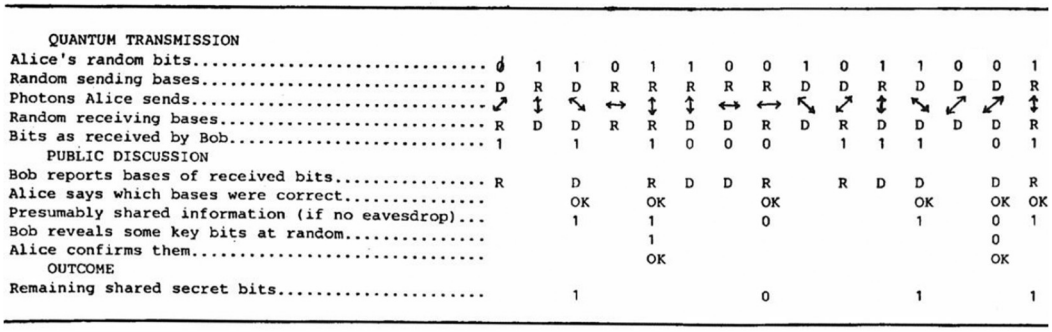
Abbe Center of Photonics | JENA
Friedrich-Schiller-Universität

Experimental Quantum Technologies

Quantum Cryptography (BB84)



QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↖	↗	↕	↘	↙	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Location: IAP – 054
Albert-Einstein-Straße 15,
07745 Jena

Instructor: Sabine Häussler
Email: sabine.haeussler@iof.fraunhofer.de

Contents

1 Introduction

Rapid development of computer systems in past decades led to availability of strong cryptography for civilian use, leading to data protection levels unimaginable before. However, even the most sophisticated algorithms (even those, which fulfill Shannon theorem of perfect secrecy) can be infective if the cipher key is intercepted. Quantum effects allow to design an approach to transfer a secret key in such a way that interception attempts will be detected.

The science of utilizing quantum mechanical features to accomplish cryptographic tasks is known as quantum cryptography. It relies on the property of measurements to alter the quantum state they are used on. The most well-known application of quantum cryptography is quantum key distribution, which provides an information-theoretically safe solution to the key exchange problem. Quantum cryptography allows realization of many cryptographic tasks that have been shown or conjectured to be impossible using only classical (i.e. non-quantum) communication. Copying data encoded in a quantum state, for example, is impossible. If the encoded data is attempted to be read, the quantum state will be altered owing to wave function collapse (no-cloning theorem). In quantum key distribution, this could be used to detect eavesdropping (QKD).

The BB84 protocol is the most well-known protocol for implementing secure key distribution. Alice sends single photons that are randomly polarized horizontally or vertically (straight base), or P (+45°) or M (-45°) (diagonal base). In this setup, one uses weak coherent pulses with adjustable average photon numbers and a half-waveplate to switch between. Bob, on the other hand, employs a polarizer that is also randomly set to these angles and attempts to detect single photons. After detecting photons, they can openly communicate over a traditional channel (usually the internet, but in this educational setup, it is done internally in the quCR control unit) about which photons were detected and compare their bases. After an error correction protocol, they will have the same key, ready to use for encryption.

2 Theory

Conventional cryptography schemes that are founded on a secret key are only secure when each key is not compromised and used only once. Thus, the encryption problem shifted to the exchange of a secret key. At the moment, mostly asymmetric schemes (e.g. RSA) using a public key (for encryption) and a private key (for decryption) are being employed. The security relies essentially on the impossibility of factorizing a large number in its prime factors. With faster computers, the possibility of a quantum computer or newly found algorithms, the security of these conventional systems is diminishing.

With the BB84 protocol, named after its inventors and the year of publication (Bennett and Brassard, 1984), it is possible to use the quantum physical properties of photons to transfer a secret key between two parties, tap-proof. When that has happened, the message can be encrypted and sent via an open classical channel. Because of that, the term quantum cryptography is actually misleading, it should be called quantum key distribution (QKD) instead.

2.1 Weak coherent pulses

A single photon at the push of a button is a subject still being researched heavily. Weak coherent pulses are an easy approximation, sufficient for many applications, e.g. quantum key distribution. Real single photon source emits exactly one photon in a specified time interval. Weak coherent pulses on the other hand are just attenuated laser pulses. As such, the photon numbers in one pulse obey the Poisson distribution, where the probability of k photons in one pulse is given by

$$P_k = e^{-\lambda}\frac{\lambda^k}{k!}, \tag{1}$$

with the average photon number λ. For most applications here, we take into account the probabilities for no photon in a pulse, exactly one photon in a pulse, and more than one photon in a pulse. Some calculations of these probabilities for different average photon numbers can be found in Tab. 1.

