Quantenkryptographie

Institut für Physik – Humboldt-Universität zu Berlin

Hannes Vogel[1] (573003), Max Dreyer[2] (573838)

[1]vogelhaq@physik.hu-berlin.de, [2]dreyermq@physik.hu-berlin.de
29. Oktober 2018

Abstract In diesem Versuch wird das BB84-Protokoll zum Quantenschlüsselaustausch (QKD) mit verschiedenen Lichtquellen untersucht. Dabei werden ein abgeschwächter Laser im Dauerstrich- sowie gepulsten Modus und eine Einzelphotonenquelle (auf Basis von Defektzentren in Nano-Diamanten) miteinander verglichen. Alle Lichtquellen ermöglichen die Übertragung nach BB84. Die Einzelphotonenquelle führt hierbei zu den geringsten Übertragungsfehlern, ist jedoch deutlich aufwändiger zu realisieren als ein Laser.

1 Hintergrund

Die Qualität sicherer Nachrichtenübertragung lässt sich an den Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität messen. Dabei soll sich der Informationsaustausch nur an bekannte Empfänger richten (Vertraulichkeit) und innerhalb kürzerer Zeit abspielen (Verfügbarkeit). Außerdem müssen etwaige Veränderungen Dritter am Inhalt erkennbar sein, also die Authentizität der Nachricht gewährleistet werden (Integrität).

Durch die Nutzung des One-Time-Pad-Verfahrens ist die Sicherheit der eigentlichen Verschlüsselung der Nachricht gewährleistet. Sender und Empfänger müssen nur noch einen Schlüssel untereinander bestimmen und austauschen. Derzeit werden dazu verschiedene Methoden wie RSA (oft in Kombination mit symmetrischen Verfahren wie AES) verwendet. Die Sicherheit dieser Methoden basiert darauf, für die Erstellung des Schlüssels asymmetrische Funktionen zu verwenden. Diese beruhen unter anderem auf der Modulo-Rechnung. Die Verschlüsselung (Modulo einer gegebenen Zahl berechnen) ist dabei deutlich einfacher als die Entschlüsselung (aus dem Modulo die ursprüngliche Zahl berechnen).

Mit der weiteren Entwicklung von Computern werden Algorithmen zur Primfaktorzerlegung voraussichtlich deutlich effizienter und die asymmetrische Verschlüsselung dadurch angreifbar. Dann werden Methoden der Quantenkryptographie wie das BB84-Protokoll (nähere Informationen zum Verfahren siehe [1]) eine tragende Rolle zur Erstellung und Übermittlung von Schlüsseln spielen. Bei diesen kann zur Darstellung von Bits polarisiertes Licht verwendet werden (Siehe Tab. 1). Bei einem Abhörversuch, in Form einer zusätzlichen Polarisationsmessung im Strahlengang zwischen Sender und Empfänger, steigt die Fehlerrate (QBER) über 12 %. Diese wird vor dem Senden des eigentlichen Nachrichtenteils über einen öffentlichen Kanal überprüft, so dass eine unsichere Verbindung vorher abgebrochen werden kann. Damit ist das BB84-Protokoll im Prinzip abhörsicher.

Basis	Zustand	Bit
HV-Basis	$\|\leftrightarrow\rangle$	0
linear polarisiert	$\|\updownarrow\rangle$	1
RL-Basis	$\|\circlearrowright\rangle$	0
zirkular polarisiert	$\|\circlearrowleft\rangle$	1

Tabelle 1 Darstellung von Bits in HV-Basis (horizontal und vertikal linear polarisiertes Licht) und RL-Basis (zirkular polarisiertes Licht)

2 Versuchsaufbau

Die Übertragung eines Schlüssels nach dem BB84-Protokoll wurde mit dem folgenden Aufbau untersucht (Siehe Abb. 1). Beim Sender, Alice, können un-

terschiedliche Photonenquellen genutzt werden: ein Laser (Roithner LaserTechnik QL65D6SA, $\lambda = 650$ nm, P=5 mW) im Dauerstrich- oder gepulsten Betrieb sowie eine Einzelphotonenquelle (SPS, genauer Aufbau siehe [1]) auf Basis von NV-Zentren in Nano-Diamanten. Die Photonen werden über Spiegel zunächst durch eine Reihe von Abschwächerplättchen gelenkt, um verschiedene Abschwächungsgrade zu realisieren. Danach folgen ein $\lambda/2$-Plättchen (L/2) sowie ein linearer Polarisator, die eine feste Polarisationsrichtung bereitstellen. Durch die Elektrooptischen Modulatoren (EOM, QIOPTIQ LM 0202) von Alice und dem Empfänger, Bob, kann die Basis-Wahl aus dem BB84-Protokoll realisiert werden. Die Detektion der Photonen durch Bob folgt dem Hanbury, Brown & Twiss-Aufbau, um eine Autokorellationsmessung durchführen zu können. Dazu wurden ein Polarisationsstrahlteiler (PBS), Linsen und Lawinenphotodioden (APD, Excelitas SPCM-AQRH) verwendet.

