QBTS NEWS

21TH JAN 2038

SAN FRANCISCO

QUBITS AUS SILICON VALLEY ENTLAUFEN.

In San Francisco treiben entlaufene Qubits aus dem Silicon Valley ihr Unwesen und helfen Grundschülern unerlaubterweise bei Kopfrechenaufgaben in Mathematiktests.

BERLIN

3 VERLETZTE BEIM REHYDRIEREN EINER PIZZA.

In einer Wohnung im Berliner Stadtteil Wedding kam es am Sonntagnachmittag zu einer Explosion als sich eine Familie zum Abendessen eine Pizza rehydrieren wollte. Alle Personen erlitten starke Verbrühungen und wurden in die Charité eingeliefert.

WETTER

MINÜTLICH UND VERLÄSSLICH.

SONNENAUFGANG 08:03 — 16:57 SONNENUNTERGANG

06:45–07:47	Leichter Regen
07:48–15:34	Sonnig
15:35–16:15	Leicht bewölkt
16:16–20:03	Regen

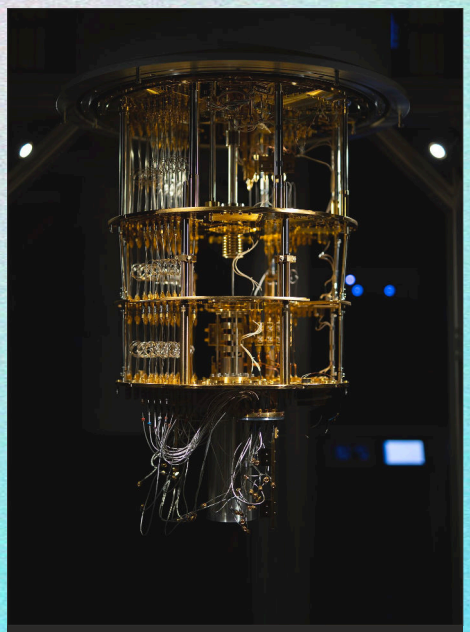
ComputingEducation

QUANTEN-INFORMATIK

REISE IN DIE QUANTENZEIT

Willkommen in der Welt im Jahr 2038! Es hat sich einiges geändert. Die Verschlüsselungssysteme, die wir bisher im Internet verwendet haben, waren nicht mehr sicher und mussten aktualisiert werden. Jetzt können persönliche Daten über Netzwerke wirklich abhörsicher übertragen werden. Dank der Quanteninformatik hat aber auch die Arzneimittelentwicklung und -forschung ganz neue Dimensionen angenommen. Und die Suche nach Informationen dauert jetzt wirklich nur noch einen Wimpernschlag.

So oder so ähnlich könnte eine Welt mit Quantencomputern zukünftig aussehen. Aber noch ist diese Zukunft nicht geschrieben. Du kannst sie selbst aktiv mitgestalten und die Quanteninformatik könnte dabei ein wichtiger Baustein sein. Dieses Heft bietet dir eine Einführung in die Welt der Quanteninformatik.



Im Jahr 2021 sahen Quantencomputer so aus (CC-BY-SA IQM).

Das Heft beinhaltet einerseits Erklärtexte und andererseits Aktivitäten, mit denen du selbst Konzepte der Quanteninformatik entdecken kannst. Es ist so gestaltet, dass du die Welt der Quanteninformatik alleine, gemeinsam mit einem Freund, einer Freundin oder deiner Lehrkraft erforschen kannst. Es ist dein Heft. Das heißt, du kannst deine Notizen direkt im Heft machen.

An vielen Stellen ergeben sich Verbindungen zu klassischen Themen der Informatik. Du brauchst aber keine Angst haben: Wir werden alle erforderlichen Begriffe und Grundlagen anschaulich erläutern. Auch wenn also Begriffe wie Bits, Schaltung oder Simulation noch neu für dich sind, wirst du mit diesem Material sehr viel Spaß haben!

Los geht’s!

PS: An manchen Stellen in dieser Broschüre haben wir Anspielungen auf eine mögliche Zukunft gemacht. Alle Fakten und Anregungen sind frei erfunden. Wir stehen in keiner Verbindung mit den genannten Firmen oder Marken.

HRSG. Stefan Seegerer, Ralf Romeike, Andreas Woitzik, Tilman Michaeli

LEICHTE & SCHWERE PROBLEME

Herkömmliche Computer (wie dein Notebook oder dein Smartphone, aber auch raumgroße Supercomputer in den Rechenzentren dieser Welt) erzielen beeindruckende Ergebnisse. Es gibt bereits in den 2020er Jahren Programme, die die grafische Ausgabe von fotorealistischen Computerspielen oder Animationsfilmen berechnen oder welche, die erkennen, was auf einem Bild abgebildet ist. Andere Programme führen komplexe, wissenschaftliche Berechnungen durch und treiben so den technischen Fortschritt voran.

Der Film „Big Buck Bunny“ wurde komplett von Computern berechnet (CC-BY Blender Foundation)

Auch wenn es manchmal so wirkt, als könnten herkömmliche Computer jede Aufgabe mit Leichtigkeit lösen, sind auch für Computer manche Probleme schwieriger als andere und einige sogar nicht mal in akzeptabler Zeit zu lösen.

Probiere es selbst aus.

Auf den folgenden Seiten findest du unterschiedlich schwere Probleme.

Nimm dir jeweils 5 Minuten Zeit und versuche zunächst selbst eine Lösung zu finden.

Bewerte anschließend: Wie schwierig würdest du das Problem auf einer Skala von 1 (kann doch jedes Kind) bis 10 (war in der Zeit gar nicht zu lösen) einstufen ? Und warum?

Alternativ kannst du auch ein Handy zur Hand nehmen und die Zeit stoppen.

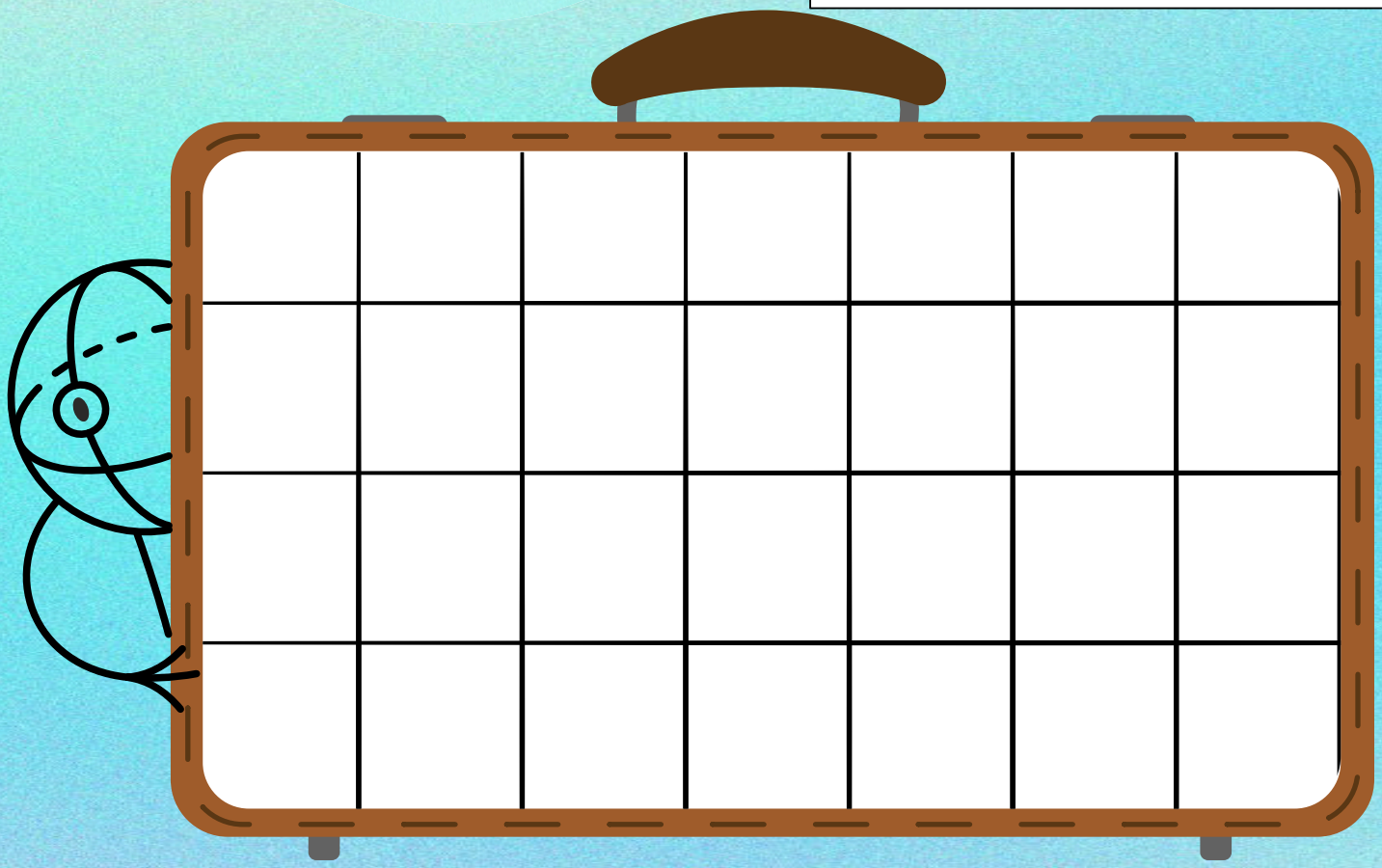
SIEHE NÄCHSTE SEITE

AKTIVITÄT 1

DAS KOFFERPROBLEM LÖSEN.

Packe den Koffer so, dass du den Platz bestmöglichst ausnutzt und die wertvollsten Objekte mitnimmst!

Hinweis: Die Gegenstandskarten findest du am Ende dieses Hefts (S. 55).



Anzahl eingepackter Gegenstände	Wert eingepackter Gegenstände

1	2	3	4	5	6	7	8	9	10
Schwierigkeit einer solchen Aufgabe für mich									

EIN BUCHSTABENGITTER LÖSEN.

Im Buchstabengitter haben sich 7 Begriffe zum Thema Computer versteckt. Diese können in Leserichtung wageerecht oder senkrecht platziert sein.

A	G	B	F	I	F	E	M	B	Q	W	X
X	I	T	M	P	K	B	Y	T	E	E	H
Z	N	S	H	E	S	M	E	O	Y	K	J
F	T	T	A	S	T	A	T	U	R	Z	U
A	E	W	R	I	M	S	D	F	E	K	E
T	R	I	D	E	B	R	O	W	S	E	R
E	N	T	W	E	T	C	U	H	T	L	B
S	E	T	A	S	O	F	T	W	A	R	E
S	T	E	R	I	S	T	A	M	M	T	X
G	U	F	E	S	T	P	L	A	T	T	E
H	S	E	E	G	Q	O	X	L	P	M	M
P	R	X	I	M	K	B	S	Y	A	X	Z

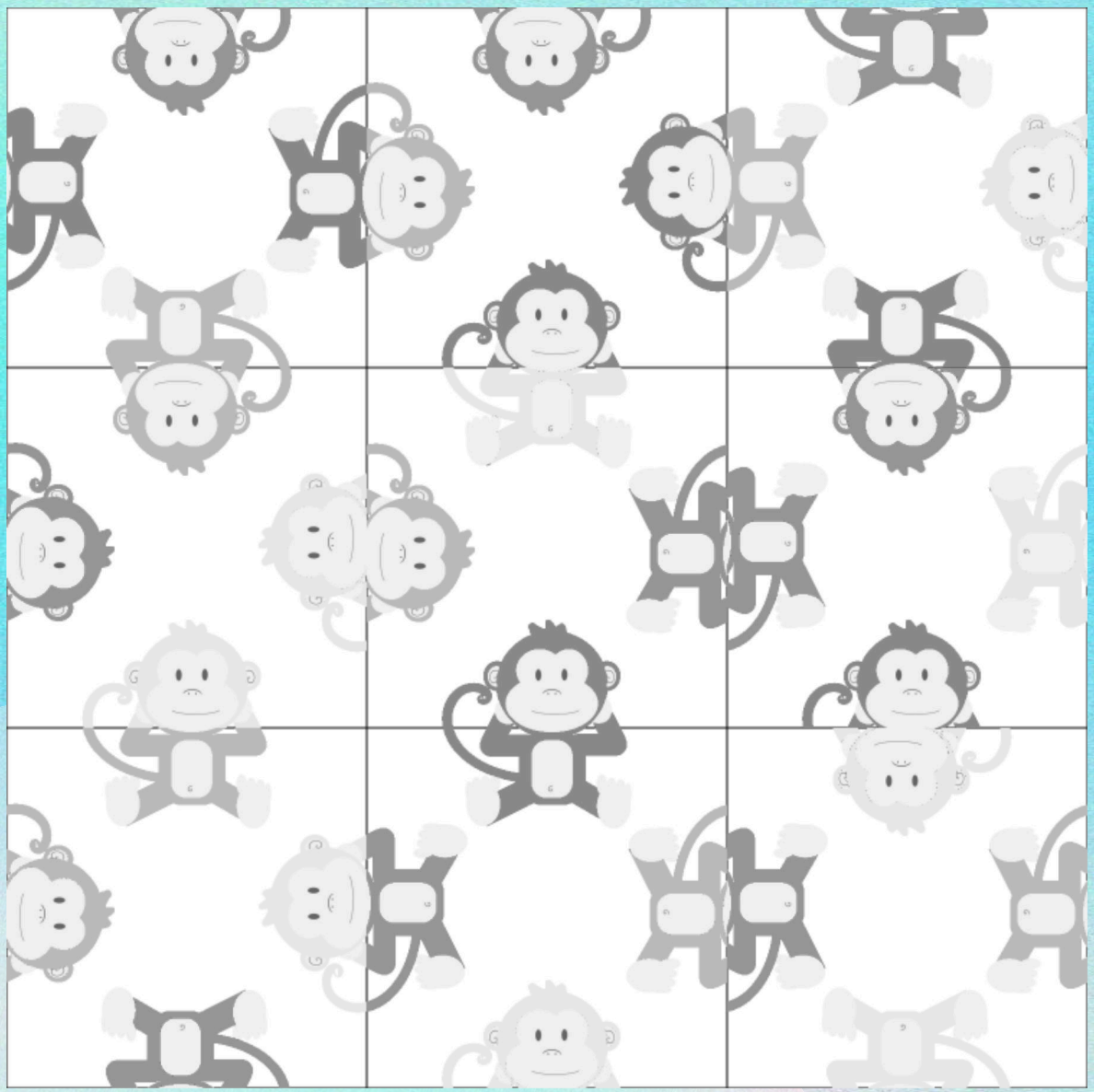
1	2	3	4	5	6	7	8	9	10

Schwierigkeit einer solchen Aufgabe für mich

EINE LÖSUNG FÜR DAS AFFENPUZZLE FINDEN.

Dir stehen Karten mit Äffchen in vier verschiedenen Farben zur Verfügung. Schaffst du es, die Karten so anzuordnen, dass die Ober- und Unterteile farblich zusammenpassen?

Hinweis: Die Karten findest du am Ende dieses Hefts (S. 53).



1	2	3	4	5	6	7	8	9	10

Schwierigkeit einer solchen Aufgabe für mich

ZWEI GEGEBENE ZAHLEN MULTIPLIZIEREN.

Schaffst du es, die beiden gegebenen Zahlen zu multiplizieren?

Hinweis: Mit Taschenrechner kann das ja jeder, also gilt: Verwende dazu keinen Taschenrechner!

$5 \cdot 7 =$ **35**
Lösung

$7 \cdot 9 =$
Lösung

$19 \cdot 23 =$
Lösung

$57 \cdot 97 =$
Lösung

1	2	3	4	5	6	7	8	9	10

Schwierigkeit einer solchen Aufgabe für mich

ZWEI ZAHLEN X UND Y FINDEN, SODASS X·Y DIE GEGEBENE ZAHL ERGIBT.

Findest du zwei Primzahlen x und y, sodass x · y die jeweilige Zahl unten ergibt?

Hinweis: Verwende dazu keinen Taschenrechner!

143	=	11 (Zahl 1)	·	13 (Zahl 2)	
169	=	(Zahl 1)	·	(Zahl 2)	
289	=	(Zahl 1)	·	(Zahl 2)	
1147	=	(Zahl 1)	·	(Zahl 2)	

1	2	3	4	5	6	7	8	9	10

Schwierigkeit einer solchen Aufgabe für mich

WARUM EIGENTLICH QUANTEN-COMPUTER?

Genau wie für dich, sind auch für den Computer Probleme unterschiedlich schwer. Für den Computer ist es egal ob er beispielsweise für die Zahl 7 herausfinden soll, ob sie gerade ist, oder für eine zwanzig-stellige Zahl, wie die 54295673818495738178.

Aber, ob er nun 1.000 Datensätze sortieren muss oder 10.000 Datensätze macht schon einen Unterschied: Der Computer braucht hierfür nicht nur 10 mal so viel Zeit, sondern je nach Umsetzung 20 oder sogar 100 mal soviel Zeit.

Und einige Aufgaben sind dann so schwer, dass sie selbst mit deutlich schnelleren Computern nicht in angemessener Zeit zu bewältigen sind. Eine leichte Vergrößerung der zu bearbeitenden Aufgabe führt dann zu einer Vervielfachung der notwendigen Rechenzeit.