You can see that by reducing the average photon number, the relation between pulses with one photon compared to pulses with more than one photon becomes greater, which is good. But at the same time, more and more pulses do not have any photons in them, making it hard to reach acceptable count rates. This is a consideration one has to make for each individual task.

λ	P_0	P_1	$P_{>1}$	$P_1/P_{>1}$
0.1	90.5%	9.05%	0.45%	20.11
0.5	60.7%	30.3%	9.0%	3.37
1.0	36.8%	36.8%	26.4%	1.39
2.0	13.5%	27.1%	59.9%	0.45
10.0	0.005%	0.05%	99.945%	0.0005

Table 1: Probabilities for the number of photons given by the Poisson distribution for different average photon numbers.

2.2 Polarization measurement with single photons

In the lab you will deal with an equipment intended for polarization control of incoming light. The light source in the setup should generate linearly polarized light in the ideal case. In schemes and descriptions below, you will also encounter a Half Wave Plate (HWP) for state preparation by Alice and a HWP together with a Polarization Beam Splitter (PBS) for measurement. These devices represent the ideal prepare and measurement apparatus for BB84. Even though it is not used like that in our laboratory setup, it is important to understand its performance for comparison with our actual implementation. In this ideal case, the first device is a HWP, which just provides rotation of polarization, allowing to encode bits in terms of polarization state. By simply changing angle between polarization vector and wave plate's axis we can obtain Vertical ($|V\rangle$), Horizontal ($|H\rangle$), Diagonal ($|P\rangle$) and Anti-diagonal ($|M\rangle$) polarizations. Two orthogonal polarization directions can be always used as a basis, such that all other polarizations can be expressed as a linear combination of the two basis polarization states. $|P\rangle$ and $|M\rangle$ are called the diagonal basis, $|H\rangle$ and $|V\rangle$ are called the straight basis. For measurement in the ideal case, a PBS is used after the HWP. A PBS is an optical device designed to separate light into two distinct beams based on their polarization. It exploits the principle of polarization-dependent reflection and transmission, allowing the splitting of light into components that are either polarized parallel or polarized perpendicular to a specific axis (basis of PBS). However, when one speaks in terms of photons, it is impossible to split a single photon into two beams, reaching detectors. In this terms PBS can be described as a device redirecting photons in one of the paths with probability equal to square modulus of a coefficient of a photon polarization state, represented in basis of a PBS. For example, assume that you PBS has a diagonal basis, and you send a photon in vertical polarization. In this case your photon polarization can be represented in a basis of a PBS in this way:

$$|V\rangle = \cos 45^\circ |P\rangle + \sin 45^\circ |M\rangle , \tag{2}$$

giving you a probability of 0.5 for your vertically polarized photon to be detected as $|P\rangle$ or $|M\rangle$ polarized one.

In our lab setup the light coming from the source is not polarized linearly but rather circularly, therefore we are using two Polarizers instead of the HWP and PBS. Its effect can be described in a similar way to a PBS. When the polarizer is oriented along one of the basis directions, the component of a polarization state corresponding to this basis state can pass through the polarizer. The other component is filtered out. So, probability of a photon to pass through a polarizer will be a squared cosine of an angle between photon's polarization and polarizer's axis.

2.3 The BB84-Protocol

The two parties involved in the secure communication are called Alice and Bob by convention, see also Fig. 1. Alice operates a source of single photons that she can individually prepare in a linear polarization state known to her and sends them to Bob. Alice chooses between two bases, e.g. straight $\oplus$ and diagonal $\otimes$. Each basis consists of two states, namely $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ ($\oplus$) and $|\mathrm{P}\rangle$ and $|\mathrm{M}\rangle$ ($\otimes$), respectively. Each state represents a binary value 0 ($|\mathrm{H}\rangle$ and $|\mathrm{P}\rangle$) or 1 ($|\mathrm{V}\rangle$ and $|\mathrm{M}\rangle$). As such, Alice can prepare a random bit sequence in random bases and send it. Randomness is important here, because if it is not guaranteed, another person can obtain a valuable information about a key later. Bob receives the photons and can choose one basis per photon for a polarization measurement. In doing so, a meaningful bit (a bit suitable for a key construction) is only received when Bob and Alice chose the same basis. Thus, they have to communicate their basis choice. If Bob detects no photon

quantum channel:														
Alice's random bit sequence	0	1	1	0	1	1	0	0	0	1	0	1	0	1
Alice's random base choice	⊗	⊗	⊕	⊕	⊗	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
sent photon polarization	P	M	V	H	M	V	H	H	P	V	P	M	H	V
Bob's random base choice	⊕	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊕
received bits	1	1	1		0	1	0	1	0	0	0		0	1
classical channel:														
Bob sends bases	⊕	⊗	⊗		⊕	⊗	⊕	⊗	⊕	⊗	⊗		⊕	⊕
Alice confirms		✓					✓				✓		✓	✓
probably shared bits		1					0				0		0	1
eavesdropper detection														
Bob shares randomly		1									0			
Alice confirms		✓									✓			
remaining key							0						0	1

Table 2: The BB84 protocol, step by step.

