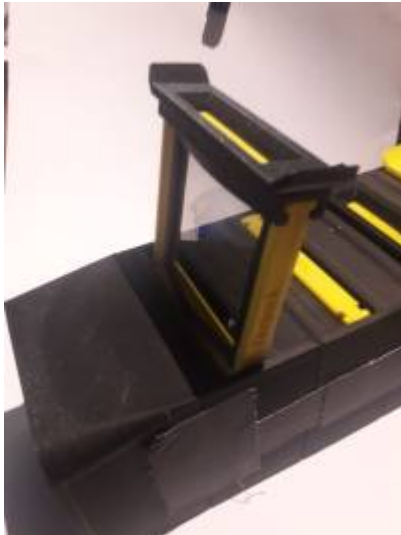


Kurzbeschreibung

Quantenverschlüsselung mithilfe von Quantencomputern ist eine der vielversprechendsten Technologien, um Bürger:innen, Unternehmen und Staaten in der Zukunft effektiv vor Cyberspionage und Cyberkriminalität zu schützen. Deshalb wird auf diesem Feld aktuell intensiv geforscht. Um den Grundgedanken und die Prozesse der Technologie anschaulich für alle Interessierten zu vermitteln, wurde die Darstellungsform eines Rätsels in einem Escape Room gewählt. Dieses nutzt die Quanteneffekte des Lichts. Bei dem Rätsel handelt es sich um eine Kammer, in die vier Polarisationsfilter eingesetzt werden können (siehe Abbildung).



An der vorderen Seite befindet sich die einzige Öffnung, durch die das Licht fallen kann. Durch die korrekte Anordnung der Polarisationsfilter werden beide Hälften der Rückwand sichtbar. Auf der einen Seite sind Benutzernamen zu sehen, während auf der anderen Seite die zugehörigen Passwörter abzulesen sind. Mithilfe von Postern im Escape Room soll die Analogie des Rätsels mit der Fähigkeit eines Quantencomputers, eine Superposition verschiedener Zustände einzunehmen sowie die damit einhergehenden Vorteile, deutlich werden.

Theorie

In diesem Experiment/Rätsel wollen wir einerseits den Fakt ausnutzen, dass Licht aus Photonen mit Quanteneffekten besteht, um eine direkte Verbindung des Rätsels zu der sonst so abstrakten Welt von Quanten aufzubauen. Desweiteren wollen wir vermitteln, dass ein Quantencomputer mehrere Zustände gleichzeitig betrachtet und bearbeitet.

Polarisationsfilter

Polarisationsfilter polarisieren Licht linear. Das bedeutet, dass die Wellen des Lichts (nahezu) alle in der selben Raumrichtung schwingen. Die Polarisation des Photon im Polarisationsfilter ist ein 2-Zustands-System. Das bedeutet, dass das Photon beim Passieren des Filters entweder in Durchlassrichtung oder in der dazu orthogonalen Sperrrichtung schwingt. Dies erfolgt durch das

Superpositionsprinzip: Ein Photon, das bsp. in einem 45° Winkel zur Durchlassrichtung des Filters auf diesen trifft wird als überlagerter Zustand aus der Durchlassrichtung und der Sperrrichtung aufgefasst, wobei beide Zustände zu einem gleichen Teil enthalten sind bzw. beide Zustände gleich wahrscheinlich gemessen werden. Dabei gilt:

$$\frac{\text{Sperrrichtung}}{\text{Durchlassrichtung}} = \tan(\theta)$$

wobei θ der Winkel des Photons zur Durchlassrichtung ist. Dies ist auch die Lichtintensität, die von bereits polarisiertem Licht an einem Filter durchgelassen wird, in Abhängigkeit des Winkels. Demnach lassen sich durch mehrere Polarisationsfilter in Folge Bilder wie dieses erzeugen:

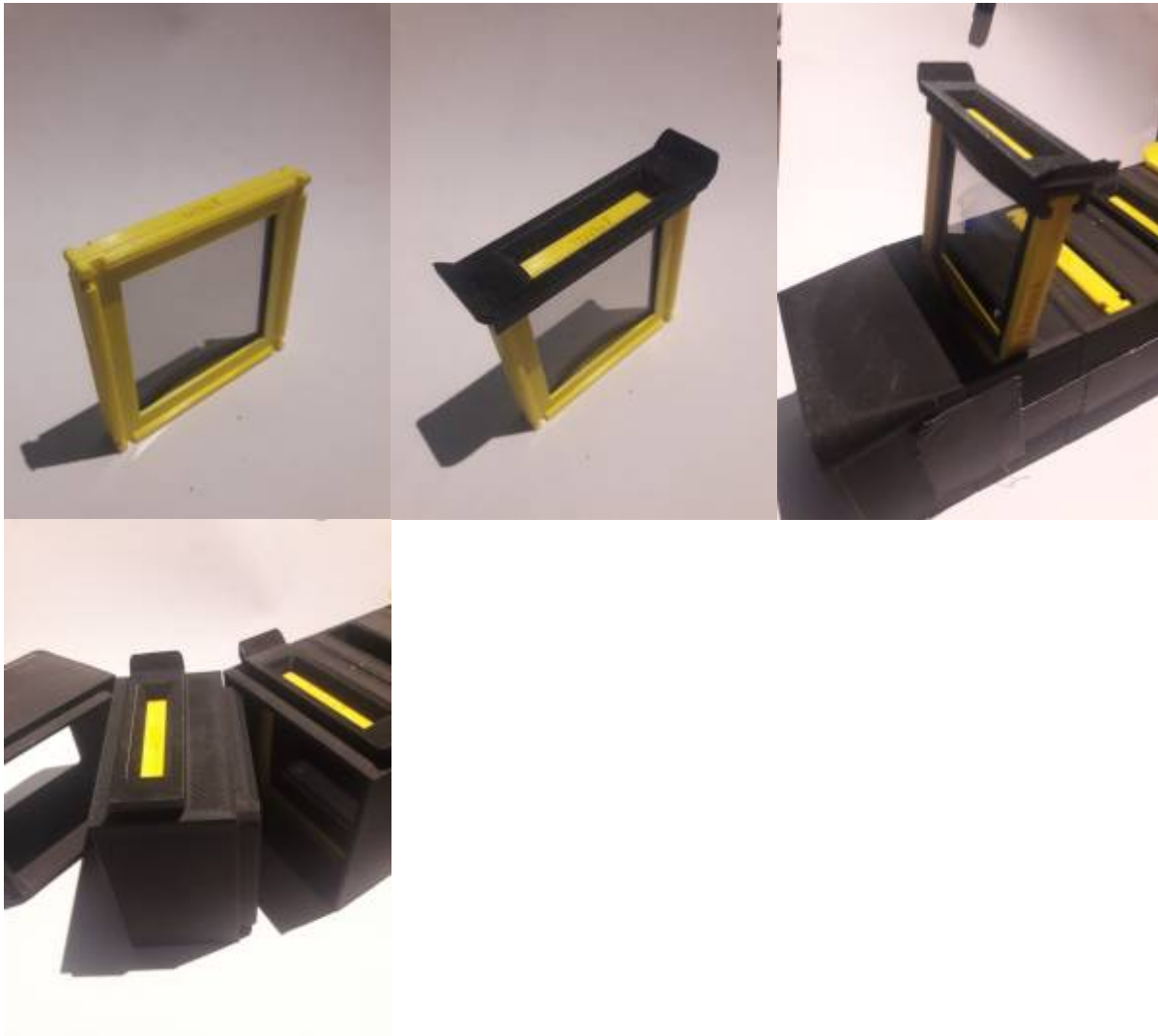


Quantencomputer

In der Realität arbeitet ein Quantencomputer mit Qubits. Diese können sich (wie gewöhnliche Bits) im Zustand 1 oder 0 / An oder aus / up oder down befinden und darüber hinaus eine Superposition beider Zustände einnehmen. Letzterer wird mit einer Wellenfunktion beschrieben, die Information über die Wahrscheinlichkeit des Messergebnisses enthält (sie beschreibt das System vollständig). Es gibt nun zwei Formen von Operationen: Messungen, die die Wellenfunktion entsprechend der in ihr enthaltenen Wahrscheinlichkeit kollabieren lassen, und Operationen, die die Wellenfunktion verändern, ohne sie kollabieren zu lassen. In jedem Fall muss jedoch zum Schluss eine Messung durchgeführt werden, um ein Ergebnis zu erhalten, das der Computer anzeigen kann. Lässt man Wellenfunktionen geschickt kollabieren, lassen sich bestimmte Probleme erheblich vereinfachen (z.B. Primfaktorzerlegung für das Brechen asynchroner Verschlüsselung). Ein Quantencomputer kann also nicht mehrere überlagerte Zustände gleichzeitig anzeigen, aber mit ihnen "rechnen". Im Moment der Ergebnismessung kollabiert der Zustand und ein Teil der Information geht verloren. Da dies jedoch sehr schwer in einem Rätsel zu vermitteln ist und wir kein Vorwissen über Quantenphysik voraussetzen wollen, kann unsere Imitation des Quantencomputers gleichzeitig zwei Zustände darstellen, während ein normaler Computer immer nur einen Zustand (die Hälfte der Lösung) anzeigen kann.

