Johannes Tränkle

Die sichere Übertragung von Information mit Hilfe der Quantenkryptographie

Ein Beitrag aus der Reihe
„Juristen erklären Physikern die Welt“

Inhaltsverzeichnis

Will Alice an Bob eine geheime Nachricht übersenden, ergibt sich ein Problem. Wie lässt sich sicher verhindern, dass Eve abhören kann? Im folgenden Text soll dieser Frage nachgegangen werden. Es wird ein – zumindest theoretisch – sicheres Verschlüsselungs- und Übertragungssystem vorgestellt.[1]

1. Die sichere Verschlüsselung

Die meisten bekannten Verschlüsselungsalgorithmen lassen sich, früher oder später, von Unbefugten entschlüsseln[2]. Damit gewähren sie keine völlig sichere Übertragung geheimer Information. Lediglich der technische Fortschritt bzw. die Rechenleistung auf der Seite des Abhörenden bestimmen, wie lange ein geheimer Text o.ä. geheim bleibt.

Bei einem Verschlüsselungsverfahren konnte jedoch mathematisch nachgewiesen werden, dass ein Entschlüsseln nicht möglich ist. Dieses Verfahren soll hier vorgestellt werden.

Hierbei handelt es sich um das sogenannte One-Time-Pad-Verfahren[3].

1.1. Das Verfahren

Eine Möglichkeit ein solches Verfahren zu implementieren ist die XOR-Verschlüsselung. Im Computer werden aus allen Buchstaben Zahlen. Diese werden letztlich binär, also als Folge von 0en und 1en dargestellt.

XOR	**0**	**1**
0	0	1
1	1	0

Verwendet wird zur Ver/Entschlüsselung obiges Schema. Aus 0 XOR 1 wird also 1. Und aus 1 XOR 1 wieder 0. Es gilt folglich

Klartext XOR Schlüssel = Geheimtext
und
Geheimtext XOR Schlüssel = Klartext.

1 Mein Dank gilt Stefan Heinz, der in zahlreichen Telefonaten vom Thema abzulenken verstand.
2 Vgl. z.B. nur Heise Newsticker vom 27.09.2002 - distributed.net knackt RC5-64-Schlüssel, http://www.heise.de/newsticker/data/anw-27.09.02-001/.
3 Vgl. z.B. http://ig.cs.tu-berlin.de/ap/rg/1998-04/glossar/o-terms/onetimepad.html oder http://www.ch280.thinkquest.hostcenter.ch/crypto/onetime.html.

Beispiel:

Klartext	1	1	0	1
Schlüssel	**0**	**0**	**1**	**0**
Geheimtext	1	1	1	1
Schlüssel	**0**	**0**	**1**	**0**
Klartext	1	1	0	1

1.2. Die Probleme

Wo liegen aber die praktischen Probleme? Das One-Time-Pad-Verfahren ist nur dann wirklich zuverlässig, wenn folgende Bedingungen erfüllt sind:

- Der Schlüssel muss mindestens so lang wie der Klartext sein,
- er muss streng zufällig generiert worden sein und
- er darf nur einmal verwendet werden.

Gründe, für diese Voraussetzungen, sind folgende: Ist der Schlüssel unbekannt, so gibt es zwei grundsätzliche Möglichkeiten, dennoch den Klartext zu erhalten: Man kann entweder den *Geheimtext analysieren* oder *alle möglichen Schlüssel anwenden*.

Analysiert man den Text, so weiß man z.B., dass in der deutschen Sprache das „e“ am häufigsten vorkommt. Es wird folglich der am häufigsten vorkommende Buchstabe im Geheimtext gesucht. Dieser wird als „e“ definiert. Hiervon ausgehen wird weitergeforscht.

Durch den streng zufällig generierten Schlüssel werden aber zwei „e“s nicht zwingend gleich verschlüsselt. Die Statistik hilft nicht. Weil der Schlüssel außerdem mindestens so lange wie der Klartext ist, wiederholt er sich bei der Verschlüsselung nicht, weshalb auch eine Wiederholung nicht zu statistischen Zwecken verwendet werden kann. Wird er außerdem nur einmal verwendet, so lassen sich, zwei oder mehr Geheimtexte vorausgesetzt, auch hieraus keine statistischen Schlüsse ziehen, der Schlüssel war ja jeweils unterschiedlich. Weiterhin muss die Schlüsselgenerierung streng zufällig erfolgt sein, weil sonst u.U. auch über die Kenntnis des verwandten Verfahrens Rückschlüsse auf den Schlüssel möglich wären.

