Quantenkryptographie

Quantenmechanik Seminar
Prof. Georg Wolschin
Wintersemester 2013/14

Nils Gählert

08. November 2013

1 Definition Quantenkryptographie

Der Begriff *Quantenkryptographie* setzt sich zum einen zusammen aus dem Begriff *Quanten*, der hinlänglich aus der Quantenmechanik bekannt ist, zum anderen aus dem Begriff *Kryptographie*, der aus dem Griechischen kommt und übersetzt so viel heißt wie „geheimes Schreiben“. Eng mit der Kryptographie verbunden ist die sog. *Kryptoanalyse*, das „Auflösen des Geheimen“. Kryptographie und Kryptoanalyse zusammen bilden die *Kryptologie*, die „Lehre des Geheimen“.

Anders, als man vielleicht erwarten würde, verbirgt sich hinter der Quantenkryptographie kein Algorithmus, mit dem man unter Verwendung von Quanten tatsächlich verschlüsseln kann; vielmehr stellt die Quantenkryptographie Werkzeuge zur Verfügung, um das Problem des Schlüsselaustausches zu beheben – man spricht hier von dem *Quantenschlüsselaustausch (Quantum key distribution)*. Die Verschlüsselung an sich erfolgt mit einer klassischen Chiffre, dem sog. *One Time Pad*; man kann beweisen, dass es beim One Time Pad nicht möglich ist, zweifelsfrei einen Schlüssel zu berechnen. Diese Art der Verschlüsselung ist somit „perfekt sicher“, a-priori und a-posteriori-Wahrscheinlichkeit sind hier identisch:

$$p(m) = p(m|c) \tag{1}$$

Hierbei bezeichnet m den Klartext und c den Geheimtext.

Das klassische Szenario in der Kryptographie ist, dass eine Person A (Alice) einer Person B (Bob) eine Nachricht schicken möchte. „Evil Eve“ versucht dagegen, diese Nachricht abzufangen/zu manipulieren/...

2 Klassische Kryptographie

Zum besseren Verständnis aller Vorteile der Quantenkryptographie ist ein grundsätzliches Wissen über die klassische Kryptographie unerlässlich. Man unterscheidet hierbei zwischen *symmetrischen* Verschlüsselungen, bei denen zum Ver- und Entschlüsseln derselbe Schlüssel benutzt wird. Bei den *asymmetrischen* Verfahren gibt es zwei verschiedene Schlüssel, einen zum Verschlüsseln, der meist öffentlich bekannt ist *(public key)*, und einen zum Entschlüsseln, der jedoch privat ist *(private key)*.

2.1 Symmetrische Verfahren

Die meisten bekannten Chiffren sind symmetrisch.

Bereits die alten Griechen hatten mit der *Skytale* eine Transpositions-Chiffre entwickelt. Hierbei wurde um einen Holzstab mit zuvor festgelegtem, spezifischen Umfang ein Lederband gewickelt

und darauf ein Text geschrieben. Wickelte man das Band ab, war die ursprüngliche Nachricht nicht mehr erkennbar. Die Entschlüsselung war jedoch unter Verwendung eines Holzstabs identischer Geometrie möglich.

Die *Caesar-Chiffre* ist dagegen eine monoalphabetische Substitution. Hierbei wird jeder Buchstabe um eine bestimmte Anzahl weitergeschoben. So wird z.B. aus `HALLO` bei einer Verschiebung von 5 Buchstaben `MFQQT`. Das Knacken dieser Chiffre erfolgt durch eine Häufigkeitsanalyse der einzelnen Buchstaben. In der deutschen Sprache sind `ENIRSAT` die sieben häufigsten Buchstaben. In einem um 5 Stellen geschobenen Text wären dies `JSNWXFY`.

Blaise de Vigenère hat mit der nach ihm benannten Chiffre die Caesar-Chiffre erweitert und erheblich verbessert. Hier wird nun erstmalig ein Schlüsselwort benutzt, mit dem buchstabenweise der Klartext ähnlich der Caesar-Chiffre verschlüsselt wird. Lange wurde dieses Verfahren *le chiffre indéchiffrable* – die unentzifferbare Verschlüsselung – genannt.
Dennoch lässt sich ein derart verschlüsselter Text geeigneter Länge mit einer Häufigkeitsanalyse knacken.

