input type="radio"/>				
Eine nutzungsfreundliche Simulation, in der man die Lerninhalte (spielerisch) in einer 3D Welt wahrnehmen kann	<input type="radio"/>				
Kleine eingebaute Anwendungen, in denen Themen schnell selbst ausprobiert werden können	<input type="radio"/>				

13. Wie würdest Du die Leistung deines PCs/Laptops einschätzen?

Markieren Sie nur ein Oval.

1 2 3 4 5

Unter dem Durchschnitt Über dem Durchschnitt

14. Hast du eine spezielle Anforderung an die Lernplattform?

Dieser Inhalt wurde nicht von Google erstellt und wird von Google auch nicht unterstützt.

Google Formulare

A.3 Anforderungsliste

ID	Name	Priorität	Klasse	Aufwan-d	Anforderungs-faktor	Dringlich-keit	Volatil-ität	Risiko	Stakeholder-Interesse	Kurzbeschreibung	Begründung
1	Statistische Webanwendung	9	Software	2	Basisfaktor	8	1	niedrig	10	Die Applikation muss eine statische Webanwendung sein, die auch lokal ausgeführt werden kann.	Interview
2	React.js Framework Grundlage oder vergleichbares	8	Software	4	Basisfaktor	10	2	niedrig	6	Die Applikation soll React oder vergleichbare Frameworks nutzen.	Interview
3	Darstellung auf Desktop Computern	6	Design	6	Basisfaktor	0	3	niedrig	10	Das Design der Applikation muss auf Desktop PCs nutzbar sein.	Interview
4	Browser: Chrome	10	Software	2	Basisfaktor	10	0	niedrig	10	Die Applikation muss aktuelle Chrome Versionen für Windows und Linux unterstützen.	Interview --> lauffähiger Prototyp für Labor, linux vm
5	Personalierungsmöglic-hkeiten	4	Software	5	Begeisterungsfak-tor	2	5	mittel	6	Die Applikation muss Möglichkeiten zur Personalisierung von Schriftgröße und Zoom bieten	Interview
6	IT Security Inhalte	7	Inhalt	7	Basisfaktor	4	2	niedrig	10	Die Applikation muss IT Security Inhalte wie Demonstration von Entschlüsselung und Verschlüsselung haben.	Interview
7	Kreativelemente	6	Inhalt	9	Leistungsfaktor	8	5	niedrig	6	Die Applikation soll Elemente zur kreativen Einbindung von Inhalten besitzen, wie z.B. visuell, interaktiv, textuell und ggf. auditiv, um verschiedene Lerntypen anzusprechen.	Interview Resultat
8	Übungen	4	Inhalt	4	Begeisterungsfak-tor	2	3	niedrig	4	Die Applikation soll Übungen am Ende der Kapitel und auch zwischendrin beinhalten	Interview
9	Strukturierung des Inhalts	6	Inhalt	7	Leistungsfaktor	4	3	niedrig	7	Die Inhalte der Applikation müssen mittels Kapitel oder eines Learning Paths strukturiert sein.	Interview Resultat
10	Speicherung des Fortschritts	6	Software	3	Leistungsfaktor	2	0	niedrig	5	Der Fortschritt innerhalb der Anwendung soll lokal gespeichert werden können.	Interview Resultat
11	Quantenbits und Quantenalgorithmen Inhalte	6	Inhalt	8	Basisfaktor	4	4	niedrig	8	Die Applikation muss Inhalte über Quantenbits und Quantenalgorithmen (BB84 und Shor) haben.	Interview

