Sicherer Kommunikation ist nicht erst seit den im Januar aufgekommenen neuen Whats-App-AGBs ein aktuelles und spannendes Thema, deshalb wollen wir uns in der heutigen Ausgabe mit einem besonderen Kryptografieansatz beschäftigen. Weltweit forschen Wissenschaftler großer IT-Firmen (Google, IBM...) aber auch Geheimdienste an Methoden zur Ausnutzung der Quantenphysik; um dies ein bisschen anschaulicher erklären zu können, bezeichnen wir im Folgenden Alice als Senderin und Bob als Empfänger – tatsächlich eine gängige Notation in der Quantenmechanik.

Das BB84-Protokoll

Tipp: Um im Weiteren alle (z. T. recht theoretischen) Erklärungen nachvollziehen zu können, verweisen wir auf die →BB84-Simulation von QuVis[1]. Dort kannst du zusammen mit Alice und Bob alle Schritte der Verschlüsselung Stück für Stück nachahmen!

Zunächst die nötige theoretische Basis: Beim BB84-Protokoll erfolgt die Verschlüsslung der zu übermittelnden Nachricht auf den Gesetzen, du kannst es dir denken, der Quantenmechanik. Drei Grundlagen sind im Folgenden für uns von großem Interesse:

1. *Für die Messung innerhalb einer Messrichtung (z. B. x- oder z-Richtung) eines Signals können nur zwei Werte auftreten, diese bezeichnen wir hier als „0“ und „1“.*

Man sagt auch, die Messwerte sind diskret.

2. *Die Messung eines quantenmechanischen Zustandes verändert diesen Zustand. Bei wiederholter Messung in der gleichen Messrichtung erhalten wir immer den gleichen Messwert.*

Dies hängt mit der *Heißenberg'schen Unbestimmtheitsrelation* zusammen – anders als in der Schule oft vermittelt, gilt diese nicht nur für *Ort* und *Impuls*, sondern für eine vielfältige Kombination von verschiedenen quantenmechanischen Eigenschaften. Sie sagt in unserem Fall aus, dass wir keinen Zustand präparieren können, der gleichzeitig Informationen für Messrichtung in x und z beinhaltet.

3. *Messen wir in zwei verschiedenen Messrichtungen und haben zuerst in x-Richtung gemessen und messen dann in z-Richtung, gilt (1) nicht mehr und wir erhalten mit 50%iger Wahrscheinlichkeit das Ergebnis von „0“ oder „1“.*

Das klingt jetzt erstmal sehr trocken, daher übertragen wir diese Grundlagen in unser Beispiel für die Verschlüsselung der Nachricht. Da wir quantenmechanische Zustände betrachten wollen, benötigen wir Datenträger, die hinreichend klein sind, um quantenmechanische Eigenschaften aufzuweisen. Dafür dienen z. B. Photonen deren

1 QuVis: Quantum Mechanics Visualisation Project: Eine Sammlung von unterschiedlichen Simulationen rund um die Quantenmechanik der University of St Andrews. Ein großer Teil der Simulationen ist auf Deutsch übersetzt.

Polarisationsrichtung wir messen können (innerhalb der jeweiligen Messrichtung). Diese Datenträger bezeichnen wir als Qubits, die im Gegensatz zu „klassischen“ Bits ein Rauschen – eine Überlagerung von „0“ und „1“ – aufweisen können. Das Qubit kann gleichzeitig ein bisschen den Wert „0“ und ein bisschen den Wert „1“ haben. Im Moment der Messung zwinge ich allerdings das Qubit, sich für einen Wert zu entscheiden und es gelten die obengenannten Grundlagen. Es wird dadurch extrem wichtig, welche MessrichtungenAlice und der Bob gewählt haben! Gleiche Messrichtungen geben die gleichen (und damit richtigen) Werte der gesendeten Qubits aus. Unterschiedliche Messrichtungen der beiden führen zu einer zufälligen Verteilung der Qubitwerte: Wenn Alice in x-Messrichtung ein Qubit mit „0“ sendet, kann es passieren, dass Bob in der z-Messrichtung eine „1“ misst… Dies kannst du ebenfalls in der Simulation erkennen! Doch wie können wir diese Effekte für die Verschlüsselung nutzen?

