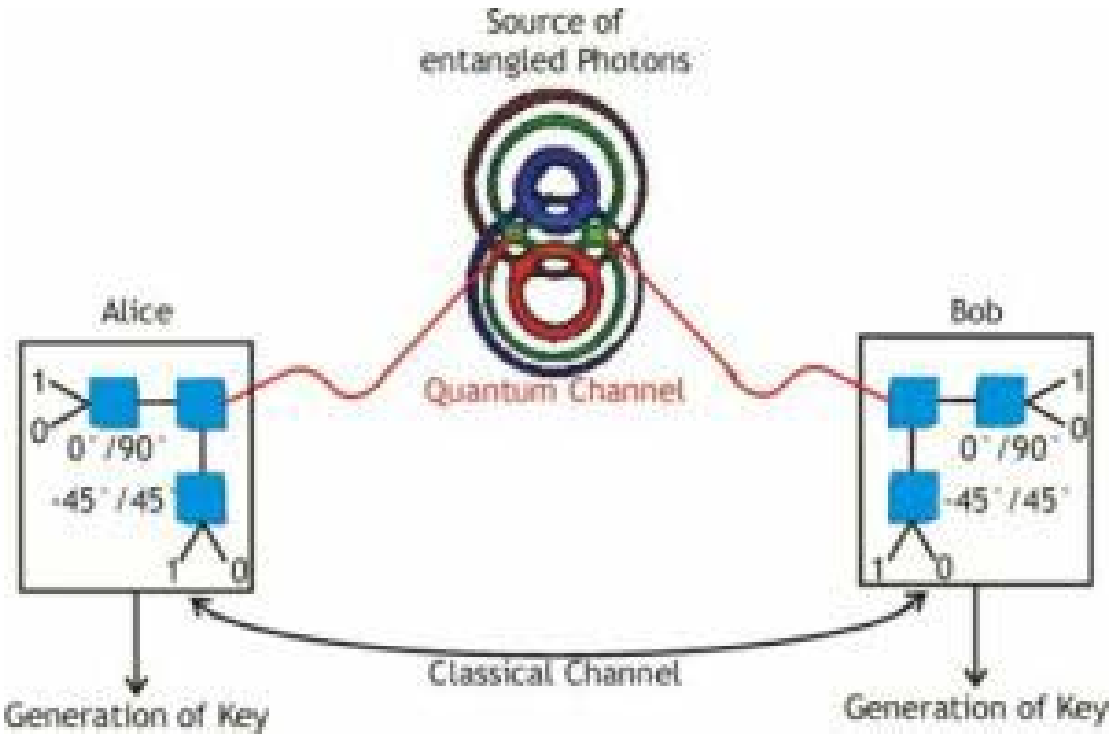
Quantenkryptographie



Ein Vortrag für das Seminar

„Quantencomputer“

von Martin Schmidt

I. Allgemeine Definitionen aus der Kryptologie

Da die Quantenkryptographie ein Teil der Kryptographie ist, macht es Sinn, zu Beginn dieser Ausarbeitung ein paar allgemeine Definitionen anzugeben. Folgende Begriffe aus der Kryptographie werden verwendet:

Definition Kryptographie

Kryptographie ist die Wissenschaft vom Übertragen von Informationen von einem Kommunikationspartner A zu einem anderen Kommunikationspartner B in einer von Gegner bedrohten Umgebung.

Definition Kryptographie

Kryptographie ist die Wissenschaft vom Übertragen von Informationen von einem Kommunikationspartner A zu einem anderen Kommunikationspartner B in einer von Gegner bedrohten Umgebung. Dazu werden Algorithmen verwendet, die Kryptosysteme genannt werden.

Definition Kryptoanalysis

Die Kryptoanalysis ist die Erforschung der Methoden eines unbefugten Angriffs gegen ein Kryptoverfahren. Zweck dieser Erforschung ist die Vereitelung des Zwecks eines Kryptosystems. Dieses Fachgebiet ist in Deutschland illegal.

Definition Kryptoanalyse

Die Kryptoanalyse ist die Analyse eines Kryptoverfahrens zum Zweck der Bewertung seiner Stärken und Schwächen. Dazu werden oft Verfahren aus der Kryptoanalysis verwendet.

Definition Kryptologie

Die Kryptologie ist die Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptographischen Verfahren. Die Kryptologie umfasst die Kryptographie und Kryptoanalyse.

Definition Quantenkryptologie

Die Quantenkryptologie ist die Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptographischen Verfahren unter Verwendung quantenmechanischer Prinzipen. Ein Beispiel aus der Quantenkryptoanalyse ist Shors Faktorisierungsalgorithmus.

II. Die Geschichte der Quantenkryptologie:

Theoretische Vorschläge

Der erste theoretische Vorschlag zur Anwendung von quantenmechanischen Prinzipien im Rahmen der Kryptographie kam von Stephen Wiesner in den 60er Jahren. Sein Vorschlag für fälschungssicheres Quantengeld war jedoch nicht technisch umsetzbar.

Diese Idee wurde von Wiesners Kollegen C. H. Bennett von IBM und Gilles Brassard von der Universität Montreal aufgegriffen und für die Konstruktion von Kryptoverfahren verwendet. Sie stellten ihre Vorschläge auf der Crypto 1982 vor. Da diese Vorschläge jedoch die Speicherung von Photonen benötigen, waren auch diese Vorschläge nicht umzusetzen.

Bennett und Brassard gaben nicht auf. Sie stellten 1984 das Protokoll BB84 vor. Dieses nutzte Photonen nicht mehr zum Speichern, sondern zum Übertragen von Information und war daher tatsächlich technisch praktikabel.

Es folgen Erweiterungen des Protokolls, die sich jedoch nicht durchsetzen.

Ein neues Verfahren wurde 1991 von Artur Eckert von der University of Cambridge vorgestellt. Das EPR (Einstein, Rosen, Podolsky)-Verfahren wurde allerdings später als kryptographisch äquivalent zu dem BB84-Protokoll bewiesen.

Praktische Erprobung

1989: IBM führt ein erstes Experiment mit dem BB84-Protokoll durch. Polarisierte Photonen übertrugen einen Schlüssel auf 32 cm Luftweg.