Abb. A.1: Anforderungen Teil 1

ID	Name	Priorität	Klasse	Aufwand d	Anforderungs-faktor	Dringlich-keit	Volatil-tät	Risiko	Stakeholder-Interesse	Kurzbeschreibung	Begründung
11	Quantenbits und Quantenalgorithmen Inhalte	6	Inhalt	8	Basisfaktor	4	4	niedrig	8	Die Applikation muss Inhalte über Quantenbits und Quantenalgorithmen (BB84 und Shor) haben.	Interview
12	Dynamisches Roadmap Menü	6	Software	0	Leistungsfaktor	7	2	niedrig	4	Die Kapitel der Applikation sollen dynamisch auf einer Roadmap aufgezeigt werden.	Interview Resultat
13	2D Grafiken	6	Design	6	Basisfaktor	3	2	niedrig	7	Die Applikation soll 2D Grafiken zur Verschönerung des Designs haben.	Interview Resultat
14	Intro	5	Inhalt	4	Begeisterungsfaktor	2	1	mittel	3	Die Applikation soll ein Erklärtutorial der Applikation als Intro für Erstbesucher haben.	Begeisterung
15	OpenAI Chat Roboter	5	Software	4	Begeisterungsfaktor	3	3	hoch	4	Die Applikation soll ein Hilfe Chatfenster haben, das an eine AI wie OpenAI angeschlossen ist.	Begeisterung
16	Kapitel durch MARKDOWN definiert	8	Software	6	Begeisterungsfaktor	8	2	mittel	7	Die Applikation muss die Seiteninhalte über Markdown Dateien laden.	Einfach erweiterbar
17	Hintergrundbild für Roadmap	6	Design	6	Basisfaktor	6	2	niedrig	5	Die Roadmap muss einen thematisch passenden Hintergrund haben.	Erster Eindruck UX
18	Kapitelbearbeitung	6	Design	3	Leistungsfaktor	6	2	niedrig	5	Die Kapitelpunkte auf der Roadmap sollen visuell aufbereitet sein.	Erster Eindruck UX
19	einheitliches Design	6	Design	6	Basisfaktor	4	2	niedrig	3	Das Design der Applikation muss einheitlich sein und einem Farbkonzept entsprechen.	Erster Eindruck UX
20	Roadmap mit Icons	6	Software	4	Leistungsfaktor	6	2	mittel	3	Die Kapitelpunkte auf der Roadmap sollen mit Icons dynamisch auf der Startseite angezeigt werden.	Erster Eindruck UX
21	Zurücksetzen der Daten	6	Software	2	Basisfaktor	2	0	niedrig	5	Die gesammelten Fortschritts- und Einstellungsdaten müssen zurückgesetzt werden können.	UX

Abb. A.2: Anforderungen Teil 2

A.4 Icons



Abb. A.3: Kapitel-Icons

Literatur

- [Alonso u. a. 2017] ALONSO, Gardenia ; BLUMENTRITT, Marianne ; OLDEROG, Torsen ; SCHWESIG, Roland: *Strategien für den Lernerfolg berufstätiger Studierender - Empirische Analysen zum Lernverhalten.* Berlin Heidelberg New York : Springer-Verlag, 2017. – ISBN 978-3-658-17530-6
- [ANIS u. a. 2021] ANIS, MD S. ; ABRAHAM, Héctor ; ADUOFFEI ; AGARWAL, Rochisha ; AGLIARDI, Gabriele ; AHARONI, Merav ; AKHALWAYA, Ismail Y. ; ALEKSANDROWICZ, Gadi ; ALEXANDER, Thomas ; AMY, Matthew ; ANAGOLUM, Sashwat ; ARBEL, Eli ; ASFAW, Abraham ; ATHALYE, Anish ; AVKHADIEV, Artur ; AZAUSTRE, Carlos ; BHOLE, PRATHAMESH ; BANERJEE, Abhik ; BANERJEE, Santanu ; BANG, Will ; BANSAL, Aman ; BARKOUTSOS, Panagiotis ; BARNAWAL, Ashish ; BARRON, George ; BARRON, George S. ; BELLO, Luciano ; BEN-HAIM, Yael ; BENNETT, M. C. ; BEVENIUS, Daniel ; BHATNAGAR, Dhruv ; BHOBE, Arjun ; BIANCHINI, Paolo ; BISHOP, Lev S. ; BLANK, Carsten ; BOLOS, Sorin ; BOPARDIKAR, Soham ; BOSCH, Samuel ; BRANDHOFER, Sebastian ; BRANDON ; BRAVYI, Sergey ; BRONN, Nick ; BRYCE-FULLER ; BUCHER, David ; BUROV, Artemiy ; CABRERA, Fran ; CALPIN, Padraig ; CAPELLUTO, Lauren ; CARBALLO, Jorge ; CARRASCAL, Ginés ; CARRIKER, Adam ; CARVALHO, Ivan ; CHEN, Adrian ; CHEN, Chun-Fu ; CHEN, Edward ; CHEN, Jielun (. ; CHEN, Richard ; CHEVALLIER, Franck ; CHINDA, Kartik ; CHOLARAJAN, Rathish ; CHOW, Jerry M. ; CHURCHILL, Spencer ; CISTERMOKE ; CLAUS, Christian ; CLAUSS, Christian ; CLOTHIER, Caleb ; COCKING, Romilly ; COCUZZO, Ryan ; CONNOR, Jordan ; CORREA, Filipe ; CROSS, Abigail J. ; CROSS, Andrew W. ; CROSS, Simon ; CRUZ-BENITO, Juan ; CULVER, Chris ; CÓRCOLES-GONZALES, Antonio D. ; D, Navaneeth ; DAGUE, Sean ; DANDACHI, Tareq E. ; DANGWAL, Animesh N. ; DANIEL, Jonathan ; DANIELS, Marcus ; DARTAILH, Matthieu ; DAVILA, Abdón R. ; DEBOUNI, Faisal ; DEKUSAR, Anton ; DESHMUKH, Amol ; DESHPANDE, Mohit ; DING, Delton ; DOI, Jun ; DOW, Eli M. ; DRECHSLER, Eric ; DUMITRESCU, Eugene ; DUMON, Karel ; DURAN, Ivan ; EL-SAFTY, Kareem ; EASTMAN, Eric ; EBERLE, Grant ; EBRAHIMI, Amir ; EENDEBAK, Pieter ; EGGER, Daniel ; ELEPT ; EMILIO ; ESPIRICUETA, Alberto ; EVERITT, Mark ; FACOETTI, Davide ; FARIDA ; FERNÁNDEZ, Paco M. ; FERRACIN, Samuele ; FERRARI, Davide ; FERRERA, Axel H. ; FOUILLAND, Romain ; FRISCH, Albert ; FUHRER, Andreas ; FULLER, Bryce ; GEORGE, MELVIN ; GACON, Julien ; GAGO, Borja G. ; GAMBELLA, Claudio ; GAMBETTA, Jay M. ; GAMMANPILA, Adhisha ; GARCIA, Luis ; GARG, Tanya ; GARION, Shelly ; GARRISON, Jim ; GATES, Tim ; GIL, Leron ; GILLIAM, Austin ; GIRIDHARAN, Aditya ; GOMEZ-MOSQUERA, Juan ; GONZALO ; PUENTE GONZÁLEZ, Salvador de la ; GORZINSKI, Jesse ; GOULD, Ian ; GREENBERG, Donny ; GRINKO, Dmitry ; GUAN, Wen ; GUIJO, Dani ; GUN-