Das lässt sich ganz gut an der Aufgabe mit dem Affenpuzzle verdeutlichen. Ein Puzzle der Größe 5x5 könnte ein schneller Computer noch innerhalb einer Minute durch Ausprobieren lösen und auch bei einem Puzzle der Größe 6x6 würde man das Ergebnis innerhalb eines halben Jahres erhalten. Aber schon auf die Lösung des Affenpuzzles der Größe 7x7 würde man auch mit den schnellsten herkömmlichen Computern länger warten, als man in einem Leben Zeit hat, nämlich ungefähr 50 Millionen Jahre. Wenn allerdings einmal eine Lösung gefunden wurde, lässt sich sehr leicht prüfen, ob sie richtig ist.

Das trifft auch auf die Zerlegung großer Zahlen in ihre Primfaktoren (also z.B. 91 in 7·13) zu: Es ist kein effizientes Verfahren bekannt, um die Primfaktoren einer sehr großen Zahl mit über 600 Stellen in angemessener Zeit zu ermitteln. Es bleibt daher nur, alle Möglichkeiten durchzuprobieren. Kennt man aber die Primfaktoren, lässt sich sehr schnell überprüfen, ob sie multipliziert die richtige Ausgangszahl ergeben. Diese Eigenschaft liegt auch vielen Verschlüsselungsverfahren zugrunde, die unsere digitale Kommunikation schützen. Findet man allerdings einen Weg, der die Primfaktoren von großen Zahlen in Sekundenschnelle liefern kann, könnte man viele heute gebräuchliche Verschlüsselungssysteme knacken!

Tatsächlich geht man davon aus, dass Quantencomputer bestimmte Probleme (nicht alle Probleme) effizienter lösen können als herkömmliche Computer. Ein Beispiel ist genau die Primfaktorzerlegung: Der Informatiker Peter Shor hat einen Algorithmus für Quantencomputer entwickelt, der eine Zahl blitzschnell in ihre Primfaktoren zerlegen kann – sofern man den entsprechenden Quantencomputer zur Verfügung hat. Aktuell ist die Technik noch nicht weit genug, um solche Quantencomputer zu bauen. Aber wer weiß schon, wie das in ein paar Jahren aussieht.

Es gibt noch weitere Anwendungsbereiche, die für herkömmliche Computer als schwierig gelten und bei denen Quantencomputer Verbesserungen versprechen. Dazu gehören die Simulation von Teilchen in der Materialforschung oder in der Beforschung und Entwicklung von Medikamenten sowie das Durchsuchen unglaublich großer Datenmengen.

SUCHE UND BIETE

ANZEIGE

Verkaufe 51 Jahre alten CD-Spieler. Gerät funktioniert noch makellos, leichte Gebrauchsspuren dem Alter entsprechend.

@schallplattenfan

AR-Fernreisen jetzt bis zu 50% billiger! Der Preis ist heiß, genau wie die Sonne auf Mallorca! Jetzt zuschlagen! Durch unser patentiertes Bräunungskonzept werden Sie auch im AR-Urlaub braun!

@reiseARlarm

KATZE ENTLAUFEN

Chipcode: Ax1t23414242
Bin um jeden Hinweis dankbar!

@katzenfreundin2021

VERKAUFE FESTPLATTE

mit 24.000 DOGECOIN,
Key unbekannt

@daddycool

SUCHE

Katze entlaufen, Chip defekt, bin über jeden Hinweis dankbar. Ruft einfach kurz durch unter: @HerrRuin.

@HerrRuin

SUCHE

alte, gute erhaltene Apple iPhones (12-14), gerne auch aus einem Antiquariat.
Bitte alles anbieten! Auch ähnliche Geräte (sog. Smartphones) sind gern gesehen.

@i-and-my-phones

SUCHE

Ich sammle Retro-Konsolen & Spiele im Disc-Format.
bitte alles anbieten, insbesondere alte Modelle wie PS4 oder PS5.

@retro_konsolero

ANZEIGE

Biete Buch “Die neue Generation Social Media - So wurde Facebook, Instagram und Snapchat der Kampf angesagt” - 25€

@Peter71

SUCHE

1-Zimmer-Appartment mit Bad und Essenshydratisierer nähe TU Nürnberg, max 3000€ kalt

@max-mustermann

ANZEIGE

Repariere und überhole antike Spielekonsolen: Nintendo Switch Pro, XBOX Series X, PS6, …

@spiele_fan

SUCHE

Wir suchen Probandinnen und Probanden für eine Studie zum Thema “Gesunde Flüssignahrung - Satt von 50ml pro Tag”. Bei Interesse melden Sie sich bei uns!

@teilnahme-studie-2038

URLAUM IM GRÜNEN

Beobachten Sie wilde Roombaherden im Schwarzwald - Ein aufregender Erlebnisurlaub für die ganze Familie!

@blackforest-holiday

ANZEIGE

Biete Zweizimmer-Wohnung im 2. OG, 65qm, 3.000€ Kaution, 1.900€ Kaltmiete, provisionsfrei, nahe FU Berlin, Telefon: @2zwhg-dahlem

@2zwhg-dahlem

AR-SERVICE

Ihre AR-Brille tut nicht was Sie wollen? Wir helfen schnell und unkompliziert, ein Videocall genügt!

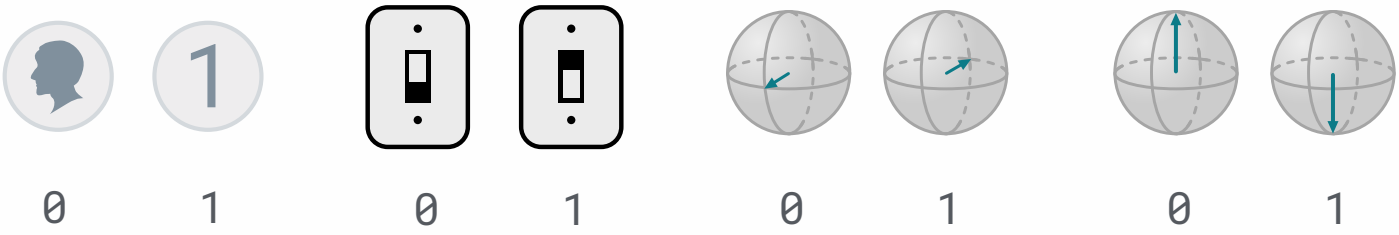
@pcservicecenterBerlin

AKTIVITÄT 2.1

Herkömmliche Computer.

Wie du vielleicht bereits gehört hast, arbeiten herkömmliche Computer (wie auch Smartphones) intern mit nur zwei Zuständen: 0 und 1.

Wir sprechen auch von **Bits**. Dazu nutzen sie elektrische Signale: Ist der Strom aus, wird das als 0 interpretiert, ist der Strom an als 1. Ein Bit lässt sich aber im Prinzip durch alles darstellen, was zwei Zustände hat: Bei Münzen durch Kopf (0) / Zahl (1), bei einem Lichtschalter durch Licht aus (0) / Licht an (1) oder bei einer Kugel entweder durch Pfeil vorne (0) / Pfeil hinten (1) oder durch Pfeil hoch (0) / Pfeil runter (1).



Gatter

Mithilfe von Bits codieren Computer Informationen wie beispielsweise Bilder, Texte oder Videos. Auch eine Glühbirne kann ein Bit an Information darstellen. Fließt Strom, brennt die Glühbirne, fließt kein Strom, bleibt sie aus.

Damit Computer nützliche Ergebnisse liefern und Programme ausführen können, brauchen sie eine Möglichkeit, diese Bits zu verarbeiten. Dafür verfügen Computer über sogenannte Gatter. Solch ein Gatter hat einen oder mehrere Eingänge, an denen es Signale (die stehen für die 0 oder die 1) entgegennimmt und Ausgänge, an denen es Signale weitergibt. Wie ein Gatter funktioniert, lässt sich am Beispiel des NICHT-Gatters und dem Lichtschalter verdeutlichen.

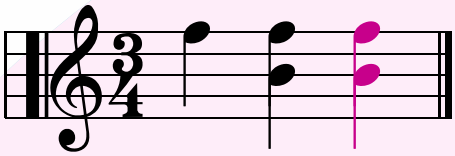
Zu beachten sind hierbei die unterschiedlichen Schalterstellungen: Ein NICHT-Gatter kehrt das eingehende Signal um. Ist der Schalter aus, fließt kein Strom und das eingehende Signal ist zunächst 0. Das NICHT-Gatter gibt also das Signal 1 weiter - die Lampe brennt.

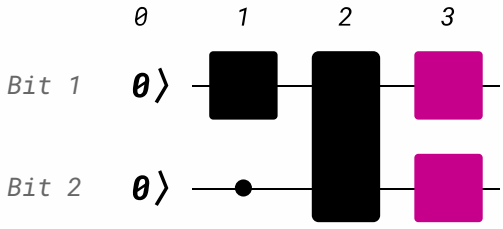
Ist der Schalter an, ist das am NICHT-Gatter anliegende Signal 1 und das NICHT-Gatter gibt kein Stromsignal (0) weiter - die Lampe bleibt damit aus.

Schaltkreise

Mehrere Gatter bilden zusammen einen **Schaltkreis** und sind so die Basis für Computer, wie wir sie kennen. Ein **Algorithmus**, der von einem Computer ausgeführt werden kann, ist dann nichts anderes als eine präzise Beschreibung, wann welches Gatter angewendet werden muss. Um zu verstehen, wie ein herkömmlicher Computer im Innersten arbeitet, ist es daher hilfreich zu verstehen, wie diese Gatter funktionieren.

Schaltkreise können ähnlich wie Musiknoten in Diagrammen dargestellt werden. Eine Musikerin bzw. ein Musiker beginnt links im Moment Null und geht in der Zeit vorwärts, indem sie oder er nach rechts liest. Am Notenschlüssel ist zu erkennen, wie die Noten zu interpretieren sind.



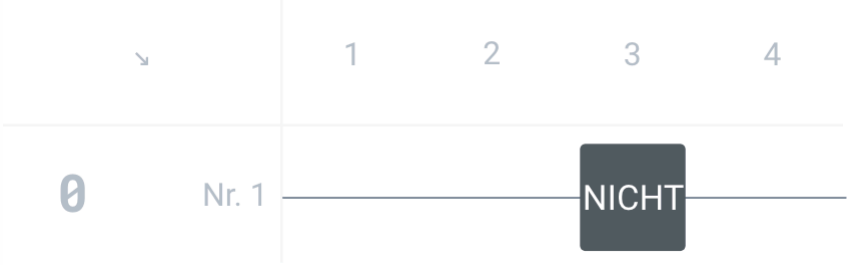


In ähnlicher Weise stellen Schaltkreise Gatteroperationen als eine Reihe von Momenten in der Zeit dar. Wie die Noten ist das Diagramm beginnend beim Moment Null von links nach rechts zu lesen. Hier haben wir einen Schaltkreis, der 3 Momente lang ist und mit 2 Bits arbeitet.

Beim Lesen von links nach rechts können wir beobachten, was in den einzelnen Momenten passiert. Wir beginnen im Moment Null (Spalte 0) mit den beiden Anfangswerten 0. Im ersten Moment wird ein Gatter nur auf Bit 1 angewandt. Mit Bit 2 passiert nichts (manchmal wird das auch - wie hier - durch einen kleinen Kreis auf dem Schaltdraht dargestellt). Das Gatter im zweiten Schritt verarbeitet Bit 1 und 2 und liefert zwei Ausgaben. In Schritt 3 (pink eingefärbt) wird auf die beiden Bits separat jeweils ein Gatter angewendet.

NICHT-Gatter

Ein bekanntes Gatter ist das NICHT-Gatter.
Auf der Website (siehe QR-Code auf S. 11) kannst du das Gatter mit den Eingaben 0 und 1 aufrufen, indem Du auf die Zahl am Anfang der Zeile und dann auf Auswerten klickst!



Eine Möglichkeit, sich die Funktionsweise von Gattern zu verdeutlichen, sind sogenannte Wahrheitstabellen. Eine Wahrheitstabelle beschreibt, wie sich ein Gatter für alle Eingaben verhält. Dazu notiert man typischerweise für jede mögliche Eingabekombination die zugehörige Ausgabe.

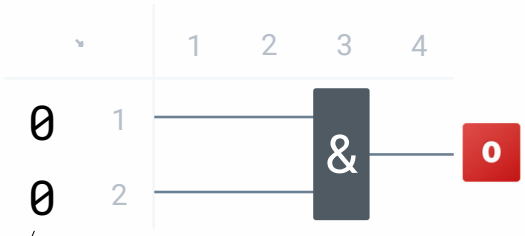
Eingabe	Ausgabe
0	1
1	0

Die Wahrheitstabelle für das NICHT-Gatter (rechts) verrät uns: Liegt am Eingang 0 an, geht der Ausgang an (wird also 1) und andersrum. Du siehst, genau wie bei der Glühbirne!

Da es nur ein Bit als Eingabe entgegennimmt, besteht die Wahrheitstabelle des NICHT-Gatters nur aus zwei Zeilen.

& -Gatter und ≥1-Gatter

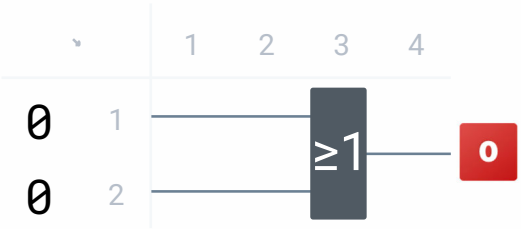
! Du bist dran! Finde heraus, welche Funktion die Gatter & und ≥1 haben, indem du verschiedene Eingabewerte online ausprobierst (siehe QR-Code auf Seite 11) und mehrere Messungen durchführst! Fülle die Wahrheitstabelle für beide Gatter aus.



Klicke hier, um den Eingabewert zu ändern

Trage hier deine Ergebnisse ein >

&	Eingabe	Ausgabe
	0 0	0
	0 1	
	1 0	
	1 1	

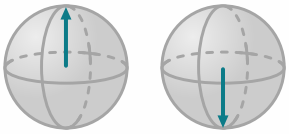


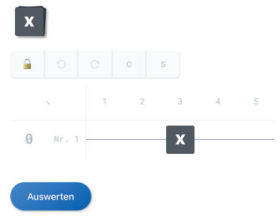
≥1	Eingabe	Ausgabe
	0 0	
	0 1	
	1 0	
	1 1	

AKTIVITÄT 2.2

Quantencomputer und Qubits.

Quantencomputer arbeiten anstelle von **Bits** mit sogenannten **Quantenbits**. Ein Quantenbit oder **Qubit** stellt die kleinste Informationseinheit in der Welt der Quantencomputer dar. Es ähnelt einem Bit insofern, als wir zwei messbare Zustände unterscheiden, die mit `0` und `1` bezeichnet werden.





Genau wie ein herkömmlicher Computer braucht auch der Quantencomputer Möglichkeiten, die Informationseinheiten (hier: die Qubits) zu beeinflussen: Quantengatter. Wir werden ab sofort daher Quantenschaltkreise nutzen, um selbst Experimente mit Quantencomputern zu machen. Anders als bisher, stellt **jede Zeile nun ein Qubit** dar!

`X`-Gatter

Das erste Quantengatter, das wir uns ansehen wollen, ist das `X`-Gatter.

> ! Untersuche, welche Auswirkungen das Gatter `X` auf ein Qubit hat, indem du
>
> > das `X`-Gatter an verschiedene Positionen schiebst und jeweils eine Messung durchführst,
>
> > den Eingabewert von `0` auf `1` änderst und eine Messung durchführst
>
> > und ein zweites `X`-Gatter hinzufügst und eine Messung durchführst!
>
> Notiere deine Beobachtungen!

Auswirkungen auf Eingabewert 0:

Auswirkungen auf Eingabewert 1:

Auswirkungen unterschiedlicher Positionen:

Auswirkungen von zwei aufeinanderfolgenden X-Gattern:

Beobachtungen

H-Gatter

Qubits haben aber auch einige Eigenschaften, die normale Bits nicht haben. Gemeinsam wollen wir herausfinden, welche das sind! Dafür nutzen wir das H-Gatter, das uns einen ersten Vorgeschmack auf das gibt, was Quantencomputer so besonders macht.

> ! Untersuche, welche Auswirkungen das Gatter H auf ein Qubit hat, indem du verschiedene Eingabewerte ausprobierst und mindestens 10 Messungen je Eingabewert durchführst. Notiere deine Beobachtungen!

Klicke hier, um den Eingabewert zu ändern

Messprotokoll für Eingabewert 0

Messprotokoll für Eingabewert 1

Meine Beobachtung

AKTIVITÄT 2.3

Die Superposition.

Während sich das X-Gatter vergleichbar wie das NICHT-Gatter eines herkömmlichen Computers verhält, wirst du festgestellt haben, dass das sogenannte **Hadamard-Gatter** H dafür sorgt, dass wir in ungefähr 50% der Fälle 0 und in den anderen 50% 1 messen.

