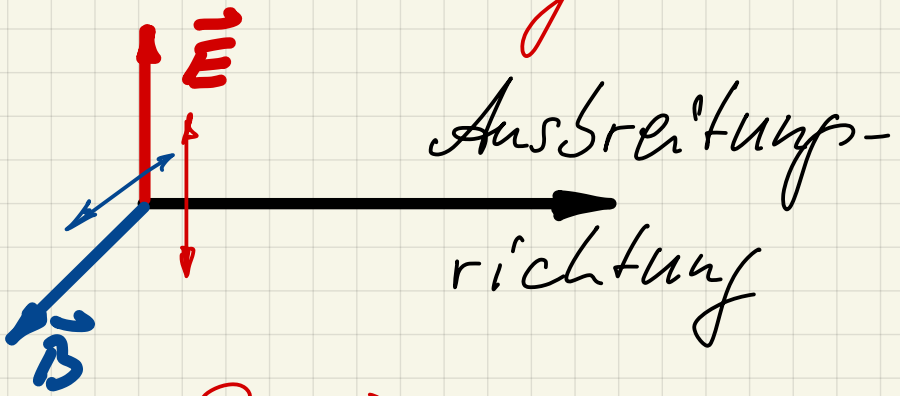
Quantenverschlüsselung

Prof. Dr. Jürgen Schnack

jschnack@uni-bielefeld.de

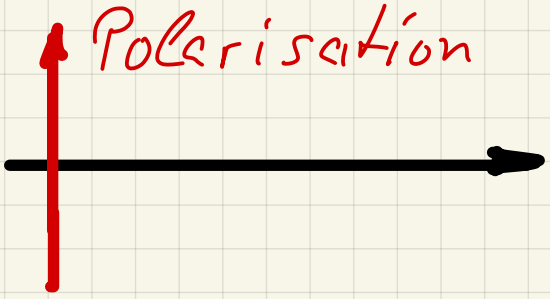
Ziel: Wir werden ausgehend von Polarisationsfiltern ein einfaches Verfahren der Quantenverschlüsselung verstehen.

