# 1 Einleitung

Bei der Quantenkryptographie handelt es sich um ein Verfahren zur sicheren Übermittlung von Daten. Dabei wird ein sogenanntes one-time pad Verfahren angewandt. Das bedeutet, dass vor den eigentlichen Daten ein Schlüssel übertragen wird, der nur für diese Kommunikation verwendet wird. Dieses Verfahren ist unter den folgenden Voraussetzungen sicher:

- Der Schlüssel darf nur einmal verwendet werden.
- Der Schlüssel muss mindestens so lange sein, wie die Nachricht.
- Der Schlüssel muss zufällig sein
- Der Schlüssel darf nur zwei Personen bekannt sein.

In der Praxis ist vor allem die letzte Bedingung nur sehr schwer umzusetzen. Nur schon, wenn ein Bote den Schlüssel transportiert, kann dieser den Schlüssel lesen und somit die Nachricht entschlüsseln. Gesucht ist folglich ein Verfahren, das es erlaubt, den Schlüssel so auszutauschen, dass jedes Mithöhren zweifelsfrei identifiziert werden kann. Und genau hier kann uns die Quantenphysik helfen.

# 2 Die physikalischen Grundlagen

Um zu verstehen, wie die Quantenkryptografie funktioniert, muss man sich mit einigen Grundlagen der Quantenphysik auseinandersetzen, die sich fundamental von der klassischen Physik unterscheiden.

## 2.1 Quantenmechanische Zustände

Eigenschaften von Teilchen werden in der Quantenphysik nicht durch Werte angegeben, sondern durch Wahrscheinlichkeiten. Ein Elektron, dass um einen Atomkern kreist, ist zu einer bestimmten Zeit nicht an einem definierten Ort, sondern es besteht eine gewisse Wahrscheinlichkeit, dass es sich an diesem Ort befindet. Dies wird durch die sogenannte Wellenfunktion beschrieben. Dabei gilt, dass das Quadrat der Zustandsfunktion angiebt, wie gross die Wahrscheinlichkeit ist, dass sich dieses Teilchen an dem Ort befindet.

Es ist übrigens nicht so, dass man nur zuwenig weiss, um den genauen Ort eines derartigen Teilchens anzugeben. Vielmehr deuten alle Experimente darauf hin, dass es nie möglich sein wird, diese Zustände genauer zu kennen. Erst im Rahmen einer Messung gerät ein derartiges System in einen definierten Zustand. Dies bedeutet natürlich, dass eine Messung das System immer auch beeinflusst. Man muss sich von der Idee einer objektiven Realität ausserhalb einer Messung verabschieden.

## 2.2 Verschränkte Teilchen

Interessant wird dieser Sachverhalt, wenn zwei Teilchen bei der Entstehung miteinander in einer bestimmten Wechselwirkung gestanden haben. Es kann dann nämlich passieren, dass diese Teilchen durch eine gemeinsame Wellenfunktion beschrieben werden, obwohl sie räumlich voneinander getrennt sind. Dieser Effekt wird übrigens nach den Entdeckern Einstein Podolski Rosen Effekt genannt. Ursprünglich war er als Argument gedacht, um zu zeigen, dass die Quantenphysik nicht vollständig ist, da das Messergebnis an einem Teilchen einen Einfluss auf das zweite, beliebig weit entfernte Teilchen hat. Diese Eigenschaft der Quantenphysik wurde von Einstein übrigens nie akzeptiert. Er hat Zeit seines Lebens versucht, durch das Einführen

neuer, bisher unbekannter Variabeln eine Variante der Quantenphysik zu entdecken, die lokal ist.

### 2.3 Die Bellsche Ungleichung

Allerdings konnte John Bell im Jahre 1964 zeigen, dass die Quantenphysik Vorhersegen macht, die von keiner lokalen Theorie jemals erklärt werden können. Er tat dies, indem er eine Obergrenze für die Korrelation von unterschiedlichen Messungen an einem verschränkten System herleitete, wie sie mit lokalen Theorien vorhergesagt werden können. Im Experiment konnte dann gezeigt werden, dass diese Obergrenze überschritten wurde. Damit ist bewiesen worden, dass es keinen Mechanismus gibt, der sowohl das Postulat der Lokalität erfüllt, als auch die Ergebnisse der Experimente wiedergeben kann. Da die Bellsche Ungleichung uns später auch noch beschäftigen wird, ist im Anhang eine Herleitung beschrieben.

