Quantum cryptography/key-exchange with single and multi-photon sources via BB84 protocoll

J. Marschner, J. Kluge
Department of Physics, Humboldt-Universität zu Berlin, Germany
Emails: jmarsch@physik.hu-berlin.de
julien@physik.hu-berlin.de

February 15, 2017

Abstract

In this work, we qualify three different ways (continuous wave operation, pulsed operation and single photon operation) of doing a safe quantum-key-exchange via the BB84-protocoll. The different properties examined where: transmission speed, efficiency, safety, quantum-bit-error-rate (QBER) and practicability. We can conclude that in this experimental setup the pulsed operation was the most suitable.

In dieser Arbeit, qualifizieren wir verschiedene Betriebsmodi (Dauerstrichlaser, gepulster Laser, Einzelphotonenübertragung) zum sicheren Quantenschlüsselaustausch via BB84-Protokoll. Zur Untersuchung stehen: Übertragungsgeschwindigkeit, Effizienz, Sicherheit, Quanten-Bit-Fehlerrate (QBER) und Praktikabilität. Es zeigt sich, dass der gepulste Lasermodus der geeignetste der drei Modi im vorliegenden Versuchsaufbau ist.

noch den Grund angeben, wieso wir denken, dass Pulsbetrieb der beste ist

1 Physikalischer Hintergrund

Den Zentralen Aspekt des Quantenschlüsselaustauschs beruht auf der auf physikalischen Gesetzmäßigkeiten basierende Sicherheit. Dafür betrachtet man Qubits der Art $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Diese beschreiben zwei überlagerte, orthogonale Zustände, die die quantenmechanischen Analoga zu den Bits in der Informatik darstellen.

die WF ist nicht ganz richtig, bzw das + dadrinn.

In diesem Versuch werden die Qubits durch polarisiertes Licht dargestellt. Dabei betrachtet man einmal linear polarisiertes Licht im Zustand:$|\Psi_{HV}\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle)$. Dabei stehen die Pfeile für die jeweilige Polarisationsrichtung und HV (horizontal/vertikal) für diese spezielle Basis (rektilineare Basis). Dabei entspricht das horizontal polarisierte Licht dem Zustand $|0\rangle$ und das vertikal polarisierte Licht dem Zustand $|1\rangle$. Zum Anderen wird zirkular polarisiertes Licht betrachtet:$|\Psi_{RL}\rangle = \frac{1}{\sqrt{2}}(|\circlearrowright\rangle + |\circlearrowleft\rangle)$. Der rechts zirkulare Zustand entspricht $|0\rangle$ und der links zirkulare Zustand entspricht $|1\rangle$. Der Index RL (rechts/links) steht für die zirkulare Basis.
Möchte man nun einen Schlüsselübertragen, muss vom Sender (im Folgenden Alice genannt) eine Basis gewählt werden um so das für den Schlüssel entsprechende Bit zu versenden. Die Basis wird dabei zufällig gewählt. Der Empfänger (im Folgenden Bob genannt) wählt ebenfalls zufällig eine Basis und erhält bei richtig gewählter Basis das gesendete Bit. Dies führen Alice und Bob solange durch bis sie einen ganzen Schlüssel übertragen haben. Durch Basisvergleich können Alice und Bob bestimmen welcher Teile des Schlüssels richtig übertragen wurde

und haben somit einen sicheren Schlüssel generiert.
Unter Berücksichtigung von Verlusten und unter Benutzung von "error correction" dürfen bei einer sicheren Übertragung weniger als 12% Fehler auftreten. Sollte der Fehler größer sein, kann davon ausgegangen werden das gelauscht wurde. Eine belauschende Person (im Folgenden Eve genannt) würde nämlich durch Messen der Polarisation die Messung von Bob stören und damit würden bei Bob weniger "richtige" Qubits ankommen.
Genauere Details können dem Script[1] entnommen werden.

2 Versuchsaufbau

In Abbildung 1 ist der Versuchsaufbau dargestellt. Dabei wurde der Aufbau in zwei Abschnitte für Alice und Bob eingeteilt. Der Strahlengang ist in rot eingezeichnet.

