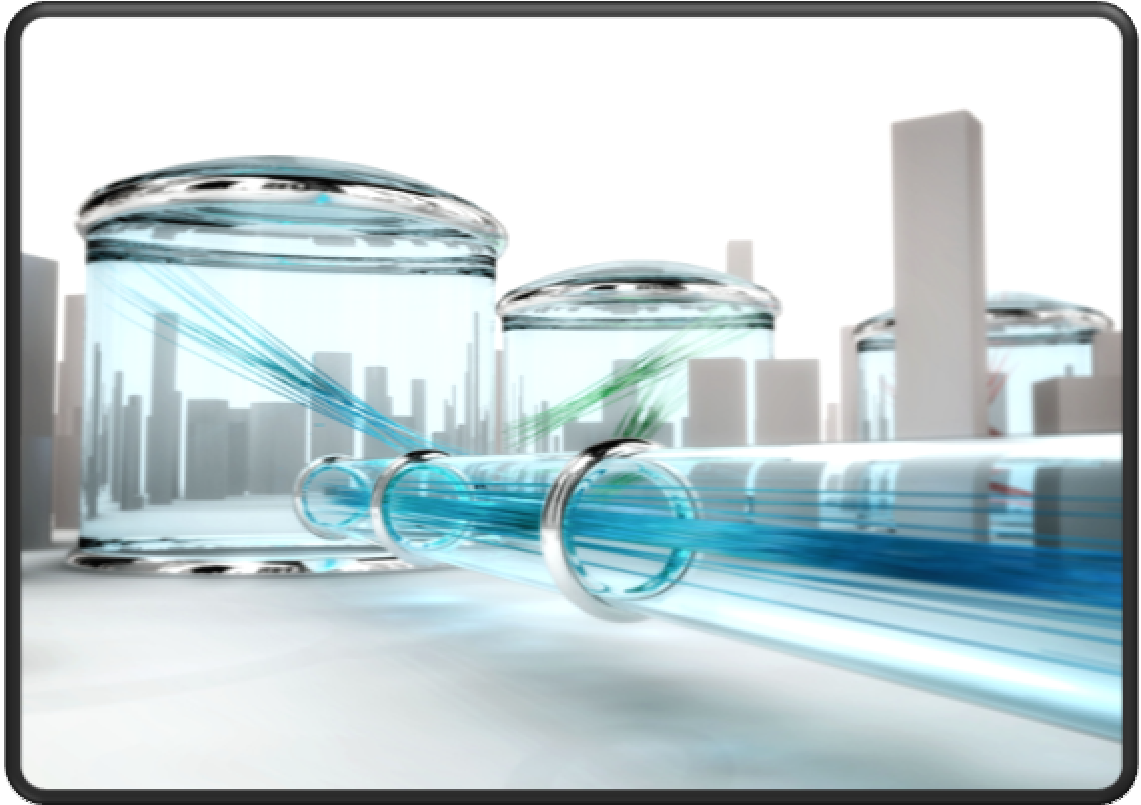


Quantenkryptographie



Ist die Quantenkryptographie wirklich abhörsicher?

Facharbeit von Lennart Moltrecht, Jahrgangsstufe 12

März 2009

Seminarfach „Chaos und Ordnung“ – Herr Utecht

Ist die Quantenkryptographie wirklich abhörsicher?

Seit Jahrhunderten besteht der Bedarf, vertrauliche Nachrichten zu übermitteln, ohne dass diese von Unbefugten gelesen werden können. Die Quantenkryptographie ist ein neuartiges Schlüsselverteilungsverfahren, welches im Gegensatz zu herkömmlichen Chiffriersystemen absolut abhörsicher sein soll. Aufgrund der wachsenden wirtschaftlichen Bedeutung dieser neuen Technologie ist es wichtig, sich mit der Frage zu befassen, ob die Quantenkryptographie tatsächlich so sicher ist, wie Wissenschaftler behaupten. Zur Beantwortung dieser Frage werden zunächst die physikalischen Grundlagen der Abhörsicherheit dargestellt und anschließend quantenkryptographische Verfahren und Methoden zur Absicherung der Vertraulichkeit erläutert. Danach werden Abhörversuche beschrieben und Prozeduren zur Abwehr dergleichen vorgestellt. Daraus lässt sich folgern, dass die Quantenkryptographie eine abhörsichere Technologie ist, zumindest solange die Grundsätze der heutigen Physik nicht widerlegt werden können.

Inhalt

1	Einleitung.....	4
2	Quantenphysikalische Grundlagen.....	5
2.1	Heisenbergsche Unschärferelation.....	5
2.2	Quantenzustände.....	5
2.3	No-Cloning-Theorem.....	6
2.4	Qubits.....	6
3	Kryptographie.....	7
3.1	Klassische Kryptographie.....	7
3.2	Vernam-Chiffre.....	8
3.3	Quantenkryptographie.....	9
4	Quantenkryptographische Verfahren.....	9
4.1	BB84-Protokoll.....	9
4.2	Technische Funktionsweise des BB84-Protokolls.....	11
4.3	E91-Protokoll.....	12
5	Abhörsicherheit.....	13
5.1	Aufdeckung von Spionen.....	13
5.2	Fehlerkorrekturverfahren.....	14
5.3	Vertraulichkeitsverstärkung.....	15
5.4	Einsatz des No-Cloning-Theorems.....	16
6	Abhörmöglichkeiten.....	16
6.1	Verschränkung durch CNOT-Gatter.....	16
6.2	Seitenkanalattacken.....	18
7	Fazit.....	20
8	Glossar.....	21
9	Literaturverzeichnis.....	24
10	Abbildungsverzeichnis.....	25
11	Erklärung.....	26

1 Einleitung

Insbesondere Regierungen, Militär, Banken und große Firmen haben seit langer Zeit das Bedürfnis, Informationen austauschen zu können, ohne dass diese von unerwünschten Lauschern mitgehört werden. Daher wurde bereits vor vielen tausend Jahren die Kryptographie entwickelt als die Wissenschaft der Verschlüsselung von Informationen. Die Qualität der Verfahren zur Nachrichtenverschlüsselung verbesserte sich mit den Jahren, bis 1977 die sogenannte „Public-Key-Kryptographie“ entwickelt wurde, welche aufgrund ihrer Komplexität als praktisch „unknackbar“ gilt.¹ Doch da in Zeiten immer leistungsfähigerer Computer auch diese Art der Verschlüsselung eines Tages unsicher werden könnte, entwickelten Wissenschaftler eine neue Art der Verschlüsselung: Die Quantenkryptographie. Da sie ausschließlich auf physikalischen Grundlagen beruht, soll sie absolut sicher sein.²

Die Quantenkryptographie ist der am weitesten fortgeschrittene Forschungsbereich der Quantenphysik und der einzige, in dem momentan kommerzielle Anwendungen realisierbar sind.³ Die Schweizer Firma „*id Quantique*“ stellte im Jahr 2002 das erste kommerziell nutzbare Gerät vor, und auch die amerikanische Firma „*MagiQ*“ produziert mittlerweile marktreife Serienmodelle.⁴ 2004 wurde die erste Banküberweisung mithilfe quantenkryptographisch verschlüsselter Informationen durchgeführt.⁵ Allein der hohe Preis von etwa 100.000 € pro quantenkryptographischem Verschlüsselungsgerät und die noch langsamen Übertragungsraten halten bislang viele Unternehmen davon ab, die Technologie einzusetzen.⁶

Aufgrund der wachsenden Bedeutung der Quantenkryptographie ist es angebracht, der Frage nachzugehen, ob diese neuartige Technologie auch wirklich sicher ist. Dies sowie die Tatsache, dass die quantenkryptographische Schlüsselerstellung ein chaotischer Prozess ist, mithilfe derer aus einer geordneten Nachricht ein chaotischer Geheimtext und *vice versa* wieder eine geordnete Nachricht erstellt werden kann, veranlasste mich dazu, meine Facharbeit im Bereich Chaos und Ordnung über das Thema Quantenkryptographie zu schreiben. Da es im begrenzten Umfang der Facharbeit nicht möglich ist, auf alle Grundlagen

¹ vgl. (Singh, 2004, S. 252)

² vgl. (Camejo, 2007, S. 270)

³ vgl. (Bruß, Quanteninformation, 2003, S. 56)

⁴ vgl. (Camejo, 2007, S. 271)

⁵ vgl. (Winkler, 2009, S. 66)

⁶ vgl. (Winkler, 2009, S. 68)

einzuwenden, wird eine grundlegende Kenntnis der Quantenphysik und der Kryptographie vorausgesetzt.