Hat der Klartext deshalb z.B. 500 Zeichen, so sind nach dem Verschlüsseln alle Texte, die 500 Zeichen umfassen gleich wahrscheinlich. Selbst wenn alle möglichen Schlüssel angewandt wurden, ist nicht bekannt, welcher der möglichen Texte der richtige war.

Für die Verschlüsselung ergeben sich jedoch einige Problem:
- Der übersandte Schlüssel ist (potentiell) sehr lang.
- Der Schlüssel muss geheim übertragen werden.

Schwer wiegt besonders das letzte Problem. Kann der Schlüssel nicht persönlich übergeben werden – was an dieser Stelle als „sichere“ Übertragung betrachtet werden soll – so ist dies der Schwachpunkt des ganzen Systems. Zwar ist das One-Time-Pad-Verfahren an sich nicht knackbar, kann aber der Schlüssel abgefangen werden, ist alle Mühe umsonst. Dieses Problem gilt es in Teil zwei zu lösen.

2. Die sichere Übertragung des Schlüssels[4]

Nachdem nunmehr geklärt ist, wie prinzipiell sicher verschlüsselt werden kann, stellt sich die Frage, wie der Schlüssel sicher übertragen werden kann.

2.1. Theoretische Grundlagen

Genutzt werden hierbei – üblicherweise – Photonen. Diese können verschieden polarisiert sein. Polarisation ist hierbei die Schwingungsebene des dazugehörenden elektrischen Feldes. Dieses setzt sich aus zwei Komponenten zusammen.
Im Rahmen der Quantenkryptographie wird die gerade (0°, 90°) und die ungerade (45°, 135°) Polarisation genutzt[5].

Das einzelne Photon hat somit zwei Eigenschaften:

1.) Die gerade Polarisation: Im Rahmen der Quantenkryptographie ist diese entweder auf 0 oder 1 gesetzt, was soviel bedeutet, wie dass bei 1 die gerade Polarisation vollständig vorhanden ist, während sie bei 0 völlig fehlt.
2.) Gleiches gilt für die ungerade Polarisation: Sie ist entweder vollständig vorhanden (1) oder eben nicht (0).

Auf diese Art und Weise lassen sich die oben schon angesprochenen vier Polarisationen erreichen:

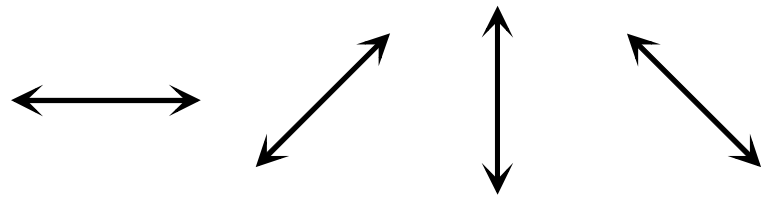


Abb. 1: Die vier Polarisationen

4 Vgl. hierzu z.B. Thomas Jennewein, Gregor Weihs, Anton Zeilinger – Schrödingers Geheimnisse, c't 2001, 260 ff.; Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden – Quantenkryptographie, Physikalische Blätter, 1999, 25 ff.

5 Hintergrund ist das Qubit. Hierbei handelt es sich um eine Einheit zur Quanteninformation. Anders als bei einer binären Speicherung, bei der zwei Zustände (0 und 1) gespeichert werden können, speichert ein Qubit zusätzlich noch die quantenmechanische Überlagerung (die sog. Superposition). Gemeint ist hiermit die Unsicherheit.
Hintergrund ist der Umstand, dass in der Quantenmechanik sichere Aussagen nicht möglich sind, es wird mit Wahrscheinlichkeiten gerechnet. Als Beispiel kann das von Ernst Schrödinger 1935 aufgestellte Gedankenexperiment gelten: In einer Kiste befindet sich eine Katze. Außerdem ist ein radioaktives Atom vorhanden. Über den Zerfall dieses Atoms gibt die Halbwertszeit Auskunft. Bei der Halbwertszeit handelt es sich aber um eine Wahrscheinlichkeitsaussage, die nur besagt, in welcher Zeit 50% der betroffenen Atome zerfallen sind. Welche genau dies sind, lässt sich nicht sagen. Somit ist unklar, wann das – einzige – Atom in der Kiste zerfällt. Mittels eines Detektors wird in dem Moment Gift freigesetzt, in dem das Atom tatsächlich zerfällt. Von außen lässt sich hierüber aber absolut keine Aussage machen. Erst, wenn die Kiste geöffnet wird, lässt sich bestimmen, ob die Katze lebt oder gestorben ist. Durch die Messung, das Öffnen der Kiste, wird ein Zustand folglich festgeschrieben, hieraiuf kommen wir später nocheinmal zurück. Solange die Kiste aber geschlossen ist, ist die Katze quantenmechanisch „tot“ und „lebendig“.
In einem Qubit ist daher ein Umstand gespeichert, über den sich nicht ohne weiteres eine Aussage machen lässt (die Superposition).