NELS, John A. ; GUPTA, Harshit ; GUPTA, Naman ; GÜNTHER, Jakob M. ; HAGLUND, Mikael ; HAIDE, Isabel ; HAMAMURA, Ikko ; HAMIDO, Omar C. ; HARKINS, Frank ; HARTMAN, Kevin ; HASAN, Areeq ; HAVLICEK, Vojtech ; HELLMERS, Joe ; HEROŁ, Łukasz ; HILLMICH, Stefan ; HORII, Hiroshi ; HOWINGTON, Connor ; HU, Shaohan ; HU, Wei ; HUANG, Junye ; HUISMAN, Rolf ; IMAI, Haruki ; IMAMICHI, Takashi ; ISHIZAKI, Kazuaki ; ISHWOR ; ITEN, Raban ; ITOKO, Toshinari ; IVRII, Alexander ; JAVADI, Ali ; JAVADI-ABHARI, Ali ; JAVED, Wahaj ; JIANHUA, Qian ; JIVRAJANI, Madhav ; JOHNS, Kiran ; JOHNSTUN, Scott ; JONATHAN-SHOEMAKER ; JOSDENMARK ; JOSH-DUMO ; JUDGE, John ; KACHMANN, Tal ; KALE, Akshay ; KANAZAWA, Naoki ; KANE, Jessica ; KANG-BAE ; KAPILA, Annanay ; KARAZEEV, Anton ; KASSEBAUM, Paul ; KELSO, Josh ; KELSO, Scott ; KHANDERAO, Vismai ; KING, Spencer ; KOBAYASHI, Yuri ; KOVI11DAY ; KOVYRSHIN, Arseny ; KRISHNAKUMAR, Rajiv ; KRISHNAN, Vivek ; KRSULICH, Kevin ; KUMKAR, Prasad ; KUS, Gawel ; LAROSE, Ryan ; LACAL, Enrique ; LAMBERT, Raphaël ; LANDA, Haggai ; LAPEYRE, John ; LATONE, Joe ; LAWRENCE, Scott ; LEE, Christina ; LI, Gushu ; LISHMAN, Jake ; LIU, Dennis ; LIU, Peng ; MADDEN, Liam ; MAENG, Yunho ; MAHESHKAR, Saurav ; MAJMUDAR, Kahan ; MALYSHEV, Aleksei ; MANDOUH, Mohamed E. ; MANELA, Joshua ; MANJULA ; MARCEK, Jakub ; MARQUES, Manoel ; MARWAHA, Kunal ; MASLOV, Dmitri ; MASZOTA, Paweł ; MATHEWS, Dolph ; MATSUO, Atsushi ; MAZHANDU, Farai ; MCCLURE, Doug ; MCELANEY, Maureen ; MCGARRY, Cameron ; MCKAY, David ; MCPHERSON, Dan ; MEESALA, Srujan ; MEIROM, Dekel ; MENDELL, Corey ; METCALFE, Thomas ; MEVISSEN, Martin ; MEYER, Andrew ; MEZZACAPO, Antonio ; MIDHA, Rohit ; MILLER, Daniel ; MINEV, Zlatko ; MITCHELL, Abby ; MOLL, Nikolaj ; MONTANEZ, Alejandro ; MONTEIRO, Gabriel ; MOORING, Michael D. ; MORALES, Renier ; MORAN, Niall ; MORCUENDE, David ; MOSTAFA, Seif ; MOTTA, Mario ; MOYARD, Romain ; MURALI, Prakash ; MÜGGENBURG, Jan ; NEMOZ, Tristan ; NADLINGER, David ; NAKANISHI, Ken ; NANNICINI, Giacomo ; NATION, Paul ; NAVARRO, Edwin ; NAVEH, Yehuda ; NEAGLE, Scott W. ; NEUWEILER, Patrick ; NGOUYEYA, Aziz ; NICANDER, Johan ; NICK-SINGSTOCK ; NIROULA, Pradeep ; NORLEN, Hassi ; NUOWENLEI ; O'RIORDAN, Lee J. ; OGUNBAYO, Oluwatobi ; OLLITRAULT, Pauline ; ONODERA, Tamiya ; OTAOLEA, Raul ; OUD, Steven ; PADILHA, Dan ; PAIK, Hanhee ; PAL, Soham ; PANG, Yuchen ; PANIGRAHI, Ashish ; PASCUZZI, Vincent R. ; PERRIELLO, Simone ; PETERSON, Eric ; PHAN, Anna ; PIRO, Francesco ; PISTOIA, Marco ; PIVETEAU, Christophe ; PLEWA, Julia ; POCREAU, Pierre ; POZAS-KERSTJENS, Alejandro ; PRACHT, Rafał ; PROKOP, Milos ; PRUTYANOV, Viktor ; PURI, Sumit ; PUZZUOLI, Daniel ; PÉREZ, Jesús ; QUANT02 ; QUINTIII ; R, Isha ; RAHMAN, Rafey I. ; RAJA, Arun ; RAJEEV, Roshan ; RAMAGIRI, Nipun ; RAO, Anirudh ; RAYMOND, Rudy ; REARDON-SMITH, Oliver ; REDONDO, Rafael Martín-Cuevas ; REUTER, Max ; RICE, Julia ; RIEDEMANN,

