Department für Physik
Ludwig-Maximilians-Universität München

Freiraumoptische Quantenkryptographie

Diplomarbeit von
Sebastian Schreiner

angefertigt unter der Anleitung von
Prof. Dr. Harald Weinfurter

Inhaltsverzeichnis

1

Einleitung

Die elektronische Verbindung von Arbeitsplätzen und Computern in lokalen Netzen und dem Internet ist heute selbstverständlich und übernimmt einen großen Teil des Informationsflusses. Viele Inhalte entstehen am Computer oder werden zumindest dort gespeichert, weshalb sie sich natürlich für die Kommunikation auf elektronischem Wege besonders eignen. Sensible Daten werden in der Regel verschlüsselt übertragen, wobei eine Reihe von Verfahren standardisiert ist und ein gewisses Maß an Sicherheit bietet. Prinzipiell kann aber eine, nach gebräuchlichen Algorithmen verschlüsselte Nachricht von einem Angreifer, wenn auch mit sehr großem Aufwand, rekonstruiert werden. Die Sicherheit basiert so lediglich auf Annahmen über die heute und in Zukunft maximal verfügbare Rechenleistung – ein Risiko, das man in Ermangelung einer sicheren Verbindung zum Schlüsselaustausch eingehen muss. Mit einer Methode der Schlüsselverteilung, deren Sicherheit durch Naturgesetze beweisbar gewährleistet ist, kann diese Lücke jedoch geschlossen werden. Es zeigt sich, dass die Quantenmechanik, insbesondere die Quanteninformationstheorie, Möglichkeiten bietet, die Risiken konventionellen Schlüsselaustauschs zu vermeiden.

Nur die Quantenmechanik kann die Effekte beschreiben, die sich an den kleinsten Einheiten physikalischer Systeme manifestieren. Die klassische, deterministische Beschreibung der Physik versagt den Zugang zu Skalen, auf denen einzelne Quanten aufgelöst werden und in Messergebnissen zunehmend Unschärfe beobachtet wird. Physikalische, in der Alltagswelt klar festgelegte Größen können einem Quant im Allgemeinen nicht mehr zugeordnet werden. Der Messvorgang an sich erhält deshalb in der Quantenmechanik eine neue Interpretation: Während klassisch eine physikalische Eigenschaft beobachtet werden kann, ohne diese zu stören, ist dies quantenmechanisch im Allgemeinen nicht möglich. Darüber hinaus ist das Messergebnis nicht in jedem Fall determiniert.

Die Quanteninformationstheorie macht sich diese Effekte zunutze, um durch den Übergang von Bits zu Qubits die Komplexität bei mathematischen Problemen in der coputerbasierten Lösung zu reduzieren. Für einen zukünftigen Quantencomputer liegen bereits Algorithmen vor, mit denen viele konventionelle Verschlüsselungen um

Größenordnungen effizienter entschlüsselt werden können [1]. Auf ihren praktischen Einsatz werden diese Verfahren jedoch noch Jahre warten müssen – bis heute sind erst experimentelle Anfänge des Rechnens mit Qubits vorgestellt [2]. Bennett und Brassard erkannten jedoch 1984 die Möglichkeit der sicheren Schlüsselübertragung als Anwendung der Informationsverarbeitung mit Qubits und konnten so den Grundstein für den Zweig der Quanteninformationstheorie legen, der bis heute der Alltagstauglichkeit am nächsten kommt: die Quanten-Schlüsselverteilung (*quantum key distribution*, QKD).

Im Gegensatz zu klassischen Kommunikationswegen, deren Nutzung jederzeit beobachtet werden kann, verhindern bei der QKD quantenmechanische Gesetze das unbemerkte Abhören eines Quantenkanals. Die Sicherheit von quantenkryptographischen Protokollen konnte für allgemeinste Angriffsszenarien, die allein durch Naturgesetze eingeschränkt sind, bewiesen werden [3, 4].

Die Realisierung des Quantenkanals unterscheidet zwei große Gruppen von QKD-Systemen: Die eine versendet die Qubits, meist Photonen, durch Glasfasern, eine andere Klasse von Systemen arbeitet mit Teleskopen, um die Quanten vom Sender freiraumoptisch (*engl.: free-space*) zum Empfänger zu übertragen. Auf diese Weise konnte Quanten-Schlüsselverteilung bereits über eine Entfernung von bis zu 144 km demonstriert werden [5–8]. Fernziel ist hier, QKD mit Hilfe von Satelliten zwischen beliebigen Punkten der Erde zu ermöglichen [9]. Ein Satellit könnte den Schlüssel, der beim Überflug einer Bodenstation ausgetauscht wurde, an anderer Position seines Orbits einer zweiten, entfernten Station übermitteln. Der Integrität des Satelliten selbst müssten die Kommunikationspartner jedoch vertrauen. Vorausgesetzt, Sender und Empfänger haben gleichzeitig eine Sichtverbindung zum Satelliten, so kann mit Protokollen, die mit einer Quelle verschränkter Teilchen an Bord des Satelliten arbeiten, diese Einschränkung vermieden werden [10, 11].

Auch die Reichweitenrekorde faserbasierter Systeme liegen in der Größenordnung von 100−200 km [12, 13], wobei jedoch zur Erweiterung der maximalen Reichweite auf globale Entfernungen eine Vielzahl von Relaisstationen benötigt werden, so genannte *quantum repeater*. Derzeit ist die typische Schlüsselrate um Größenordnungen niedriger als bei freiraumoptischen Systemen[1], da für Wellenlängen, wie sie in Telekommunikations-Glasfasern verwendet werden, keine Detektoren mit hoher Quanteneffizienz und geringem Rauschen zur Verfügung stehen. Trotzdem sind bereits faserbasierte Netzwerkgeräte kommerziell verfügbar, die eine konventionelle Verschlüsselung mit einem quantenkryptographisch ausgetauschten Schlüssel kombinieren[2]. Über Glasfasern können so etwa verschiedene Firmengebäude mit hoher Sicherheit vernetzt werden.

[1] Die Rohschlüsselrate über 122 km Faser in [13] ist 9,2 Bit/s, freiraumoptisch konnte in [6] *sicherer* Schlüssel über 144 km mit mehr als 200 Bit/s erzeugt werden.

[2] idQuantique, http://idquantique.com – MaqiQTechnologies, http://www.magiqtech.com – SmartQuantum, http://www.smartquantum.com

Einen anderen Ansatz verfolgen Experimente, die auf kürzesten Strecken mit möglichst kleinen, günstigen Geräten QKD implementieren. Mit solchen mobilen Geräten können Verbraucheranwendungen im Internet, wie z.B. Kreditkartenapplikationen, mit Einmal-Schlüsseln gesichert werden, die auf einem tragbaren Gerät gespeichert sind und die der Kunde nach Verbrauch an einer QKD-Station erneuert [14].

Die Versuchsanlage für QKD, deren Aufbau Gegenstand dieser Arbeit ist, arbeitet ebenfalls freiraumoptisch, verwendet also Teleskope, um einen Quantenkanal durch die Luft zu etablieren. Dabei liegt der Schwerpunkt hier auf kurzen Distanzen (bis zu etwa 2 km) zu Gunsten eines einfachen, robusten Systems. Das hier beschriebene Experiment soll als Prototyp für eine QKD-Strecke fungieren, die eine sichere Vernetzung von Gebäuden im städtischen Raum ermöglicht, indem sie als autonome und kontinuierliche Quelle für Schlüsselmaterial bestehende Netzwerktechnik ergänzt.

Für derartige Anwendungen kann auf große Hochleistungsteleskope verzichtet werden, weshalb Sender und Empfänger klein und relativ leicht bleiben. So bietet sich die Möglichkeit, das QKD-System flexibel und auch für kurzfristige Anwendungen einzusetzen. Der Aufwand zur Installation ist minimal: Neben der Energieversorgung und dem klassischen Kanal, der prinzipiell mit jedem kommerziell verfügbaren Netzwerk realisiert werden kann, muss keine Infrastruktur aufgebaut werden. Insbesondere entfällt die Verlegung von Kabeln bzw. Lichtwellenleitern durch den öffentlichen Raum, was nicht zuletzt ein Kostenfaktor ist. Die verwendete Technik erlaubt hohe Geschwindigkeiten für die Übertragung, so werden mit dem hier beschriebenen Aufbau sichere Schlüsselraten in der Größenordnung von ISDN-Geschwindigkeit (64 kBit/s) angestrebt. Zudem wurde beim Aufbau der Anlage speziell die Verwundbarkeit über so genannte Seitenkanäle geprüft. Diese entstehen, wenn Daten auf physikalische Eigenschaften der Photonen moduliert werden, deren Codierung vom Protokoll nicht vorgesehen ist. Für die Sicherheit der QKD ist es aber wichtig, dass die Photonen für einen Angreifer in jeder Hinsicht ununterscheidbar sind. Das Maß der Ununterscheidbarkeit in spektraler, zeitlicher und räumlicher Hinsicht wird hier für den QKD-Sender ermittelt.

Die vorliegende Arbeit liefert in Kapitel 2 einen kurzen Einblick in moderne kryptographische Verfahren, bevor im Kapitel 3 eine Einführung in die QKD gegeben wird, die auch die zu Grunde liegenden physikalischen, quantenmechanischen Prinzipien erläutert. Kapitel 4 und 5 befassen sich mit dem Aufbau von Sender und Empfänger für die QKD-Anlage. Dabei wird die Charakterisierung des Systems in Bezug auf Seitenkanäle eingehend dokumentiert. Die Installation und Inbetriebnahme des Systems wird, zusammen mit ersten Resultaten aus Schlüsselübertragungen, in Kapitel 6 vorgestellt.

2

Klassische Kryptographie

Die alte Kunst, Geheimnisse zu kommunizieren, ist längst zur Wissenschaft geworden. Mathematiker und Computerwissenschaftler arbeiten auf der ganzen Welt daran, Informationen effektiv und sicher mit immer neuen Algorithmen vor fremden Augen zu schützen, d.h. zu chiffrieren. Ein nicht weniger bedeutendes, wenn auch oft weniger öffentliches Arbeitsfeld, ist die Entschlüsselung geheimer Inhalte, also der Angriff auf Algorithmen und schließlich auf die dahinter verborgenen Geheimnisse. Die Lehre dieser beiden Fertigkeiten ist die Kryptologie: Kryptographie und Kryptanalyse – das „verborgene Schreiben“ und die „Lösung von Verborgenem“.

Die verwendeten Methoden haben sich seit den Anfängen der Kryptologie grundlegend weiterentwickelt. Wo früher ein geheimes Alphabet ausreichend war, um den Inhalt einer Nachricht vor den Augen eines Neugierigen als wirre Zeichenfolge zu schützen, kommen heute Computer, manchmal sogar spezialisierte integrierte Schaltkreise zum Einsatz, um mit immer längeren Schlüsseln Daten zu chiffrieren.

Die Abkehr von geheimen Verfahren zugunsten der Kombination aus einem geheimen Schlüssel und einem allgemein bekannten Algorithmus war ein entscheidender Schritt in der Geschichte der Kryptographie. Als Forderung zuerst von Kerckhoff formuliert [15], ermöglicht dieser Ansatz die Evaluation eines kryptographischen Verfahrens durch Dritte. Proprietäre und geheime Algorithmen stellen sich unter Umständen zu spät als schwach oder fehlerbehaftet heraus, wie etwa die Verschlüsselungsverfahren A5/1 und A5/2, die die Übertragung im GSM Netz sichern sollten. Sie gelten seit spätestens 1999 durch die Beschreibung von Briceno, Goldberg, und Wagner [16] als gebrochen[1].

Auch moderne Chiffren sind, mit Ausnahme der *Vernam-Chiffre* (siehe 2.2), keinesfalls *unbedingt* sicher. Vielmehr begründet sich deren Sicherheit auf die Annahme, dass die technische und damit auch finanzielle Ausstattung eines potentiellen Abhörers auf ein gewisses Maß beschränkt ist. Für langfristige Sicherheit von Systemen,

[1] A5/1 und A5/2 arbeiten auch mit einem geheimen Schlüssel, jedoch ist der proprietäre Algorithmus zu einfach, so dass der Schlüssel ermittelt werden kann

die nur schwer oder gar nicht modernisiert werden können (etwa Kryptographie-Hardware in einem Satelliten), muss zusätzlich der technische und wissenschaftliche Fortschritt richtig eingeschätzt werden. Die sichere Schlüsselverteilung stellt aber, auch im Fall der Vernam Chiffre, eine gesonderte Aufgabe dar – für heutige Methoden der Schlüsselverteilung gelten die gleichen Sicherheitsvorbehalte, wie für die Verschlüsselungsalgorithmen selbst. Die einzige Lösung bietet hier die QKD, die Thema des nächsten Kapitels ist, nachdem hier zunächst ein kurzer Überblick über die klassische Kryptographie gegeben wird.

2.1 Grundlegende Techniken

Für die unterschiedlichsten Anwendungen, Software Plattformen und Geräte sind heute eine Vielzahl von Chiffren standardisiert. Hier sollen aber nur einige Prinzipien erläutert und kurz wichtige Verschlüsselungsverfahren vorgestellt werden. Dabei bezieht sich der Ausdruck „klassische Verfahren“ auf Algorithmen, die nicht quantenmechanisch erklärt werden müssen. Weiterführende Einblicke liefert das Buch von Schneier [17].

Um aus Klartext eine Chiffre zu erzeugen, kommen zwei prinzipielle Methoden, meist in einer Kombination, zum Einsatz:

Transposition

Das Vertauschen der Positionen von Zeichen im Klartext. – Die Permutationsvorschrift kann z.B. in Form einer Zeilenlänge angegeben werden. Der Klartext wird in Zeilen eben dieser Länge aufgeschrieben, die Chiffre ergibt sich, indem Spaltenweise gelesen wird. So wird aus folgendem Satz mit der Zeilenlänge zehn („10“ ist hier der Schlüssel):

Klartext: ES GIBT KEINE GEHEIMSCHRIFT, DIE SICH NICHT MIT EIN WENIG GEDULD ENTZIFFERN LIESSE. [18]

E	S	G	I	B	T	K	E	I	N
E	G	E	H	E	I	M	S	C	H
R	I	F	T	D	I	E	S	I	C
H	N	I	C	H	T	M	I	T	E
I	N	W	E	N	I	G	G	E	D
U	L	D	E	N	T	Z	I	F	F
E	R	N	L	I	E	S	S	E	

Chiffertext: EERHIUE SGINNLR GEFIWDN IHTCEEL BEDHNNI TIITITE KMEMGZS ESSIGIS ICITEFE NHCEDF

Das Vorgehen zur Entschlüsselung ist offensichtlich. Auch komplizierte Permutationsvorschriften können heute mit Computern meist leicht analysiert werden. Eine reine Transpositionsverschlüsselung wird deshalb praktisch nicht verwendet.

Substitution

Das Ersetzen von Zeichen im Klartext gegen andere an der gleichen Position. – Ein einfaches Beispiel ist eine Verschiebechiffre (auch Caesarchiffre) wie z.B. ROT13. Jedes Zeichen wird ersetzt (rotiert) gegen den Buchstaben, der im Alphabet gerade gegenüber liegt, man vertauscht also die Buchstaben über die Linie hinweg:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Die Sicherheit ist aber nicht viel höher, als die einer am Kopf geschriebenen Botschaft, die Anwendungsgebiete hingegen sind sehr ähnlich. Hier geht auch schon ein Schlüssel mit ein, die Zahl „13“ erzeugt eine von 25 Ersetzungslisten, die durch Verschiebung des Alphabets entstehen.

In der Weiterentwicklung solch einfacher Substitutionsvorschriften werden je nach Position im Klartext verschiedene Ersetzungstabellen, kontrolliert durch einen Schlüssel, angewendet. Man spricht dann von Vigenère Chiffre [19], auf der auch die Arbeitsweise elektromechanischer Verschlüsselungsmaschinen aus der Zeit des zweiten Weltkriegs beruht, wie etwa der bekannten ENIGMA [20].

Moderne Chiffren arbeiten stets mit beiden Techniken: Der Klartext, dargestellt in Binärwerten, wird, oft in mehreren Durchgängen, permutiert und durch Substitution verändert.

Eine weitere Unterscheidung gebräuchlicher Verfahren lässt sich über den bzw. die Schlüssel treffen. Eine Klasse von Algorithmen arbeitet mit einem einzigen Schlüssel zur Ver- und Entschlüsselung, wie etwa die Zahl „13“ im Beispiel zur Substitution. Man spricht von *symmetrischen* Verschlüsselungen. Auf der anderen Seite gibt es *asymmetrische* Verfahren, die für Chiffrierung und Dechiffrierung jeweils eigene Schlüssel benutzen. Im Folgenden werden die Vor- und Nachteile an Beispielen deutlich werden.

2.2 Symmetrische Verschlüsselungen

DES

Ein spezieller symmetrischer Algorithmus, der über 20 Jahre hinweg weit verbreitet war, ist DES (*data encryption standard*). Der Hauptgrund für seine Ablösung 2001 als Standard durch AES (*advanced encryption standard*) liegt in der geringen Schlüssellänge von nur 56 Bit. Der Anstieg der Rechenleistung neuer Computer hatte nach und nach einen Angriff durch Probieren aller möglichen Schlüssel (ca. 10^{17}) in überschaubarer Zeit immer aussichtsreicher gemacht. Man spricht in diesem Fall von einem so genannten *brute-force* Angriff, übersetzt in etwa „Methode der rohen Gewalt“.

Der DES Algorithmus [17, 21] wird als Blockchiffre bezeichnet. Jeweils 64 Bit des Klartextes werden auf einmal bearbeitet. Für diese Blöcke wird eine spezielle Kombination von Permutationen und Substitutionen in 16 Runden wiederholt. Dabei ist DES so angelegt, dass der Algorithmus, bis auf eine Umordnung des Schlüssels, selbstinvers ist.

Erweiterungen von DES können, etwa durch mehrmalige Verschlüsselung (z.B. Triple DES) oder durch eine Verlängerung des Schlüssels, ein ausreichendes Sicherheitsniveau wiederherstellen. Der Nachfolger AES [22] ist ebenfalls ein Blockalgorithmus mit variabler Schlüssellänge bis 256 Bit, basiert aber nicht auf DES.

Vernam Chiffre

Ein einziges Verschlüsselungsverfahren ist bewiesen sicher [23]: Die Vernam Chiffre lässt keinen effektiveren Angriff zu als das direkte Erraten der Nachricht. Unabhängig von Annahmen über Wissen oder Technologie des Abhörers bietet der auch als *one-time-pad* bezeichnete Algorithmus[2] absolute Sicherheit, jedoch bei hohem Schlüsselaufwand: Jedes Bit einer Nachricht wird per XOR mit genau einem Bit des Schlüssels verknüpft, dieser muss also genau so lang sein, wie der Klartext selbst.

Da der Schlüssel natürlich sowohl dem Sender als auch dem Empfänger zur Verfügung stehen muss, verschiebt die Vernam Chiffre also das Problem der sicheren Kommunikation der Nachricht auf die des Schlüssels und ist so, ohne einen sicheren Kommunikationskanal, weitgehend unpraktisch für den Einsatz in größerem Rahmen. Trotzdem gibt es Beispiele, in denen die geforderte Sicherheit den Aufwand rechtfertigt. So werden auf *one-time-pad* basierende Kryptographie-Produkte zum Beispiel von einer Firma Mils[3] in Österreich vertrieben.

Kann man auf absolute Sicherheit verzichten, können asymmetrische Algorithmen die Schlüsselverteilung, auch unter vielen Parteien, einfach bewerkstelligen.

2.3 Asymmetrische Verschlüsselungen

Sender und Empfänger verwenden hier zwei verschiedene Schlüssel. Dabei darf der zur Verschlüsselung verwendete, je nach Verfahren auch öffentlich bekannt sein, man spricht dann von *public-key* Systemen [25, 26]. Was die Verteilung trivial ermöglicht, gefährdet auf der anderen Seite jedoch die Sicherheit: Der geheime Schlüssel zur Decodierung der Nachricht kann prinzipiell berechnet werden, wenn man den öffentlichen Schlüssel kennt. Der numerische Aufwand wird jedoch als extrem hoch betrachtet, weshalb *public-key*-Verfahren oft ein ausreichendes Maß an Sicherheit bieten und vielfach eingesetzt werden. Das bekannteste Beispiel eines

[2] Die Chiffre von Vernam [24] sieht den, für die Sicherheit essentiellen, *zufälligen* Schlüssel noch nicht vor, „Vernam Chiffre“ wird jedoch synonym mit *one-time-pad* verwendet.

[3] `http://www.mils.com`

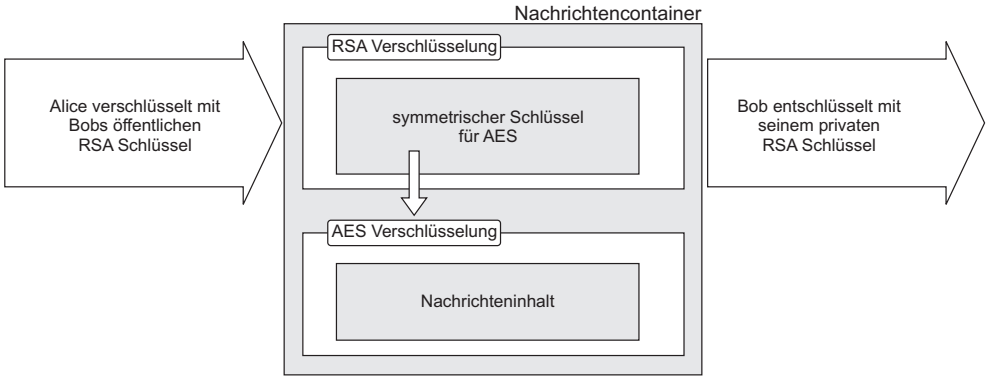


Abb. 2.1: Nachrichtencontainer für hybride Kryptographiesysteme. Bei diesen Verfahren werden die Vorteile symmetrischer und asymmetrischer Verfahren kombiniert: Die Nachricht wird schnell und effizient z.B. mit AES symmetrisch verschlüsselt, der dazu verwendete Schlüssel asymmetrisch mit RSA. Der Container, der letztendlich verschickt wird, enthält beides.

public-key-Systems ist wohl der Standard RSA[4] [27, 28], der auch im Rahmen der Email Verschlüsselung (openPGP Standard) Anwendung findet.

Ein Empfänger muss also zunächst ein Paar von Schlüsseln, bestehend aus dem privaten und dem so genannten öffentlichen Teil, erzeugen und letzteren dem Sender übermitteln[5]. Dieser nutzt den öffentlichen Schlüssel, um die Nachricht zu verschlüsseln. Der Empfänger kann schließlich mit dem geheimen Schlüssel den Klartext rekonstruieren.

Das Schlüsselpaar für Verfahren wie RSA entsteht aus zwei großen Primzahlen. Während es sehr einfach ist, diese bei der Schlüsselerzeugung zu multiplizieren, muss für einen erfolgreichen Angriff das Produkt wieder faktorisiert werden. Die Zerlegung in Primfaktoren ist jedoch auch mit dem besten bekannten Algorithmus exponentiell aufwendig und gilt für Zahlen der verwendeten Größe als nicht durchführbar [17].

Der Rechenaufwand im Rahmen der Verschlüsselung nach RSA ist relativ hoch, symmetrische Verfahren sind in dieser Hinsicht wesentlich genügsamer. In der Praxis werden deshalb Hybrid-Systeme verwendet: Zur Verschlüsselung der eigentlichen Nachricht nutzt man ein symmetrisches Verfahren, anschließend versendet man aber zusammen mit der Chiffre den asymmetrisch verschlüsselten Schlüssel. In Abbildung 2.1 ist ein typischer Nachrichtencontainer für hybride Verfahren gezeigt. Auf diese Weise können beispielsweise die Effizienz von AES und die Vorteile der Schlüsselverteilung mit RSA gemeinsam genutzt werden.

RSA bietet in einigen Ausprägungen auch die Möglichkeit, Nachrichten zu signieren, indem diese, bzw. eine Prüfsumme des Inhalts, mit dem geheimen Schlüssel

[4] RSA steht für die Initialen von Ron Rivest, Adi Shamir und Leonard Adleman, von denen der Vorschlag zu RSA stammt.

[5] In der Regel übernehmen so genannte *public key server* die Verteilung der öffentlichen Schlüssel über das Internet.

des Absenders chiffriert wird. Der Empfänger kann mit dem öffentlichen Schlüssel des Senders dann die Herkunft und Integrität des Inhalts überprüfen. In diesem Fall tauschen also die beiden Schlüssel die Rollen des Ver- und Entschlüsslers: Um sicherzustellen, dass die Signatur tatsächlich vom Absender erstellt wurde, kommt dessen privater Schlüssel zum Einsatz, auf der anderen Seite ist es, mit dem zugehörigen öffentlichen Schlüssel, jedem möglich, die Integrität der Nachricht zu prüfen.

2.4 Sicherheitsaspekte klassischer Kryptographie

Das Verhältnis von Kryptographen und Kryptanalytikern ist keinesfalls das zwischen Gut und Böse. Vielmehr sind letztere heute entscheidend an der Entwicklung neuer Methoden beteiligt und prüfen laufend, ob bestehende Chiffrierverfahren noch als sicher verwendet werden können. Die Vorgehensweisen sind jedoch bei Angreifern und Analytikern identisch. Über das direkte Probieren aller Schlüssel hinaus, wird stets versucht, Schwächen des Algorithmus und nicht zuletzt Bedienerfehler auszunutzen:

Bei DES ist immer noch die *brute-force* Attacke die am schnellsten Erfolg versprechende, da die Schlüssellänge für heutige Verhältnisse zu kurz ist. Die Sicherheit von RSA hingegen steht und fällt mit der Möglichkeit, große Zahlen zu faktorisieren. Die Existenz eines effizienten Algorithmus ist nicht ausgeschlossen, wenn auch unwahrscheinlich. Für einen zukünftigen Quantencomputer hingegen liegt von Shor bereits eine nur polynomial aufwendige Lösung vor [1].

Darüber hinaus gibt es verschiedene Szenarien, die unbedingt zu vermeiden sind, um die Sicherheit einer Nachricht nicht zu gefährden. So darf etwa kein unbekannter Inhalt direkt mittels RSA signiert werden. Der private Schlüssel könnte dann leicht von einem Angreifer berechnet werden, dem dann der Klartext *und* die Chiffertexte zu beiden Schlüsseln, dem öffentlichen und dem privaten, vorliegen [17]. In der Regel werden derartige Schwachstellen aber durch übergeordnete Protokolle oder die spezielle Implementierung verhindert. In diesem Beispiel besteht der Ausweg etwa im Signieren einer Prüfsumme an Stelle der unter Umständen vom Angreifer speziell konstruierten Nachricht.

Im Fall von AES war, auf Grund der Schlüssellänge, bisher nur eine Art von Angriffen erfolgreich: So genannte Seitenkanalattacken (*engl.: side channel attacks*). Diese richten sich nicht gegen den Schlüsseltext oder den Algorithmus direkt, sondern versuchen andere Informationskanäle heranzuziehen. Bei AES konnte über eine Analyse der genauen Zeitabläufe auf Prozessor- bzw. Prozessorcacheebene der Schlüssel ermittelt werden, wofür allerdings ein Zugriff auf den entsprechenden Computer nötig war [29]. Weitere Seitenkanalangriffe anhand von Leistungsaufnahme oder elektromagnetischer Abstrahlung sind vorstellbar.

Durch hinreichend lange Schlüssel kann also ein beliebig kleines Risiko, bis hin zu absoluter Sicherheit wie im Fall der Vernam Chiffre, für eine vertrauliche

Kommunikation erreicht werden. Letztendlich bleibt für alle Kryptographieverfahren aber das Problem der sicheren Schlüsselübertragung zu lösen – dies fordert einen eher sparsamen Umgang mit aufwendig verteiltem Schlüsselmaterial. Selbst das Verfahren zum Schlüsselaustausch von Diffie und Hellman [25], findet es auch breite Anwendung, unterliegt den gleichen Einschränkungen an die Sicherheit wie RSA. Moderne kryptographische Verfahren stellen deshalb meist einen Kompromiss, zwischen Schlüsselaufwand (Verbrauch) auf der einen Seite und Sicherheit auf der anderen Seite dar. Bis heute bietet nur die QKD die Möglichkeit, Schlüsseldaten sicher und automatisch zu erzeugen und zu verteilen.

2.5 Authentifizierung

Ein Szenario, gegen das auch die QKD im folgenden Kapitel nicht gefeit ist, ist der so genannte *Man-in-the-middle*-Angriff (*deutsch: Mann-in-der-Mitte-Angriff*, Janusangriff). In diesem Fall unterbricht der Abhörer die Verbindung, um sich gegenüber dem Sender als vermeintlicher Empfänger auszugeben und umgekehrt. Gelingt es ihm, die rechtmäßigen Kommunikationspartner auf diese Weise zu täuschen, so erhält er unbemerkt alle gesendeten Nachrichten, bevor er sie als falscher Sender an den echten Empfänger weiterleitet. Zudem ist der Angreifer in der Lage, den Inhalt der Kommunikation nach seinem Belieben zu ändern, was diese Strategie noch gefährlicher macht.

Die Authentifizierung hat somit zwei Aufgaben: Zum einen muss der Sender sicherstellen, dass sein Kommunikationspartner tatsächlich der wahre, authentische Empfänger ist. Zum anderen hat dieser die Aufgabe, die Nachricht auf ihre Unversehrtheit, d.h. ihre Authentizität, zu prüfen. Im Briefverker, lange vor dem Computerzeitalter, wurden diese Anforderungen durch die Unterschrift des Absenders (Authentifizierung seiner Person) und einen versiegelten Umschlag (Integrität der Nachricht) erfüllt. Heute, im Rahmen elektronischer Kommunikation, werden digitale Signaturen verwendet um Authentifizierung durchzuführen.

3

Quantenkryptographie

Auch wenn die vorgestellten klassischen Kryptographieverfahren zum Teil sehr hohe Sicherheit versprechen, ist diese immer bedingt. Die Computerleistung steigt stetig an, so dass man sich Fragen muss, ob, oder zumindest bis wann, man Algorithmen trauen darf, die die Geheimhaltung einer Nachricht nur an begrenzte Rechenkapazitäten knüpfen. Dabei sind die aktuellen Grenzen keineswegs öffentlich bekannt. Sicher ist, je größer die Notwendigkeit zur Geheimhaltung, desto größer wird auch der materielle Einsatz eines Angreifers sein.

Schon 2001 ist von Vandersypen et al. ein Quantencomputer auf der Basis von Kernspin Resonanzmessungen (NMR) realisiert worden [2]. Dieser konnte mit dem Algorithmus von Shor die Zahl 15 faktorisieren. Auch wenn das aktuell keine Bedrohung für RSA mit 200-stelligen Zahlen darstellt, so ist doch ein erster Schritt gemacht.

Sogar der an sich unüberwindbare *one-time-pad* muss auf eine sichere Schlüsselübertragung vertrauen. Die Kommunikationspartner müssen für unbedingte Sicherheit zuvor einen Schlüssel persönlich ausgetauscht haben. Da dieser aber nur genau einmal verwendet werden darf, muss der Vorrat auch regelmäßig wieder aufgefüllt werden. In der Praxis ist dieses Verfahren daher nur in Ausnahmefällen anwendbar.

Die Quantenkryptographie bietet hier den Ausweg: Tatsächlich ist es möglich, einen Kommunikationskanal zwischen Sender und Empfänger aufzubauen, dessen Sicherheit man prüfen kann: Die Messung eines unbekannten quantenmechanischen Zustands durch einen Angreifer wird diesen in der Regel verändern, was in der Folge Übertragungsfehler verursacht. Wird über einen, mittels QKD gesicherten Kanal nun ein Schlüssel ausgetauscht, kann man dessen Unversehrtheit nachträglich, anhand der Fehlerrate der Übertragung, kontrollieren und den Schlüssel, im Falle eines Angriffs, verwerfen. Dabei wird die Sicherheit nicht durch Annahmen über die Fähigkeiten eines potentiellen Angreifers, sondern auf Basis quantenmechanischer Gesetze gewährleistet. Zusammen mit der Idee des *one-time-pads* bietet sich so die Möglichkeit, *unbedingt* sicher zu kommunizieren.

Quantenkryptographische Protokolle senden einen Schlüssel in den meisten Fällen nicht direkt. Vielmehr *entsteht* dieser im Rahmen der QKD-Übertragung, weshalb auch der Begriff „quantenmechanische Schlüssel*erzeugung*“ berechtigt ist. Zufällige Prozesse an beiden Enden des Quantenkanals, zusammen mit einer Auswahl, die die Kommunikationspartner öffentlich abstimmen, erzeugen die finalen Schlüsseldaten. Aus der Diskussion des Auswahlprozesses lassen sich keine Informationen über den Schlüssel gewinnen.

Die im letzten Kapitel angesprochene Authentifizierung hingegen muss auch in der QKD klassisch bewerkstelligt werden. Um einen *Man-in-the-middle*-Angriff ausschließen zu können, müssen Sender und Empfänger schon *vor* Beginn der quantenkryptographischen Übertragung einen geheimen Schlüssel teilen, mit dem sie sich und die Information, die über den klassischen Kanal ausgetauscht wird, authentifizieren können. Diese Schlüsseldaten bezeichnet man als *pre-shared secrets* also zuvor verteilte Geheimnisse. In diesem Sinne spricht man deshalb auch von *quantum key growing* (QKG), da über einen Quantenkanal die Menge an Schlüssel vermehrt werden kann, die die Kommunikationspartner teilen.

Die quantenmechanischen Grundlagen der QKD sind überschaubar und sollen im Folgenden kurz erläutert werden. Weitere Themen dieses Kapitels sind dann unter anderem das QKD-Protokoll von Bennett und Brassard, das auch Grundlage für das Experiment im Rahmen dieser Arbeit ist, sowie dessen Erweiterung um Decoy-Zustände, die durch die Implementierung erforderlich wird. Eine umfassender Überblick über die QKD findet sich in [31].

3.1 Quantenmechanische Grundlagen

Die kleinste Speichereinheit klassischer Informationsverarbeitung ist ein Bit. Es kann gerade die Datenmenge entsprechend einer ja/nein-Entscheidung aufnehmen, im Computer beschrieben mit 0 und 1, z.B. mit zwei verschiedenen Spannungen. Der große Schritt zur Quanteninformation liegt im Übergang zu Qubits (*quantum bits*). Diese können in Form eines beliebigen Quanten-Systems, bestehend aus zwei orthogonalen Zuständen, realisiert werden. Die Beschreibung erfolgt in einem zweidimensionalen, komplexen Hilbertraum. Wählt man eine Basis $\{|0\rangle;|1\rangle\}$ orthogonaler Vektoren, so kann man den Zustand eines Qubits $|\psi\rangle$ durch

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad ;\alpha,\beta \in \mathbb{C} \tag{3.1}$$

ausdrücken. Dabei gilt die Normierungsbedingung $|\alpha|^2 + |\beta|^2 = 1$, was mit den Winkeln φ und ϑ durch die äquivalente Form

$$|\psi\rangle = \cos{}^{\vartheta}\!/_{2}\,|0\rangle + e^{i\varphi}\sin{}^{\vartheta}\!/_{2}\,|1\rangle \tag{3.2}$$

automatisch gegeben ist. Mit dem Vektor $(\cos\varphi\sin\vartheta, \sin\varphi\sin\vartheta, \cos\vartheta)$ lässt sich der Zustand auf einer Kugel mit Radius $r = 1$, der Blochkugel, veranschaulichen.