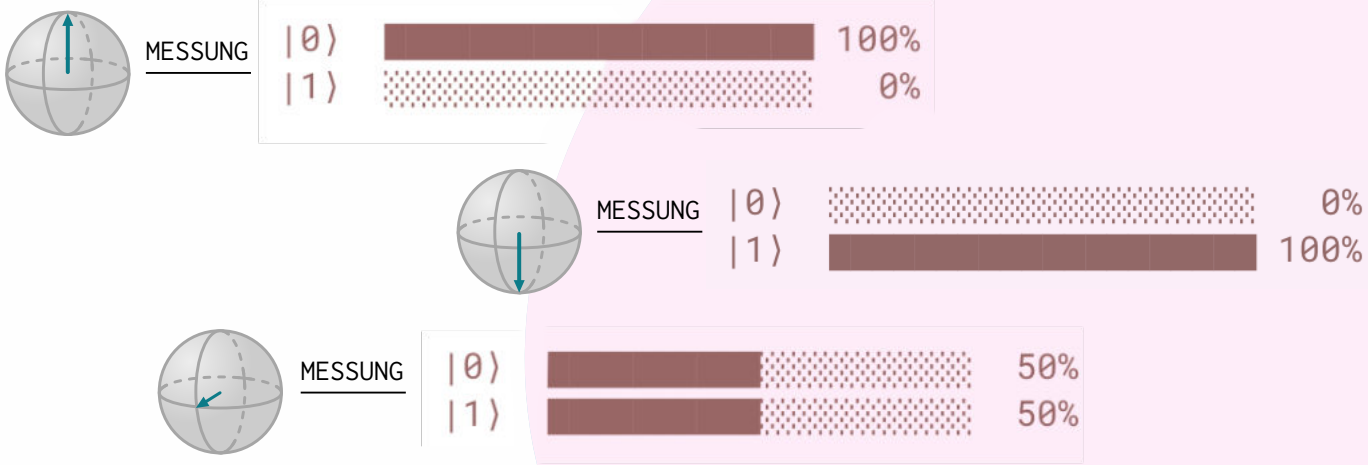
Die Anwendung des Hadamard-Gatters bringt das Qubit also in einen Zustand, bei dem die Wahrscheinlichkeit 0 bzw. 1 zu messen, jeweils 50% beträgt.

Damit hast du eine der Besonderheiten aus der Welt der Quantencomputer kennengelernt:

Ein Qubit kann den Wert 0 und den Wert 1 annehmen oder in einer **Superposition** aus 0 und 1 sein. Dann hat es eine bestimmte Wahrscheinlichkeit als 0 bzw. 1 gemessen zu werden. Eine Messung zerstört allerdings die Superposition - die Messung kann also nicht wiederholt werden.

Denken wir noch einmal an das Kugelmodell, das wir bei Bits bereits kennengelernt haben und bei dem wir Pfeil runter als 0 und Pfeil hoch als 1 interpretiert haben. Betrachten wir nun Qubits, kann der Pfeil in eine andere Richtung als oben oder unten zeigen. Nach Anwendung des Hadamard-Gatters auf ein Qubit im Zustand 1 zeigt der Pfeil nach vorne. Messen wir, fällt die Kugel mit einer gewissen Wahrscheinlichkeit in den Basiszustand oben oder in den Basiszustand unten zurück.

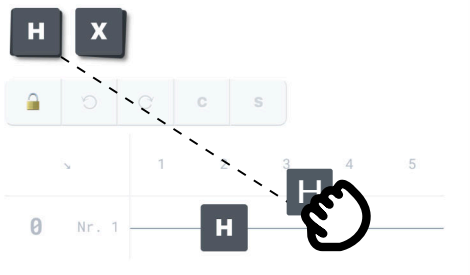
Die Superposition eines Qubits ist deshalb so schwer vorstellbar, weil sie die Überlagerung zweier Zustände sehr kleiner Objekte wie Elektronen oder Photonen (Lichtteilchen) beschreibt. Daher hilft uns bei Qubits unsere Kugeldarstellung. Einen Aspekt können wir uns aber auch schon mithilfe von Münzen verdeutlichen: Eine Münze hat eine 50/50-Wahrscheinlichkeit auf Kopf bzw. auf Zahl zu landen. Wir können sagen, dass sich die Münze in einer Superposition aus Kopf und Zahl befindet. Wenn sie landet, hat sie aber einen eindeutigen Zustand, entweder Kopf oder Zahl - die Superposition wird also zerstört.



Hadamard-Gatter zweimal anwenden

Es wirkt zunächst so, als würde das Hadamard-Gatter jede im Qubit gespeicherte Information löschen, denn egal ob Startwert 1 oder 0, die Wahrscheinlichkeit, das eine bzw. das andere zu messen, beträgt in beiden Fällen jeweils 50%. Nach unserer Messung wirken die beiden Zustände also nicht unterscheidbar. Aber ist das wirklich so? Finden wir es heraus!

! Wende das Hadamard-Gatter **H** zweimal hintereinander an, wobei du einmal **0** und einmal **1** als Eingabewert wählst. Beschreibe deine Beobachtung! Was bedeutet das für die im Qubit gespeicherte Information?



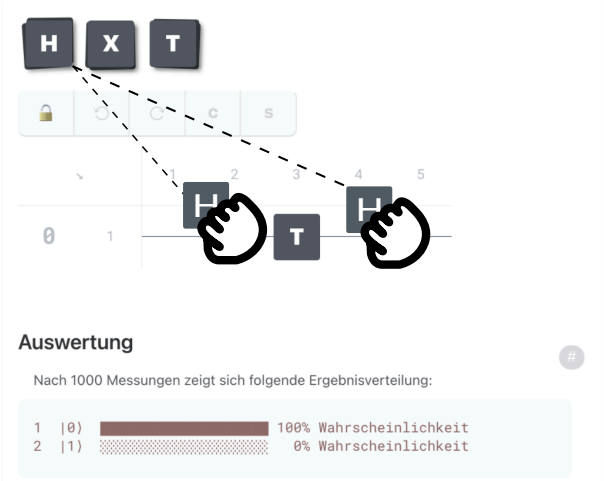
Meine Beobachtung

Für die im Qubit gespeicherte Information bedeutet das …

Kombination verschiedener Gatter

Neben dem H-Gatter verfügen Quantencomputer noch über weitere Gatter. Eines davon ist das T-Gatter, das man sich als Drehung um 22,5° entlang des Äquators der Kugel vorstellen kann.

! Das bisher unbekannte T-Gatter scheint zunächst keinen Effekt zu haben. Füge vor und nach dem T-Gatter je ein Hadamard-Gatter H ein. Wie wirkt sich das auf das Messergebnis aus? Notiere deine Beobachtung!



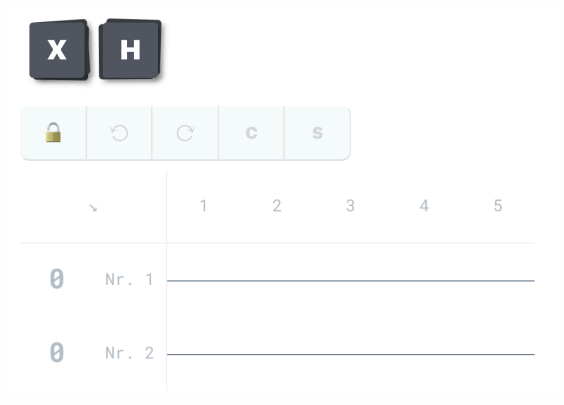
Meine Beobachtung

AKTIVITÄT 2.4

Mehrere Qubits.

Natürlich kann ein Quantencomputer mit nur einem Qubit keine Wunder vollbringen. Wir brauchen also weitere Qubits.

> ! Probiere den folgenden Schaltkreis mit zwei Qubits aus. Wie viele verschiedene Messergebnisse kannst du durch Anwendung von Gattern herstellen?



> 00
>

Liste herstellbarer Messergebnisse

Ein Gatter für 2 Qubits

Außerdem brauchen wir ein Gatter, das mit zwei Qubits arbeitet. Um zu verstehen, warum dieses Gatter einen echten Vorteil für Quantencomputer liefert, wollen wir uns zunächst einmal seine grundlegende Funktionsweise ansehen.

> ! Unten findest du ein Gatter, das mit zwei Qubits arbeitet. Beschreibe den Effekt dieses Gatters in eigenen Worten, indem du verschiedene Eingabewerte ausprobierst und mehrere Messungen durchführst.

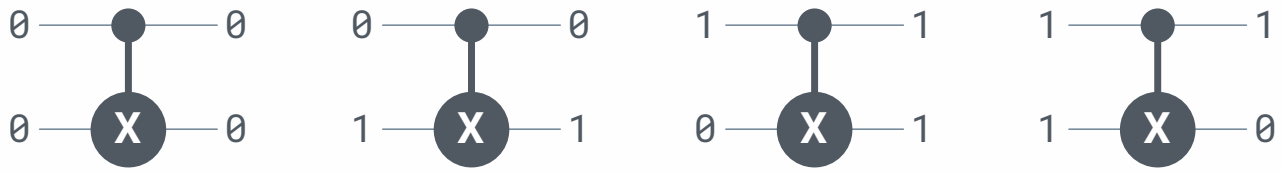
Effekt des Gatters in eigenen Worten

Du kannst ein CNOT-Gatter erstellen, indem du ein X-Gatter und ein ·- Gatter in einer Spalte anordnest, beide markierst und auf C klickst.

AKTIVITÄT 2.5

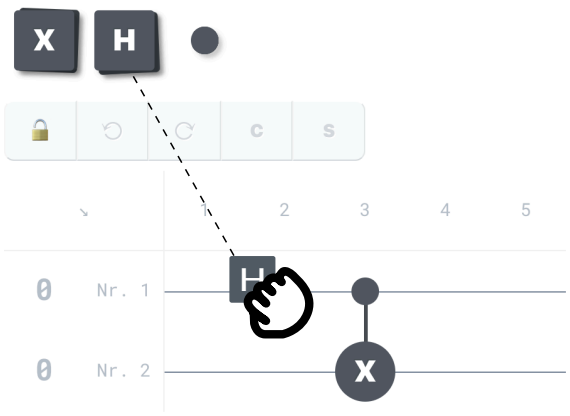
CNOT und Hadamard.

Das gerade kennengelernte Gatter nennen wir **CNOT** (Controlled NOT, engl. für kontrolliertes NICHT-Gatter). Es wendet ein X-Gatter auf das untere Qubit (Ziel-Qubit) an, sofern das obere Qubit (Kontroll-Qubit) im Zustand 1 ist. Ist das obere Qubit (Kontroll-Qubit) im Zustand 0, ändert sich nichts am unteren Qubit.



Was aber passiert, wenn das Kontroll-Qubit nicht im Zustand 0 oder im Zustand 1 ist, sondern in einem Superpositionszustand?

! Wende ein Hadamard-Gatter H auf das erste Qubit vor der Anwendung des CNOT-Gatters an, um es in eine gleichmäßige Superposition zu bringen. Führe dann erneut einige Messungen mit verschiedenen Eingabewerten durch. Welchen Effekt hat das Gatter auf das Gesamtergebnis?



Meine Beobachtung

HIER SELBST AUSPROBIEREN

AKTIVITÄT 2.6

Verschränkte Qubits.

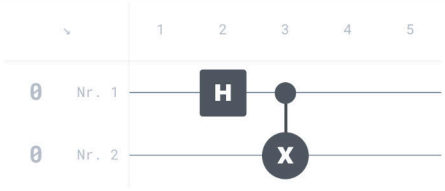
HIER SELBST AUSPROBIEREN

Wie du mit deinen Messungen vermutlich bereits festgestellt hast, steht das Ergebnis eines Schaltkreises bei Quantencomputern oft nicht von Anfang an fest. Auch im Falle von zwei Qubits erhalten wir – genau wie im Falle nur eines Qubits – bei einer Messung mit einer bestimmten Wahrscheinlichkeit ein bestimmtes Ergebnis. Um also ein verlässliches Ergebnis über den Zustand zu erhalten und zwischen den verschiedenen Superpositionszuständen unterscheiden zu können, müssen wir wieder eine Vielzahl an Messungen durchführen.

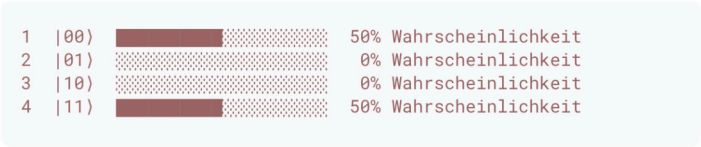
Spannend wird das in Verbindung mit dem CNOT-Gatter: Ist das Kontroll-Qubit in einer Superposition, hängt das Messergebnis des Ziel-Qubits davon ab, welchen Wert das Kontroll-Qubit nun annimmt. Damit hast du eine weitere Besonderheit von Qubits kennengelernt:

Zwei Qubits können miteinander **verschränkt werden**. Misst man dann den Zustand eines der Qubits, kennt man auch automatisch den Zustand des anderen Qubits.

Mit verschränkten Qubits können wir jetzt auch Zustände schaffen, die wir sonst nicht erreicht hätten – beispielsweise einen Zustand, bei dem wir in 50% der Fälle `00` messen und in 50% der Fälle `11`.



Diese Ergebnisverteilung lässt sich wirklich nur mit Verschränkung von Qubits erreichen.



! Den Wert welches Eingabe-Qubits müssen wir ändern, dass eine 50% Wahrscheinlichkeit besteht als Ausgabe `10` und eine 50% Wahrscheinlichkeit als Ausgabe `01` zu erhalten? Überprüfe Deine Vermutung!

Deine Vermutung (kreuze an):

☐ Qubit Nr. 1

☐ Qubit Nr. 2

Vermutung ließ sich bestätigen:

AKTIVITÄT 2.7

Anzahl darstellbarer Zustände.

HIER SELBST AUSPROBIEREN

Auf den letzten Seiten haben wir gesehen:

> Qubits können nicht nur in den beiden Zuständen 0 und 1 sein, sondern auch in einer Superposition aus 0 und 1. Dann haben sie eine gewisse Wahrscheinlichkeit als 0 bzw. 1 gemessen zu werden. Eine Messung zerstört allerdings die Superposition.

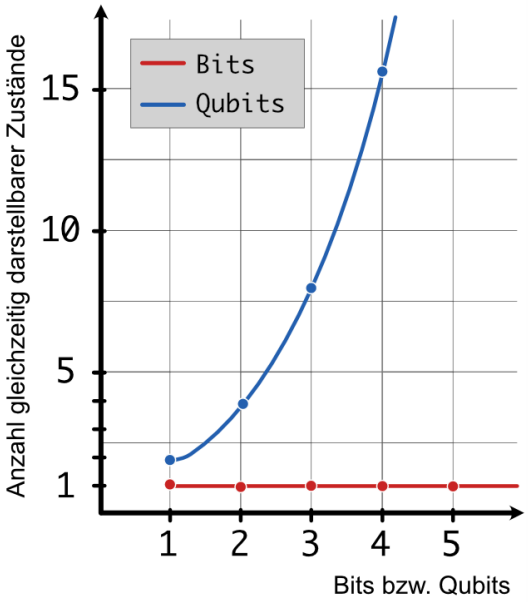
> Auch wenn die Messergebnisse eines Qubits zufällig sind, ist das Qubit dennoch stets in einem genau definierten Zustand.

> Zwei Qubits können miteinander verschränkt werden. Misst man dann den Zustand eines der Qubits, kennt man auch automatisch den Zustand des anderen Qubits.

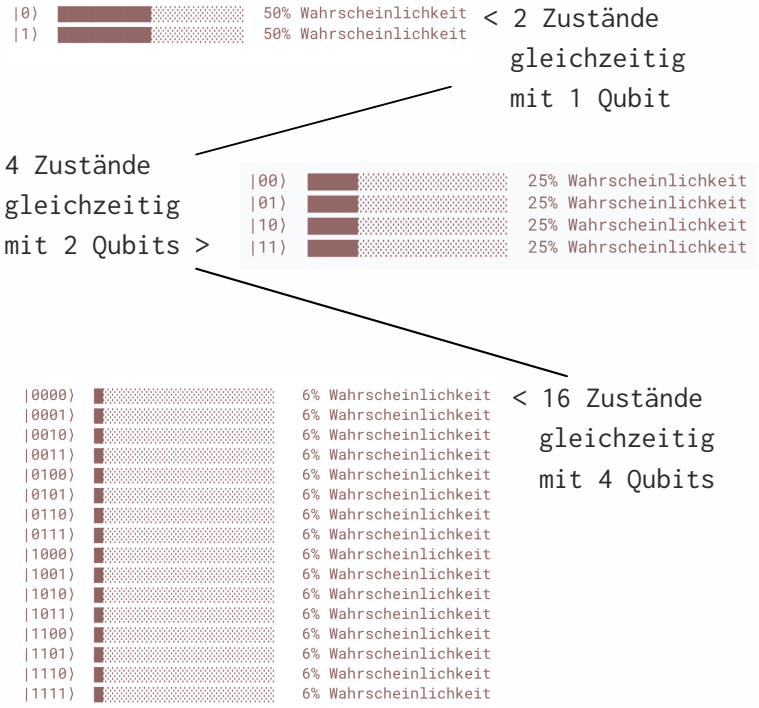
> Quantencomputer nutzen spezielle Quantengatter, um den Zustand von Qubits zu manipulieren.

Der Vorteil von Quantencomputern für bestimmte Probleme zeigt sich, wenn wir uns ansehen, wie viele Informationen wir mit n Qubits potenziell speichern und verarbeiten können.

Während ein klassischer Computer mit n Bits nur einen Zustand darstellen kann, kann ein Quantencomputer mit n Qubits 2^n Zustände gleichzeitig repräsentieren, wobei jedem Zustand eine bestimmte Wahrscheinlichkeit zugeordnet ist.