Durchläuft ein Photon nun eine Messeinheit (genannt Kalkspat), so kann immer nur eine dieser Komponenten gemessen werden. Folge hiervon ist, dass im Hinblick auf die andere Komponenten der diese betreffende Informationsteil verloren geht. Der Grund für diesen Umstand liegt in der *Heisenbergschen Unschärferelation*. Diese besagt für komplementäre Komponenten, wie wir sie hier vor uns haben, dass die Aussagen, die ich über die eine Komponente machen kann, immer ungenauer werden, je genauer ich die andere Komponente bestimme[6].

Bestimme ich die eine Komponente genau, kann ich über die zweite Komponente keinerlei Aussagen mehr machen.

Dieser Umstand soll hier an einem kurzen Beispiel veranschaulicht werden.

Fall A)
Gemessen werden soll ein 0° Photon. Der Kalkspat ist so eingestellt, dass er 0°- und 90°-Photonen messen kann. Mithin stimmt die Messung.

Fall B)
Betroffen ist ein 90° Photon. Wiederum ist der Kalkspat richtig eingestellt. Auch hier stimmt die Messung.

Fall C)
Gesendet wurde ein 45° Photon. Der Kalkspat ist zur Messung von 0°- und 90°-Photonen eingestellt. Somit ist eine korrekte Messung nicht möglich. Das Ergebnis der Messung ist völlig zufällig, kann also entweder bei 0° oder bei 90° liegen, da auch bei einem 45°- bzw. 135°-Photon gerade Polarisationen vorhanden sind.

Welche Folgerungen können nun gezogen werden, wenn der Kalkspat 0° ausgibt?

1.)Das Photon hatte tatsächlich eine Polarisation von 0° (Fall A)
2.)Das Photon hatte eine Polarisation von 45°, das Ergebnis war zufälligerweiße 0° (Fall C).
3.)Das Photon hatte eine Polarisation von 135°, das Ergebnis war wiederum zufälligerweiße 0° (Fall C).

Ohne zusätzliche Informationen lässt sich bei einem gemessenen Photon wegen der Heisenberschen Unschärferelation daher nur mit Sicherheit sagen, dass das Photon nicht mit 90° polarisiert war.

6 Vgl. hierzu z.B. den kurzen Aufriss bei http://www.quanten.de/unschaerferelation.html.

2.2. Praktische Umsetzung

2.2.1. Die Übertragung des Schlüssels

Soll ein Schlüssel übertragen werden, so werden zuvor den vier möglichen Polarisationen verschiedene Werte zugewiesen:

Polarisation	***Zuweisung***
0°, 45 °	logisches '0'
90°, 135°	logisches '1'

So ist die Übertragung eines Schlüssels möglich, wie er bei dem One-Time-Pad geschildert wurde.

Alice sendet nun also verschieden polarisierte Photonen, wobei sie sich die gewählte Polarisation merkt. Wichtig hierbei ist, dass die Polarisation tatsächlich völlig zufällig erfolgt. Andernfalls kann Eve u.U. Rückschlüsse auf die Einstellungen ziehen und so die Verschlüsselung brechen.
Bob auf der Gegenseite empfängt die Photonen und versucht, ihre Polarisation zu messen. Der von ihm verwendete Kalkspat kann wie dargelegt entweder 0° und 90° korrekt erkennen oder aber 45° und 135°.