1994: British Telecom verkündet erfolgreichen Schlüsselaustausch über Glasfaserkabel von 10 km Länge. Gleichzeitig wird zum ersten Mal das EPR-Protokoll praktisch erprobt.

1995: Der Längenrekord für Schlüsselübertragung beträgt nun 23 km über optische Fasern.

1997: Erfolgreiche Versuche über einen 205 Meter langen Freiluftkanal bei Tageslicht werden durchgeführt.

1998: Es gelingt der Nachweis von nichtlokalen Korrelationen über 10 km hinweg. Damit vergrößert sich die praktikable Reichweite des EPR-Protokolls auf 10 km.

Heutzutage sind mit Glasfaser über 100 km erreichbar.

III. Messung zu alternativen Basen

Ein Qubit wird, wie bekannt, gemessen, indem mit Hilfe eines Messgeräts, das zwei Basiszustände des verwendeten Quanteninformationsträger unterscheiden kann, festgestellt wird, in welchem Basiszustand sich das Qubit befindet. Dabei wird allerdings dieser Basiszustand erst durch die Messung festgelegt. Bis dahin lassen sich nur die Wahrscheinlichkeiten dafür angeben, ob das Qubit in dem einen oder dem anderen Basiszustand ist.

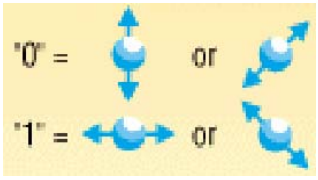
Für diese zwei Basiszustände existiert nur eine Anforderung: Sie müssen orthonormal zu einander stehen, das heißt, ihr inneres Produkt muss gleich Null sein. So sind verschiedene Basen denkbar, zu denen gemessen werden kann, und sie alle ergeben ein verwendbares System für einen Quantenrechner.

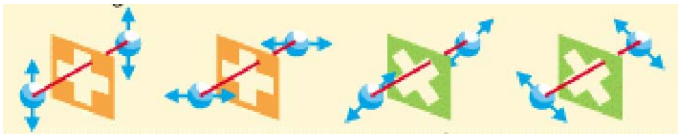
Die Quantenzustände lassen sich wie gewohnt darstellen: Seien $|a\rangle$, $|b\rangle$ Basiszustände für Qubits, die orthonormal zueinander stehen. $|a\rangle$ und $|b\rangle$ werden beliebig mit den Werten klassischer Bits assoziiert, z. b. 1 mit $|a\rangle$ und 0 mit $|b\rangle$. Jeder Quantenzustand lässt sich dann in der Form $\alpha|a\rangle + \beta|b\rangle$ darstellen.

Misst man einen Quantenzustand zu diesen Basen, so ergeben sich die gewohnten Wahrscheinlichkeiten für die zwei Werte: $|a\rangle$ ergibt sich mit $|\mathsf{a}|^2$, $|b\rangle$ ergibt sich mit $|\mathsf{b}|^2$.

An dieser Stelle eine Anmerkung: Da die technische Realisierung von Quantenkryptographischen Verfahren vollständig auf der Verwendung von polarisierten Photonen basiert, wird diese Abhandlung immer wieder auf diese physikalische Umsetzung zurückgreifen, um die beschriebenen Verfahren anschaulich zu machen. In diesem System werden Qubits erzeugt, indem man sie polarisiert. Zwei Polarisationsebenen, die rechteckig zu einander stehen, dienen als Basis. Das Messen erfolgt durch den Einsatz von Polarisationsfiltern, die nur Photonen einer bestimmten Polarisation registrieren, aber Photonen, deren Polarisationsebene nicht zu sehr von ihrer Messpolarisation abweicht, so polarisieren können, dass sie doch gemessen werden.

Das Messen zu verschiedenen Basen in diesem System erfolgt durch Assoziation zweier nicht senkrecht zu einander stehenden Polarisationsebenen mit einem klassischen Bitwert. Die rechtwinklig zu den beiden Ebenen stehenden Polarisationen werden dem anderen Bitwert zugeordnet.





Die Messung zu alternativen Basen erfolgt dann, wie dargestellt, einfach durch Wahl der entsprechenden Messfilter.

Eine praktische Anwendung dieses Verfahrens ist die Implementation eines quantenmechanischen Zufallsgenerators. Das Qubit $|\varphi\rangle$ werde bezüglich der Dualbasis B' gemessen, für die gilt:

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|0'\rangle + |1'\rangle\right),\ |1\rangle = \frac{1}{\sqrt{2}}\left(|0'\rangle - |1'\rangle\right) \qquad \text{(III.1)}$$

$$|\varphi\rangle = \frac{a}{\sqrt{2}}\left(|0'\rangle + |1'\rangle\right) + \frac{b}{\sqrt{2}}\left(|0'\rangle - |1'\rangle\right) = \frac{a+b}{\sqrt{2}}|0'\rangle + \frac{a-b}{\sqrt{2}}|1'\rangle \qquad \text{(III.2)}$$

Wenn $|\varphi\rangle$ gleich $|0\rangle$ ist, also a = 1 und b = 0 sind, dann ergeben die Wahrscheinlichkeiten der Zustände für die Messung $|\varphi\rangle = |0\rangle$ 0,5. Der Wahrheitswert der Gleichung ist also ein probabilistisches Bit.

IV. Klassische Kryptologie

Die Verfahren der Quantenkryptologie kommen im Bereich symmetrischer Kryptoverfahren zur Anwendung. Diese sind klassische Kryptoverfahren und sollen hier kurz erläutert werden.