Matt ; RIETESH ; RISINGER, Drew ; ROCCA, Marcello L. ; RODRÍGUEZ, Diego M. ; ROHITHKARUR ; ROSAND, Ben ; ROSSMANEK, Max ; RYU, Mingi ; SAPV, Tharr-mashastha ; SA, Nahum Rosa C. ; SAHA, Arijit ; ASH-SAKI, Abdullah ; SANAND, Sankalp ; SANDBERG, Martin ; SANDESARA, Hirmay ; SAPRA, Ritvik ; SARGSYAN, Hayk ; SARKAR, Aniruddha ; SATHAYE, Ninad ; SCHMITT, Bruno ; SCHNABEL, Chris ; SCHOENFELD, Zachary ; SCHOLTEN, Travis L. ; SCHOUTE, Eddie ; SCHULTERBRANDT, Mark ; SCHWARM, Joachim ; SEWARD, James ; SERGI ; SERTAGE, Ismael F. ; SETIA, Kanav ; SHAH, Freya ; SHAMMAH, Nathan ; SHARMA, Rohan ; SHI, Yunong ; SHOE-MAKER, Jonathan ; SILVA, Adenilton ; SIMONETTO, Andrea ; SINGH, Deeksha ; SINGH, Divyanshu ; SINGH, Parmeet ; SINGKANIPA, Phattharaporn ; SIRAICHI, Yukio ; SIRI ; SISTOS, Jesús ; SITDIKOV, Iskandar ; SIVARAJAH, Seyon ; SLETFJERDING, Magnus B. ; SMOLIN, John A. ; SOEKEN, Mathias ; SOKOLOV, Igor O. ; SOKOLOV, Igor ; SOLOVIEV, Vicente P. ; SOOLUTHOMAS ; STARFISH ; STEENKEN, Dominik ; STYPULKOSKI, Matt ; SUAU, Adrien ; SUN, Shaojun ; SUNG, Kevin J. ; SUWAMA, Makoto ; SŁOWIK, Oskar ; TAKAHASHI, Hitomi ; TAKAWALE, Tanvesh ; TAVERNELL, Ivano ; TAYLOR, Charles ; TAYLOUR, Pete ; THOMAS, Soolu ; TIAN, Kevin ; TILLET, Mathieu ; TOD, Maddy ; TOMASIK, Miroslav ; TORNOW, Caroline ; TORRE, Enrique de la ; TOURAL, Juan Luis S. ; TRABING, Kenso ; TREINISH, Matthew ; TRENEV, Dimitar ; TRISHAPE ; TRUGER, Felix ; TSILIMIGKOUNAKIS, Georgios ; TULSI, Davindra ; TURNER, Wes ; VAKNIN, Yotam ; VALCARCE, Carmen R. ; VARCHON, Francois ; VARTAK, Adish ; VAZQUEZ, Almudena C. ; VIJAYWARGIYA, Prajwal ; VILLAR, Victor ; VISHNU, Bhargav ; VOGT-LEE, Desiree ; VUILLOT, Christophe ; WEAVER, James ; WEIDENFELLER, Johannes ; WIECZOREK, Rafal ; WILDSTROM, Jonathan A. ; WILSON, Jessica ; WIN-STON, Erick ; WINTERSOLDIER ; WOEHR, Jack J. ; WOERNER, Stefan ; WOO, Ryan ; WOOD, Christopher J. ; WOOD, Ryan ; WOOD, Steve ; WOOTTON, James ; WRIGHT, Matt ; XING, Lucy ; YU, Jintao ; YANG, Bo ; YERALIN, Daniyar ; YONEKURA, Ryo-ta ; YONGE-MALLO, David ; YOSHIDA, Ryuhei ; YOUNG, Richard ; YU, Jessie ; YU, Lebin ; ZACHOW, Christopher ; ZDANSKI, Laura ; ZHANG, Helena ; ZOUFAL, Christa ; IBM aeddins ; ALEXZHANG13 ; B63 ; BARTLOMIEJ bartek ; BCAMORRISON ; BRAND-HSN ; CHARMERDARK ; DEEPLOKHANDE ; DEKEL.MEIROM ; DIME10 ; DLASECKI ; EHCHEN ; FANIZZAMARCO ; FS1132429 ; GADIAL ; GALEINSTON ; GEORGEZHOU20 ; TS georgios ; GRUU ; HHORII ; HYKAVITHA ; ITOKO ; ANGEL7 jessica ; JEZERJOJO14 ; JLIU45 ; JSCOTT2 ; KLINVILL ; KRUTIK2966 ; MA5X ; MICHELLE4654 ; MSUWAMA ; NTGIWSVP ; ORDMOJ ; PAHWA sagar ; PRITAMSINHA2304 ; RYANCOCUZZO ; QISKIT saswati ; SEPTEMBRR ; SETHMERKEL ; SHAASHWAT ; STERNPARKY ; STRICKROMAN ; TIGERJACK ; CRISALDO tsura ; VADEBAYO49 ; WELIEN ; WILLHBANG ; COLLABSTAR wmurphy ; YANG.LUH ; ČEPULKOVSKIS, Mantas: *Qiskit: An Open-source Framework for Quantum Computing.* 2021