Mit dem *One Time Pad* von 1918 wurde die Vigenère-Chiffre perfektioniert; das One Time Pad ist perfekt sicher und kann somit nicht geknackt werden. Das Besondere ist hierbei, dass die Schlüssellänge gleich der Textlänge ist. Eve hat keine Möglichkeit, den richtigen Schlüssel zu berechnen; sie kann zwar Schlüssel raten, die zufällig einen sinnvollen Text ergeben. Allerdings kann sie nicht sicher sein, dass Alice denselben Schlüssel verwendet hat, es gibt schließlich nahezu unendlich viele Möglichkeiten, sinnvolle Buchstabenkonstrukte zu generieren.

Mit dem *Data Encryption Standard (DES)* von 1976 wurde eine symmetrische Verschlüsselung entwickelt, die dem zunehmendem Einsatz von Computern gerecht wurde. 2000 wurde DES von dem *Advanced Encryption Standard (AES)* ersetzt. Auch heute wird AES weiterhin benutzt, zumeist mit einer Schlüssellänge von 256 Bit.

Das große Problem bei allen symmetrischen Verschlüsselungen ist, dass sich Alice und Bob auf einen gemeinsamen Schlüssel einigen müssen. Dies kann sich als schwierig erweisen, wenn sich Alice beispielsweise in den USA, Bob aber in Südafrika befindet. Mögliche Wege zum Schlüsselaustausch wären eine Telefonleitung, Brief, … die Eve aber auch alle abhören könnte.

2.2 Asymmetrische Verfahren

Das Problem des Schlüsselaustauschs kann mit asymmetrischen Verfahren gelöst werden. Das bekannteste Verfahren ist das *RSA*-Verfahren von 1977.

Hierbei gibt es einen *public key*, der auf entsprechenden Servern zentral gespeichert und somit der ganzen Welt zur Verfügung gestellt wird. Der *private key* verbleibt bei der jeweiligen Partei. Beide Schlüssel korrelieren miteinander; das Zurückrechnen des privaten Schlüssels aus dem öffentlichen Schlüssel ist extrem aufwendig und auch mit heutigen Rechnern kaum zu realisieren[1].

Hervorzuheben ist, dass mit RSA auch Signaturen erstellt werden können. Somit kann Bob auch verifizieren, dass er die Nachricht tatsächlich von Alice und nicht von Eve erhalten hat.

Die Nachteile der asymmetrischen Verfahren liegen in deren Effizienz; sie sind meist sehr langsam, da mit großen Zahlen potenziert werden muss.

2.3 Hybride Verschlüsselung

Durch geschickte Kombination von symmetrischer und asymmetrischer Verschlüsselung ist es möglich, die einzelnen Vorteile beider Systeme zu verbinden, um so eine möglichst gute und effiziente

[1] Die Großrechner der NSA sind hier natürlich eine Ausnahme!

Alice	Bob's Basis	Bob's Messung	Bob's Ergebnis	Kompatibilität	Schlüssel
$\|\updownarrow\rangle$	$\oplus$	$\|\updownarrow\rangle$	1	✓	1
$\|\updownarrow\rangle$	$\otimes$	$\|\nwarrow\rangle$,$\|\nearrow\rangle$	0,1	✗	-
$\|\leftrightarrow\rangle$	$\oplus$	$\|\leftrightarrow\rangle$	0	✓	0
$\|\leftrightarrow\rangle$	$\otimes$	$\|\nwarrow\rangle$,$\|\nearrow\rangle$	0,1	✗	-
$\|\nwarrow\rangle$	$\otimes$	$\|\nwarrow\rangle$	0	✓	0
$\|\nwarrow\rangle$	$\oplus$	$\|\leftrightarrow\rangle$,$\|\updownarrow\rangle$	0,1	✗	-
$\|\nearrow\rangle$	$\otimes$	$\|\nearrow\rangle$	1	✓	1
$\|\nearrow\rangle$	$\oplus$	$\|\leftrightarrow\rangle$,$\|\updownarrow\rangle$	0,1	✗	-

Tabelle 1: BB84 – Alle möglichen Kombinationen

Verschlüsselung zu erhalten.
Die Verschlüsselung der eigentlichen Daten erfolgt symmetrisch mit dem *session key*. Dieser wird bei jeder Verschlüsselungs-Session zufällig von einer der zwei Parteien generiert und asymmetrisch übertragen. Somit wird die Datenmenge, die asymmetrisch übertragen wird, auf ein Minimum reduziert, das Problem des Schlüsselaustauschs dagegen elegant gelöst.