Symmetrische Kryptoverfahren ermöglichen einem Sender A, einem Empfänger B eine Nachricht zu schicken, nur B entziffern kann, indem er spezielles Wissen benutzt, um sie zu entschlüsseln. Dieses Wissen wird „Schlüssel genannt und mit k (für Key) abgekürzt. Ein Symmetrisches Kryptoverfahren funktioniert wie folgt:

- Sender A verschlüsselt eine Nachricht m durch einen Schlüssel k mit Hilfe einer Verschlüsselungsfunktion f: f(m,k)= verschlüsselte Nachricht.
- Empfänger B entschlüsselt die Nachricht mithilfe desselben Schlüssels und der der zu f inversen Entschlüsselungsfunktion $f^{-1}(x, k)$. Es gilt: $f^{-1}(f(m, k),k) = m$

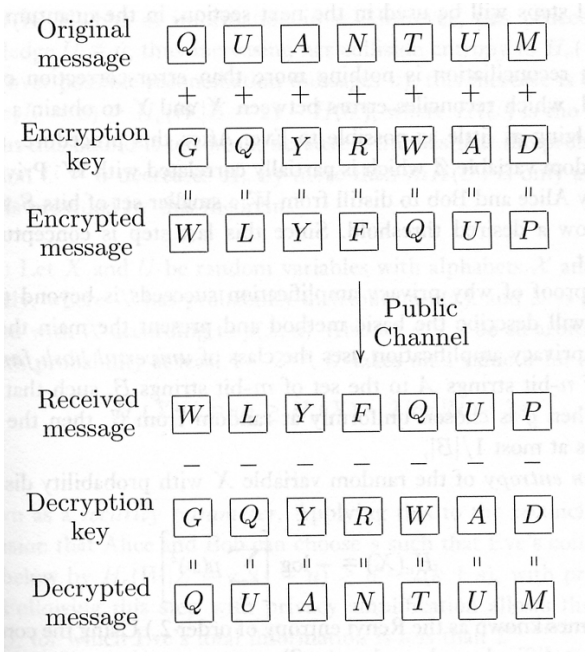
Dieses Verfahren heißt symmetrisches Kryptoverfahren, weil zur Ver- wie zur Entschlüsselung derselbe Schlüssel benutzt wurde. Dies ist nicht bei allen Kryptoverfahren der Fall.

Ein bekanntes Beispiel dieser Verfahren ist das so genannte One-Time-Pad-Verfahren. Es ist das einzige Verfahren, für das je bewiesen wurde, dass es die Anforderung an ein *informationstheoretisch sicheres Kryptoverfahren* erfüllt, auch wenn allerdings die Bedingung eingehalten werden muss, dass jeder Schlüssel nur einmal verwendet wird. Alle anderen Kryptoverfahren leiten ihre Sicherheit von unbewiesenen Aussagen über die Komplexität ihrer Verschlüsselungs- und Entschlüsselungsfunktionen ab.

Wie funktioniert dieses Verfahren? Es verwendet so genannte One Time Pads. Das sind zufällige Folgen von Buchstaben, oder, im digitalen Fall, Bits.

Das Verfahren produziert zunächst einen One Time Pad in der Länge der zu verschlüsselnden Nachricht. Die Verschlüsselungsfunktion „addiert“ dann das One Time Pad auf die Nachricht. Die Entschlüsselungsfunktion subtrahiert den Schlüssel von der chiffrierten Nachricht und macht sie so wieder lesbar.

Rechts ist ein Beispiel für die Verschlüsselung von Texten zu sehen.



Wenn Bitfolgen verschlüsselt werden sollen, dient die XOR-Verknüpfung von Nachricht und Schlüssel sowohl die Ver- als auch die Entschlüsselungsfunktion zur Verfügung. Auf Bitebene lässt sich dieses Kryptoverfahren dementsprechend sehr effizient implementieren.

Das einzige Problem stellt die Tatsache dar, das sowohl A als auch B in Besitz des Schlüssels k sein müssen. Dieser muss also irgendwie vereinbart werden, und da jeder, der k kennt, auch die verschlüsselte Nachricht lesen könnte, muss dies über einen sicheren Kanal geschehen.

Diesen sicheren Kanal zur Verfügung zu stellen ist Aufgabe der meisten Quantenkryptoverfahren.

V. Das BB84-Protokoll

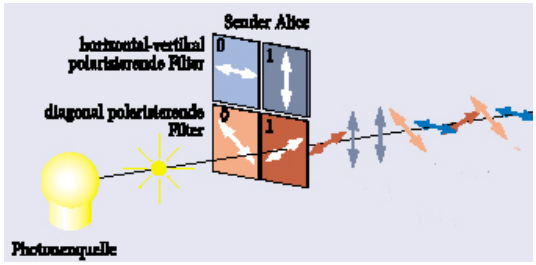
Das Verfahren

Das BB84-Protokoll von Bennett und Brachard ist ein Schlüsselübergabeprotokoll, welches seine Sicherheit aus quantenmechanischen Prinzipien ableitet und so die „Achilles-

ferse“ des One-Time-Pad-Verfahrens beseitigt, wenn es in Kombination mit ihm angewendet wird.

Um einen Schlüssel der Länge n zu übermitteln, geht Sender A folgendermaßen vor:

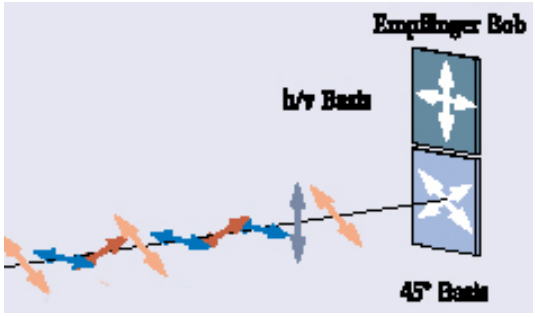
- Wähle a, b œ $\{0, 1\}^{4n}$ zufällig
- FOR i=1 TO 4n DO:
  - $|q_i\rangle \begin{cases} |a_i\rangle, \text{ falls } b_i=0 \\ H|a_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle)+(|-1\rangle^{a_i}|1\rangle), \text{ falls } b_i=1 \end{cases}$
- Schicke $|q_1\rangle \ldots |q_{4n}\rangle$ an B



Die Graphik veranschaulicht, wie diese Schritte vorgenommen werden, wenn ein Photonenbasiertes System verwendet wird. Um noch einmal zu paraphrasieren: A erzeugt aus dem klassischen Bitvektor einen Vektor von Qubits, wobei er in Abhängigkeit von b für jedes Element von a eine andere Basis wählt. Im Beispiel wird die Standard und die Hadamard-Basis verwendet, aber jedes Basenpaar, das nicht orthonormal zueinander steht, ist geeignet.