Im Gegensatz zum klassischen Bit kann ein Qubit alle Überlagerungen der beiden Basisvektoren einnehmen, was sich die Quanteninformationstechnologie zu Nutzen macht, um die Komplexität von mathematischen Problemen zu reduzieren.

Die Sicherheit der QKD hingegen beruht unter anderem auf der Ununterscheidbarkeit nichtorthogonaler Zustände: Es existiert keine Messung, die deterministisch zwischen zwei Zuständen $|\psi\rangle$ und $|\varphi\rangle$ differenzieren kann, wenn für diese $\langle\psi\,|\,\varphi\rangle \neq 0$ gilt.

Quantenmechanische Messungen werden durch hermitische Operatoren beschrieben, deren Spektrum jeweils alle möglichen Messergebnisse beinhaltet. Nimmt man widersprüchlicher Weise an, eine Messung, beschrieben durch einen Operator A, könne zwei nichtorthogonale Zustände $|\psi\rangle$ und $|\varphi\rangle$ unterscheiden, so muss sie zwei unterschiedliche Eigenwerte $a_\psi \neq a_\varphi$ liefern:

$$A|\psi\rangle = a_\psi|\psi\rangle \tag{3.3a}$$
$$A|\varphi\rangle = a_\varphi|\varphi\rangle \tag{3.3b}$$

Berechnet man aber $\langle\varphi\,|A|\psi\rangle$ und lässt dabei den Operator A einmal nach rechts und einmal nach links ($A^\dagger = A$) wirken, so folgt sofort

$$(a_\psi - a_\varphi)\langle\psi\,|\,\varphi\rangle = 0 \quad . \tag{3.4}$$

Zusammen mit obiger Annahme, dass die Eigenwerte verschieden sind, dass also die Messung eine Unterscheidung der beiden Zustände erlaubt, findet man den Widerspruch $\langle\psi\,|\,\varphi\rangle = 0$. Dies zeigt die Ununterscheidbarkeit nichtorthogonaler Zustände für beliebige Messungen.

Häufig haben Messungen den Charakter von Projektoren in eine Messbasis. Auch in diesem Fall können zwei Zustände, die einen Winkel $< 90\,^\circ$ einschließen, nicht zuverlässig unterschieden werden. Man kann jedoch die Wahrscheinlichkeit angeben, einen Zustand $|\psi\rangle$ wie in (3.1) nach der Projektion in einem der Basiszustände $|0\rangle$ oder $|1\rangle$ zu finden:

$$p(0) = |\langle 0\,|\,\psi\rangle|^2 = |\alpha|^2 \tag{3.5a}$$
$$p(1) = |\langle 1\,|\,\psi\rangle|^2 = |\beta|^2 \tag{3.5b}$$

Ein Spezialfall, der später relevant sein wird, ergibt sich für $\alpha = \beta$. Das Ergebnis einer Projektion in die Basis $\{|0\rangle; |1\rangle\}$ (einer Messung) ist dann völlig unbestimmt:

$$p(0) = \tfrac{1}{2}|\langle 0\,|\,0\rangle|^2 + \tfrac{1}{2}\cancel{|\langle 0\,|\,1\rangle|^2} = \tfrac{1}{2} \tag{3.6a}$$
$$p(1) = \tfrac{1}{2}\cancel{|\langle 1\,|\,0\rangle|^2} + \tfrac{1}{2}|\langle 1\,|\,1\rangle|^2 = \tfrac{1}{2} \tag{3.6b}$$

3.1.1 Kopieren von Quantenzuständen

Ein weiterer wichtiger Unterschied zwischen Bits und Qubits, der gleichzeitig ein entscheidender Aspekt für die Sicherheit der QKD ist, wird durch das *no-cloning*-Theorem beschrieben. Es besagt, dass es unmöglich ist, einen unbekannten, quantenmechanischen Zustand exakt zu kopieren, d.h. zu klonen [32]. Nimmt man im Widerspruch an, es gäbe eine solche Kopiermaschine, die mit einer unitären Transformation U ein Eingangsregister, geladen mit dem beliebigen, unbekannten Zustand $|\psi\rangle$ und einem Ausgangszustand des Kopierers $|\bullet\rangle$, in der Form

$$|\psi\rangle \otimes |\bullet\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \tag{3.7}$$

bearbeitet, so führt dies unweigerlich auf einen Widerspruch: Sei $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$ normiert, so ist

$$\begin{aligned} |\psi\rangle \otimes |\bullet\rangle \quad \xrightarrow{U} \quad & \alpha|\psi_1\rangle \otimes |\psi_1\rangle + \beta|\psi_2\rangle \otimes |\psi_2\rangle \\ & \neq |\psi\rangle \otimes |\psi\rangle \qquad \lightning. \end{aligned} \tag{3.8}$$

Ziel des Kopiervorgangs wäre ein Zustand in der Form

$$|\psi\rangle \otimes |\psi\rangle = \alpha^2|\psi_1\rangle \otimes |\psi_1\rangle + \alpha\beta|\psi_1\rangle \otimes |\psi_2\rangle + \beta\alpha|\psi_2\rangle \otimes |\psi_1\rangle + \beta^2|\psi_2\rangle \otimes |\psi_2\rangle \tag{3.9}$$

gewesen. Auch wenn die perfekte Kopie unmöglich ist, so lassen Wootters und Zurek in [32] die maximale erreichbare Qualität einer fiktiven Quanten-Kopiermaschine doch offen.

Ein Maß für die Wiedergabetreue ist die *fidelity* in der Form

$$\mathcal{F} = \int \mathrm{d}\Omega \, \langle\psi|\rho_{\mathrm{out}}|\psi\rangle \quad . \tag{3.10}$$

Das Integral berechnet den Überlapp aller möglichen Eingangszustände mit den potentiell gemischten Kopiezuständen. Eine obere Grenze für $\mathcal{F}$ wird in [33] von Gisin und Massar formuliert. Sie ist abhängig von der Anzahl der identischen Vorlagen und der Zahl der zusätztlichen Kopien, die erzeugt werden sollen. Für einen einzelnen, unbekannten Zustand kann demnach von einer optimalen Maschine eine Kopie mit einer maximalen *fidelity* von $^5/_6$ hergestellt werden. Will man hingegen einer großen Menge identischer Vorlagen einen Klon hinzufügen, so ist dies nahezu perfekt möglich:

$$\mathcal{F}_{1,2} \quad = \quad {}^5/_6 \tag{3.11a}$$

$$\mathcal{F}_{n,n+1} \quad \xrightarrow{n\to\infty} \quad 1 \tag{3.11b}$$

Verwendet man einzelne Quanten als Träger der Information, so ist die Qualität von Kopien, also der Informationsgewinn eines Abhörers minimal. Zusätzlich ist die Wahrscheinlichkeit, dass ein Angreifer durch den Kopiervorgang einen Fehler in der Übertragung verursacht, maximal. Der Anteil der Bits, die von einem QKD-System mit jeweils mehr als einem Quant übetragen wurden, muss deshalb möglichst klein, vor allem aber bekannt sein, damit ein sicherer Schlüssel extrahiert werden kann.

3.1.2 Implementierung von Qubits

Wie schon angedeutet, bietet sich bei der Realisierung eines Qubits prinzipiell jedes physikalische Zwei-Zustands-System an, mit jeweils spezifischen Vor- und Nachteilen. Der experimentelle Quantencomputer aus [2] verwendet die zwei Energieniveaus, die der Ausrichtung eins Kernspins entsprechen und nutzt dabei unter anderem die Fähigkeit von Atomen (hier im Molekül) zu kontrollierter Wechselwirkung. In der QKD hingegen ist die Transportierbarkeit der Qubits wichtig, weshalb sich Photonen als Informationsträger anbieten. Allerdings können derzeit solche Qubits kaum gespeichert oder untereinander zur Wechselwirkung gebracht werden.

In dieser Arbeit werden die Qubits durch Photonen realisiert, da die Transportierbarkeit im Vordergrund steht. Der zweidimensionale Hilbertraum wird hier durch orthogonale Polarisationen der Photonen aufgespannt. Es existieren drei konjugierte Basen, entsprechend den Eigenbasen der Pauli Matrizen σ_x, σ_y und σ_z:

$$\begin{array}{lcl} \sigma_z: & \{H;V\} & \text{horizontal/vertikal polarisiert} \\ \sigma_x: & \{+45°;-45°\} & \text{diagonal polarisiert} \\ \sigma_y: & \{R;L\} & \text{rechts/links zirkular polarisiert} \end{array} \tag{3.12}$$

3.1.3 Verschränkung in der Quantenmechanik

Verschränkung ist ein rein quantenmechanisches Phänomen und zugleich einer der entscheidenden Prüfsteine, auf den sich Kritiker der Quantenmechanik in der Vergangenheit berufen haben. Der Zustand eines zusammengesetzten Systems wird – im Gegensatz zu *separierbar* – als *verschränkt* bezeichnet, wenn er nicht durch ein Tensorprodukt bestehend aus Zuständen der Subsysteme beschrieben werden kann. Für zwei auf diese Weise verschränkte Teilchen folgert die Quantenmechanik korrelierte Eigenschaften, selbst wenn sie räumlich getrennt sind.

Aus dem theoretisch erwarteten Verhalten solcher verschränkter Teilchen konstruierten Einstein, Podolsky, und Rosen 1935 ein Paradoxon, das die Interpretation und die Vollständigkeit der Quantenmechanik selbst in Frage stellte – heute bekannt als das EPR-Paradoxon [34]. In der Modifikation durch Bohm [35], der auch ein vereinfachtes Experiment zur Verifikation der Verschränkungseffekte vorschlug [36], stellt sich die von Einstein et al. beschriebene Problematik wie folgt dar:

Zwei Teilchen A und B werden von einer so genannten EPR-Quelle verschränkt emittiert und jeweils an verschiedene Orte versandt. Bei verschwindendem Gesamtspin befinden sich A und B auf Grund der Drehimpulserhaltung in dem Singulett-Zustand

$$|\psi\rangle = {}^1\!/\!_{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right) \quad , \tag{3.13}$$

wobei die Pfeile den Spin in z.B. der z-Richtung angeben. Für beide Teilchen wird dann in gleichen Basen der Spin bestimmt. Während jede der Messungen mit der Wahrscheinlichkeit $p = {}^1\!/\!_2$ $|\uparrow\rangle$ wie $|\downarrow\rangle$ liefert, legt das erste Messergebnis den

Zustand des jeweils anderen Teilchens instantan fest: Abhängig vom ersten Ergebnis kollabiert der Zustand $|\psi\rangle$ (bzw. die Wellenfunktion) entweder in $|\psi'\rangle = |\uparrow\rangle_A|\downarrow\rangle_B$ oder $|\psi'\rangle = |\downarrow\rangle_A|\uparrow\rangle_B$, was jeweils Produktzustände mit festgelegtem Spin für beide Teilchen sind. Es besteht also keine Verschränkung mehr und die Ergebnisse für die beiden Teilchen sind perfekt antikorreliert.

Gerade die sofortige Wirkung der Messung an einem Teilchen auf den Zustand des anderen, schien 1935 Unvollständigkeiten der Quantenmechanik zu offenbaren. Die Vermutungen gingen deshalb in Richtung der Existenz von Variablen, die ein deterministisches Verhalten beschreiben, auch wenn sie selbst der quantenmechanischen Beschreibung verborgen sind. Fast 30 Jahre später konnte Bell in seiner Arbeit [37] eine auch experimentell zugängliche Möglichkeit aufzeigen, wie die Frage der Existenz solcher verborgenen Variablen zu klären wäre. Die Quantenmechanik widerspricht der von ihm aufgestellten Bellschen Ungleichung, die für eine realistische, lokale Theorie *mit* verborgenen Variablen gilt. Bis heute konnten verschiedenste Experimente die Bellsche Ungleichung mit großer experimenteller Sicherheit verletzen, was die Existenz von Variablen, durch die sich das Verhalten quantenmechanischer Teilchen deterministisch beschreiben ließe, verneint. Im Abschnitt 3.3 wird ein Protokoll für QKD beschrieben, dessen Sicherheit durch die Prüfung der Bellschen Ungleichung, z.B. in der Form vorgeschlagen von Clauser et al., gewährleistet werden kann.

3.2 QKD nach BB84 und Sicherheitsaspekte

Die Kommunikation mit Qubits allein schafft noch keinen sicheren Schlüsselaustausch. Dies kann erst mit einem übergeordneten Protokoll bewerkstelligt werden. Der Vorschlag für das erste QKD-Verfahren kommt von Bennett und Brassard. 1984 beschrieben sie in ihrer Arbeit [30] ein Protokoll, das mit Qubits in zwei konjugierten Basen arbeitet und heute mit ihren Initialen als BB84 bezeichnet wird. Bereits 1989 konnten sie selbst den, wie sie es nannten, „Beginn einer neuen Ära der Quantenkryptographie“ mit einer experimentellen Verwirklichung einleiten [39]. Andere Protokolle folgten bald, das genannte ist aber wohl das am weitesten verbreitete und auch Grundlage des QKD-Systems dieser Arbeit.

BB84 Protokoll

Für die sichere Schlüsselübertragung kombiniert das BB84 Protokoll zwei quantenmechanische Effekte: Zum einen die Ununterscheidbarkeit zweier orthogonaler Zustände in einer dazu diagonalen Basis (siehe Gl. (3.6)) und zum anderen das *no-cloning* Theorem aus 3.1.1. Anstatt die Information immer in der selben Basis auf die Qubits zu modulieren, also etwa ein klassisches Bit 0 mit horizontaler ($|H\rangle$) und ein Bit 1 mit vertikaler Polarisation ($|V\rangle$) zu codieren, wechselt der Sender laufend die Polarisationsbasis. So wird für jedes Bit einzeln und zufällig entschieden ob $\{|H\rangle; |V\rangle\}$ oder die um 45 ° gedrehte Basis $\{|+45\rangle; |-45\rangle\}$ zu verwenden ist.

Tabelle 3.1: Codierung klassischer Bits in Polarisation für die Verwendung zwei verschiedener Basen.

Basis	klassischer Bitwert	Winkel der Polarisation
$\{\|H\rangle;\|V\rangle\}$	0	0°
	1	90°
$\{\|+45\rangle;\|-45\rangle\}$	0	45°
	1	−45°

Letztere besteht aus den beiden diagonalen Polarisationen. Tatsächlich wird also eine Folge von Photonen gesendet, die in vollkommen zufälliger Weise je eine der Polarisationen $|H\rangle, |V\rangle, |+45\rangle$, und $|-45\rangle$ tragen. Sender und Empfänger müssen sich entsprechend auf eine Codierung wie z.B. in Tabelle 3.1 einigen. Mit dieser Codierung wird es ohne Kenntnis über die jeweilige Basis unmöglich, deterministisch zu entscheiden, ob ein abgefangenes Photon eine 0 oder eine 1 darstellen soll. Da aber auch der Empfänger die Information über die Basis zunächst nicht hat, kann auch er seine Messbasis nur zufällig wählen und wird so in der Hälfte der Fälle ein nicht determiniertes Ergebnis erhalten. Durch anschließende klassische Kommunikation der verwendeten Basen kann er jedoch zusammen mit dem Sender diese Fälle aussortieren. Übrig bleibt im Idealfall ein identischer Schlüssel auf beiden Seiten.

Der Ablauf des Protokolls zur quantenmechanischen Schlüsselübertragung zwischen Alice und Bob (von Sender „A“ zum Empfänger „B“) nach BB84 sieht also wie folgt aus:

1. Alice wählt zufällig zwei Bits: eines als potentielles Schlüsselbit, ein weiteres, um die zu verwendende Basis zu entscheiden und notiert diese zusammen mit einer laufenden Nummer.

2. Sie präpariert die Polarisation genau eines Photons gemäß den beiden Zufallsbits und Tabelle 3.1 und versendet es über den Quantenkanal an Bob.

3. Dieser wählt zuvor, ebenfalls mit einem zufällig erzeugten Bit, die Basis zur Polarisationsmessung des empfangenen Photons. Er misst das Qubit und notiert das Ergebnis zusammen mit der verwendeten Basis und einer laufenden Nummer.

4. Die beiden wiederholen die Schritte 1–3 um weitere potentielle Schlüsselbits auszutauschen.

5. Nach Abschluss der Übertragung teilt Bob Alice öffentlich, also über einen klassischen Kanal, die Indizes der Photonen mit, die er nicht detektieren konnte, Alice streicht diese von ihrer Liste.

6. Weiter kommunizieren Alice und Bob die Basen, die für jedes Qubit beim Senden sowie anschließend beim Empfangen und Messen, verwendet wurden. Geheim bleibt aber natürlich der Bitwert bzw. das Mess*ergebnis*. In den Fällen, in denen die beiden zufällig die gleiche Basis gewählt haben, ist die Polarisationsanalyse von Bob determiniert und und sie behalten die entsprechenden Bits, alle anderen verwerfen sie. Dieser Prozess wird als Sifting bezeichnet (*von engl.: to sift*, aussieben), an dessen Ende steht im Idealfall eine identische Bitfolge auf beiden Seiten, tatsächlich enthält diese aber stets einen Anteil fehlerhafter Bits. Die weitere Vorgehensweise weicht heute vom Originalprotokoll in [30] meist ab:

7. Um die Unterschiede der Schlüssel bei Alice und Bob, d.h. die Fehler, zu beseitigen, wenden die beiden einen klassischen Algorithmus zur Fehlerkorrektur an. Dieser liefert auch die Häufigkeit der Fehler – die Qubit-Fehlerrate (*quantum bit error rate*, QBER).

8. Um die Sicherheit des Schlüssels zu gewährleisten, wird schließlich ein Verfahren angewandt, das als *privacy amplification* in 3.6 beschrieben werden wird. Dies erlaubt, durch Reduktion der Anzahl übertragener Bits in Abhängigkeit der QBER und ggf. weiterer messbarer Parameter, sicheren Schlüssel zu destillieren. Im Falle eines Angriffs kann die verbleibende Schlüsselrate allerdings bis auf Null sinken.

Integritätsprüfung nach der Übertragung

Die QKD bietet die Möglichkeit, *nach* dem Schlüsselaustausch die Integrität zu prüfen. Die Entdeckung eines Angreifers (üblicherweise „Eve“ genannt) ist auf Grund seines Eingriffs in den Quantenkanal möglich. Im Gegensatz zu klassischen Informationsträgern können Qubits nicht störungsfrei gemessen werden und auch ein vollständiges Kopieren ist unmöglich.

Im einfachsten Fall arbeitet Eve mit einer *intercept-resend*-Strategie (*deutsch: abfangen und weitersenden*) und entscheidet sich ebenfalls für eine der beiden Basen $\{|H\rangle;|V\rangle\}$ und $\{|+45\rangle;|-45\rangle\}$. Sie unterbricht also den Kanal, indem sie eine Messung an den Photonen durchführt und sendet anschließend, gemäß ihrem Ergebnis, ein neu präpariertes Photon weiter zu Bob. Wie schon in 3.1 gezeigt, ist das Messergebnis von Eve aber nicht verlässlich, da sie nicht weiß, welche Basis von Alice benutzt wurde. Wenn sie tatsächlich die falsche Basis gewählt hat, so besteht auch immer noch die Möglichkeit, dass Bob, dessen Messung dann ebenfalls nicht determiniert ist, zufällig die von Alice gesendete Polarisation beobachtet. Es können also für jedes Photon die, in Abbildung 3.1 aufgeführten Szenarien stattfinden. Nur in einem Fall, mit der Wahrscheinlichkeit $p = 0{,}25$, verrät sich Eve durch das falsche Messergebnis bei Bob. Durchschnittlich hätte Eve über ein

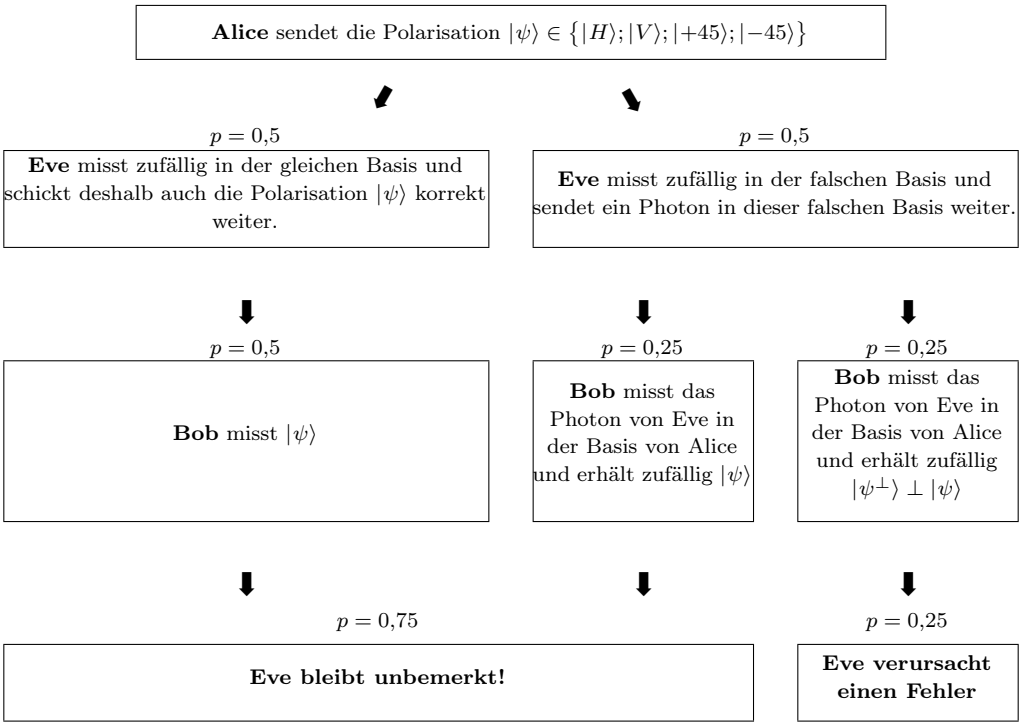


Abb. 3.1: Szenarien und zugehörige Wahrscheinlichkeiten p des *intercept-resend* Angriffs. Betrachtet werden nur Fälle in denen Alice und Bob die gleiche Basis gewählt hatten.

Qubit 0,19 Bit (mit der gleichen Strategie bei einer Messung in der Breidbart Basis[1] sogar 0,40 Bit) Information gewonnen [40]. Die QBER ist mit 25 % aber so hoch, dass Alice und Bob den Schlüssel sofort als kompromittiert erkennen können (bzw. müssen) und ihn verwerfen. Durch die öffentliche Kommunikation von Alice und Bob während des Siftings und anschließend während der Fehlerkorrektur, erhöht sich die Informationsmenge noch, die Eve über (pro Qubit) hat [40]. Durch die Trennung von Schlüssel- und Nachrichtenübertragung werden auch im Fall eines Angriffs keine geheimen Inhalte öffentlich.

Eine solch hohe Fehlerrate kann Eve jedoch vermeiden. Nimmt man an, sie befindet sich in Besitz einer optimalen Quanten-Kopiermaschine, wie sie in 3.1.1 beschrieben ist, und hat darüber hinaus einen großen Speicher für Qubits der die Photonen in ihrem Polarisationszustand erhält – beides Geräte, deren Entwicklung alles andere als absehbar ist – so kann Eve einen mächtigeren Angriff versuchen, den man als *quantum cloning attack* bezeichnet. Die Verwendung eines Quantenspeichers erlaubt Eve, mit ihrer Messung zu warten, bis sie aus der öffentlichen Kommunikation während dem Sifting die zu verwendende Basis erfahren hat. Auch die Maschine von

[1] Die Breidbart Basis erhält man durch eine Drehung um 22,5 ° aus der $\{|H\rangle; |V\rangle\}$ Basis, sie liegt also genau zwischen den Basen die Alice und Bob verwenden.

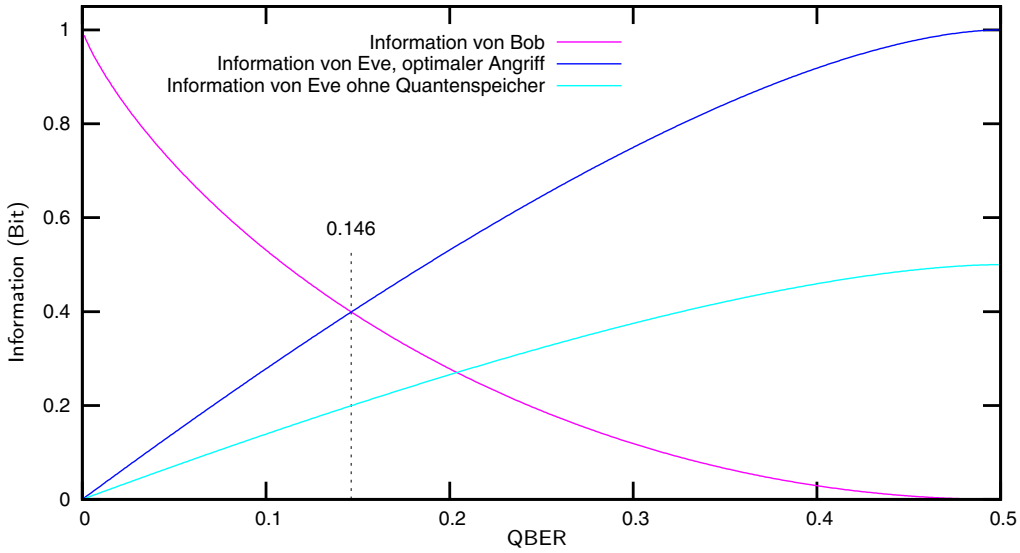


Abb. 3.2: Information, die Bob bzw. Eve mit Alice über ein Bit teilt. Bei einem optimalen Angriff mit Quantenspeicher steigt die Information von Eve bis auf 1 Bit an, ohne Quantenspeicher maximal bis auf 0,5 Bit

Eve kann aber nicht das theoretische Maximum von $\mathcal{F} \approx 0{,}833$ für die Qualität der Kopien überwinden, das durch quantenmechanische Gesetze und nicht durch Annahmen an ihre Fähigkeiten bestimmt ist. Man erwartet in einem solchen Szenario also eine QBER von $1 - \mathcal{F} \approx 16{,}7\,\%$ was immer noch in starkem Kontrast zu Fehlerraten von wenigen Prozent in einem realistischen Experiment steht.

Die QBER, die Alice und Bob beobachten, erhöht sich, je mehr Information Eve über ein Qubit abhört. Der Zusammenhang ist in Abbildung 3.2 für verschiedene Attacken dargestellt. Zum einen, für einen optimalen *individuellen* Angriff, bei dem Eve wie oben ein Quantenspeicher zur Verfügung steht [41]. Zum anderen, für einen optimalen individuellen Angriff, bei dem Eve die Qubits sofort misst und keinen Quantenspeicher verwendet [42], was zum heutigen Zeitpunkt realistischer erscheint.

„Individuell“ bezieht sich hier auf die Messweise von Eve. Bei individuellen Angriffen, betrachtet sie alle abgefangenen Qubits einzeln. Darüber hinaus gibt es kollektive und kohärente Attacken [31, 43], bei denen Eve Messungen gleichzeitig an allen Photonen durchführen kann. Ihr Informationsgewinn ist bei gleicher QBER so noch etwas höher. Hier sollen jedoch nur individuelle Angriffe betrachtet werden.

Unter obiger Annahme erkennt man also eine Grenze bei einer QBER von 14,6 %, jenseits derer Eve mehr Information mit Alice teilt als Bob. Beobachten die rechtmäßigen Kommunikationspartner eine höhere QBER, so ist es nicht mehr möglich, sichere QKD zu betreiben und der Schlüssel muss verworfen werden. Liegt die QBER unter diesem Wert, kann durch Fehlerkorrektur und *privacy amplification* ein sicherer Schlüssel aus den übertragenen Bits extrahiert werden.

3.3 Weitere Protokolle für QKD

Schon bald nach dem Vorschlag für BB84 wurden weitere Protokolle entwickelt. So z.B. das 1992 von Bennett vorgeschlagene B92 Verfahren, das mit nur zwei, nichtorthogonalen, Zuständen auskommt. Andere Protokolle verwenden verschränkte Paare von quantenmechanischen Teilchen, ein erster Vorschlag stammt von Ekert (EKERT91-Protokoll). QKD unter Verwendung solcher Paare ist prinzipiell vergleichbar zu Verfahren, die ohne Verschränkung arbeiten, da die Messung eines Konstituenten aus dem Paar an die Stelle der Präparation eines zufälligen Zustands durch Alice tritt [45].

3.3.1 B92

Dieses Verfahren [44] benötigt zwei nichtorthogonale Zustände, die von Alice in zufälliger Folge gesendet werden. Nennt man diese $|u\rangle$ und $|v\rangle$, so müssen die Photonen bei Bob einer Messung bestehend aus den Projektoren auf die orthogonalen Zustände

$$P_v = 1 - |u\rangle\langle u|\,, \tag{3.14a}$$

$$P_u = 1 - |v\rangle\langle v| \tag{3.14b}$$

$$\text{sowie} \quad P_? = 1 - P_u - P_v \tag{3.14c}$$

zugeführt werden[2]. Ein positives Ergebnis von P_u schließt dabei aus, dass Alice $|v\rangle$ gesendet hat und umgekehrt. Bei einem Klick im Detektor für $P_?$ lässt sich keine Aussage über den gesendeten Zustand treffen.

Wie beim BB84-Protokoll muss auch hier ein Sifting erfolgen: Bob teilt Alice öffentlich mit, in welchen Fällen das Photon von $P_?$ registriert wurde, wann er den gesendeten Zustand also nicht erkennen konnte. Die beiden vereinbaren, alle diese Qubits zu verwerfen. Übrig sollte ein Anteil von im Mittel $(1 - |\langle u\,|\,v\rangle|^2)/2$ perfekt korrelierter Bits bleiben.

Damit ist jedoch die Sicherheit des Schlüssels noch nicht gegeben. Ein Angreifer könnte jederzeit die gleiche Messung wie Bob durchführen und im Falle eines deterministischen Ergebnisses ein entsprechend codiertes Photon weitersenden. Kann er den Bitwert und damit die Polarisation nicht bestimmen, so blockiert er das jeweilige Qubit ganz. Ohne einen Fehler im Schlüssel von Alice und Bob zu verursachen erhält der Angreifer so volle Information, wobei er jedoch starke Abschwächung verursacht. Im Rahmen der *privacy amplification* kann jedoch, sogar im Fall von beliebigen individuellen Angriffen, ein sicherer Schlüssel gewonnen werden, was die unbedingt sichere Schlüsselverteilung mittels B92 erlaubt [47]. Durch Variation des Winkels

[2] P_u, P_v und $P_?$ bilden mit geeigneten Normierungsfaktoren ein so genanntes POVM (*positive operator valued measure*), die allgemeinste Beschreibung einer quantenmechanischen Messung (vgl. [46]).

zwischen den Zuständen, die Alice sendet, kann die verbleibende sichere Schlüsselrate für eine spezielle Abschwächung des Quantenkanals maximiert werden. Trotzdem fällt diese mit zunehmender Dämpfung bzw. mit der Entfernung schnell ab [48].

3.3.2 EKERT91

Auch wenn Bennett et al. [45] die Ähnlichkeiten von QKD ohne verschränkte Qubits beschreiben, so bieten Protokolle auf Basis von EPR Paaren doch weitere Möglichkeiten und Vorteile. Das Verfahren EKERT91 [10] nutzt nicht direkt die Fehlerrate, um einen Angriff zu entdecken, sondern prüft vielmehr, ob die Qubits bei Alice und Bob immer noch verschränkt sind. Zudem kann eine EPR-Quelle von den Kommunikationspartnern auf ihre Integrität geprüft werden, Alice und Bob müssen ihr also nicht vertrauen, da Manipulationen sich sofort bemerkbar machen würden. Die Quelle muss also nicht vor dem Zugriff eines Angreifers geschützt werden und lässt sich deshalb an beliebigen, günstigen Orten, auch auf einem Satelliten der eventuell kompromittiert werden könnte, ohne Sicherheitseinschränkung einsetzen.

Nach dem Vorschlag von Ekert erhalten Alice und Bob je ein Teilchen aus jedem Paar, emittiert als Singlett-Zustand aus einer EPR-Quelle. Ekert beschreibt sein Protokoll für verschränkte Spin-$^1/_2$-Teilchen[3] im gleichen Zustand wie schon oben:

$$|\psi\rangle = {}^1/_{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right) \tag{3.15}$$

$|\uparrow\rangle$ steht für ein Teilchen mit positiver Spinkomponente in z-Richtung und für Wert 1 in Einheiten von $\hbar/2$, $|\downarrow\rangle$ umgekehrt für eine negative z-Komponente und -1. Sender und Empfänger – hier verschwimmen die Rollen, da eigentlich beide Empfänger sind – führen nun eine Messung in einer von *drei* Richtungen durch: Alice bestimmt die Spinkomponente in einer der Richtungen $0\,°(\boldsymbol{a}_1)$, $45\,°(\boldsymbol{a}_2)$ oder $90\,°(\boldsymbol{a}_3)$ als Vielfaches von $\hbar/2$, Bob wählt für seine Analyse aus $45\,°(\boldsymbol{b}_1)$, $90\,°(\boldsymbol{b}_2)$ und $135\,°(\boldsymbol{b}_3)$, jeweils aber senkrecht zum Weg der Teilchen. Die Entscheidung erfolgt zufällig sowie unabhängig, und Alice und Bob erhalten das Messergebnis 1 oder -1 in der jeweils ausgewählten Richtung. Nach der Übertragung kommunizieren die beiden die Information über die gewählte Ausrichtung und behalten nur die Bits (Messerwert 1 steht für Bitwert 1, -1 für 0) für den Schüssel, bei welchen die Messrichtungen übereinstimmen (Sifting). Die Prüfung auf einen Angreifer erfolgt nun mit den restlichen Bits, bei denen das Ergebnis nicht determiniert war: Die obigen Winkel sind so gewählt, dass sich aus den Messergebnissen der beiden Spinmessungen die Größen in der CHSH Ungleichung bestimmen lassen. CHSH steht für die Initialen der Autoren Clauser, Horne, Shimony, und Holt, die in ihrer Arbeit [38] eine spezielle Form der Bellschen Ungleichung formulieren:

$$S = \left|E(\boldsymbol{a}_1, \boldsymbol{b}_3) - E(\boldsymbol{a}_3, \boldsymbol{b}_1) - E(\boldsymbol{a}_1, \boldsymbol{b}_1) - E(\boldsymbol{a}_3, \boldsymbol{b}_3)\right| \leq 2 \tag{3.16}$$

[3] Das Protokoll kann auch leicht mit einer anderen Implementation der Qubits realisiert werden, z.B. polarisationsverschränkten Photonen

Die Größen $E(\boldsymbol{a}_i, \boldsymbol{b}_i)$ stehen für die Korrelationskoeffitienten[4] der Messungen, wenn Alice in Richtung $\boldsymbol{a}_i$ und Bob in Richtung $\boldsymbol{b}_i$ gemessen hat. Die Quantenmechanik führt auf den Zusammenhang

$$E(\boldsymbol{a}_i, \boldsymbol{b}_i) = -\boldsymbol{a}_i \cdot \boldsymbol{b}_i \quad , \tag{3.17}$$

für verschränkte Teilchen bedeutet das mit den verwendeten Winkeln aber

$$S = 2\sqrt{2} \quad . \tag{3.18}$$

Hier manifestiert sich die schon in 3.1.3 angesprochene Verletzung der Bellschen Ungleichung.