Das *SSL/TLS*-Protokoll ist das wohl bekannteste Beispiel für eine hybride Verschlüsselung. Man kann am `https://` erkennen, dass man verschlüsselt im Internet surft.

Die Quantenkryptographie ist im Grunde genommen auch eine hybride Verschlüsselung. Wenn Alice und Bob es schaffen, unerkannt von Eve einen Schlüssel zu übertragen, den nur sie beide kennen, haben sie mit dem One Time Pad eine perfekte Verschlüsselung – somit können die beiden sicher miteinander kommunizieren.

3 Quantenschlüsselaustausch

Die Grundlagen für den Quantenschlüsselaustausch ist die Polarisation von Photonen. Ebenso kann man auch den Spin, … von Teilchen nutzen.

3.1 BB84

Bennet und Brassard haben 1984 eine erste Möglichkeit vorgeschlagen, wie man mit Hilfe von polarisierten Photonen einen Schlüssel austauschen kann.

Hierbei polarisiert Alice Photonen zufällig in einer von vier möglichen Polarisationsrichtungen $|\updownarrow\rangle$, $|\leftrightarrow\rangle$,$|\nearrow\rangle$, $|\nwarrow\rangle$ und schickt diese Photonen über einen Quantenkanal (Glasfaserkabel, Teleskopleitung) zu Bob. Dieser misst die Polarisation in einer zufällig ausgewählten Basis $\oplus$ oder $\otimes$. Da Alice und Bob sich zuvor darauf verständigt haben, welche Polarisation in welcher Basis dem Bit „1“ und welche Polarisation dem Bit „0“ entspricht, übertragen sie so einen Schlüssel.

Allerdings wird Bob in 50% aller Fälle die falsche Basis wählen. Durch einen Vergleich der gewählten Basen können Alice und Bob diese 50% herausfinden und aus dem übertragenen Schlüssel streichen. Dieser Vergleich kann über eine öffentliche Leitung (z.B. Telefon) stattfinden, da keinerlei Information über den Schlüssel ausgetauscht wird. Die möglichen Kombinationen können aus Tabelle 1 entnommen werden.

Falls Eve lauscht, hat sie natürlich auch das Problem, dass sie zufällig eine Messbasis auswählen muss. Ein mögliches Angriffsszenario ist die sog. *Intercept and Resend*-Attacke. Hierbei misst Eve Alice's Photon und präpariert ein entsprechendes Photon, welches sie an Bob schickt.

Wählen Alice und Bob jetzt die identische Basis, Eve aber die falsche, präpariert sie ein „falsch“ polarisiertes Photon. Gemäß den Gesetzen der Quantenmechanik erhält Bob jetzt nun wiederum nur in 50% aller Fälle das korrekte Ergebnis. Ein Beispiel: Alice schickt $|\updownarrow\rangle$, Eve misst mit $\otimes$ und

Alice	Bob's Basis	Bob's Messung	Bob's Ergebnis	Kompatibilität	Schlüssel
$\|\leftrightarrow\rangle$	$\oplus$	$\|\leftrightarrow\rangle$	0	✗	-
$\|\leftrightarrow\rangle$	$\otimes$	$\|\swarrow\nearrow\rangle$	1	✗	-
$\|\leftrightarrow\rangle$	$\otimes$	$\|\nwarrow\searrow\rangle$	0	✓	0
$\|\swarrow\nearrow\rangle$	$\otimes$	$\|\swarrow\nearrow\rangle$	1	✗	-
$\|\swarrow\nearrow\rangle$	$\oplus$	$\|\leftrightarrow\rangle$	0	✗	-
$\|\swarrow\nearrow\rangle$	$\oplus$	$\|\updownarrow\rangle$	1	✓	1