2 Quantenphysikalische Grundlagen

2.1 Heisenbergsche Unschärferelation

- 5 Die heisenbergsche Unschärferelation ist eine quantenphysikalische Grundlage, die 1927 von Werner Heisenberg im Alter von nur 26 Jahren erstellt wurde. Sie besagt, dass es einen einschränkenden Bezug zwischen zwei Messgrößen eines quantenphysikalischen Teilchens gibt, sodass nicht beide Größen gleichzeitig beliebig genau bestimmbar sind.⁷ Meistens wird dieser Bezug zwischen der Ortsunschärfe Δx und der Impulsunschärfe Δp hergestellt, wobei
- 10 Δx die Ungenauigkeit des Ortes des Teilchens und Δp die Ungenauigkeit seines Impulses darstellt. Die Gleichung der heisenbergschen Unschärferelation⁸ lautet

$$\Delta x * \Delta p \geq \frac{\hbar}{2}$$

- wobei $\hbar = \frac{h}{2\pi} \approx 1,055 * 10^{-34} Js$ ist und als reduziertes Plancksches Wirkungsquantum bezeichnet wird.⁹ Die Bedeutung der Gleichung liegt darin, dass bei einer genaueren Bestimmung des Ortes x , infolge derer Δx kleiner wird, der Impuls unbestimmter werden,
- 15 also Δp wachsen muss. Folglich ändert sich der Impuls des Teilchens durch die Messung des Ortes und somit wird der Zustand des Teilchens durch die Messung beeinflusst. Dieser Zusammenhang beruht auf der Tatsache, dass das Produkt von Δx und Δp auf der rechten Seite immer größer als die Konstante auf der linken Seite sein muss.¹⁰

2.2 Quantenzustände

- 20 Der Zustand eines Quantenobjekts, also beispielsweise eines Photons oder Elektrons, ist die Wellenfunktion $|\psi\rangle$. Sie beschreibt den Zustand eines Quantensystems vollständig und enthält Informationen über Aufenthaltsort, Energie und Spin des Teilchens.¹¹

Für die Quantenkryptographie werden hauptsächlich Photonen benutzt, deren am einfachsten zu messende Größe die Polarisation ist. Polarisation bedeutet, dass das

⁷ vgl. (Camejo, 2007, S. 89)

⁸ vgl. (Camejo, 2007, S. 87)

⁹ vgl. (Camejo, 2007, S. 39)

¹⁰ vgl. (Camejo, 2007, S. 88)

¹¹ vgl. (Bruß, Quanteninformation, 2003, S. 14)

elektromagnetische Feld eines Teilchens in einer bestimmten festen Richtung schwingt; das Teilchen wird dann linear polarisiert genannt.¹² Die Polarisation kann entlang jeder Richtung erfolgen, also nicht nur in x- bzw. y-Richtung. Jeder Polarisationsvektor kann als Summe eines Vektors in x- und eines Vektors in y-Richtung definiert werden. Diese Zustände bilden
5 eine Basis und werden als $|0\rangle$ für die x-Richtung und $|1\rangle$ für die y-Richtung notiert.

Die im weiteren Verlauf eingeführte Messung der Polarisation erfolgt üblicherweise in einer der zwei Standardbasen: Die sogenannte „gerade“ Basis für horizontale und vertikale Polarisation mit den Zuständen $|0\rangle$ und $|1\rangle$ und die „schräge“ Basis für Polarisation im Winkel von 45° beziehungsweise 135° zur horizontalen Achse mit den Zuständen $(|0\rangle + |1\rangle)/\sqrt{2}$ (entspricht 45°) oder $(|0\rangle - |1\rangle)/\sqrt{2}$ (entspricht 135°).¹³
10

2.3 No-Cloning-Theorem

Im Jahr 1982 folgerten W. Wootters und W. Zurek aus der Quantentheorie das sogenannte „No-Cloning“-Theorem, welches besagt, „[...] dass ein unbekannter Quantenzustand – beispielsweise ein Qubit – nicht kopiert werden kann, ohne den ursprünglichen Zustand dabei
15 zu zerstören.“¹⁴ Die Aufstellung dieses Theorems folgte einer Publikation von N. Herbert, in der dieser ein Prinzip vorschlug, mithilfe dessen die Übertragung von Informationen mit Überlichtgeschwindigkeit möglich wäre, wenn sehr viele Kopien von einem Quantenobjekt vorlägen. Da niemand einen Fehler in Herberts Argumentation erkennen konnte, wurde der Artikel veröffentlicht und führte zu einer Diskussion, deren Ergebnis das Theorem von
20 Wootters und Zurek war.¹⁵

Auf die Begründung des Theorems soll hier nicht weiter eingegangen werden, da nur die Wirkung für die Quantenkryptographie wichtig ist.

2.4 Qubits

Ein quantenphysikalisches Bit, auch Qubit genannt, trägt ähnlich wie ein normales Bit zwei
25 binäre Zustände. Diese Basiszustände werden als $|0\rangle$ und $|1\rangle$ bezeichnet und können, abhängig vom verwendeten Elementarteilchen, unterschiedlich sein: beispielsweise ein in eine von zwei möglichen Richtungen polarisiertes Photon, ein Atom entweder im Grundzustand oder im angeregten Zustand, oder ein Elektron mit Spin in positive oder

¹² vgl. (Bruß, Quanteninformation, 2003, S. 14)

¹³ vgl. (Bruß, Quanteninformation, 2003, S. 54)

¹⁴ (Baeyer & Filk, 2007, S. 218)

¹⁵ vgl. (Bruß, Quanteninformation, 2003, S. 37)

negative z-Richtung.¹⁶ Ein Qubit kann, anders als ein normales Bit, nicht nur einen der beiden Basiszustände annehmen, sondern sich in einer Superposition mit der Schreibweise

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

befinden, wobei $|a|^2 + |b|^2 = 1$ gilt. Da $|a|$ und $|b|$ jeden Wert zwischen 0 und 1 annehmen können, gibt es unendlich viele solcher Superpositionen. Dies bedeutet jedoch nicht, dass ein

5 Qubit mehr verwendbare Informationen als ein normales Bit enthält, da man die Information nur durch die Messung in einer bestimmten Basis auslesen kann. Diese Messung wiederum verändert den Zustand, sodass nicht in einer anderen Basis erneut gemessen werden kann.¹⁷

Dem Messergebnis in einer Basis wird üblicherweise ein binärer Wert zugewiesen, 10 beispielsweise definiert man bei der Messung der Polarisation in der „geraden“ Basis ein Ergebnis von 0° als 0 und ein Ergebnis von 90° als 1.