Sender B führt nach Empfang der Übertragung folgende Schritte aus:

- Wähle c œ $\{0, 1\}^{4n}$ zufällig
- FOR i=1 TO 4n DO:
  - Falls $c_i = 0$: Messung von q_i bezüglich Standard-Basis
  - Falls $c_i = 1$: Messung von q_i bezüglich Hadamard-Basis

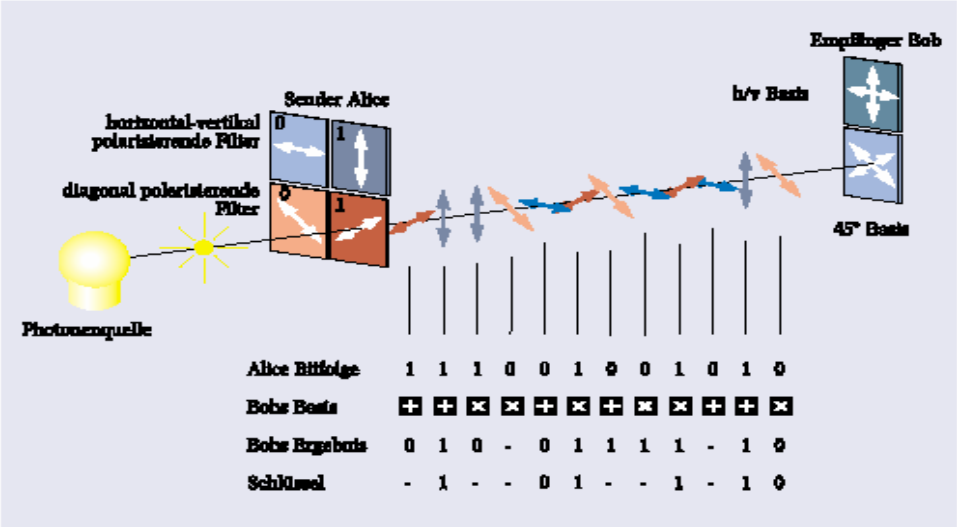


B rät also zufällig, zu welcher Basis er die empfangenen Qubits misst. Dabei merkt er sich sowohl den Vektor c, der bestimmt, zu welcher Basis er gemessen hat, als auch seine Messergebnisse.

A und B gleichen dann die Vektoren b und c über einen öffentlichen Kanal ab und ermitteln, welche Qubits von B mit derselben Basis gemessen wurden, mit der sie von A verschlüsselt wurden. Im statistischen Mittel wird dies bei 2n Qubits der Fall sein.

B schickt n dieser Messergebnisse an A, A schickt für diese n Messergebnisse die klassischen Bitwerte, die er verschlüsselt hat. Wenn Messung und Bitwert übereinstimmen, gilt die Übertragung als sicher. Die n Bits, die nicht über den öffentlichen Kanal gesandt wurden, werden als Schlüssel verwendet. Die folgende Grafik illustriert das gesamte Verfahren:

Die Begründung für die Sicherheit des Schlüsselaustauschs liegt darin, dass ein Angreifer C nur Informationen über den Schlüssel erhalten kann, indem er die von A zu B gesandten Qubits abfängt und selbst misst. Da er zu diesem Zeitpunkt allerdings nicht weiß, mit welcher Basis die Qubits erzeugt worden sind, kann er die korrekte Basis nur raten. Da die Messung den Superpositionszustand zerstört, kann C, um unentdeckt zu bleiben, nur das Ergebnis seiner Messung an B weitersenden, da ansonsten fehlende Übertragungen auffallen würden.



Sobald C eine andere Basis wählt als jene, die von A gewählt worden ist, bekommt er in 50 % der Fälle ein falsches Ergebnis heraus. Sollte B bei der Messung des veränderten Photons jedoch dieselbe Basis wie A wählen, müssten beide denselben klassischen Bitwert erhalten. Da aber C dem B ein falsches Ergebnis zugesandt hat, ist die Gleichheit verletzt und C ist entdeckt.

Mögliche Angriffspunkte

Es gibt mehrere theoretisch denkbare Angriffsverfahren. Es existiert jedoch kein momentan technisch mögliches Verfahren, welches keine Spuren hinterlässt. Vier Szenarien sind in der Diskussion erwogen worden. Sie bauen meist auf der etablierten Technik der durch polarisierte Photonen realisierten Qubits auf:

Intercept and Resend: Der Angreifer muss in diesem Fall die Gefahr, entdeckt zu werden, auf sich nehmen und vertraut darauf, dass die abweichenden Ergebnisse auf Rauschen in der Leitung zurückgeführt werden. Bei Systemen mit Polarisierten Photonen kann der Angreifer die Wahrscheinlichkeit, das richtige Ergebnis an B weiterzusenden, auf 85 % erhöhen, wenn er die abgefangenen Photonen zur so genannten „Breidbard“-Basis misst, einer Überlagerung zw. Linearer u. zirkulärer Polarisierung. Dafür erhält C nicht mehr mit jedem gemessenen Bit Informationen über den verwendeten Schlüssel.

Beamsplitting: Dieses Angriffszenario baut darauf, dass es sehr schwer ist Photonenpulse zu erzeugen, die nur aus einem Photon bestehen. Normalerweise schickt A mehrere

Photonen pro Puls, die alle dieselbe Polarisation aufweisen. Der Angreifer kann die Anzahl von Photonen in einem Puls messen, ohne Störungen zu erzeugen, die ihn verraten würden.

Falls ein Puls aus mehreren Protonen besteht, kann der Angreifer Photonen abzweigen (etwa durch einen halbdurchlässige Spiegel) und dennoch einen genügend hellen Impuls an B weiterleiten, um nicht aufzufallen. Mit dieser Methode würde sein Abhören der Leitung nicht entdeckt.