Tabelle 2: B92 – Alle möglichen Kombinationen

erhält $|\swarrow\nearrow\rangle$, Bob misst dagegen korrekt mit $\bigoplus$. Dann gilt:

$$|\swarrow\nearrow\rangle = \frac{1}{\sqrt{2}} \left(|\updownarrow\rangle + |\leftrightarrow\rangle \right) \tag{2}$$

$$| \langle \updownarrow | \swarrow\nearrow \rangle |^2 = \frac{1}{2} \tag{3}$$

$$| \langle \leftrightarrow | \swarrow\nearrow \rangle |^2 = \frac{1}{2} \tag{4}$$

Falls Eve lauscht, stimmen im Schnitt also 25% des übertragenen Schlüssels nicht überein! Die Sicherheit von BB84 liegt nicht im Verhindern, sondern im Erkennen von möglichen Lauschangriffen.

Um zu überprüfen, ob Eve gelauscht hat, können Alice und Bob entweder Teile des Schlüssels vergleichen oder einen Paritätsvergleich durchführen. Hierbei gilt für den partiellen Schlüsselvergleich:

$$p(n \text{ übereinstimmende Bits}) = \left(\frac{3}{4} \right)^n \tag{5}$$

Die verglichenen Positionen müssen selbstverständlich aus dem Schlüssel gestrichen werden. Dagegen bleibt beim Paritätsvergleich der gesamte Schlüssel erhalten. Hierbei werden Teilmengen des Schlüssels auf eine gerade/ungerade Anzahl von 0/1 verglichen. Es gilt:

$$p(n \text{ übereinstimmende Bereiche}) = \left(\frac{1}{2} \right)^n \tag{6}$$

Mit dem so generierten Schlüssel können Alice und Bob einen One Time Pad starten – die beiden kommunizieren nun perfekt sicher!

3.2 B92

Bennet hat 1992 mit B92 eine Vereinfachung gegenüber BB84 vorgeschlagen. Hier hat Alice nur die 2 Zustände $|\leftrightarrow\rangle$, was dem Bit „0“ entspricht, und $|\swarrow\nearrow\rangle$, was Bit „1“ entspricht, zur Verfügung. Bob misst wiederum mit $\bigotimes$ und $\bigoplus$. Die möglichen Kombinationen sind in Tabelle 2 dargestellt.

Misst Bob $|\leftrightarrow\rangle$ oder $|\swarrow\nearrow\rangle$, so werden diese Positionen im Schlüssel verworfen, da Bob sich nicht sicher sein kann, ob Alice tatsächlich diese Zustände benutzt hat oder ob er die falsche Basis gewählt hat.

Die weiteren Schritte stimmen mit denen in BB84 überein. Es ist zu bemerken, dass bei B92 im Schnitt nur 25% aller Photonen am Ende für den Schlüssel benutzt werden können, während es bei BB84 50% sind.

Alice's Basis	Bob's Basis
0°	0°
45°	-22.5°
22.5°	22.5°

Tabelle 3: E91 – Die Basen von Alice und Bob

3.3 E91

Das E91 Protokoll wurde 1991 von Artur Ekert vorgeschlagen und beruht auf der Verschränkung von den zu messenden Teilchen. Alice und Bob wählen je drei aus vier verschiedenen Basen bzw. Polarisatorwinkeln; zwei müssen dabei identisch sein (siehe auch Tabelle 3). Alice und Bob verständigen sich darauf, ob dem Ereignis „Ein Photon wird detektiert" das Bit „1" oder „0" zuzuordnen ist. Alice und Bob erhalten ihre Photonen aus einer Photonenquelle, die verschränkte Photonen erzeugt. Obwohl es sich um zwei Teilchen handelt, sind diese zwei Teilchen als ein System zu betrachten. Mögliche Wellenfunktionen sind z.B. die sog. *Bell-Zustände*:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left|H_A H_B\right\rangle \pm \frac{1}{\sqrt{2}}\left|V_A V_B\right\rangle \qquad \text{(symmetrisch)} \tag{7}$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left|H_A V_B\right\rangle \pm \frac{1}{\sqrt{2}}\left|V_A H_B\right\rangle \qquad \text{(antisymmetrisch)} \tag{8}$$