## 3 Das Ekert-Verfahren

Es ist allen Verfahren der Quantenkryptografie gemeinsam, dass man sich quantenphysikalische Verfahren zu Nutze macht, um einen gemeinsamen Schlüssel über eine separate Leitung sicher zu übertragen. Die eigentliche verschlüsselte Übertragung findet dann über einen klassischen Kanal mit dem ausgehandelten Schlüssel statt.

Beim Ekert Verfahren nutzt man für den sicheren Schlüsselaustausch die Tatsache, dass Messungen an verschränkten Teilchen die Bellsche Ungleichung verletzen. Der entscheidende Punkt bei diesen Verfahren ist, dass ein Lauscher, der eine man-in-the-middle Atacke startet, um diesen Vorgang abzuhören, unweigerlich die Verschränkung zwischen den Messwerten der beiden Komunikationspartner aufhebt. Dies kann erkannt werden, indem untersucht wird, ob die Bellsche Ungleichung in der Statistik der Messwerte von Sender und Empfänger verletzt wird. Ist dies nicht mehr der Fall, muss davon ausgegangen werden, dass die Verschränkung aufgehoben wurde, was nur dadurch geschehen kann, dass jemand die Leitung abhört.

### 3.1 Das Verfahren im Detail

Wir nehmen im Folgenden an, dass Alice mit Bob kommunizieren möchte. Warum es bei Beispielen aus der Kryptografie immer Alice und Bob sind, die miteinander komunizieren, weiss ich leider auch nicht, aber es hängt wohl mit den Anfangsbuchstaben der Namen zusammen.

Als erstes wird über eine spezielle Leitung der Schlüssel ausgehandelt. Diese Leitung muss in der Lage sein, einzelne Photonen zu übertragen, ohne dass Verstärker dazu beitragen. Letztere würden, genau wie jemand der mithört, die Verschränkung aufheben. Diese Einschränkung begrenzt die mögliche Reichweite einen quantenkryptografischen Übertragung, aber mitlerweile hat man so bereits Distanzen von über 100km überwunden. Zudem braucht man noch einen Sender, der verschränkte Photonen erzeugt und je eines an Bob und Alice schickt. Typischerweise benutzt man hierfür die Verschränkung der Polarisation. Wenn bei einem Photon eine Polarisation von 90 Grad gemessen wird, dann würde beim anderen eine Polarisation von 0 Grad gemessen, wenn der Analysator entsprechend eingestellt wäre. Bei zwei beliebigen Stellungen ist die Wahrscheinlichkeit, dass beide Photonen die Polarisationsfilter passieren gleich $sin^2(\alpha)$, wobei $\alpha$ den Zwischenwinkel der beiden Stellungen der Filter bezeichnet.

Sowohl Alice als auch Bob, können die Polarisation des Photons, das sie empfangen in drei verschiedenen Richtungen messen. Getrennt und unabhängig voneinanden wählen beide zufällig eine dieser Richtungen aus. Nach einer bestimmten Zeit

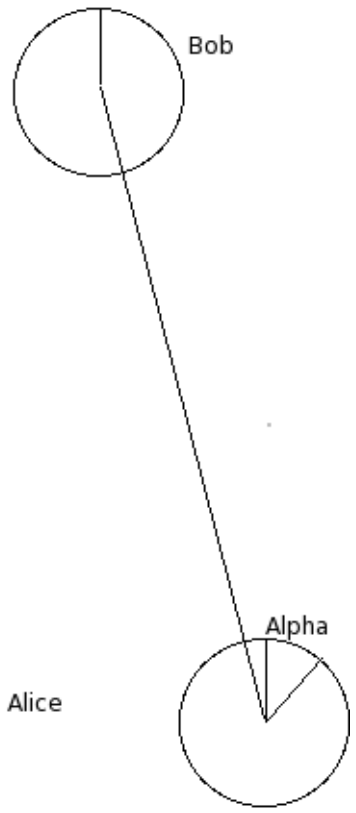


Abbildung 1: Der Schlüsselaustausch

vergleichen sie die vorgenommenen Einstellungen der Analysatoren. Dabei können zwei Fälle unterschieden werden:

- Die Analysatoren waren gleich eingestellt. In diesem Fall wissen sie vom jeweiligen Partner das Messergebnis, da die Photonen ja verschränkt waren. Diese Ereignisse können zur Erzeugung eines Schlüssels verwendet werden.

- Die Einstellungen waren unterschiedlich In diesem Fall können die Messergebnisse herangezogen, um zu testen, ob die Bellsche Ungleichung verletzt wurde. Ist dies nicht der Fall, muss davon ausgegangen, dass der Austausch abgehört wurde.

Die folgende Tabelle zeigt einen möglichen Teil eines derartigen Schlüsselaustausches. In der untersten Zeilen wird angegeben, was bei der Auswahl der Basen im jeweiligen Fall gemacht wird. Als mögliche Orientierungen werden dabei 0, 22.5 und 45 Grad angenommen.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Basis A | 22.5° | 22.5° | 0° | 45° | 45° | 45° | 0° | 45° | 0° |
| Messung A | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| Basis B | 22.5° | 22.5° | 0° | 22.5° | 45° | 22.5° | 22.5° | 22.5° | 45° |
| Messung B | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Klasse | Key | Key | Key | Bell | Key | Bell | Bell | Bell | Bell |

Ist der Schlüssel einmal ausgetauscht, kann er verwendet werden, um über eine klassische Leitung verschlüsselt zu komunizieren.

## 3.2 Eine Attacke

Ein Angreifer, der versucht, den Schlüsselaustausch zu belauschen, muss zwingend eine Messung an dem Photon vornehmen. Dadurch hebt er die Verschränkung zwischen Alice und Bob auf. Alternativ besteht die Möglichkeit, eine identische Kopie des Photons herzustellen und die Messung an einem der beiden Photonen vorzunehmen. Allerdings ist es in der Quantenphysik nicht möglich einr Kopie eines Teilchens, dass sich in einem beliebigen, unbekannten Zustand befindet, herzustellen, ohne das ursprüngliche Teilchen zu verändern. Wäre so eine Kopie möglich, könnte man zum Beispiel an einem Teilchen den Impuls messen und am anderen die Geschwindigkeit, was die Unschärfenrekation verletzen würde. Dieses Gesetz ist übrigens als no-cloning Prinzip bekannt. Aus diesen Gründen ist es theoretisch nicht möglich, den Austausch der Schlüssel zu belauschen, ohne dass dies entdeckt wird.

## 3.3 technische Realisierung

Abgesehen von der oben erwähnten Limitierung der Reichweite, gibt es noch ein zusätzliches Problem bei der Realisierung. Man muss in der Lage sein, ein einzelnes Photon zu detektieren. Genau in diesem Punkt haben Qin Liu und Sebastien Sauge angesetzt, um den Austausch des Schlüssels abzuhören. Der Ansatz wurde am 26. Chaos Comunication Congres vorgestellt. Der Vortrag kann hier angeschaut werden: http://events.ccc.de/congress/2009/Fahrplan/events/3576.en.html

Natürlich wurden hier nicht die Gesetze der Physik widerlegt, sondern es wurde eine Schwäche der Messinstrumente ausgenutzt. Aus diesem Grund ist auch nicht davon auszugehen, dass dieser Vortrag das Ende der Quantenkryptografie bedeutet. Aber es werden wohl bessere Messgeräte gebaut werden müssen. Zudem zeigt dieses Beispiel eines ganz deutlich. Auch wenn ein Verfahren in der Theorie noch so sicher ist, muss man bei der Implementierung sehr vorsichtig sein, um wirklich sicher zu sein.