Ein Computer mit 2 Bits kann beispielsweise im Zustand 10 sein, also die Zahl 2 repräsentieren. Ein Quantencomputer mit 2 Qubits in einer Superposition kann als 00, 01, 10 und 11 gemessen werden, also mit bestimmten Wahrscheinlichkeiten die Zahlen 0,1,2 und 3 gleichzeitig repräsentieren.



Mit 2 Qubits lassen sich so zunächst schon 4 Zustände gleichzeitig darstellen, bei 3 Qubits erhöht sich diese Zahl auf 8 und bei 4 Qubits sind es sogar 16. Schon mit 300 Qubits kann man mehr Zustände gleichzeitig darstellen als es Teilchen im Universum gibt.

Erstaunlich oder? n Qubits können also 2^n Zustände gleichzeitig darstellen.

Messen können wir aber trotzdem nur einen dieser Zustände. Daher brauchen wir clevere Algorithmen, die die Besonderheiten von Qubits nutzen und dafür sorgen, dass das richtige Messergebnis aus diesen 2^n Zuständen sehr wahrscheinlich wird. Mit den richtigen Algorithmen könnten Quantencomputer dann eben unter anderen auch in der Erforschung neuer Medikamente und Impfstoffe, bei der Verkehrsoptimierung oder bei der Entwicklung von KI-Lösungen helfen.

Wir erinnern uns: Algorithmen geben an, welche Gatter zu welchem Zeitpunkt auf welche Qubits angewendet werden.

Aber wir erinnern uns: Nicht alle Probleme können durch Quantencomputer effizienter gelöst werden. Der normale Taschenrechner etwa, kann von Superposition und Verschränkung nicht profitieren.

Moderne Quantencomputer verfügen aktuell über gut 50 bis 70 Qubits. 50 bis 70 Qubits klingt schonmal nicht schlecht! Aber in der Praxis reicht es nicht nur, eine große Anzahl von Qubits zu haben, sondern ihr Zustand muss auch über einen möglichst langen Zeitraum gehalten werden können. Daran scheitern moderne Quantencomputer (noch) und sind so bisher kaum praxistauglich.

! Zum Schluss: Schaffst du es, bei 4 Qubits eine gleichmäßige Superposition aller 16 Zuständen erzeugen? Wie viele Gatter benötigst du dafür mindestens?

Deine Antwort:

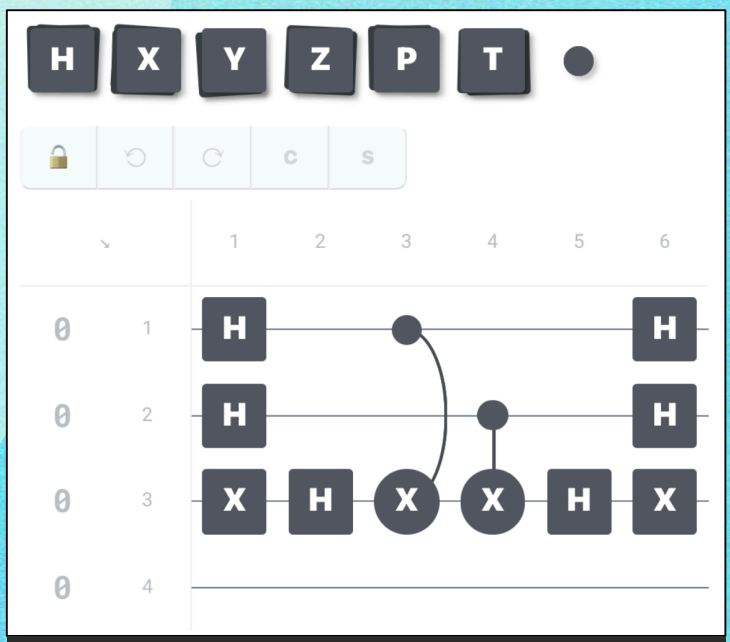
Anzahl Gatter

SIMULATION VON QUANTEN-COMPUTERN

Solange man sich nur Quantencomputer mit wenigen Qubits ansieht, können diese auch mit auf einem Computer simuliert (d.h. ihr Verhalten nachgeahmt) werden.

Auch du hast auf den vergangenen Seiten einen simulierten Quantencomputer verwendet, den du samt praktischen Drag&Drop-Editor einfach über deinen Browser aufrufen konntest.

Dabei haben wir aber noch längst nicht alle Funktionalitäten erkundet. Wenn du Lust hast, findest du auf der Seite eine Version mit zusätzlichen Funktionalitäten zum Ausprobieren..



Der Simulator verfügt noch über weitere Gatter, die über den Fokus dieses Hefts hinausgehen.

SCAN

interaktive Version

Es gibt noch weitere Tools, mit denen du Quantenalgorithmen erforschen kannst.

> Es gibt Anbieter, bei denen kannst du deine entwickelten Algorithmen bzw. Schaltkreise sogar auf realen Quantencomputern laufen lassen.

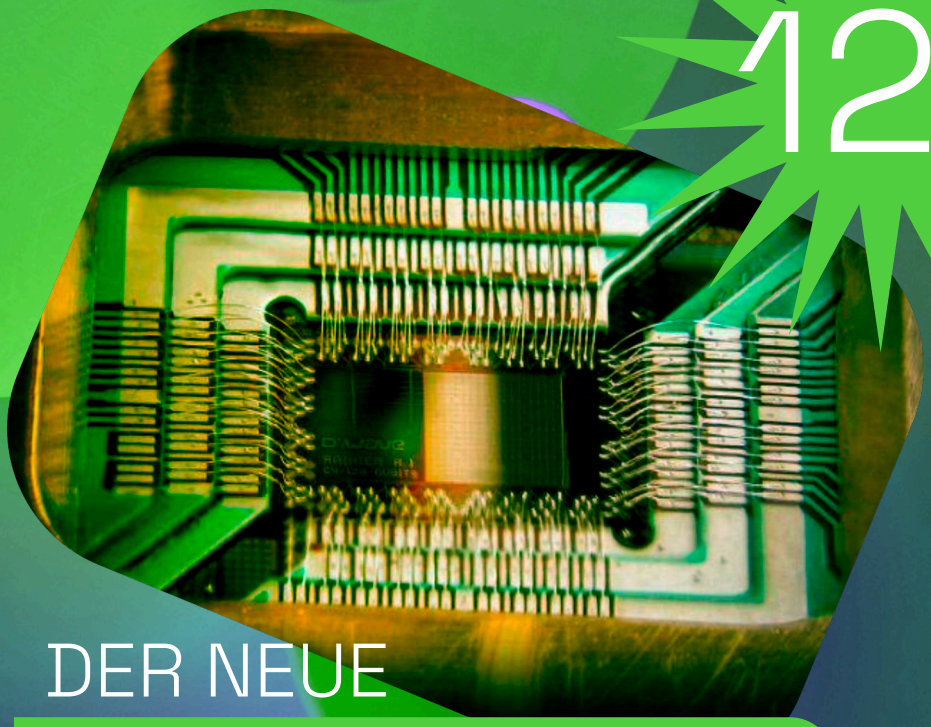
> Auf https://algassert.com/quirk hast du die Möglichkeit, auch komplexere Algorithmen auszuprobieren. Der Editor hat deutlich mehr Möglichkeiten, ist aber auch deutlich komplexer in der Bedienung.

> Falls du dir ansehen möchtest, wie man Quantencomputer in einer textuellen Programmiersprache programmiert, kannst du einen Blick auf https://qiskit.org/ werfen.

TALOS
COMPUTING INC

UNFASSBAR. SCHNELL.

ab 12,– ₿



DER NEUE
talos COMPUTING QC IV

50% MEHR LEISTUNG
ALS DER VORGÄNGER

128 Qubits // leise // sofort lieferbar

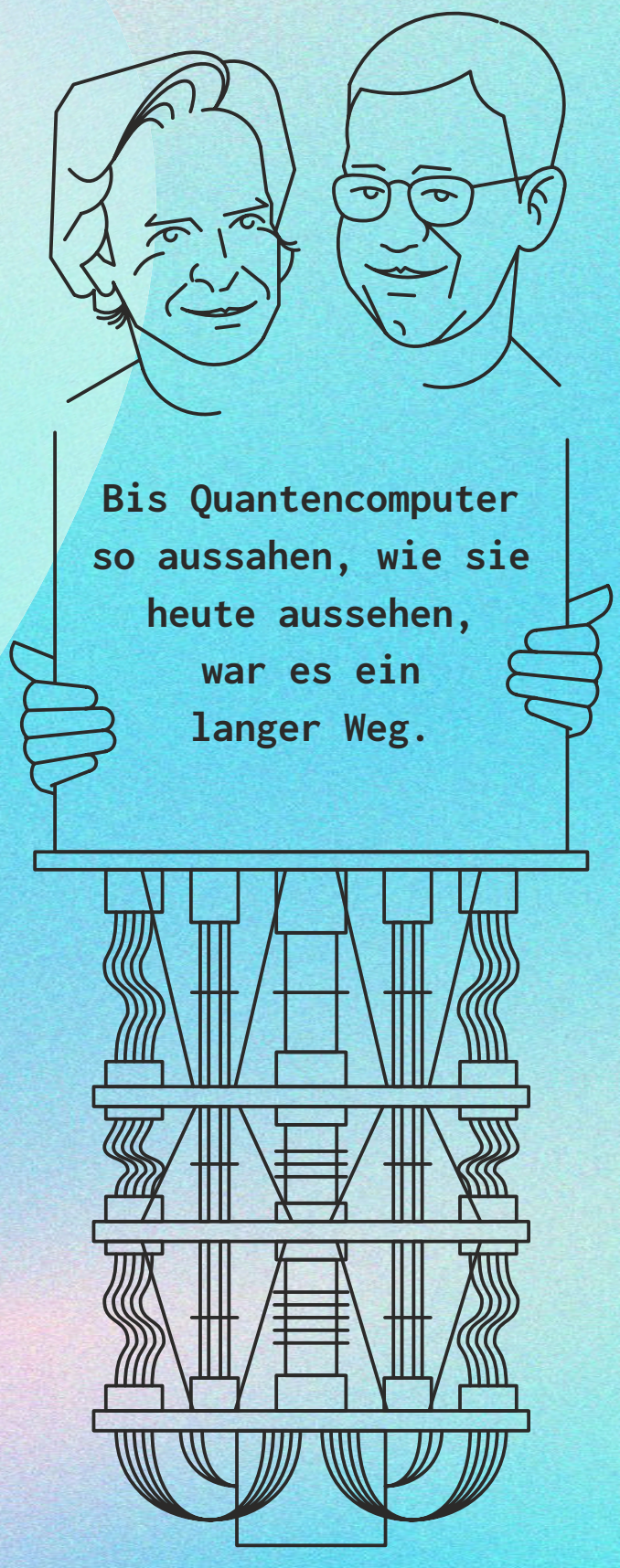
ENTWICKLUNGSPFADE DER QUANTENINFORMATIK

Diese Seite führt dich zurück zu den Anfängen der Quanteninformatik.

Dazu müssen wir noch kurz einige Physiker nennen, die wertvolle Vorarbeiten für die Forschung an der Quanteninformatik geleistet haben. Anfang des 20. Jahrhunderts fanden Physiker nämlich heraus, dass die bislang seit Newton bekannten und akzeptierten Gesetze der klassischen Physik für sehr, sehr kleine Teilchen wie Photonen (Lichtteilchen) nicht mehr greifen. Für diese kleinen Teilchen, die Quanten, musste eine neue Theorie her: Die Quantenmechanik. Mit ihr ließen sich Phänomene wie Superposition oder Verschränkung doch erklären.

Für mehrere Jahrzehnte hatte das Thema außerhalb der Physik kaum Relevanz.

In den 80er Jahren – Computer wurden immer leistungsfähiger, waren aber dennoch nicht im Stande, einfache Moleküle zu simulieren – kamen Richard Feynmann und David Deutsch die Idee, dass man einen Computer konstruieren müsste, der - genau wie Moleküle - nicht den Newtonschen Gesetzen der klassischen Mechanik, sondern denen der Quantenmechanik folgen sollte ... Leichter gesagt als getan. Auch wenn wir dem Ziel heute näher sind als damals, ist noch einiges zu tun. Ein paar wichtige Meilensteine auf diesem Weg haben wir auf der rechten Seite zusammengetragen.



Im Bild zu sehen sind die Silhouetten von Richard Feynman und Paul Benioff.

MEILENSTEINE DER ENTWICKLUNG DER QUANTENINFORMATIK

um 1980 Wissenschaftler wie Richard Feynman oder Paul Benioff skizzieren erste Visionen eines Quantencomputers.

1984 Charles Bennett und Gilles Brassard schlagen ein mit Qubits arbeitendes Verfahren zum sicheren Austausch von kryptografischen Schlüsseln, die zum sicheren Austausch von Nachrichten wichtig sind, vor (mehr dazu auf S. 38).

1985 David Deutsch zeigt, wie sich das Konzept der Turingmaschine (ein theoretisches Modell eines Computers) ins Quantenreich übertragen lässt und dass sich jede Turingmaschine auf einem Quantencomputer simulieren lässt – d.h. das, was mit einem herkömmlichen Computer möglich ist, ist theoretisch auch auf einem Quantencomputer machbar.

1992 David Deutsch und Richard Jozsa entwickeln den ersten Quantenalgorithmus, der zeigt, dass Quantencomputer effizienter als herkömmliche Computer arbeiten können (mehr dazu auf S. 43).

1994 Peter Shor entwickelt einen Quantenalgorithmus zur Primfaktorzerlegung, der in der Theorie deutlich schneller ist als ein Algorithmus für herkömmliche Computer. Die richtige Hardware vorausgesetzt, kann dieser Algorithmus einen großen Teil der Verschlüsselung im Internet knacken.

1996 Lov Grover stellt einen Quantenalgorithmus zur Suche in unsortierten Datenbanken vor – auch dieser ist deutlich schneller als der schnellste Algorithmus für herkömmliche Computer.

1998 Wissenschaftler der Oxford University stellen den ersten Quantencomputer der Öffentlichkeit vor. Dieser verfügt über zwei Qubits.

2001 Shors Algorithmus wird zum ersten Mal auf einem Quantencomputer mit sieben Qubits durchgeführt.

2005 Forscher schaffen es, einen Quantencomputer mit acht Qubits herzustellen.

2011 Zum ersten Mal wird ein Quantencomputer auch kommerziell angeboten.

2019-2020 Die ersten Forscherinnen und Forscher verkünden das Erreichen der Quantenüberlegenheit: Quantencomputer hätten es erstmals geschafft, eine schwere Aufgabe, für die ein herkömmlicher Computer unglaublich lange brauchen würde, in akzeptabler Zeit zu lösen.

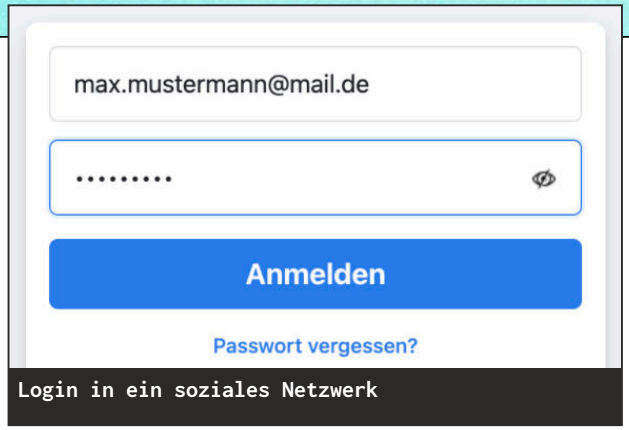
2021 Der erste Quantencomputer steht in Deutschland.

AKTIVITÄT 3.1

Datenübertragung im Netz.

Ein weiteres Anwendungsgebiet, das von der Quanteninformatik beeinflusst wird, ist der sichere Austausch von Nachrichten, zum Beispiel von unserem Computer zu Hause zum Server unserer Bank oder beim Chatten.

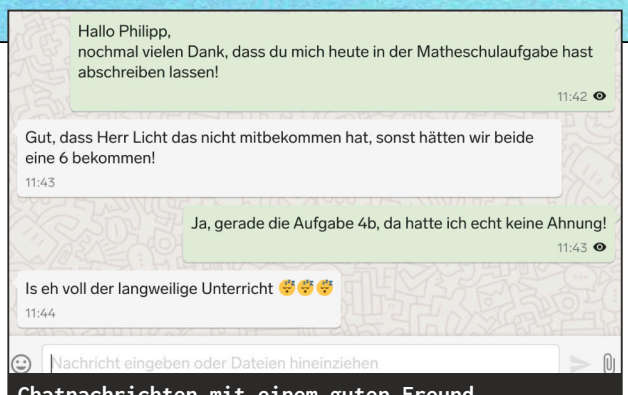
Schau dir die fünf Abbildungen an. Welche privaten Daten werden hier übermittelt? Warum sind diese Daten schützenswert? Was könnte ein Dritter damit anstellen? Halte deine Gedanken neben den Bildern fest!