Hierbei ist klar, dass bei den symmetrischen Wellenfunktionen Alice und Bob dasselbe Ergebnis messen, d.h. bei einer Messung mit derselben Polarisatoreinstellung entweder beide das Photon detektieren oder eben nicht detektieren. Detektiert Alice ein Photon der asymmetrischen Wellenfunktion, so kann sie sich sicher sein, dass Bob dieses nicht detektiert:

$$\left|\left\langle V_A V_B|\Phi\right\rangle\right|^2 = \left|\left\langle H_A H_B|\Phi\right\rangle\right|^2 = \frac{1}{2} \qquad \text{(symmetrisch)} \tag{9}$$

$$\left|\left\langle V_A H_B|\Psi\right\rangle\right|^2 = \left|\left\langle H_A V_B|\Psi\right\rangle\right|^2 = \frac{1}{2} \qquad \text{(antisymmetrisch)} \tag{10}$$

$|V_i\rangle$ und $|H_i\rangle$ stehen hierbei für Vertikal bzw. Horizontal, was aber identisch mit einem detektierten bzw. absorbierten Photon ist.

Nachdem Alice und Bob die Photonen von der Photonenquelle empfangen haben, kommunizieren sie über einen öffentlichen Kanal und streichen nun zunächst alle Positionen, bei denen die Polarisatoren eine Winkeldifferenz von $\delta = 45°$ haben. In dieser Einstellung stimmen nur 50% der Messergebnisse überein.

Alle Positionen, an denen die Differenz $\delta = 0°$ beträgt, werden als Schlüssel benutzt. Hat die Photonenquelle Photonen mit antisymmetrischer Wellenfunktion ausgesendet, so muss einer der beiden seine Messergebnisse flippen. Allerdings ist die Wahrscheinlichkeit, dass Alice und Bob dieselbe Basis wählen lediglich $\frac{2}{9}$.

Es bleiben noch die Photonen, bei der Alice und Bob eine Differenz von $\delta = \pm 22.5°$ und $\delta = 67.5°$ haben. Mit diesen Photonen überprüfen die beiden die Sicherheit ihres Kommunikationskanals über die sog. *CHSH-Ungleichung*, die 1969 als Verallgemeinerung der Bellschen-Ungleichungen entwickelt wurde. Hierbei spielen der Erwartungswert $\mathbb{E}$ und der Korrelationskoeffizient $\mathbb{S}$ eine wichtige

Rolle:

$$\begin{aligned}
\mathbb{E}(a_i, b_j) :=& \langle\psi| E_a \otimes E_b |\psi\rangle && (11)\\
=& \langle\psi| (|a_i^+\rangle\langle a_i^+| - |a_i^-\rangle\langle a_i^-|) \otimes (|b_j^+\rangle\langle b_j^+| - |b_j^-\rangle\langle b_j^-|) |\psi\rangle && (12)\\
=& \langle\psi| \, |a_i^+, b_j^+\rangle\langle a_i^+, b_j^+| + |a_i^-, b_j^-\rangle\langle a_i^-, b_j^-| - \\
& |a_i^+, b_j^-\rangle\langle a_i^+, b_j^-| - |a_i^-, b_j^+\rangle\langle a_i^-, b_j^+| \, |\psi\rangle && (13)\\
=& P(a_i^+, b_j^+) + P(a_i^-, b_j^-) - P(a_i^+, b_j^-) - P(a_i^-, b_j^+) && (14)\\
=& \pm\cos(a_i - b_j) && (15)\\
\mathbb{S} =& \mathbb{E}(a_1, b_3) + \mathbb{E}(a_1, b_2) + \mathbb{E}(a_2, b_3) - \mathbb{E}(a_2, b_2) && (16)
\end{aligned}$$