Alice und Bob können also prüfen, ob und wie stark die Ungleichung (3.16) verletzt wurde und erhalten so eine Aussage über die verbliebene Qualität der Verschränkung. Diese wird durch einen Angriff, wenn etwa Eve versucht, weitere Teilchen mit den Qubits zu verschränken und zu speichern, stets entsprechend dem Informationsgewinn des Abhörers verringert werden und eignet sich so als Indikator für einen Angriff.

3.4 Angriffe über Seitenkanäle

Die Sicherheit der obigen quantenkryptographischen Protokolle ist jeweils bewiesen, basierend auf quantenmechanischen Gesetzen [3, 4]. Die sichere Implementierung ist jedoch nicht gewährleistet. Der kritische Moment, z.B. im BB84-Protokoll, ist oft der 2. Punkt (S. 19): Alice muss genau *ein* Photon in einer bestimmten Polarisation präparieren.

Abhängig vom elektronischen und mechanischen Aufbau können bei diesem Vorgang auch weitere Freiheitsgrade moduliert werden. Neben der Polarisation sind jedem Qubit/ Photon auch noch Spektrum, Emissionszeitpunkt sowie -ort und -richtung zugeordnet.

Diese, und je nach Implementierung der Qubits auch weitere Freiheitsgrade, nennt man Seitenkanäle. Besteht ein prinzipieller Zusammenhang zwischen einem oder sogar mehreren von ihnen mit der Polarisation oder der Basis, das heißt also letztlich mit dem gesendeten Bitwert, so kompromittiert das die Übertragung doppelt: Zum einen kann der Angreifer nun durch eine Messung ganz oder teilweise in Kenntnis des gesendeten Bitwerts gelangen, zum anderen kann er auch der Entdeckung entgehen, da eine Messung in den Seitenkanälen die Polarisationseigenschaften eines Photons nicht beeinflussen muss. Ist die Ununterscheidbarkeit der Qubits in den Seitenkanälen aufgebrochen, versagen die bisherigen Sicherheitsbeweise. Natürlich

[4] $E(\boldsymbol{a}_i, \boldsymbol{b}_i) = P_{1;1}(\boldsymbol{a}_i, \boldsymbol{b}_i) + P_{-1;-1}(\boldsymbol{a}_i, \boldsymbol{b}_i) - P_{1;-1}(\boldsymbol{a}_i, \boldsymbol{b}_i) - P_{-1;1}(\boldsymbol{a}_i, \boldsymbol{b}_i)$, zugänglich über die relativen Häufigkeiten, 1 und 1 oder 1 und -1 etc. beobachtet, die beim Sifting bestimmt werden können.

werden sich Seitenkanäle durch reale Systeme nie vollständig vermeiden lassen, sie müssen jedoch quantifiziert werden. Die Informationslecks können dann, soweit sie nicht zu gravierend sind, durch anschließende *privacy amplification* ausgeglichen werden, bei der die Schlüssellänge zu Gunsten der Sicherheit reduziert wird.

Die sorgfältige Behandlung von Seitenkanälen eines QKD-Systems ist nicht zuletzt relevant, da es neben den theoretischen Vorschlägen auch schon experimentelle Demonstrationen gibt, die auf diesem Weg, am Protokoll vorbei, an Schlüsseldaten gelangen: Ein Angriff basierend auf zeitlichen Informationen wird in [49] vorgestellt[5] und Zhao et al. zeigen in [50] die Verwundbarkeit eines kommerziell erhältlichen QKD-Systems[6].

3.4.1 QKD mit abgeschwächten Laserpulsen

Die Substitution der geforderten Einzelphotonenquelle durch abgeschwächte Laserpulse, wie auch im hier beschriebenen System, bringt einen weiteren Seitenkanal mit sich, der direkt die Vorgaben des Protokolls verletzt. Die Zahl der Photonen in einem Puls unterliegt einer Poissonverteilung mit Erwartungswert μ. Die Wahrscheinlichkeit, in einem Puls n Photonen vorzufinden, kann man also mit

$$p(n) = \frac{\mu^n}{n!} e^{-\mu} \tag{3.19}$$

angeben. Das bedeutet, dass bei einer mittleren Photonenzahl von $\mu = 0{,}1$ in 905 von 1000 Pulsen gar kein Photon zu erwarten ist. Dies muss man in Kauf nehmen, damit die Zahl der Multiphotonpulse möglichst gering ausfällt. In diesem Beispiel präpariert Alice ungewollt in fünf der 1000 Pulse mindestens zwei Photonen. Die Sicherheit der Übertragung erfordert also, trotz der negativen Auswirkung auf die Schlüsselrate, solch niedrige Werte von μ, da jedes zusätzliche Photon ein einem Puls von einem Angreifer unbemerkt abgezweigt werden kann. Im Folgenden wird das Angriffsszenario auf diese Mehrphotonpulse beschrieben.

3.4.2 Angriff gegen Multiphotonpulse: Photon Number Splitting

Ist dem Angreifer bekannt, dass ein QKD-System mit abgeschwächten Laserpulsen an Stelle echter Einzelphotonen arbeitet, so kann er eine spezielle Strategie, vorgeschlagen von Huttner et al. [51] und bekannt als *photon number splitting* (PNS) [52], verfolgen. Man nimmt an, Eve ist in der Lage, die Zahl n der Photonen in einem Puls, ohne Störung der Polarisation zu ermitteln. Das Ergebnis bestimmt dann ihr weiteres Vorgehen, zum Beispiel:

[5] Dieser Angriff bezieht sich zunächst auf Detektionszeitpunkte des Empfängers, die öffentlich werden. Dies ist jedoch bei dem hier beschriebenden System nicht der Fall. Der Angriff ist aber analog zu einer Attacke auf Grund verschiedener Emissionszeitpunkte der Photonen bei Alice, wenn der Empfänger nur eine binäre Entscheidung trifft.

[6] ID-500 der Firma idQuantique

$n = 0$: kein weiterer Eingriff

$n = 1$: Photon wird geblockt

$n > 1$: ein Photon wird in einen Quantenspeicher abgezweigt, um es zu messen, wenn die Basis bekannt ist, alle anderen $n - 1$ werden, eventuell sogar ohne weitere Verluste, an den Empfänger weitergeleitet.[7]

Alles, was Alice und Bob beobachten, ist eine starke Abschwächung im Quantenkanal (alle Einzelphotonpulse werden geblockt), die Fehlerrate bleibt gleich. In obigem Beispiel, für einen idealen Quantenkanal ohne Verluste und Detektoren bei Bob mit Quanteneffizienz 1, ändert sich die Transmission T_{AB}, die Alice und Bob bei mittlerer Photonenzahl μ ohne Angreifer beobachten, um einen Faktor von

$$\frac{T_{\mathrm{PNS}}}{T_{\mathrm{AB}}} = \frac{1 - (1 + \mu)e^{-\mu}}{1 - e^{-\mu}} = \frac{0{,}005}{0{,}095} = 0{,}0526 \quad . \tag{3.20}$$

Dies entspricht einer Abschwächung von etwa 13 dB, wobei Eve vollständige Information über den Schlüssel gewinnt. Der Zähler im Ausdruck (3.20) steht für den Anteil der Pulse mit mehr als einem Photon, der Nenner für den Anteil nicht leerer Pulse. Die Abschwächung ist entsprechend kleiner, wenn Eve nicht alle Pulse kontrolliert und so nur einen Teil des Schlüssels abhört.

Mit einem realistischen Kanal und echten Detektoren ist die Situation für Alice und Bob noch schlechter, da zunehmend mehr Multiphotonpulse zur Schlüsselverteilung beitragen. Eve kann dann den realistischen durch einen idealen, verlustfreien Quantenkanal ersetzen und die, durch Abfangen der Einzelphotonpulse entstandene Abschwächung teilweise oder sogar ganz kompensieren. Ein Szenario, das zunächst keine Hinweise auf einen Angriff bietet, die Fehlerrate und die Transmission des Kanals bleiben konstant, Eve erhält jedoch vollständige Information, da sie die gespeicherten Qubits nach dem Sifting in der richtigen Basis messen kann [52].

Um die unbedingte Sicherheit der Schlüsselübertragung bei Verwendung abgeschwächter Pulse wieder herzustellen, ist eine Erweiterung des Protokolls notwendig, mit der ein Angreifer, auch bei einem PNS Angriff erkannt wird.

3.5 Protokollerweiterung: Decoy-Zustände

Die Verwendung von Decoy (*deutsch: Köder*) Zuständen bietet einen Ausweg angesichts des PNS Angriffs[8], weil sie einen Abhörer enttarnen können und eine Aussage zulassen, wie viele sichere Schlüsselbits sich aus den Rohdaten durch

[7] Eine vereinfachte Strategie arbeitet nur mit einem Strahlteiler, also ohne Photonenzahl auflösende Messung [53], ist aber auch weit weniger effizient für Eve.

[8] Eine andere Möglichkeit wird z.B. in [54] von Scarani et al. vorgeschlagen: BB84 mit einer modifizierten Siftingstrategie, die Schlüsselrate ist deshalb jedoch um einen Faktor $^1/_2$ kleiner.

privacy amplification (siehe 3.6) trotzdem gewinnen lassen. Um den Freiheitsgrad der Photonenzahl zu sichern kommt hier wiederum die Ununterscheidbarkeit nichtorthogonaler Zustände zum Einsatz: An Stelle stets gleicher Intensität (d.h. mittlerer Photonenzahl) sendet Alice eine zufällige Folge von Pulsen mit z.B. zwei verschiedenen Intensitäten. Es gibt aber keine Messung, die Eve erlauben würde, gesendete Pulse unterschiedlichen mittleren Photonenzahlen zuzuordnen und sie ist somit gezwungen, auf alle Pulse die gleiche Strategie anzuwenden. Eine Strategie, wie oben als PNS beschrieben, wirkt sich jedoch unterschiedlich auf die beiden Mengen von Pulsen einer Intensität aus und kann deshalb enttarnt werden.

Das Decoy-Verfahren ermöglicht so zum einen den sicheren Einsatz von abgeschwächten Laserpulsen, der technologisch wesentlich einfacher zu realisieren ist als echte Einzelphotonquellen, zum anderen wird die maximale Reichweite eines QKD-Systems trotz eines verlustbehafteten Kanals und Detektoren mit begrenzter Effizienz signifikant erhöht [55, 56].

Die Theorie führt dazu zwei Konzepte zusammen: Gottesman, Lo, Lütkenhaus, und Preskill erklären in ihrer Arbeit [57], bekannt als GLLP und basierend auf [55], wieviel sicherer Schlüssel angesichts von Informationsverlusten über Seitenkanäle aus den Rohdaten nach dem Sifting destilliert werden kann. Sie führen den Begriff der *tagged bits* (*deutsch: markierte Bits*) ein – Bits, deren Wert man als dem Angreifer bekannt annehmen muss. Dabei ist der konkrete Seitenkanal, der die Daten preisgibt, hier die Multiphotonpulse, zunächst irrelevant für ihren Formalismus. Lässt sich eine obere Grenze für den Anteil derart kompromittierter Bits angeben, so beantworten GLLP die Frage, wie stark man die Schlüsselrohdaten reduzieren muss, um beliebige Sicherheit zu garantieren. Die Menge der markierten Bits zuverlässig anzugeben, ist jedoch nicht trivial.

Auf der anderen Seite steht die Idee von Hwang [58]: Indem Alice zufällig an Stelle normaler Signalpulse Decoypulse mit höherer mittlerer Photonenzahl $\mu' > \mu$ versendet, schafft sie eine Möglichkeit, Eve zu enttarnen und den, von GLLP benötigten Anteil markierter Bits Δ abzuschätzen.

Eve kann angesichts eines μ-Photon Pulses nicht entscheiden, ob es sich um einen Signal- oder Decoypuls handelt. Die Wahrscheinlichkeit für die erfolgreiche Detektion eines Decoypulses bei Bob wird deshalb im Fall eines PNS Angriffs überproportional höher sein als die, einen Signalpuls zu registrieren, da Decoypulse öfter mehr als ein Photon enthalten und Eve diese Pulse, im Vergleich zu den Signalpulsen, auch öfter weiterleitet. Alice und Bob können während dem Sifting die relativen Häufigkeiten, mit denen Pulse aus der Signal- und der Decoyklasse erfolgreich übertragen wurden, bestimmen. Weicht das Verhältnis der gemessenen Häufigkeiten zu weit vom erwarteten Wert μ'/μ ab, so können Alice und Bob auf einen PNS Angriff schließen und die Schlüsselverteilung abbrechen. In jedem Fall liefert Δ jedoch eine obere Grenze für den Anteil kompromittierter Pulse, also die Zahl der Multiphotonpulse, die in den gesifteten Schlüssel Eingang gefunden haben.

Mit diesem Wissen ist es möglich, durch geeignete Reduktion des Schlüssels trotzdem Sicherheit zu gewährleisten.

Versendet Alice einen Signalpulses mit der mittleren Photonenzahl μ, lässt sich der Zustand im Fockraum ohne den Polarisationsfreiheitsgrad durch die Dichtematrix

$$\rho_\mu = e^{-\mu}|0\rangle\langle 0| + \mu e^{-\mu}|1\rangle\langle 1| + \underbrace{{}^1\!/_c \sum_{n=2}^{\infty} \frac{e^{-\mu}\mu^{-n}}{n!}|n\rangle\langle n|}_{\rho_c} \tag{3.21}$$

beschreiben [59, 60]. Dies spiegelt die Poissonverteilung der Photonen (Gl. (3.19)) wieder, wobei die leeren und die Einzelphotonpulse abgespalten sind und c die geeignete Normierung bezeichnet. Versendet Alice einen Decoypuls, so kann man für diesen ρ' mit $\mu' > \mu$ analog formulieren und ρ_c einsetzen:

$$\rho_{\mu'} = e^{-\mu'}|0\rangle\langle 0| + \mu' e^{-\mu'}|1\rangle\langle 1| + c\frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}}\rho_c + d\rho_d \quad , \tag{3.22}$$

wobei im Folgenden nur verwendet wird, dass ρ_d ein Dichteoperator und $d \geq 0$ ist.

Definiert man wie in [59] die Detektionswahrscheinlichkeit (*yield*) als Wahrscheinlichkeit für einen Detektorklick bei Bob, vorausgesetzt, dass Alice einen Puls gesendet hat (die bedingte Wahrscheinlichkeit) und bezeichnet mit s_c, S_μ und $S_{\mu'}$ die Detektionswahrscheinlichkeiten, resultierend aus ρ_c, ρ_μ und $\rho_{\mu'}$, so kann man den gesuchten Anteil der Multiphotonpulse Δ, die von Alice gesendet und von Bob detektiert werden, in der Form

$$\Delta = c\frac{s_c}{S_\mu} \tag{3.23}$$

schreiben und auch eine Abschätzung in der Form

$$\Delta \leq \frac{\mu^2 e^{-\mu} S_{\mu'}}{\mu'^2 e^{-\mu'} S_\mu} \tag{3.24}$$

finden, bei der die messbaren Detektionswahrscheinlichkeiten (-Häufigkeiten) aus den beiden Klassen der Signal- und Decoypulse auftauchen, nicht jedoch die unbekannten Detektionswahrscheinlichkeit aus Pulsen mit genau n-Photon.

Diese obere Grenze kann noch deutlich verringert werden, insbesondere wenn die Dunkelzählrate mit einbezogen wird [59]. Wichtig ist jedoch, dass die rechtmäßigen Kommunikationspartner durch die Verwendung von Decoy-Zuständen einen messbaren Zugang zu Δ erhalten, dem Parameter, der nach GLLP den Grad der nötigen Reduktion der Rohdaten bestimmt, damit ein sicherer Schlüssel verbleibt.

Der Einsatz von *zwei* Decoy-Pulsintensitäten $\mu' > \mu$ und $\mu_0 = 0$, so genannte Vakuumpulse, neben den Signalpulsen, stellt sich als optimal heraus [56, 61]. So steht die Hintergrundzählrate direkt zur Verfügung und auch bei endlich langen Schlüsselübertragungen können die statistischen Parameter noch genau genug bestimmt werden. Bei größerer Anzahl von verschiedenen Pulsintensitäten weichen die

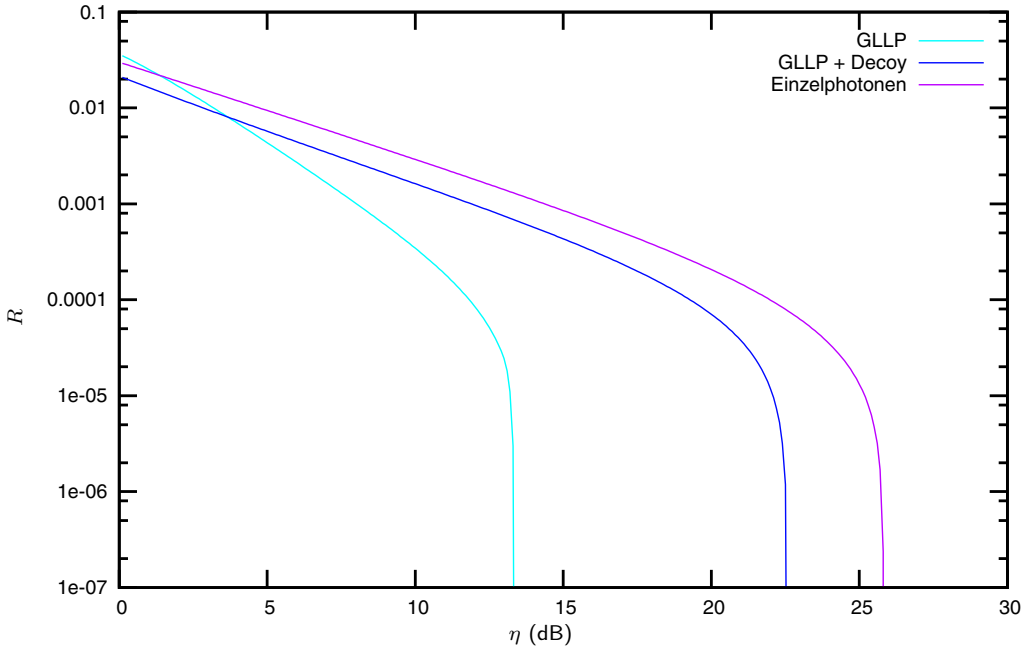


Abb. 3.3: Berechnete Rate sicheren Schlüssels R nach für QKD gemäß BB84 mit abgeschwächten Pulsen (cyan), zusätzlich mit Decoy-Zuständen (blau) und mit echten Einzelphotonen (violett), aufgetragen gegen die Abschwächung im Quantenkanal [59, 62]. Während R bei abgeschwächten Pulsen quadratisch abfällt, kann mit Decoy-Zuständen über weite Bereiche das lineare Verhalten, das auch echte Einzelphotonen zeigen, beobachtet werden. μ und μ' sind in jedem Punkt für maximales R optimiert.

beobachteten Häufigkeitswerte, die in obige Berechnung eingehen, zunehmend von den asymptotischen Wahrscheinlichkeiten ab, da die Stichprobenlänge für die Klassen der einzelnen μ_i kleiner wird.

In Abbildung 3.3 ist die Entwicklung der maximalen Rate sicheren Schlüssels R für steigende Kanalabschwächung η dargestellt. Dabei sind für jedes η die Werte μ und μ' jeweils optimal, im Sinne sicherer Schlüsselrate, gewählt. Hier zeigt sich der große Vorteil der Verwendung von Decoy-Zuständen: Während bei QKD-Systemen, die mit abgeschwächten Pulsen *einer* Intensität arbeiten, die Schlüsselrate mit der Transmission zum Quadrat abfällt, kann mit dem Decoy-Protokoll über weite Strecken ein Verlust erreicht werden, der nur linearer in der Transmission ist. Die maximale Reichweite ist dann der von Systemen, die mit echten Einzelphotonen arbeiten, vergleichbar. Die Ursache liegt im Verhalten von Δ als Funktion von η, dargestellt in Abbildung 3.4. Indem Δ früh konvergiert, ist die maximale Reichweite eines Decoy-unterstützten Systems vor allem durch die QBER begrenzt, die von Dunkelzählereignissen verursacht wird und Ursache des steilen Abfalls von R in Abbildung 3.3 ist.

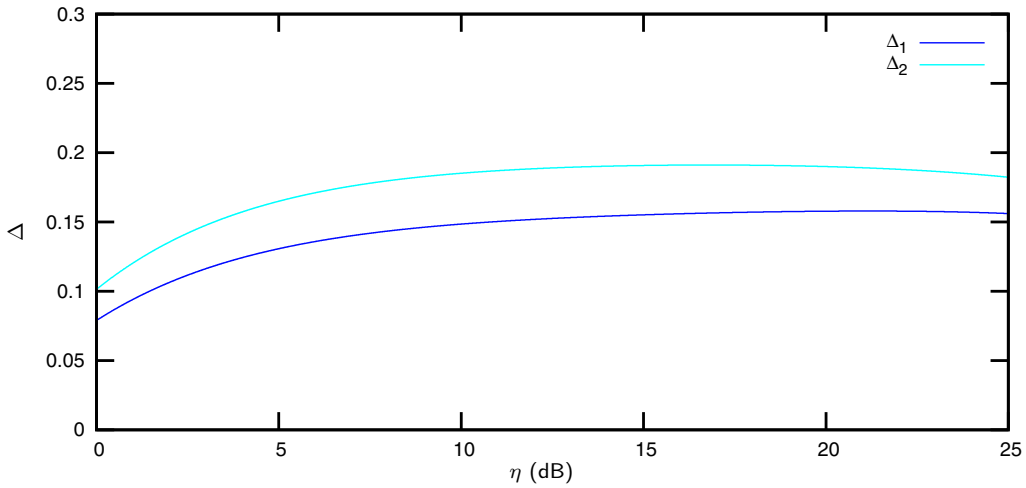


Abb. 3.4: Entwicklung von $\Delta_{1,2}$ für zunehmende Abschwächung des Quantenkanals η für ein QKD-System, das mit abgeschwächten Laserpulsen und Decoy-Zuständen arbeitet. Simuliert für mittlere Photonenzahlen von $\mu = 0{,}15$ und $\mu' = 0{,}2$ pro Puls [59].

3.6 Fehlerkorrektur und privacy amplification

In der Realität wird der Quantenkanal, den Alice und Bob benutzen, nicht perfekt sein. Unvollkommene Justage und Dunkelzählraten in den Detektoren sind zwei Hauptgründe für Rauschen. Trotzdem muss man im Sinne der Sicherheit annehmen, dass ein Angreifer Ursprung von Übertragungsfehlern ist. Zudem kann, wie oben beschrieben, Information über die gesendeten Bits über Seitenkanäle an einen Gegner gelangt sein. Zwei Dinge müssen deshalb im letzten Schritt des Protokolls sichergestellt werden, bevor die ausgetauschte Bitfolge als geheimer Schlüssel verwendet werden kann:

1. Es ist essentiell, dass Alice und Bob am Schluss einen identischen Schlüssel teilen. Sie müssen sich deshalb auf einen Algorithmus zur Fehlerkorrektur einigen.

2. Die beobachtete QBER, die Fehlerkorrektur sowie die Charakterisierung des QKD-Systems müssen dahingehend untersucht werden, wie viel Information ein Angreifer maximal über die potentiellen Schlüsselbits erhalten konnte. Auf dieser Basis muss die Bitfolge reduziert werden um einen sicheren Schlüssel zu erhalten.

Der erste Punkt ist durch klassische Kommunikation und konventionelle Protokolle lösbar. Ein Verfahren dazu ist CASCADE, wie in [63] beschrieben. Shannon zeigt in seiner Arbeit [64], dass Fehlerkorrektur aber nicht möglich ist, ohne eine gewisse Menge an Information aufzudecken und gibt eine untere Grenze für den im Mittel benötigten Anteil in Abhängigkeit von der zu beseitigenden Fehlerrate δ an:

$$H_2(\delta) = -\delta \log_2(\delta) - (1-\delta)\log_2(1-\delta) \tag{3.25}$$

H_2 wird als binäre Entropiefunktion bezeichnet. Die tatsächlich benötigte Informationsmenge ist in der Regel, wie auch bei CASCADE, größer und muss, neben anderen Informationslecks, im zweiten Punkt berücksichtigt werden. Dieser wird als *privacy amplification* (*deutsch: Privatsphären-Verstärkung*) bezeichnet, deren Ziel es ist, einen vollständig geheimen Schlüssel aus den teilweise bekannten Rohdaten zu berechnen.

Als geheim und sicher wird ein Schlüssel bezeichnet, der zum einen mit der gleichen Wahrscheinlichkeit auftritt wie alle anderen möglichen Schlüssel gleicher Länge, zum anderen sollen für einen Angreifer a priori und a posteriori Wahrscheinlichkeit, also die Werte vor und nach der Attacke, für diesen speziellen Schlüssel identisch sein [62].

Tatsächlich kann man diese Vorgaben erfüllen, wenn man die Bitfolge nach dem Sifting mit einer Streuwertfunktion (*engl. hash functions*) ausreichend komprimiert. Die maximale Schlüsselrate R, also die Menge sicheren Schlüssels bezogen auf die Länge nach dem Sifting, die aus dem Rohmaterial destilliert werden kann, geben GLLP in [57] mit dem Ausdruck

$$R = \max\left(\quad (1-\Delta) - f(\delta)H_2(\delta) - (1-\Delta)H_2\left(\frac{\delta}{1-\Delta}\right) \quad , \, 0 \quad \right) \quad , \tag{3.26}$$

an, in den Δ aus dem vorigen Abschnitt mit eingeht. (3.26) verwendet mit $(1-\Delta)$ die Rate nicht markierter Bits als Ausgangspunkt und reduziert diese um die Informationsmenge, die im Rahmen der Fehlerkorrektur öffentlich gemacht werden muss wie in (3.25), wobei $f(\delta)$ die Effektivität des verwendeten Algorithmus beschreibt. Der letzte Term bezeichnet die nötige Schlüsselreduktion, die auf Grund der QBER, die man als von Eve verursacht betrachtet, nötig ist. Dabei geht man davon aus, dass Eve nur auf unmarkierten Bits einen Fehler δ verursacht. Deshalb wird dieser auf die Menge unmarkierter Bits $(1-\Delta)$ skaliert, dafür jedoch, muss aber auch nur auf die unmarkierten Bits *privacy amplification* angewendet werden, daher der Vorfaktor $(1-\Delta)$ im letzten Term.

Die *privacy amplification* wird im nötigen Umfang schließlich mit Streuwertfunktionen durchgeführt, die eine Bitfolge derart komprimieren, dass die Änderung von nur einzelnen Bits in der Eingabe einen gänzlich verschiedenen Funktionswert ergibt[9]. Alice und Bob wählen zufällig aus einer Klasse $\mathcal{G}$ von universellen Streuwertfunktionen die $\{0;1\}^N$ auf $\{0;1\}^n$ $(n < N)$ abbilden, damit Eve zuvor keinen Gewinn aus

[9] Zum Beispiel liefert das Verfahren SHA1 für den ersten Absatz in diesem Abschnitt den Hash-Wert:

`4BEB9 93E3A 0C007 3270D DB66C B0B5F 3F41E 7F0A5`

Ersetzt man den abschließenden Doppelpunkt „:“ durch einen einfachen Punkt „.“ erhält man den Folgenden Hash-Wert:

`4ACE8 C200F F2670 9050B 65280 F753B 6B3A2 CD768`

SHA1 findet breite Anwendung im Rahmen der Protokolle SSL, PGP, SSH etc. bei der Sicherung von Kommunikation über das Internet.

der Kenntnis der speziellen Funktion ziehen kann [65]. Universell bedeutet, dass bei gleichverteilter Auswahl von Funktionen $g \in \mathcal{G}$ die Wahrscheinlichkeit, zwei identische Hashwerte für verschiedene Argumente zu erhalten, maximal 2^{-n} beträgt. Als praktisch im Hinblick auf den Kommunikations- und Rechenaufwand bei der Einigung auf eine Funktion haben sich Töplitz-Matrizen bewährt. Diese erlauben eine Beschreibung durch nur $n + N - 1$ Bits. Der Finale Schlüssel kann dann durch eine Matrixmultiplikation berechnet werden und steht für klassische symmetrische Verfahren zur Verfügung.

4

Aufbau des Senders

In diesem und dem folgenden Kapitel soll der Aufbau des Senders bzw. Empfängers dokumentiert werden. Die Anlage wird dabei im Hinblick auf die zu erwartende QBER charakterisiert. Um *privacy amplification* korrekt durchführen zu können, erfolgt die Messung und Berechnung der möglichen Informationsverluste über Seitenkanäle.

Das QKD-System dieser Arbeit verwendet das BB84 Protokoll mit einer Repetitionsrate von 10 MHz. Die Qubits werden, durch polarisationscodierte, abgeschwächte Laserpulse mit einer Wellenlänge von $\lambda = 850\,\text{nm}$ realisiert. Um einen Angriff durch PNS dennoch erkennen zu können, wird BB84 hier um Decoy-Zustände erweitert.

Der Sender muss Pulse in vier verschiedenen Polarisationen aussenden können, jeweils zwei Paare von orthogonalen Richtungen, 45 ° gegeneinander verdreht (0 ° und 90 ° sowie 45 ° und 135 °). Die Decoy-Erweiterung erfordert darüber hinaus mindestens zwei Intensitäten für jede dieser vier Polarisationszustände, die auch im Betrieb genau kalibrier- und kontrollierbar sein müssen. Der Empfänger hingegen, der im folgenden Kapitel behandelt wird, hat die Aufgabe, die Polarisationszustände, wiederum in zwei Basen, zu analysieren, wobei die Basis zufällig gewählt wird. Dabei müssen die Detektoren in der Lage sein, einzelne Photonen zu registrieren.

Die Übertragung der Photonen erfolgt über einen Quantenkanal frei durch die Luft. Dazu werden Sender und Empfänger jeweils mit Teleskopen ausgestattet, die auf der einen Seite die Photonen auf einen engen Strahl fokussieren, auf der anderen Seite die Empfindlichkeit der Detektoren auf die Verbindungsachse konzentrieren. Dabei liegt die angestrebte Reichweite zwischen 500 m (dies ist die Entfernung der Teststrecke vor Ort) und ca. 2 km.

Da die Anlage im Freien von Dach zu Dach betrieben wird, ist weiterhin ein entsprechend wetterfester Aufbau sowie eine robuste Elektronik und Optik nötig. Außerdem soll das System automatisch arbeiten – manuelle Eingriffe müssen ferngesteuert möglich sein, was einen zusätzlichen Aufwand an Elektronik und Mechanik wie z.B. Schrittmotoren erfordert.

Die im Rahmen dieser Arbeit durchgeführten Arbeiten konzentrierten sich auf den Aufbau des Senders, speziell auf die Entwicklung des so genannten Alicemoduls, das die benötigten abgeschwächten Pulse mit Laserdioden erzeugt und auf eine räumliche Mode gefiltert aussendet. Der Aufbau dieses Moduls und des Senders wird im Folgenden beschrieben, worauf ein Überblick der elektronischen Baugruppen folgt. Weiter stand die Charakterisierung des Senders hinsichtlich potentieller Seitenkanäle im Vordergrund. Deren Messung sowie die Berechnung der maximalen Informationsmenge, die ein Angreifer durch eine Seitenkanalattacke in den charakterisierten Freiheitsgraden gewinnen kann, nehmen den Rest des Kapitels ein.

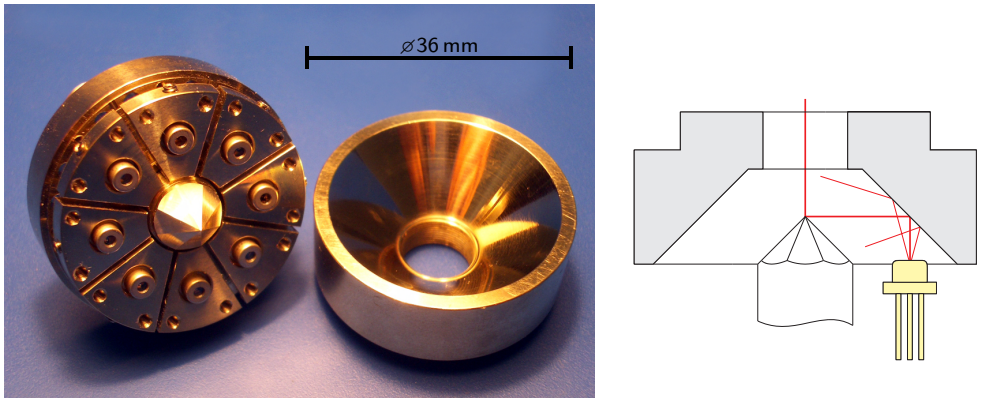
4.1 Mechanische und optische Komponenten des Senders

4.1.1 Der Diodenkopf

Dieses Bauteil nimmt die Laserdioden zur Erzeugung der abgeschwächten Pulse auf und bildet später zusammen mit dem Modenfilter das Alice-Modul. Dem Design des Diodenkopfes liegt eine frühere Baustufe zu Grunde [66], die jedoch mit nur vier, radial eingebauten, Dioden (ohne Decoy-Zustände) arbeitete. Darüber hinaus gab es Probleme, die nötige mittlere Photonenzahl durch ausreichend gute Kopplung in das anschließende Modenfilter zu erreichen. Der neue Diodenkopf bietet deshalb die Möglichkeit, jede der acht Dioden einzeln räumlich auszurichten. Verwendet werden hier Laserdioden in einem 5,6 mm Gehäuse mit einer nominalen Wellenlänge von $\lambda = 850\,\mathrm{nm}$. Neben der guten atmosphärischen Transmission, stehen bei dieser Wellenlänge mit Silizium-APDs (*avalanche photo diodes*) Einzelphotondetektoren zur Verfügung, die bei geringer Dunkelzählrate eine hohe Quanteneffizienz aufweisen[1]. Außerdem sind Laserdioden mit $\lambda = 850\,\mathrm{nm}$ und auch passende optische Komponenten kommerziell aus dem Serienprogramm verfügbar.

Die Laserdioden sind nun wie in Abbildung 4.1(a) auf einem Kranz angeordnet. Dieser besteht aus acht Flügeln die über je drei Schrauben auf der Rückseite einzeln gekippt und geneigt werden können. Die mittlere schiebt den Flügel nach vorne, die beiden äußeren ziehen ihn nach unten bzw. verkippen ihn. Alle Dioden sind parallel zur Achse in einen Innenkegelspiegel gerichtet, von dem die Strahlen zum Zentrum abgelenkt werden. Dort befindet sich ein pyramidaler Spiegel, der auf der Achse mit einem Gewinde positioniert werden kann und mit acht Seiten die radial einfallenden Photonen parallel zur Achse ausspiegelt. Eine Skizze der Strahlverlaufs ist in Abbildung 4.1(b) zu sehen und in Anhang B finden sich die technischen Zeichnungen der verschiedenen Bauteile.