Beim BB84-Protokoll sendet Alice eine beliebige Anzahl von Qubits an Bob, wobei sie für jedes Qubit rein zufällig eine Messrichtung auswählt. Bob stellt seinen Detektor ebenfalls so ein, dass die Messrichtung für jede Messung zufällig gewählt wird. Die Folge – Alice und Bob wissen zunächst nicht, welche Qubitwerte übereinstimmen und welche aufgrund der zufälligen Verteilung bei verschiedenen Messrichtungen voneinander abweichen…

Daher ist es notwendig, über einen öffentlichen Kanal die Reihenfolge der Messrichtungswechsel bekannt zu geben (aber NICHT die Qubitwerte!). Öffentlich meint hierbei einen unverschlüsselten Kanal: Alice könnte z. B. ihre Messrichtungswechsel als lange Liste via E-Mail schicken. Somit wird ermittelt, wann die Messrichtungen übereinstimmten und dadurch welche Qubits richtig detektiert wurden. Mit den richtig detektierten Qubitwerten schreibt Alice eine Nachricht an Bob. Beispielsweise verrechnet sie die jeweiligen Qubitwerte und teilt die Rechenoperationen öffentlich. Da NUR Bob über die richtigen Qubitwerte für die Berechnung verfügt, kann er als einziger das richtige Rechenergebnis und damit die Nachricht entschlüsseln.

Alice könnte schreiben: „*Hallo Bob, nimm den Wert aus Messung 1, multipliziere mit 4 und addiere den Wert aus Messung 3. Die Zahl gibt dir die Stelle im Alphabet an… Gruß Alice*“. Es kommen in diesem Beispiel für jemand außen stehenden vier Möglichkeiten in Betracht (0, A, D, E; probiere es selbst einmal!), Bob hingegen weiß genau, welche Zahlen er einsetzten muss.

Um sicherzugehen, dass kein Spion die übermittelten Qubits abgefangen hat, sollten Alice und Bob etwa die Hälfte der Qubits (mit gleicher Messrichtung) öffentlich bekannt geben. War kein Spion anwesend, stimmen alle Qubitwerte (bei gleicher

Messrichtung!) überein... War ein Spion anwesend, greifen die oben genannten Gesetze der Quantenmechanik.

Der Spion müsste ähnlich wie Bob eine zufällige Messrichtung wählen, Alice' Nachrichten abfangen, messen und mittels neu generierter Qubits seine Messergebnisse an Bob weiterleiten. Da der Spion aber genau wie Bob die verwendeten Messrichtungen von Alice nicht kennt, sind seine Ergebnisse mit Sicherheit fehlerhaft. Tauschen sich Alice und Bob öffentlich über einen Teil ihrer Qubitwerte (bei gleicher Messrichtung) aus und stimmen einige dieser Werte nicht überein, müssen sie davon ausgehen, dass ein Spion die Qubitsignale abgefangen und manipuliert hat. Somit würde Alice keine (verschlüsselte) Nachricht schreiben, sondern eher eine neue beliebige Anzahl an Qubits an Bob senden (hoffentlich habe die beiden den Standort gewechselt, um den Spion abzuschütteln). Der Spion wäre also entdeckt, bevor die eigentliche, geheime Nachricht geschrieben würde...

Und die Aussichten? Derzeit bereitet vor allem die Übertragung der Qubits über längere Distanzen die größten Probleme, aber die ersten Realisierungen fanden schon statt: So wurde 2014 in Wien die weltweit erste Geldüberweisung via Quantenverschlüsselung durchgeführt. Es bleibt spannend...