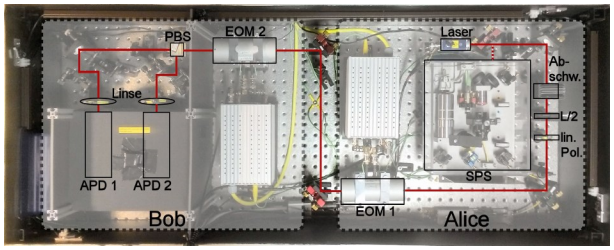

Figure 1: Foto vom Versuchsaufbau und übergelegtes Schema des Strahlengangs und der Komponenten Quellenverweis auf Script

Die für Alice wichtigen Bauteile, die Lichtquellen, gibt es zum einen einen roten Laser, der im gepulsten als auch CW-Modus betrieben werden kann, als auch eine Einzelphotonenquelle (SPS). Den Lichtquellen folgen Abschwächer, die die Intensität des Lichts senken. Darauf folgt ein einstellbares $\frac{\lambda}{2}$-Plättchen mit dem das Licht mit maximaler Intensität auf den linearen Polarisator treffen kann. Danach folgt ein elektrooptischer Modulator, der durch eine anliegende Spannung wie ein $\frac{\lambda}{2}$ oder $\pm\frac{\lambda}{4}$-Plättchen wirkt. Damit stellt Alice sowohl die Basis als auch die Polarisation des Qubits ein. Danach folgt der Aufbau für Bob. Dieser beginnt wieder mit einem elektrooptischem Modulator (EOM2). Mit diesem kann Bob seine Basis wählen. Nach EOM2 trifft der Strahl auf einen Strahlteiler (PBS) der das Licht entsprechend seiner Polarisation auf die Lawinenphotodioden(APD1 und APD2) schickt. Diese dienen als Detektoren der Photonen.

3 Versuchsdurchführung

Um mit der Messung beginnen zu können, musste zunächst der Strahlengang richtig eingestellt werden, so dass der Strahl des Lasers auch auf die APDs treffen kann. Die geschah durch Einstellung der Spiegel im Strahlengang (auch *Beamwalking* genannt). Danach wurden die Abschwächer in den Strahlengang gestellt und anschließend Feineinstellungen vorgenommen damit beide APD die maximale und gleichmäßige verteilte Intensität bekommen haben. Nun wurde durch Abrastern der EOMs die Spannungspaare gesucht, die benötigt werden damit die Basen von Alice und Bob richtig gemessen werden. Die so gewonnen Daten wurden zwischengespeichert und im folgenden immer eingestellt (bis auf eine weitere Kalibrierung bei der SPS-Messung). Danach konnte mit den ersten Schlüsselübertragungen begonnen werden. Dabei wurde ~~die Anzahl der Verstärker~~ verändert um Unterschiede in der Übertragungsrate zu generieren. Die Übertragungen fanden jeweils für den CW- als auch den gepulsten Modus statt.
Nach den Messungen wurden die nötigen Vorbereitungen zur Messung mit der Einzelphotonenquelle vorgenommen. Zunächst wurde mit dem grünen Anregungslaser erneut der Strahlengang nachjustiert, damit der Strahl die APDs trifft und beide Photodioden das Maximum an Licht erhalten.
Um die SPS richtig zu nutzen, musste der Anregungslaser noch auf ein Stickstoff-Fehlstellen-Zentrum eingestellt werden, damit auch Einzelphotonen gemessen werden können. Dabei wurde zunächst ein nicht allzu intensives Zentrum gewählt, um auch wirklich eine Einzelphotonenquelle zu untersuchen. Danach wurde ein sehr intensives Zentrum zum Vergleich gewählt. Dabei fanden zuerst Schlüsselübertragungen bei verschiedenen Intensitäten statt, danach wurde eine TimeHarp-

Karte an die APDs angeschlossen um die Autokorrelation der Einzelphotonenquelle zu messe. Damit lässt sich bestimmen, ob die SPS wirklich einzelne Photonen ausgesendet hat.