[1] In Anhang A sind einige typische Werte für Silizium-APDs aufgeführt, sowie die Zusammenhänge mit der Temperatur und der Vorspannung kurz beschrieben. Weitere Charakteristika finden sich in [67]



(a) (b)

Abb. 4.1: (a) Diodenkopf zur Aufnahme der acht Laserdioden im Winkelabstand von 45 °, der pyramidale Spiegel im Zentrum sowie der Innenkegelspiegel. Durchmesser des Diodenkopfes: 36 mm. **(b)** Skizze des Strahlverlaufs im Alicekopf: Der Innenkegelspiegel richtet die Strahlen auf das Zentrum, dort spiegelt sie der pyramidale Spiegel parallel zur Achse aus. Oben kann eine Linse eingeschraubt werden, die die Einkopplungseffizienz in das anschließende Modenfilter erhöht.

Die intrinsische Polarisation der Dioden ist besser als 1:1000 und wird durch entsprechenden Einbau in den Diodenkopf jeweils radial ausgerichtet. Bei gleichmäßiger Aufteilung auf dem Kranz ergibt sich so der benötigte Winkel von 45 ° zwischen den Laserdioden. Auf diese Weise können einerseits die Photonen mit den 4 Polarisationsrichtungen für das BB84 Protokoll erzeugt werden, andererseits gibt es für jede Polarisationsrichtung zwei Dioden, die elektronisch, wie für das Decoy-Protokoll erforderlich, auf unterschiedliche Pulsintensitäten eingestellt werden.

Die Justiermöglichkeiten sind hier ausreichend, da nur eine sehr geringe Kopplungseffizienz benötigt wird. Gleiches gilt auch für die einfache Strahlführung mit nur einer Linse vor dem Modenfilter – nur einzelne Photonen aus jedem Puls müssen aufgefangen werden.

4.1.2 Das Modenfilter

Da hier verschiedene Dioden für die vier Polarisationen und die zwei Intensitäten verwendet werden, ist ein Raumfilter unbedingt erforderlich. Nur wenn das Licht von allen Dioden am Ausgang des Senders die immer gleiche Mode aufweist, ist die räumliche Ununterscheidbarkeit der Photonen gewährleistet.

In den Arbeiten [66] und [68] wurden ebenfalls mehrere Dioden verwendet um die verschiedenen Polarisationszustände zu erzeugen. Dabei wurde das Raumfilter durch zwei Lochblenden mit einem Durchmesser von 100 µm und einem Abstand von 9,2 mm realisiert [68]. Das Einkoppeln in solch ein Modenfilter erwies sich hier jedoch als sehr schwierig, da für Decoy-Zustände deutlich höhere mittlere Photonenzahlen erlaubt und erforderlich sind. Zudem ist die räumliche Filterung mit

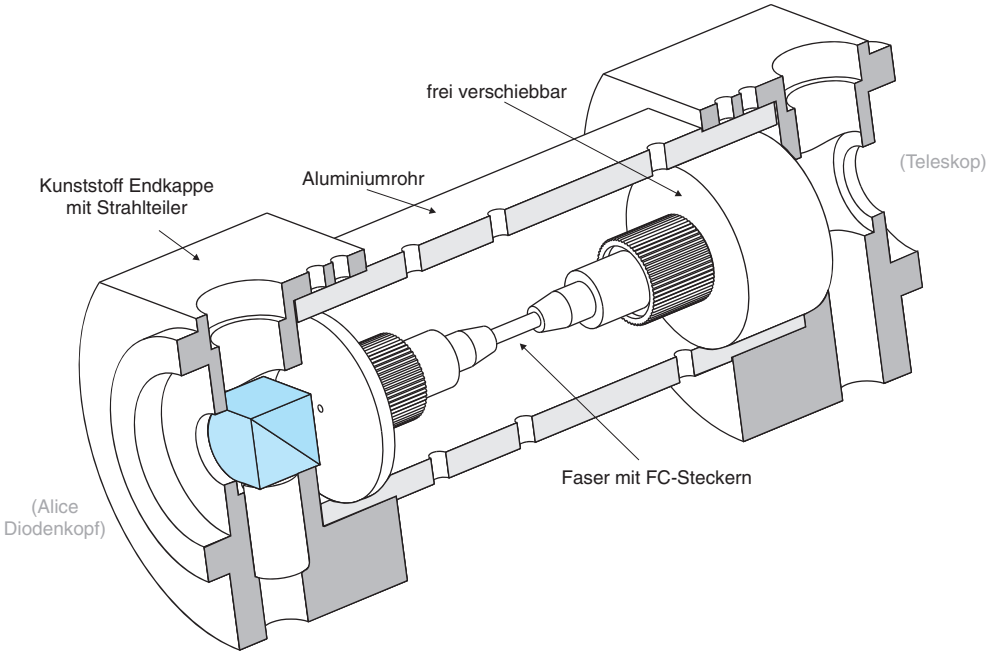


Abb. 4.2: Das Glasfaserstück zur räumlichen Filterung, eingegossen in ein Aluminium Rohr (Schnittdarstellung). Nur das linke Faserende ist fest mit dem Rohr verbunden. Rechts ist die Aufnahme für eine Auskoppellinse vorgesehen. Der Strahlteiler ermöglicht das Einkoppeln von leistungsstärkeren Lasern auf die gleiche Mode für Justageaufgaben. Außen ist das Rohr an vier Seiten Abgeflacht, so dass die Peltierelemente mit den Kühlkörpern aufgeklebt werden können.

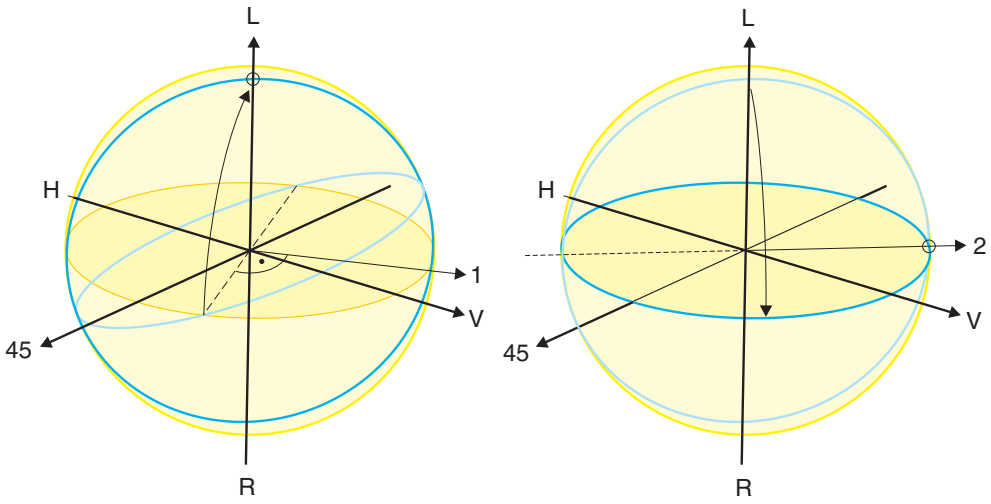


Abb. 4.3: Kompensation der Glasfaser, dargestellt auf der Blochkugel, hellblau ist jeweils die einfallende, dunkelblau die ausfallende Polarisationsebene: Nach der Glasfaser ist der Großkreis der linearen Polarisationen verkippt. Im ersten $\lambda/4$ (links) wird der Großkreis so gedreht, dass er die Pole schneidet. Die Achse des Wellenplättchens (1) muss dazu senkrecht zur gestrichelten Schnittgerade stehen. Im zweiten Schritt (rechts) dreht ein weiteres $\lambda/4$ den Kreis zurück auf den Äquator. Die Achse des zweiten Wellenplättchens (2) geht durch den Schnittpunkt mit dem Äquator. Die verbleibende Drehung in der Äquatorebene wird durch das anschließende $\lambda/2$ korrigiert (nicht dargestellt).

zwei Lochblenden nicht hinreichend möglich, so dass die verschiedenen Sendedioden auch nach dem Filter noch teilweise unterscheidbar sind. Deshalb wird das neue Modenfilter durch ein 5 cm langes Stück Singlemode-Faser (mit FC/PC-Steckern an jedem Ende, siehe Abb. 4.2) realisiert.

Durch die Verwendung einer Glasfaser erfolgt jedoch eine unberechenbare Drehung der Polarisation. Die vier, für BB84 benötigten, linearen Zustände liegen auf der Blochkugel in einer Ebene, welche durch die Glasfaser verkippt und rotiert wird. Dies muss wieder kompensiert werden, um die Lesbarkeit der polarisationscodierten Information zu gewährleisten. Die Drehung ist jedoch von der mechanischen Verspannung oder Verformung der Faser abhängig. Spannungsdoppelbrechung kann durch eine Änderung der räumlichen Lage aber auch schon durch die Temperatur bedingt sein. Letztere schwankt in der Senderbox jedoch mit dem Tag-Nacht-Rhythmus, sowie auch mit dem Wetter stark (siehe Abb. 4.4). Eine ständige Korrektur der Kompensation wäre also nötig, um die Polarisation konstant zu halten.

Um dies zu vermeiden und eine weitgehend statische Kompensation verwenden zu können, wurde eine Aufnahme in Form eines Aluminiumrohrs gebaut, in das die Glasfaser mit Silikon eingegossen und so vor äußeren Einflüssen geschützt wird. Dies fixiert sie räumlich und erzeugt keine zusätzlichen Spannungen da das Silikon langfristig flexibel bleibt. Beide Enden der Glasfaser sind mit den Steckern aufgenommen, jedoch ist zur Vermeidung einer Streckung oder Stauchung nur eine Seite fest mit dem Rohr verbunden.

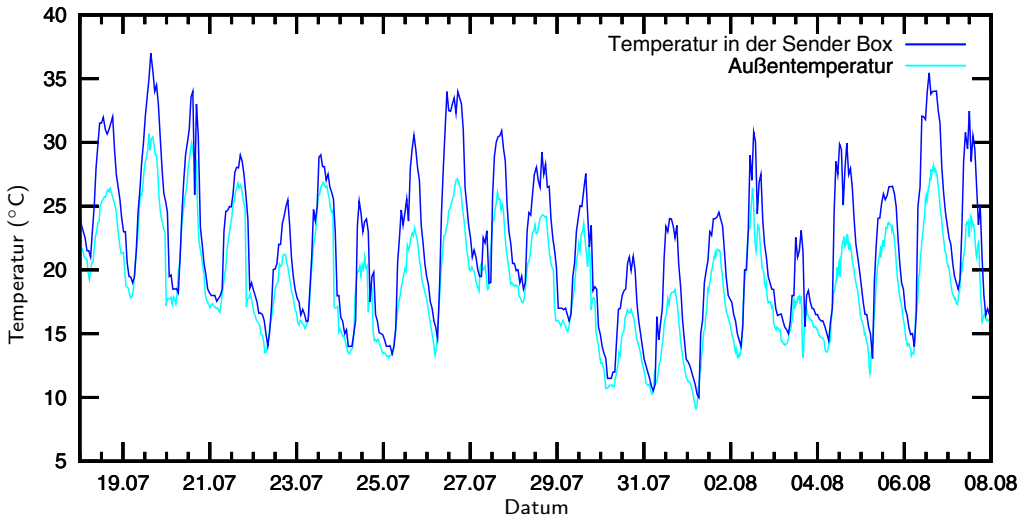


Abb. 4.4: Temperaturen in der Sender Box (blau) in Relation zu den Umgebungstemperaturen (cyan). Messung über mehrere Tage. [69]

Mit Hilfe von Peltierelementen wird das komplette Raumfilter auf konstanter Temperatur gehalten. Die thermische Isolation gegen den Diodenkopf und die Befestigung erfolgt mittels zweier Endkappen aus Kunststoff, die zudem die Möglichkeit zur Aufnahme eines Strahlteilers bieten. Abwärme können die Peltierelemente über passive Kühlkörper, wie in Abbildung 4.7 zu sehen, an die Umgebung abgegeben.

Für die eigentliche Kompensation der Polarisation werden schließlich zwei Viertel- und anschließend ein Halbwellenplättchen verwendet (siehe Abb. 4.3). Zunächst ist nur das Halbwellenplättchen durch einen Schrittmotor zu verstellen, dieses dient auch der Anpassung der Basen von Alice und Bob, die beiden Viertelwellenplättchen sollen jedoch in Zukunft ebenfalls motorisiert werden.

Um zu klären, ob die Stabilität der Polarisation nach diesem Modenfilter ausreichend für den Betrieb der QKD-Strecke im Freien ist, wurden einige vorbereitende Messungen durchgeführt. Der Aufbau bestand jeweils aus einer Laserdiode mit Polarisator, die in das Modenfilter eingekoppelt wurde. Danach wurden zirkulare Anteile der Polarisation mit zwei Viertelwellenplättchen kompensiert. Die Analyse erfolgte schließlich mit einem Polarisator, angetrieben durch einen Schrittmotor, und mit einer Photodiode.

Gemessen wurde jeweils der Kontrast V (die *visibility*) der Intensität, bzw. der Zählrate R, in der Form

$$V = \frac{R_{\max} - R_{\min}}{R_{\max} + R_{\min}} \tag{4.1}$$

in einer raumfesten Basis. Das heißt, zu Beginn der Messung wurde der Polarisator auf minimale Intensität eingestellt um dann in regelmäßigen Zeitabständen den Kontrast zwischen dieser und einer um 90 ° verdrehten Position des Polarisators, also bei maximaler Intensität, zu ermitteln.

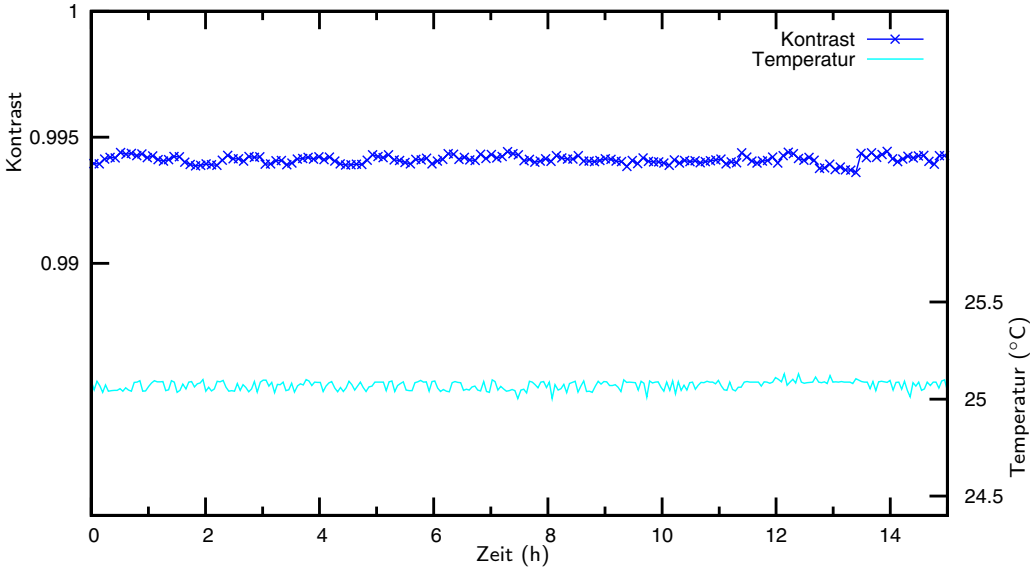


Abb. 4.5: Messung des Kontrastes zwischen Minimum und Maximum der Polarisationsanalyse in einer festen Basis über 15 h.

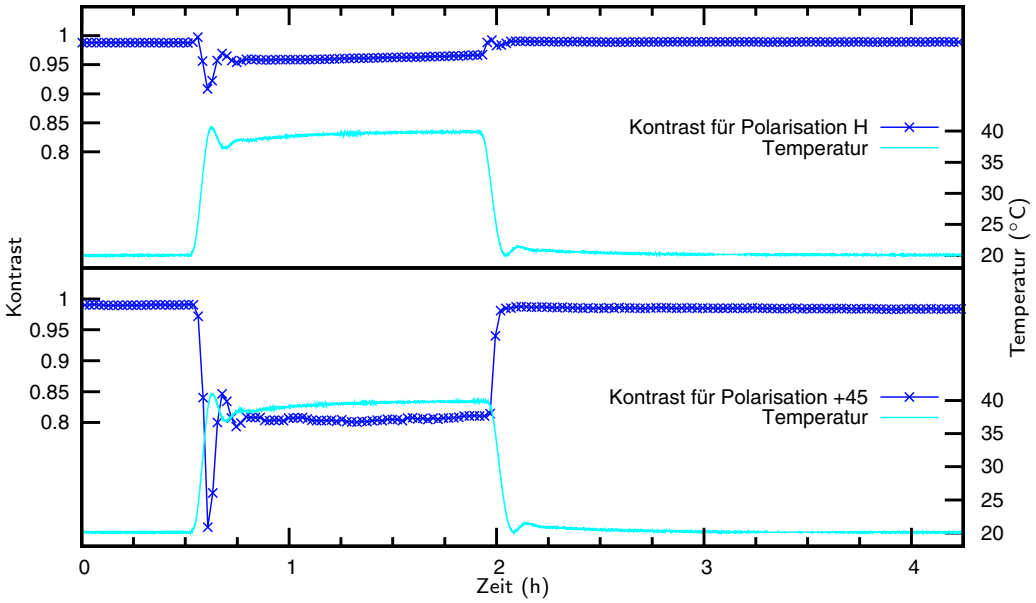


Abb. 4.6: Entwicklung der Polarisation nach dem Modenfilter in Reaktion auf eine Temperaturstufe. Oben für eine horizontale, unten für eine unter 45 ° eingekoppelte Polarisation.

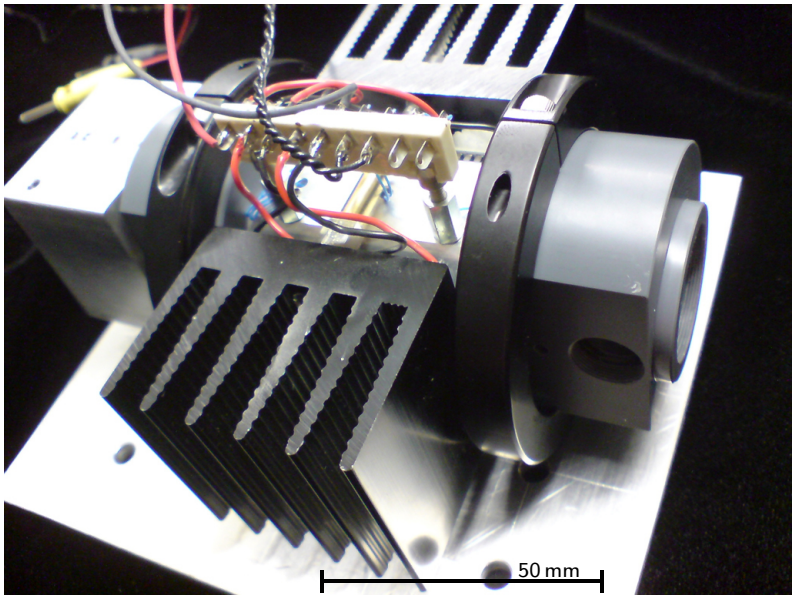


Abb. 4.7: Fertiges Alice-Modul bestehend aus Diodenkopf (links, eingebaut in einen Aluminium Würfel) und Modenfilter mit Kühlrippen. Oben aufgelegt sind die Anschlüsse der Peltierelemente sowie von Thermistoren die mit der Glasfaser eingegossen wurden.

Eine erste Messung betrachtet das Verhalten über einen Zeitraum von etwa 12 h (Abb. 4.5). Der Kontrast in der Polarisationsanalyse blieb dabei weitgehend konstant. Die zweite Messung (Abb. 4.6) bestimmt das Verhalten nach einer kurzfristigen Temperaturänderung. Dazu wurde die Temperatur der Faser für etwa 90 Minuten auf 40 ° erhöht und dann wieder auf 20 ° zurück gesetzt. Bei erhöhter Temperatur und besonders während der Temperaturänderung sinkt der Kontrast stark ab, um dann, wenn die Glasfaser zurück auf Solltemperatur ist, wieder auf den ursprünglichen Wert anzusteigen. Weitere Versuche mit kleineren Stufen und auch mit langsamen, stetigen Temperaturschwankungen zeigen ein ähnliches Verhalten.

Die Ergebnisse versprechen eine gute Verwendbarkeit des Modenfilters im Rahmen des Experimentes vor Ort, soweit die Temperatur auf etwa ±1 °C genau stabilisiert werden kann. Für echt fern-gesteuerte Anwendungen müssen jedoch die beiden Viertelwellenplättchen ebenfalls motorisiert werden, da es dann nicht möglich ist, die Kompensation nach einigen Wochen manuell nachzustellen. Eine ständige Korrektur in Echtzeit sollte jedoch in keinem Fall nötig sein.

In Abbildung 4.7 ist schließlich das komplette Alice-Modul zu sehen. Eine Linse zwischen Diodenkopf und Modenfilter sowie eine weitere zur Auskopplung aus der Faser (beide $f = 11\,\mathrm{mm}$) ist bereits integriert, so dass nach dem Modenfilter ein kollimierter Strahl zu Verfügung steht. Die Außenmaße betragen etwa $12\,\mathrm{cm} \times 17\,\mathrm{cm}$ bei einer Höhe von 12 cm, der Strahl verlässt das Modul parallel zur Auflage in einer Höhe von 38 mm.

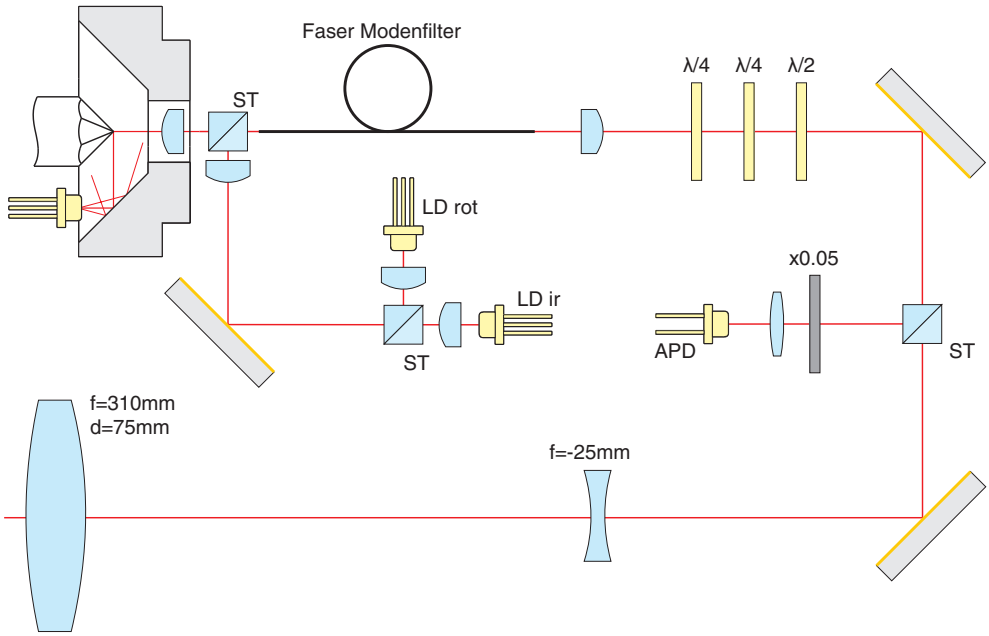


Abb. 4.8: Schematischer Aufbau der kompletten Sendeeinheit: Direkt nach dem Diodenkopf und dem Modenfilter (links oben) kommen die Wellenplättchen, so kann deren Einfluss auf die Pulsintensität kompensiert werden. Rechts wird mit einem Strahlteilerwürfel ein Teil der Photonen ausgespiegelt. Diese werden nach einem Graufilter auf eine APD fokussiert und gezählt. Über einen weiteren Spiegel wird der Strahl zum Teleskop geführt. Die helleren Laser für Justageaufgaben werden zusätzlich mit einer Linse über den Strahlteiler in das Modenfilter eingekoppelt. Ein Foto des Aufbaus findet sich in 4.9.

4.1.3 Strahlverlauf und weitere optische Komponenten

Alle optischen Komponenten des Senders sind auf einem Breadboard aufgebaut (vgl. Abb. 4.8 und 4.9): Das Alice-Modul, die Polarisationskompensation, eine APD zur Kalibrierung der Pulsintensitäten sowie die Ziellaser mit Einkopplung und das Teleskop.

Bei der Messung der Pulsintensitäten müssen das Verhältnis von Transmission zu Reflexion des Strahlteilers r, die Transmission des Graufilters T und die Detektionseffizienz der APD η (zusammen mit dem Tageslichtfilter, die Effizienz wurde in [67] gemessen) berücksichtigt werden. Die mittlere Photonzahl pro gesendetem Puls μ ergibt sich dann mit der gemessenen Zählrate R und der Pulsrate des Senders $R_{\text{rep}} = 10^7\,\text{s}^{-1}$ zu:

$$\mu = -\frac{r}{\eta T} \ln\left(1 - \frac{R}{R_{\text{rep}}}\right) \tag{4.2}$$

Die Berechnung mit dem Logarithmus resultiert aus der Poissonverteilung der Photonen und führt zu einem überproportionalen Anstieg von μ bei größeren Werten von R/R_{rep}.

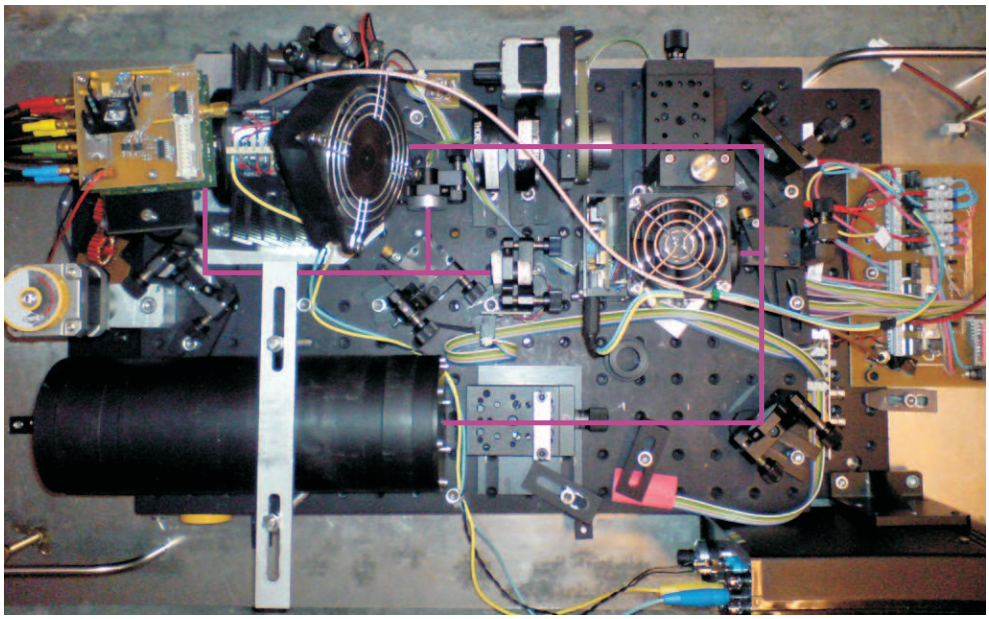


Abb. 4.9: Foto des Sendeaufbaus, wie er in Abbildung 4.8 beschrieben ist.

Im Betrieb muss μ für jede Diode immer wieder kontrolliert und nachjustiert werden, um die Sicherheit der Übertragung zu gewährleisten. Nur so können die richtigen Parameter für das Decoy Protokoll ermittelt und eingehalten werden.

Das Sendeteleskop muss schon im ersten Schritt sehr genau ausgerichtet werden, um den Empfang von Photonen zu ermöglichen, da schon wenige $1/10$ mrad Abweichung ausreichen, um auf die Entfernung vollständig am Empfänger vorbei zu zielen. Das bedeutet, dass ohne einen helleren Ziellaser kaum eine Chance besteht, den Empfänger zu finden und zu treffen. Um das erste Einrichten auf dem Dach zu erleichtern ist deshalb ein roter, heller Laser vorgesehen der ebenfalls in das Modenfilter eingekoppelt wird, damit er in die gleiche Richtung zeigt wie später die Signalstrecke.

Desweiteren wird ein infraroter Laser mit $\lambda = 850\,\text{nm}$ eingekoppelt. Dieser arbeitet also auf der gleichen Wellenlänge wie die Laserdioden für die Kryptographie und dient in erster Linie dazu, die Positionen und Abstände der Linsen zu justieren.

4.2 Elektronik des Senders

Hier soll zunächst ein Überblick der elektronischen Baueinheiten des Senders gegeben werden (siehe Abb. 4.10), bevor einzelne Module genauer beschrieben werden: Die Kontrolle des Senders erfolgt mit einem 64 Bit Computersystem, eine Netzwerkverbindung sorgt für die notwendige Fernsteuerbarkeit. Als Schnittstellen werden drei digital und analog Ein-/Ausgabe-Karten, jeweils am PCI Bus, verwendet. Darüber hinaus steht mit einem USB auf I^2C Adapter ein weiterer Ein- und

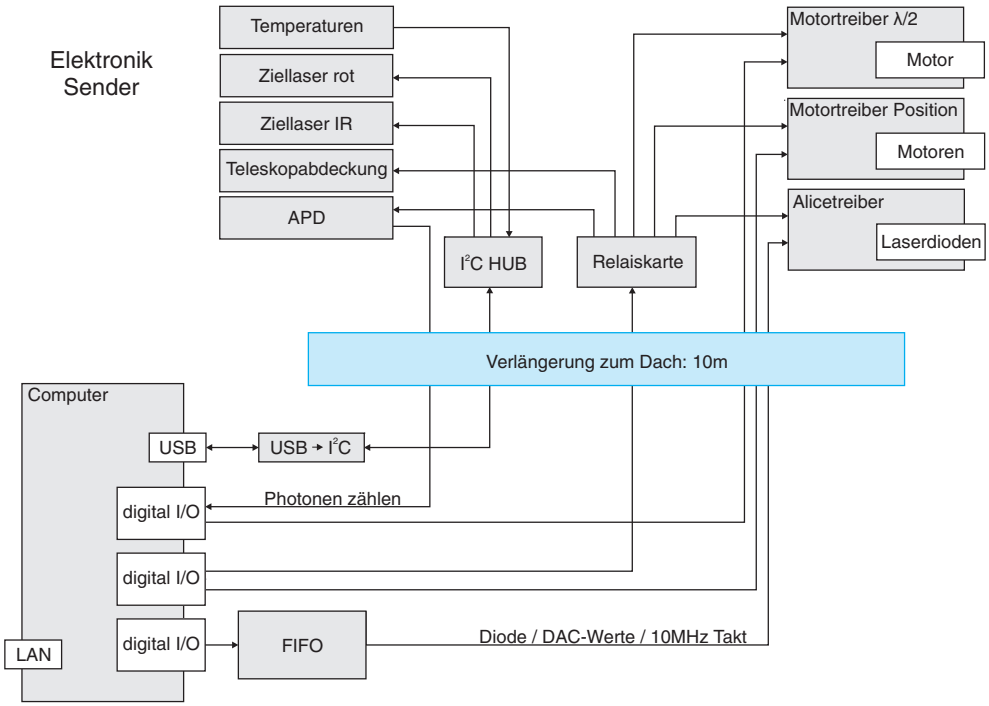


Abb. 4.10: Blockdiagramm der gesamten Sendeelektronik. Die Kabelverbindungen aufs Dach sind 10 m lang und durch einen Schlauch zusammengefasst, der sie vor Sonnenlicht (UV) schützt. FIFO bezeichnet einen so genannten *first in first out* Speicher.

Ausgabekanal zur Verfügung, der in Zukunft zumindest eine der PCI-Karten ersetzen soll. Als Stromversorgung für die Module auf dem Dach kommen 5 V, 12 V und ±15 V Schaltnetzteile zum Einsatz. Aufgrund der langen Kabel und der Steckverbindungen können dort jedoch Spannungsabfälle bei höheren Strömen auftreten. Teilweise, insbesondere für den Alicetreiber, werden deshalb die Versorgungsspannungen erst auf dem Dach, mit separaten Festspannungsreglern, bereitgestellt.

Bereits gebaut, jedoch noch nicht eingebunden, ist ein Generator für echte Zufallszahlen zum Anschluss über USB 2.0, zuletzt entwickelt im Rahmen der Arbeit von Davide Marangon [70]. Dieser nutzt Einzelphotondetektionen, die jeweils ein Flipflop umschalten. Die Abfrage des Zustands dieses Flipflops in festen Zeitabständen liefert dann die Zufallszahlen. Vorerst werden aber noch pseudozufällige Bitfolgen, generiert vom Computer, verwendet.

4.2.1 Alicetreiber

Diese Baugruppe hat die Aufgabe, die jeweils richtige Diode, zu einem genauen Zeitpunkt, mit einem definierten elektrischen Puls anzusteuern. Dazu sind ein Takt-Eingang für das 10-MHz-Signal, ein vier Bit breiter TTL-Eingang zur Wahl der Polarisation (H,V,±45) sowie ein weiterer TTL-Eingang zum Umschalten Decoy/$\overline{\text{Decoy}}$ vorhanden (siehe Abb. 4.11). Durch logische Operationen können so

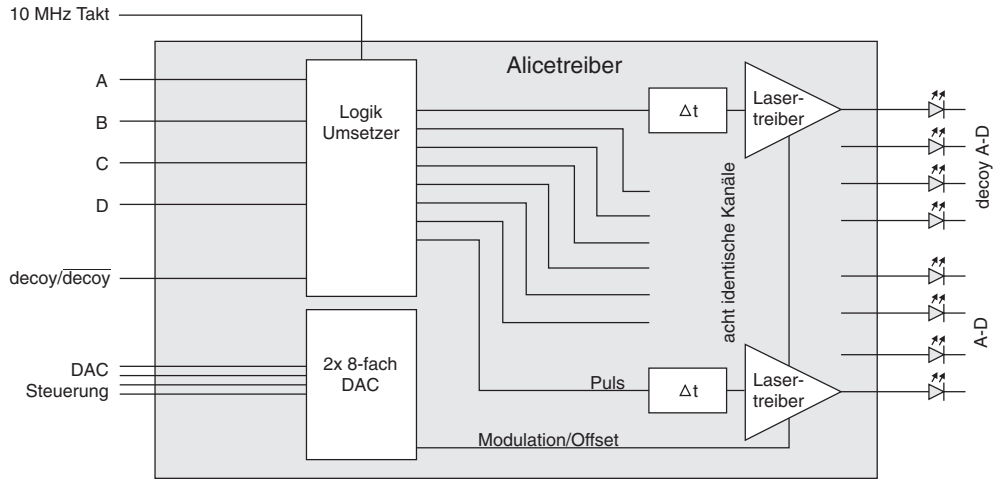


Abb. 4.11: Blockdiagramm des Alicetreibers. Genaue Beschreibung im Text.

alle acht Dioden einzeln angesprochen werden. Über weitere vier Anschlüsse sind zwei Digital-Analog-Wandler (DACs) für jeden Kanal einzeln programmierbar.