Die Werte $P(a_i^\pm, b_j^\pm)$ sind hierbei die Wahrscheinlichkeiten bzw. die relativen Häufigkeiten, dass Alice mit Polarisatorstellung i ein Photon detektiert (+) bzw. nicht detektiert (-). Dasselbe gilt für Bob mit Polarisatorstellung j. Für $\mathbb{S}$ liefert die Quantenmechanik:

$$\mathbb{S} = \pm\, 2\sqrt{2} \tag{17}$$

Die CHSH-Ungleichung sagt nun, dass im Falle einer Theorie mit „verborgenen Variablen“, d.h. wenn Eve tatsächlich gelauscht hat, für $\mathbb{S}$ gelten muss:

$$-2 \leq \mathbb{S} \leq 2 \tag{18}$$

Wenn Eve lauscht, sind die beiden Photonen nicht verschränkt. Sie muss nun entweder Bob und/oder Alice ein Photon schicken. Wir gehen hier davon aus, dass sie beiden eines schickt und für die beiden jetzt sozusagen die „Quelle“ ist. Allgemein macht sie das mit einer Verteilung $p(\varphi_a, \varphi_b)$, wobei φ_i die Polarisation darstellt. Nun gilt:

$$\mathbb{E} = \iint p(\varphi_a, \varphi_b) \cos(a_i - \varphi_a) \cos(b_j - \varphi_b) \, \mathrm{d}\varphi_a \mathrm{d}\varphi_b \tag{19}$$

Und für $\mathbb{S}$ ergibt sich:

$$\begin{aligned}
\mathbb{S} = \iint p(\varphi_a, \varphi_b) (& \cos(a_1 - \varphi_a) \cos(b_3 - \varphi_b) \\
& + \cos(a_1 - \varphi_a) \cos(b_2 - \varphi_b) \\
& + \cos(a_2 - \varphi_a) \cos(b_3 - \varphi_b) \\
& - \cos(a_2 - \varphi_a) \cos(b_2 - \varphi_b)) \, \mathrm{d}\varphi_a \mathrm{d}\varphi_b
\end{aligned} \tag{20}$$

Und daraus:

$$\begin{aligned}
\mathbb{S} =& \iint p(\varphi_a, \varphi_b) \sqrt{2} \cos(\varphi_a - \varphi_b) \, \mathrm{d}\varphi_a \mathrm{d}\varphi_b && (21)\\
\Leftrightarrow |\mathbb{S}| \leq& \sqrt{2} \iint p(\varphi_a, \varphi_b) \, \mathrm{d}\varphi_a \mathrm{d}\varphi_b && (22)\\
\Leftrightarrow |\mathbb{S}| \leq& \sqrt{2} && (23)
\end{aligned}$$

Somit wird das Ergebnis von $\mathbb{S}$ eklatant vom erwarteten Wert abweichen.

Wenn Alice und Bob nun ihre Ergebnisse mit Hilfe der CHSH-Ungleichung überprüfen, können sie feststellen, ob ihre Photonen tatsächlich verschränkt waren (Eve hat nicht gelauscht) oder nicht (eventuell hat Eve gelauscht). In letzterem Fall sollte natürlich das Protokoll von vorne gestartet werden. Die Sicherheit dieses Protokolls beruht somit auch der Erkennung eines Lauschangriffs und der Tatsache, dass es nicht möglich ist, ein Teilchen mit seinen Eigenschaften zu klonen *(No-Cloning-Theorem)*.

Es ist allerdings anzumerken, dass die Sicherheit von E91 nicht zu 100% geklärt ist.

4 Heutiger Stand der Technik

4.1 Hardware

Um einen Quantenschlüsselaustausch erfolgreich durchzuführen, ist die richtige Wahl von Quantenkanal und Detektoren wichtig. Da in allen drei oben vorgestellten Protokollen eine zufällige Wahl der Messbasis nötig ist, stellt sich zunächst die Frage, wie man eine solche zufällige Messung durchführen könnte.

Abbildung 1 zeigt eine mögliche Messapparatur. Der Strahlteiler (BS) im Eingang dient dem gleichmäßigen Verteilen auf die beiden Messbasen ($\otimes$ und $\oplus$). Im diagonalen Strahlengang dreht ein $\lambda/2$-Plättchen die Polarisation um 45°, sodass letztlich für beide Strahlgänge der gleiche experimentelle Aufbau verwendet werden kann. In diesem teilt der Polarisierende Strahlteiler (PBS) die Photonen nach ihren Polarisationsrichtungen (H oder V).