Bei der Quantenkryptographie wird generell mit der Polarisation von Photonen gearbeitet, da diese relativ einfach zu messen ist.¹⁸

15 3 Kryptographie

Die Kryptographie befasst sich im Allgemeinen mit der Verschlüsselung von Daten und somit dem Schutz von Informationen vor unerwünschtem Ausspähen. Schon in der Antike wurden Verschlüsselungsverfahren für militärische Zwecke eingesetzt, damit der Inhalt der Nachrichten nur von dem erwünschten Empfänger gelesen werden konnte.¹⁹

20 3.1 Klassische Kryptographie

Klassischerweise werden in der Kryptographie die Partner, die eine Nachricht geheim austauschen wollen, Alice und Bob genannt. Alice will eine Nachricht an Bob senden und verschlüsselt diese so, dass Eve (von engl. *eavesdropping* = Abhören, Lauschen²⁰) ohne Kenntnis des Schlüssels die Nachricht nicht dechiffrieren kann.²¹ Allerdings können Alice und

¹⁶ vgl. (Bruß, Quanteninformation, 2003, S. 32-33)

¹⁷ vgl. (Camejo, 2007, S. 257-258)

¹⁸ vgl. (Bruß, Quanteninformation, 2003, S. 14)

¹⁹ vgl. (Singh, 2004, S. 11)

²⁰ vgl. (Klett, 2003, S. 186)

²¹ vgl. (Camejo, 2007, S. 262)

Bob Angriffe durch Eve bei der klassischen Kryptographie nicht verhindern, denn sie bemerken nicht einmal, dass die Nachricht abgehört wurde.²²

Bei klassischen Verschlüsselungsverfahren hängt die Sicherheit des Geheimtextes allein davon ab, wie komplex die Art und Weise der Umwandlung ist. Simple Verfahren wie
5 beispielsweise die monoalphabetische Verschlüsselung geben dem Geheimtext daher eine sehr geringe Sicherheit, da der Schlüssel nach sehr kurzer Zeit durch einfaches Probieren herausgefunden werden kann. Variationen und Erweiterungen dieser Verfahren machen die Schlüsselsuche zwar komplizierter, jedoch nicht unmöglich, sodass eine Entschlüsselung durch Eve letztendlich nur eine Frage der Zeit ist.²³

10 3.2 Vernam-Chiffre

Gilbert Vernam, ein US-amerikanischer Ingenieur, erfand 1918 die sogenannte „Vernam-Chiffre“, auch unter dem Namen „One-Time-Pad“ bekannt. Dieses neue Verschlüsselungsverfahren machte es potentiellen Spionen, die die verschlüsselte Nachricht
15 abhörten, absolut unmöglich, die Nachricht durch systematische Verfahren zu entschlüsseln.²⁴ Da der Verschlüsselung keinerlei Ordnung zugrunde liegt, ist sie ein chaotischer Prozess. Selbst mit modernen Super-Computern und perfekten Verfahren zur Entschlüsselung bleibt einem Spion keine andere Wahl, als jeden möglichen Schlüssel zur Dechiffrierung auszuprobieren.

Die Vernam-Chiffre benötigt einen Schlüssel, der die gleiche Länge hat wie der zu
20 chiffrierende Klartext. Das Prinzip des Verfahrens ist das folgende:

1. Der Klartext wird in Binärcode umgeschrieben.
2. Ein zufälliger binärer Schlüssel mit gleicher Länge wie der Klartext wird erstellt, den nur Alice und Bob kennen.
3. Alice addiert Bit für Bit den Klartext mit dem Zufallsschlüssel modulo 2 (auch als XOR-
25 Verknüpfung bekannt). Das Ergebnis der Addition ist ein chaotischer Geheimtext.
4. Der Geheimtext wird durch einen beliebigen Informationskanal von Alice zu Bob übertragen. Dieser Informationsweg muss nicht sicher sein; es kann also beispielsweise das Internet oder das Telefon benutzt werden.

²² vgl. (Beutelspacher, Schwarzpaul, & Neumann, 2006, S. 289)

²³ vgl. (Singh, 2004, S. 28)

²⁴ vgl. (Bruß, Quanteninformatio, 2003, S. 50)

5. Bob addiert Bit für Bit den Geheimtext mit dem Zufallsschlüssel modulo 2. Das Ergebnis der Addition ist wieder der geordnete Klartext.

Da der Zufallsschlüssel keiner Gesetzmäßigkeit folgt, kann ein möglicher Spion aus dem abgehörten Geheimtext keinesfalls auf den Klartext schließen. Daher ist ein Brechen dieses Verschlüsselungsverfahrens, wie mathematisch bewiesen werden kann, unmöglich.²⁵ So genial und unknackbar die Vernam-Chiffre auch sein mag, besteht dennoch ein Problem, welches die praktische Umsetzung als sehr schwierig gestaltet: Der zweite Schritt setzt einen zufälligen Schlüssel mit gleicher Länge wie der Klartext voraus. Dies ist ein großes logistisches Problem für den Einsatz, denn einerseits ist es schwer, einen solch langen Schlüssel sicher an Bob zu übermitteln; andererseits darf jeder Schlüssel nur ein Mal verwendet werden, da es sich ansonsten nicht um einen wirklichen Zufallsschlüssel handeln würde. Dieses Problem der Schlüsselverteilung machte die Vernam-Chiffre für die heutigen, langen Nachrichten ungeeignet, weshalb sich andere, unsichere Verschlüsselungsverfahren durchsetzten.²⁶

An diesem Punkt kommt die Quantenkryptographie ins Spiel.

15 3.3 Quantenkryptographie

Die Quantenkryptographie bietet eine Lösung für das Problem der Schlüsselverteilung, welches die Vernam-Chiffre bislang nicht praktikabel machte: Sie ermöglicht es, den für die Vernam-Chiffre nötigen Schlüssel vollkommen abhörsicher zu verteilen. Daher kann die Quantenkryptographie nicht als neuartiges Verschlüsselungsverfahren angesehen werden, sondern wird als Schlüsselverteilungsverfahren (engl. *quantum key distribution*, QKD²⁷) bezeichnet.²⁸ Auf die genauere Funktionsweise soll im folgenden Kapitel eingegangen werden.

4 Quantenkryptographische Verfahren

4.1 BB84-Protokoll

25 1984 stellten die beiden bei IBM arbeitenden Wissenschaftler Charles Bennett und Gilles Brassard das nach ihnen und dem Erscheinungsjahr benannte BB84-Protokoll vor, welches

²⁵ vgl. (Camejo, 2007, S. 264-265)

²⁶ vgl. (Camejo, 2007, S. 265)

²⁷ vgl. (Winkler, 2009, S. 66)

²⁸ vgl. (Bruß, Quanteninformaton, 2003, S. 52)

eine sichere Übertragung von Informationen ermöglicht und dabei nicht auf der Komplexität des Verschlüsselungsalgorithmus, sondern allein auf physikalischen Grundlagen basiert.²⁹

Der genaue Prozess läuft wie folgt ab und ist zur Veranschaulichung in Abbildung 3.1 dargestellt:³⁰

- 5 1. Alice sendet einzelne Photonen an Bob (siehe 4.2), die jeweils zufällig in einer von zwei vorher definierten Basen polarisiert wurden (hier werden zur Veranschaulichung die oben erwähnte „grade“ und „schräge“ Basis verwendet).
2. Bob misst die empfangenen Photonen in einer ebenfalls jeweils zufälligen und von Alices gewählter Basis unabhängigen Basis und notiert die Ergebnisse.
- 10 3. Nach der Messung informiert Bob Alice über einen klassischen Informationskanal, welche Basis er für welches Photon verwendet hat, teilt jedoch nicht das Messergebnis mit. Alice vergleicht die verwendeten Basen und teilt Bob mit, in welchen Fällen die von ihr versendeten Photonen in der gleichen Basis polarisiert waren, in der Bob gemessen hat. Alle anderen Messergebnisse werden verworfen.