Das eingehende Taktsignal wird zu kurzen Pulsen geformt und an alle acht identischen Kanäle weitergeleitet. Wenn die UND-Operation aus Dioden und Decoy-Information für eine Laserdiode ein positives Ergebnis geliefert hat, kann der Puls über ein programmierbares Verzögerungsglied den Lasertreiber ansteuern, wodurch Laufzeitunterschiede ausgeglichen werden können.

Als Lasertreiber kommt für jeden Kanal ein integrierter Baustein zum Einsatz. Dieser bietet zwei analoge Eingänge für die Einstellung eines Offsetstroms (*bias*), der ständig fließt, und eines Modulationsstroms, der zusätzlich, während eines Pulses, überlagert wird. Beide sind mit den DACs per Software vorgegeben. Auf diese Weise können mit jeder Diode, unabhängig von deren spezieller elektrischer Charakteristik und Einkopplungseffizienz, Pulse mit gleicher mittlerer Photonenzahl erzeugt werden.

Die Elektronik des Alicetreibers besteht insgesamt aus drei $60\,\mathrm{mm} \times 60\,\mathrm{mm}$ große Platinen, die direkt am Diodenkopf angebracht sind. Mit kurzen, geschirmten Kabeln zu den Dioden können so Verluste minimiert werden.

4.2.2 Temperatursteuerung des Modenfilters

Um die Glasfaser zur Raumfilterung auf konstanter Temperatur zu halten und so dynamische Verdrehungen der Polarisation weitestgehend zu vermeiden, steuert eine Elektronik die Peltierelemente am Modenfilter. Die Spannung an einem Thermistor wird mit dem Sollwert von $5\,\mathrm{V}$ ($\widehat{=}\ 25\,^{\circ}\mathrm{C}$) verglichen und verstärkt. Ein PI-Regler steuert schließlich eine Leistungsstufe, mit der sowohl Kühlen als auch Heizen möglich ist. Die im Mittel, relativ zur Umgebung, hohe Temperatur wurde gewählt, da ein Heizen mit Peltierelementen, auf Grund ihrer eigener Leistungsabgabe stets effektiver

ist als ein Kühlen. Eine weiterführende Beschreibung der Temperatursteuerung findet sich in [68].

4.3 Charakterisierende Messungen

Wie schon in 3.4 beschrieben, bieten Ungenauigkeiten in der Implementierung eines quantenkryptographischen Protokolls Angriffspunkte. Einem Angreifer wird es dadurch möglich, übertragenen Photonen nicht anhand ihrer Polarisation, sondern auf Grund eines weiteren Freiheitsgrades, Bitwerte zuzuordnen. Auch wenn nur die Basis über einen solchen Freiheitsgrad sicher oder mit hoher Wahrscheinlichkeit bekannt wird, kann ein Angreifer das jeweilige Photon messen, erhält volle Information über den Bitwert und kann eine Kopie weitersenden, ohne einen Fehler zu verursachen.

Ein zusätzlich und in der Regel ungewollt modulierter Freiheitsgrad kann z.B. räumlicher, zeitlicher oder spektraler Natur sein. Nur wenn die Ununterscheidbarkeit der Photonen in jeder Hinsicht gewährleistet ist, sind solche Angriffe ausgeschlossen – eine Anforderung, die in realen Systemen jedoch nie erreicht wird. Nachträglich kann die Sicherheit durch *privacy amplification* garantiert werden, wozu es jedoch notwendig ist, den Informationsgewinn eines Angreifers abschätzen zu können. Dazu werden hier Messungen dokumentiert, die den Sender im Hinblick auf die zeitliche, räumliche und spektrale Unterscheidbarkeit der Photonen charakterisieren und die die QBER, die aus Ungenauigkeiten im Aufbau stammt, abschätzen.

4.3.1 Kalibrierung der mittleren Photonenzahl pro Puls

Soweit möglich, werden alle folgenden Messungen mit Offset- und Modulationswerten für die Laserdioden durchgeführt, die den bei der Kryptographie verwendeten Einstellungen entsprechen. Dies stellt spezielle Anforderungen an die Messweise, da stets einzelne Photonen detektiert werden müssen. Um die richtigen Parameter für den Alicetreiber zu finden, also definierte Pulsintensitäten einzustellen, werden diese für jede einzelne Diode getestet und inkrementell angepasst. Dabei wird ein möglichst niedriger Offsetwert bei maximaler Modulation angestrebt, um die Hintergrundzählrate klein zu halten.

Die Messung der mittleren Photonenzahl pro Puls μ erfolgt durch eine APD, auf die der Strahl des Alice-Moduls nach einem Graufilter fokussiert wird. Auch im fertigen Aufbau am Dach können so jederzeit Änderungen festgestellt und korrigiert werden (vgl. 4.1.3 und Abb. 4.8). Auf Grund der empfindlichen Abhängigkeit der mittleren Photonenzahl μ vom Offsetstrom (Abb. 4.12) ist dies notwendig. Kleine Schwankungen der DAC Spannungen können große Veränderungen von μ bedeuten. In regelmäßigen Abständen von etwa einer viertel Stunde werden im Betrieb deshalb die Werte überprüft und ggf. neu eingestellt.

Dies geschieht durch ein Programm, das nacheinander die Dioden einzeln aktiviert, die Zählrate misst und, wenn diese zu große Abweichung vom Sollwert

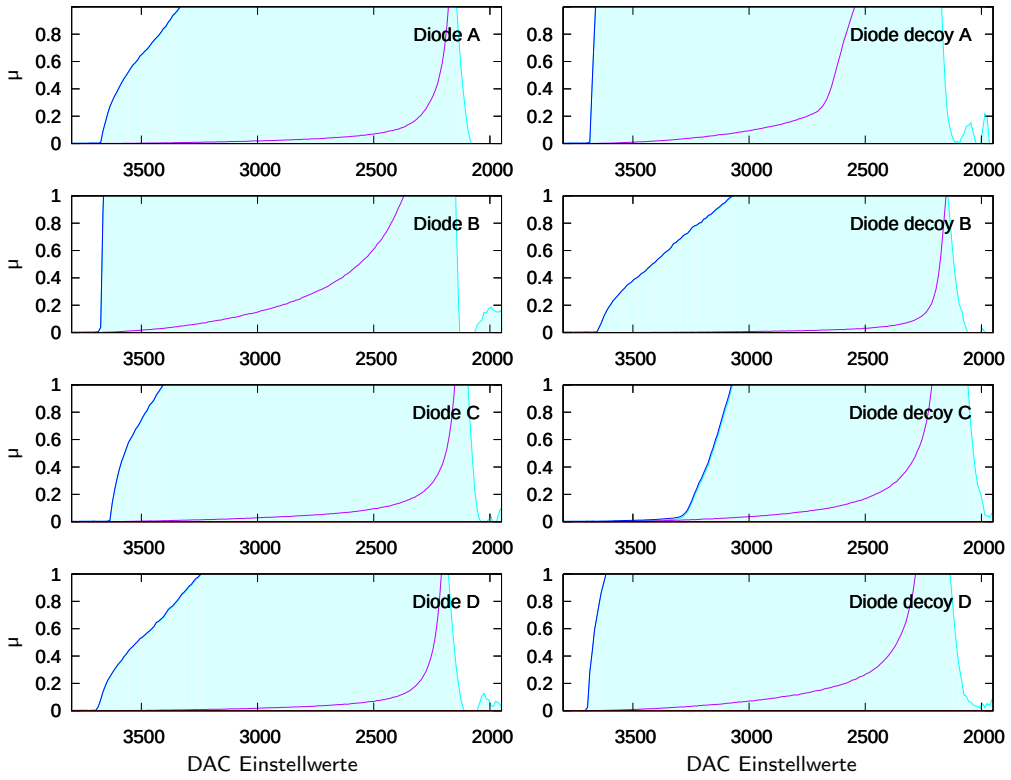


Abb. 4.12: Messung zur mittleren Photonenzahl pro Puls in Abhängigkeit des Offset Stroms in DAC Einstellwerten bei maximaler Modulation im fertigen Aufbau. Aufgetragen ist violett: Hintergrundzählrate, blau: Zählrate im gepulsten Betrieb und cyan: Differenz aus gepulstem Betrieb und Hintergrundzählrate. Die DAC Werte liegen zwischen 4095 (minimaler Offsetstrom/minimale Modulation) und 0 (Maximum). Das Programm zur Einstellung der Differenz-Zählrate (cyan), prüft und sucht die richtigen Parameter zunächst für den Offsetstrom, indem es einzelne Dioden aktiviert und von der Zählrate des Kalibrierdetektors (blau) den Hintergrund (violett) abzieht. Ist der Zusammenhang sehr steil, z.B. bei Diode B, wird auch der Wert der Modulation variiert, um Pulse mit einem exakten Wert von μ zu erzeugen.

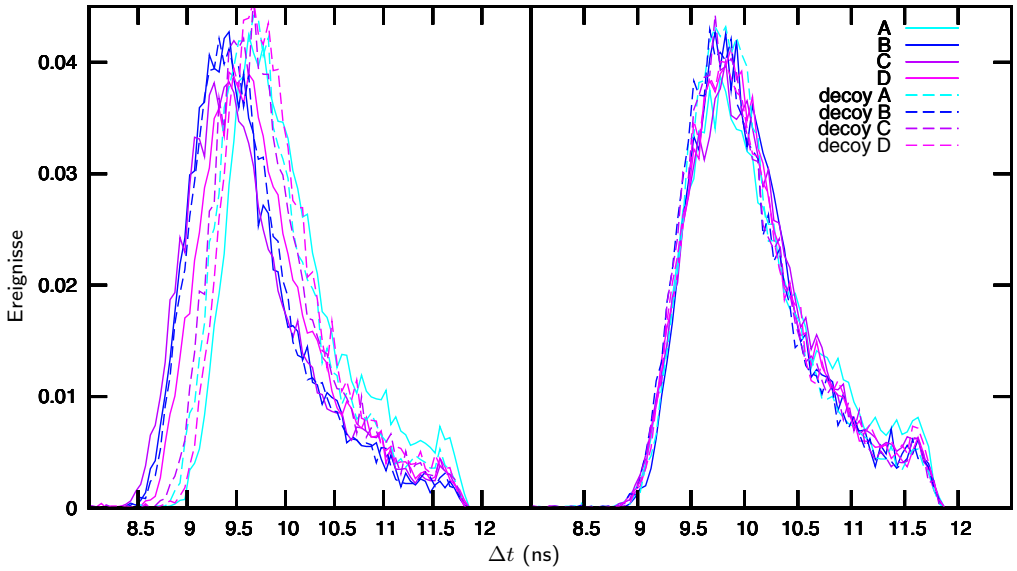


Abb. 4.13: Histogramm der Emissionszeitpunkte der Photonen relativ zum 10 MHz Takt. Links: vor dem Einstellen der programmierbaren Verzögerungsbausteine auf dem Alicetreiber, rechts: danach

aufweist, den richtigen Wert für den Offsetstrom durch Intervallhalbierung sucht. Dabei wird die Modulation auf Maximum eingestellt. Erst wenn sich herausstellt, dass μ so sensitiv auf den Offsetstrom reagiert, dass keine ausreichende Genauigkeit erzielt werden kann (siehe Abb. 4.12), schaltet das Programm um und reduziert in geeigneter Weise den Modulationswert bei festem Offset. Die gewonnenen Parameter werden am Schluss in eine Konfigurationsdatei für den Alicetreiber geschrieben.

Der Einstellbereich mit Hilfe der DACs ist jedoch begrenzt, da mit den Werten für Offset und Modulation auch die Pulslänge schwankt. Auch das Spektrum der Pulse wird hier Abhängigkeiten zeigen. Reichen kleine Anpassungen der DAC Werte nicht mehr aus, so muss deshalb die Einkopplung der Dioden modifiziert werden.

4.3.2 Emissionszeitpunkte der Photonen

Um den Informationsgewinn zu minimieren, den ein Angreifer aus einer sehr exakten Messung der Ankunftszeit gewinnen kann, müssen die Pulse aller Dioden mit jeweils gleicher Verzögerung relativ zum 10 MHz Takt ausgesendet werden. Dieser zeitliche Freiheitsgrad lässt sich mit den Verzögerungsbausteinen des Alicetreibers (vgl. 4.2.1) digital einstellen. Programmierbar ist eine Verzögerung von bis zu 2 ns mit einer Auflösung von < 50 ps.

Um für die Messung der Emissionszeitpunkte die Photonen zu registrieren, wird auch hier eine APD verwendet, auf die der Strahl aus dem Alicemodul fokussiert wird. Ein Oszilloskop erstellt ein Histogramm der Zeitabstände zwischen dem 10-MHz-Taktsignal, welches als Trigger verwendet wird, und den Pulsen der APD, die die Detektion eines Photons anzeigen. Die Messung mit einer schnellen Photodiode

Tabelle 4.1: Mittelwerte der Emissionszeitpunkte aus Abbildung 4.13 für alle acht Laserdioden bezogen auf das Takt Signal.

Diode	gemittelte Position (ns)	Abweichung vom Mittelwert (ns)
A	10,12	0,06
B	10,07	0,01
C	10,09	0,03
D	10,05	0,00
Decoy A	10,03	−0,03
Decoy B	10,01	−0,05
Decoy C	10,03	−0,03
Decoy D	10,07	0,01
Mittelwert:	10,06	

an einem Oszilloskop ist auf Grund der niedrigen Intensitäten nicht möglich. Insgesamt wurden für jede Diode etwa 12000 Ereignisse ausgewertet. Das Ergebnis der Messung ist in Abbildung 4.13 zu sehen, jeweils vor und nach der Einstellung der Verzögerungsbausteine und einzeln normiert auf gleiche Gesamtzählrate. Nach der Justage ergeben sich die Werte in Tabelle 4.1.

Für alle Dioden liegt die Breite der Verteilungen (FWHM) bei 1 ns. Dieser Wert enthält jedoch noch die Jitter der APD mit ihrer Elektronik von etwa 600 ps und des Oszilloskops mit etwa 40 ps. Man kann also von einer zeitlichen Breite der Alicepulse von etwa 0,8 ns ausgehen.

4.3.3 Räumliche Unterscheidbarkeit der Photonen

Hier soll geprüft werden, inwieweit alle acht Dioden nach dem Modenfilter tatsächlich räumlich als eine Lichtquelle erscheinen, um auszuschließen, dass ein nicht zu vernachlässigender Teil der Photonen, die in die Faserummantelung eingekoppelt wurden, zur Kryptographie beiträgt. Die Glasfaser ist mit einer Länge von nur 5 cm so kurz, dass sich die Dämpfung in der Ummantelung als nicht ausreichend herausstellen könnte.

Bei der Messung tastet eine APD, ohne weitere Optik, bewegt von zwei Schrittmotoren, den Strahl des Alicemoduls etwa 40 cm nach dem Raumfilter zweidimensional ab. Die Linse zur Auskopplung der Photonen aus der Faser wurde zuvor so eingestellt, dass der Strahl des hellen Ziellasers (ebenfalls mit Wellenlänge $\lambda = 850\,\text{nm}$) über mehrere Meter keine Aufweitung zeigt, so dass er am Ort der Messung gut kollimiert ist. Indem der erste Spiegel in Abbildung 4.8 gedreht wurde trifft der Strahl senkrecht auf den außen montierten Detektor. Dessen Schrittweite beträgt 250 µm,

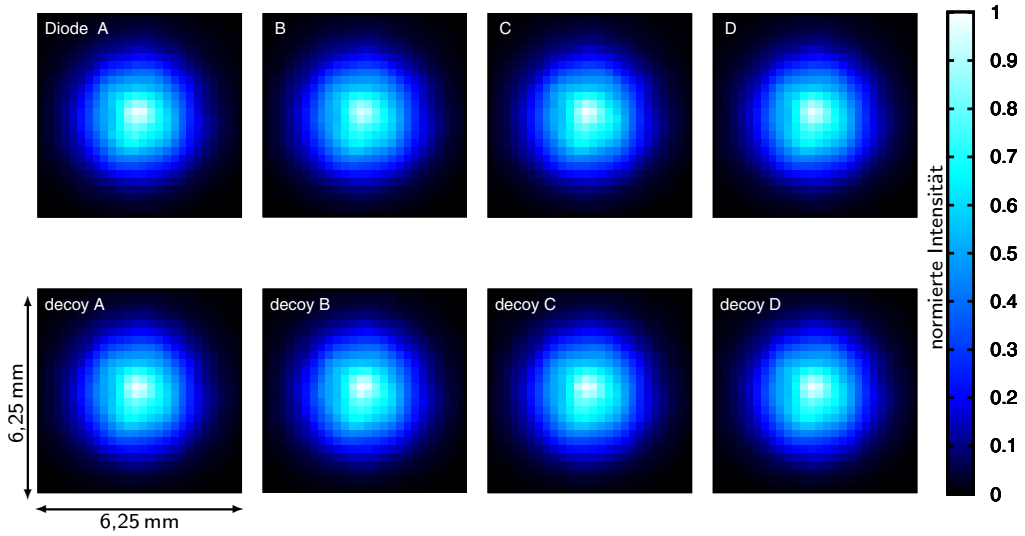


Abb. 4.14: Intensitätsprofile der acht Sendedioden, aufgenommen im kollimierten Strahl nach dem Modenfilter.

die kreisförmige Detektorfläche der APD hat einen Durchmesser von 500 µm und für jeden Punkt wird die Zählrate 1 s lang integriert. Die Intensitätsprofile sind in Abbildung 4.14 dargestellt.

Wie nach einer Singlemode-Faser zu erwarten, zeigen die Profile gute Übereinstimmung, ein Beitrag von Photonen aus der Ummantelung kann nicht festgestellt werden. Ein quantitatives Maß für die Abweichungen wird in Abschnitt 4.3.5 berechnet.

4.3.4 Spektrale Unterscheidbarkeit der Photonen

Auch anhand der Wellenlänge könnte ein Angreifer den Photonen Bitwerte zuordnen. Es ist jedoch, vor allem angesichts der Umwelteinflüsse im Freien, nicht praktikabel, mit vertretbarem Aufwand, acht Dioden so auszuwählen, zu temperieren und anzusteuern, dass sie in dieser Hinsicht, auch im Pulsbetrieb, ununterscheidbar sind. Deshalb soll zur Vermeidung eines solchen Angriffs in Zukunft ein schmales Interferenzfilter bei Alice sowie bei Bob, dort jedoch zur Unterdrückung des Hintergrundes, eingesetzt werden. Durch automatisches Verkippen eines solchen Filters mit einem Schrittmotor können dann kleine Schwankungen der Wellenlänge ausgeglichen und der Sender spektral mit dem Empfänger abgestimmt werden. Die Messungen der Spektren hier sollen deshalb auch klären, ob die einzelnen acht Dioden spektral ausreichend überlappen, dass auch nach einem engen Farbfilter jeweils genug Intensität zur Verfügung steht.

Die Spektren in Abbildung 4.15 entstanden mit einem offen aufgebauten Gitterspektrometer, dessen Gitter mit einem Schrittmotor bewegt wird. Als Detektor kommt eine APD zum Einsatz, die Intensitäten werden also in Form von Zählraten

Tabelle 4.2: Zentralwellenlängen und spektrale Breiten der acht Sendedioden gepulst, aus der Messung in Abbildung 4.15.

Diode	zentrale Wellenlänge (nm)	Breite (FWHM) (nm)
A	849,7	2,4
B	848,8	2,9
C	849,1	3,0
D	850,0	2,5
Decoy A	850,0	2,5
Decoy B	849,5	2,5
Decoy C	849,3	2,8
Decoy D	849,5	2,5
Mittelwert	849,48	2,6

ermittelt. Für die Dauerstrichspektren wurde ein geeigneter Graufilter verwendet um den linearen Bereich der APD nicht zu überschreiten. Die Auflösung des Spektrometers beträgt 0,6 nm und die absolute Eichung erfolgt mit dem Licht eines Helium-Neon-Lasers (genaue Charakterisierung des Aufbaus in [71]).

Abbildung 4.15 sowie die Werte in Tabelle 4.2 zeigen, dass auch bei Verwendung eines schmalbandigen Interferenzfilters ausreichend Intensität von allen Dioden zur Verfügung stehen sollte. Unter der Annahme, dass die Spektren im Transmissionsbereich des Interferenzfilters nur gering voneinander abweichen, kann man nach dem Filter von weitgehend ununterscheidbaren Photonen ausgehen.

Auch wenn diese ideale Voraussetzung natürlich nicht erfüllt ist, so verringert ein solcher Filter den Verlust von Schlüssel wegen der dann geringen Verluste bei der *privacy amplification* doch erheblich. Auch ohne einen zusätzlichen Interferenzfilter ist, wie sich in 4.3.5 herausstellt, die Information, die ein Angreifer aus der Messung der Wellenlänge erhält, jedoch vergleichbar mit der Informationsmenge, die Unschärfe des Emissionszeitpunkts preisgibt.

4.3.5 Informationsverlust über Seitenkanäle

Um das Maß an Information abzuschätzen, das ein Angreifer durch eine Messung in den oben behandelten Freiheitsgraden gewinnen kann, muss geklärt werden, welchen Informationsgehalt etwa die gemessene Wellenlänge über den Bitwert bzw. über die Basis enthält. Kann ein Angreifer letztere ermitteln, ist ihm auch der Bitwert durch eine Messung zugänglich. Eine aussagekräftige Größe ist die wechselseitige Information (*mutual information*) I, definiert über die Entropie H zweier Zufallsvariablen A und B: [64, 72]

$$I(A:B) = H(A) - H(A|B) \tag{4.3}$$

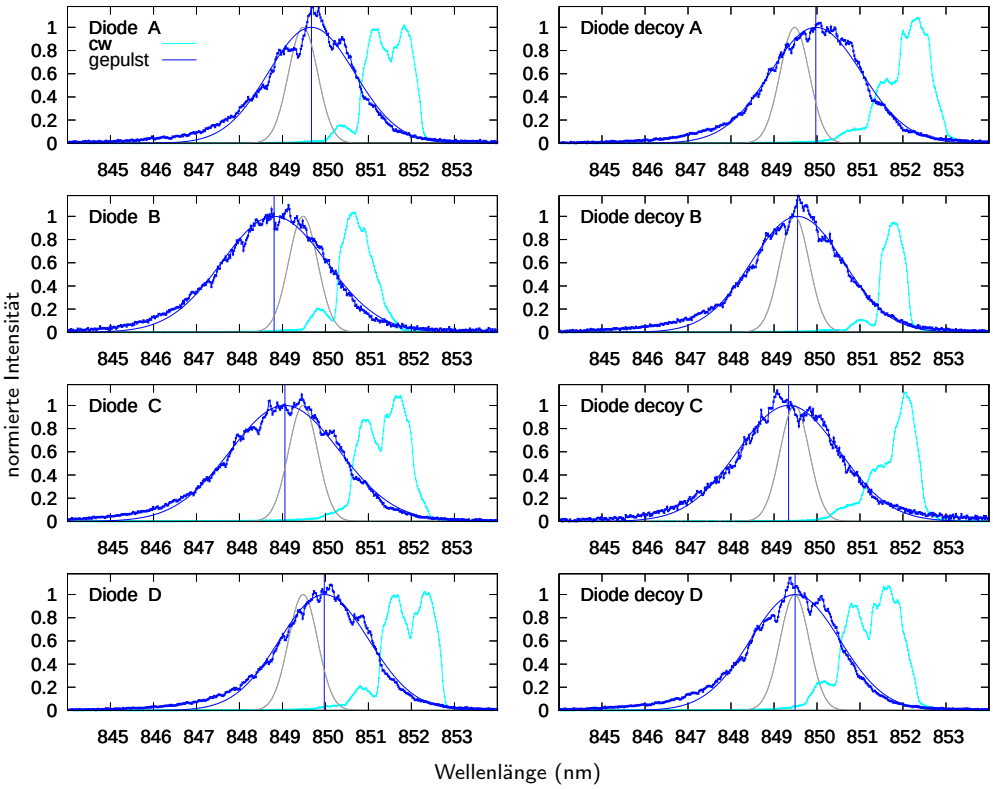


Abb. 4.15: Messung der Spektren für alle acht Dioden des Senders, Dauerstrich sowie gepulst, jeweils normiert. Zusätzlich ist die theoretische Transmission eines Interferenzfilters mit 0,8 nm Breite (FWHM) gezeichnet (grau). Eine Aufstellung der Zentralwellenlängen und spektralen Breiten im Pulsbetrieb findet sich in Tabelle 4.2

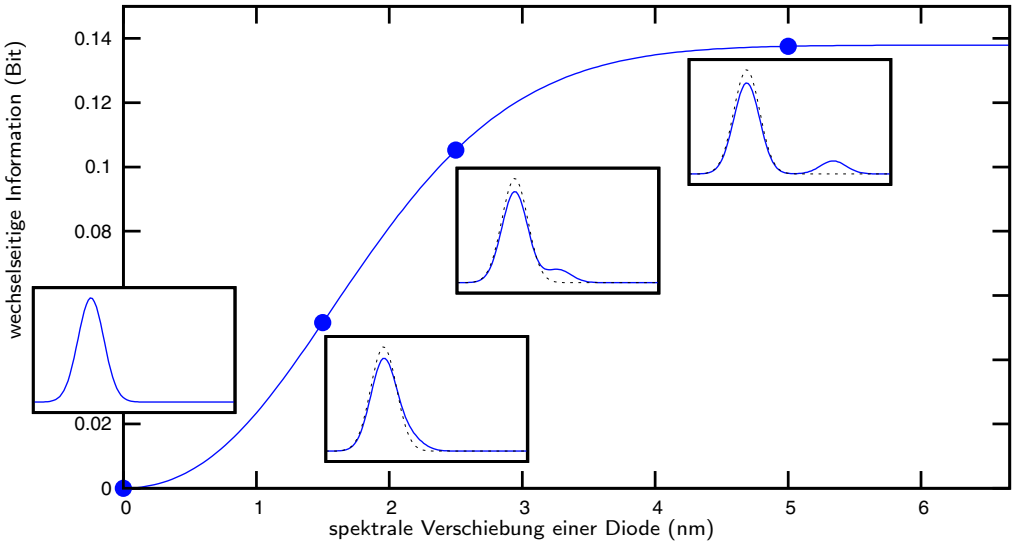


Abb. 4.16: Simulierte wechselseitige Information zwischen dem Spektrum und dem Bitwert, aufgetragen gegen die spektrale Verschiebung einer von acht Sendedioden. Für die blauen Punkte $\Delta\lambda = 0; 1{,}5; 2{,}5; 5\,\mathrm{nm}$ ist jeweils qualitativ die Wahrscheinlichkeitsverteilung $p(\lambda)$ (blau) mit der ungestörten Verteilung (schwarz, gestrichelt) dargestellt. Die spektrale Breite jeder einzelnen Diode beträgt hier 2 nm (FWHM).

Die Definition beschreibt die wechselseitige Information als den Betrag, um den sich die Unsicherheit (Entropie) einer Zufallsvariable A verringert, wenn eine andere Zufallsvariable B bekannt ist. Dieser Wert ist symmetrisch in Bezug auf die beiden Zufallsvariablen: $I(A:B) = I(B:A)$.

Schreibt man die Wahrscheinlichkeit, ein spezielles $a \in A$ zu erhalten mit $p(a)$ sowie die bedingte Wahrscheinlichkeit $p(a|b) = p(A = a|B = b)$, so sind die Entropie $H(A)$ und die bedingte Entropie $H(A|B)$ ihrerseits wie folgt definiert:

$$H(A) = -\sum_{x\in A} p(a)\log_2 p(a) \tag{4.4a}$$

$$H(A|B) = -\sum_{b\in B} p(b)\sum_{a\in A} p(a|b)\log_2 p(a|b) \tag{4.4b}$$

Zur Veranschaulichung soll hier für einen simulierten Sender, der ebenfalls mit zwei Dioden für jeden Zustand arbeitet, die Information berechnet werden, die ein Angreifer aus der Messung der Wellenlänge eines Photons über den gesendeten Bitwert gewinnen kann. Ausgehend von einem idealen Aufbau mit ununterscheidbaren Dioden, sind die Werte des maximal möglichen Informationsgewinns in Abbildung 4.16 für wachsende spektrale Verschiebungen *einer* der acht Dioden dargestellt. Simuliert wird also ein Fehler, auf Grund dessen sieben Dioden weiter ununterscheidbar bleiben, eine jedoch zunehmend und zuletzt eindeutig zu erkennen ist. Sind die beiden Spektren im Grenzwert schließlich komplett getrennt, konvergiert die

wechselseitige Information gegen etwa $^1/_7$ Bit:

$$\begin{aligned} I(\text{Bit} : \text{Spektrum}) &= H(\text{Bit}) - H(\text{Bit}|\text{Spektrum}) \\ &= 1 + \sum_{\lambda} p(\lambda) \sum_{\text{Bit}} p(b|\lambda) \log_2 p(b|\lambda) \\ &= 1 + {}^7/_8 \cdot ({}^4/_7 \log_2 {}^4/_7 + {}^3/_7 \log_2 {}^3/_7) - {}^1/_8 \cdot (1 \log_2 1) \\ &\approx 0.138 \end{aligned}$$

Um die Informationsmenge, die ein Angreifer aus einer Messung wie in 4.3.2–4.3.4 gewinnen kann, zu berechnen, sollen die obige Messungen als diskrete, bedingte Wahrscheinlichkeitsverteilungen der Zufallsgrößen Λ (Spektrum), X (räumliche Verteilung) und T (Verteilung der Emissionszeitpunkte) interpretiert werden. Die Diode bzw. die Basis, mit der ein Photon erzeugt wurde, ist ebenfalls eine Zufallsgröße und soll mit D und B bezeichnet werden. Man erhält so aus den Messungen für die Dioden $d \in D$

$$\begin{aligned} & p(\Lambda = \lambda | D = d) \quad \text{(spektral)} \quad , \\ & p(X = x | D = d) \quad \text{(räumlich)} \quad , \\ \text{und} \quad & p(T = t | D = d) \quad \text{(zeitlich)} \quad . \end{aligned} \tag{4.5}$$

Auf Grund der vorliegenden Messungen wird hier eine Vereinfachung in der weiteren Berechnung vorgenommen: Für jede Diode wurden die Verteilungen (4.5) jeweils in *einzelnen* Freiheitsgraden gemessen. Eventuelle Abhängigkeiten der Verteilungen einer Diode in X, T und Λ können also nicht betrachtet werden.

Durch die Ansteuerung der Laserdioden ist es beispielsweise aber wahrscheinlich, dass die spektralen Eigenschaften der Photonen aus einer Laserdiode abhängig vom Emissionszeitpunkt sind, da der Strom durch die Laserdiode während der Pulsdauer nicht konstant, also kein Rechtecksignal ist. Vielmehr steigt er zu Beginn steil an, und fällt dann wieder ab, so dass der Emissionszeitpunkt bestimmt, bei welchem Laserdiodenstrom ein Photon erzeugt wurde. Da jedoch eine gleichzeitige Messung der Freiheitsgrade mit den zur Verfügung gestandenen Messgeräten nicht möglich war, wird hier die Näherung unabhängiger Verteilungen betrachtet.

In diesem Fall ergeben sich weitere Vereinfachungen. So gilt für die Verbundwahrscheinlichkeit $p(A, B)$ unabhängiger Zufallsvariablen:

$$p(A, B) = p(A)\, p(B) \qquad ; A, B \text{ unabhängig} \tag{4.6}$$

weshalb hier

$$p(\lambda, x, t|d) = p(\lambda|d)\, p(x|d)\, p(t|d) \tag{4.7}$$

gelten soll.

Für die Berechnung der wechselseitigen Information zwischen Messung und verwendeter Basis benötigt man jedoch die durch die Basen $b \in B$ bedingten

Wahrscheinlichkeiten, die sich durch Summation ergeben:

$$p(\lambda, x, t|B = b) = {}^1\!/_4 \sum_{d \in b} p(\lambda, x, t|d) \tag{4.8}$$

Der Faktor ${}^1\!/_4$ sorgt für die neue Normierung, hier sind jeweils vier Dioden einer Basis zugeordnet. Die gesuchte wechselseitige Information $I(\Lambda, X, T : B)$ kann dann mit (4.4) als

$$\begin{aligned} I(\Lambda, X, T : B) &= H(B) - H(B|\Lambda, X, T) \\ &= 1 + \sum_{\lambda,x,t} p(\lambda, x, t) \sum_{b} p(b|\lambda, x, t) \log_2 p(b|\lambda, x, t) \end{aligned} \tag{4.9}$$

geschrieben werden, wobei von einer Gleichverteilung der beiden verwendeten Basen ausgegangen wird: $p(HV) = p(\pm 45) = {}^1\!/_2$. Der Satz von Bayes

$$p(B|A) = \frac{p(B)}{p(A)}\, p(A|B) \tag{4.10}$$

für zwei Zufallsgrößen A und B erlaubt das Einsetzen der gemessenen Verteilungen in (4.9):

$$I(\Lambda, X, T : B) = 1 + \sum_{\lambda,x,t} \sum_{b} p(b) p(\lambda, x, t|b)\ \log_2 \left(\frac{p(b) p(\lambda, x, t|b)}{p(\lambda, x, t)} \right) \tag{4.11}$$

Dabei ist $p(\lambda, x, t)$ die Wahrscheinlichkeit, ein Photon mit diesen Parametern zu finden. Die wechselseitige Information einzelner Messungen berechnet sich analog, deren Summe ist unter Umständen jedoch kleiner als die insgesamt offenbarte Information:

$$I(\Lambda : B) + I(X : B) + I(T : B) \leq I(\Lambda, X, T : B) \tag{4.12}$$

Der Grund für diese Subadditivität erklärt sich wie folgt: Wenn einem Angreifer alle drei Messungen gleichzeitig zur Verfügung stehen, kann er Dioden, die in den einzelnen Freiheitsgraden nicht zu unterscheiden sind, eventuell trotzdem auflösen, da die messbaren Charakteristika immer über die Diode verknüpft sind. Letztlich erhält er also auch mehr Information über die Basis. Bestehen keine Korrelationen zwischen den Dioden und den verschiedenen Freiheitsgraden, so ist auch kein zusätzlicher Informationsgewinn aus der Kenntnis aller drei Parameter möglich und es gilt das Gleichheitszeichen.

Für die Messdaten aus den Abschnitten 4.3.2–4.3.4 ergeben sich, einzeln und in Kombination (im Sinne von Gl. (4.12)), die Werte der wechselseitigen Information wie in Tabelle 4.3 aufgelistet. Die Wellenläge oder der Emissionszeitpunkt sind in ihrem Informationsgehalt über die Basis etwa gleichwertig. Die Messung des räumlichen Freiheitsgrades hingegen liefert um zwei Größenordnungen weniger Information über das gesendete Bit. Dies entspricht gerade den Erwartungen für die räumliche Ununterscheidbarkeit nach einer Singlemode-Faser.