- [Asfaw und Qiskit] ASFAW, Abraham ; QISKIT: *Shor's Algorithm I: Quantum Fourier Transform, Quantum Phase Estimation Part 3.* – URL <https://www.youtube.com/watch?v=5kcoaanYyZw>
- [Bolkart 2022] BOLKART, J: *Anzahl der in Quantencomputern erreichten Qubits nach Unternehmen/Organisation von 1998 bis 2021 und Prognose bis 2023.* Jan 2022. – URL <https://de.statista.com/statistik/daten/studie/1198694/umfrage/anzahl-der-erreichten-qubits-nach-unternehmen/#:~:text=Anzahl%20der%20in%20Quantencomputern%20erreichten%20Qubits%20nach%20Unternehmen%20bis%202023&text=Im%20Jahr%20202021%20gab%20IBM,Quantencomputer%20mit%20%C3%BCber%201.000%20Qubits..> – zuletzt aufgerufen am: 11.7.2022
- [Brands 2011] BRANDS, Gilbert: *Einführung in die Quanteninformatik.* Heidelberg Dordrecht New York : Springer-Verlag, 2011. – ISBN 978-3-642-20647-4
- [Groß und Bastian 2017] GROSS, Lena ; BASTIAN, Jasmin: *Lerntechniken und Wissensmanagement - Wissen erwerben, speichern und verwerten.* Paderborn, München : UTB, 2017. – ISBN 978-3-825-24895-6
- [Krause 2021] KRAUSE, Jörg: *Developing Web Components with TypeScript - Native Web Development Using Thin Libraries.* New York : Apress, 2021. – URL <https://doi.org/10.1007/978-1-4842-6840-7>. – ISBN 978-1-4842-6840-7
- [Miller 1976] MILLER, Gary L.: Riemann's hypothesis and tests for primality. In: *Journal of Computer and System Sciences* 13 (1976), Nr. 3, S. 300–317. – URL <https://www.sciencedirect.com/science/article/pii/S002200076800438>. – ISSN 0022-0000
- [Nielsen und Chuang 2001] NIELSEN, Michael A. ; CHUANG, Isaac L.: Quantum computation and quantum information. In: *Phys. Today* 54 (2001), Nr. 2, S. 60
- [Pohl und Rupp 2015] POHL, Klaus ; RUPP, Chris: *Basiswissen Requirements Engineering - Aus- und Weiterbildung zum "Certified Professional for Requirements Engineering"; Foundation Level nach IREB-Standard/ Klaus Pohl ; Chris Rupp.* Dpunkt-Verlag, 2015. – ISBN 978-3-864-90283-3
- [QuVis 2015] QUVIS: *SIMULATION 11 - Quanten Kryptographie (BBM92).* 2015. – URL https://www.st-andrews.ac.uk/physics/quvis/de/embed_item_DE.php?anim_id=11&file_sys=index
- [Reinhaus 2011] REINHAUS, David: *Lerntechniken.* Planegg, München : Haufe-Lexware, 2011. – ISBN 978-3-648-01788-3