Kohärenter Angriff: Sollte der Angreifer in der Lage sein, Photonen zu speichern, könnte er mittels der Beamsplitting-Attacke Informationen erlangen und dann warten, bis A und B sich darüber verständigen, zu welchen Basen sie jeweils gemessen haben. Dann wäre er selbst in der Lage, die gespeicherten Qubits mit der korrekten Basis zu messen und so vollständige Informationen über den Schlüssel zu erhalten, ohne entdeckt zu werden.

Momentan ist es technisch unmöglich, Photonen zu speichern.

Generell gilt, dass die drei möglichen Angriffspunkte vereitelt werden können, wenn es zuverlässig gelingt, Photonenpulse zu erzeugen, die aus einem Photon bestehen. Dementsprechend wird in diese Richtung fieberhaft geforscht.

VI. Das B92-Protokoll

Das B92-Protokoll stellt eine Variante des BB82 Protokolls dar. Es nutzt physikalische Eigenschaften von Photonen aus und ist daher nicht auf andere Quantencomputervarianten übertragbar.

Das B92-Protokoll verwendet ebenso wie das BB84-Protokoll zwei Polarisationsfilter. Es werden also wieder zwei Basen verwendet, zu denen die Qubits erzeugt werden. Doch anstatt zwei Varianten für jeden klassischen Bitwert zu benutzen, wird ein Grundzustand der einen Basis mit der klassischen 1, ein Grundzustand der anderen Basis mit dem klassischen Wert 0 assoziiert.

Es werden generell zwei Basen verwendet, die zueinander um 45° verschoben sind.

So wie a nur zwei Grundzustände, einen pro Basis, erzeugt, so misst B auch nur für zwei Grundzustände. B misst jedoch auf die beiden nicht verwendeten Grundzustände(!). Das lässt sich mit Polarisationsfiltern einfach bewerkstelligen. Das Ergebnis ist, dass B zu 50 % mit genau der anderen Basis den Grundzustand misst, den A mit der einen Basis erzeugt. Hat. Zu 50 Prozent jedoch erhält er kein Signal. Misst er dagegen zur selben Basis, zu der A das

Photon polarisiert hat, so erhält er kein Signal, da er nach dem Grundzustand fahndet, der senkrecht auf dem steht, den das Photon aufweist.

Um das Verfahren ein wenig klarer werden zu lassen, benutzen wir ein Beispiel. Die verwendeten Polarisationebenen seien 0° x 90° für die erste und 45° x 135° für die zweite Basis. A versendet Photonen in den Grundzuständen 0°, assoziiert mit 1, und 45°, assoziiert mit 0. Bei einer Messung von B können dann folgende Ergebnisse auftreten (der assoziierte klassische Bitwert steht in Klammern):

Gesendet wird	0° (1)	0° (1)	45° (0)	45° (0)
Gemessen wird mit	90° (0)	135° (1)	90° (0)	135° (1)
Photon wird detektiert?	Nein	Vielleicht(1)	Vielleicht(0)	nein

B hält das Ergebnis seiner Messungen in b fest. Wann immer B das Photon detektiert hat, stimmt sein klassisches Messergebnis mit dem versendeten Bit von A überein. B übermittelt A die Position der von ihm gemessenen Photonen in dem von A versendeten Vektor (nicht sein Messergebnis!). Alle diese Positionen können dann als Schlüssel oder zum Fahnden nach möglichen Angreifern verwendet werden. Diese Verfahren funktionieren wie im BB84-Protokoll, und es existieren auch dieselben Angriffsmöglichkeiten.

VII: Das EPR-Protokoll

Das EPR-Protokoll ist das aktuellste voll ausgearbeitete Schlüsselübergabeprotokoll. Es verwendet so genannte nichtlokale Korrelationen verschränkter Zweiteilchensysteme. solche Korrelationen treten unter anderem bei Spin, Ortsimpuls und Polarisationszustand von Zweiteilchensystemen auf. Zunächst muss allerdings noch ein wenig Vorarbeit geleistet werden.

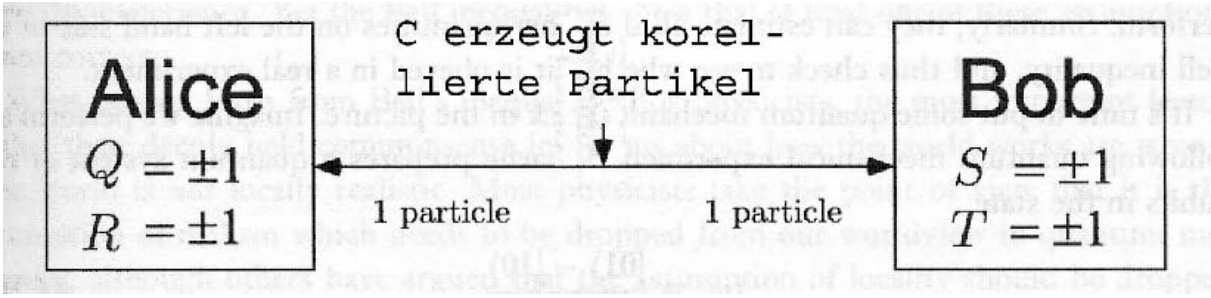
Die Bellsche Ungleichung

Die Bellsche Ungleichung ist eine Gleichung aus der klassischen Mechanik, das Verhalten zweier korrelierter Teilchen behandelt.

Das Herleitungsszenario ist wie folgt: Eine Partei C erzeugt Paare von korrelierten Teilchen, welche an die Experimentteilnehmer A und B gesendet werden. Die genaue Art von Cs Tätigkeit ist unwichtig, da in der klassischen Physik jede Art von Korrelation eine bestimmte Schwelle nicht überschreiten darf.

A und B erhalten jeder ein Teilchen. Jeder von beiden misst sein Teilchen auf eine charakteristische Eigenschaft. Dabei hat jeder von beiden zwei verschiedene Eigenschaften zur Wahl, von der er nur eine misst. Die Messmethoden von A seien bezeichnet als bezeichnet als P_Q und P_R, die Ergebnisse der Messungen heißen Q und R. Analog heißen die Messmethoden von B P_S, welches S ergibt, und P_T, deren Ergebnis T heißt. Die möglichen Ergebnisse mögen nur +1 und -1 betragen. Weiterhin messen A und B zum exakt gleichen Zeitpunkt an verschiedenen Orten, so dass sich die Messungen nicht gegenseitig beeinflussen können.