Aufbau

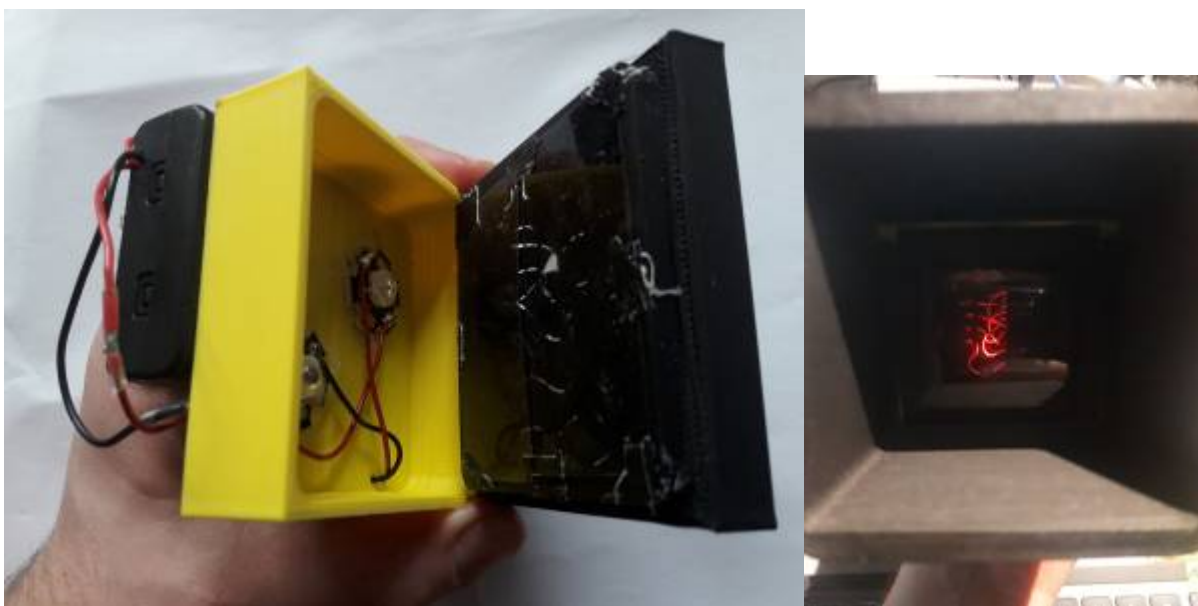
Grundsätzlich wurde der Aufbau möglichst einfach gehalten, lässt sich aber auch erweitern und auf andere/komplexere Aufgabe anpassen. Die Idee war es, eine simple Mechanik zu entwickeln, die jederzeit und überall reproduzierbar ist. So können die einzelnen Module mit einem normalen 3D Drucker erzeugt werden. Die Dateien hierzu werden dem Dokument angehängt. Die Polarisations scheiben können dann zugeschnitten in einen dafür vorgesehenen Rahmen eingeklemmt werden.



Dabei sind auf den Rahmen Markierungen, die durch ein Fenster auf der Oberseite erkennbar sind. So kann die Position (also Polarisation) der Scheibe erkannt und in das Rätsel eingebaut werden. Das „eigentliche Rätsel“, also der Teil, der nur vollständig zu erkennen ist, wenn alle Polarisations scheiben richtig eingesetzt sind, kann ebenfalls im 3D-Druck hergestellt werden. Das hier verwendete Beispiel ist allerdings qualitativ grenzwertig und benötigt eigentlich eine feinere Druckauflösung oder einen Lasercutter. Auf die Licht zugewandten Seite des Rätsels müssen außerdem zwei Filter 90° zueinander aufgebracht werden, um das Licht nach eine Polarisation auszurichten.



Das Licht, das für das Rätsel verwendet wird, kann entweder aus der Umgebung kommen - in dem Fall lässt man das letzte Modul weg - oder es kommt von einem Schluss Modul, welches als letztes hinten aufgesetzt wird und mit LEDs bestückt ist.