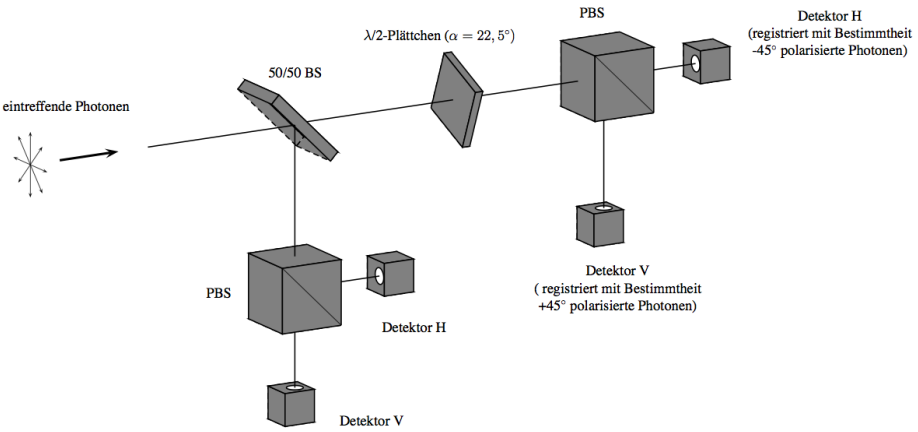

Abbildung 1: Möglicher experimenteller Aufbau für Bob. [13]

Für den Quantenkanal bieten sich unter anderem Glasfaserleitungen oder Teleskopverbindungen an. Die Vorteile von Glasfaserleitungen liegen auf der Hand: Es gibt keine störenden Interferenzen (z.B. durch Luftverwirbelungen). Allerdings sind Glasfaserkabel sehr teuer; ein weltumspannendes Netz zum Verwendung bei der Quantenkryptographie wäre sowohl in der Anschaffung als auch in der Instandsetzung unökonomisch.

Bei Teleskopverbindungen können zwar Beeinträchtigungen durch verunreinigte Luft und Verwirbelungen auftreten, allerdings bieten sie eine große Entfernung bei etwaiger Verwendung mit einem Satellit im All. Weiterhin sind kleine Systeme mobil einsetzbar und nicht an bereits vorhandene Hardware gebunden.

4.2 Bisherige Experimente

- 1989: Charles H. Bennet; weltweit erster Schlüsselaustausch nach BB84 über 30 cm
- 1995: Universität Genf; Schlüsselaustausch über eine 23 km lange Glasfaserverbindung zw. Nyon und Genf [7]
- 2002: Schlüsselaustausch über 23.4 km an der Zugspitze [5]
- 21.04.2004: Erste Geldtransaktion über ein 1.5 km langes Glasfaserkabel [2]
- 2007: Schlüsselaustausch über 144 km von La Palma nach Teneriffa [10]
- 2012: Schlüsselaustausch vom Boden zu einem fliegenden Flugzeug [8]

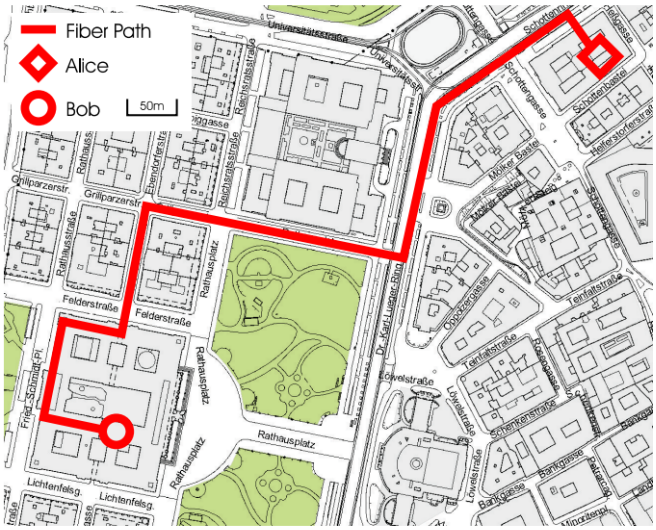

Abbildung 2: Weltweit erste Geldtransaktion mittels Quantenkryptographie.

