### 3.3.5 Verschlüsseln im Binärsystem[1]

Wie zuvor erläutert, können Buchstaben und somit ganze Wörter bzw. Sätze durch eine Folge von 0 und 1 dargestellt werden. Diese „Übersetzung“ ins Binärsystem reicht als sichere Verschlüsselung einer Nachricht natürlich nicht aus. Es wird ein Schlüssel - ebenfalls eine Folge aus 0 und 1 - benötigt. Die Zahlenfolge muss dabei mindestens so lang sein, wie die zu verschlüsselnde Nachricht in ihrer binären Darstellung. Außerdem sollte der Schlüssel zufällig generiert sein und immer nur einmal verwendet werden (als sog. One-Time-Pad), um die Sicherheit der Verschlüsselung zu erhöhen.
Liegen nun Schlüssel und Nachricht in binärer Darstellung vor, erfolgt die eigentliche Verschlüsselung durch Addition der einander entsprechenden Elemente beider Zahlenfolgen. Das heißt, die erste Ziffer der Nachrichtenfolge wird zu der ersten Ziffer der Schlüsselfolge addiert und ergibt so die erste Ziffer in der Folge der codierten Nachricht. Ebenso wird für alle weiteren Elemente der Folgen verfahren (Beispiel Tab. 6).
Damit als verschlüsselte Nachricht wieder eine Folge von 0 und 1 entsteht, ist die Addition in diesem Falle wie folgt definiert:

| *Binäre Addition* | $1+0=1 \quad ; \quad 0+1=1 \quad ; \quad 0+0=0 \quad ; \quad 1+1=0$ |
|---|---|

Beispiel

| **Nachricht** | H | A | L | L | O |
|---|---|---|---|---|---|
| **binäre Darstellung** | 00111 | 00000 | 01100 | 01100 | 01111 |
| **Schlüssel** | 11110 | 11001 | 11101 | 10100 | 11010 |
| **verschlüsselte Nachricht** | 11001 | 11001 | 10001 | 11000 | 10101 |

Tabelle 6

## 3.4 Quantenkryptographie

Aus den vorherigen Kapiteln lässt sich schließen, dass die Übermittlung der verschlüsselten Nachricht nicht das Problem für eine sichere Kommunikation ist. Diese kann über einen beliebigen klassischen Kanal stattfinden. Stattdessen sind die Hauptprobleme der klassischen Kryptographie die Erzeugung und die sichere Übertragung eines zufällig generierten Schlüssels. Klassische Computer sind jedoch nicht in der Lage echte Zufallszahlen zu generieren. Für eine sichere Verschlüsselung ist das aber unbedingt notwendig. Die Quantenphysik bietet eine Lösung für dieses Problem.

### 3.4.1 Grundlagen

Wir betrachten Photonen hinsichtlich ihrer Polarisation, die vor einem Messprozess in einer Superposition zweier Basiszustände (bzw. Grundzustände) vorliegen. Zwei solche Basiszustände können beispielsweise die Zustände „horizontal polarisiert“ (↔) und „vertikal polarisiert“ (↕) sein. Die Basiszustände schließen sich dabei gegenseitig aus und bilden zusammen eine Basis (hier die +-Basis). Führt man nun einen Messprozess bezüglich dieser Basis durch, so löst sich die Superposition bezüglich der +-Basis auf und die Photonen nehmen einen der Basiszustände (↕ oder ↔) an. Welcher Zustand dabei

[1] Das Binär- bzw. Dualsystem ist ein Zahlensystem, welches zur Darstellung von Zahlen nur die Ziffern 0 und 1 verwendet.

realisiert wird, ist nicht vorhersagbar aufgrund des statistischen Charakters von Einzelereignissen in der Quantenphysik. Das heißt, die Messergebnisse sind nicht deterministisch - also zufällig.

| Messbasis | Polarisations-zustand | Signal |
|---|---|---|
| + | ↔ | 0 |
| | ↕ | 1 |

Tabelle 7

Bei der sogenannten Quantenkryptographie werden die Nachrichten unter Zuhilfenahme des Binärsystems verschlüsselt (Kapitel 3.3.5). Das heißt, als Schlüssel wird eine zufällige Folge von 0 und 1 benötigt. Ordnet man nun dem Zustand ↔ den Wert 0 und ↕ den Wert 1 zu (Tab. 7) und misst mehrere Photonen bezüglich der +-Basis, so ergibt sich eine zufällige Folge von 0 und 1 - der Schlüssel.

Erzeugung eines zufälligen Schlüssels

Zur Erzeugung des Schlüssels präpariert der Sender eine Reihe von Photonen mit Hilfe einer Einzelphotonenquelle[1] und eines Polarisationsdrehers[2] in der +-Basis. Dabei entscheidet er sich immer wieder zufällig, ob das aktuelle Photon im Basiszustand ↔ oder ↕ polarisiert werden soll.