Tabelle 4.3: Wechselseitige Information jeweils der Basis mit den Messungen des räumlichen, zeitlichen und spektralen Freiheitsgrades, sowie die simulierte wechselseitige Information bei Verwendung eines Interferenzfilters mit einer Breite von 0,8 nm.

		wechsels. Information (Bit)
spektral	$I(\Lambda : B)$	0,001436
(mit simuliertem Interferenzfilter		0,000725)
zeitlich	$I(T : B)$	0,001247
räumlich	$I(X : B)$	0,000027
gemeinsam	$I(\Lambda, X, T : B)$	0,002836

Mit der spektralen Messung aus 4.3.4 lässt sich zudem der zu erwartende Informationsverlust an einen Angreifer, bei Verwendung eines engen Interferenzfilters (FWHM 0,8 nm), abschätzen. Dazu werden die Spektren der Dioden mit der Transmissionsfunktion des Filters multipliziert und neu normiert. In diesem Fall ist die wechselseitige Information $I(B : \Lambda)$ etwa auf die Hälfte reduziert (siehe Tab. 4.3). Eine vollständige Auslöschung der Unterscheidbarkeit durch den Filter ist nicht zu erwarten, da die Spektren in dessen Transmissionsbereich teilweise signifikant asymmetrisch sind. Dies führt auch für die gefilterten Photonen zu einer spektralen Verschiebung der Zentralwellenlänge.

Die Berechnung der wechselseitigen Information erfolgt hier mit diskreten Summen. Eine alternative Vorgehensweise besteht im Übergang zu Integralen, nachdem die Messungen mit geeigneten Modellen stetig beschrieben wurden. In diesem Fall sind zunächst höhere Werte von I zu erwarten. Spezielle Charakteristika einzelner Dioden können unter Umständen jedoch bei der Modellierung nicht wiedergegeben werden, so dass diese Unterscheidbarkeiten nicht in die Rechnung mit eingehen und die wechselseitige Information zu niedrig ausfällt. Die Entscheidung für die Berechnung anhand der Summen begründet sich deshalb auf die starke Abweichung der Messkurven von analytischen Modellfunktionen.

Der Wert der wechselseitigen Information, wie er in Tabelle 4.3 aufgeführt ist, muss im Rahmen der *privacy amplification* berücksichtigt werden. Nimmt man im schlimmsten Fall an, Eve hat nicht nur 0,28 Bit Information über jedes Bit des gesamten Schlüssels, sondern kennt genau 0,28 % der Schlüsselbits, also ihre Position im Schlüssel und deren Wert, so kann das Modell von GLLP angewendet werden. Man betrachtet also die 0,28 % als im Sinne von GLLP *markiert* und addiert den Wert der wechselseitigen Information zu Δ in Gleichung (3.26), wobei, wiederum zu Gunsten der Sicherheit, angenommen wird, dass nur die Einzelphotonpulse die Seitenkanalinformation tragen. Tatsächlich stellt sich aber heraus, dass der Anteil der Multiphotonpulse am Informationsverlust mit $\Delta \approx 0{,}15$ um zwei Größenordnungen höher ist als $I(\Lambda, X, T|B)$, dass also die potentiellen Informationsverluste über die

behandelten Seitenkanäle hier vernachlässigbar gering sind.

4.3.6 Polarisation der gesendeten Zustände

Anders als die oben charakterisierten Ungenauigkeiten des Senderaufbaus führt die tatsächlich emittierte Polarisation der einzelnen Laserdioden nicht zu deren Unterscheidbarkeit, sie kann jedoch verantwortlich für eine ungleich gewichtete Verteilung von 0- und 1-Werten im Schlüssel verantwortlich sein. In erster Linie haben Abweichungen aber Übertragungsfehler, also eine höhere QBER zur Folge. Ein Photon, dessen Polarisation um den Winkel α vom Sollwert abweicht, wird bei der Polarisationsanalyse mit der Wahrscheinlichkeit $\sin^2(\alpha)$ falsch zugeordnet.

Fehler in der Polarisation entstehen durch geringfügig verdreht eingebaute Dioden, sowie durch schlechte Kompensation der Glasfaser, die als Modenfilter dient. Erstere führen zu einer abweichenden Polarisation einzelner, letztere zu zirkularen Anteilen in den Pulsen aller Dioden[2]. Beide Effekte verringern den Kontrast der Polarisationsanalyse. Eine Messung der Polarisation der acht Dioden liefert hier die genauen Werte und erlaubt, diesen Beitrag zur QBER abzuschätzen.

Der Messaufbau besteht aus dem Alice-Modul, einem Polarisator in einer motorisierten Rotationsstufe und einer APD, auf die der Strahl fokussiert wird. Für jede Diode wird die Zählrate in Abhängigkeit von der Stellung des Analysators gemessen. Die Werte werden in Schritten von 1,5 ° über einer vollen Umdrehung aufgenommen. Das normierte Ergebnis ist in Abbildung 4.17 zu sehen.

Um den Kontrast zwischen Minimum und Maximum jeder Diode zu ermitteln, sind die Extrema der Messkurven lokal mit Parabeln genähert. Auf diese Weise erhält man einen interpolierten Messwert am Ort des 45 °-Rasters. Nur dort ist der Kontrast relevant, da später der (ideale) Analysator (Empfänger) in dieser Basis arbeitet. Die so gewonnenen Werte sind in Tabelle 4.4 aufgelistet.

[2] Drehungen in der H/V-Ebene der Blochkugel können durch das motorisierte $\lambda/2$-Wellenplättchen automatisch ausgeglichen werden.

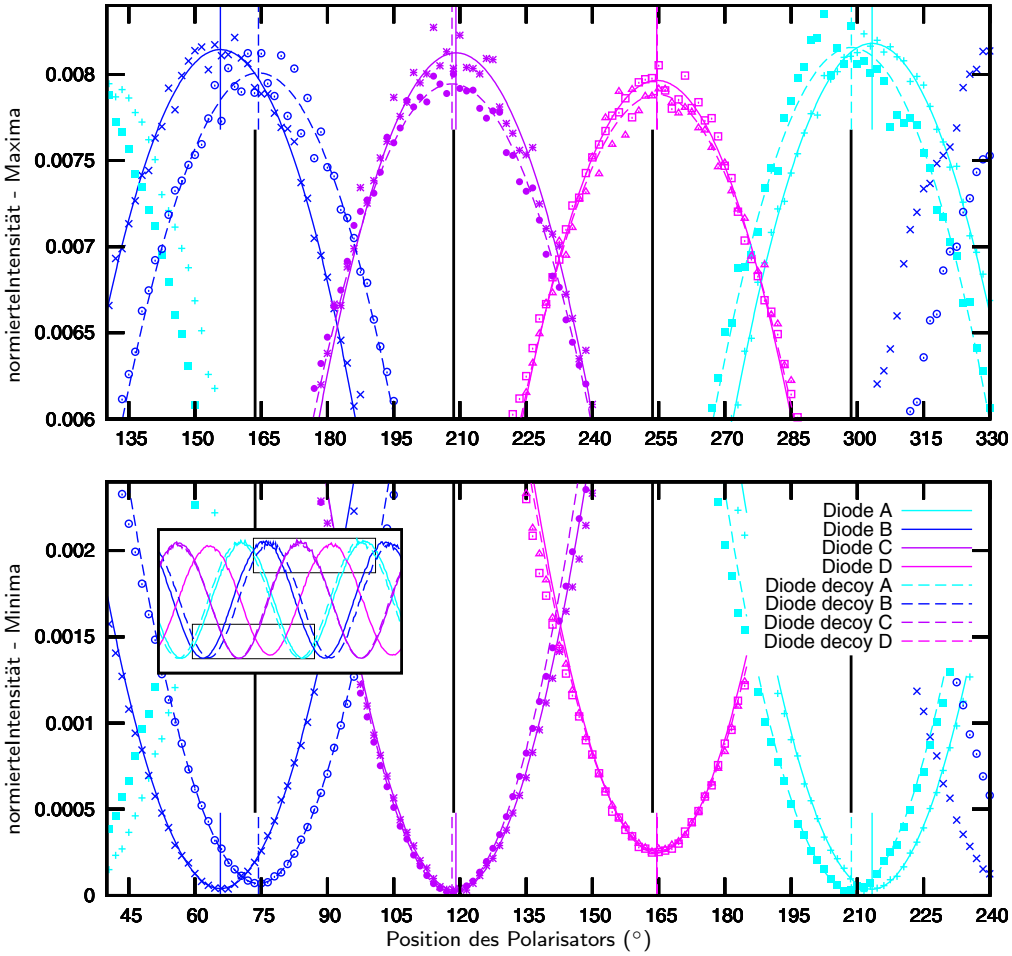


Abb. 4.17: Normierte Messung der emittierten Polarisation der acht Sendedioden (Hintergrund abgezogen). Im Fenster ist die vollständige Messung zu sehen, oben der Ausschnitt der Maxima und unten die zugehörigen Minima. Die Extrema sind jeweils mit Parabeln genähert um den tatsächlichen Extremwert und dessen Position zu ermitteln. In schwarz ist das theoretische 45 ° Raster markiert, auf dem alle Extrema liegen sollten. An diesen Positionen wird der interpolierte Wert zur Bestimmung des Kontrastes in Tabelle 4.4 ermittelt.

Tabelle 4.4: Winkel der Polarisation der Sendedioden sowie die Abweichung vom Sollwinkel aus der Messung in Abbildung 4.17. Das 45 °-Raster dort ist gerade so gewählt, dass hier eine mittlere Abweichung von 0 ° resultiert, was dem Fall eines idealen Empfängers entspricht, der die hier aufgelisteten Kontraste beobachtet.

Diode	Position des Minimums (Grad)	Abweichung von Sollpolarisation (Grad)	Kontrast
A	213,3	4,7	0,977
B	65,8	−7,8	0,952
C	119,1	0,5	0,993
D	164,6	1,0	0,939
Decoy A	208,7	0,1	0,992
Decoy B	74,4	0,8	0,982
Decoy C	118,2	−0,4	0,995
Decoy D	164,7	1,1	0,936
Mittelwert		0,0	0,971

5

Der Empfänger

Der Empfänger hat die Aufgabe einen möglichst großen Teil der gesendeten Qubits einer Polarisationsanalyse, zufällig in einer der beiden Basen, zuzuführen. So muss das Empfangsteleskop einerseits möglichst effektiv alle Photonen des Senders auffangen, andererseits darf nicht zu viel Licht aus anderen Quellen auf die Detektoren gelangen damit die Hintergrundzählrate klein bleibt.

Um Beiträge von Streulicht zu begrenzen erfolgt deshalb eine räumliche Filterung mittels einer Lochblende. Diese hat einen Durchmesser von 100 µm und befindet sich im Fokus des Teleskops. Weiter werden die Photonen bereits im Teleskop spektral gefiltert. Dies geschieht durch einen Interferenzfilter mit einer Breite von 10,9 nm (FWHM) und einer Transmission bei $\lambda = 850\,\text{nm}$ von 83,7 % (siehe Abb. 6.4). Die Photonen, die die Lochblende passiert haben, werden mit einer weiteren Linse auf die Detektoren im Bobmodul abgebildet. In diesem Modul wird zufällig eine der Basen gewählt und die Polarisation analysiert.

Der Aufbau ist weitgehend analog zu den Experimenten in [66]. Deshalb soll hier nur eine knappe Beschreibung und Dokumentation der Unterschiede erfolgen. Ähnlich wie für den Sender in 4.3.6, wird auch hier der Kontrast, nun aber der Polarisationsanalyse, bestimmt. Ein weiterer Beitrag zur gesamten QBER kann so quantifiziert werden.

5.1 Bobmodul

Die Detektion der Photonen im Bobmodul erfolgt durch APDs, die bei $-14\,^{\circ}\text{C}$ arbeiten. Die niedrige Temperatur ist notwendig, um die Dunkelzählrate klein zu halten. Der genaue Wert jedoch ist ein Kompromiss aus akzeptabler Dunkelzählrate und der Leistungsfähigkeit des Kühlsystems. Dieses arbeitet mit Peltierelementen und Luftkühlung, weshalb die Leistung auch von der Umgebungstemperatur abhängt. Der eingestellte Wert von $-14\,^{\circ}\text{C}$ kann über weite Bereiche (von unter $0\,^{\circ}\text{C}$ bis mindestens $30\,^{\circ}\text{C}$) der Außentemperatur gehalten werden und ermöglicht eine niedrige

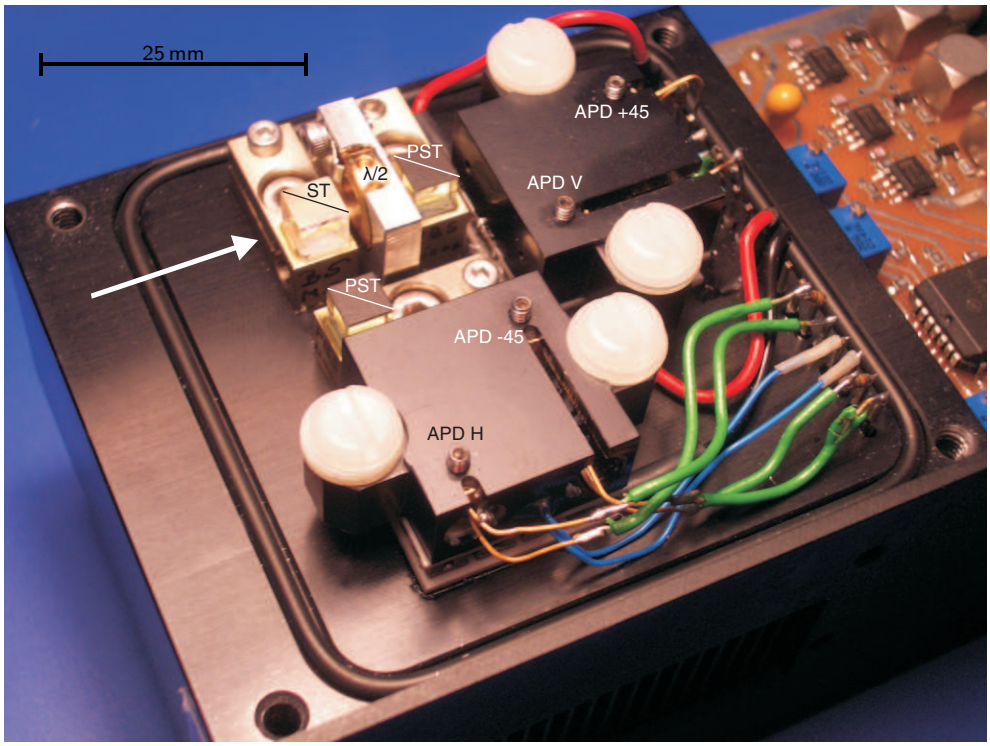


Abb. 5.1: Bobmodul geöffnet, der Pfeil markiert die Eintrittsachse. Der Strahlteiler (ST) wählt die Basis ($\{|H\rangle, |V\rangle\}$ oder $\{|+45\rangle; |-45\rangle\}$), das Halbwellenplättchen in einem Zweig dreht die Polarisation dort um 45 °. Dann kommen zwei gleiche Polarisationsanalysen mit je einem polarisierenden Strahlteiler (PST) und zwei APDs.

Dunkelzählrate im Bereich von unter $1000\,\mathrm{s}^{-1}$ pro Kanal. Die Detektionseffizienz der APDs hängt hingegen kaum von der Temperatur ab, sie wird vielmehr durch die Vorspannung in Sperrrichtung beeinflusst, die jedoch spezifisch für jede Temperatur eingestellt werden muss (siehe Anhang A).

Damit möglichst wenig Hintergrundlicht in die APDs gelangt, ist die Anordnung in einem lichtdichten Gehäuse untergebracht. Dieses ist zudem luftdicht, da sich sonst durch ständige Kondensation an den kalten Bauteilen Wasser im Inneren sammeln würde.

Die Photonen werden nach dem Raumfilter von einer Linse in das Bobmodul fokussiert. Dort treffen sie zuerst auf einen Strahlteiler an dem die zufällige Entscheidung für eine Basis, $\{|H\rangle, |V\rangle\}$ oder $\{|+45\rangle; |-45\rangle\}$, erfolgt. Die reflektierten Strahlen werden an einem polarisierenden Strahlteiler in der Basis $\{|H\rangle, |V\rangle\}$ analysiert und von zwei APDs an dessen Ausgängen registriert. Die Polarisationen der transmittierten Photonen wird zunächst von einem Halbwellenplättchen um 45° gedreht, $\{|+45\rangle; |-45\rangle\}$ wird damit zu $\{|H\rangle, |V\rangle\}$, bevor sie in einer identischen Konfiguration aus polarisierendem Strahlteiler und zwei APDs analysiert werden. Die Entscheidung am Strahlteiler ist für jedes Photon im Sinne der Quantenmechanik

zufällig. Anhand der APD, die das Photon registriert hat, kann Bob aber auf die „gewählte“ Basis schließen.

Alle drei Strahlteilerwürfel sind geringfügig verkipp- und drehbar, damit alle vier APDs möglichst gleichmäßig beleuchtet werden können. Nur so kann später die maximale Empfindlichkeit jeder der vier APDs, durch Positionieren des gesamten Empfängers, auf den Sender gerichtet werden.

Die Elektronik im Bobmodul liefert die Hochspannungen für den Betrieb der vier APDs und formt den elektrischen Puls eines Detektionsereignisses zu logikkompatiblen Signalen. Auch die Steuerung der Peltierelemente zur Temperaturregelung der APDs ist bereits integriert.

Unterschiedliche Detektionswahrscheinlichkeiten der einzelnen APDs können Ursache eines weiteren Seitenkanals sein, gleiches gilt, wenn diese zeitlich nicht für alle vier Dioden übereinstimmen [73]. Im Extremfall könnte Bob in bestimmten Zeitfenstern blind für den Wert 1 sein, während zu anderer Zeit die Detektionswahrscheinlichkeit für ein Photon das den Wert 0 überträgt verschwindet. In dieser Situation kann Eve Photonen, je nach ihrem Wert, zu Zeitpunkten senden, bei denen die Wahrscheinlichkeit für das Auftreten eines Fehlers minimiert wird und so die QBER, die aus ihrem Angriff resultiert deutlich senken. Eine Messung, die diesen Seitenkanal quantifiziert, steht hier noch aus.

5.2 Überblick Gesamtaufbau

Genau wie beim Sender kommt hier ein 64 Bit Computer zum Einsatz. Auch die verwendeten Schnittstellen sind sehr ähnlich. Ein Blockdiagramm des elektronischen Aufbaus findet sich in Abbildung 5.1.

Die vom Bobmodul erfassten Photonen, werden als elektrische Impulse von einer externen Zeitstempel-Elektronik (*timestamp unit*) eingelesen. Diese stellt für jedes Detektionsereignis des Bobmoduls einen Eintrag, bestehend aus APD-Nummer und Detektionszeitpunkt, in einem FIFO-Speicher zur Verfügung. Die Synchronisation von Sender und Empfänger erfolgt erst auf Programmebene im Computer. Die genaue Funktionsweise ist in [66] beschrieben und beruht auf einer Fourieranalyse zur Bestimmung der Taktfrequenz und -phase, und auf der Identifikation von pseudozufälligen Bitmustern, die im Kopf jedes Datenblocks gesendet werden.

5.3 Polarisationsmessung im Empfänger

Die Photonen, die den Empfänger erreichen, müssen jeweils in einer von zwei orthogonalen Basen, die um 45 ° gegeneinander verdreht sind, analysiert werden. Die polarisierenden Strahlteiler, sowie die APDs können jedoch in diesem kompakten Aufbau nicht in allen Freiheitsgraden positioniert bzw. gedreht werden. Das führt dazu, dass die Trennung der Polarisation unter Umständen nicht vollständig oder

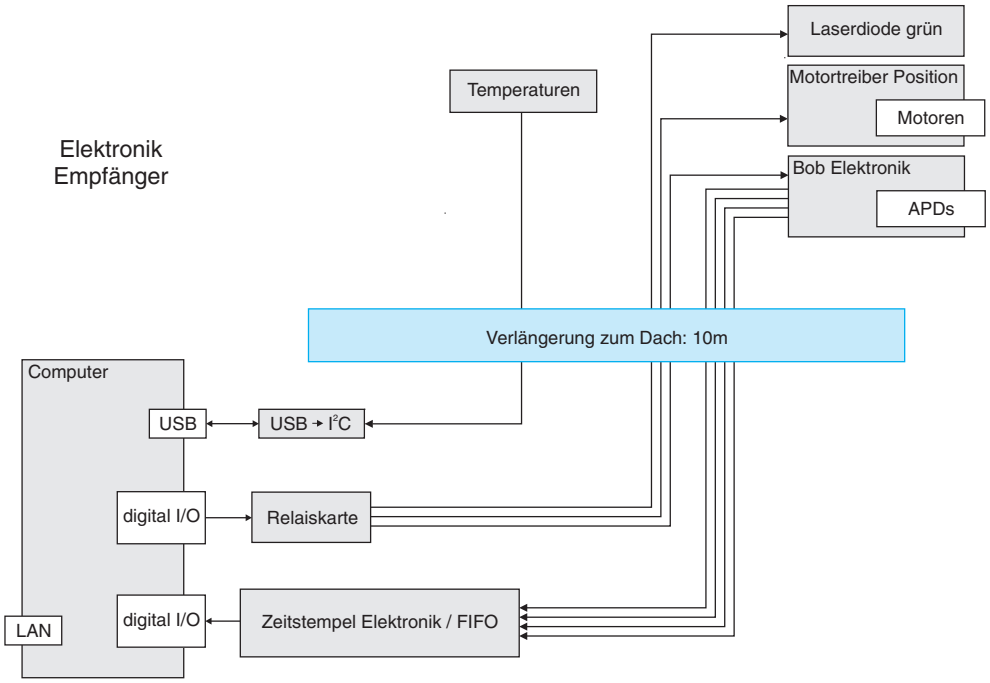


Abb. 5.2: Blockdiagramm der gesamten Empfangselektronik.

Tabelle 5.1: Winkel der Polarisationsanalyse für die vier APDs, sowie die Abweichung vom Sollwinkel aus der Messung in Abbildung 5.3. Das 45 °-Raster in 5.3 ist gerade so gewählt, dass hier eine mittlere Abweichung von 0 ° resultiert, was dem Fall eines idealen Senders entspricht, der exakte polarisierte Photonen versenden kann.

Diode	Position des Minimums (Grad)	Abweichung von Sollposition (Grad)	Kontrast
A	210,6	−1,0	0,972
B	77,3	0,7	0,987
C	166,9	0,3	0,976
D	121,6	0,0	0,986
Mittelwert		0,0	0,980

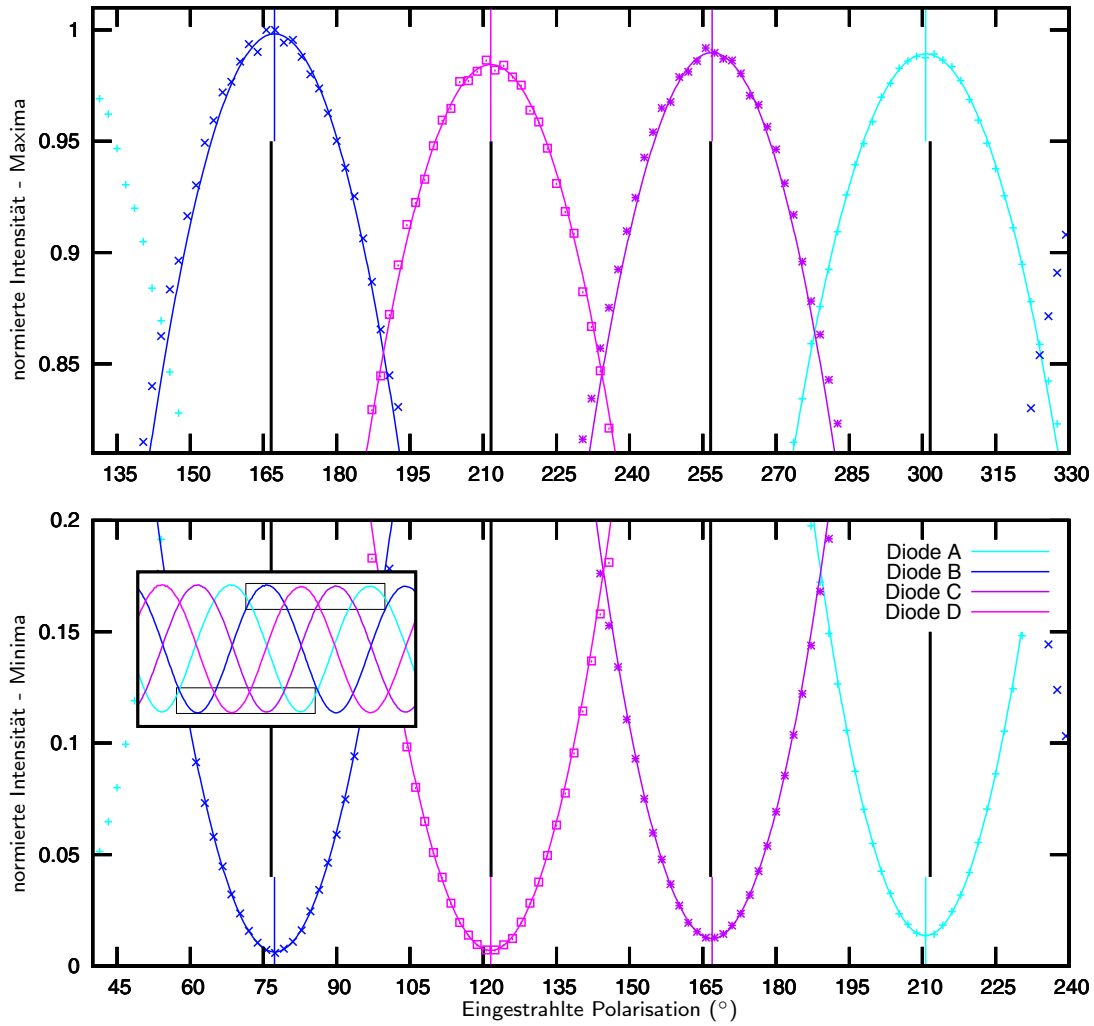


Abb. 5.3: Normierte Messung der detektierten Zählrate des Bobmoduls aufgetragen gegen die eingestrahlte Polarisation, Hintergrund abgezogen. Im Fenster ist die vollständige Messung zu sehen, oben der Ausschnitt der Maxima und unten die zugehörigen Minima. Die Extrema sind jeweils mit Parabeln gefittet, um den tatsächlichen Extremwert und dessen Position zu ermitteln. In schwarz ist das theoretische 45 °-Raster markiert. An diesen Positionen wird der interpolierte Wert zur Bestimmung des Kontrastes in Tabelle 5.1 ermittelt.

in einer geringfügig verkippten Basis erfolgt. Nicht zuletzt arbeiten die polarisierenden Strahlteiler nicht perfekt und auch der normale Strahlteiler kann, wenn er Polarisationsabhängigkeiten aufweist, Fehler induzieren. Dies wurde, schon für kleine Winkelabweichungen von der Eintrittsachse senkrecht zum Eintrittsfenster, bei der folgenden Messung beobachtet. Schließlich muss auch die Position des Halbwellenplättchens überprüft werden, eine Ungenauigkeit führt sonst zu einen Fehler im Winkel zwischen den beiden Basen.

Um die Anordnung in dieser Hinsicht zu prüfen und die zu erwartende QBER zu bestimmen, wird eine Messung durchgeführt, die der für die Polarisationen der gesendeten Photonen in 4.3.6 gleicht. Dazu wurde das Licht einer Laserdiode, nach einem Polarisator und einem Halbwellenplättchen in einer motorisierten Rotationsstufe, von einer Linse auf die Detektoren des justierten Bobmoduls fokussiert. Programmgesteuert konnten für alle eingehenden Polarisationen in Schritten von 0,9 ° die Zählraten der vier Detektoren aufgenommen werden.

Das Ergebnis ist in Abbildung 5.3 zu sehen. Aus den Daten wird für jede Diode der Kontrast zwischen den Zählraten bei der „richtigen“ (H bei APD H, +45 bei APD +45, etc.) und der dazu orthogonalen Polarisation ermittelt. Man erhält so ein Maß für den Anteil der Photonen, die richtig analysiert werden, nachdem sie an Bobs Strahlteiler der Analyse in der „richtigen“ Basis zugeführt wurden.

5.4 Abschätzung Gesamt-QBER

Der, ohne Angreifer zu erwartende Bitfehler nach dem Sifting (QBER) ist durch abweichende Polarisationen der Photonen von Alice, sowie durch fehlerhafte Polarisationsanalyse und Dunkelzählereignisse bei Bob begründet. Der Hintergrund, der vom Sender erzeugt wird, soll zusammen mit der Dunkelzählrate des Empfängers behandelt werden.

Die QBER selbst ist zunächst für einen einzelnen Detektor definiert und wird für den Gesamtwert addiert. Betrachtet man den Detektor für einen Zustand $|\alpha\rangle$ und sendet auch diesen Zustand, so berechnet sich die QBER aus dessen Zählrate $n(|\alpha\rangle)$ und der des Detektors für die orthogonale Polarisation $n^{\perp}(|\alpha\rangle)$:

$$\mathrm{QBER}_{|\alpha\rangle} = \frac{n^{\perp}(|\alpha\rangle)}{n(|\alpha\rangle) + n^{\perp}(|\alpha\rangle)} \tag{5.1}$$

Sind alle Detektoren gleich effizient, so kann die Näherung $\mathrm{QBER} = (1 - V)/2$ mit dem Kontrast V (*visibility*, Werte in den Tab. 4.4 und 5.1) verwendet werden.

Werden keine Pulse gesendet, so beobachtet man etwa $3000\,\mathrm{s}^{-1}$ Detektionsereignisse des Empfängers (Summe über vier APDs), die mit einer nominellen zeitlichen Auflösung von etwa 0,1 ns im Computer registriert werden. Die Zeit von einem Puls zum nächsten (100 ns) wird von der Zeitstempel-Elektronik in 1024 Intervalle geteilt, in denen ein Ereignis stattfinden kann. Im Rahmen der zeitlichen Filterung

werden dann alle Detektionen verworfen, die außerhalb eines Fensters von $\pm 2\,\mathrm{ns}$ (± 20 Intervalle) liegen. Ein zufälliges Dunkelzählereignis wird also nur mit einer Wahrscheinlichkeit von $p = {}^{40}/_{1024}$ verwendet, und verursacht dann auch nicht in jedem Fall einen Fehler. Dazu muss es in der richtigen Basis und dort im falschen Detektor auftreten, was einen weiteren Faktor ${}^{1}/_{4}$ bedeutet (vgl. Abb. 3.1). Die Fehlerrate aus Dunkelzählrate beträgt also etwa $30\,\mathrm{s}^{-1}$, was gegenüber einer absoluten Zählrate bei Bob von $10^5\,\mathrm{s}^{-1}$ also zu vernachlässigen ist.

Die Beiträge des Senders und des Empfängers zur QBER ergeben sich aus den Messungen, die in den Abbildungen 4.17 und 5.3 dargestellt sind. Mit der Definition (5.1) findet man, jeweils über die Dioden bzw. APDs gemittelt:

$$\begin{array}{lcl} \mathrm{QBER}_{\mathrm{Sender}} & = & 1{,}5\% \\ \mathrm{QBER}_{\mathrm{Empfänger}} & = & 1{,}0\% \\ \hline \mathrm{QBER} & \leq & 2{,}5\% \end{array} \tag{5.2}$$

Diese Fehler sind jedoch unter Laborbedingungen gemessen. Vor allem die Kompensation der Glasfaser ist aber im Freien langfristig nicht perfekt und auch die möglicherweise unvollkommene Anpassung der Basen von Alice und Bob geht in (5.2) noch nicht mit ein. Weiter ist die Analysequalität des Bobmoduls stark vom Einfallswinkel, bezogen auf die Normale des Eintrittsfensters, abhängig. Die Montage an das Teleskop kann also noch zusätzliche QBER verursachen, wenn dort Abweichungen auftreten. Im Betrieb auf dem Dach ist deshalb mit einem signifikant höheren Fehler zu rechnen.

6

Installation des Systems und erste Schlüsselerzeugung

Das vorliegende Experiment demonstriert die Stärken eines freiraumoptischen QKD-Systems im Betrieb unter realen Bedingungen. Von Dach zu Dach wird zwischen zwei Gebäuden der Universität Schlüssel ausgetauscht. Ohne Leitungen oder Glasfasern verlegen (oder mieten) zu müssen, können zwei Parteien die unbedingte Sicherheit von quantenkryptographischen Methoden nutzen. Dabei wird hier für den klassischen Kanal auf das bestehende Intranet zurückgegriffen. Im Allgemeinen ist aber jede Datenverbindung verwendbar. Konventioneller optischer Richtfunk bietet sich jedoch an, da ohnehin eine Sichtverbindung besteht und die QKD-Sender und -Empfänger mit den klassisch arbeitenden Geräten in jeweils eine Einheit auf beiden Seiten zusammengefasst werden können.

Erste Tests des QKD-Systems wurden noch auf einer Distanz von etwa 50 m unter „Laborbedingungen“ im Hausgang gemacht. So konnten vor allem die elektronischen Baugruppen und die Software getestet werden. Erst dann folgte die Installation von Sender und Empfänger auf den beiden Dächern. Im Abstand von 500 m stehen dafür zwei Gebäude der Universität zur Verfügung, auf denen Strom- und Netzwerkanschluss vorhanden sind und die vor allem eine direkte Sichtverbindung erlauben. In Abbildung 6.1 erkennt man den Verlauf des Quantenkanals vornehmlich über Wohnhäuser hinweg. Um die Sichtverbindung herzustellen, musste der Sender allerdings etwa 80 cm erhöht montiert werden, so dass die Verbindungslinie jetzt nur sehr knapp über den Dächern liegt.

Sowohl der Sender- als auch der Empfängeraufbau können mit Mikrometerschrauben in zwei Achsen bewegt werden. Diese werden durch Schrittmotoren angetrieben. Das ist nötig damit ein automatischer und ferngesteuerter Betrieb möglich ist, andernfalls geht, durch thermische Ausdehnungen der Aufbauten sowie unter Umständen auch der Gebäude, die Verbindung schnell verloren. Die Konstruktion des Ausrichtungsmechanismus ist der in [66] sehr ähnlich, lediglich die Abmessungen

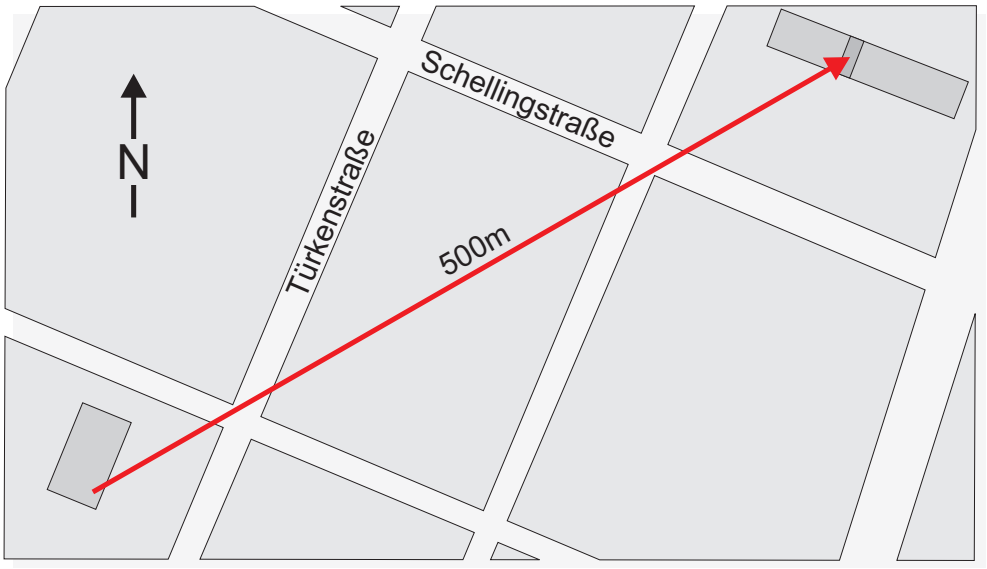


Abb. 6.1: Lage der QKD-Strecke auf dem Stadtplan. Der Ausschnitt befindet sich etwa 1 km nördlich des Stadtzentrums München.

und damit auch die Umrechnungsfaktoren von Motorschritten auf den Strahlversatz nach 500 m weichen ab (siehe Tab. 6.1).