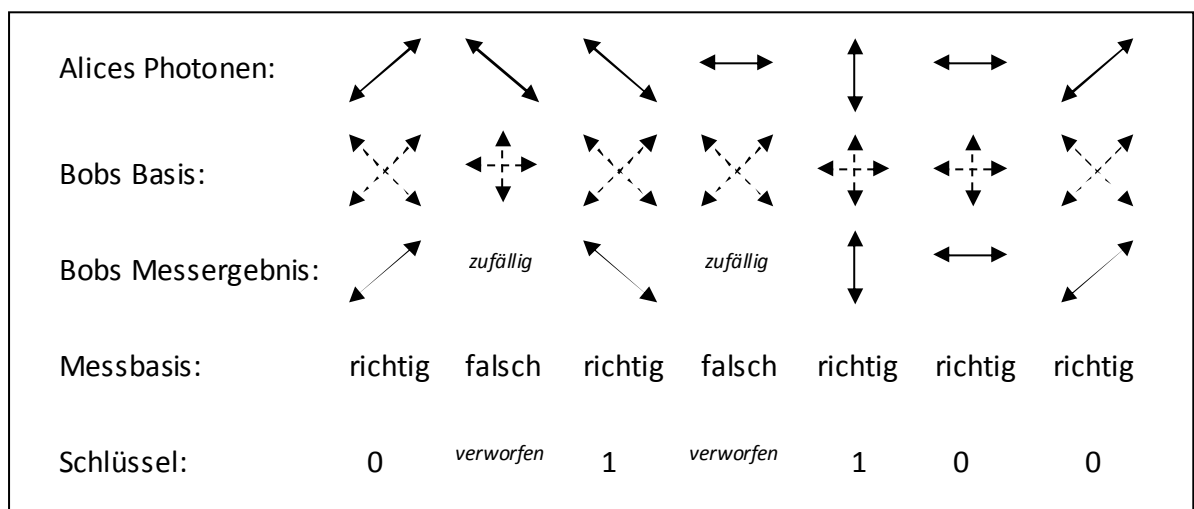


Abbildung1: Ein beispielhafter Ablauf einer Schlüsselübertragung nach dem BB84-Protokoll.

- 15 Nach Abschluss des Verfahrens besitzen Alice und Bob einen identischen Zufallsschlüssel, mithilfe dessen die zu versendende Nachricht mit der Vernam-Chiffre sicher verschlüsselt werden kann.³¹

²⁹ vgl. (Singh, 2004, S. 273)

³⁰ vgl. (Camejo, 2007, S. 268)

³¹ vgl. (Camejo, 2007, S. 267)

Die Schlüsselerstellung ist ein chaotischer Prozess, da der endgültige Schlüssel ausschließlich von der zufälligen Wahl der Basen der beiden Partner abhängt und somit ein zufälliger, chaotisch erstellter Schlüssel entsteht.

- 5 Doch wie können Alice und Bob sicher sein, dass Eve den Schlüssel nicht abgehört hat? Eine Antwort darauf bietet die heisenbergsche Unschärferelation, deren Wirkungsweise im Zusammenhang mit der Quantenkryptographie im nächsten Kapitel genauer erläutert wird.

4.2 Technische Funktionsweise des BB84-Protokolls

Die Quantenkryptographie ist, wie oben erwähnt, nur ein Schlüsselverteilungsverfahren. Sie macht es möglich, Schlüssel beliebiger Länge zu verteilen und ist

- 10 „[...] das einzige Verfahren, bei dem man nach der Schlüsselverteilung sicher weiß, ob jemand diese belauscht hat.“³²

- Wie bereits ausgeführt, reicht ein Schlüsselverteilungsverfahren alleine jedoch nicht aus, um Nachrichten auch wirklich sicher übertragen zu können; zusätzlich wird ein sicheres Verfahren zur Verschlüsselung benötigt. Hier bietet sich die oben erläuterte Vernam-Chiffre an: Sofern komplett zufällige Schlüssel vorliegen, kann hiermit eine Nachricht nachweislich
15 sicher chiffriert werden. Diese zufälligen Schlüssel kann die Quantenkryptographie liefern und damit das oben erwähnte Schlüsselverteilungsproblem aus dem Weg räumen.

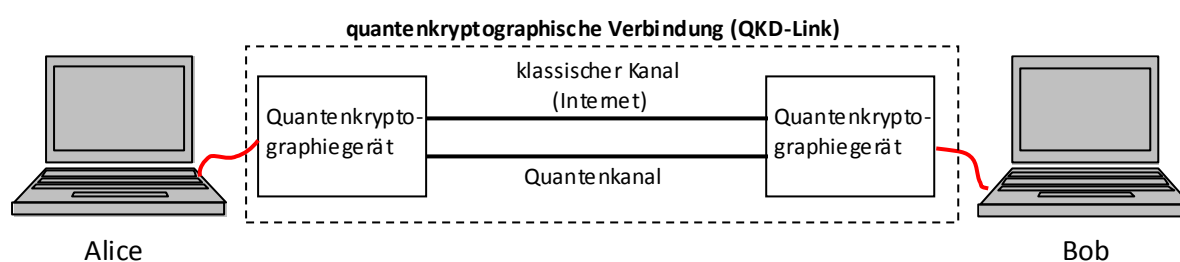


Abbildung 2: Schematischer Aufbau einer quantenkryptographischen Verbindung nach dem BB84-Protokoll

- Eine quantenkryptographische Verbindung besteht aus einem klassischen Kanal, der öffentlich zugänglich ist, sowie einem Quantenkanal (siehe Abbildung 3.2). Der klassische
20 Kanal wird zur Übertragung der mit der Vernam-Chiffre verschlüsselten Nachricht und zur generellen Kommunikation zwischen Alice und Bob benötigt, welche zum Beispiel für den Abgleich der verwendeten Messbasen benötigt wird.³³ Der Quantenkanal besteht meistens

³² (Winkler, 2009, S. 67)

³³ vgl. (Winkler, 2009, S. 67)

aus Glasfaserkabeln oder Teleskopverbindungen. Durch ihn werden die von Alice polarisierten Qubits an Bob übertragen.³⁴

4.3 E91-Protokoll

Ein anderer Ansatz der Quantenkryptographie ist das 1991 von Artur Ekert vorgestellte E91-
5 Protokoll (wieder benannt nach dem Erfinder und dem Entwicklungsjahr). Dieses Protokoll
arbeitet im Gegensatz zum BB84-Protokoll nicht mit einzelnen Photonen, sondern mit
verschränkten Photonenpaaren. Jeweils eines der verschränkten Photonen besitzt Alice
beziehungsweise Bob. Wenn ein gemeinsamer Schlüssel benötigt wird, führen beide
entsprechende Messungen (zum Beispiel Polarisation) in einer der beiden Basen durch.
10 Wenn beide die gleichen Basen verwenden, sind die Ergebnisse der Messung aufgrund der
Verschränkung perfekt korreliert. Das bedeutet, wenn Alice bei einer Messung in der
geraden Basis eine horizontale Polarisation misst, muss Bobs Photon vertikal polarisiert
sein.³⁵ Im Anschluss muss einer der beiden Partner sein Messergebnis negieren, also anstatt
einer 1 eine 0 und statt einer 0 eine 1 verwenden, damit beide den gleichen Schlüssel
15 besitzen.³⁶

Das E91-Protokoll bietet gegenüber dem BB84-Protokoll einige Vorteile. Zur Verteilung der
verschränkten Photonen kann entweder eine zentrale, unabhängige Quelle verwendet
werden, von der beide Partner eines der verschränkten Photonen vermittelt bekommen.
Dies macht eine direkte Verbindung zwischen den Partnern überflüssig und könnte bei einer
20 Vielzahl an die Quelle angeschlossenen Technologienutzern die Schlüsselverteilung deutlich
erleichtern, da nun nicht mehr zwischen jedem der Nutzer eine direkte Verbindung bestehen
muss.³⁷ Eine andere Möglichkeit besteht darin, einige Photonen zu verschränken und
solange bei Alice und Bob aufzubewahren, bis ein Schlüssel benötigt wird. Damit wird eine
Quantenverbindung zwischen beiden Partnern komplett überflüssig und die Technologie
25 könnte auch in entlegenen Gebieten angewendet werden. Zusätzlich bietet die
Aufbewahrung der Photonen den Vorteil, dass Eve keine Chance hat, den Schlüssel
abzuhören, da keine Photonen verschickt werden. Technisch ist es bisher jedoch nicht
möglich, Photonen länger als eine Sekunde aufzubewahren.³⁸ Da die Schlüsselerstellung mit

³⁴ vgl. (Winkler, 2009, S. 66)

³⁵ vgl. (Bruß, Quanteninformatio, 2003, S. 89)

³⁶ vgl. (Ilic, 2007, S. 3)

³⁷ vgl. (Bruß, Quanteninformatio, 2003, S. 88)

³⁸ vgl. (Bruß, Quanteninformatio, 2003, S. 87)

verschränkten Photonen deutlich komplizierter und teurer ist als mit einzelnen Photonen, wird das E91-Protokoll trotz seiner Vorteile seltener eingesetzt und soll daher in dieser Facharbeit nicht weiter berücksichtigt werden.