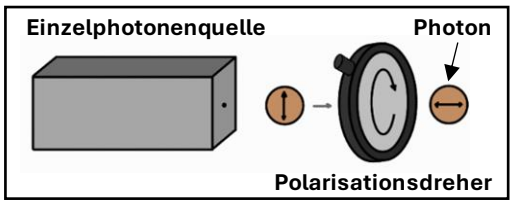


Abbildung 19

Schlüsselübertragung

Um den Schlüssel zu übertragen, werden die präparierten Photonen[3] vom Sender zum Empfänger geschickt (bspw. über Glasfaser oder via Satellit). Letzterer misst die in den Basiszuständen vorliegenden Photonen ebenfalls bezüglich der +-Basis (Abb. 20). Dabei wird er mit 100%iger Wahrscheinlichkeit jeweils die gleichen Messergebnisse erhalten wie der Sender, da die Superposition beider Basiszustände nach dem ersten Messprozess aufgelöst wurde und das Messergebnis bezüglich der gleichen Basis somit determiniert ist. Dementsprechend misst der Empfänger das gleiche wie der Sender und erhält so die gleiche Folge von 0 und 1.

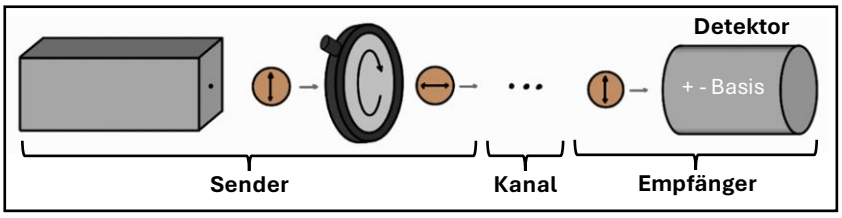


Abbildung 20

Problem

Bei diesem Verfahren treten jedoch zweierlei Probleme auf. Zunächst kann auf diese Weise nicht sichergestellt werden, dass der Schlüssel unverändert beim Empfänger angekommen ist. Die Photonen könnten durch etwaige äußere Einwirkungen beeinflusst worden sein, wodurch die Messergebnisse des zweiten Messprozesses nicht mehr deterministisch sind. Sender und Empfänger könnten also unwissentlich unterschiedliche Schlüssel erhalten. Die einzige Lösung für dieses Problem wäre, wenn beide ihre jeweiligen Messergebnisse vergleichen würden. Dies widerspricht jedoch der Geheimhaltung.

[1] Die erzeugten Photonen müssen dabei alle den gleichen Polarisationszustand besitzen.
[2] Bauteil, welches die Polarisation um einen festen Winkel drehen kann.
[3] Die Präparierung des Polarisationszustands der Photonen durch den Sender stellt einen Messprozess dar.

Das andere Problem ist, dass mit diesem Verfahren kein Spionageangriff identifiziert werden kann. Ein potenzieller Spion kann die Photonen auf ihren Weg zum Empfänger abfangen, in der gleichen Basis messen und an den Empfänger weiterschicken. Somit erhält er ebenfalls den Schlüssel, ohne dass der Zustand der Photonen verändert wurde. Eine mögliche Lösung für beide Probleme bietet das sogenannte BB84-Protokoll.

### 3.4.2 Das BB84-Protokoll

Beim BB84-Protokoll wird neben der Polarisation bzgl. der +-Basis eine weitere Basis - die ×-Basis - verwendet. Die ×-Basis hat die Basiszustände „positiv-diagonal polarisiert“ (⬀) und „negativ-diagonal polarisiert“ (⬂). Auch diesen Zuständen werden die Werte 0 bzw. 1 zugeordnet (Tab. 8).

| Messbasis | Polarisations-zustand | Signal |
|---|---|---|
| + | ↔ | 0 |
| | ↕ | 1 |
| × | ⬀ | 0 |
| | ⬂ | 1 |

Tabelle 8

Die genaue Schrittfolge des BB84-Protokolls wird im Folgenden beschrieben.

Erzeugung einer zufälligen Zahlenfolge

Der Sender präpariert eine Reihe von Photonen. Hierbei wechselt er zufällig zwischen den Basiszuständen der ×-Basis und der +-Basis[1]. Die gewählten Eigenschaften der präparierten Photonen (Basis, Messergebnis und entsprechendes Signal) werden gemeinsam mit der Nummer des Photons notiert (Beispiel Tab. 9).

Erzeugung und Übertragung des Schlüssels

Der Sender schickt die präparierten Photonen zum Empfänger. Dieser misst die Photonen in einer der beiden Basen, wobei er diese ebenfalls individuell zufällig wechselt (Abb. 21). Die Nummer des Photons, die Messbasis, das zugehörige Messergebnis und das entsprechende Signal werden notiert (Beispiel Tab. 9).