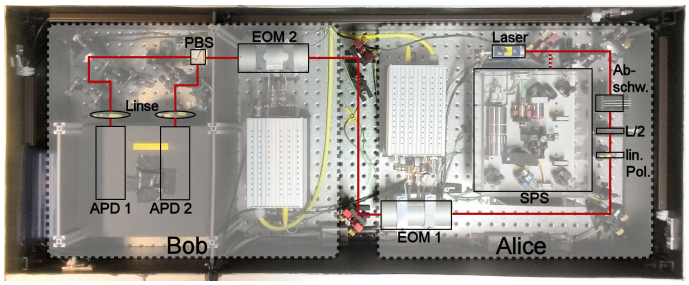

Abbildung 1 Foto des Versuchsaufbaus aus [1]. Eingezeichnet sind Strahlengang (rot) sowie optische Elemente: Einzelphotonenquelle (SPS), $\lambda/2$-Plättchen (L/2), Elektrooptische Modulatoren (EOM), Polarisationsstrahlteiler (PBS) und Lawinenphotodiode (APD).

3 Versuchsdurchführung

Die Durchführung folgt dem Skript [1]. Zunächst muss der Strahlverlauf so ausgerichtet werden, dass bei einem Scan der EOM-Einstellungen gleichmäßig verteilte Intensitäten bei beiden APDs gemessen werden. Danach werden die Spannungspaare für die Basenwahl von Alice und Bob im Scan der EOM-Spannungen ausgewählt. Die Basen-Einstellungen werden im weiteren Versuchsablauf beibehalten. Nun erfolgt die Schlüsselübertragung, um die Übertragungsrate und die Fehlerrate für verschiedene Abschwächungen des Laserlichts (gepulst und im Dauerstrichbetrieb) zu messen. Um die gleichen Messungen mit den NV-Zentren der SPS vorzunehmen, wird der reflektierte Strahl des Anregungslasers über Beamwalking mit dem ursprünglichen Strahl des ersten Lasers in Übereinstimmung gebracht, damit beide APD erneut ein gleichmäßiges Signal empfangen. Danach wird auf dem piezoelektrischen Probentisch durch Abrasterung mit dem Anregungslaser ein geeignetes NV-Zentrum gesucht, das als Einzelphotonenquelle dient. Ob eine echte Einzelphotonenquelle gefunden wurde, kann mit der Autokorrelationsmessung untersucht werden.

4 Messwerte

4.1 Schlüsselübertragung per BB84-Protokoll

Abbildung 2 zeigt die verwendeten Lichtquellen und gemessene Fehlerrate (QBER) der Übertragung für verschiedene Abschwächungen. Es ist erkennbar, dass eine höhere Übertragungsrate zu einem kleineren QBER-Wert führt. Außerdem führt die Einzelphotonenquelle bei konstanter Übertragungsrate zu dem geringsten Fehler, gefolgt von dem Laser im Dauerstrichbetrieb.

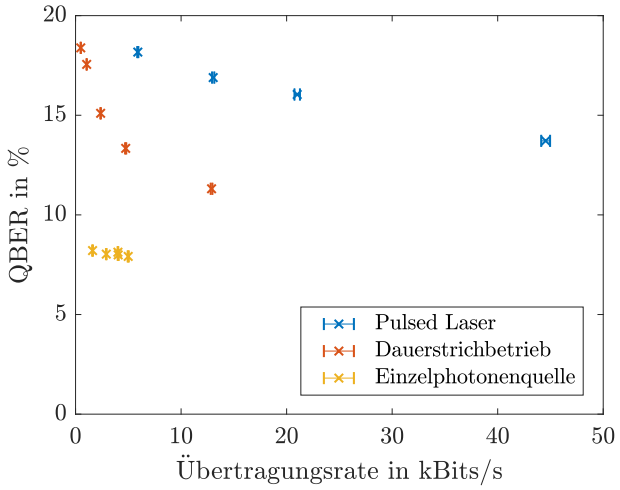

Abbildung 2 QBER in Abhängigkeit der Übertragungsrate für verschiedene Lichtquellen.

4.2 Autokorellation der Einzelphotonenquelle

Um einzuschätzen, ob die SPS einzelne Photonen emittiert, wird eine Autokorrellationsmessung durchgeführt. Im Versuch wird der Hanbury Brown & Twiss Aufbau verwendet, bei dem eingestrahlte Photonen an einem 50:50-Strahlteiler zufällig in einen von zwei Photodetektoren geleitet werden. Ein Detektor startet die Messung und der zweite beendet die Messung, wenn ein Photon gemessen wird. Einer der beiden Kanäle wird dabei gegenüber dem anderen verzögert.

Emittiert der Detektor zwei Photonen gleichzeitig und werden sie in den unterschiedlichen Detektor registriert, dann entspricht die gemessene Zeit der Verzögerung. Wird die Anzahl der Koinzidenzen gegenüber der Messzeit dargestellt, dann wird für eine gute SPS ein klares Minimum bei der Verzögerungszeit erwartet.