- [Roden 2020] RODEN, Golo: *Was man über React wissen sollte / heise Developer.* Nov 2020. – URL <https://www.heise.de/developer/artikel/Was-man-ueber-React-wissen-sollte-4966420.html>. – zuletzt aufgerufen am: 03.05.2022
- [Shor 1997] SHOR, Peter W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In: *SIAM Journal on Computing* 26 (1997), Oct, Nr. 5, S. 1484–1509. – URL <http://dx.doi.org/10.1137/S0097539795293172>. – ISSN 1095-7111
- [Shor und Preskill 2000] SHOR, Peter W. ; PRESKILL, John: Simple proof of security of the BB84 quantum key distribution protocol. In: *Physical review letters* 85 (2000), Nr. 2, S. 441
- [Smith 2022] SMITH, Steve: *Übersicht über ASP.NET core MVC.* Feb 2022. – URL <https://docs.microsoft.com/de-de/aspnet/core/mvc/overview?view=aspnetcore-6.0>. – zuletzt aufgerufen am: 02.03.2022
- [Stack Overflow 2021] STACK OVERFLOW: *Most used web frameworks among developers worldwide, as of 2021 [Graph].* Aug 2021. – URL <https://www-statista-com.ezproxy-dhbw-redi-bw.de/statistics/1124699/worldwide-developer-survey-most-used-frameworks-web/>. – In Statista. abgerufen am 21.03.2022
- [Steane 1998] STEANE, Andrew: Quantum computing. In: *Reports on Progress in Physics* 61 (1998), Nr. 2, S. 117
- [Steane 2021] STEANE, Andrew: *Is the eigenvalue of an eigenstate the same as its (global) phase?* Physics Stack Exchange. January 2021. – URL <https://physics.stackexchange.com/q/687904>