

Ein kurzer Einblick in die Quantenkryptographie

Gernot Goluch
Technical University
Vienna

October 29, 2004

Contents

1	Theorie	2
1.1	Schrödingers Katze	2
1.2	Photon und dessen Polarisation	3
1.3	Messung und Superposition	3
2	Die Ver- und Entschlüsselung	4
2.1	Eve	4
3	Schlüsselverteilung	5
3.1	Die Lösung	5
3.2	Eve	6
4	Die Schwachstelle: DOS	6
	References	7

1 Theorie

Alle bisher eingesetzten, moderneren, Kryptographieverfahren beruhen auf der Anwendung mathematischer Funktionen, wie z.B.: das RSA Verfahren sich die Eigenschaften einer Falltürfunktion zu Nutze macht. Die revolutionäre Erneuerung in der Quantenkryptographie ist es nun eben dies nicht zu machen, sie lässt die Mathematik und ihre Angriffspunkte außer Acht. Diese Methode der Kryptographie macht sich eine grundlegende Eigenschaft, die Superposition, in der Quantenphysik zu Nutze um den gewünschten Effekt der Ver- und Entschlüsselung zu erzielen. Diesen Effekt möchte ich im folgenden Kapitel kurz erklären. Das Verb erklären ist hier an sich nicht angebracht, da sich schon weit mehr Physik bewanderte Menschen, als ich einer bin, den Kopf wegen dieses Effektes zerbrochen haben. Für die vereinfachte Funktionsweise der Quantenkryptographie sollte dies jedoch reichen

1.1 Schrödingers Katze

Erwin Schrödinger, der 1933 den Nobelpreis für Physik erhielt, fand ein Gedankenexperiment, das als Schrödingers Katze bekannt wurde und verwendet wird um das Prinzip der Superposition zu erklären: Eine Katze kann zwei Zustände haben, nämlich lebendig oder tot. Wir stecken nun die Katze in eine Kiste, die wir so verschließen dass niemand die Katze mehr beobachten kann. Als letzten Schritt wird eine Kapsel mit Gift in diese Kiste geworfen, die wenn sie von der Katze gefressen wird den sofortigen Tod eben dieser herbeiführt. Genau hier verlagern sich nun die zwei Zustände der Katze, sie ist laut Quantentheorie tot und lebendig.

Genau diese Überlagerung mehrerer Zustände, die Superposition, machen wir uns in der Quantenkryptographie zu Nutze. Nur das wir hier nun nicht mit Katzen sondern mit Teilchen bzw. Wellen arbeiten. Unsere Katze ist nun ein Photon und der Zustand ist durch die Polarisation gegeben. Es sei hier angemerkt das man dies auch mit einem Teilchen (z.B.: einem Elektron) und dessen Spin durchführen kann. Die Funktionsweise der kryptographischen Methode bleibt exakt die gleiche.

1.2 Photon und dessen Polarisation

Jedes Photon kann in einer gewissen Weise polarisiert werden. Der Einfachheit halber nehmen wir an das nur vier mögliche Polarisationen bestehen:

1. rektileare Polarisation *VERTIKAL*(in weiterer Folge v genannt)
2. rektileare Polarisation *HORIZONTAL*(in weiterer Folge h genannt)
3. diagonale Polarisation *DIAGONALLR*(in weiterer Folge dlr genannt)
4. diagonale Polarisation *DIAGONALLL*(in weiterer Folge drl genannt)

Wir besitzen auch die notwendigen Filter um ein Photon auf die richtige Weise zu polarisieren.

1. Filter rektileare: *FR*
2. Filter diagonale: *FD*

1.3 Messung und Superposition

Wir können nun mit unseren im vorherigen Kapitel definierten Filtern die Polarisation eines Photons nicht nur erzeugen, sondern natürlich auch messen. Messen wir ein horizontal oder vertikale polarisiertes Photon mit einem rektilearen Filter so erhalten wir exakt die Polarisation, das selbige wenn wir ein diagonal polarisiertes Photon mit dem dementsprechenden Filter messen. Um dies zu verdeutlichen folgende Graphik:

Messen wir nun jedoch ein rektilear polarisiertes Photon mit unserem diagonalen Filter so tritt das Prinzip der Superposition ein, sprich wir können die Polarisation nicht feststellen. Und genau das macht die Quantenkryptographie zur unknackbaren kryptographischen Methode, lässt man die Möglichkeit der Schlüsselerrattung aus. Folgende Graphik soll dies verdeutlichen (für rektileares Schema):

2 Die Ver- und Entschlüsselung

Alice will nun die Meldung 1101101001 an Bob schicken.
Wir definieren:

$$\begin{aligned} 0 &= v / \text{drl} \\ 1 &= h / \text{dlr} \end{aligned}$$

Sie muss nun die Photonen in die gewünschte Polarisierung bringen, hierfür definiert sie folgendes Schema, das zugleich unser Schlüssel sein wird.