Quantitativ kann davon ausgegangen werden, dass es sich um eine SPS handelt, wenn die normierte Autokorrellationsfunktion zweiter Ordnung $g^{(2)}(0) < 1/2$ ist [1]. Für das verwendete NV-Zentrum lässt sich $g^{(2)}$ über die Fitfunktion

$$f(t) = C_1 \left(1 - (K+1)e^{k_1|t-t_0|} + Ke^{k_2|t-t_0|}\right) + C_0$$

annähern. Es gilt

$$g^{(2)}(0) = \frac{C_0}{C_0 + C_1}\,. \tag{1}$$

Der Fit (siehe Abb. 3) ergibt für die SPS mit $C_1 = (92 \pm 6)$ und $C_0 = (33 \pm 6)$:

$$g^{(2)}(0) = (0{,}27 \pm 0{,}06)$$

nach Gaußscher Fehlerfortpflanzung und somit einen Wert kleiner als $\frac{1}{2}$, was darauf hindeutet, dass ein einzelnes NV-Zentrum (und somit SPS) gefunden wurde.

Es ist anzumerken, dass eine spätere Messung der Autokorellation bei weiteren Abschwächungen zu keinem charakteristischen Signal mehr führte. Dies ist möglicherweise darauf zurückzuführen, dass der Tisch mit dem Diamanten gedriftet ist und somit ein NV-Zentrum mit mehreren Defekten angeregt wurde.

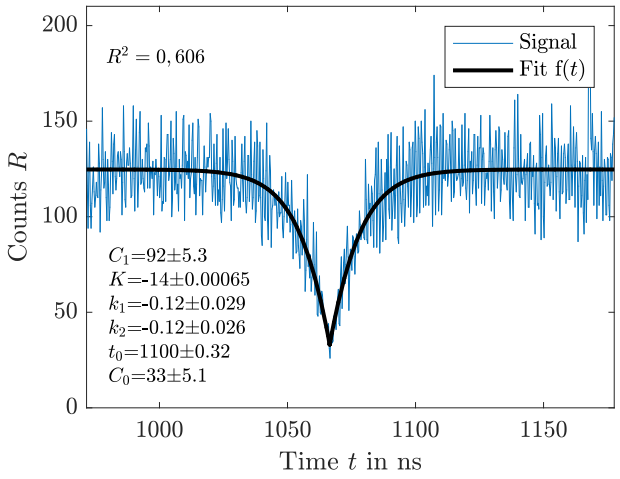

Abbildung 3 Autokorrelationssignal mit Fit $f(t)$ für ein NV-Zentrum.

5 Auswertung

5.1 Schlüsselübertragung

QBER Die Messwerte (dargestellt in Abbildung 2) zeigen, dass der QBER-Wert für die SPS im Vergleich zum Laser (konst. Übertragungsrate) am geringsten ist. Der gepulste Modus führt hierbei zu den größten Fehlerraten.
Da zwischen den Pulsen Pausen sind, in denen keine Photonen zum Detektor gesendet werden, führt Streulicht, Dunkelstrom etc. zu fehlerhaften Signalen im Detekor und somit einem größeren QBER-Wert. Hinzukommt, dass der Laser sehr stark abgeschwächt wird (zufälliger Prozess) und somit auch Zeiträume entstehen, in denen kein Signal gesendet wird. Die Einzelphotonenquelle gibt das regelmäßigste Signal und führt somit zu einem kleineren QBER-Wert.

Sicherheit Die zufällige Absorption von Photonen der Abschwächer führt auch dazu, dass es Pulse aus zwei Photonen gleichzeitig geben kann. Somit ist es

prinzipiell möglich, das Signal abzuhören ohne bemerkt zu werden.

Zusammenfassung Die Einzelphotonenquelle führt zu den kleinsten Fehlerraten und ist im Prinzip abhörsicher, weil im Idealfall keine Pulse mit mehreren Photonen emittiert werden. Andererseits ist die Methode aufwändig zu realisieren, da zuerst ein NV-Zentrum gefunden werden muss, welches nur aus einem Defekt besteht. Ein Driften des Diamantentisches ist in dem verwendeten Aufbau nicht auszuschließen.
Vergleichsweise einfach zu realisieren ist der Betrieb eines Lasers mit Abschwächern. In dem verwendeten Aufbau führt letzterer bei genügend hohen Übertragungsraten zu einem QBER-Wert unter 12%. Abgesehen von Pulsen mit teilweise mehr als einem Photon, kann also auch erkannt werden, ob der Schlüssel abgehört wurde.

Literatur

[1] AG Nano-Optik. Quantenkryptographie mit einzelnen photonen – qkd via bb84 [online]. Oktober 2018. URL: https://moodle.hu-berlin.de/pluginfile.php/2412430/mod_resource/content/1/Versuchsanleitung_QKD_2018_10_08.pdf.