Die untenstehende Graphik veranschaulicht das Experiment.



Im statistischen Mittel müsste dann, da die Entfernung jede Beeinflussung der Messungen unter einander ausschließt, im statistischen Mittel folgende Ungleichung gelten, die als Bellsche Ungleichung bezeichnet wird:

E(QS)+E(RS)+E(RT)-E(QT)≤2

E(x) ist der Durchschnitt der Werte, die x annimmt. Die Herleitung ergibt sich aufgrund einfacher algebraischer Umformungen.

Was hat dieses Ergebnis nun mit der Quantenmechanik zu tun? Eine der verblüffenden Eigenschaften der Quantenmechanik ist, dass die Bellsche Ungleichung dort nicht gilt! Quantenmechanisch beeinflusste Teilchen weisen wesentlich stärkere Korellationen über wesentlich weitere Entfernungen auf, als es die klassische Physik erlaubt.

Der Grund dafür ist, dass in die Formulierung der Bellschen Ungleichung zwei Voraussetzungen eingeflossen sind:

Die Messgrößen haben feste Werte. Diese Annahme heißt *Assumption of realism*.

A und B beeinflussen sich nicht. Diese Annahme heißt *Assumption of localism*.

Eine von beiden Annahmen stimmt in der Quantenmechanik nicht. Da man meist von der Assumption of localism ausgeht, heißen solche quantenmechanischen Wechselwirkungen auch nichtlokale Korellationen. Wie wir gesehen haben, sind in gewissen Fällen diese Korrelationen stärker als alle Korrelationen, die von der klassischen Physik erlaubt sind. Bell bewies, dass diese Korrelationen nicht dadurch zustande kommen, dass beide mit denselben Eigenschaften geschaffen werden, sondern dass das eine Teilchen während der Messung zu-

fällig eine Eigenschaft annimmt, die ab dann sofort auch bei dem anderen Teilchen zu messen ist. Aus dieser Untersuchung ist die Bellsche Ungleichung entstanden.

Damit kann man die Bellsche Ungleichung benutzen, um Teilchen auf nichtlokale Korrelationen zu testen, da diese die Bellsche Ungleichung verletzen.

Das Verfahren

Auch dieses Verfahren verwendet in der Praxis polarisierte Photonen als Quantenträger. Eine unabhängige Quelle produziert Paare verschränkter Photonen (korrelierter Bits), die getrennt werden. Eines erhält A, eines erhält B, die zwei Parteien, die sich über einen Schlüssel einigen sollen. Wichtig ist hierbei zu bemerken, dass bei diesem Protokoll, keiner der Parteien den Schlüssel erzeugt, statt dessen entsteht er wirklich zufällig (siehe VIII.).

Wieder werden die Photonen sowohl von A als auch von B zu verschiedenen Basen gemessen. Die tatsächlich verwendete Basis wird zufällig gewählt. A und B merken sich das Ergebnis ihrer Messung.

Dann vergleichen A und B öffentlich die Wahl ihrer Basen. Dabei können drei Fälle auftreten:

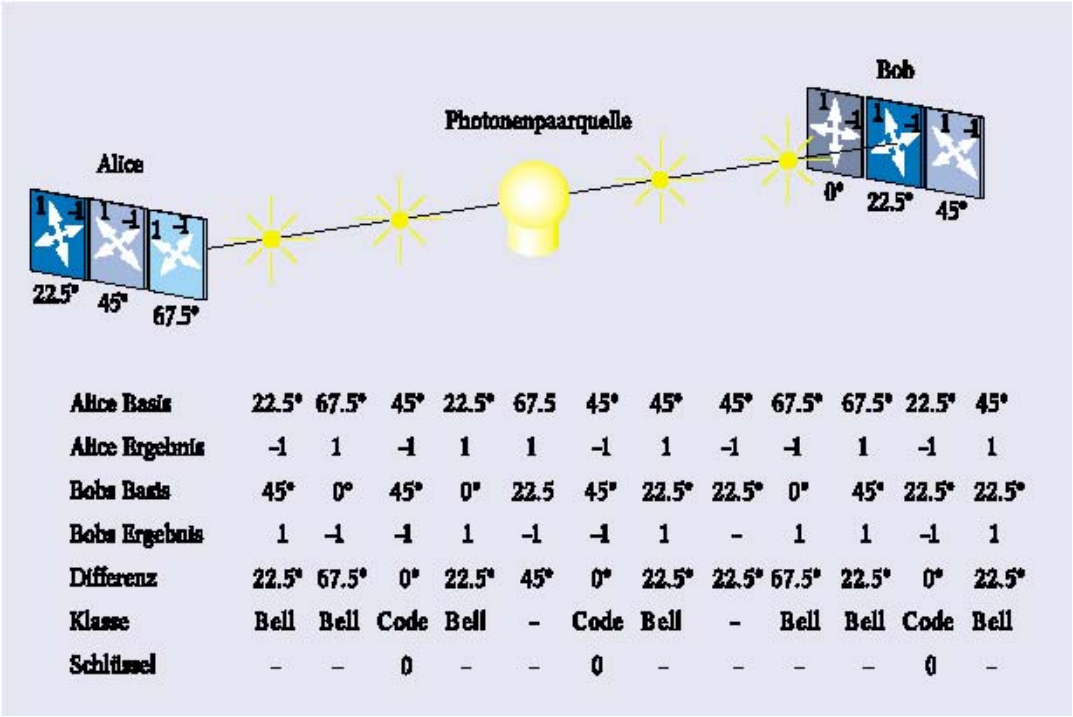
A und B haben dieselbe Basis gewählt. In diesem Fall korrelieren die Ergebnisse perfekt, falls kein Angreifer mithörte. Die sich ergebenden klassischen Bits sind identisch und können als Schlüsselbits verwendet werden, da sie nicht veröffentlicht wurden.

A und B haben verschiedene, mit einander vereinbare Basen gewählt: Die Schlüsselbits korrelieren zwar mit einander, aber sie sind im mittel nicht identisch. Solche Bits können mit der Bell-Ungleichung getestet werden.