# A Herleitung der Bellschen Ungleichung

## A.1 klassische Betrachtung

Wir stellen uns zwei verschränkte Photonen vor, die immer unterschiedliche Polarisationszustände haben. Diese werden jeweils an drei verschiedenen Filtern gemessen, welche Photonen, die in einer bestimmten Richtung polarisiert sind, durchlassen. Die drei Richtungen bezeichnen wir als $\vec{a}, \vec{b}$ und $\vec{c}$. Ein Photon, das durch $\vec{a}$ durchgeht, nennen wir $a^+$, eines, das gefiltert wird, $a^-$. Dabei sind folgende Ergebnisse möglich:

| Anzahl Photonen | Erstes Photon | zweites Photon |
|---|---|---|
| $N_1$ | $(a^+, b^+, c^+)$ | $(a^-, b^-, c^-)$ |
| $N_2$ | $(a^+, b^+, c^-)$ | $(a^-, b^-, c^+)$ |
| $N_3$ | $(a^+, b^-, c^+)$ | $(a^-, b^+, c^-)$ |
| $N_4$ | $(a^+, b^-, c^-)$ | $(a^-, b^+, c^+)$ |
| $N_5$ | $(a^-, b^+, c^+)$ | $(a^+, b^-, c^-)$ |
| $N_6$ | $(a^-, b^+, c^-)$ | $(a^+, b^-, c^+)$ |
| $N_7$ | $(a^-, b^-, c^+)$ | $(a^+, b^+, c^-)$ |
| $N_8$ | $(a^-, b^-, c^-)$ | $(a^+, b^+, c^+)$ |

Aus der obigen Tabelle können wir herauslesen, dass die Menge der Teilchen, bei denen das erste Teilchen durch $a^+$ gehen, und das zweite durch $b^+$ gehen, gleich $N_2 + N_3$ ist. Wenn viele Versuche gemacht werden, dann ist die Wahrscheinlichkeit für diese Ergebnisse:
$p(a^+; b^+) = \frac{N_3+N_4}{N}$
Allerdings gilt dies nur, wenn die Resultate unabhängig voneinander sind, also eine lokale Theorie zugrunde gelegt wird. Entsprechend erhalten wir folgende Beziehungen:
$p(a^+; c^+) = \frac{N_2+N_4}{N}$
$p(c^+; b^+) = \frac{N_3+N_7}{N}$
Daraus wird ersichtlich: $p(a^+; c^+) + p(c^+; b^+) = \frac{N_2+N_4}{N} + \frac{N_3+N_7}{N} \geq \frac{N_3+N_4}{N} = p(a^+; b^+)$

## A.2 quantenmechanische Betrachtung

In der quantenphysik ist die Wahrscheinlichkeit dafür, dass das erste Teilchen durch $\vec{a}$ geht genau 50%. Die Wahrscheinlichkeit, dass ein Teilchen sowohl durch $\vec{a}$ als auch durch $\vec{b}$ geht, beträgt $\frac{1}{2}\cos^2(\alpha)$ wobei $\alpha$ den Winkel zwischen den beiden Vektoren bezeichnet. Damit ist die Wahrscheinlichkeit dafür, dass das erste Teilchen durch $\vec{a}$ geht, und das zweite Teilchen durch $\vec{b}$ geht, die Gegenwahrscheinlichkeit, nämlich $1 - \cos^2(\alpha) = \sin^2(\alpha)$, da die Teilchen komplementär verschränkt sind. Somit erhalten wir für
$p(a^+; b^+) = \frac{1}{2}\sin^2(\alpha)$.
Analog erhalten wir für die beiden Richtungen $\vec{a}$ und $\vec{c}$:
$p(a^+; b^+) = \frac{1}{2}\sin^2(\beta)$
mit $\beta$ als Winkel zwischen den beiden Vektoren. Wählen wir nun $\beta < \alpha$, dann ist der Winkel zwischen $\vec{b}$ und $\vec{c}$ gleich $\alpha - \beta$. Somit erhalten wir für
$p(\vec{c}; \vec{b} = \frac{1}{2}\sin^2(\alpha - \beta)$.
Setzen wir diese Ergebnisse nun in die Bellsche Ungleichung ein, dann erhalten wir:
$\sin^2(\alpha) \leq \sin^2(\beta) + \sin^2(\alpha - \beta)$.