Licht ist eine elektromagnetische Welle,

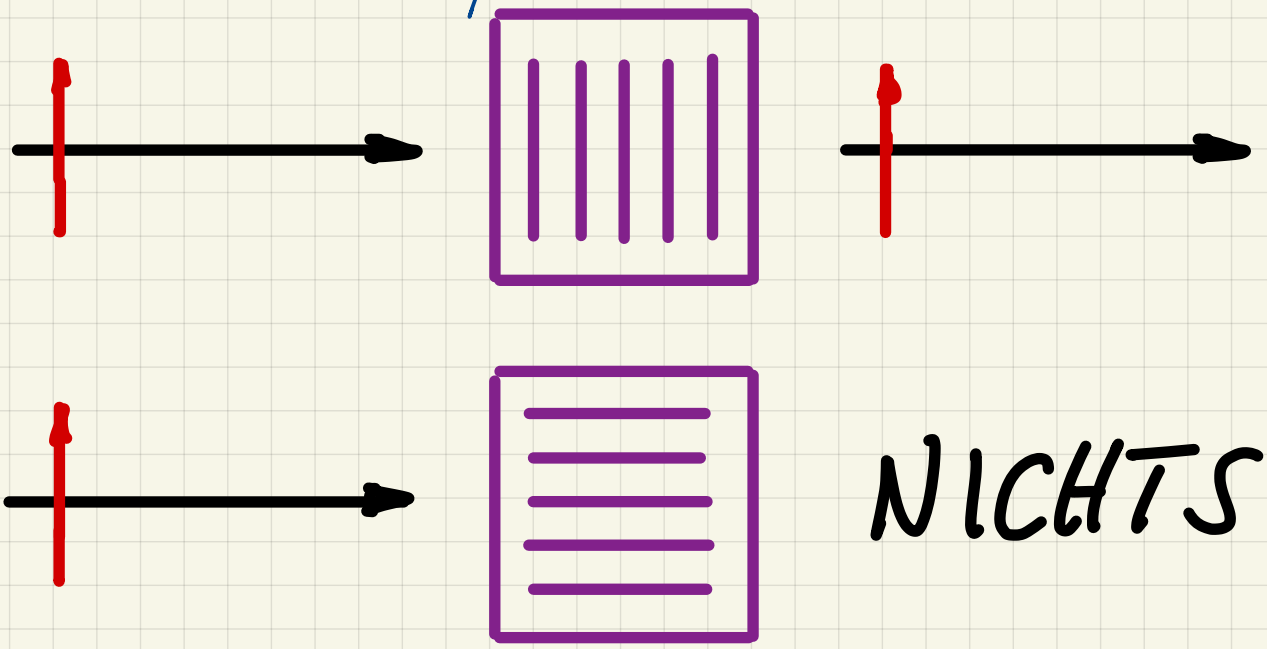


in der die elektrische ($\vec{E}$) und magnetische ($\vec{B}$) Komponente schwingen.

⇒ Wir bezeichnen die Richtung von $\vec{E}$ als Polarisation

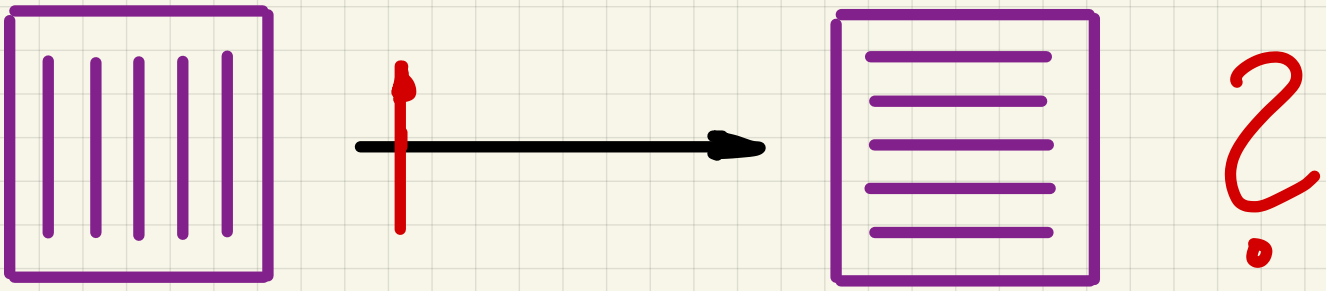


Polarisationsfilter:

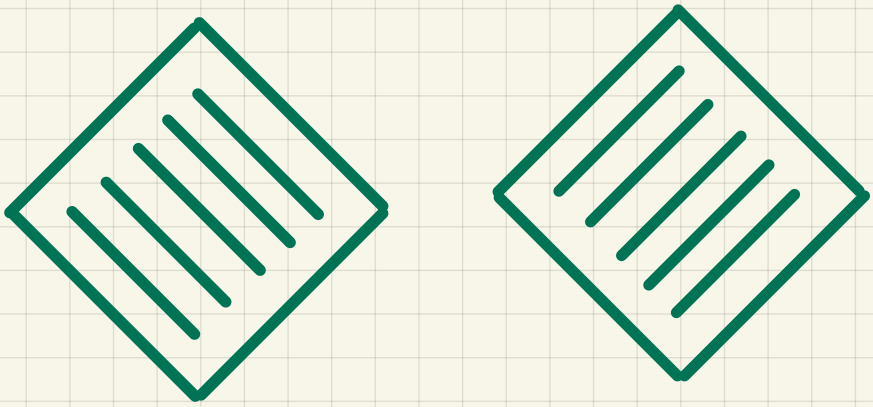


Ein Polarisationsfilter lässt nur eine Richtung durch.