A und B haben verschiedene, mit einander nicht vereinbare Basen gewählt: Diese Messergebnisse werden ignoriert.

Die Detektierung eines Lauschers geschieht mit Hilfe des Bell-Ungleichungstests. Wann immer die Photonen aus Fall 2 die Bell-Ungleichung nicht verletzen, ist die Korrelation zwischen den beiden Bits durch einen Lauscher zerstört worden und die Leitung nicht sicher.

Die unten stehende Graphik veranschaulicht das Verfahren.



Alice Basis	22.5°	67.5°	45°	22.5°	67.5	45°	45°	45°	67.5°	67.5°	22.5°	45°
Alice Ergebnis	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
Bobs Basis	45°	0°	45°	0°	22.5	45°	22.5°	22.5°	0°	45°	22.5°	22.5°
Bobs Ergebnis	1	-1	-1	1	-1	-1	1	-	1	1	-1	1
Differenz	22.5°	67.5°	0°	22.5°	45°	0°	22.5°	22.5°	67.5°	22.5°	0°	22.5°
Klasse	Bell	Bell	Code	Bell	-	Code	Bell	-	Bell	Bell	Code	Bell
Schlüssel	-	-	0	-	-	0	-	-	-	-	0	-

VIII. Ein paar generelle Bemerkungen zur Sicherheit

Die Sicherheit der quantenkryptologischer Verfahren beruht auf zwei Gesetzen der Quanteninformatik:

Das No Cloning Theorem: Qubits können nicht kopiert werden. Dieses Gesetz verhindert, dass ein eventueller Angreifer abgehörte Übertragungen einfach kopiert und das Qubit unverändert zum eigentlichen Adressaten weitersendet, ohne entdeckt zu werden.

Das **Information Gain implies Disturbance** Theorem: Jeder Versuch, nicht orthogonale Zustände von einander zu unterscheiden, erzeugt Störungen im Signal. Dieses Gesetz beruht darauf, dass Informationen über den Zustand eines Qubits nur durch Messung erlangt werden können, und diese zerstört den Superpositionszustand des Qubits.

Die hier diskutierten drei Verfahren weisen noch eine Sicherheitstechnische Besonderheit gegenüber allen anderen Schlüsselübergabeprotokollen auf: Eigentlich wird kein Schlüssel übergeben. Stattdessen entsteht der Schlüssel durch den Austausch von Information. Er entsteht „truly random“, nur durch den Zufall bestimmt. Das kann man sich wie folgt klarmachen:

Angenommen, A erzeugt ein zufälliges klassisches Bit b, und misst, abhängig vom zufälligen Vektor b, ihre Hälfte des EPR-Paares in der einen oder der anderen Basis und erhält so a. B tut dasselbe, abhängig von b', und erhält a'. Nun tauschen A und B b und b' aus, und wählen Messergebnisse aus a bzw. a', die sie mit derselben Basis gemessen haben, um sie als Schlüsselbits zu nutzen. Nun lässt sich feststellen, dass der Schlüssel erst feststeht, nachdem A bzw. B gemessen haben. Keiner von beiden kann im Vornherein festlegen, welcher Schlüssel sich ergeben wird.

Die Argumentation lässt sich leicht vom EPR-Protokoll auf die anderen beiden behandelten Protokolle übersetzen.

Daher werden die Verfahren der Quantenkryptologie gern auch als Geheimschlüsselerzeugungsverfahren statt als Schlüsseltransferprotokolle bezeichnet.

IX. Quantenkryptologie in der Praxis

1999 benutzten alle praktischen Experimente Photonen als Informationsträger und ihre Polarisationsebenen als Träger der Superpositionszustandsinformation. Damit geht jedoch ein Problem einher: Der Superpositionszustand lässt sich bei Photonen nicht verstärken.

Die Unvollkommenheit der Messgeräte wirft ein weiteres Problem auf: In der Praxis existiert auch bei Nichtvorhandensein eines abhörenden Angreifers eine Wahrscheinlichkeit, dass unkorrelierte Bits auftreten. Die Rate solcher Vorkommen, die so genannte Quantenbitfehlerrate, liegt momentan bei wenigen Prozent. Sie rührt aus Ungenauigkeit der Messungen, Doppelbrechung optischer Fasern (die Polarisation der Photonen ändert), und dem „Rauschen" der Detektoren, das Photonen „simulieren" kann, her

Um diese Probleme zu beheben, werden die von den Quantenkryptoverfahren erzeugten „Rohschlüssel durch zwei klassische Verfahren „veredelt", die man unter der Bezeichnung „Privacy Amplification" zusammenfasst.

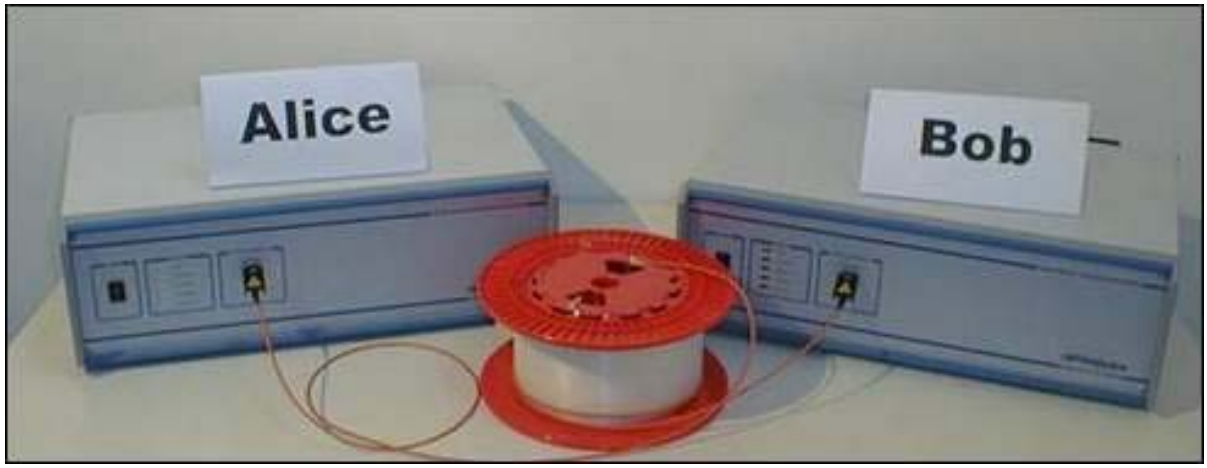
Zuerst erfolgt eine Fehlerkorrektur, auch „Information Reconciliation genannt. Für diese Aufgabe sind verschiedene klassische Verfahren bekannt, die auch alle genutzt werden. Ein praktisches Beispiel ist die Kontrolle der korrekten Übertragung durch Vergleichen des Parity Bits, so dass fehlerhaft übertragene Blöcke verworfen werden können.