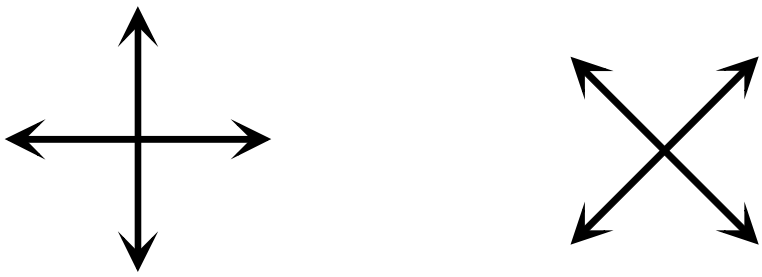


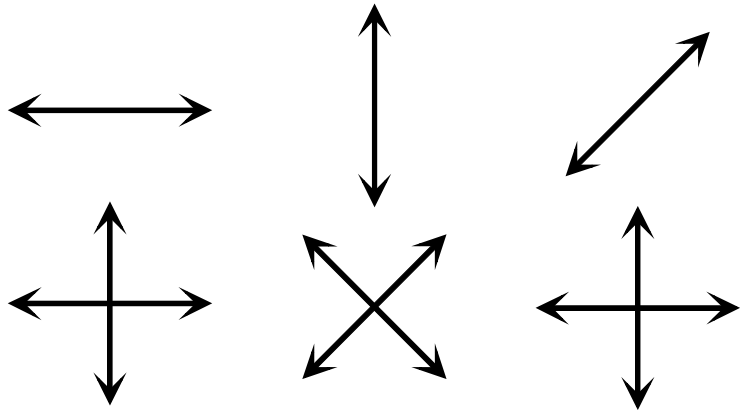
Abb. 2: Die möglichen Einstellungen des Kalkspats

Da Bob nicht weiß, wie die versendeten Photonen polarisiert sind, kann er seinen Polarisator nur völlig zufällig einzustellen. Die führt dazu, dass bei einem falsch eingestellten Polarisator ein völlig zufälliges Ergebnis erzielt wird[7].

Um feststellen zu können, welche Ergebnisse Bob korrekt gemessen hat, muss daher eine Abstimmung erfolgen. Hierzu überträgt Bob auf einem möglichst offenen Kanal die Einstellungen seines Polarisators. Der Kanal sollte deshalb offen sein, um Eve ein Dazwischenschalten schwerer zu machen[8]. Alice meldet jeweils zurück, ob Bobs Einstellungen richtig waren, ob die von ihm gemessenen Ergebnisse also mit der Wirklichkeit übereinstimmen. Falls Eve diese Übertragung abhört, kann sie folglich nur sagen, welche zwei von vier Möglichkeiten letztendlich in Betracht kommen[9].

7 Vgl. 2.1 a.E.
8 Es ist komplizierter, ein öffentliches Telefonnetz für die eigenen Zwecke zu missbrauchen, als ein Haustelefonsystem.
9 Teilt Bob mit, dass sein Polarisator 0° und 90° messen kann, so scheiden für Eve nur 45° und 135° als mögliche Messergebnisse aus. Welches Ergebnis Bob tatsächlich gemessen hat, lässt sich von Eve nicht feststellen. Hierzu aber später mehr.

Sowohl Bob als auch Alice wissen nun, welche Messergebnisse bei Bob korrekt gemessen werden. Diese werden als zum Schlüssel gehörend betrachtet. Die falschen Daten werden einfach gestrichen.



Treffer: '1' Verwerfen Verwerfen

Abb. 3: Was wurde empfangen und welche Schlüsse können daraus gezogen werden?

Damit ist der Schlüssel bekannt und es kann prinzipiell mit der Verschlüsselung und der Übertragung des Geheimtextes begonnen werden.

2.2.2. Wurde abgehört?

Zuvor muss aber noch festgestellt werden, ob abgehört wurde. Um dies feststellen zu können, wird ein Teil des Schlüssels offen von Bob an Alice übertragen. Beispielsweise könnten die Stellen 50 bis 100 übertragen werden. Im Anschluss werden diese, nun allgemein bekannten, Schlüsselteile gelöscht. Der Rest der übertragenen Daten ist der neue Schlüssel. Nun wird noch überprüft, ob die so übertragenen Schlüsselteile übereinstimmen. Ist dies nicht der Fall, so wurde potentiell abgehört.
Weshalb ist dem so?