Login in ein soziales Netzwerk

Private Daten:

Möglicher Missbrauch:



Chatnachrichten mit einem guten Freund

Private Daten:

Möglicher Missbrauch:

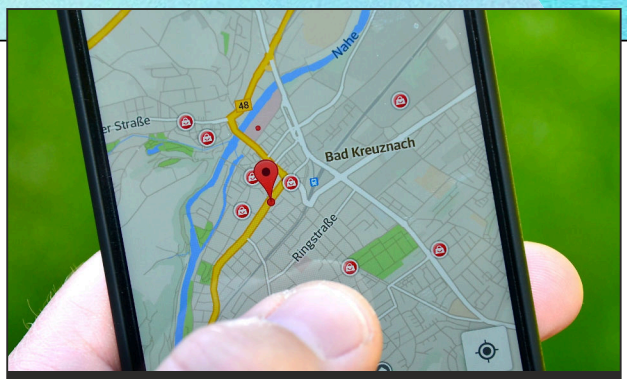
Einkauf in einem Online-Shop

Private Daten:

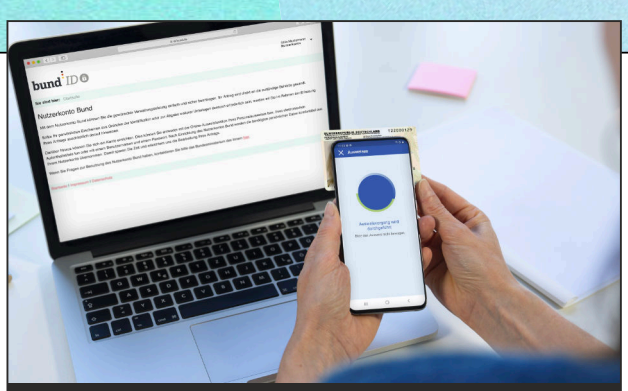
Möglicher Missbrauch:

Private Daten:

Möglicher Missbrauch:



Kartendienst auf dem Smartphone

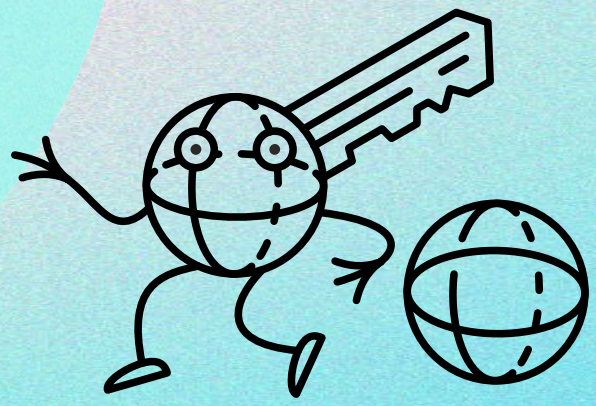


Online-Identifikation mit Personalausweis (© Bundesministerium des Innern, für Bau und Heimat)

Private Daten:

Möglicher Missbrauch:

VERSCHLÜSSELUNG IM QUANTEN-ZEITALTER



Immer wenn sensible Informationen (z. B. private Nachrichten, Kreditkartendaten oder sogar Staatsgeheimnisse) über das Internet übertragen werden, haben alle Beteiligten großes Interesse daran, sicherzustellen, dass nur berechtigte Personen die Informationen erhalten. Sonst könnte ja ein Fremder z. B. auf unser Konto zugreifen und sich bedienen. Deshalb ist es notwendig, alle Daten, die über das Internet gesendet werden, zu verschlüsseln. Ein verschlüsselter Datenverkehr stellt sicher, dass nur Sender und Empfänger die Nachricht lesen können.

Die Verschlüsselung beruht darauf, dass Sender und Empfänger einen geheimen Schlüssel teilen und diesen zum Ver- und Entschlüsseln von Nachrichten verwenden. Da niemand sonst den geheimen Schlüssel hat, kann auch niemand sonst die Nachrichten verstehen. Dieser Ansatz hat aber eine Schwachstelle: Es wird ein sicherer Kanal benötigt, um den geheimen Schlüssel erstmal auszutauschen (ansonsten könnte jemand anderes den geheimen Schlüssel mitbekommen und man kann sich die Verschlüsselung gleich sparen). Aber wenn man den sicheren Kanal hätte, müsste man ja eigentlich gar nicht verschlüsseln….

Was wir brauchen, ist eine Möglichkeit, den geheimen Schlüssel über einen unsicheren Kanal (einen, in dem theoretisch jeder mitlesen kann) auszutauschen. Im Internet lautet die Lösung hierfür Public-Key-Kryptografie: Eine Person (nennen wir sie Alice) erstellt zwei Schlüssel, einen sogenannten privaten und einen öffentlichen Schlüssel. Alice kann dann den öffentlichen Schlüssel an jeden auf der Welt weitergeben, behält aber den privaten Schlüssel für sich. Jeder andere, sagen wir Bob, der eine private Nachricht an Alice senden möchte, muss seine Nachricht mit dem öffentlichen Schlüssel verschlüsseln, den Alice erzeugt hat.

Das Besondere an dieser Art der Verschlüsselung ist, dass nur der private Schlüssel von Alice die Nachricht entschlüsseln kann, die mit dem öffentlichen Schlüssel von Alice verschlüsselt wurde. Auf diese Weise kann nur Alice die Nachricht von Bob lesen. Da niemand sonst den privaten Schlüssel von Alice besitzt, kann auch niemand sonst Bobs Nachricht lesen.

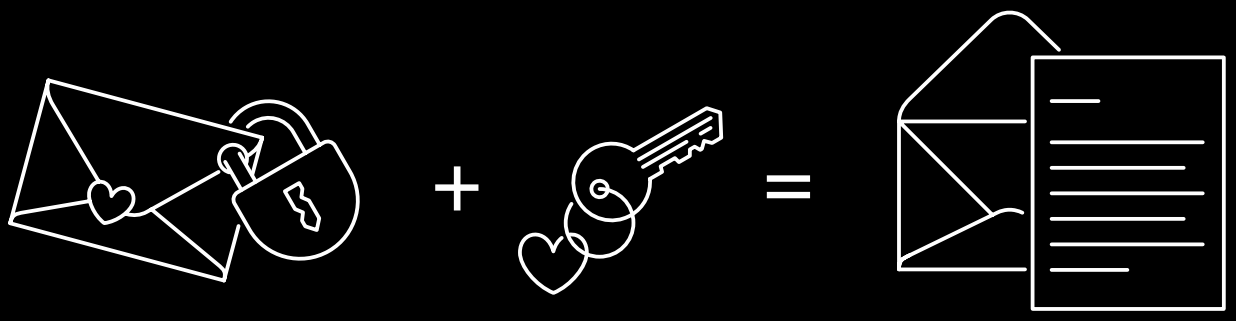
Dieses Verfahrens beruht auf der Annahme, dass niemand es bisher schafft, den privaten Schlüssel aus dem öffentlichen

Schlüssel zu rekonstruieren. Die Sicherheit des Nachrichtenaustauschs im Internet basiert also auf dem Prinzip, dass die eine Richtung sehr leicht (nämlich die Bestimmung des öffentlichen Schlüssels aus dem privaten Schlüssel), die andere (nämlich die Bestimmung des privaten Schlüssels aus dem öffentlichen) sehr schwer zu berechnen ist. Das hast du bereits in Aktivität 1 erfahren: Zwei gegebene (Prim-)Zahlen zu multiplizieren ist sehr einfach. Andersrum ist es bislang aber unmöglich, in angemessener Zeit eine große Zahl in ihre Primfaktoren zu zerlegen.

Wie bereits angesprochen, könnten Quantencomputer dieses Sicherungssystem obsolet machen. Denn der lange unmögliche Vorgang der Zerlegung einer sehr großen Zahl in ihre Primfaktoren würde, genügend Qubits vorausgesetzt, in kürzester Zeit möglich sein. Kurz gesagt, man könnte ganz einfach aus dem öffentlichen Schlüssel von Alice den privaten Schlüssel von Alice berechnen. Und jeder kann lesen, was die beiden für sich behalten wollten.

Höchste Zeit also, sich über Verschlüsselungsverfahren Gedanken zu machen, die trotz - oder gerade wegen - Quantencomputern absolut sicher sind.

Als erstes wollen wir uns jetzt einen Kandidaten für so ein Verschlüsselungs-verfahren ansehen, das One-Time-Pad.



Bobs Nachricht, verschlüsselt für Alice | **privater Schlüssel von Alice** | **Bobs Nachricht, wieder im Klartext**

Das mit dem öffentlichen und privaten Schlüssel kann man sich mithilfe von Vorhängeschlössern erklären: Wenn wir ein offenes Vorhängeschloss an unsere Freunde geben und den Schlüssel für uns behalten, können andere das Schloss nutzen, um eine Schatulle (oder ein Kuvert) mit Nachrichten an uns zu verschließen. Da niemand außer uns einen Schlüssel hat, kann auch niemand anderes die Schatulle (oder das Kuvert) öffnen.

AKTIVITÄT 3.2

Das One-Time-Pad.

VERSION ALICE

Am besten, bearbeitest du die folgenden Seiten mit einer Person, die ebenfalls dieses Heft hat. Du übernimmst die Rolle der Senderin, Alice. Achte darauf, dass die andere Person die Version Bob dieser Aufgabe hat. Falls du alleine dran arbeitest, haben wir dir Münzwurfergebnisse und die Nachrichten eines fiktiven Gesprächspartners auf S. 60 in den Anhang gepackt.

Schlüsselerzeugung

Einigt euch auf einen gemeinsamen Schlüssel. Werft dazu eine Münze 8 mal, wobei Kopf = 0 und Zahl = 1 ist. Trage den gemeinsamen Schlüssel hier ein!

Gemeinsamer Schlüssel

Verschlüsselung

1. Gehe nun an einen Ort, wo niemand sieht, was du aufschreibst. Wähle dann einen Buchstaben, den du versenden möchtest, und notiere ihn hier:

2. Der Buchstabe soll nun deine Nachricht sein. Nutze nun den Auszug aus der ASCII-Tabelle (rechts), um deine Nachricht binär (also mit 0en und 1en) zu kodieren:

Binär kodierte Nachricht

3. Vergleiche deine binär kodierte Nachricht nun Zeichen für Zeichen mit dem gemeinsamen Schlüssel. Dabei gilt: 0&0 → 0, 0&1 → 1, 1&0 → 1 und 1&1 → 0. (z.B. gemeinsamer Schlüssel: 0110, binär kodierte Nachricht: 0101 → verschlüsselte Nachricht: 0011):

Verschlüsselte Nachricht

4. Trage deine verschlüsselte Nachricht zusätzlich in das Feld am Ende dieser Seite ein und schneide den Abschnitt ab, um deine Nachricht an die andere Person zu schicken.

Alices Nachricht an Bob

Verschlüsselte Nachricht

Entschlüsselung

1. Notiere die verschlüsselte Nachricht, die du erhalten hast:

Verschlüsselte Nachricht von Bob

2. Entschlüssle die Nachricht genau so, wie du sie verschlüsselt hast:

Entschlüsselte Nachricht von Bob

2. Welchen Buchstaben hat man dir geschickt?

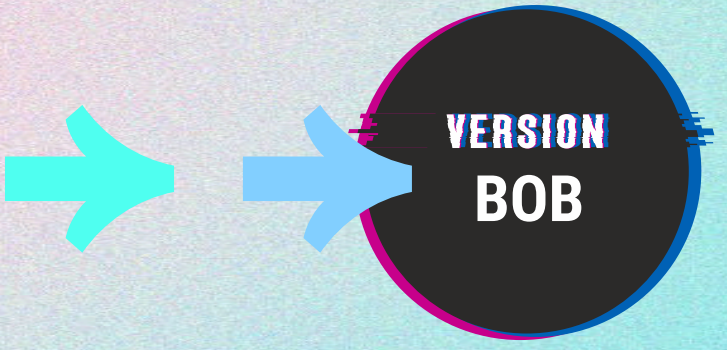
Auszug aus ASCII-Tabelle

Da Computer nur mit binären Codes arbeiten, müssen wir Buchstaben auch als Binärcode ausdrücken. Diese Übersetzung wurde wie folgt festgelegt.

Buchstabe	Binärcode	Buchstabe	Binärcode
A	01000001	N	01001110
B	01000010	O	01001111
C	01000011	P	01010000
D	01000100	Q	01010001
E	01000101	R	01010010
F	01000110	S	01010011
G	01000111	T	01010100
H	01001000	U	01010101
I	01001001	V	01010110
J	01001010	W	01010111
K	01001011	X	01011000
L	01001100	Y	01011001
M	01001101	Z	01011010

AKTIVITÄT 3.2

Das One-Time-Pad.



Am besten, bearbeitest du die folgenden Seiten mit einer Person, die ebenfalls dieses Heft hat. Du übernimmst die Rolle des Empfängers, Bob. Achte darauf, dass die andere Person die Version Alice dieser Aufgabe hat. Falls du alleine dran arbeitest, haben wir dir Münzwurfergebnisse und die Nachrichten eines fiktiven Gesprächspartners auf S. 60 in den Anhang gepackt.

Schlüsselerzeugung

Einigt euch auf einen gemeinsamen Schlüssel. Werft dazu eine Münze 8 mal, wobei Kopf = 0 und Zahl = 1 ist. Trage den gemeinsamen Schlüssel hier ein!

Gemeinsamer Schlüssel

Verschlüsselung

1. Gehe nun an einen Ort, wo niemand sieht, was du aufschreibst. Wähle dann einen Buchstaben, den du versenden möchtest, und notiere ihn hier:

2. Der Buchstabe soll nun deine Nachricht sein. Nutze nun den Auszug aus der ASCII-Tabelle (rechts), um deine Nachricht binär (also mit 0en und 1en) zu kodieren:

Binär kodierte Nachricht

3. Vergleiche deine binär kodierte Nachricht nun Zeichen für Zeichen mit dem gemeinsamen Schlüssel. Dabei gilt: 0&0 → 0, 0&1 → 1, 1&0 → 1 und 1&1 → 0. (z.B. gemeinsamer Schlüssel: 0110, binär kodierte Nachricht: 0101 → verschlüsselte Nachricht: 0011):

Verschlüsselte Nachricht

4. Trage deine verschlüsselte Nachricht zusätzlich in das Feld am Ende dieser Seite ein und schneide den Abschnitt ab, um deine Nachricht an die andere Person zu schicken.

Bobs Nachricht an Alice

Verschlüsselte Nachricht

Entschlüsselung

1. Notiere die verschlüsselte Nachricht, die du erhalten hast:

Verschlüsselte Nachricht von Alice

2. Entschlüssle die Nachricht genau so, wie du sie verschlüsselt hast:

Entschlüsselte Nachricht von Alice

2. Welchen Buchstaben hat man dir geschickt?

Auszug aus ASCII-Tabelle

Da Computer nur mit binären Codes arbeiten, müssen wir Buchstaben auch als Binärcode ausdrücken. Diese Übersetzung wurde wie folgt festgelegt.

Buchstabe	Binärcode	Buchstabe	Binärcode
A	01000001	N	01001110
B	01000010	O	01001111
C	01000011	P	01010000
D	01000100	Q	01010001
E	01000101	R	01010010
F	01000110	S	01010011
G	01000111	T	01010100
H	01001000	U	01010101
I	01001001	V	01010110
J	01001010	W	01010111
K	01001011	X	01011000
L	01001100	Y	01011001
M	01001101	Z	01011010

Lauschangriff

Nun hast die die Grundlagen des One-Time-Pad-Verschlüsselungsverfahrens kennengelernt, es ist theoretisch unknackbar. Die folgenden Fragen sollen dir helfen, zu verstehen, warum das Verfahren so sicher ist. Nutze die Fragen als Orientierungshilfe, im Feld unten kannst du dir Notizen machen. Wenn möglich, diskutiere deine Überlegungen mit einer weiteren Person oder innerhalb der Klasse.

1. Angenommen, du fängst die Nachricht 10110010 ab. Welche Möglichkeiten siehst du, die ursprüngliche Nachricht wiederherzustellen?

2. Wie viele verschiedene Schlüssel müsstest du ausprobieren?

3. Wie viele verschiedene Schlüssel müsstest du ausprobieren, wenn die Nachricht 5 Buchstaben hätte?

4. Du fängst eine Nachricht mit 5 Buchstaben ab und findest zufällig einen Schlüssel, der die Nachricht entschlüsselt, sodass sie HALLO lautet. Welche anderen Wörter wären möglich?

Notizen

Fragen zur Diskussion

1. Warum lässt sich die ursprüngliche Nachricht durch Hinzufügen des Schlüssels wiederherstellen?

2. Warum ist das One-Time-Pad theoretisch unknackbar?

3. Welche praktischen Probleme seht ihr beim Einsatz des One-Time-Pads?

Notizen

#INFORMATIK 2038

Die Gesellschaft für Informatik lädt zur größten europäischen Informatik-Konferenz ein. Erleben Sie spannende Vorträge!

Ralf Romeike und Stefan Seegerer berichten in einer interaktiven, historischen Reise aus der Zeit, als Informatikunterricht noch nicht ab der ersten Klasse unterrichtet wurde und - unvorstellbar - als es oftmals noch keine ausreichenden Computer in den Schulräumen gab! VR-Brille einschalten!

> Luise Müller, Chief Engineer bei CO2-Limit-Solutions, spricht über die neueste Generation der gesteuerten CO2 Absorption, die sie und ihr Team erfolgreich weltweit einsetzen.

> Code via Mind: Das Team rund um Benno Schnitzler lädt zum Mind-Coding ein: Programmieren ohne jedes Tool, einfach mittels Mind-to-Code-Cap.