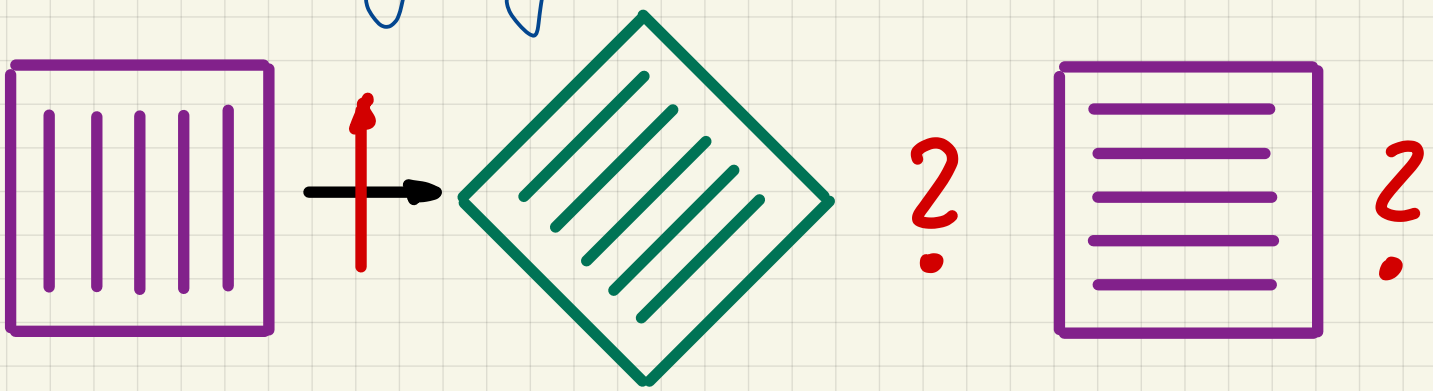
Überlegung 1



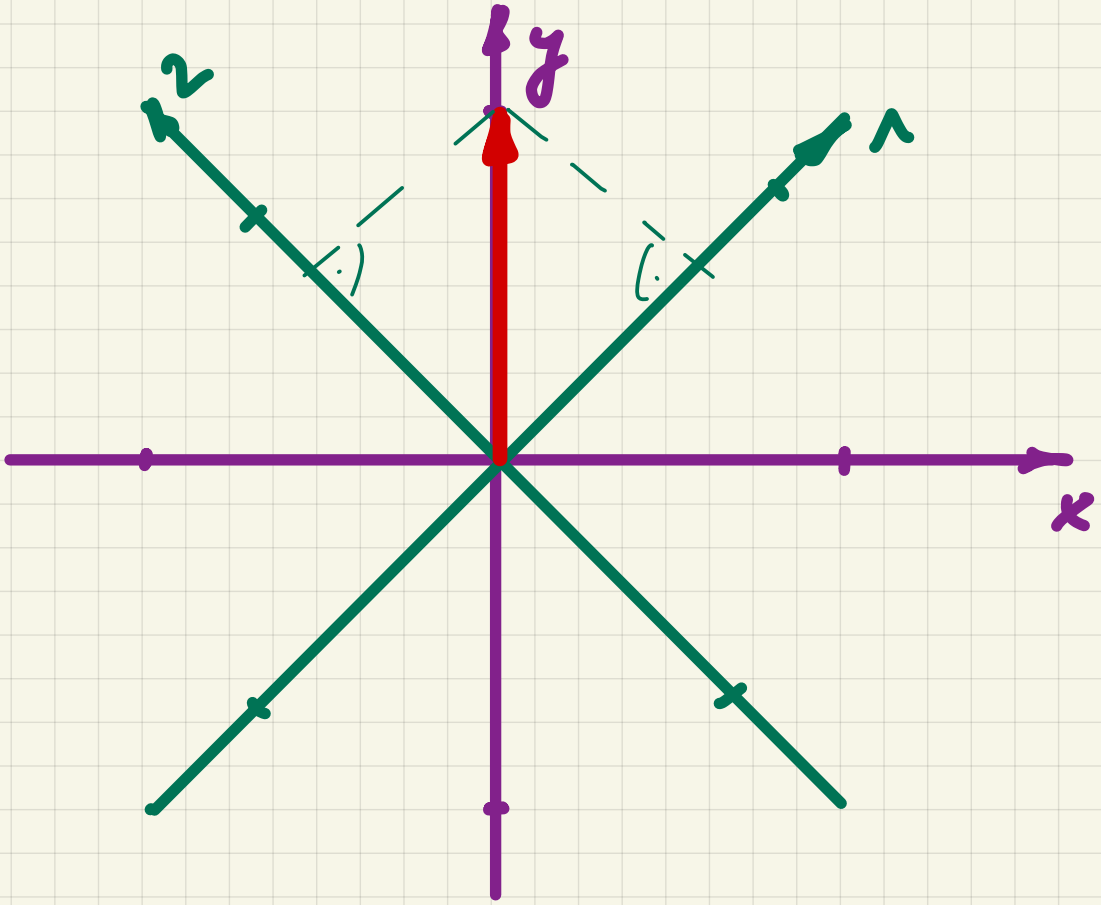
Nutzen noch zweite Gruppe von Orientierungen