Für $\alpha = 45\,\text{deg}$ und $\beta = 22.5\,\text{deg}$ ergiebt das: $0.5 \leq 0.146 + 0.146$, was offensichtlich falsch ist. Damit is gezeigt, dass das Prinzip der Lokalität in der Quantenphysik nicht immer erfüllt ist.

# B Simulation eines Schlüsselaustausches

Das folgende kurze Programm simuliert einen Schlüsselaustausch. Es sollte durch die Komentare eigentlich selbsterklärend sein.

Listing 1: key exchange

```
#!/usr/bin/perl

use strict;
use warnings;

my $i;
my $pi = 3.1415926;

my @a = ((0*2*$pi)/360, (22.5*2*$pi)/360, (45*2*$pi)/360);
my @a_deg = (0, 22.5, 45);

my @b = ((0*2*$pi)/360, (22.5*2*$pi)/360, (45*2*$pi)/360);
my @b_deg = (0, 22.5, 45);

my @orientation_a;
my @orientation_deg_a;
my @orientation_b;
my @orientation_deg_b;
my @measurement_a;
my @measurement_b;
my @class;
my @Bell;
my $n_ap_bp = 0;
my $n_ap_cp = 0;
my $n_cp_bp = 0;

srand();
for ($i=0; $i<10000; $i++) {
    # Randomly chose the orientation of the filters
    # for measuring
    my $r1 = int(rand(3.0));
    my $r2 = int(rand(3.0));
    $orientation_a[$i] = $a[$r1];
    $orientation_deg_a[$i] = $a_deg[$r1];
    $orientation_b[$i] = $b[$r2];
    $orientation_deg_b[$i] = $b_deg[$r2];

    # Result of the measurement for a (always 50%
    $measurement_a[$i] = int(rand(2.0));
    # Probability for the same measurement at a and b
    my $p_ab = sin($orientation_a[$i] - $orientation_b[$i])
             * sin($orientation_a[$i] - $orientation_b[$i]);
    my $tmp = rand(1.0);
    if ($tmp > $p_ab) {
        # Different results at the two measurements
        if ($measurement_a[$i] == 0) {
            $measurement_b[$i] = 1;
        } else {
            $measurement_b[$i] = 0;
        }
    } else {
       # Same results
       $measurement_b[$i] = $measurement_a[$i];
    }
    if ( $orientation_deg_a[$i] == $orientation_deg_b[$i] ) {
        $class[$i] = "Key";
    } else {
        $class[$i] = "Bell";
        # Compute Bell's inequality with a=0, b=45, c=22.5
        if ( ($orientation_deg_a[$i]==0)
              && ($measurement_a[$i]==1) ) {
            if ( ($orientation_deg_b[$i]==45)
                  && ($measurement_b[$i]==1) ){
                # Number of a+,b+
                $n_ap_bp++;
            } elsif ( ($orientation_deg_b[$i]==22.5)
                        && ($measurement_b[$i]==1) ) {
                # Number of a+,c+
                $n_ap_cp++;
            }
        }
        if ( ($orientation_deg_a[$i]==45)
              && ($measurement_a[$i]==1) ) {
            if ( ($orientation_deg_b[$i]==22.5)
                  && ($measurement_b[$i]==1) ){
                # Number of c+,b+
                $n_cp_bp++;
            }
        }
    }
    print "$orientation_deg_a[$i]\t_$orientation_deg_b[$i]\t";
    print "$measurement_a[$i]\t_$measurement_b[$i]\t";
    print "$n_ap_bp\t_$n_ap_cp\t_$n_cp_bp\t_$class[$i]\n";
}

# vim: set tabstop=4 expandtab:
```