Berlin // VR-Room // 15.-17.09.2038

AKTIVITÄT 3.3

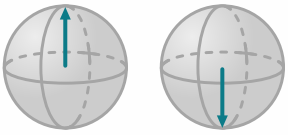
BB84 – der Quanten-schlüsseltausch.

VERSION ALICE

Sicher verschlüsseln können wir jetzt, aber um das One-Time-Pad für sichere Kommunikation verwenden zu können, müssen beide Gesprächspartner über denselben Schlüssel verfügen. Bei dem Erzeugen eines gemeinsamen Schlüssels ohne sich persönlich zu treffen, kann jetzt die Quanteninformatik helfen. Aber wie?

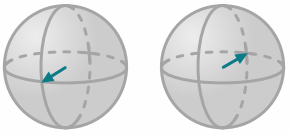
Das wollen wir uns am Schlüsselaustauschprotokoll BB84 anschauen. Für die Übertragung sind nun jedoch Qubits als Informationsträger nötig. Alice als Senderin kann die Ausrichtung der Kugel festlegen und so den Bit-Wert des Schlüssels in der Ausrichtung der Qubits kodieren. Genau wie wir bei klassischen Bits, Strom an als 1 und Strom aus als 0 festgelegt haben, kann Alice festlegen, wie die Ausrichtung als klassisches Bit interpretiert werden muss (wir sprechen hier auch von einer Basis). Eine Möglichkeit wäre es, wie bisher die Position oben als 0 und die Position unten als 1 zu interpretieren, genauso lassen sich aber auch vorne als 0 und hinten als 1 festlegen.

Das BB84-Verfahren wurde 1984 von Bennett und Brassard vorgeschlagen.



0 1

Alice kann sich entscheiden 0 und 1 als oben und unten **ODER** als vorne und hinten zu kodieren



0 1

Quantenschlüsseltausch ohne Eve (Lauscherin)

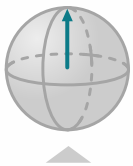
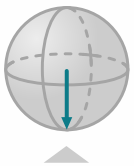
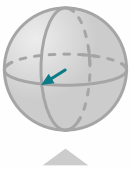
Du sendest eine Nachricht an Bob. Um 0 und 1 darzustellen, kannst du entweder die Positionen oben und unten oder die Positionen vorne und hinten verwenden.

1. Wähle zufällig, ob du die Information über oben/unten (⇅) oder vorne/hinten (⇄) kodiert übermitteln willst (man nennt das auch Basis). Trage dazu zufällig ⇅ oder ⇄ ins erste freie Feld der ersten Zeile der Tabelle ein.

2. Das Qubit, das du an Bob schickst, kodiert entweder 0 oder 1. Wirf dazu erneut die Münze (Kopf ist 0, Zahl ist 1) und notiere das Ergebnis im ersten freien Feld der zweiten Zeile der Tabelle.

3. Gib dann die richtige Karte (Karten zum Ausschneiden: S.57) verdeckt an Bob weiter. Welche das ist, verrät dir die Grafik rechts.

4. Wiederhole das Vorgehen (1-3) für die nächsten 7 Zeichen des Schlüssels.

	0	1
Oben/unten (⇅)		
Vorne/hinten (⇄)		

5. Wenn du die Tabelle vollständig ausgefüllt hast, teile Bob mit, ob du die Zeichen des Schlüssels in der Basis oben/unten (⇅) oder vorne/hinten (⇄) kodiert hast. Wenn Bob dir sagt, dass du ein Zeichen "verwerfen" sollst, streiche die Spalte in der Tabelle durch.

⇅/⇄								
0/1								

6. Übertrage die nicht durchgestrichenen 0er und 1er der Reihe nach in das Feld gemeinsamer Schlüssel. Überprüfe dann, ob du den gleichen Schlüssel wie Bob hast.

Gemeinsamer Schlüssel

Quantenschlüsseltausch mit Eve (Lauscherin)

Diese Aufgabe lässt sich nicht alleine durchführen. Und auch wenn ihr zu zweit seid, sucht euch eine dritte Person, die in die Rolle von Eve schlüpft (Arbeitsblatt Eve, siehe S. 59).

1. Du bist weiterhin in der Rolle von Alice. Wiederhole das Vorgehen, gib die Karte aber diesmal zuerst an Eve.

⇅/⇄								
0/1								

Gemeinsamer Schlüssel:

Gemeinsamer Schlüssel

2. Vergleicht dann die gemeinsamen Schlüssel nacheinander. Wie lässt sich feststellen, ob Eve die Nachricht abgefangen hat?

Notizen

AKTIVITÄT 3.3

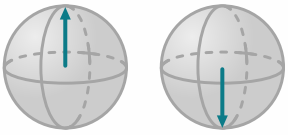
BB84 – der Quanten-schlüsseltausch.

VERSION BOB

Sicher verschlüsseln können wir jetzt, aber um das One-Time-Pad für sichere Kommunikation verwenden zu können, müssen beide Gesprächspartner über denselben Schlüssel verfügen. Bei dem Erzeugen eines gemeinsamen Schlüssels ohne sich persönlich zu treffen, kann jetzt die Quanteninformatik helfen. Aber wie?

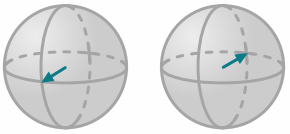
Das wollen wir uns am Schlüsselaustauschprotokoll BB84 anschauen. Für die Übertragung sind nun jedoch Qubits als Informationsträger nötig. Alice als Senderin kann die Ausrichtung der Kugel festlegen und so den Bit-Wert des Schlüssels in der Ausrichtung der Qubits kodieren. Genau wie wir bei klassischen Bits, Strom an als 1 und Strom aus als 0 festgelegt haben, kann Alice festlegen, wie die Ausrichtung als klassisches Bit interpretiert werden muss (wir sprechen hier auch von einer Basis). Eine Möglichkeit wäre es, wie bisher die Position oben als 0 und die Position unten als 1 zu interpretieren, genauso lassen sich aber auch vorne als 0 und hinten als 1 festlegen.

Das BB84-Verfahren wurde 1984 von Bennett und Brassard vorgeschlagen.



0 1

Alice kann sich entscheiden 0 und 1 als oben und unten **ODER** als vorne und hinten zu kodieren



0 1

Quantenschlüsseltausch ohne Eve (Lauscherin)

Du empfängst eine Nachricht von Alice. Um 0 und 1 darzustellen, kann Alice entweder die Positionen oben und unten oder die Positionen vorne und hinten verwenden.

1. Wähle zufällig, ob du die Information über oben/unten (⇅) oder vorne/hinten (⇄) messen willst (man nennt das auch Basis). Trage dazu zufällig ⇅ oder ⇄ ins erste freie Feld der ersten Zeile der Tabelle ein.

2. Nimm die Karte von Alice entgegen und drehe sie um. Notiere dann passend 0 bzw. 1 in der dafür vorgegebene Zeile entsprechend folgender Regeln:

> Wenn du dich für dieselbe Basis wie Alice entschieden hast, notiere den entsprechenden Wert des übertragenen Bits.

> Wenn du in der anderen Basis gemessen hast, wähle zufällig 0 oder 1 (Münzwurf!).

Empfangene Karte / Deine Messung				
⇅	0	1	zufällig 0 oder 1	zufällig 0 oder 1
⇄	zufällig 0 oder 1	zufällig 0 oder 1	0	1

3. Wiederhole das Vorgehen (1-2) für die nächsten 7 Bits.

4. Wenn du die Tabelle vollständig ausgefüllt hast, wird Alice dir mitteilen, ob sie die Zeichen des Schlüssels in der Basis oben/unten (⇅) oder vorne/hinten (⇄) kodiert hat. Wenn du in einer anderen Basis gemessen hast als das Zeichen kodiert wurde, sag ihr, dass sie das Zeichen "verwerfen" soll. Streiche die Spalte außerdem in deiner Tabelle durch.

⇅/⇄								
0/1								

6. Übertrage die nicht durchgestrichenen 0er und 1er der Reihe nach in das Feld gemeinsamer Schlüssel. Überprüfe dann, ob du den gleichen Schlüssel wie Alice hast.

Gemeinsamer Schlüssel

Quantenschlüsseltausch mit Eve (Lauscherin)

Diese Aufgabe lässt sich nicht alleine durchführen. Und auch wenn ihr zu zweit seid, sucht euch eine dritte Person, die in die Rolle von Eve schlüpft (Arbeitsblatt Eve, siehe S. 59).

1. Du bist weiterhin in der Rolle von Bob. Wiederhole das obige Vorgehen, du wirst die Karte aber diesmal von Eve erhalten.

⇅/⇄								
0/1								

Gemeinsamer Schlüssel:

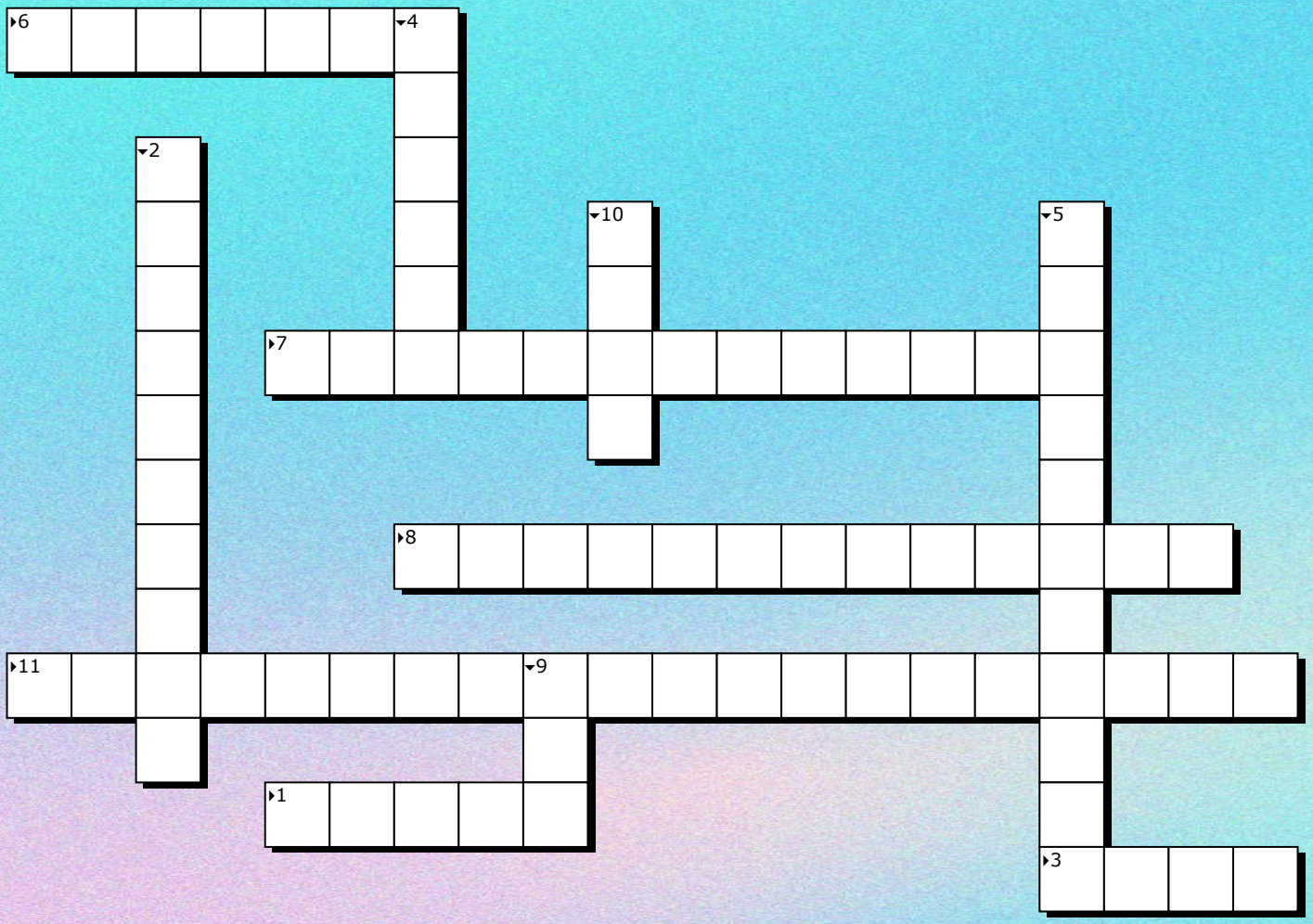
Gemeinsamer Schlüssel

2. Vergleicht dann die gemeinsamen Schlüssel nacheinander. Wie lässt sich feststellen, ob Eve die Nachricht abgefangen hat?

Notizen

Knobelecke

1. Informationsträger in einem Quantencomputer
2. Unknackbares Verschlüsselungsverfahren (ohne Bindestriche)
3. Erfinder des Algorithmus zur Faktorisierung von Primzahlen mit Quantencomputern: Peter …
4. Verändern den Zustand von Qubits
5. Eindeutige Handlungsvorschrift zur Lösung eines Problems
6. Zerstört eine Superposition
7. Die Eigenschaft zweier Qubits, dass bei Kenntnis des Werts des einen Qubits der Wert des anderen ebenso feststeht
8. Zustand eines Qubits, in dem eine gewisse Wahrscheinlichkeit (>0%) besteht, 0 bzw. 1 zu messen
9. Informationsträger in einem herkömmlichen Computer
10. Anzahl der mit 3 Qubits gleichzeitig darstellbaren Zustände
11. Zeitpunkt, ab dem Quantencomputer eine Aufgabe in akzeptabler Zeit lösen kann, die ein herkömmlicher Computer nicht lösen kann



AKTIVITÄT 4

Quantenüberlegenheit – der Deutsch-Jozsa Algorithmus.

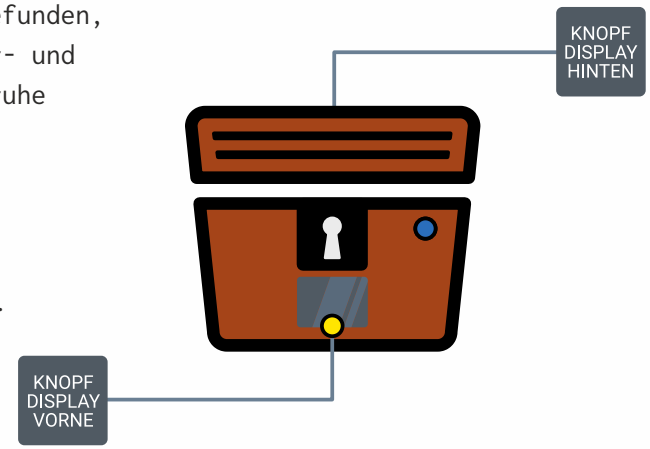
HIER SELBST AUSPROBIEREN

Wir haben bereits gesehen, dass Quantencomputer mit Qubits rechnen. Ein Vorteil der Qubits ist die Möglichkeit, Superpositionszustände anzunehmen. Für Aufgaben wie die Addition zweier Zahlen haben Quantencomputer dabei keine Vorteile gegenüber herkömmlichen Computern. Aber bei manchen Aufgaben sind diese Superpositionszustände sehr hilfreich und beschleunigen Berechnungen ungemein. Die dabei angewendeten Quantenschaltkreise können allerdings sehr kompliziert werden. Trotzdem können wir die Quantenüberlegenheit an einem einfachen Beispiel verstehen.

Stellt euch vor, wir haben eine antike Kiste gefunden, die drei verschiedene Knöpfe und auf der Vorder- und Rückseite einen Bildschirm hat. Man kann die Truhe öffnen, wenn man angibt, ob beide Bildschirme denselben Inhalt anzeigen.

> Der erste Knopf aktiviert den Bildschirm auf der Vorderseite und zeigt eine `0` oder `1` an.

> Der zweite Knopf aktiviert den Bildschirm auf der Rückseite und zeigt eine `0` oder `1` an.



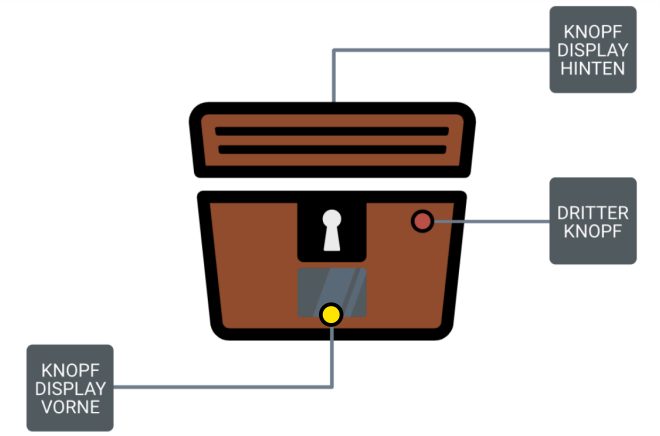
└ Diese Schaltfläche aktiviert den Knopf für das vordere Display

! Eigentlich ganz einfach oder? Probiere es einmal aus, indem du online die Knöpfe in der obigen Grafik anklickst! Zeigen beide Displays dieselbe Zahl oder unterschiedliche Zahlen?

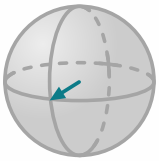
Knifflig wird es allerdings, wenn wir nur einen Knopf drücken dürfen.