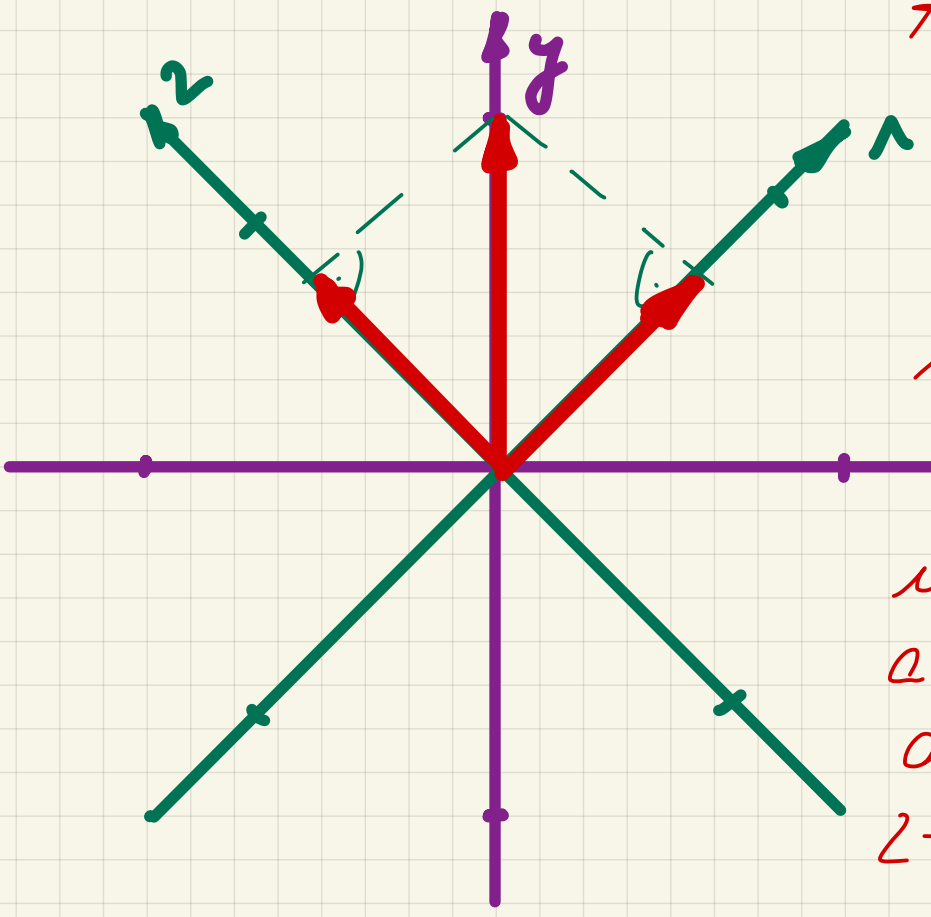


Überlegung 2



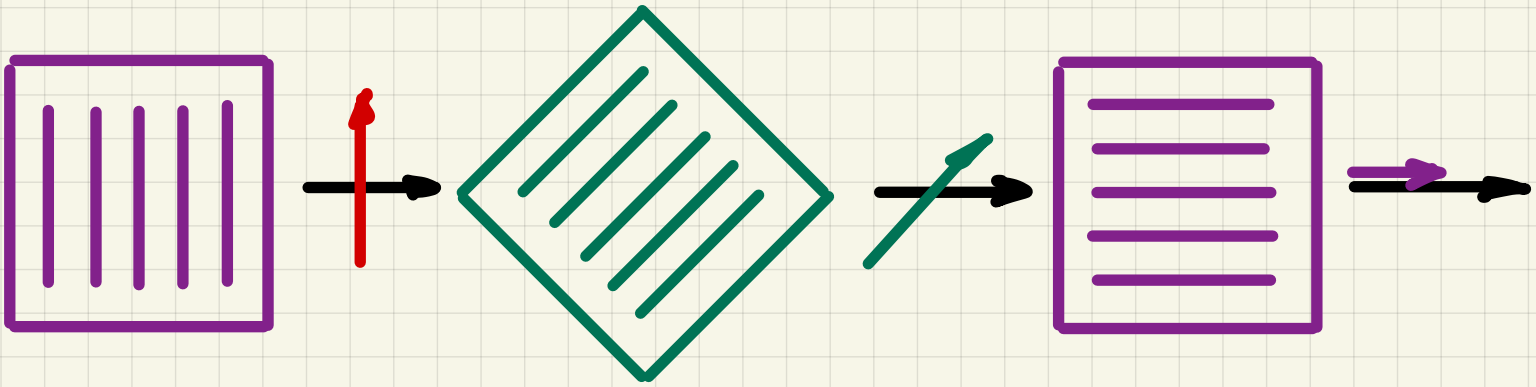
Lösung: Die Polarisation ist ein Vektor, der in Komponenten zerlegt werden kann, wie die Kraft bei der Kräftezerlegung.





Aha, die y-Polarisation besteht zur Hälfte aus 1-Polarisation

und zur anderen Hälfte aus 2-Polarisation.