4 Auswertung

4.1 Untersuchung der Autokorrelation der Einzelphotonenquelle

Um die Autokorrelation der Einzelphotonenquelle zu bestimmen, wurden die dabei aufgenommen Messwerte mit folgender Funktion gefittet:

$$C_1 \left[1 - (K+1)\, e^{-k_1|x-x_0|} + K e^{-k_2|x-x_0|}\right] + C0 \tag{1}$$

Für verschiedene Intensitäten des weniger intensiven Zentrums sind die Fitkurven in Abbildung 2 zu sehen.

evtl. R normieren

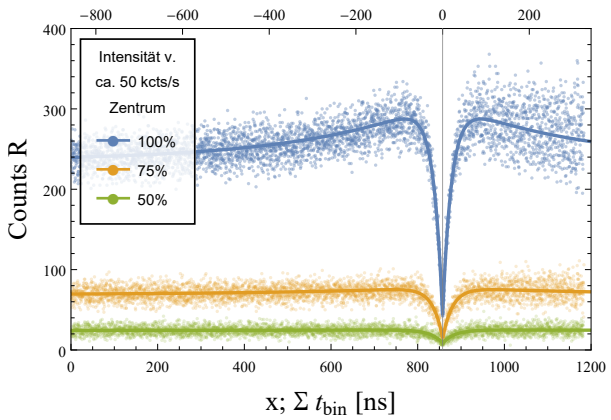

Figure 2: Fit der Autokorrelationen für verschiedene Intensitäten an einem Stickstoff-Fehlstellen-Zentrum nach Formel (1)

kurzes Resultat des graphen

Die Fitkurve für das intensivere Zentrum sind in der folgenden Abbildung zu sehen.

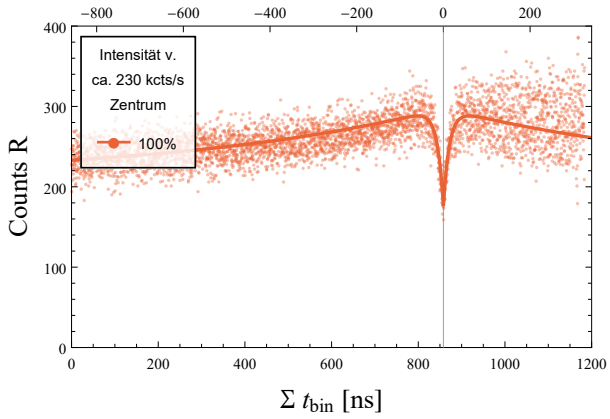

Figure 3: Fit der Autokorrelationen für volle Intensität an einem Stickstoff-Fehlstellen-Zentrum nach Formel (1)

Die Ergebnisse der Parameter sind in Tabelle 2 einsehbar. Es fällt auf, dass die Parameter K und k_2 in direkter Korrelation mit der Anzahl an registrierter Counts einhergeht und im Fit der 50%-Intensität sogar vollständig statistisch Insignifikant ist ($p - value \approx 0.63$). Dies ist auch leicht in der Form der Graphen erkennbar die keinen Anstieg vor dem x_0-Tal aufzeigen. Allerdings fehlt eine schlüssige Erklärung, warum die niedrigeren Intensitäten diese Verlaufsform nicht aufzeigen oder nur insignifikant wenig.
Mithilfe der gewonnen Parameter kann nun der Test auf Einzelphotonen mit der Autokorrelation durchgeführt werden, welche sich durch folgende Formel berechnet.

$$g^{(2)}(0) = \frac{C_0}{C_0 + C_1} \tag{2}$$

Damit es sich eindeutig um Einzelphotonen handelt, muss in etwa $g^{(2)}(0) < \frac{1}{2}$ gelten. Folgende Werte berechnen sich unter korrelierter Gaußscher Fehlerfortpflanzung:

g^(2)(0)<<1/2

Table 1: Autokorrelationsfaktoren der 4 Messdurchgänge mit Überprüfung auf Einzelphotonen

Intensität	$g^{(2)}(0)$	$g^{(2)}(0) < 0.5$
100% 50 kcts/s	(0.179 ± 0.016)	✓
75% 50 kcts/s	(0.213 ± 0.022)	✓
50% 50 kcts/s	(0.34 ± 0.04)	✓
100% 230 kcts/s	(0.827 ± 0.029)	×

erklären warum schlechter für kleinere Intensitäten, da es ja andersrum sein müsste

Die verschiedenen ~~Autokorellationen~~ sind in Tabelle 1 zu sehen. Wie zu erwarten war, ist der Einzelphotonencharakter bei nicht allzu großer Intensität gegeben. Bei sehr großer Intensität verschwindet der Einzelphotonencharakter wiederum.

4.2 Untersuchung der Effizienz der verwendeten Lichtquellen

Um die Effizienz der Lichtquellen zu bestimmen, wird die Übertragungsrate R_u in Abhängigkeit zur Detektionsrate R_d dargestellt und ein linearer Fit nach $R_u(R_d) = R_{eff} \cdot R_d$ erstellt. Dabei ist R_{eff} die Effizienz. Die Fits für die Einzelphotonenquelle und den Laser im CW- und gepulsten Modus sind in Abbildung 4 zu sehen.