Die eigentliche „Privacy Amplification" findet danach mit dem von Fehlern gereinigten Schlüssel statt. Sie hat zum Ziel, das Wissen, das ein Angreifer von dem zu verwendenden Schlüssel hat, zu verringern. Solche Verfahren setzen voraus, dass der Schlüssel bei beiden

Parteien simultan auf die gleiche eise verändert wird, ohne das weiteres Abgleichen über einen öffentlichen Kanal notwendig ist. Ein Beispiel dafür ist eine öffentlich bekannte Menge von Hashfunktionen, die so gewählt sind, dass sehr ähnliche Argumente sehr unterschiedliche Ergebnisse produzieren. A und B machen eine dieser Funktionen aus und wenden sie parallel auf ihre Rohschlüssel an. Solange ein Angreifer kein vollständiges Wissen über den Rohschlüssel hat, kann er kein Wissen über den veränderten Schlüssel erlangen.

Das Vorhandensein der Quantenbitfehlerrate stellt noch eine weitere Anforderung an die praktisch eingesetzten Versionen der vorgestellten Protokolle: A und B können Fehler in der Übertragung nicht von Folgen des Auftretens eines Angreifers unterscheiden. Es müssen also Fehlerraten festgesetzt werden, die als Messfehler akzeptiert werden.

Trotz dieser Probleme existiert bereits eine kommerziell verwertbare Implementation: Auf der CeBIT 2002 stellte die schweizerische Firma ID Quantique ein funktionierendes System vor. Die Daten: Entfernungsgrenzen 70 km (angegeben), 1000 Bit/s Übertragungsrate. Es ist untenstehend abgebildet.



X. Das Quantengeld

Die Idee stammt von Stephen Wiesner, aus den 60-er Jahren und war der erste Ansatz der Quantenkryptologie überhaupt. Vorgeschlagen wurde eine Möglichkeit, Geld fälschungssicher zu machen.

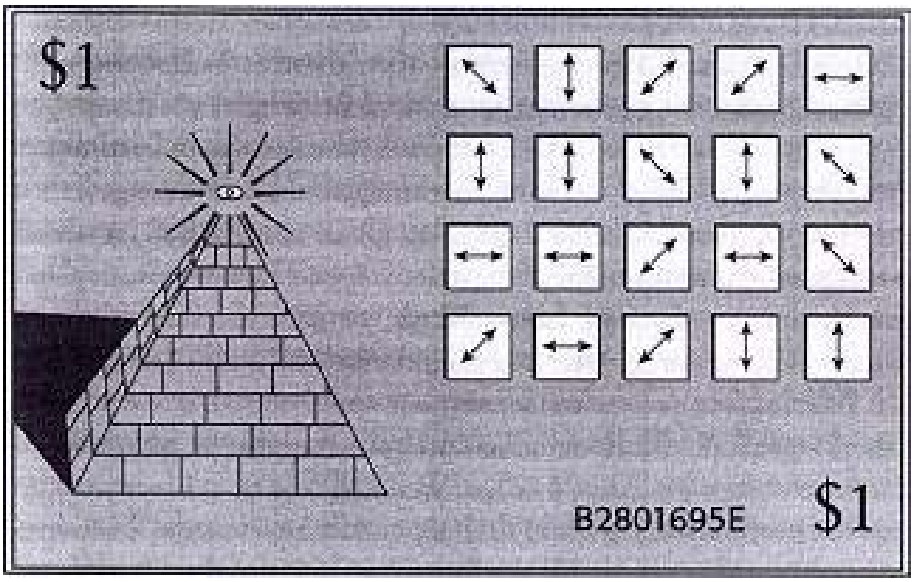
Ein Geldschein sollte Lichtfallen (Vorschlag 20) und eine Seriennummer erhalten. Die Lichtfallen würden Photonen mit verschiedenen Polarisierungen enthalten.

Diese Polarisierungen würden auf einer Urliste mit der entsprechenden Seriennummer in Verbindung gebracht, die nur Autorisierte besitzen würden.

Gefälschte Geldscheine ohne Vorlage würden schon wegen der Nummer beziehungsweise einem Konflikt zwischen Nummer und Polarisierung auffliegen.

Nach einer Vorlage erstellte Fälschungen würden scheitern, weil der Fälscher die Polarisationsfilter raten müsste, mit denen er die Photonen in den Fallen misst. Bei falsch gewähltem Filter würde er falsche Ergebnisse erhalten, da um 45° oder weniger von der Messbasis verschobene Polarisationsebenen „umspringen“ würden. Diese umgesprungenen Photonen würden die Fälschung auffliegen lassen.

Der technischen Realisierung des fälschungssicheren Geldes steht leider ein Problem entgegen: Es existieren noch keine Lichtfallen, die dauerhaft in der Lage sind, Photonen zu speichern. Die Idee wird daher allgemein abgelehnt. Untenstehend eine Konzeptzeichnung:



XI. Literaturverzeichnis:

- M.A. Nielsen, I.L. Chuang: Quantum Information and Quantum Computation, Cambridge University Press, 2000
- J. Torán: Skript zur Vorlesung Quantencomputer im SS 2003 an der Universität Ulm
- Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden: Quantenkryptographie, Artikel im Internet: http://www.pro-physik.de/Phy/pdfs/ISSART12536DE.PDF
- Christoph Heym, Quantenkryptographie, Vortrag im Internet: http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/stepan/index.htm

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!