Zusammenfassung bis hier

1. Polarisationsfilter

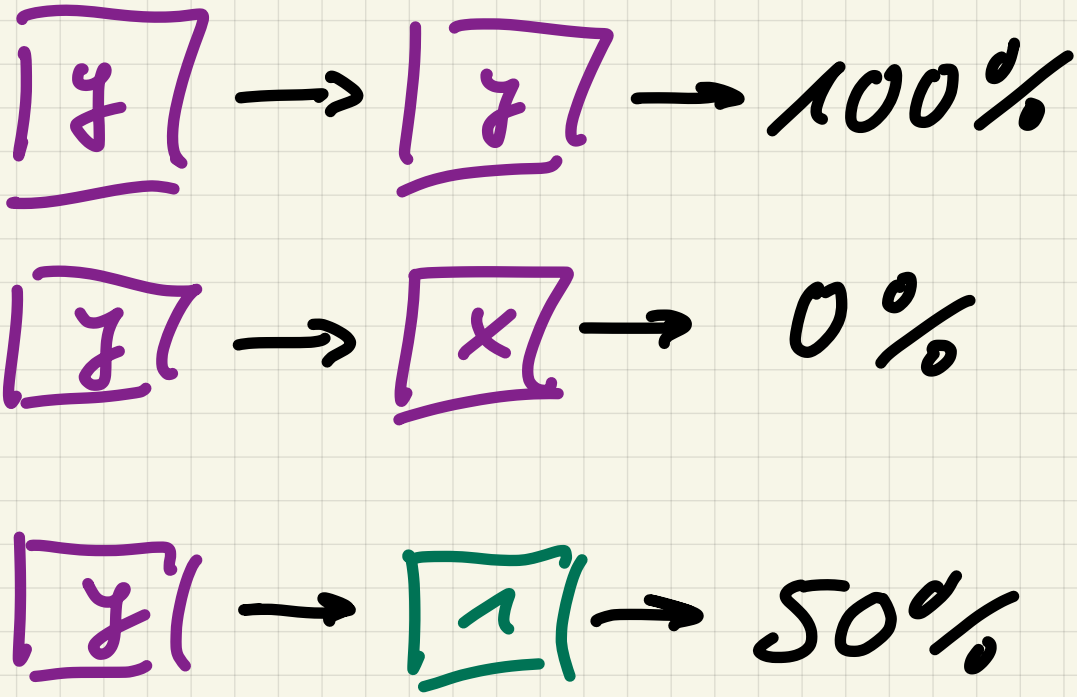
A polarisieren entlang x Str. y

2. Polarisationsfilter

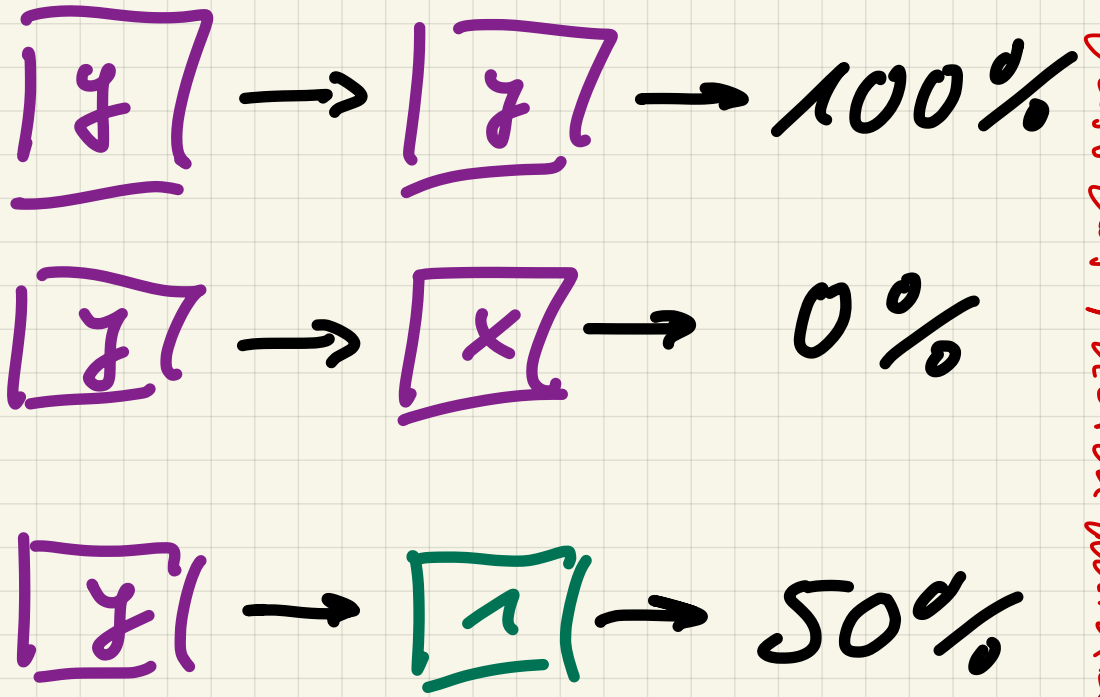
B polarisieren entlang 1 Str. 2
(45° zu x & y)