Dabei kann der Aufbau so erweitert werden, dass die LEDs nur dann angehen, wenn alle Scheiben eingesetzt sind. Das kann über Reed Schalter geschehen, die an der Seite des gesamten Aufbaus

angebaut werden können. Diese werden dann über Magneten in den Rahmen geschaltet.

Material

- Polarisations scheiben zum Zerschneiden
- Reedschalter
- Magneten
- Helle LEDs
- Batterie
- Draht
- 3d-Finalment
- 3D-Drucker

Wichtichtiges zum Aufbau

- Die Ausrichtung der Magneten muss so sein, dass die Reed Schalter richtig geschaltet werden, wenn die Einschübe drin sind, unabhängig von Ausrichtung der Rahmen.
- Die LEDs müssen sehr stark sein, um durch das Rätsel und alle Folien durch zukommen → je filigraner die Linien des Rätsel, desto heller sollten die LEDs sein.
- Die einzelnen Module sind nicht verbunden, nur geklemmt. Um den Aufbau richtig zu nutzen, müssen die Module fest verbunden (geklebt oder geschraubt) werden.

Poster

Um den Spieler:innen einige Hinweise mit auf den Lösungsweg zu geben, kann ein extra für dieses Rätsel designtes Poster im Escape Room angebracht werden. Das Poster weist darauf hin, dass die „Quantenerweiterung“ benötigt wird, um beide Teile des an der Rückwand des Prototypen versteckten Codes lesen zu können. Es gibt den Spielenden außerdem einige weiterbildende Informationen zu Quantencomputern allgemein.

Eine Konzeptskizze findet sich im folgenden Bild:

Superpositioning
the present &
the future

Quantum Technology

Hey, ich bin Q!
Kennst Du das auch, wenn
Dein Computer einfach zu
LANGSAM ist?

Kein Wunder!
Dein Alter muss sich
ja auch zwischen
zwei Zuständen
entscheiden!

Ein Quantencomputer
kann dank Qubits alle
Zustände gleichzeitig im
Blick behalten und so viel
SCHNELLER
rechnen - egal, ob
Wegoptimierung, Simulation oder
Verschlüsselung & Sicherheit!

Bestell Dir eine Quantenerweiterung*
und überzeuge Dich selbst!

* Eine Quantenerweiterung imitiert
nur einen Quantencomputer. Es ist
nicht möglich, einen herkömmlichen
Computer um Quantentechnologie zu erweitern

Quantum Technology

Fazit

Das aktuelle Design lässt sich leicht in ein bestehendes Escape Game integrieren, indem der Code,

der in dem Rätsel sichtbar wird, angepasst wird. Alternativ kann auch der Lösungsweg des Rätsels verändert werden, sodass nicht die Eingabe der richtigen Benutzernamen und Passwörter die Lösung des Rätsels ist, sondern beispielsweise die richtige Anordnung der in die Slides gravierten Wellenbilder.

Durch den simplen Aufbau des Rätsels kann außerdem die äußere Gestaltung angepasst werden, um optisch mit dem Escape Room zu harmonisieren. Beispielsweise kann eine Zylinderform gewählt werden und das Gehäuse wie ein Teleskop gestaltet werden. So wird für die Spieler:innen außerdem klarer, dass sie durch das Teil hindurch gucken sollen.

Das Rätsel wurde von einigen Personen auf Verständlichkeit und Komplexität getestet. Es empfiehlt sich, weitere Probeläufe mit unterschiedlich erfahrenen Personengruppen zu machen, um die benötigte Zeit für das Rätsel besser abschätzen zu können. Dies ist allerdings erst dann sinnvoll, wenn das Rätsel in einen Escape Room integriert ist, da backtracking, Zusammenspiel mit der Story oder Platzierung im Ablauf des Escape Games die Lösungsgeschwindigkeit maßgeblich beeinflussen können.

Credit

Moritz von Ravenstein (455527) Juls Brühne (409248) Alexander Nütz (375059) Camilla Iffert (393974)

From:

<http://www.labprepare.tu-berlin.de/wiki/> - **Project Sci.Com Wiki**

Permanent link:

<http://www.labprepare.tu-berlin.de/wiki/doku.php?id=ss21:quantenescape&rev=1642928141>

Last update: **2022/01/23 09:55**

