Quanten Computing

1 Praktische Arbeit -> Demonstration im Unterricht

1.1 Quantenkryptographie mit Schokoladebällchen

In der langen Nacht der Forschung 2005[1] wurde das Prinzip der Quantenkryptographie anhand des BB84-Protokolls demonstriert.

Damit die Schüler in der Stunde das Prinzip der Quantenkryptographie selbst „nachspielen" können muss jede Kugel vorbereitet werden(z.B. roter und grüner Punkt). Wir wollen ja darstellen wie die Information mittels Photonen prinzipiell funktioniert.

Also Photonen können

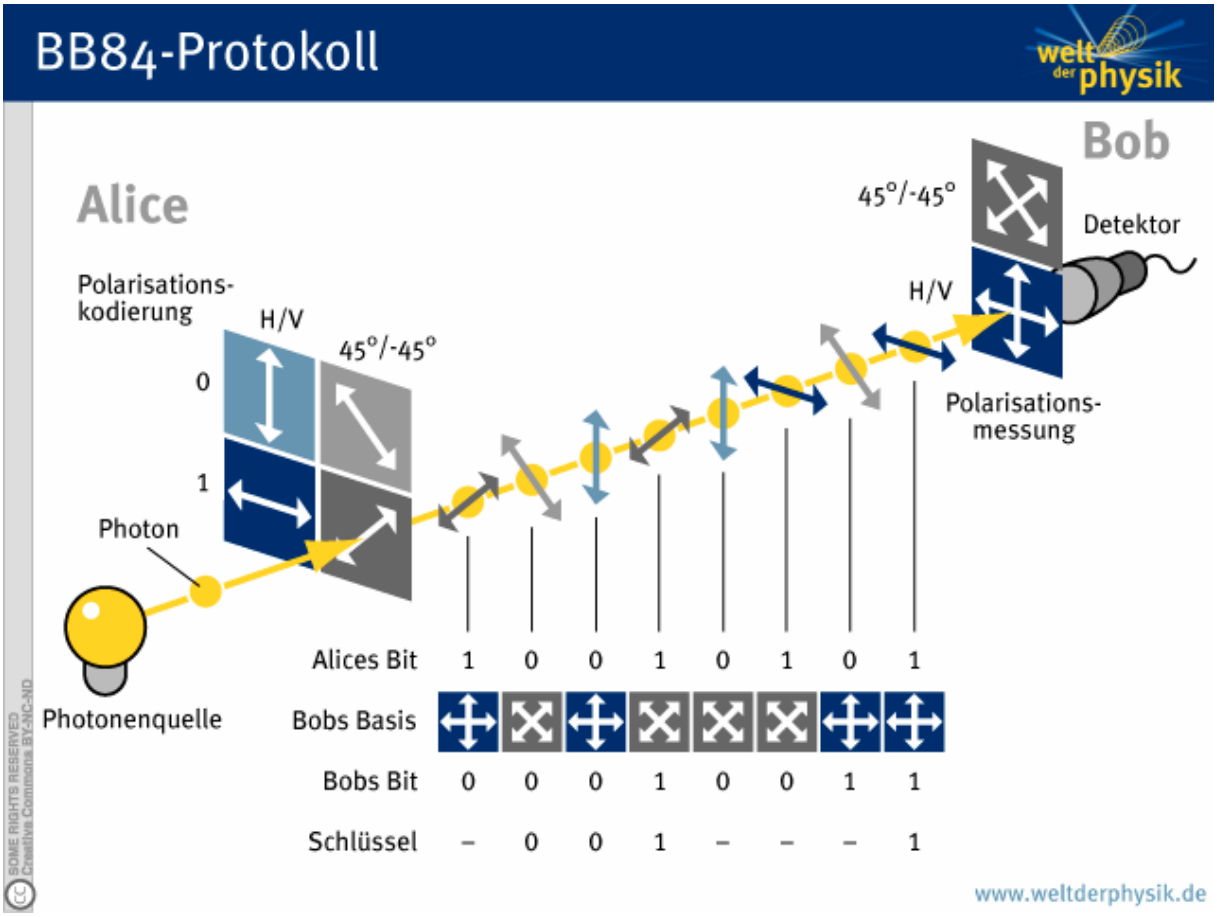
a.) H horizontal oder V vertikal polarisiert sein (– oder |) : Diese wird
b.) diagonal polarisiert sein (/, „rechtsdiagonal +45°"; oder \, „linksdiagonal- 45°").

Ein rechdiagonaler polarisiertes Photon wird einen linksdiagonalen Filter nicht passieren können.

Die Klassenschülerzahl so aufteilen, dass eine Hälfte (Alice) und die andere Hälfte (Bob) sind. Nun wirft die erste Alice das „Photon" zum ersten Bob usw.

Alice kodiert den Bit-Wert des Schlüssels (0 oder 1) in der Polarisation einzelner Photonen. Sie wählt dabei zufällig aus zwei Basen (H/V oder +45°/-45°). Jeder Bit-Wert kann somit in einer der beiden Basen kodiert werden, in diesem Beispiel wird 0 in V oder -45 Grad, 1 in H oder +45 Grad geschrieben. Bei der Messung hat Bob nun wiederum die Möglichkeit, das Photon in einer der beiden Basen zu analysieren. Entscheidet er sich für die falsche Basis (hier beim von links 1., 5., 6. und 7. Photon), so sind seine Ergebnisse der Polarisationsmessung nicht mit Alice korreliert. Diese Photonen werden aus dem Schlüssel gestrichen. Wählt er aber dieselbe Basis wie Alice (2., 3., 4. und 8. Photon), so ist seine gemessene Polarisation gleich der, die von Alice kodiert wurde. Diese Werte können also für den Schlüssel verwendet werden. Um zu wissen, welche Photonen in der gleichen Basis gemessen wurden und für den Schlüssel verwendet werden können, müssen Alice und Bob ihre Basiswahl für jedes Photon austauschen und vergleichen (Das erfolgt über einen unsicheren Kanal, in unserem Fall durch Zuruf) . Die Information der Basis allein enthält keinen Aufschluss darüber, welcher Bit-Wert mit ihr kodiert wurde. Somit können Lauscher auch nichts über den geheimen Schlüssel erfahren, wenn sie den Basisvergleich mithören.

[1] Karl Svozil; *Institut für Theoretische Physik, University of Technology Vienna*



Anschließend werden die Schokoladebällchen verzehrt ☺.