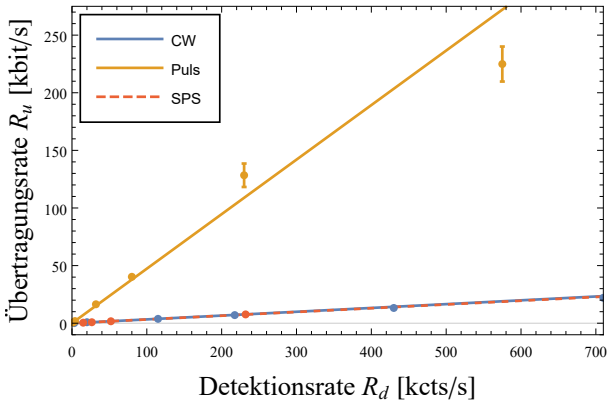

Figure 4: Übertragungsrate R_u in Abhängigkeit zur Detektionsrate R_d für CW, Puls und SPS Photonenquellen

Die Effizienz ergibt sich dadurch mitunter zu:

$$R_{eff} = \frac{R_u}{R_d} \hat{=} \left[\frac{\text{kbit}}{\text{kcts}}\right]$$

Macht das nicht. Aller Versuchsbetreuer, mögen dieses R_eff nicht

Mit den linearen Regressionen erhält man für die verschiedenen Modi folgende Effizienzen:

Modi	Effizienz R_{eff}
CW	$(0.0315 \pm 0.0004)^{\text{kbit}/\text{kcts}}$
Puls	$(0.487 \pm 0.013)^{\text{kbit}/\text{kcts}}$
SPS	$(0.0324 \pm 0.0010)^{\text{kbit}/\text{kcts}}$

Es zeigt sich dabei, dass die Effizienz im gepulsten Betrieb am besten ist.

4.3 Betrachtung der QBER

Um nun entscheiden zu können, ob die Übetragung sicher ist bzw. sichere Schlüssel übertragen werden, muss die Fehlerrate (quantum bit error rate - QBER) bei den Übertragungen kleiner als 12% sein. Bei den Übertragungen bei verschiedenen Intensitäten und Betriebsmodi blieb die Fehlerrate meist kleiner als 12% bis zu einem Spitzenwert von4%. Lediglich bei zwei sehr kleinen Intensitäten lag die Fehlerrate bei 12%. ~~Dabei waren wohl die Verluste bei der Übertragung so groß, so dass die Verluste durch die Intensität nicht kompensiert werden konnten.~~
Somit kann man schon mal festhalten, dass die hier angewendete Methode zum Quantenschlüsselaustausch wie durch die Theorie vorhergesagt funktioniert. Dabei wurden zwar etwaige Lauschangriffe vernachlässigt, diese sind aber auch vernachlässigbar, da das Funktionieren der Methode im Vordergrund steht. Die QBER wird in folgender Tabelle für jeden Modus und mit der zugehörigen Detektionsrate dargestellt:

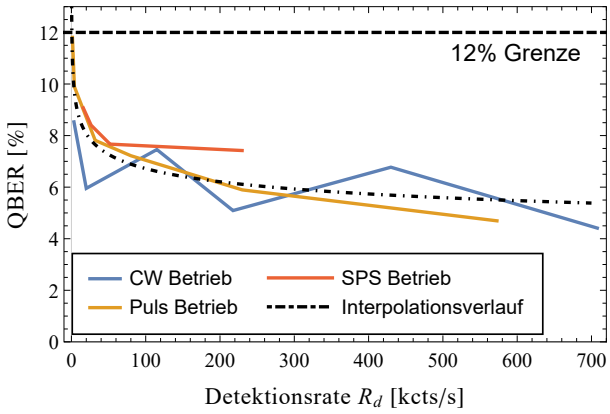

Figure 5: QBER in Abhängigkeit zur Detektionsrate und Interpolation der Gesamten Daten