4.3 Ein möglicher Angriff

Obwohl BB84 und B92 theoretisch sicher sind, gibt es eine Möglichkeit für Eve, durch einen geschickten Angriff bis zu 100% des geheimen Schlüssels auszulesen, ohne dass Alice und Bob etwas davon mitbekommen. Dieser Angriff beruht auf der Tatsache, dass die meisten heute eingesetzten

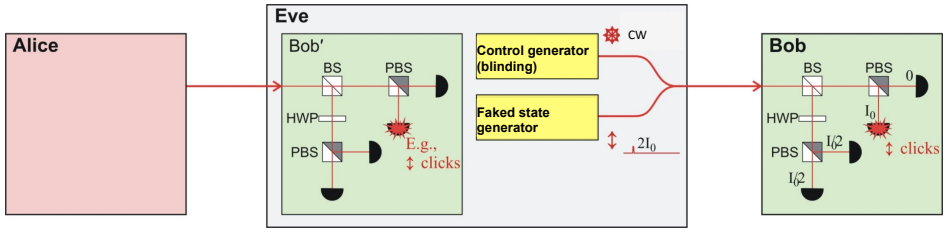

Abbildung 3: Schematischer Aufbau des Angriffs. [6]

Detektoren den „Fehler“ haben, dass sie sich klassisch verhalten, d.h. auf hohe Intensitäten reagieren, wenn nicht nur ein Photon, sondern ein ganzer Photonenpuls auf sie eintreffen.

Eve führt einen Intercept and Resend-Angriff durch und präpariert einen Photonenpuls gemäß der von ihr gemessenen Polarisation. Gleichzeitig „blendet“ sie Bob mit zirkular polarisiertem Licht [3]. Eve schafft es somit, dass unter Bob's vier Detektoren exakt dieser anspricht, welchen sie zur Messung des Photons benutzt hat. Eve hat also an jeder Position des Schlüssels dasselbe Ergebnis und dieselbe Basis wie Bob. Somit kann sie auch den Schlüssel auslesen.

Literatur

[1] Moritz Bubek. *Quantenkryptographie*. Techn. Ber. 2003. URL: http://www.bubek.org/physics/seminar_stuff/quantenkryptografie.pdf.

[2] Allessandro Fedrizzi u. a. "Practical Quantum Cryptography with Polarization-Entangled Photons". In: *CLEO Europe* (2005). URL: http://www.quantenkryptographie.at/PracticalQKD_poster_eng.pdf.

[3] Ilja Gerhardt u. a. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system". In: *Nature Communications* 2 (2011), S. 349.

[4] Christian Kollmitzer. *Applied quantum cryptography*. Heidelberg New York: Springer, 2010. ISBN: 978-3642048296.

[5] Christian Kurtsiefer u. a. "Quantum cryptography: A step towards global key distribution". In: *Nature* 419.6906 (2002), S. 450–450.

[6] Qin Liu und Sebastien Sauge. *How you can build an eavesdropper for a quantum cryptosystem*. 2009. URL: http://events.ccc.de/congress/2009/Fahrplan/events/3576.en.html.

[7] A Muller, H Zbinden und N Gisin. "Quantum cryptography over 23 km in installed under-lake telecom fibre". In: *EPL (Europhysics Letters)* 33.5 (1996), S. 335.

[8] Sebastian Nauerth u. a. "Air-to-ground quantum communication". In: *Nature Photonics* (2013).

[9] Hiroyuki Sagawa und Nobuaki Yoshida. *Fundamentals of Quantum Information*. World Scientific, 2011. ISBN: 978-9814324236.

[10] Tobias Schmitt-Manderbach u. a. "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km". In: *Phys. Rev. Lett.* 98 (1 2007), S. 010504.

[11] Simon Singh. *Geheime Botschaften: die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. München: Dt. Taschenbuch-Verlag, 2006. ISBN: 978-3423330718.

[12] *Wie geheim ist geheim, Herr Ekert?* Technology Review. 2012. URL: http://www.heise.de/tr/artikel/Wie-geheim-ist-geheim-Herr-Ekert-1746772.html.

[13] Mirko Zeppmeisel. *Einführung in die Grundlagen der Quantenkryptographie*. Techn. Ber. Ludwig-Maximilians-Universität München, 2006. URL: http://homepages.physik.uni-muenchen.de/~milq/quantenkryp/Quantenkryptographie.pdf.