Key: FR FD FR FD FD FD FR FR FD FD
Msg: 1 1 0 1 1 0 1 0 0 1

Pol: h dlr v dlr dlr drl h v drl dlr

Folgende Graphik soll diesen Schritt nochmals verdeutlichen (f/ur FR):

Wenn Bob nun den Schlüssel besitzt (zum Problem der Schlüsselverteilung siehe später) kann er ohne weiteres die Nachricht wieder in ihre ursprüngliche Form bringen.

2.1 Eve

Nun kommt die böse Eve ins Spiel die unsere Nachricht abfängt und entschlüsseln will.

Sie kann nun ebenfalls einen Filter auf die Photonen anwenden.

Key: FR FR FD FD FR FD FD FD FR FR
Pol: h dlr v dlr dlr drl h v drl dlr

Msg: 1 ? ? 1 ? 0 ? ? ? ?

Wie wir sehen erhält sie für jeden falsch erratenen Filter ein Photon dessen Polarisierung nicht identifizierbar ist, wegen des Prinzips der Superposition. Sie kann auch nicht nochmals einen neuen Filter zur Bestimmung benutzen da die

Photonen nun eine andere bzw. keine eindeutige Polarisation mehr aufweisen
-; Die Information wurde zerstört! Und damit hat Eve keine Chance mehr
die Nachricht zu entziffern.

3 Schlüsselverteilung

Wie bekommt Bob nun den Schlüssel? Wir haben hier ein, schon seit des One
Time Pads, bekanntes Problem. Unsere unknackbare Methode hilft uns sehr
wenig wenn wir den Schlüssel über ein knackbares Medium, wie z.B.: der Post
oder ein mathematisches Kodierungsverfahren, übermitteln. Jedoch gibt es
auch für dieses Problem eine Lösung innerhalb der Quantenkryptographie.

3.1 Die Lösung

Alice wählt:

Zufallsfolge: 1 0 0 1 1 0 1 0

ZufallskeyA: FR FR FD FD FD FR FD FR

Zufallspol: h v drl dlr dlr v dlr v

Bob bekommt die polarisierten Photonen, ohne das er den Schlüssel weiß,
und nimmt einen eigenen Zufallsschlüssel:

Zufallspol: h v drl dlr dlr v dlr v

ZufallskeyB: FD FD FR FD FD FR FR FR

ZufallsMsg: ? ? ? 1 1 0 ? 0

Nun ruft Alice Bob auf dem unsichersten Kanal, der auf der Welt existiert
an, z.B.: mit dem Handy und berichtet ihm ihren Zufallsschlüssel. Bob löscht
nun alle falsch gemessenen Werte aus seiner Message heraus und berichtet
Alice welche er richtig gemessen hat.

Nun wissen beide dass ihr Key 1100 (FR FR FD FD oder FD FD FR FR)

3.2 Eve

Das Ganze sieht auf dem ersten Blick nicht sehr sicher aus. Bringen wir also Eve ins Spiel. Eve misst nun den Key ebenfalls mit einem von ihr erzeugten Zufallsschlüssel, wird jedoch nicht den gleichen erfinden wie Bob. Nun bekommt sie ebenfalls eine Message, mit der sie jedoch, da sie nicht die gleiche ist wie Bob sie ermittelt, nichts anfangen kann, auch nicht wenn sie das Telefonat von Alice und Bob mithört.

4 Die Schwachstelle: DOS

Die Nachrichten die Alice und Bob austauschen sind nun nicht mehr knackbar, geht man von davon aus das Alice und Bob eine vernnftige Schlssellänge wählen (nicht so wie im vorherigen Beispiel). Wenn nun jedoch Eve einen Kanal zwischen Alice und Bob kontrolliert, kann sie jede Nachricht unbrauchbar fr die Kommunikation machen, sie muss nur irgendeinen Filter dazwischen schalten. Alice und Bob werden dies zwar bemerken, doch kontrolliert Eve nun viele oder vielleicht sogar alle Kanäle zwischen den beiden, ist eine Kommunikation unmöglich. Man spricht in diesem Zug auch von Denial of Service Attacken.

References

- [1] Simon Singh, Geheime Botschaften (1999)