Tabelle 6.1: Umrechnung der Motorbewegungen auf den Strahlversatz nach 500 m

	Sender		Empfänger	
	X	Y	X	Y
	(mm)	(mm)	(mm)	(mm)
Strahlversatz/Motorhalbschritt	1,8	1,6	0,69	0,60

Zunächst werden hier Messungen zu weiteren Merkmalen des Systems beschrieben, die nur im Freien problematisch sind, wie etwa die korrekte Arbeitsweise der Temperatursteuerungen, oder solche, die erst über die Distanz von 500 m zugänglich sind. Dazu gehören vor allem Eigenschaften der automatischen Ausrichtung von Sende- und Empfangsteleskop und damit verbunden die Effizienz der Übertragung für einzelne Photonen.

Danach werden erste Versuche zur Schlüsselerzeugung vorgestellt und die Leistung des Systems in Bezug auf die sichere Schlüsselrate bestimmt. Die Rate an Schlüsselrohdaten ist dabei nur *ein* Faktor. Entscheidend ist vor allem, wie viel Schlüssel nach der Aufbereitung verbleibt – ein wesentlicher Teil der Schlüsselrohdaten, abhängig von der QBER, muss für *privacy amplification* geopfert werden.

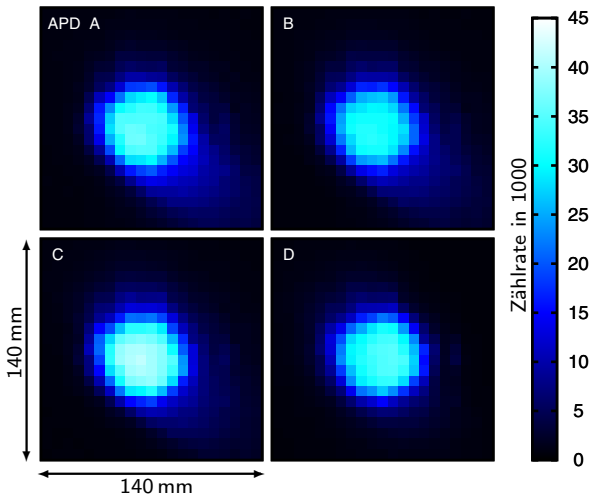


Abb. 6.2: Bild einer punktförmigen Lichtquelle am Ort des Senders, aufgenommen mit jeweils einer APD des Empfängers über die Distanz von 500 m. Die Abmessungen gelten am Ort des Senders.

6.1 Eigenschaften des optischen Kanals

Die maximale Übertragungsrate wird entscheidend durch die Anpassung und Ausrichtung der Teleskope beeinflusst. Darüber hinaus hat die Quanteneffizienz der Detektoren und die Abschwächung durch spektrale und räumliche Filterung großen Einfluss. Die Verluste in der Luft jedoch sind, ohne Niederschlag oder Nebel, meist zu vernachlässigen. In [31] findet sich eine Messung der Transmittivität von Luft. Für Licht der Wellenlänge 850 nm liegt diese nahe bei 1. Depolarisation ist, auch auf größeren Entfernungen, ebenfalls zu vernachlässigen [74].

6.1.1 Räumliche Charakteristik von Sender und Empfänger

Damit nicht systematisch Qubits verloren gehen, muss der Strahl des Senders auch nach 500 m einen kleineren Durchmesser aufweisen als das Teleskop des Empfängers. Eine Kontrollmöglichkeit bietet sich mit dem infraroten Ziellaser, der ebenfalls durch das Modenfilter geführt ist. So kann der Fokus des Senders schon grob angepasst werden[1]. Die Feineinstellung des Senderfokus bzw. der Anpassung der beiden Teleskope aneinander erfolgt später auf maximale Zählrate des Empfängers.

Der Öffnungswinkel des Empfängers kann durch die Fokussierung des Teleskops beeinflusst werden. Um maximale Unterdrückung des Umgebungslichts zu erreichen, sollen Photonen nur aus einem möglichst engen Kegel um die Verbindungslinie zum Sender in den Empfänger gelangen können. Diese Öffnung des Kegels kann im Querschnitt am Ort des Senders bestimmt werden, indem die Achse des Empfängers im Raster über eine punktförmige Lichtquelle neben dem Sendeteleskop bewegt wird.

[1] Der minimal erreichbare Strahldurchmesser liegt im Bereich von 25 mm, also deutlich unter der Öffnung des Empfangsteleskops von 75 mm.

Tabelle 6.2: Position und Verschiebung relativ zum gemittelten Zentrum der Bilder einer punktförmigen Lichtquelle am Ort des Senders, aufgenommen mit je einer APD des Empfängers. Die Daten entstanden aus der Messung in Abbildung 6.2.

APD	Position in X (mm)	Position in Y (mm)	Abstand vom Zentrum (mm)
A	0,1	−1,6	1,6
B	−0,4	−0,5	0,6
C	−1,3	0,6	1,5
D	1,6	1,5	2,2
Mittelwert:	0,0	0,0	1,5

Die Wendel von etwa 1,5 mm Länge einer kleinen Glühbirne wird für die Aufnahmen in guter Näherung einer punktförmigen Quelle genutzt. Durch Variation der Betriebsspannung lässt sich die Lichtmenge an die Empfindlichkeit des Empfängers anpassen. Die Rasteraufnahmen in Abbildung 6.2 entstanden so bei nur schwach glimmendem Glühfaden.

Anhand dieser Messung lässt sich auch feststellen, ob alle vier Detektoren aus Sicht des Senders zur Deckung kommen. Dazu sind in Tabelle 6.2 die Verschiebungen der vier Bilder gegeneinander aufgelistet. Die Werte wurden als Abweichung der Zentren jeweils eines Fits der Empfindlichkeit, d.h. der Zählrate, mit einer 2D-Gaußfunktion gewonnen[2]. Die geringen Abweichungen in Relation zum Durchmesser von $d = 32\,\mathrm{mm}$ (FWHM) zeigen, dass durch eine Bewegung des gesamten Empfängers auch wirklich alle vier APDs gleichzeitig auf den Sender ausgerichtet werden können.

6.1.2 Automatische Ausrichtung der Teleskope

Während des Betriebs der QKD-Strecke wird die Position ständig korrigiert, da sonst die Qualität der Verbindung schnell abfällt. Thermische Kontraktionen und Ausdehnungen im Aufbau des Senders, aber eventuell auch der Bauwerke, können im Abstand von 500 m einen Strahlversatz zur Folge haben. Gleiches gilt für den Empfänger. Die Korrektur geschieht automatisch nach einem Verfahren, bei dem sowohl die Achse des Senders als auch die des Empfängers laufend Kreise beschreiben. Aus der Zählrate beim Empfänger kann dann für beide eine Positionskorrektur berechnet werden. Dabei sind die Radien der Kreise flexibel: Ist die Zählrate konvergiert, werden sie verringert, fällt sie ab, werden sie wieder vergrößert. Wichtig ist, dass die Perioden für die beiden Kreisbewegungen keine gemeinsamen Teiler

[2] Die Verteilungen in Abbildung 6.2 weisen ein Überlappintegral mit der gemittelten Verteilung von jeweils $> 0{,}99$ auf.

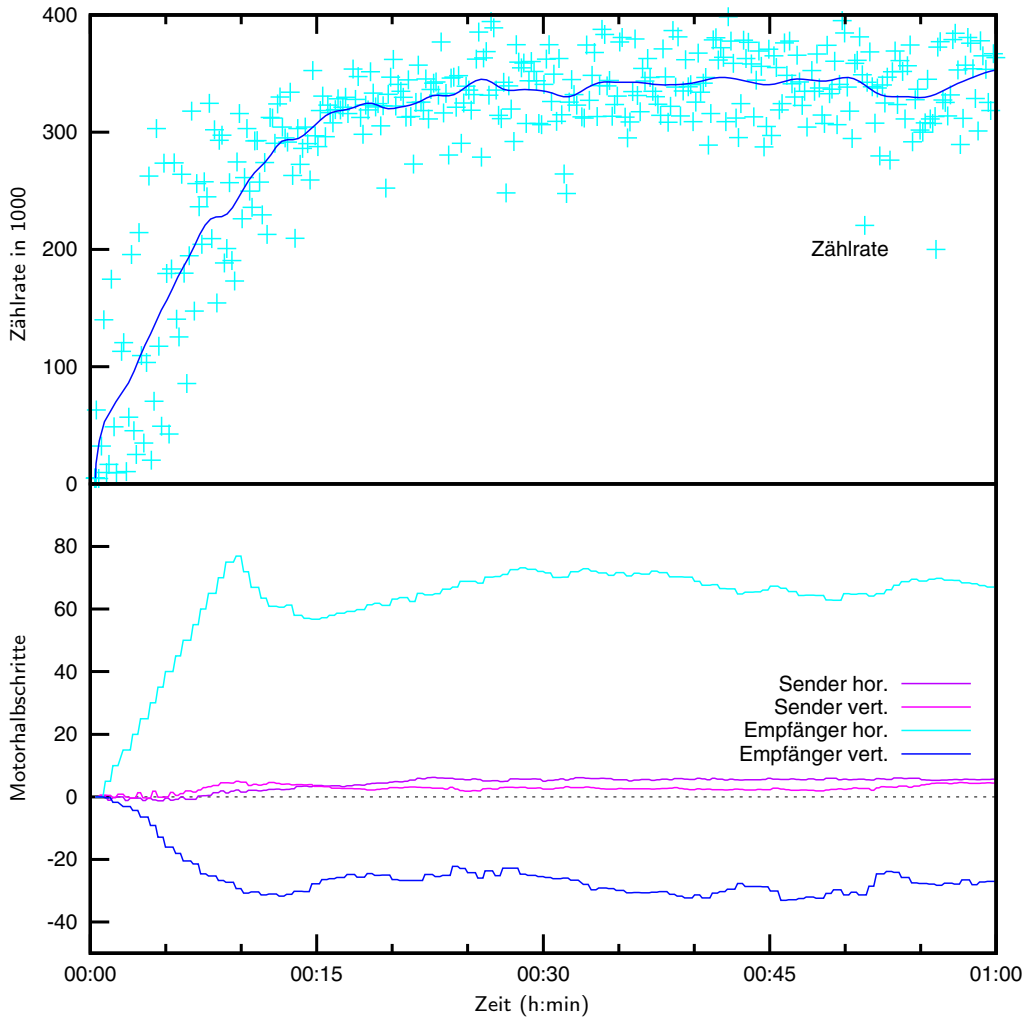


Abb. 6.3: Startphase eines Schlüsselaustauschs. Oben Zählraten, unten Ausrichtung der Teleskope, aufgetragen sind jeweils die Zentren, um die die maximale Zählrate auf kleinen Kreisen gesucht wird. Zu Beginn ist vor allem das Empfangsteleskop schlecht ausgerichtet. Die Motoren fahren deshalb mit maximal erlaubter Schrittgröße, wenn die Zählrate konvergiert, werden die Motorschritte kleiner und es erfolgen nur noch geringe Korrekturen.

haben und auch nicht zu nah beieinander liegen, da sich die Positionskorrekturen sonst nicht berechnen lassen [66].

In Abbildung 6.3 sind die ersten Minuten nach dem Start einer Verbindung zur Schlüsselerzeugung zu sehen. Die zu Beginn sehr niedrige Zählrate des Empfängers steigt schnell an während die Motoren die Teleskope ausrichten. Sind die richtigen Positionen erreicht, erfolgen nur noch kleine Korrekturen.

6.1.3 Transmission der Verbindung

Auf die tatsächliche Transmission haben alle Komponenten Einfluss, die zwischen der Kalibrierung der mittleren Photonenzahl pro Puls beim Sender und der Zeitstempelelektronik des Empfängers angeordnet sind. Im einzelnen sind das, abgesehen von der Abschwächung durch die Luft:

- im Sender ein Spiegel und die beiden Linsen des Teleskops,
- die beiden Teleskoplinsen des Empfängers,
- der Interferenzfilter,
- die Lochblende zur Raumfilterung und die Linse zur Abbildung auf die APDs,
- die Strahlteiler und das Wellenplättchen zur Polarisationsanalyse im Empfänger und
- die Detektionseffizienz der APDs.

Insgesamt wurde eine typische Abschwächung[3] bei günstigen Bedingungen im Bereich von 10 dB beobachtet. Davon entfällt für die beiden letzten Punkte ein Beitrag von zusammen 4 dB (siehe 4.1.3). Es kann also über die Entfernung von 500 m eines von vier Photonen erfolgreich eine der Detektorflächen erreichen, ohne in der Atmosphäre oder an einem der optischen Elemente absorbiert oder gestreut worden zu sein. Bei einer durchschnittlichen mittleren Photonenzahl pro Puls von $\mu = 0{,}16$ erreichen jede APD also gut 10^5 Photonen in jeder Sekunde. Im Bereich wesentlich höherer Zählraten sinkt jedoch die Effizienz von APDs, deren Lawinenstrom passiv gedämpft wird, weshalb eine weitere Verbesserung der Kopplung zwischen Sender und Empfänger oder auch eine höhere Repetitionsfrequenz nicht mehr zu größerer Schlüsselrate führen würde.

6.1.4 Tageslicht Tauglichkeit

Das QKD-System ist zum jetzigen Zeitpunkt nur zum Betrieb bei Dunkelheit geeignet. Bei Tageslicht sind die Detektoren im Empfänger schnell gesättigt. Die bestehende räumliche und spektrale Filterung ist noch nicht restriktiv genug. Um bei Tageslicht einzelne Photonen in den APDs differenzieren zu können, muss die Unterdrückung des Hintergrunds noch um einen Faktor von etwa 20 verbessert

[3] Als „gesamte Abschwächung“ soll hier das Verhältnis aus der berechneten Zahl von Photonen pro Puls wie in 4.3.1 × Repetitionsfrequenz und der Zahl, im Computer des Empfängers gezählter Pulse, bezeichnet werden.

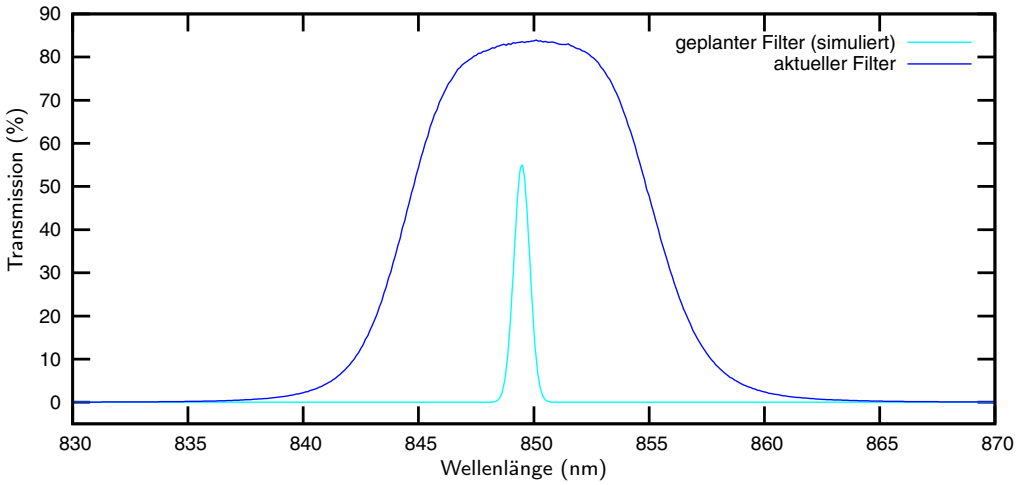


Abb. 6.4: Transmissionsmessung des spektralen Filters im Empfängeraufbau (blau). Transmission bei $\lambda = 850\,\text{nm}$: 83,7 %. Breite (FWHM): 10,9 nm. Cyan: simulierte Transmission des geplanten Filters mit einer Breite von 0,8 nm. Das Verhältnis der gesamten (integrierten) Transmissionen ist 17:1.

werden. Dazu ist der Einsatz eines Interferenzfilters mit einer Breite von 0,8 nm statt dem aktuellen Filter mit 10 nm Breite geplant, was die Hintergrundzählrate bereits etwa um einen Faktor 17 reduzieren sollte. Die Transmissionscharakteristik des aktuell verwendeten Filters ist, zusammen mit der Transmission des geplanten Filters (simuliert), in Abbildung 6.4 zu sehen.

Darüber hinaus wird aber in Zukunft auch eine aufwendigere räumliche Filterung erfolgen müssen, da diese im bestehenden System nur durch die *Kombination* aus Lochblende und Detektorfläche verwirklicht ist. Auf diese Weise gelangt auch Licht in das APD Gehäuse (wenn auch neben den Detektor), das von außerhalb des eigentlichen Sichtbereichs des Empfängers stammt, wie er in der Messung zu Abbildung 6.2 bestimmt wurde. Handelt es sich dabei nur um kleine Intensitäten, also bei Dunkelheit, stellt das kein Problem dar. Tagsüber jedoch, werden diese Photonen innerhalb des APD Gehäuses gestreut und können so doch auf die Detektorfläche gelangen. Abbildung A.1 zeigt eine APD, wie sie hier verwendet wird.

6.2 Wirksamkeit der Temperatursteuerungen

Für die korrekte Arbeitsweise des QKD-Systems sind die Temperaturen zweier Komponenten wesentlich: Die Temperatur des Glasfaser-Raumfilters im Sender (4.1.2) und die der APDs im Empfänger (5.1) sind mit Peltierelementen stabilisiert. Im ersten Fall ist die Polarisationskorrektur betroffen, im zweiten die Effizienz der Detektoren. Diese sinkt mit steigender Temperatur, wenn die Vorspannung in Sperrrichtung nicht angepasst wird.

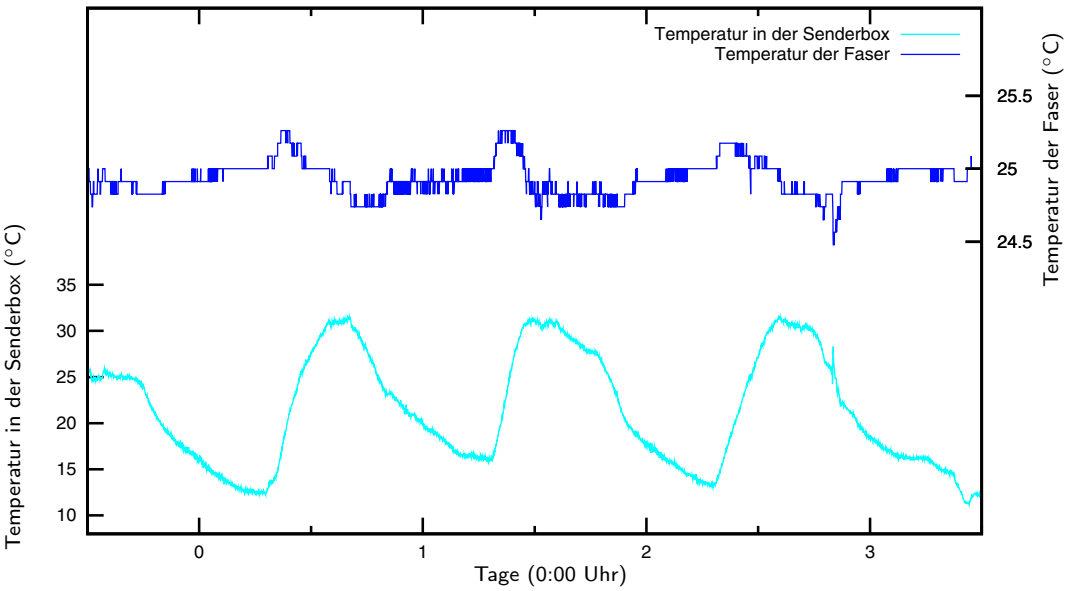


Abb. 6.5: Temperaturen der Glasfaser im Modenfilter des Senders, in Relation zur Temperatur in der Senderbox, gemessen über vier Tage.

Temperatur des Modenfilters

Nach den Erfahrungen aus den ersten Tests des Modenfilters im Labor war hier eine Genauigkeit von $\pm 1\,°C$ angestrebt, um eine stationäre Polarisationskompensation verwenden zu können. In Abbildung 6.5 sind die Messwerte der Fasertemperatur in Relation zur Temperatur in der Sender Box dargestellt. Die verbleibenden Schwankungen sind kleiner als $\pm 0{,}4\,°C$.

Die Regelungsungenauigkeiten sind besonders bei steilen An- oder Abstiegen der Außentemperatur ausgeprägt, was teilweise darauf zurückgeführt werden kann, dass für die Kontrollmessungen in Abbildung 6.5 ein zusätzlicher Temperaturfühler verwendet wurde. Dieser ist ebenfalls mit der Faser eingegossen, befindet sich aber nicht am exakt gleichen Ort, wie der Fühler der Temperatursteuerung.

Temperatur der APDs

Um eine gleichbleibend hohe Detektionseffizienz zu gewährleisten, muss die Temperatur der Detektoren des Empfängers auf einem konstant niedrigen Wert gehalten werden. Die Vorspannung wurde im Labor bei einer APD-Temperatur von $-14\,°C$ (siehe 5.1) jeweils 20 V über dem Wert eingestellt, bei dem die ersten Pulse direkt an der APD messbar sind. Die leichten Schwankungen der APD-Temperaturen mit der Außentemperatur, die man in Abbildung 6.6 sieht, haben keinen wesentlichen Einfluss auf die Effizienz und spiegeln das für reine Proportionalsteuerungen natürliche Verhalten wieder: Der Strom durch die Peltierelemente ist proportional der Differenz aus Temperatursoll- und istwert. Diese Differenz ist im Allgemeinen jedoch von null verschieden wenn sich das System im Gleichgewicht befindet, wenn also die

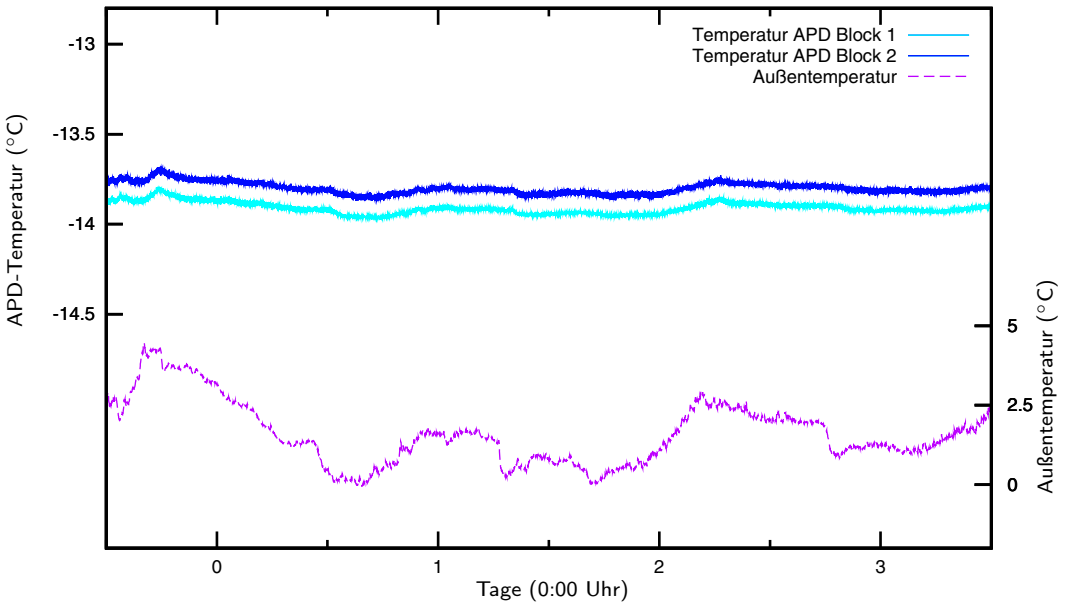


Abb. 6.6: Temperaturen der beiden APD-Blöcke des Empfängers, gemessen über vier Tage, zum Vergleich die Außentemperatur. Wie für eine Proportionalsteuerung zu erwarten (Kühlleistung $\propto$ Temperaturfehler), schwankt die APD-Temperatur leicht mit den Umgebungswerten.

aus dem Temperaturfehler resultierende Kühlleistung gleich den Wärmeeinträgen aus der Umgebung ist.

6.3 Erste Versuche zur Schlüsselübertragung

Die Schlüsselerzeugung lässt sich mit Programmen am Computer starten, steuern und überwachen. Neben einer zentralen Instanz, die die Synchronisation herstellt und aufrechterhält, werden von einem anderen Programm laufend die anfallenden Schlüsselrohdaten gesiftet. Die automatische Ausrichtung der Teleskope arbeitet eigenständig, indem sie die Gesamtzählrate maximiert. Die Programme sind im Rahmen von [66] erarbeitet worden und werden dort auch genauer erläutert.

Die Daten aus den übertragenen Qubits werden laufend gesiftet, wobei die verschiedenen Schlüsselraten ermittelt werden können. Neben der absoluten Zählrate, also der Zahl an Photonen, die Bob in jeder Sekunde registriert, ist die Rate gesifteten Schlüssels (*sifted key rate* SKR) relevant. Auch die QBER steht schon während der Übertragung zur Verfügung[4]. Die *sichere* Schlüsselrate nach *privacy amplification* wird noch nicht sofort ermittelt, kann aber nachträglich berechnet werden. Diese Werte sind in Abbildung 6.7 für mehrere Stunden eines typischen Schlüsselaustauschs dargestellt. Die Zählrate des Bobmoduls liegt bei etwa 2,5 $\times$

[4]Dazu steht ein spezieller Programm-Modus zur Verfügung, der zu Testzwecken die gesifteten Schlüssel sofort vergleicht.

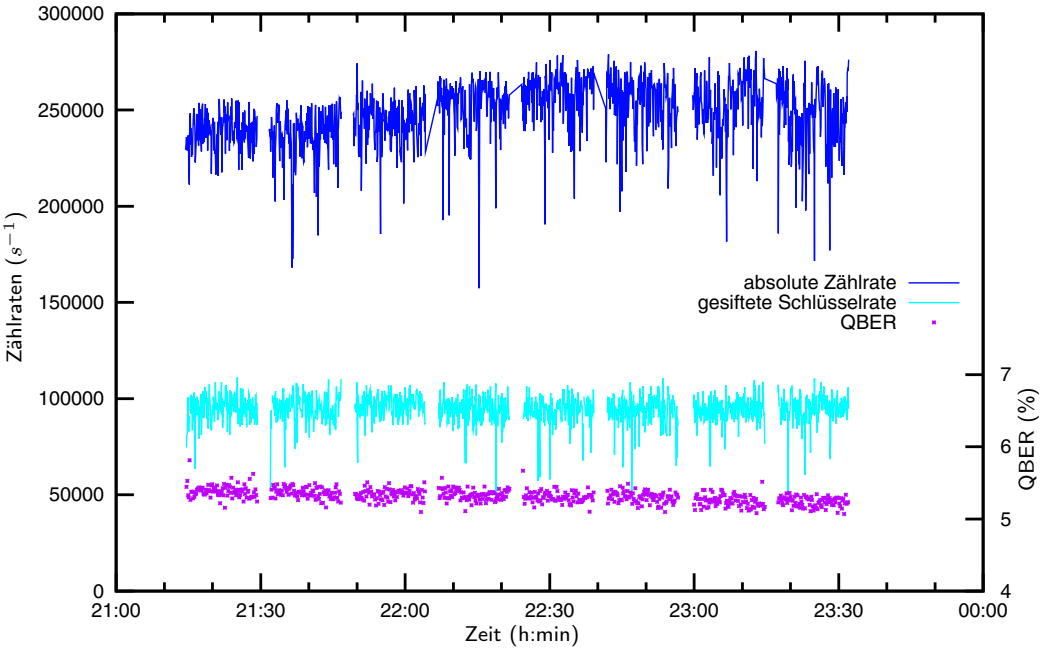


Abb. 6.7: Typische Werte der absoluten Zählrate bei Bob (blau), der Rate an gesiftetem Schlüssel (SKR, cyan)) und der QBER (violett). Deutlich zu erkennen sind die Einheiten von 15 min, zwischen denen die Sendedioden neu kalibriert werden. Zum jetzigen Zeitpunkt können auf Grund begrenzter Netzwerkleistung nicht alle detektierten Ereignisse in Echtzeit gesiftet werden, weshalb ggf. Datenblöcke verworfen werden. Die verbleibende SKR liegt im Mittel bei etwa 95 kBit/s. Mittelwert der QBER ist 5,3 %.

$10^5\,\mathrm{s}^{-1}$. Nicht alle Ereignisse können aber unmittelbar gesiftet werden, da die Netzwerkleistung zwischen Alice und Bob nicht ausreicht. Um einen Überlauf des Puffers zu verhindern werden deshalb regelmäßig Datenblöcke verworfen. Es verbleibt eine Rate an gesiftetem Schlüssel SKR von 95 kBit/s. Die QBER liegt im Moment typischerweise bei etwa 5.3 %.

Dieser Wert der QBER ist leider deutlich höher als die Abschätzung die in 5.4 getroffen wurde. Es besteht die Vermutung, dass die Verzögerung des Halbwellenplättchens, das bei Alice für die Anpassung der Basen auf beiden Seiten sorgt, bei den kalten Außentemperaturen nicht mehr exakt $\lambda/2$ beträgt. Die Kompensation der Faser durch die Viertelwellenplättchen wurde kontrolliert und nachgestellt und sollte deshalb keine zusätzliche QBER hervorrufen. Eine weitere Ursache kann in der Montage des Bobmoduls an das Teleskop liegen. Schon im Labor hat sich, im Zusammenhang mit der Messung zu Abbildung 5.3, herausgestellt, dass der Kontrast der Polarisationsanalyse empfindlich vom Eintrittswinkel der Photonen abhängt. Nur nach sorgfältiger Justage der Messstrahls mit Hilfe des Rückreflexes vom Eintrittsfenster konnte das Ergebnis (5.2) gemessen werden. Die vorhandene Mechanik lässt aber keine Justage dieses Winkels zu, weshalb der vorhandene Aufbau, der weitgehend noch aus der Arbeit [66] stammt, bald durch einen neuen ersetzt werden soll[5].

Decoy-Protokoll

Der Schlüsselaustausch wird in Zeitabständen von 15 min unterbrochen (siehe Abb. 6.7), um das Programm zur Kalibrierung der mittleren Photonenzahlen μ auszuführen. Auf diese Weise soll verhindert werden, dass unbemerkt zu hohe Intensitäten gesendet werden, was problematisch für die Sicherheit wäre. Die Werte von μ und μ' werden gemäß Gleichung (4.2) aus den Zählraten des Kalibrierdetektors bei Alice berechnet und für die spätere *privacy amplification* protokolliert. Die Daten in 6.8 zeigen, dass sich μ über einen längeren Zeitraum, hier 4 h genau einstellen lässt. Kleinere Abweichungen von den Sollwerten für die Signal- und Decoyintensität gehen nicht in die weitere Rechnung ein, da für die *privacy amplification* der tatsächliche Istwert relevant ist und dieser mit hoher Präzision, d.h. mit entsprechend langer Integrationszeit der Zählrate des Kalibrierdetektors, bestimmt wird.

Während des Siftings zählt der Empfänger erfolgreiche Übertragungen von Signal- und Decoypulsen in jeweils einem Decoy-Rahmen von 450 s. Diese absolute Zahl von erfolgreich registrierten Photonen ist für Signal- und Decoypulse sowie für die Zahl der Hintergrundereignisse in Abbildung 6.9 für den gleichen Zeitraum wie

[5] Bei dem aktuell verwendeten Bobmodul handelt es sich um ein Ersatzgerät, das im September für ein defektes Modul getauscht wurde. Vor dem Tausch konnten bereits Fehler von 2,5 % beobachtet werden, jedoch waren zu diesem Zeitpunkt andere Komponenten noch nicht einsatzbereit. Alle Messungen in dieser Arbeit wurden bereits mit dem neuen Modul durchgeführt.

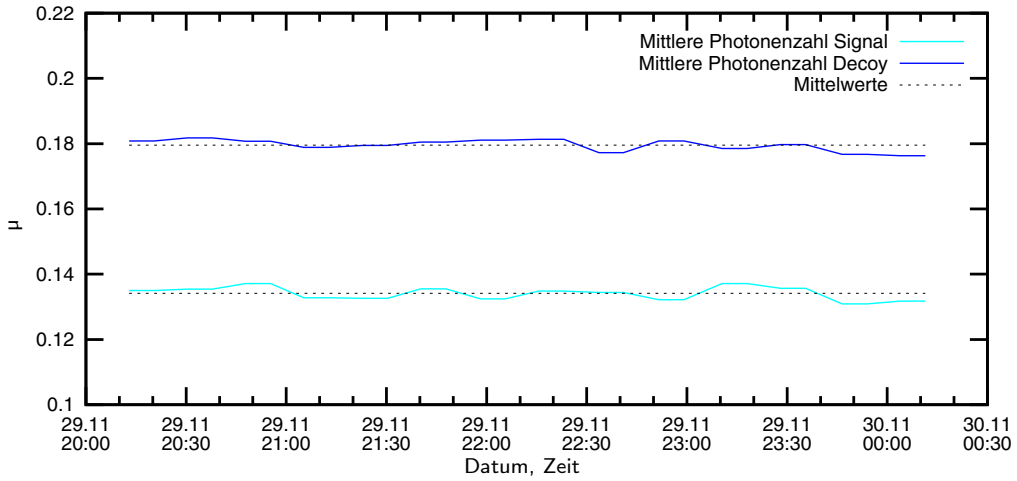


Abb. 6.8: Bei Alice gemessene mittlere Photonenzahl μ während dem Schlüsselaustausch. Die Mittelwerte (gestrichelt) liegen bei $\mu = 0{,}134$ und $\mu' = 0{,}180$

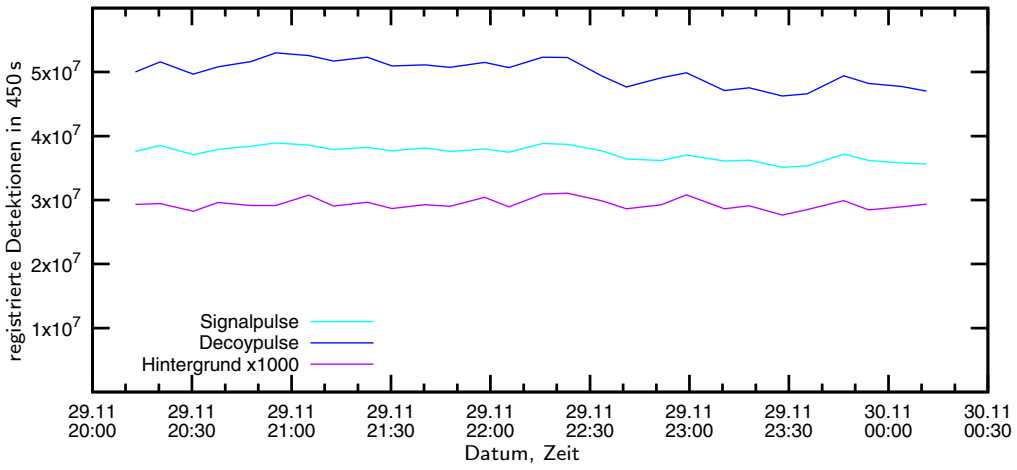


Abb. 6.9: Absolute Zahl von Detektionen in 450 s der verschiedenen Pulsklassen während des Schlüsselaustauschs: Signalpulse, Decoypulse und Vakuumpulse.