Als Ergebnis liegen Sender und Empfänger je eine Ziffernfolge vor, die aber aufgrund der jeweils zufällig getroffenen Entscheidungen beider nicht übereinstimmt. Im nächsten Schritt müssen also beide Folgen verglichen und alle Messwerte gestrichen werden, die nicht übereinstimmen. Ein direkter Vergleich der gewählten/gemessenen Basiszustände widerspricht jedoch der Geheimhaltung. Aus Kapitel 3.4.1 wissen wir aber, dass das Messergebnis des zweiten Messprozesses determiniert ist, wenn Sender und Empfänger das Photon in der gleichen Basis messen. Somit erhalten beide das gleiche Messergebnis. Demnach reicht es aus, wenn beide lediglich ihre Basenwahl vergleichen (Tab. 9 - nur die schwarzen Einträge). Haben sie die gleiche Wahl getroffen, so stimmt automatisch auch ihr Ergebnis und damit das zughörige Signal überein (Tab. 9 - grün markiert). Haben Sender und Empfänger jedoch unterschiedliche Basen für dasselbe Photon gewählt, so besteht die Möglichkeit, dass die entsprechenden Signale nicht übereinstimmen. Daher werden diese Messwerte verworfen (Tab. 9 - rot markiert). Nach dem Austausch über alle Basen liegt beiden der Schlüssel vor.

[1] Wird der Polarisationsdreher auf den Basiszustand ↔ oder ↕ gestellt, so entspricht das einem Messprozess bezüglich der +-Basis. Ebenso verhält es sich mit den Zuständen ⬀ bzw. ⬂ und der ×-Basis.

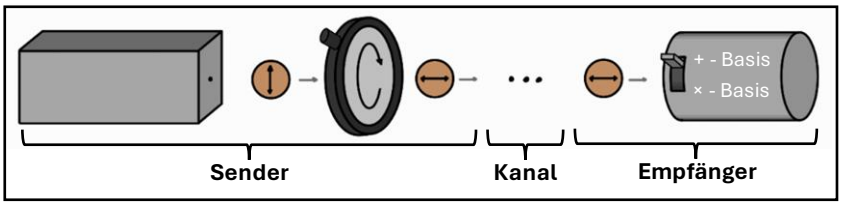


Abbildung 21

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Sender** | **Nr. Photon** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | **Basis** | + | + | × | | × | | | × |
| | Ergebnis | ↔ | ↕ | ⤡ | ↔ | | ⤢ | ↕ | |
| | Signal | 0 | 1 | | | | 0 | | 1 |
| **Empfänger** | **Nr. Photon** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | **Basis** | × | + | + | × | | × | | + |
| | Ergebnis | ⤡ | ↕ | | | ⤡ | | ↕ | |
| | Signal | 1 | 1 | 0 | | | | 1 | |

Tabelle 9

Spionage entdecken

Auch bei diesem Verfahren besteht die Möglichkeit, dass sich ein Spion zwischenschaltet und die Übertragung „abhört“. Daran können wir nichts ändern. Wir können aber eine Möglichkeit finden, den Spion zu entdecken. Dafür nutzen wir die Komplementarität. Hier wird jedoch nicht die Komplementarität zwischen Unterscheidbarkeit und Interferenz betrachtet, sondern die Komplementarität zwischen den beiden verwendeten Basen.

Beim BB84-Protokoll werden die +- und die ×-Basis verwendet. Die Polarisation eines Photons kann nicht gleichzeitig hinsichtlich beider Basen gemessen werden. Wir sagen: Die Basen sind komplementär. Das heißt, wird bezüglich der einen Basis gemessen, kann der Polarisationszustand bezüglich der anderen Basis nicht bestimmt werden. Das nutzen wir, um den Spion zu identifizieren:

Fängt der Spion die Photonen auf ihrem Weg zwischen Sender und Empfänger ab, so muss er sich seinerseits für Messbasen entscheiden, um die Photonen messen zu können. Diese Entscheidungen muss er ebenfalls zufällig treffen, da er die Wahl vom Sender bzw. Empfänger nicht kennt. Haben Sender und Empfänger dasselbe Photon in der +-Basis gemessen, der Spion dazwischen aber in der ×-Basis, so kann es sein, dass Sender und Empfänger trotz gleicher Basenwahl verschiedene Messwerte erhalten. Ursache dafür ist, dass der Spion durch seinen Messprozess das Photon beeinflusst. Demnach ist das Messergebnis beim Empfänger nicht mehr determiniert und kann von dem Ergebnis des Senders abweichen.

Daher wird der Schlüsselübertragung ein zusätzlicher Schritt hinzugefügt: Sender und Empfänger nehmen einen Teil (10%-20%) ihres erzeugten Schlüssels und vergleichen für diesen ebenfalls die Messergebnisse. Stimmen alle dieser Ergebnisse überein, so wurden die Photonen auf ihrem Weg sehr wahrscheinlich nicht beeinflusst. D.h. es gab vermutlich auch keinen Spion. Die verglichenen Messwerte werden entfernt und die übrigen bilden den Schlüssel. Stimmen aber einige der Messwerte nicht überein, dann weist das auf eine Beeinflussung der Photonen und damit auf einen Abhörangriff hin. In der Folge muss die Kommunikation abgebrochen werden.