Quantenkryptographie im Analogieversuch

Aufgaben zur Vorbereitung und zur Versuchsdurchführung

Bild: Thorlabs GmbH

Praktikum Moderne Physik für Lehramtskandidaten

Aufgaben zur Vorbereitung zuhause

Aufgabe 1: *Erklären Sie kurz in eigenen Worten, was man unter dem „Quantenschlüsselaustausch“ versteht. Wo steckt bei der „Quantenkryptografie“ die Quantenphysik?*

Aufgabe 2: *Worauf kommt es bei der Erstellung des Schlüssels an? Wo liegen Schwachpunkte?*

Aufgabe 3: *Worin besteht die Sicherheit der Quantenkryptografie? D.h.*

- *Warum kann ein quantenkryptografischer Code nicht geknackt werden, im Gegensatz zu anderen Verfahren?*
- *Warum ist das Verfahren abhörsicher bzw. wie kann der Lauscher Eve erkannt werden?*

Aufgabe 4: *Warum könnte eine Nachricht, die mit dem hier verwendeten Quantenkryptografie-Analogie-Versuchsaufbau übertragen wird, letztlich doch abgehört werden? Wie könnte Eve das in diesem Fall bewerkstelligen?*

Aufgabe 5: *Was unterscheidet eine „Pseudozufallszahl“ von einer „echten“ Zufallszahl? Wie kann man diese Zahlen jeweils erzeugen?*

Versuchsdurchführung

Der Versuchsablauf im Praktikum gliedert sich in drei Teile:

- Generierung eines mindestens 20bit langen Schlüssels
- Verschlüsseln und Übertragen eines 4-Buchstaben Wortes
- Einbau von Eve und Lauscher identifizieren

Die Messprotokolle finden Sie als Vorlage im Extra Dokument.

Teil 1: Schlüsselgenerierung

Versuch 1: Bauen Sie Alice und Bob so auf, dass sich beide in größerem Abstand gegenüber stehen (sodass also noch Platz für Eve ist). Justieren Sie beide so ein, dass bei allen acht $\lambda/2$ -Kombinationen (zwei Einstellungen bei Bob, vier bei Alice) reproduzierbar die richtigen LEDs leuchten. Stellen Sie dafür sicher, dass die Sensorelektronik im Justiermodus ist (gelbe LED). Eine Anleitung zum Aufbau finden Sie in Anhang B.

Versuch 2: In der nächsten Aufgabe soll der Schlüssel generiert werden. Als Vorbereitung müssen Alice und Bob zufällig ihre Basen wählen und Alice zusätzlich ihre Bits. Es hat sich als sinnvoll erwiesen, das vorab zu tun – füllen Sie also die Messprotokolle für Alice und Bob in Anhang C aus (Bob nur die Basis).

Hinweis: Um echte Zufallszahlen zu erhalten, können Sie die beiliegende Würfelbox verwenden. Definieren Sie z.B. „gerade Zahl = +“, „ungerade Zahl = x“ „gerade Zahl = 0“, „ungerade Zahl = 1“ und würfeln Sie so Ihre Basen bzw. Zufallsbits aus!

Versuch 3: Alice und Bob sollen nun einen mindestens 20 Bit langen Schlüssel generieren. Führen Sie dafür 52 Messungen durch – dies ist ein empirischer Wert, bei dem fast immer 20 Mal die Basen übereinstimmen (und damit 20 Schlüsselbits erzeugt werden). Sollten 52 Messungen nicht ausreichen, müssen weitere erfolgen, bis 20 Schlüsselbits generiert sind.

Noch einmal zur Orientierung: Wenn Alice

- „0°“ einstellt, dann sendet sie in der „+“ Basis eine 0.
- „90°“ einstellt, dann sendet sie in der „+“ Basis eine 1.
- „-45°“ einstellt, dann sendet sie in der „x“ Basis eine 0
- „45°“ einstellt, dann sendet sie in der „x“ Basis eine 1

Alice und Bob übertragen die Bits anhand der in Versuch 2 erstellten Tabelle. Dafür sendet Alice ihr Bit und Bob notiert seine Messung (reflektiert = 1, transmittiert = 0). Am Ende tauschen sich beide über ihre Basen aus und streichen die Messungen, bei denen die Basen nicht übereinstimmen. Die restlichen Messungen stellen dann den Schlüssel dar.

Teil 2: Verschlüsseln und Übertragen des 4-Buchstaben Worts

Versuch 4: Alice, verschlüsseln Sie ihre Nachricht (4 Buchstaben) mit dem generierten Schlüssel.

Versuch 5: Übertragen Sie die Nachricht von Alice zu Bob.

Versuch 6: Bob, entschlüsseln Sie die Nachricht.

Teil 3: Einbau von Eve und Detektion des Abhörens

Versuch 7: Setzen Sie Eve zwischen Alice und Bob und schalten Sie beide Sensorelektroniken auf den Justiermodus (LED leuchtet gelb). Justieren Sie den Empfangsteil von Eve so ein, dass alle 8 Fälle mit Alice funktionieren. Justieren Sie nun den Sender von Eve so, dass alle 8 Fälle mit Bob funktionieren.

Versuch 8: Füllen Sie die Tabelle für Eve aus, in der sie sich für die + oder die x Basis entscheidet. Sie brauchen außerdem wieder zufällige Basen für Alice und Bob, sowie zufällige Bits für Alice.

Versuch 9: Generieren sie mit Alice und Bob wieder einen Schlüssel mit mindestens 20 Schlüsselbits wie in Versuch 3. Vergleichen Sie dann den gefundenen Schlüssel.

Hinweis: Unser Versuch arbeitet mit einem Laserpuls und damit mit Milliarden von Photonen. Die echte Quantenkryptografie arbeitet mit einzelnen Photonen. Trotzdem sind der Versuchsaufbau und die Messmethode völlig identisch. Die Abhörsicherheit ist allerdings nur bei einzelnen Photonen gewährleistet, da bei vielen Photonen EVE nicht alle Photonen zum Lauschen benötigt, sondern prinzipiell nur ein einziges von den Milliarden. ALICE und BOB würden einen solchen Lauscher dann nicht finden.