3. Die Polarisation ist immer <u>senkrecht</u> zur Ausbreitungsrichtung. Die Skizzen geben das nicht so wieder. Das Licht fällt senkrecht durch die Filter durch.

Haupterkenntnis



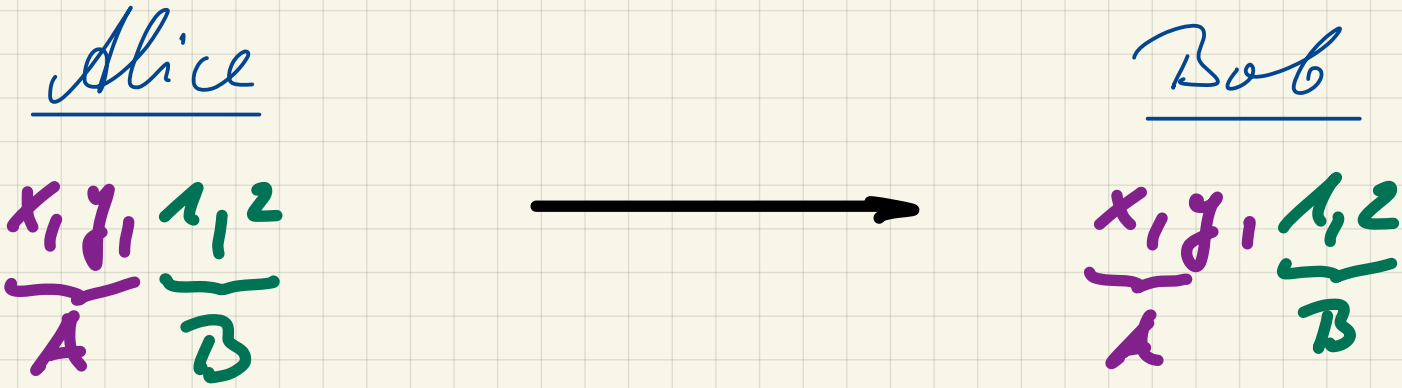
Dieses Experiment kann man mit einzelnen Photonen machen!