5 5 **Abhörsicherheit**

Die Sicherheit des BB84-Protokolls beruht auf dem durch die heisenbergsche Unschärferelation beschriebenen Messproblem: Da eine Messung den Zustand der gemessenen Quanten verändert, kann Eve die gesendeten Informationen nicht unbemerkt abhören.³⁹

10 5.1 **Aufdeckung von Spionen**

Wenn Eve sich in den Quantenkanal einklinkt und Messungen an den von Alice gesendeten Photonen in einer von ihr zufällig gewählten Basis durchführt, zerstört sie durch den Messvorgang den ursprünglichen Zustand des Photons, weil die Messung den Zustand irreparabel reduziert.⁴⁰ Das von Eve an Bob weitergeschickte Photon ist nur mit einer Wahrscheinlichkeit von 50% mit dem ursprünglich von Alice gesendeten Photon identisch.⁴¹ Dies beruht auf der Tatsache, dass die Basis, in der gemessen wurde, nur in 50% aller Fälle mit der Polarisationsrichtung des originalen Photons übereinstimmt. Wenn die Messung in der richtigen Basis erfolgte, wird der Zustand nicht verändert; wenn jedoch eine andere Basis gewählt wurde, sendet Eve das Photon in der falschen Basis an Bob weiter.⁴² Falls auch Bob die falsche Basis verwendet, wird das Messergebnis aus Prinzip verworfen. Sollte er aber die richtige Basis wählen, ergibt die Messung mit gleicher Wahrscheinlichkeit entweder das richtige oder das falsche Ergebnis. Somit werden 25% der nicht verworfenen Ergebnisse von Bob falsch gemessen, obwohl dieselbe Basis verwendet wurde.⁴³ Wenn Alice und Bob nun einige Bits des Schlüssels vergleichen werden sie bemerken, dass eine ungewöhnlich hohe Anzahl von Bits fehlerhaft übertragen worden ist. Daraus schließen sie, dass Eve ihre Übertragung mitgehört hat und können daraufhin entweder die Übertragung abbrechen oder mithilfe sogenannter Fehlerkorrekturverfahren und Methoden zur

³⁹ vgl. (Bruß, Quanteninformation, 2003, S. 53)

⁴⁰ vgl. (Beutelspacher, Schwarzpaul, & Neumann, 2006, S. 289)

⁴¹ vgl. (Camejo, 2007, S. 270)

⁴² vgl. (Bruß, Quanteninformation, 2003, S. 55)

⁴³ vgl. (Bruß, Quanteninformation, 2003, S. 56)

Vertraulichkeitsverstärkung einen neuen Schlüssel „destillieren“, den Eve mit ihrer begrenzten Menge an Information nicht erraten kann.⁴⁴

5.2 Fehlerkorrekturverfahren

Zu Fehlern bei der Übertragung kann es aus mehreren Gründen kommen, beispielsweise wegen Rauschens, Kurzzeitstörungen im Übertragungskanal oder aufgrund eines Lauschers Eve.⁴⁵

Damit der übertragene Schlüssel trotzdem verwendet werden kann, werden Fehlerkorrekturverfahren angewendet. Ein sehr einfaches Fehlerkorrekturverfahren ist das sogenannte „redundante Kodieren“, welches zur Sicherstellung der Korrektheit der empfangenen Information Wiederholungen verwendet. Anstatt des Bits 0 wird zum Beispiel ein aus drei gleichen Bits bestehendes Codewort generiert, in diesem Falle 000. Wenn der Empfänger anstatt des gesendeten Codeworts zum Beispiel das Wort 010 erhalten sollte, kann er aufgrund des häufigeren Auftretens von 0 schließen, dass das zweite Bit falsch ist und somit zum richtigen Ergebnis des eigentlichen Wertes, nämlich 0, kommen. Da das redundante Kodieren eine mehrfache Übertragung des gleichen Bits erfordert, ist eine Anwendung in der Quantenkryptographie nicht sinnvoll: Durch die dreifache Übertragung desselben Bits wird Eve zusätzliche Information gegeben.⁴⁶

Bei der linearen Fehlerkorrektur wählt Alice zufällig zwei Bits aus dem Schlüssel aus, berechnet deren XOR-Wert und gibt Bob die Positionen der Bits sowie den XOR-Wert bekannt. Bob bildet den XOR-Wert von seinen Bits an der jeweiligen Position und teilt diesen Alice mit. Leider ließen sich zu diesem Thema nur zwei Quellen finden, die sich gegenseitig widersprechen. Anton Haase beschreibt das weitere Vorgehen in seiner Publikation wie folgt: Wenn die XOR-Werte unterschiedlich sind, werden beide Bits gestrichen, andernfalls nur das letztere.⁴⁷ Diese Methode hat den Nachteil, dass in Sonderfällen der Fehler nicht korrigiert wird. Falls beispielsweise Alice die Bitwerte $b_1 = 0$ und $b_2 = 1$, Bob jedoch $b_1 = 1$ und $b_2 = 0$ besitzt, errechnen beide den XOR-Wert $b_1 \oplus b_2 = 1$. Allerdings würde Alice dann die 1 und Bob die 0 streichen; als Ergebnis bliebe Alice eine 0 und Bob eine 1. Die von Sebastian Kühn veröffentlichte Quelle behauptet, man müsse bei übereinstimmendem XOR-

⁴⁴ vgl. (Singh, 2004, S. 270)

⁴⁵ vgl. (Zeppmeisel, 2006, S. 81)

⁴⁶ vgl. (Bruß, Quanteninformation, 2003, S. 93)

⁴⁷ vgl. (Haase, 2007, S. 31)

Wert das erste Bit durch den XOR-Wert ersetzen und das zweite streichen.⁴⁸ Dies würde Eve allerdings zusätzliche Informationen über den Schlüssel zuspüren, wodurch die Sicherheit des Schlüssels herabgesetzt wird. Das ist genauso wenig wünschenswert wie ein Fehler im Schlüssel und somit keine Verbesserung. Aufgrund dieser Probleme kann an dieser Stelle
5 keine genauere Auskunft über ein einfaches und sicheres Fehlerkorrekturverfahren gegeben werden.

Da die oben genannte lineare Fehlerkorrektur sehr ineffizient ist, wurden andere Verfahren wie beispielsweise der Hamming-Code entwickelt, mit deren Hilfe gewährleistet werden kann, dass Alice und Bob beide einen identischen, von Fehlern bereinigten Schlüssel
10 besitzen, ohne dass Eve mehr Informationen über den Schlüssel erhält.⁴⁹ Der Hamming-Code ist jedoch zu komplex, um in dieser Facharbeit näher behandelt zu werden.