4.4 Diskussion zur Praktikabilität des Aufbaus

Um die Praktikabilität des Aufbaus zu diskutieren, müssen die einzelnen Bauteile des Aufbaus betrachtet werden. Am wichtigsten sind hierbei die Lichtquellen. Zunächst ist die Effizienz der Übertragung entscheidend. Dabei schnitt der gepulste Laser am besten ab. Das

heißt, falls man längere Schlüssel übertragen möchte, muss man den gepulsten Modus wählen, um in angemessener Zeit den Schlüssel zu übertragen.
Alle drei Betriebsmodi zeigen außerdem QBER-Werte unterhalb von 12%, womit auch die Sicherheit und die vernünftige Übertragung von Schlüsseln gewährleistet ist. Ein weiterer Aspekt ist die Sicherheit vor *Photon-Splitting-Angriffe*. Dabei sticht wohl die Einzelphotonenquelle hervor, da sie die wenigsten Photonen pro Information sendet.
Somit sollte für einen kommerziellen Gebrauch ein gepulster Laser bevorzugt werden, da er Effizient ist und eine gute Fehlerrate besitzt. Möchte man jedoch auf absolute Sicherheit setzen muss eine Einzelphotonenquelle gewählt werden, jedoch wären dabei die Übertragungsraten viel zu gering. Eine Schlüsselübertragung könnte also zu lange dauern. Das Problem der Übertragungsdauer ließe sich umgehen, indem man durch diese Methode viele Schlüssel generiert bevor man sie nutzt. Somit könnte man erstmals Schlüssel ansammeln bevor zeitkritische Faktoren auftreten. Der Versuch zeigt die Möglichkeit der Automatisierung der Übertragung.
Beim Gebrach der Einzelphotonenquelle muss jedoch beachtet werden, dass durch das genauer Treffen eines Stickstoff-Fehlstellen-Zentrums die Gefahr besteht, dass man öfters nachjustieren muss. Bei der Durchführung hat sich nämlich gezeigt, dass der Tisch, auf dem der Nano-Diamant lag, gedriftet ist.
Betrachtet man die Justierung des Strahlenganges, lässt sich festhalten, dass dieser nach einmaliger Einstellung nicht nochmal eingestellt werden musste, die ist für eine kommerzielle Nutzung von Vorteil. Jedoch beträgt die Länge der Freistrahlstrecke einen halben Meter, dies wäre kommerziell nicht nützlich. Für eine kommerzielle Nutzung musste auf alle Fälle die Übertragungsreichweite vergrößert werden.
Die Messung mit den APDs ist kommerziell schwer nutzbar, es ist außerdem zu beachten, dass die APDs nicht für hohe Intensitäten ausgelegt sind. Unsachgemäßer Umgang könnte die APDs beschädigen.
Zusammenfassend kann gesagt werden, dass ein gepulster Laserbetrieb am vorteilhaftesten erscheint, die Einzelphotonenquelle dafür aber sicherer wäre. Der Aufbau ist ohne erhebliche Verbesserungen und Verkleinerungen schwerlich kommerziell nutzbar und außerdem müsste die Übertragungsreichweite vergrößert werden was aber eines der größten Probleme der Quantenkryptografie darstellt.

5 Anhang

ihm hat ein bisschen die Diskussion über einzelphotonen und die Sicherheit an sich gefehlt

Table 2: Ergebnis der Fitparameter für die nichtlineare Regression der Autokorrelationsfunktion (1)

Variable	$100\% \times 50\,\mathrm{kcts/s}$	$75\% \times 50\,\mathrm{kcts/s}$
C_1	193 ± 4	54 ± 2
K	0.39 ± 0.02	0.17 ± 0.02
k_1	0.048 ± 0.002	0.044 ± 0.003
x_0	857.4 ± 0.2	857.6 ± 0.4
k_2	0.0033 ± 0.0003	0.0027 ± 0.0010
C_0	42 ± 4	15 ± 2
Variable	$50\% \times 50\,\mathrm{kcts/s}$	$100\% \times 230\,\mathrm{kcts/s}$
C_1	16.0 ± 0.9	37 ± 7
K	0.06 ± 0.03	2.3 ± 0.6
k_1	0.037 ± 0.004	0.071 ± 0.005
x_0	857.6 ± 0.9	858.0 ± 0.4
k_2	0.003 ± 0.007	0.0016 ± 0.0003
C_0	8.3 ± 0.8	176 ± 5

6 Referenzen

1. AG Nano-Optik, *Anleitung zum Versuch: Quantenkryptographie mit einzelnen Photonen – QKD via BB84*, Dec. 2016