2.2.3. Abhörmöglichkeiten

Welche Möglichkeiten stehen Eve zum Abhören zur Verfügung? Eve kann sich

- zum einen Dazwischenschalten, das Photon abfangen, es analysieren und es sodann weitersenden,
- zum anderen kann sie „überzählige“ Photonen abfangen und diese analysieren.

Zu „überflüssigen“ Photonen kommt es, wenn Alice nicht sicherstellen kann, dass immer nur ein einziges Photon versendet wird.

2.2.3.1. Dazwischenschalten

Schaltet sich Eve dazwischen, so kann sie, genau wie Bob, immer nur eine Komponente des Photons messen. Auch ihr steht nur ein „normaler“ Kalkspat zur Verfügung. Die korrekte Polarisatoreinstellung ist ihr (noch) nicht bekannt[10], sie weiß also nicht, welche Ergebnisse ihrer Messung korrekt sind und welche nicht.

10 Wir befinden uns noch bei der Übertragung der Photonen an sich. Die Polarisatoreinstellungen werden wie beschrieben erst im Anschluss offen übertragen.

Ihr ist deshalb auch (nur) das Weitersenden ihres gemessenen Ergebnisses möglich, nicht des korrekten Ergebnises.

In 50% der Fälle hat Eve – die ihren Polarisator ebenfalls zufällig ausrichtet – die richtige Einstellung gewählt, das von ihr gemessene Ergebnis stimmt also mit dem tatsächlich von Alice versendeten Photon überein. Bei den restlichen 50% erhält sie ein völlig zufälliges Ergebnis. Je nachdem, wie Bob seinen Polarisator eingestellt hat, stimmt das von ihm empfangene Ergebnis aber in wiederum 50% der Fälle zufälligerweise dennoch.

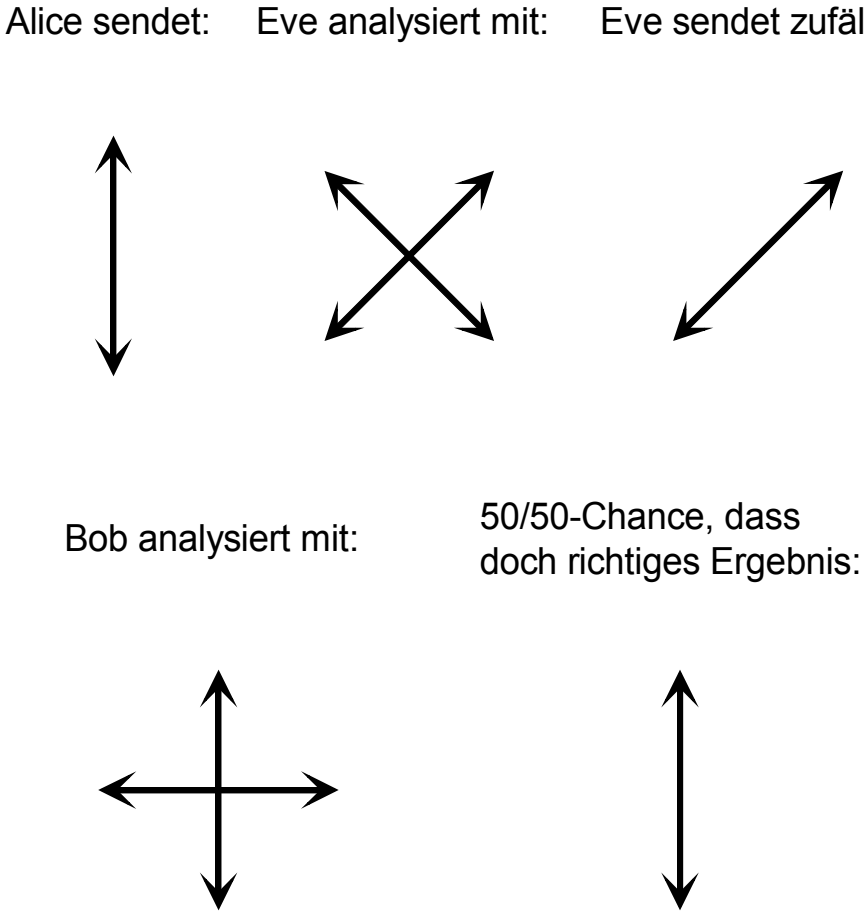


Abb. 4: Wann wird trotz Abhören dennoch ein richtiges Ergebnis übertragen?