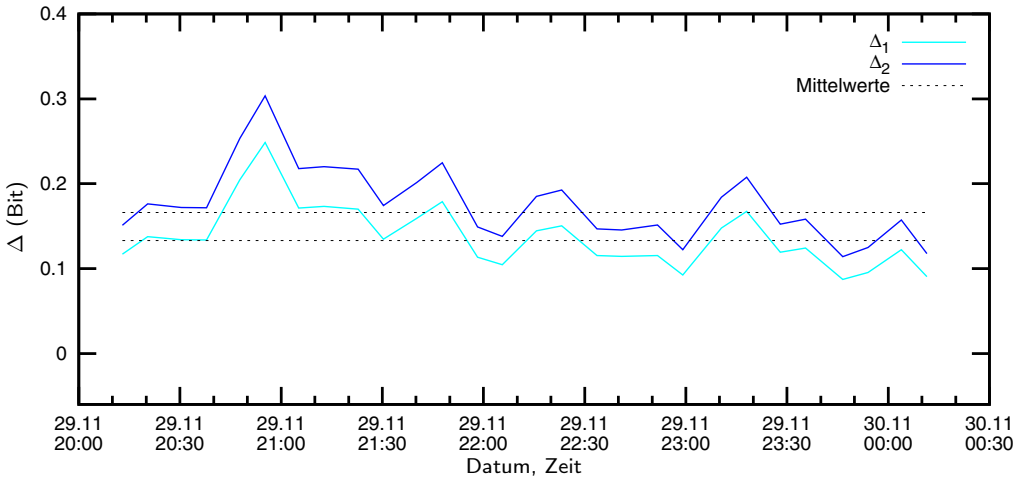


Abb. 6.10: Berechnete Werte für Δ_1 und Δ_2 während des Schlüsselaustauschs und deren Mittelwerte mit $\Delta_1 = 0{,}138$ und $\Delta_2 = 0{,}176$. Δ_1 bezeichnet den Anteil gemäß GLLP markierter Signalpulse. Um auch aus den Decoypulsen einen sicheren Schlüssel erzeugen zu können, vertauscht man gedanklich die Rollen von Signal- und Decoypulsen. Δ_2 gibt dann den Anteil markierter Decoypulse an.

in Abbildung 6.8 dargestellt. Der generelle Trend der beiden ersteren spiegelt die Entwicklung der Gesamtzählrate wieder.

In Abbildung 6.10 sind die, gemäß [60] berechneten Werte von Δ zu sehen. Δ_1 entspricht dem Wert wie in Abschnitt 3.6 beschrieben, Δ_2 ergibt sich, wenn die Rollen von Signal- und Decoypulsen vertauscht werden und aus letzteren der Schlüssel erzeugt wird. Auf diese Weise können alle Pulse für den Schlüssel genutzt werden. Die *privacy amplification* wird dann getrennt für die Unterschlüssel, bestehend aus den beiden Klassen von Pulsen, mit dem jeweiligen Wert von Δ durchgeführt. In den Wert von $\Delta_{1,2}$ gehen alle Größen aus den Abbildungen 6.8 und 6.9 ein, so dass sich die Schwankungen um die erwarteten Werte von $\Delta_1 = 0{,}133$ und $\Delta_2 = 0{,}166$ erklären.

Im Mittel liefert (3.26) für die hier beobachteten Parameter eine verbleibende Schlüsselrate von $R = 22\,\%$, wobei bereits die zu erwartende Effizienz der Fehlerkorrektur nach Cascade (relativ zum theoretischen Minimum $H_2(\delta)$ nach Shannon [64]) mit $f(\delta = 0{,}053) = 1{,}15$ in (3.26) mit einbezogen ist. Aus der Rate gesifteten Schlüssels von oben (95 kBit/s) und einer QBER von 5,3 % können also etwa 21 kBit sicheren Schlüssels pro Sekunde erzeugt werden.

Diese Rate sicheren Schlüssels ist der letztlich relevante Wert und kann noch deutlich gesteigert werden. Sobald die QBER wieder auf 2,5 % reduziert sein wird, können 47 kBit/s sicherer Schlüssel, bei gleicher SKR, erzeugt werden. Die SKR selbst ist wie schon gesagt noch durch die Netzwerkkapazitäten im klassischen Kanal beschränkt. Hier sollte jedoch, angesichts der absoluten Zählraten, durch effizientere Programmierung eine SKR von 125 kBit/s möglich werden, so dass eine sichere Schlüsselrate von über 60 kBit/s für die nahe Zukunft realistisch erscheint.

Für weitere Geschwindigkeitssteigerungen müssten aber dann Detektoren mit kürzerer Totzeit und eine leistungsfähigere Zeitstempel-Elektronik verwendet werden, bevor schließlich eine Erhöhung der Repetitionsrate noch weitere Verbesserung brächte.

6.4 Stand des Experiments zum Ende der vorliegenden Arbeit

Mit Abschluss der vorliegenden Arbeit konnte QKD erfolgreich durchgeführt werden, wobei die erreichten Schlüsselraten realistische Anwendungen erlauben. Für die nahe Zukunft bleiben jedoch noch weitere Aufgaben offen. So ist vor allem die QBER wieder auf die schon beobachteten Werte von 2,5 % zu reduzieren, was den Schlüsselverlust im Rahmen der *privacy amplification* drastisch reduzieren wird. Der Anstieg der QBER wurde nach dem Tausch des defekten Bobmoduls beobachtet, jedoch können andere Ursachen, die durch den einsetzenden Winter und die damit verbundenen niedrigen Temperaturen begründet sind, noch nicht ausgeschlossen werden.

Die Erweiterung von BB84 durch Decoy-Zustände ist vollständig implementiert. Die Kalibrierung der mittleren Photonenzahl pro Puls μ kann jedoch noch verbessert werden um stabilere Parameter für Δ (Gl. (3.26)) auf der Empfängerseite zu erhalten. Langfristig soll μ auch im Betrieb ständig überwacht und nachgestellt werden, indem die Zählrate des Kalibrierdetektors (Abb. 4.8) während der Schlüsselübertragung einzelnen Dioden zugeordnet wird. Regelmäßige Unterbrechungen zur Kalibrierung von μ könnten so ebenfalls vermieden werden.

Dringliche Aufgaben auf Softwareseite liegen vor allem in einer effizienteren Programmierung des Siftings. Aktuell ist die Auslastung des klassischen Kanals ein begrenzender Faktor. Es ist jedoch nicht die Datenmenge an sich, sondern die hohe Zahl von einzelnen Paketen, die die Kapazität des Netzwerks erschöpft.

Nicht zuletzt im Hinblick auf größere Distanzen zwischen Sender und Empfänger muss der Einsatz von feiner aufgelösten Schrittmotoren zur Ausrichtung der Teleskope geprüft werden. Eventuell bieten sich auch Piezokippspiegel für eine Feinausrichtung an. Die Auflösung wie in Tabelle 6.1 hat sich, vor allem auf Senderseite, als gerade ausreichend herausgestellt.

Bei der Analyse des gesifteten Schlüssels konnten Antikorrelationen in benachbarten Bits beobachtet werden. So ist die Wahrscheinlichkeit, für zwei gleiche Bitwerte an aufeinanderfolgenden Positionen (00 oder 11) mit 44 % in einem Schlüssel der Länge 10,3 MByte deutlich niedriger als für die Kombinationen 01 und 10 mit zusammen 56 %. Der Grund hierfür ist in der Totzeit der APDs zu vermuten, während der der Empfänger blind für ein nachfolgendes Photon gleicher Polarisation und Basis ist. Vor allem bei der Planung von höheren Repetitionsraten muss dieser Effekt besonders beachtet werden.

Die Tageslichttauglichkeit des Systems bleibt eine weitere Aufgabe zukünftiger Entwicklung. Durch aufwendigere räumliche und spektrale Filterung sollte dieses Ziel jedoch in einer neuen Baustufe des Empfängers erreichbar sein. Der geplante Interferenzfilter (Breite 0,8 nm FWHM, vgl. Abb. 6.4) verspricht ein entscheidender Schritt in Richtung Tageslichttauglichkeit zu werden.

7

Zusammenfassung und Ausblick

Im Rahmen dieser Arbeit konnte ein freiraumoptisches QKD-System erfolgreich aufgebaut und in Betrieb genommen werden, das unter realen Bedingungen den Schlüsselaustausch über eine Sichtverbindung von 500 m erlaubt. Die Anlage zeigt die geforderte Wetterfestigkeit und auch der ferngesteuerte Betrieb ist wie geplant möglich. Dabei werden Schlüsselraten erreicht, die realistische Anwendungen erlauben.

Über die Vorgängerarbeiten [66] und [68] hinaus erlaubt hier die vollständige Implementation von Decoyzuständen den Einsatz von abgeschwächten Laserpulsen an Stelle von echten Einzelphotonen und auch auf die Sicherheit des Schlüsselaustauschs im Hinblick auf Seitenkanäle wurde besonders geachtet. Die Charakterisierungen der räumlichen, zeitlichen und spektralen Eigenschaften des Senders stellt einen entscheidenden Schritt für die Sicherheit der Anlage dar, weitere Seitenkanäle müssen jedoch noch quantifiziert werden.

Die Abschätzungen bezüglich der maximal erreichbaren sicheren Schlüsselrate von über 60 kBit/s (siehe S. 81) basieren auf fundierten Werten sowie realistischen Annahmen und sollten in naher Zukunft zu erreichen sein. Die dazu nötigen Maßnahmen wurden identifiziert, wie z.B. die Beschleunigung des Siftings über den klassischen Kanal, vor allem aber die Reduktion der QBER. Auch schon jetzt kann aber mit einer Rate von bis zu 21 kBit/s (etwa 9 MByte/h) sicherer Schlüssel erzeugt werden.

Nachdem im Rahmen dieser Arbeit hauptsächlich der QKD-*Sender* weiterentwickelt wurde, muss in naher Zukunft auch der Empfänger auf eine neue Entwicklungsstufe gehoben werden. Dabei wird nicht zuletzt die Tageslichttauglichkeit – also der Betrieb rund um die Uhr – ein zentrales Ziel darstellen. Die Charakterisierung der Seitenkanäle eines neuen Empfängeraufbaus wird zudem Sicherheitslücken bei Bob schließen, die es Eve erlauben, einen Angriff ganz oder teilweise zu verschleiern. Dazu sind neben den Freiheitsgraden, die hier schon für den Sender untersucht wurden, auch die Abhängigkeiten der Detektoreffizienzen zu analysieren.

Das hier vorgestellte Experiment kann als Prototyp für kommerzielle freiraumoptische QKD-Implementationen verstanden werden, wofür sich die Aufbauten, vor allem des Senders wie in Abbildung 4.9, noch deutlich kompakter gestalten lassen. An Stelle der Ausrichtung des gesamten Systems bieten sich zudem bewegte Spiegel an, wie sie an anderer Stelle vielfach eingesetzt werden und wodurch das System flexibler aufgestellt und eingesetzt werden könnte.

Ähnlich wie die schon heute erhältlichen, faserbasierten Systeme, die moderne, klassische Kryptographie durch quantenkryptographisch ausgetauschten Schlüssel ergänzen, ist auch für das hier vorgestellte System eine Symbiose mit konventioneller Netzwerktechnik denkbar. Insbesondere schneller, optischer Richtfunk mittels heller Laserstrahlen bietet sich für die Kombination mit einem freiraumoptischen QKD-System an. Es könnte dann der klassische Sender für den Datenverkehr mit dem QKD-Sender zum Schlüsselaustausch in einem Gerät vereinigt werden. Gleiches gilt für die beiden Empfänger. Ein Teil der Optik, vor allem aber auch die Steuerung und Mechanik zur Ausrichtung können gemeinsam verwendet werden und ein derart kombiniertes System sollte einfach gegen eine herkömmliche Richtfunkstrecke austauschbar sein. Im nächsten Schritt können dann auch kleinere Netzwerke aufgebaut werden.

Die Schlüsselrate wird auch auf längere Sicht weit hinter heute üblichen Netzwerkgeschwindigkeiten zurückbleiben, was die Anwendung als *one-time-pad* in den meisten Fällen ausschließen wird. Trotzdem können durch den Einsatz quantenkryptographisch erstellter Schlüssel, zusammen mit mächtigen Algorithmen wie AES für den Datenverkehr, hybride Systeme geschaffen werden, die ein Höchstmaß an Sicherheit bieten. Die manuelle Schlüsselverwaltung und -verteilung – sofern man ein Verfahren wie das von Diffie und Hellman [25] aus Sicherheitsgründen vermeiden will – entfällt da laufend, automatisch und autark, neuer Schlüssel erzeugt und in gewissem Umfang gepuffert wird.

Mit der Produktreife eines zukünftigen freiraumoptischen QKD-Systems nach diesem Konzept erscheint die Installation, Inbetriebnahme und Einbindung in vorhandene Infrastruktur auch durch Netzwerk-Administratoren und Anwender möglich. So könnten schließlich auch die letzten beiden Forderungen Kerckhoffs erfüllt werden [15], der schon 1883 erkannte, dass die Zahl eingeweihter (heute eher *zugangsberechtigter*) Personen einen entscheidenden Sicherheitsfaktor für ein Verschlüsselungssystem darstellt: Ein kryptographisches System muss ohne Hilfe weiterer Personen (Experten, Physiker) gemäß einfachen Regeln verwendbar sein.

Anhang A

Eigenschaften von Silizium- APDs

In diesem Experiment werden für die Detektion von Einzelphotonen durchwegs Silizium-APDs vom Typ PerkinElmer C30902S verwendet, deren kreisförmige aktive Detektorfläche einen Durchmesser von 500 µm besitzt. Die Dioden registrieren ein Photon im Geigermodus mit einer Effizienz von ca. 38 % [67], indem der Lawineneffekt ausgenutzt wird: Durch eine hohe Vorspannung in Sperrrichtung werden, primär von einem Photon freigesetzte Elektronen-Loch-Paare stark auseinander beschleunigt und schlagen ihrerseits weitere Paare los, so dass ein messbarer Strom auftritt. Dieser Strompuls wird passiv durch einen Vorwiderstand von 390 kΩ begrenzt (*gequenscht*) und von nachfolgender Elektronik zu logikkompatiblen Pulsen geformt.

Der Arbeitspunkt der Vorspannung wird für jede Diode 20 V über die individuelle Durchbruchspannung, dem Wert, bei dem die ersten vereinzelten Lawinen gemessen werden können, eingestellt. Die konkrete Spannung ist von der Temperatur abhängig und von Diode zu Diode leicht variierend. Weiter ist eine Totzeit nach der Detektion eines Photons charakteristisch, in der die Wahrscheinlichkeit ein weiteres zu registrieren verschwindet. Diese kann bis zu 1 µs betragen und ist ein begrenzender Faktor für die maximale Zählrate.

Abbildung A.1 zeigt eine APD wie sie in dieser Arbeit verwendet wird, die oben angesprochenen Zusammenhänge sind in den darauf folgenden Abbildungen für eine typische APD dargestellt.

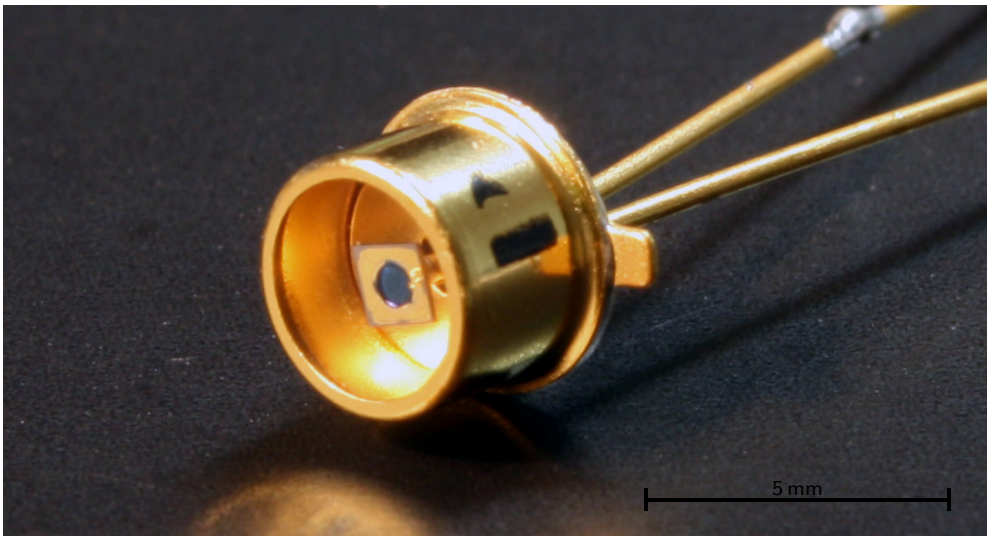


Abb. A.1: Foto einer Silizium-APD, wie sie in dieser Arbeit verwendet wird. In der Mitte ist hinter dem Eintrittsfenster der Halbleiter zu erkennen. Die aktive Fläche liegt innerhalb des sichtbaren Kreises mit ⌀500 µm.

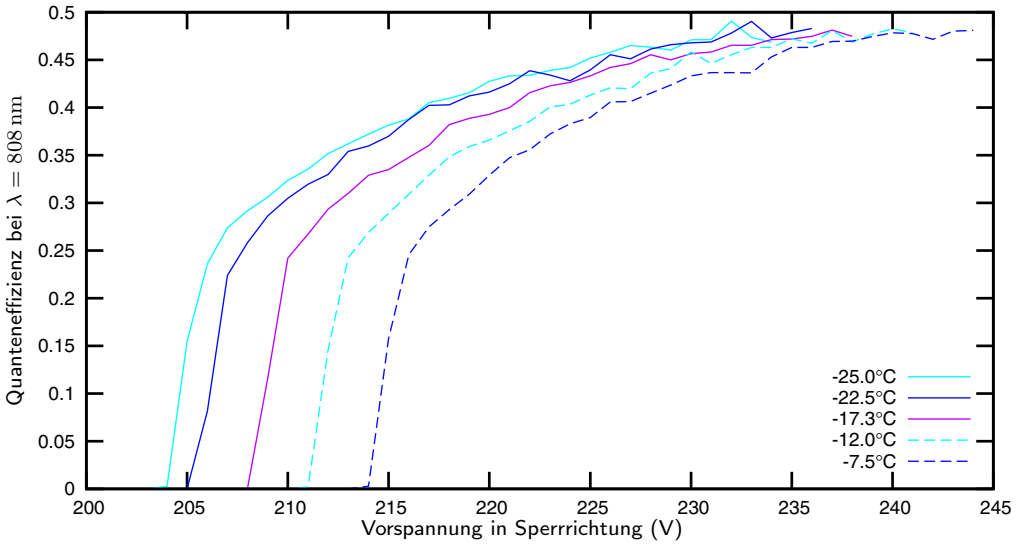


Abb. A.2: Detektionseffizienz einer Silizium-APD aufgetragen gegen die Vorspannung für verschiedene Temperaturen. Die Messung der Effizienz erfolgte mit Photonpaaren aus parametrischer Fluoreszenz und einem Triggerdetektor in [67]. Die Effizienz bei $\lambda = 850\,\mathrm{nm}$ ist entsprechend dem Herstellerdatenblatt um einen Faktor 0,87 kleiner [6].

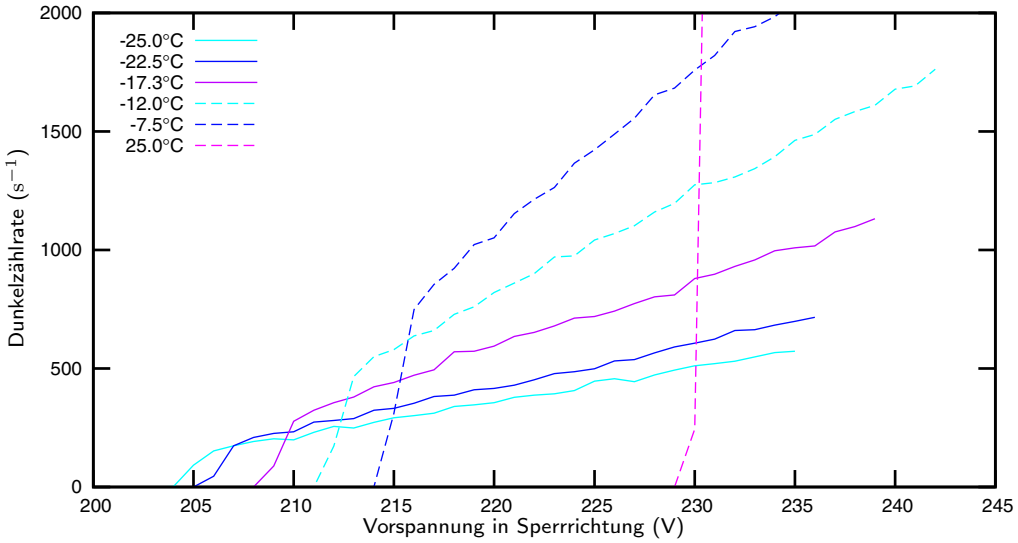


Abb. A.3: Dunkelzählrate abhängig von der Vorspannung in Sperrrichtung, aufgetragen für verschiedene Temperaturen am Beispiel einer APD [67].

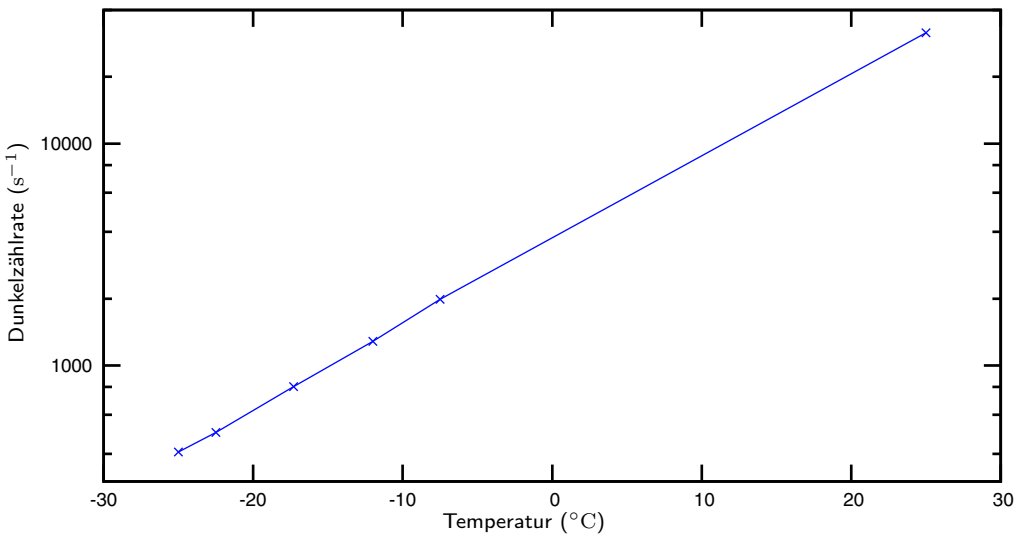


Abb. A.4: Halblogarithmische Darstellung der Dunkelzählrate gegen die Temperatur. Die Vorspannung in Sperrrichtung liegt für jeden Messpunkt 20 V über der Durchbruchspannung bei der jeweiligen Temperatur [67].

Anhang B

Technische Zeichnungen

Auf den folgenden Seiten sind mit technischen Zeichnungen die Bauteile dokumentiert, die für das Alice-Modul hergestellt wurden, im Einzelnen:

Diodenkopf: Aufnahme der Laserdioden, schwenkbar durch Verkippung der radialen Flügel.

Aufnahmewürfel: Gehäuse, das den Diodenkopf und den Innenkegelspiegel aufnimmt. Dieses Bauteil ist in Abbildung 4.7 links zu sehen.

Innenkegelspiegel: Das Gewinde M11×0,5 ist für die Aufnahme einer Linse vorgesehen, die die Einkopplung in das anschließende Modenfilter verbessert.

Pyramidenspiegel: Die Spiegelflächen wurden aufwendig poliert, es hat sich ein großer Einfluss ihrer Oberflächenqualität auf die erreichbare mittlere Photonenzahl μ gezeigt.

Kunststoff Adapterring: Zur thermischen Isolation gegen den Alicekopf und zur Aufnahme von Ein- und Auskoppelstrahlteiler vor bzw. nach der Glasfaser. Der Zusammenbau mit Rohr und Glasfaser ist in Abbildung 4.2 zu sehen.

Aluminium Rohr: Die Glasfaser wird in diesem Rohr eingegossen. Die äußeren Flachstellen dienen zur Aufnahme der Peltierelemente.

Onlineversion enthält keine technischen Zeichnungen!
Bitte persönlich anfragen.

Literaturverzeichnis

[1] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[2] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood und I. L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, **414**(6866):883–887, 2001.

[3] H.-K. Lo und H. F. Chau. Unconditional security of quantum key distribution over arbitrarily. *Science*, **283**(5410):2050–2056, 1999.

[4] P. W. Shor und J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, **85**(2):441–444, 2000.

[5] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger und H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, **98**(1):010504, 2007.

[6] T. Schmitt-Manderbach. *Long distance free Space quantum key distribution*. PhD thesis, Ludwig-Maximilians-Universität München, 2007.

[7] R. J. Hughes, J. E. Nordholt, D. Derkacs und C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, **4**:43, 2002.

[8] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster und J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, **419**(6906):450–450, 2002.

[9] J. G. Rarity, P. R. Tapster, P. M. Gorman und P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, **4**: 82, 2002.

[10] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, **67**(6):661–663, 1991.

[11] C.-Z. Peng, T. Yang, H.-X. Bao, J. Zhang, M.-X. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian und W.-J. Pan. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. *Phys. Rev. Lett.*, **94**(15):150501, 2005.

[12] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, Y. Hao, H.-P. Zeng, T. Yang, X.-B. Wang und J.-W. Pan. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.*, **98** (1):010505, 2007.

[13] C. Gobby, Z. L. Yuan und A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.*, **84**(19):3762–3764, 2004.

[14] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro und J. G. Rarity. Low cost and compact quantum key distribution. *New Journal of Physics*, **8** (10):249, 2006.

[15] A. Kerckhoff. La cryptographie militaire. *Journal des sciences militaires*, **9**: 5–38, 161–191, 1883.

[16] M. Briceno, I. Goldberg und D. Wagner. *A pedagogical Implementation of the GSM A5/1 and A5/2*, 1999. URL http://www.scard.org.

[17] B. Schneier. *Applied Cryptography. Protocols, Algorithms and Source Code in C.* John Wiley & Sons, Inc, 1995.

[18] U. Eco. *Im Namen der Rose.* dtv, 1980. Burkhart Kroeber aus dem Italienischen, 1982.

[19] S. Singh. *The Code Book.* Anchor Book, Random House, 1999.

[20] D. H. Hamer, G. Sullivan und F. Weierud. Enigma variations: An extended family of machines. *Cryptologia*, **22**(3):221–229, 1998.

[21] FIPS PUB 46-3. *Data Encryption Standard.* NIST, 1999.

[22] FIPS PUB 197. *Advanced Encryption Standard.* NIST, 2001.

[23] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, **28**(4):656–715, 1949.

[24] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the AIEE*, **45**:109, 1926.

[25] W. Diffie und M. E. Hellman. New directions in cryptography. *IEEE T. Inform. Theory.*, **IT-22**(6):644–654, 1976.

[26] R. C. Merkle. Secure communications over insecure channels. *Comm. of the ACM*, **21**(4):294–299, 1978.

[27] PKS #1 v2.1. *RSA Cryptography Standard*. RSA Laboratories, 2002. URL http://www.rsa.com.

[28] R. L. Rivest, A. Shamir und L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. of the ACM*, **21**(2):120–126, 1978.

[29] D. A. Osvik, A. Shamir und E. Tromer. Cache attacks and countermeasures: The Case of AES. In *CT-RSA*, pages 1–20, 2006.

[30] C. H. Bennett und G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984.

[31] N. Gisin, G. Ribordy, W. Tittel und H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, **74**(1):145–195, 2002.

[32] W. K. Wootters und W. H. Zurek. A single quantum cannot be cloned. *Nature*, **299**(5886):802–803, 1982.

[33] N. Gisin und S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.*, **79**(11):2153–2156, 1997.

[34] A. Einstein, B. Podolsky und N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, **47**(10):777–780, 1935.

[35] D. Bohm. *Quantum Theory*. Prentice-Hall, Inc., New York, 1951.

[36] D. Bohm und Y. Aharonov. Discussion of experimental proof for the paradox of einstein, rosen, and podolsky. *Phys. Rev.*, **108**(4):1070–1076, 1957.

[37] J. S. Bell. On the einstein-podolski-rosen paradox. *Physics 1*, pages 195–200, 1964.

[38] J. F. Clauser, M. A. Horne, A. Shimony und R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, **23**(15):880–884, 1969.

[39] C. H. Bennett und G. Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *SIGACT News*, **20**(4):78–80, 1989.

[40] B. Huttner und A. K. Ekert. Information gain in quantum eavesdropping. *J. Mod. Opt.*, **41**(12):2455–2466, 1994.

[41] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu und A. Peres. Optimal eavesdropping in quantum cryptography. 1. information bound and optimal strategy. *Phys. Rev. A*, **56**(2):1163–1172, 1997.

[42] H. Bechmann-Pasquinucci. Eavesdropping without quantum memory. Los Alamos e-print archive, 2005. quant-ph/0504003.

[43] E. Biham und T. Mor. Security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, **78**(11):2256–2259, 1997.

[44] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, **68**(21):3121–3124, 1992.

[45] C. H. Bennett, G. Brassard und N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, **68**(5):557–559, 1992.

[46] M. A. Nielsen und I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

[47] K. Tamaki, M. Koashi und N. Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Phys. Rev. Lett.*, **90**(16):167904, 2003.

[48] K. Tamaki, M. Koashi und N. Imoto. Security of the bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. *Phys. Rev. A*, **67**(3):032310, 2003.

[49] A. Lamas-Linares und C. Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Opt. Express*, **15**(15):9388, 2007.

[50] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen und H.-K. Lo. Experimental demonstration of time-shift attack against practical quantum key distribution systems, 2007. arxiv:0704.3253v1.

[51] B. Huttner, N. Imoto, N. Gisin und T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, **51**(3):1863–1869, 1995.

[52] G. Brassard, N. Lütkenhaus, T. Mor und B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, **85**(6):1330–1333, 2000.

[53] M. Dušek, O. Haderka und M. Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Opt. Commun.*, **169**:103–108, 1999.

[54] V. Scarani, A. Acín, G. Ribordy und N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, **92**(5):057901, 2004.

[55] H. Inamori, N. Lütkenhaus und D. Mayers. Unconditional security of practical quantum key distribution, 2001. quant-ph/0107017.

[56] H.-K. Lo, X. Ma und K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, **94**(23):230504, 2005.

[57] D. Gottesman, H.-K. Lo, N. Lütkenhaus und J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.*, **5**:325, 2004.

[58] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, **91**(5):057901, 2003.

[59] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, **94**(23):230503, 2005.

[60] X.-B. Wang. A review on the decoy-state method for practical quantum key distribution. Los Alamos e-print archive, 2005. quant-ph/0509084.

[61] X. Ma, B. Qi, Y. Zhao und H.-K. Lo. Practical decoy state for quantum key distribution. *Physical Review A*, **72**(1):012326, 2005.

[62] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, **61**(5):052304, 2000.

[63] G. Brassard und L. Salvail. Secret key reconciliation by public discussion. In *Advances in Cryptology: Eurocrypt́93*, volume 765, pages 410–423, 1993.

[64] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, **27**:379–423, 623–656, 1948.

[65] C. H. Bennett, G. Brassard, C. Crepeau und U. M. Maurer. Generalized privacy amplification. *IEEE T. Inform. Theory.*, **41**(6):1915–1923, 1995.

[66] H. Weier. Experimental quantum cryptography. Diplomarbeit, Technische Universität München, 2003.

[67] M. Kaminska. Effciency measurement and timing jitter measurement of apds with downconverted photons. Masterarbeit, Ludwig-Maximilians-Universität München, 2006.

[68] I. Ordavo. Free-space quantum cryptography. Diplomarbeit, Ludwig-Maximilians-Universität München, 2006.

[69] Die Daten für die Aussentemperatur wurden freundlicherweise vom Meteorologischen Institut der Ludwig-Maximilians-Universität München zur Verfügung gestellt.

[70] D. Marangon. noch nicht veröffentlicht. Masterarbeit, Ludwig-Maximilians-Universität München, 2007.

[71] S. Mayer. N/V Zentren als Einzel Photonenen Quelle. Zulassungsarbeit, Ludwig-Maximilians-Universität München, 2000.

[72] T. M. Cover und J. A. Thomas. *Elements of Information Theory. (Wiley Series in Telecommunications)*. John Wiley & Sons, Inc, 1991.

[73] V. Makarov, A. Anisimov und J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, **74**(2):022313, 2006.

[74] D. H. Höhn. Depolarization of a laser beam at 6328 a due to atmospheric transmission. *Appl. Opt.*, **8**:367–369, 1969.

Danksagung

Mit herzlicher Dank geht an Prof. Harald Weinfurter, der mir in seiner Gruppe eine interessante Diplomarbeit ermöglicht hat, die nicht nur im Labor, sondern auch auf dem Dach entstand. Vielen Dank auch an alle Cryptos für die tägliche und vor allem für die nächtliche Unterstützung: Henning, Martin, Tobias und Davide.

Allen weiteren Weinfurterleuten möchte ich ebenfalls, vor allem für das sehr angenehme Arbeitsklima danken: Andreas, Christian, Christian, Chunlang, Daniel, Daniel, Florian, Fredrik, Jan, Jürgen, Juliane, Markus, Michael, Nikolai, Pavel, Reinhold, Roland, Wenjamin und Witlef.

Erklärung

Mit der Abgabe dieser Diplomarbeit versichere ich, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 21. Dezember 2007

Sebastian Schreiner