! Probiere es einmal aus, indem du einen der beiden Knöpfe der zweiten Grafik online anklickst! Kannst du noch herausfinden, ob beide Display dieselbe Zahl oder unterschiedliche Zahlen zeigen?

Zum Glück gibt es noch einen **dritten Knopf**: Der dritte Knopf wechselt in den Quantenmodus und führt eine Quantenoperation auf einem Qubit aus, die wir uns im Folgenden anschauen möchten.

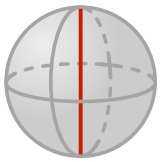


Unser Qubit ist zuerst im Zustand `0`, das heißt, es zeigt auf den Nordpol der Zustandskugel.



Im zweiten Schritt wenden wir ein Hadamard-Gatter an, das du aus Aktivität 2.3 kennst.

Nun kommt der Quantentrick: Der dritte Knopf dreht für jede `1`, die auf der Kiste gezeigt wird, um 180° an der Achse zwischen Nord- und Südpol. Daraus ergeben sich folgende Möglichkeiten:



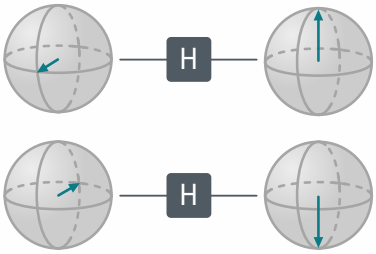
> Falls beide Bildschirme eine `1` zeigen würden, wird das Qubit um $2 \cdot 180° = 360°$ gedreht (360° entspricht auch 0°).

> Falls beide eine `0` zeigen würden, wir das Qubit um 0° gedreht.

> Falls das vordere Display eine `1` und das hintere eine `0` zeigen würde, wird das Qubit um 180° gedreht.

> Falls das vordere Display eine `0` und das hintere eine `1` zeigen würde, wird das Qubit um 180° gedreht.

Es zeigt sich, dass das Qubit "nach vorne zeigt", falls beide Display die gleiche Zahl anzeigen würden. Würden beide Displays unterschiedliche Zahlen anzeigen, zeigt das Qubit nach der Drehung "nach hinten".

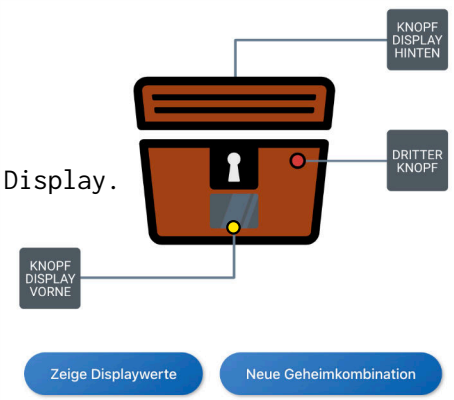


Nun kommt erneut das Hadamard-Gatter `H` zum Einsatz.

Nach Anwendung des Hadamard-Gatters ergeben sich damit die folgenden zwei finalen Zustände:

> Falls das Qubit nach vorne zeigt (und damit beide Displays die gleichen Zahlen zeigen würden), zeigt das Qubit nach Anwendung von Hadamard nach oben und wir erhalten das Messergebnis 0 auf einem dritten Display.

> Falls das Qubit nach hinten zeigt (und damit beide Displays unterschiedliche Zahlen zeigen würden), zeigt das Qubit nach Anwendung von Hadamard nach unten und wir erhalten das Messergebnis 1 auf einem dritten Display.



! Probiere nun den Quantenmodus der Truhe aus! Wie viele Werte musst du auslesen, um die Truhe zu öffnen (also zu entscheiden, ob beide Displays dieselbe Zahl anzeigen)?

Verrückt, oder? Während man bei unserem Beispiel mit der Truhe mit einem herkömmlichen Computer 2 Werte eingeben und das Ergebnis überprüfen muss, um zu wissen, ob beide Displays gleiche oder unterschiedliche Werte anzeigen, muss mit Quantencomputern nur ein Wert eingegeben und überprüft werden. Es geht aber noch beeindruckender: Wenn wir nicht nur auf der Vorder- und Rückseite einen Bildschirm haben, sondern auf jeder Seite einen Bildschirm haben, funktioniert der Quantentrick auch. Das heißt, es muss immer noch nur ein Wert eingegeben und überprüft werden. Es muss dann allerdings um 60° gedreht werden.

Das, was wir uns hier anhand einer geheimnisvollen Truhe überlegt haben, heißt in der Welt der Quanteninformatik Deutsch-Jozsa-Algorithmus. Dort geht es darum, herauszufinden, ob eine Funktion f, die lediglich ein Bit als Eingabe entgegennimmt, konstant (also f(0)=f(1)) oder balanciert ist (also f(0)≠f(1)). Während der Algorithmus bei einem herkömmlichen Computer mit den beiden Eingaben 0 und 1 aufgerufen werden muss (f(0) wäre dann das Ergebnis auf dem vorderen und f(1) das auf dem hinteren Display), reicht es im Quantenfall, die Funktion f nur einmalig mit einer Superposition aus 0 und 1 aufzurufen (so, wie es bei der Truhe mit dem dritten Knopf möglich war). Der Deutsch-Josza-Algorithmus ist das einfachste Beispiel, das aufzeigt:

Quantencomputer können bestimmte aber nicht alle Probleme effizienter lösen als klassische Computer.

Den Zeitpunkt, ab dem ein Quantencomputer eine Aufgabe in akzeptabler Zeit lösen kann, die ein herkömmlicher Computer nicht (oder nicht in akzeptabler Zeit) lösen kann, nennen wir auch **Quantenüberlegenheit**. 2019 haben Wissenschaftlerinnen und Wissenschaftler diese zum ersten Mal ausgerufen: Ihr Computer löste ein eigens für ihn geschaffenes Problem (das in der Praxis allerdings absolut nutzlos ist) in ungefähr drei Minuten. Ein wirklich schneller herkömmlicher Computer hätte nach Aussagen der Wissenschaftlerinnen und Wissenschaftler um die 10.000 Jahre dafür gebraucht. Bis die Quantenüberlegenheit bei praxisnahen Problemen erreicht werden kann, dürfte es aber noch ein bisschen dauern.

AKTIVITÄT 5

Anwendungen von Quantencomputern.

Quantenalgorithmen wie der von Peter Shor zum Finden von Primfaktoren einer Zahl funktionieren ähnlich wie der Algorithmus von Deutsch. Auch wenn die praktische Anwendbarkeit von Quantenalgorithmen bislang beschränkt ist, erwarten Expertinnen und Experten, dass sie zukünftig bei einer ganzen Reihe von Problemstellungen Einsatz finden können. Verbesserungen verspricht man sich vor allem bei rechenintensiven Problemen, die von herkömmlichen Computern nicht in akzeptabler Zeit gelöst werden können. Dazu gehören unter anderem die folgenden Einsatzbereiche.

Simulation von Molekülen: Bei der Entwicklung und Erforschung neuer pharmazeutischer Wirkstoffe gilt es immer wieder Simulationen mit den beteiligten Molekülen durchzuführen, z. B. um die Wechselwirkungen verschiedener Wirkstoffe zu prüfen und diese so zu optimieren. Aktuell muss der Aufbau der Moleküle dafür stark vereinfacht werden, um sie auf klassischen Computern berechnen zu können. Mit Quantencomputern würden diese Vereinfachungen wegfallen und die Moleküle könnten mit all ihren Eigenschaften simuliert werden. Statt für die Erforschung der Wirkstoffe von Medikamenten könnten die Verfahren auch zur Optimierung von Materialeigenschaften (wie etwa bei Batterien) eingesetzt werden.

Optimierungen in Verkehr und Logistik: Ein weiterer Bereich, in dem sich Wissenschaftlerinnen und Wissenschaftler Fortschritte durch Quantencomputer versprechen, ist die Beschleunigung von Optimierungsproblemen, wie sie beispielsweise in Verkehr und Logistik auftreten. Ziel der Forscherinnen und Forscher ist es, auch bei erhöhtem Verkehrsaufkommen die Routen aller Autos so zu optimieren, dass Staus gänzlich vermieden werden können. Auch die effiziente Verteilung von Gütern beispielsweise für die Fertigung von Autos könnte mithilfe von Quantencomputern optimiert werden.

Maschinelles Lernen beschleunigen: Maschinelles Lernen ist ein Bereich der künstlichen Intelligenz, in dem Computer aus großen Datenmengen lernen. Quantencomputer versprechen gegenüber herkömmlichen Computern eine noch größere Menge an Daten in derselben Zeit verarbeiten zu können. Die Algorithmen des Maschinellen Lernens lassen sich für Quantencomputer so anpassen, dass Datensätze in einem einzigen Schritt verarbeitet und so Muster in Daten entdeckt werden können, die herkömmliche Computer nicht in akzeptabler Zeit finden würden.

Neben diesen Anwendungen, die bereits jetzt erforscht werden, werden sich in Zukunft viele weitere finden. Auch die sichere Kommunikation durch quantenkryptographische Verfahren wie BB84 bietet spannende Zukunftsperspektiven und kann bereits heute realisiert werden.

Was würdest du mit Quantencomputern machen wollen? Notiere deine Prioritäten basierend auf den Beispielen auf der linken Seite und einer Internetrecherche. Diskutiere deine Ideen mit einem Freund oder einer Freundin.

Nach aktuellem Stand sind Quantencomputer eher dazu bestimmt, herkömmliche Computer zu ergänzen, nicht aber dazu, sie zu ersetzen. Wir erwarten also nicht, in absehbarer Zeit ein Quantensmartphone in der Hand zu halten. Aber darüber, ob das irgendwann anders sein wird, lässt sich aktuell nur spekulieren. Wir dachten ja auch mal, dass das mit dem Internet nicht so interessant für die breite Öffentlichkeit wird ;)

AKTIVITÄT 6

Zurück ~~in die~~ aus der Zukunft.

Natürlich wissen wir nicht, wie die Welt im Jahr 2038 aussieht. Aber wir können uns eine eigene Vision erarbeiten, wie die Welt im Jahr 2038 aussehen könnte.

Dazu ist ein Blick in die Geschichte hilfreich.

1. Informiere dich im Internet: Wie sahen Computer und Telefone in den 1970er Jahren aus? Halte deine Erkenntnisse in Stichworten fest!

Notizen

2. Informiere dich im Internet: Wie sahen Computer und Telefone Anfang der 2000er Jahre aus? Halte deine Erkenntnisse in Stichworten fest!

Notizen

3. Wirf einen Blick auf Videos, die die Welt in den Jahren 2000-2020 zeigen (sollen), aber deutlich vorher gedreht wurden. Schau dir die Videos an und mache dir Notizen.

> Welche Ähnlichkeiten zur Gegenwart fallen dir auf?
> Welche Unterschiede zur Gegenwart stellst du fest?
> Welche Vorhersagen sind so eingetreten?
> Welche Vorhersagen sind zumindest ähnlich eingetreten?
> Welche Vorhersagen stimmten so nicht?

Notizen

Technologie hat sich in den letzten Jahren und Jahrzehnten rasant entwickelt und vieles verändert, von dem wir nicht gedacht hätten, dass es sich verändert. Vielleicht ist es im Jahr 2038 möglich, Staus vollständig abzuschaffen, weil auf Quantencomputern berechnete Verkehrsmodelle den selbstfahrenden Autos optimale Routen vorschlagen. Vielleicht finden wir – dank neuer Simulationsmöglichkeiten auf Quantencomputern – Materialien, die extrem robust, aber trotzdem umweltfreundlich sind. Niemand weiß, wie die Zukunft aussehen wird. Science-Fiction-Filme zeigen uns eine Vision, wie die Zukunft aussehen könnte. Aber Science-Fiction-Autorinnen und Autoren haben vor allem eines, eine blühende Fantasie.

Die Zukunft ist aber noch nicht geschrieben. Vielleicht trifft eine dieser Visionen genau so ein, wie sie vorhergesagt wurde. Vielleicht trifft sie sogar ein, weil du dich entschieden hast, sie umzusetzen? Du bist in der Lage, diese Zukunft mitzugestalten!

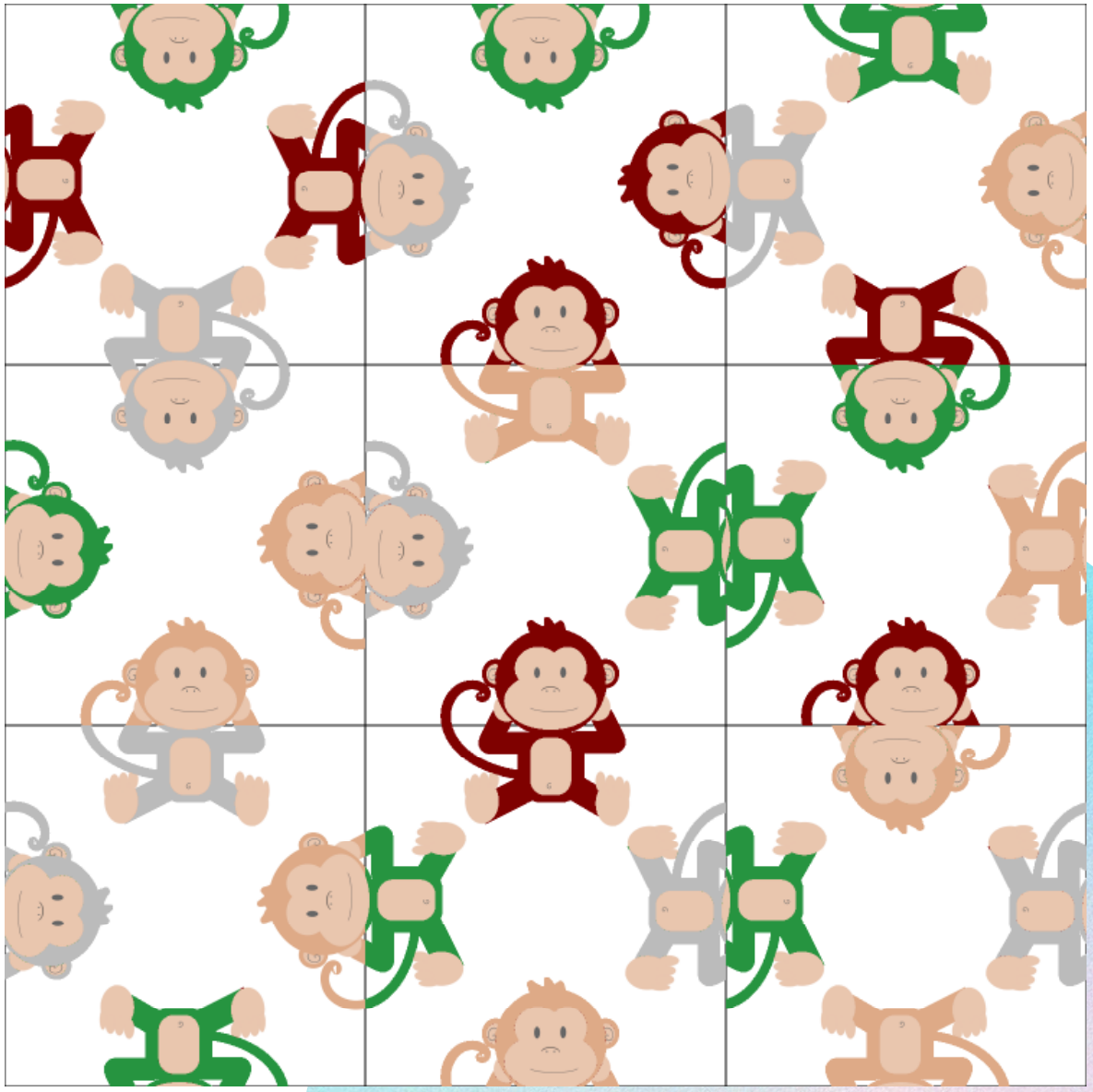
4. Wie stellst du dir die Zukunft vor? Nutze die nachfolgende Doppelseite, um deine Vision der Zukunft zu skizzieren (z.B. mit Bildern oder als Mind-Map). Welche Rolle spielen in dieser Zukunft die Quantencomputer?

NOTIZEN

Du kannst diese Seite für deine Notizen nutzen.

AKTIVITÄT 1

Zum Ausschneiden.