5.3 Vertraulichkeitsverstärkung

Mit der sogenannten Vertraulichkeitsverstärkung (engl. *privacy amplification*) lässt sich Eves Kenntnis des Schlüssels weiter verringern. Dabei wird der nur teilweise geheime Schlüssel,
15 denn Eve kann ja Teile abgehört haben, in einen kürzeren, dafür aber sehr geheimen Schlüssel umgewandelt.⁵⁰

Auch hier bietet die XOR-Verknüpfung eine sichere Lösung: Angenommen, Alice und Bob hätten zwei Bits b_1 und b_2 ausgetauscht, von denen Eve b_1 abhören konnte. Jetzt bilden Alice und Bob mithilfe der XOR-Verknüpfung ein weiteres Bit $b_3 = b_1 \oplus b_2$. Wenn Eve weiß,
20 dass $b_1 = 0$ ist, aber den Wert von b_2 nicht kennt, somit $b_2 = 0$ beziehungsweise $b_2 = 1$ gleich wahrscheinlich sind, weiß sie auch nichts über b_3 . Genauso verhält es sich mit der Summe $b_1 \oplus b_2 \oplus \dots \oplus b_k$, wenn Eve ein einziges der k Bits nicht kennt. Wenn man aus einer Folge von m Bits x neue Bits erzeugen will, wählt man x zufällige Teilmengen der Bits aus und bildet deren XOR-Summen. Wenn Alice und Bob ihren Schlüssel mithilfe der
25 Vertraulichkeitsverstärkung um die Anzahl Bits verkürzen, die Eve maximal kennen kann (gegeben durch die Fehlerrate des BB84-Protokolls, im Extremfall also 25%), können sie sich sicher sein, dass Eve mit großer Wahrscheinlichkeit nur eine sehr geringe Anzahl an Bits kennt.⁵¹

⁴⁸ vgl. (Kühn, 2007, S. 7)

⁴⁹ vgl. (Bruß, Quanteninformaton, 2003, S. 56)

⁵⁰ vgl. (Bruß, Quanteninformaton, 2003, S. 56)

⁵¹ vgl. (Homeister, 2005, S. 180)

5.4 Einsatz des No-Cloning-Theorems

Man könnte sich jetzt fragen, warum Eve nicht einfach das abgefangene Photon kopiert, um dann die Messung am geklonten durchzuführen und das originale unverändert weiter zu schicken.

- 5 Das oben erwähnte No-Cloning-Theorem postuliert jedoch, dass es nicht möglich sei, perfekte Kopien eines unbekanntes Quantenzustands zu erzeugen. Dies schließt jedoch nicht aus, dass überhaupt Kopien erstellt werden können. Im Jahr 2000 konnte Francesco De Martini in Rom nachweisen, dass statt einer perfekten Kopie, die eine Güte (engl. *fidelity*⁵²) von $F = 1$ besäße, Kopien mit einer maximalen Güte von $F = 5/6$ erreicht werden
- 10 können.⁵³ Diese reichen jedoch nicht dazu aus, um den zwischen Alice und Bob verschickten Schlüssel abzuhören.

6 Abhörmöglichkeiten

6.1 Verschränkung durch CNOT-Gatter

- 15 Im Jahr 2008 gelang es Taehyun Kim und Kollegen vom *Massachusetts Institute of Technology* (MIT), mithilfe eines CNOT-Gatters bis zu 90% des Schlüssels abzuhören, ohne dabei die Fehlerrate zu erhöhen und somit entdeckt zu werden. Sie verwendeten die bereits 1998 vorgestellte *Fuchs-Peres-Brandt entangling probe* (auch bekannt als FPB-Verfahren) und bewiesen damit, dass das damals entwickelte Verfahren tatsächlich funktioniert.⁵⁴
- 20 Ein CNOT-Gatter ist ein Quantengatter, das sich auf zwei Qubits bezieht, und funktioniert nach dem folgenden Prinzip: Auf jeden der beiden Eingänge des Gatters wird ein Qubit gegeben. Wenn der Wert des ersten Qubits 0 ist, wird nichts verändert, anderenfalls wird der des zweiten Qubits negiert. Somit sieht eine Wertetabelle eines CNOT-Gatters aus wie folgt:

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$$

$$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$$

$$|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

⁵² vgl. (Klett, 2003, S. 221)

⁵³ vgl. (Bruß, Quanteninformation, 2003, S. 39-40)

⁵⁴ vgl. (Kim, 2008, S. 1)

$$|1\rangle|1\rangle \rightarrow |1\rangle|0\rangle$$

Ein einzelnes, von Alice verschicktes Photon kann gemäß der SPTQ Logik (engl. *single-photon two qubit*⁵⁵) als ein Zwei-Qubit-System aufgefasst werden, wobei ein Qubit die Polarisierung und das andere den Impuls enthält. Eve muss jetzt ein Qubit vorbereiten, welches sie auf den zweiten Eingang des CNOT-Gatters gibt, sobald Alices Photon am ersten Eingang
5 ankommt. Durch die Eigenschaft des CNOT-Gatters, das zweite Qubit zu negieren, werden der Impuls von Alices Photon und Eves Qubit verschränkt.⁵⁶ Auf die genaueren Gründe dieser Tatsache soll hier nicht näher eingegangen werden.

Nun kann Eve ihr Qubit messen, ohne dabei die Polarisierung des ursprünglich von Alice gesendeten Qubits zu verändern. Allerdings erhielte sie bei einer Messung der Polarisierung
10 ein zufälliges Ergebnis, welches nichts über die Polarisierung von Alices Photon aussagt, da die Polarisierungen nicht verschränkt sind. Bei einer Messung des Impulses dagegen erhielte sie ein zuverlässiges Ergebnis, welches die Negation des Impulses von Alices Photon darstellt. Bob wird die Messung nicht bemerken, da er nur die Polarisierung misst, die unverändert bleibt.⁵⁷

15 Durch die Kenntnis des Impulses und der von Alice und Bob verwendete Messbasis, die ja öffentlich auf dem klassischen Kanal ausgetauscht wird, kann Eve nun Rückschlüsse auf die Polarisierung des Photons ziehen.⁵⁸

Dieser Versuch stellt unter den momentanen Bedingungen trotz der hohen Abhörquote von 90% nur ein sehr geringes Risiko für die Quantenkryptographie dar, denn damit das Ergebnis
20 der Impulsmessung Rückschlüsse auf die Polarisierung zulässt, muss Eves Impulsmessung zeitgleich mit der Messung der Polarisierung durch Bob stattfinden. Um diese perfekte Synchronisation der Messungen zu erreichen, ist ein physikalischer Zugriff auf Bobs Empfangsgerät erforderlich (jedoch kein Zugriff auf seine Messwerte). Da Eve unter normalen Bedingungen jedoch keinen Zugriff auf Bobs Empfangsgerät hat, kann sie die
25 Impulsmessung auch nicht zur richtigen Zeit durchführen; falls sie dennoch Zugriff auf das Empfangsgerät hätte, könnte sie auch gleich den empfangenen Schlüssel auslesen und bräuchte die Übertragung nicht zu belauschen. Außerdem konnten Forscher der *University*

⁵⁵ vgl. (Kim, 2008, S. 1)

⁵⁶ vgl. (Kim, 2008, S. 2)

⁵⁷ vgl. (Kim, 2008, S. 2)

⁵⁸ vgl. (Kim, 2008, S. 2)

of Waterloo in Kanada zeigen, dass schon seit einigen Jahren Methoden existieren, um Angriffe wie die der Gruppe des MIT unmöglich zu machen, die jedoch im von Kim verwendeten Empfangsgerät nicht aktiviert waren.⁵⁹ Somit bleibt die Quantenkryptographie vor Angriffen mit dem FPB-Verfahren sicher.⁶⁰