Damit liegt die Fehlerquote, die sich ergibt, wenn sich Eve dazwischenschaltet bei 25%[11]. Auch bei einer ungestörten Übertragung kann es zwar wegen äußeren Einflüssen zu Fehlern kommen. Dieser „normale“ Informationsverlust liegt aber bei wenigen Prozent. Damit lässt sich ein Abhören von einem normalen Rauschen abgrenzen[12].

Wird auf diese Art und Weise ein Abhören festgestellt, so wird der übersendete Schlüssel einfach verworfen und Alice beginnt mit einer erneuten Übertragung. Durch das Abhören hat Eve also nichts gewonnen. Der von ihr abgefangene Schlüssel wird nie benutzt.

11 50% sind korrekt. Von 50% sind wiederum 50% korrekt. Damit sind 25% der übertragenen Ergebnisse falsch.

12 Auch mit verfeinerten Abhörmethoden lässt sich die Fehlerquote nicht unter 14% drücken. Damit ist ein Abhören aber immer noch deutlich erkennbar.

2.2.3.2. Abfangen

Verwendet Alice keine saubere Datenquelle, sendet diese also mehr als ein Photon gleichzeitig aus, so könnte Eve eines dieser Photonen abfangen und analysieren. Damit ist sie in derselben Position wie Bob, der ja andere, gleich polarisierte Photonen empfängt. Nachdem zwischen Alice und Bob die korrekten Polarisatoreinstellungen übertragen wurden, steht also auch Eve der korrekte Schlüssel zur Verfügung.
Wurde so abgehört, kann dies nicht festgestellt werden. Aus diesem Grund ist es für die hier vorgestellte Übertragung wichtig, dass nur saubere Datenquellen verwendet werden.

2.3. Praktische Probleme

Vorliegend wurde eine abhörsichere Schlüsselübertragung vorgestellt[13]. Abschließend soll noch auf einige praktische Probleme eingegangen werden:

1.) Wie soeben dargelegt, funktioniert das vorgestellte Verfahren nur dann zuverlässig, wenn eine saubere Datenquelle verwendet wird[14].
2.) Auch bei einer ungestörten Kommunikation kommt es zu Übertragungsfehlern. Diese können aber durch geläufige Fehlerkorrekturmaßnahmen unterbunden werden.
3.) Die Reichweite der Übertragung ist beschränkt[15]. Aus denselben Gründen, aus denen Eve nicht abhören kann, kann das Signal aber auch nicht verstärkt werden. Auch der Verstärker könnte nur einen Teil der Informationen auswerten, es käme zu einer Fehlerquote von 25%.
4.) Je länger der Übertragungsweg, desto mehr Photonen gehen auf dem Weg verloren. Dies führt dazu, dass der verwendete Schlüssel länger sein muss bzw. dass sich die Übertragungszeit verlängert, müssen doch verlorene Photonen kompensiert werden. Es stellt sich die Frage, wie Alice und Bob feststellen können, ob Photonen verloren gegangen sind. Hierzu sendet Alice immer in einem bestimmten Abstand neue Photonen. Wenn Bob in dieser Zeitspanne kein Messung vornehmen konnte, ging das Photon verloren, auch dieser Eintrag kann später nicht als Schlüsselteil verwendet werden.

3. Ergebnis

Als Ergebnis kann festgehalten werden, dass eine abhörsichere Übertragung von Information zwischen Bob und Alice theoretisch möglich ist. Wann bzw. ob das hier vorgestellte Verfahren jedoch massentauglich ist, kann noch nicht abgesehen werden, auch wenn entsprechende Systeme im kleinen Rahmen schon am Markt vorzufinden sind.

13 Vgl. hierzu auch den Artikel von Alexander Stirn in der SZ vom 18.12.03 – Alltagsprobleme einer schönen Theorie; http://www.sueddeutsche.de/sz/wissenschaft/red-artikel701/.
14 Vgl. hierzu Florian Rötzer „Quantenkryptographie - Wissenschaftler konnten ein System herstellen, dass nur ein Photon erzeugt“, Heise Online, 28.12.2000, http://www.heise.de/tp/deutsch/inhalt/co/4571/1.html.
15 Z.Zt. wohl auf ca. 67 km.