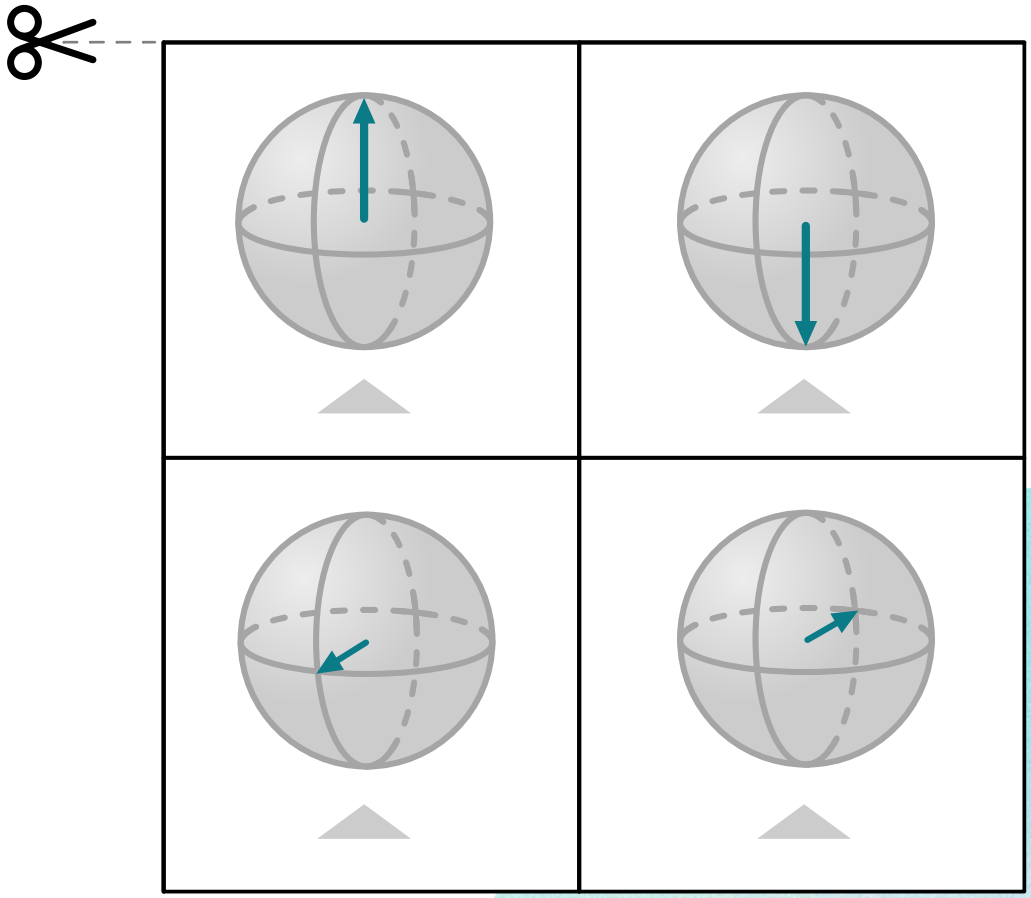


Diese Seite wurde absichtlich freigelassen.

Diese Seite wurde absichtlich freigelassen.

AKTIVITÄT 3

Zum Ausschneiden.



Diese Seite wurde absichtlich freigelassen.

AKTIVITÄT 3.3

BB84 – der Quanten-schlüsseltausch.

VERSION EVE

Quantenschlüsseltausch ohne Eve (Lauscherin)

Um zu erfahren, wie Alice und Bob einen geheimen Schlüssel vereinbaren, beobachte zuerst wie Alice vorgeht, um die ersten 4 Qubits an Bob zu senden. Beobachte dann, wie Bob vorgeht, wenn er die letzten 4 Qubits empfängt. Notiere, welche Informationen beide öffentlich austauschen!

Ausgetauschte Informationen

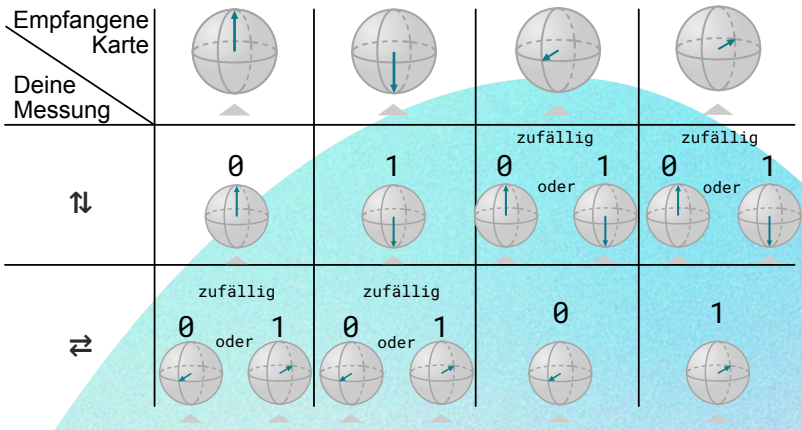
Quantenschlüsseltausch mit Eve (Lauscherin, also mit dir!)

1. Wähle zufällig, ob du die Nachrichten von Alice mit der Basis über oben/unten (⇅) oder vorne/hinten (⇄) messen willst. Trage dazu zufällig ⇅ oder ⇄ ins erste freie Feld der ersten Zeile der Tabelle ein.

2. Nimm die Karte von Alice entgegen und drehe sie um.

> Wenn deine Basis mit der auf der Karte übereinstimmt, notiere den Bitwert in der Zeile 0/1 und gib sie an Bob weiter.

> Wenn deine Basis eine andere ist, wähle zufällig eine Karte passend zu deiner Basis, notiere den Bitwert und gib die Karte an Bob weiter.



3. Wiederhole das Vorgehen (1-2) für die nächsten 7 Bits.

4. Lausche, wie Alice und Bob ihre Basen vergleichen. Wenn Bob sagt, dass Alice das Bit "verwerfen" soll, streiche es auch in deiner Tabelle durch.

⇅/⇄								
0/1								

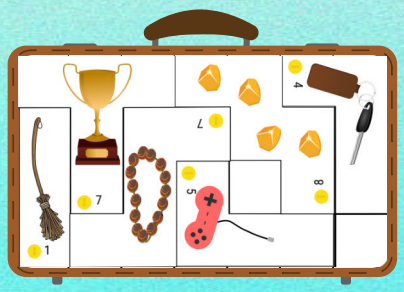
5. Die nicht durchgestrichenen Zahlen sind dein abgefangener Schlüssel. Trage diesen rechts ein.

Abgefangener Schlüssel

5. Vergleiche den von dir abgefangenen Schlüssel mit Alices und Bobs Schlüssel. War der Lauschangriff erfolgreich?

Lösungen

Aktivität 1:
Kofferproblem: Es ist möglich, 6 Gegenstände im Wert von 32 Münzen einzupacken.
Vielleicht hast du es ja geschafft, noch wertvollere Gegenstände einzupacken?

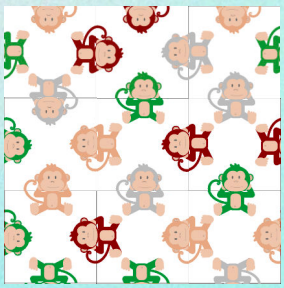


Buchstabengitter:

A	G	B	F	I	F	E	M	B	Q	W	X
X	I	T	M	P	K	B	Y	T	E	E	H
Z	N	S	H	E	S	M	E	O	Y	K	J
F	T	T	A	S	T	A	T	U	R	Z	U
A	E	W	R	I	M	S	D	F	E	K	E
T	R	I	D	E	B	R	O	W	S	E	R
E	N	T	W	E	T	C	U	H	T	L	B
S	E	T	A	S	O	F	T	W	A	R	E
S	T	E	R	I	S	T	A	M	M	T	X
G	U	F	E	S	T	P	L	A	T	T	E
H	S	E	E	G	Q	O	X	L	P	M	M
P	R	X	I	M	K	B	S	Y	A	X	Z

Ein Byte ist übrigens die Menge von 8 Bit und wird auch als Größenangabe für Festplatten oder Arbeitsspeicher verwendet, etwa als MB (Megabyte) oder GB (Gigabyte).

Affenpuzzle:



Zahlen multiplizieren:
$7 \cdot 9 = 63$, $19 \cdot 23 = 437$, $57 \cdot 97 = 5529$
Ganz einfach klappt es mit der schriftlichen Multiplikation:

$$\begin{array}{r} 19 \cdot 23 \\ \hline 380 \\ +\ 57 \\ \hline 437 \end{array}$$

Zwei natürliche Zahlen finden:
Hier bleibt nicht viel über außer ausprobieren. Die Lösungen lauten: $169 = 13 \cdot 13$, $289 = 17 \cdot 17$, $1147 = 31 \cdot 37$

Aktivität 2:
Lösungen gibt's online auf https://www.stefanseegerer.de/reise-in-die-quantenzeit/curriculum01.html

Aktivität 3.2:

Münzwurfergebnisse und Nachrichten von Bob:

Kopf	Zahl	Zahl	Zahl	Kopf	Zahl	Kopf	Kopf
Münzwurfergebnisse							

0	0	1	1	0	1	0	0
Verschlüsselte Nachricht von Bob							

Falls du mit den obigen Nachrichten gearbeitet hast, lautet die Nachricht von Bob A.

Lauschangriff:
1. Ein erster Gedanke könnte das Ausprobieren möglicher Schlüssel sein.
2. Bei dieser Nachricht müssen allerdings sehr viele Schlüssel ausprobiert werden, nämlich alle Schlüssel mit Länge 8, das sind 256, da wir pro

Stelle 2 Möglichkeiten (0 oder 1) haben.
3. Dann wären es sogar noch mehr Möglichkeiten: Bei 5 Buchstaben brauchen wir Schlüssel mit der Länge 5 · 8 = 40 Schlüssel (für einen Buchstaben benötigen wir 8 Bit). Daraus ergeben sich dann 2^{40} = 1.099.511.627.776 mögliche Schlüssel, die alle durchprobiert werden müssten.
4. Hier wären tatsächlich alle Wörter mit 5 Buchstaben möglich. Die Entschlüsselung mit Hallo war also reiner Zufall.

Fragen zur Diskussion:
1. Die ursprüngliche Nachricht lässt sich durch Hinzufügen des Schlüssels wiederherstellen, weil sie die ursprüngliche Verschlüsselungsoperation (0&0 → 0, 0&1 → 1, 1&0 → 1 und 1&1 → 0) durch erneutes Anwenden des Schlüssels umgekehrt wird: Wurde bei der Verschlüsselung eine 0 angewendet, wird jetzt wieder eine 0 angewendet und es ändert sich nichts. Bei einer 1 im Schlüssel wird der Wert hingegen wieder zurückgeändert.
2. Das One-Time-Pad ist deshalb unknackbar, weil keinerlei Information über den Schlüssel aus dem verschlüsselten Text gewonnen werden kann. Es bleibt lediglich das Ausprobieren aller möglichen Schlüssel, wobei dann allerdings auch ALLE Ausgangstexte möglich sind. Welcher die eigentliche Nachricht von Alice an Bob darstellt, wird sich so nicht herausfinden lassen.

3. Das größte Problem beim Einsatz des One-Time-Pads ist der Austausch der Schlüssel, der vor jeder Nachricht erforderlich ist. Dafür ist ein sicherer Kanal erforderlich. Auch ein Schlüsseltausch über Public-Key-Kryptografie würde dafür sorgen, dass das Verfahren zumindest theoretisch knackbar ist.

Aktivität 3.3:
Münzwurfergebnisse und Nachrichten von Bob:

⇅	⇄	⇄	⇅	⇅	⇄	⇅	⇄

Zufällige Entscheidung für ⇅/⇄

Zahl	Kopf	Kopf	Zahl	Zahl	Kopf	Kopf	Zahl

Münzwurfergebnisse

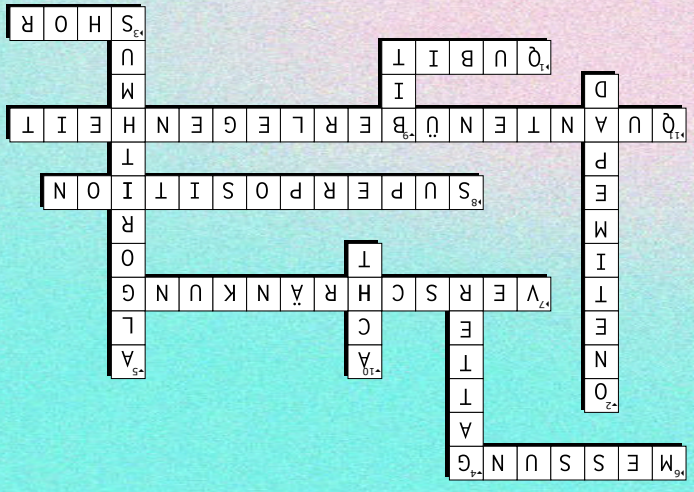
	verwerfen				verwerfen		verwerfen

Information von Bob, welche Qubits du verwerfen sollst

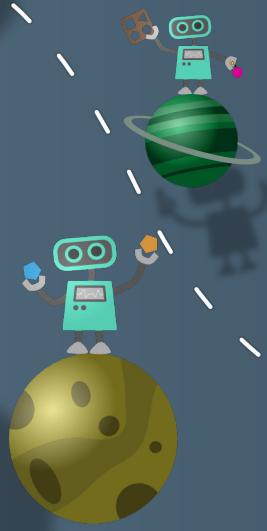
Falls du mit diesen Nachrichten gearbeitet hast, lautet der gemeinsame Schlüssel mit Bob (ohne Lauscherin): 10110

Mit Lauscherin:
Versucht sich Eve an einem Man-in-the-Middle Angriff (bei dem sie sich zwischen Alice und Bob positioniert und mit beiden kommuniziert), so wird das nicht nur nicht von Erfolg gekrönt sein, vielmehr noch wird ihr Lauschen sogar bemerkt, da Alice und Bob so unterschiedliche Schlüssel erhalten. Um die Lauscherin zu enttarnen, müssen die beiden nur einen Teil ihres Schlüssels öffentlich vergleichen. Gibt es keine Unterschiede, ist es sehr unwahrscheinlich, dass es einen Lauschangriff gab und der restliche Teil des Schlüssels kann für die verschlüsselte Kommunikation verwendet werden. Bei Abweichungen ist klar, Eve hat versucht zu lauschen! Dieses Verfahren verdeutlicht damit nicht zuletzt, dass die Fragilität von Quanteninformationen, die beim Rechnen zwar unpraktisch ist, in der Quantenkryptografie die Sicherheit garantiert.

Knobelecke:



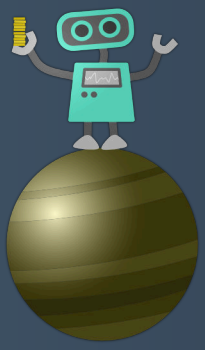
DIE WELT DER KI ENTDECKEN

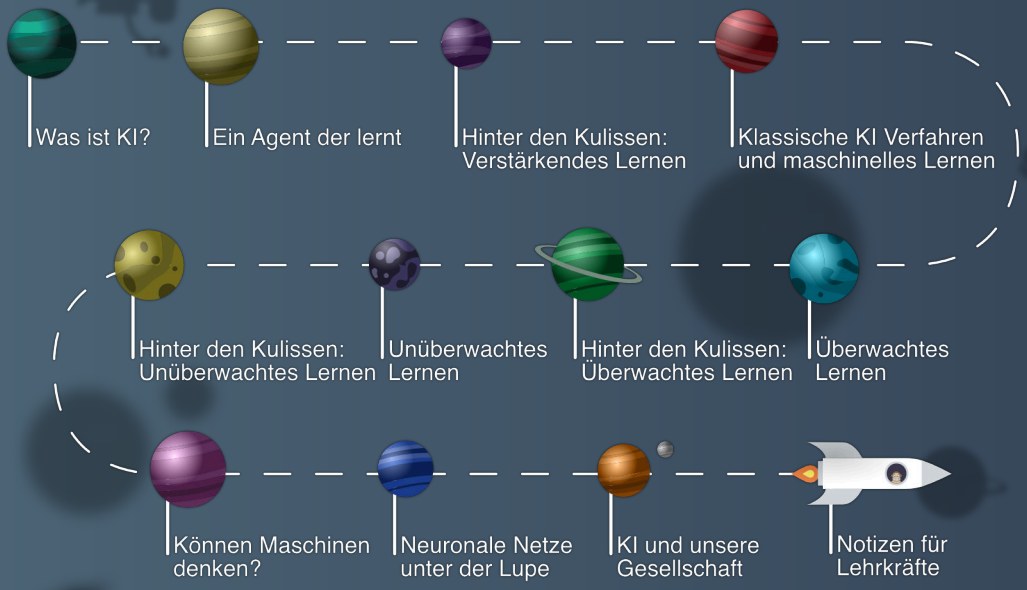


KOSTENFREIER ONLINE-KURS FÜR KI-INTERESSIERTE.

SPANNENDE MATERIALIEN UND AKTIVITÄTEN, UM KI SELBST ZU ENTDECKEN.

ÜBER 3 STUNDEN VIDEOMATERIAL, VIELE INTERAKTIVE ÜBUNGEN UND MEHR.





BEGLEITE UNS AUF UNSERER REISE

Stefan Seegerer - Tilman Michaeli

computingeducation.de

Impressum

Herausgeber
Freie Universität Berlin,
Didaktik der Informatik

Idee
Stefan Seegerer, Ralf Romeike

Konzeption und Texterstellung
Stefan Seegerer, Andreas Woitzik,
Ralf Romeike

Redaktion und Gestaltung
Stefan Seegerer, Denis Rockmann

Danksagung/Mitarbeit
Julian Dorn, Anna Lieckfeld, Franziska Greinert, Cin Pietschmann, Sabine Tornow, Till Zoppke

Projektunterstützung
Bundesministerium für Bildung und Forschung – Förderstrang Quantum Aktiv, Gesellschaft für Informatik e.V.

Auflage
5000 Stück

Stand
September 2021

Mehr über Informatik erfährst du unter
https://computingeducation.de/

Quantenschaltkreiseditor
Aktivität 2 und 4 verwenden Code aus dem Q.js Projekt von Stewart Smith (MIT-Lizenz).

ComputingEducation
Computer science explained!

Freie Universität Berlin

GESELLSCHAFT FÜR INFORMATIK

...UND WAS ERWARTET UNS MORGEN?

KONNTEN DIE ENTLAUFENEN QUBITS WIEDER EINGEFANGEN WERDEN?

ComputingEducation

QBTSNEWS