5 6.2 Seitenkanalattacken

Eine weitere Methode, um Informationen über den Schlüssel zu erlangen, sind sogenannte Seitenkanalattacken, die nicht das kryptographische Verfahren selbst, sondern die verwendeten Geräte angreifen:

10 *„Seitenkanalattacken sind Angriffe, die physikalische Implementierungen kryptografischer Geräte ins Visier nehmen: etwa, indem sie deren Energieverbrauch oder Rechenzeit beim Abarbeiten einer Aufgabe beobachten.“⁶¹*

Vadim Makarov von der Universität Trondheim gelang es, durch die Injektion kurzer, sehr heller Laserimpulse in den Quantenkanal zwischen Alice und Bob, die Detektoren des Empfangsgeräts zu stören.⁶² Die von Eve gesendeten Signale setzen aufgrund ihrer Helligkeit 15 die Empfindlichkeit aller Sensoren für verschiedene Polarisationen (für die gerade und die schräge Basis) im Empfangsgerät für kurze Zeit herab. Nun kann Eve die Polarisation des eingespeisten Lichts verändern (nur noch in der schrägen Basis polarisiertes Licht), sodass der Sensor, der genau auf diese Polarisation nicht anspricht (also derjenige, der auf die gerade Basis anspricht), seine Empfindlichkeit normalisiert und wieder einzelne Photonen 20 misst. Die anderen Sensoren bleiben in der Zwischenzeit geblendet. Damit hat Eve die Möglichkeit, Bobs Sensoren nach Belieben an- und auszuschalten. Nun kann Eve einzelne Photonen mit der Polarisation des Sensors, den sie als einzigen nicht geblendet hat, in den Quantenkanal injizieren und hat komplette Kontrolle über Bobs Messgerät.⁶³

Mithilfe dieser Kontrolle über Bobs Messgerät kann Eve nun einen „intercept-resend“ (engl. 25 für „abfangen-weitersenden“⁶⁴) Angriff durchführen.⁶⁵ Sie misst die von Alice gesendeten Photonen genauso, wie Bob es normalerweise durchführen würde. Wenn sie nun eine 0 in

⁵⁹ vgl. (Winkler, 2009, S. 70)

⁶⁰ vgl. (Kim, 2008, S. 4)

⁶¹ (Winkler, 2009, S. 70)

⁶² vgl. (Makarov, 2008, S. 1)

⁶³ vgl. (Makarov, 2008, S. 1)

⁶⁴ vgl. (Klett, 2003, S. 318, 576)

⁶⁵ vgl. (Wolf, 2006, S. 395)

der geraden Basis misst, stellt sie das Störsignal so ein, dass Bobs Sensoren für die schräge Basis geblendet sind und erzeugt ein neues Photon mit dem Wert 0 in der geraden Basis, das sie an Bob weitersendet. Falls dieser die schräge Basis wählt, wird er nichts messen, denn die Sensoren sind geblendet. Falls er jedoch die gerade Basis wählt, misst er den von Eve
5 eingespeisten Wert 0. Dieses Verfahren gilt entsprechend für die drei anderen möglichen Messwerte. Somit hat Eve die zufällige Wahl der Messbasis durch Bob ausgeschaltet.⁶⁶

Wenn Alice und Bob am Ende der Übertragung ihre verwendeten Messbasen vergleichen, entfallen alle Ergebnisse, bei denen Alice eine andere Basis hatte als Eve. Bei den restlichen Ergebnissen haben Alice, Bob und Eve jeweils den gleichen Wert gemessen, somit ist es Eve
10 gelungen, den kompletten Schlüssel abzuhören.⁶⁷

Jedoch stellt laut Norbert Lütkenhaus von der Universität Erlangen und auch laut Vadim Makarov selbst dieses Verfahren bisher keine direkte Gefahr für die Quantenkryptographie dar. Damit eine solche Seitenkanalattacke funktioniert, muss dem Angreifer der genaue Aufbau der Sende- und Empfangsgeräte von Alice und Bob bekannt sein. Zusätzlich werden
15 nur spezielle Detektoren von diesem Verfahren geblendet, die in kommerziellen Geräten nicht eingesetzt werden.⁶⁸

*“In this paper, I report an imperfection found in single photon detectors (SPDs) of one particular type, namely those based on passively-quenched avalanche photodiodes (APDs). [...] The current commercial devices working at longer telecommunication
20 wavelengths are not affected by this pa[r]ticular vulnerability, because they use another type of SPD, a gated APD.”⁶⁹*

Darüber hinaus müssten Alice und Bob bemerken, dass Bob nur etwa die Hälfte der von Alice gesendeten Photonen empfängt, da Bob aufgrund der Blendung der Sensoren nichts misst, wenn er eine andere Basis wählt als Eve. Dies wird statistisch gesehen in etwa der Hälfte
25 aller Fälle passieren, sodass Alice und Bob auf den Angriff eines Lauschers schließen können. Makarov nimmt in seinem Artikel zu dieser Tatsache keine Stellung.

⁶⁶ vgl. (Makarov, 2008, S. 4)

⁶⁷ vgl. (Makarov, 2008, S. 4)

⁶⁸ vgl. (Makarov, 2008, S. 1)

⁶⁹ vgl. (Makarov, 2008, S. 1)

7 Fazit

Aus den vorgestellten Verfahren und Methoden geht hervor, dass Angriffe von Lauschern generell nicht verhindert werden können. Jedoch ist die Quantenkryptographie die einzige kryptographische Technik, bei der die beiden geheim kommunizierenden Partner mit Sicherheit bemerken, dass sie belauscht werden. Im Falle einer belauschten Übertragung können Alice und Bob trotzdem aus den übertragenen Informationen einen geheimen Schlüssel erstellen, indem sie Fehlerkorrekturverfahren anwenden, um die fehlerhaften Bits, die sich durch Eves Abhörvorgang eingeschlichen haben, zu neutralisieren. Die Vertraulichkeitsverstärkung ist ein weiteres Instrument, um die Sicherheit des Schlüssels zu erhöhen. Aufgrund des No-Cloning-Theorems ist es Eve zudem nicht möglich, das Messproblem durch die Erstellung von Kopien zu umgehen. Daher kann der Schluss gezogen werden, dass die Quantenkryptographie eine absolut sichere Schlüsselübertragung gewährleistet.

Wie gezeigt wurde, kann selbst mit solch aufwändigen Abhörtechniken wie dem von Kim realisierten FPB-Verfahren kein Schlüssel abgehört werden, solange Eve keinen Zugriff auf das Messgerät hat. Ein Lauschangriff, der die zeitgleiche Präsenz des Lauschers am Empfangsgerät zur Voraussetzung macht, ist aber kein Lauschangriff, sondern Einbruch, und somit nicht Thema dieser Arbeit. Auch mit den in Trondheim demonstrierten Seitenkanalattacken kann kein erfolgreicher Lauschangriff durchgeführt werden, ohne dass dies von Alice und Bob bemerkt werden müsste.

Aufgrund der oben angeführten Argumente komme ich zu dem Schluss, dass die Kryptographie mithilfe quantenkryptographischer Schlüsselverteilung ein absolut sicheres Verfahren ist, Informationen geheim zu übermitteln, solange die heute bekannten physikalischen Gesetzmäßigkeiten gültig bleiben. Falls es jedoch gelänge, zum Beispiel das No-Cloning-Theorem zu widerlegen, wäre diese Aussage allerdings zu revidieren. Bis dahin können streng vertrauliche Nachrichten weiterhin mithilfe sicherer, chaotischer Schlüssel zu einem chaotischen Geheimtext verschlüsselt werden, welcher wiederum in geordnete Information zurückkonvertiert werden kann.

8 Glossar

Chiffrierung

Als Chiffrierung wird der Vorgang bezeichnet, bei dem ein Klartext mithilfe eines Verschlüsselungsverfahrens in den unlesbaren Geheimtext umgewandelt wird.