Dann sind die Wahrscheinlichkeiten, dass das Photon durchkommt!

Damit haben wir alles für die Quantenkryptographie.

Ziel: Wir generieren einen zufälligen Schlüssel (aus 0 und 1), den nur Alice und Bob kennen.



Beide haben vier Polarisatoren, diese werden zufällig eingesetzt.

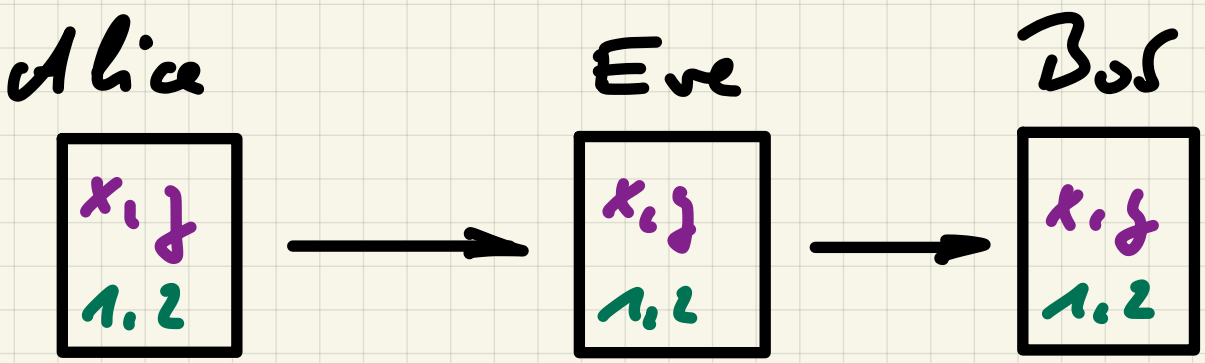
Alice wählt eine der vier Richtungen und schickt das entsprechend polarisierte Photon auf die Reise. Bob misst mit einem der vier Polarisatoren.

Kommt das Photon durch, teilt Bob Alice mit, welche Polarisatoren-gruppe – A oder B – er verwendet hat. Sagt sie: „Hand“,

1. wissen beide, welche der vier Polarisatoren das war. Warum?
2. ist es ein gültiges Bit und wird dem Schlüssel hinzugefügt.
3. Wert des neuen Bit z.B.
   0, wenn Polarisation x oder 1 war
   1, wenn Polarisation y oder 2 war

Warum ist das sicher?

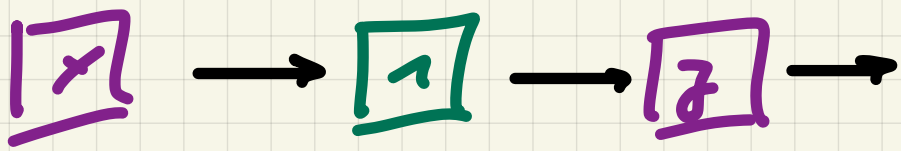
Jetzt kommt der Spion, Eve, ins Spiel.



In festgelegten Abständen werden Bits als Kontrollbits versendet. Sie kommen nicht zum Schlüssel, sondern dienen der Enttarnung von Eve. Bob teilt Alice dazu die genaue Polarisationsrichtung mit.

Wenn er ein Photon gemessen hat, das gar nicht durchkommen dürfte, muss ein Spion in der Leitung sein!

Bsp:



ohne Eve würde nichts durchkommen!

QM: Es gibt keine zerstörungsfreie Quantenmessung!