5 Klartext

Als Klartext wird der Text bezeichnet, der durch ein Verschlüsselungsverfahren geschützt werden soll.

Geheimtext

10 Als Geheimtext wird der Text bezeichnet, der durch ein Verschlüsselungsverfahren chiffriert wurde.

Schlüssel

Als Schlüssel wird die Information bezeichnet, die benötigt wird, um einen Klartext zu verschlüsseln und auch umgekehrt aus einem Geheimtext durch Entschlüsselung den Klartext zu gewinnen.

15 Binärcode

Binärcode ist eine Darstellung von Informationen wie Zahlen oder Text im Binärsystem, das heißt lediglich durch 1 und 0 oder wahr und falsch. Zur Umwandlung in Binärcode können verschiedene Methoden verwendet werden, beispielsweise das BCD-Verfahren für Zahlen.

Modulo-Operator

20 Modulo (mathematisch als „mod“ geschrieben) ist eine mathematische Funktion, die den Rest aus der Division zweier ganzer Zahlen angibt. Beispiel: $11 \bmod 3 = 2$, da $11/3 = 9$ Rest 2.

One-Time-Pad

25 Ein One-Time-Pad ist ein Verschlüsselungsverfahren, dessen Güte nicht von der Komplexität des Verfahrens an sich abhängt, sondern allein von der Zufälligkeit des verwendeten Schlüssels. Wenn Schlüssel verwendet werden, die die gleiche Länge wie der Klartext

besitzen, ist dieses Verfahren unknackbar. Da die Güte jedoch von der Zufälligkeit des Schlüssels abhängt, darf jeder Schlüssel nur ein einziges Mal verwendet werden.⁷⁰

Basis

Mithilfe einer Basis lässt sich jeder Vektor als eine endliche Linearkombination der Basisvektoren darstellen. Zum Beispiel wäre die Basis des normalen zweidimensionalen Raumes $x = (1; 0)$ und $y = (0; 1)$. Der Vektor $a = (5; 2)$ ließe sich als Linearkombination $a = 5x + 2y$ darstellen.

Monoalphabetische Verschlüsselung

Die monoalphabetische Verschlüsselung ist ein Verschlüsselungsverfahren, bei dem ein einziges, festes Alphabet zur Verschlüsselung genutzt wird. Jeder Klartextbuchstabe wird bei der Verschlüsselung durch einen ihm zugeordneten Geheimtextbuchstaben ersetzt.⁷¹

Klassischer Informationskanal

Ein Informationskanal wie beispielsweise das Telefon oder Internet, über den Informationen nicht abhörsicher versendet werden können.

15 Vertraulichkeitsverstärkung

Die Vertraulichkeitsverstärkung ist eine Methode zur Verringerung der von einem Spion abgehörten Information. Alice und Bob müssen dazu ihren fehlerkorrigierten gemeinsamen Schlüssel mit einem systematischen Verfahren verkürzen.⁷²

XOR-Verknüpfung

20 Eine XOR-Verknüpfung, auch als Exklusiv-Oder bekannt, ergibt genau dann 1, wenn beide eingegangenen Bits nicht gleich sind. In der Literatur wird oft das Symbol \oplus verwendet. Beispiel: $1 \oplus 0 = 1$; $0 \oplus 0 = 0$; $1 \oplus 1 = 0$.

Verschränkung

25 Die Verschränkung ist ein quantenphysikalisches Phänomen zwischen zwei oder mehreren Teilchen. Wenn zwei Teilchen verschränkt sind, dass heißt sich in einem verschränkten

⁷⁰ vgl. (Beutelspacher, Schwarzpaul, & Neumann, 2006, S. 39-40)

⁷¹ vgl. (Singh, 2004, S. 32)

⁷² vgl. (Vertraulichkeitsverstärkung - Fischer Kompakt, 2009)

Zustand befinden, besteht eine Korrelation zwischen beiden Teilchen: Wenn man das eine Teilchen misst, wird das andere beeinflusst, egal wo im Universum es sich befindet.⁷³

⁷³ vgl. (Bruß, Quanteninformation, 2003, S. 23)

9 Literaturverzeichnis

- Baeyer, H. C., & Filk, T. (2007). *Das informative Universum*. München: C.H.Beck.
- Beutelspacher, A., Schwarzpaul, T., & Neumann, H. B. (2006). *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk*. Wiesbaden: Vieweg+Teubner Verlag.
- Bruß, D. (2003). *Quanteninformation*. Frankfurt am Main: Fischer Taschenbuch Verlag.
- Bruß, D., & Weinfurter, H. (April 2005). Geheime Botschaften aus Licht. *Physik Journal*, S. 57-62.
- Camejo, S. A. (2007). *Skurrile Quantenwelt*. Frankfurt am Main: S. Fischer Verlag GmbH.
- Haase, A. (2007). *Quantenkryptographie- und Kommunikation*. Abgerufen am 4. März 2009 von http://users.physik.fu-berlin.de/~haase/physics/reports/quantum_computation_slides.pdf
- Homeister, M. (2005). *Quantum Computing verstehen*. Wiesbaden: Vieweg+Teubner Verlag.
- Ilic, N. (2007). The Ekert Protocoll. *JOURNAL OF PHY334*, 1-4.
- Kim, T. (2008). *Complete physical simulation of the entangling-probe attack on the BB84 protocol*. Abgerufen am 26. Februar 2009 von http://arxiv.org/PS_cache/quant-ph/pdf/0611/0611235v1.pdf
- Klett. (2003). *Pons Schülerwörterbuch Englisch-Deutsch/Deutsch-Englisch*. Stuttgart: Ernst Klett Sprachen.
- Kühn, S. (2007). *Quantenkryptographie*. Abgerufen am 11. März 2009 von <http://www.physik.uni-kl.de/agfleischhauer/Uebungen/handout-Kuehn.pdf>
- Makarov, V. (2008). *Controlling passively-quenched single photon detectors by bright light*. Abgerufen am 17. März 2009 von http://arxiv.org/PS_cache/arxiv/pdf/0707/0707.3987v2.pdf
- Patalong, F. (12. 10 2007). *QUANTENKRYPTOGRAPHIE: Die sicherste Datenleitung der Welt*. Abgerufen am 5. 3 2009 von SPIEGEL ONLINE Netzwerk: <http://www.spiegel.de/netzwelt/tech/0,1518,511087,00.html>
- Singh, S. (2004). *Codes - Die Kunst der Verschlüsselung*. München: Deutscher Taschenbuch Verlag GmbH & Co. KG.

Vertraulichkeitsverstärkung - Fischer Kompakt. (17. März 2009). Abgerufen am 17. März 2009 von Fischer Kompakt: http://www.fischer-kompakt.de/sixcms/detail.php?template=glossar_detail&id=187057

Winkler, D. V. (5. Januar 2009). Abhörsichere Quanten - Quantenkryptographie auf dem Weg zur Marktreife. *c't*, S. 66-71.

Wolf, E. (2006). *Progress in Optics*. Philadelphia: Saunders Ltd.

Zeppmeisel, M. (2006). Einführung in die Grundlagen der Quantenkryptographie. München.

10 Abbildungsverzeichnis

Titelbild: Grafische Darstellung eines Quantenkanals.

Quelle: <http://idw-online.de/pages/de/newsimage?id=76783>.....1

Abbildung 1: Ein beispielhafter Ablauf einer Schlüsselübertragung nach dem BB84-Protokoll.

Quelle: Lennart Moltrecht 10

Abbildung 2: Schematischer Aufbau einer quantenkryptographischen Verbindung nach dem BB84-Protokoll. Quelle: Lennart Moltrecht 11

11 Erklärung

Ich erkläre hiermit, dass ich die Facharbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benutzt habe.

.....

Ort, Datum

.....

Unterschrift des Schülers