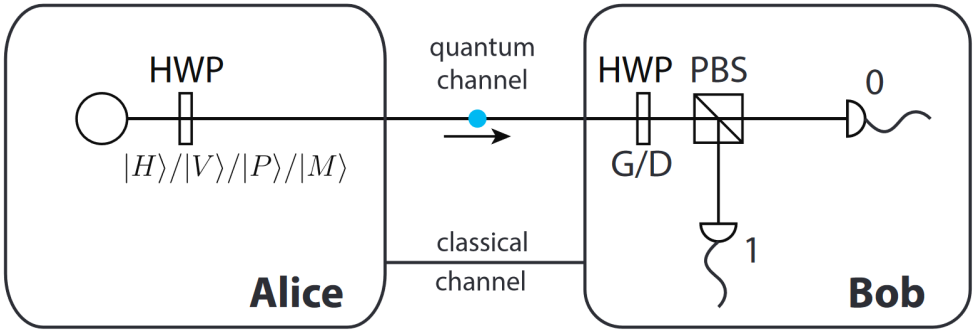


Figure 1: Schematic setup for implementation of the BB84 protocol. Pay attention, that HWP in front of Bob's PBS is intended to change polarization of incoming signal to a PBS basis and determines a basis for Bob's measurement.

because of losses in the quantum channel, the corresponding bit is discarded. The following steps are then done using a classical (public) channel. Bob sends a list with his measurement bases to Alice. She compares the list to her own and tells Bob which bases match. All bits with non-matching bases are discarded by both parties. The remaining bits make up the secret key (Table 2).

2.4 Detection of Eavesdroppers

In general, it is assumed that Eve (from eavesdropper) can intercept both the classical communication channel and the photons sent by Alice, see Fig. 2. So how is it still possible to exchange a secret key, or rather, to detect the attempt of intrusion? The BB84 protocol takes advantage of two important properties of single photons:

- By a single measurement, the polarization state of a single photon can not be determined fully.
- The polarization state of a single photon may not be copied. (No-Cloning-Theorem).

Eve could, e.g., intercept part of the photons from Alice and perform a polarization measurement, just as Bob would. But, if Bob receives no photons at the proper time, the bits are just discarded and Eve gains no information about the key. Therefore, Eve sends one photon onward to Bob in each case, with the polarization measured by Eve. This kind of attack is called an intercept-resend attack. Bob and Alice can detect such an attempt by comparing part of the key. That is to say, if Eve chooses a basis that does not conform with Alices and Bobs, the Bit received by Bob is random. Thus, it can happen that Bob's Bit does not match with Alice's. If some of those "errors" are found, they can assume that the photon channel is compromised and their key is not secure. However, Bob also has its own source

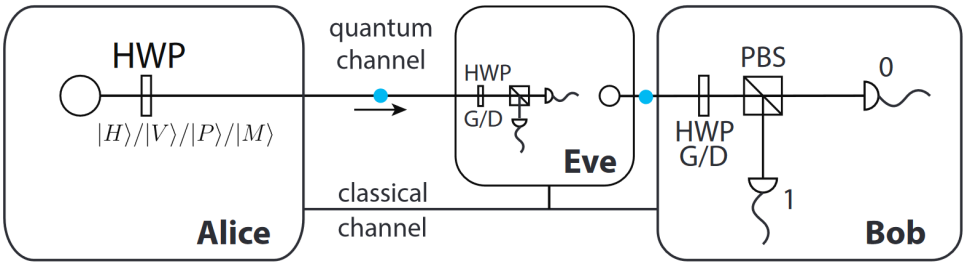


Figure 2: Eve can eavesdrop on the classical channel and intercept the photons in the quantum channel.

of such errors, motivated by imperfections of his detectors. Sometimes detectors can signal a 'click' event (presence of a photon) even without a proper photon, this is so called "dark count" event. The rate of this type of error should be a rather small and known value, to be able to be distinguished from addition errors due to intervention in a channel. There are of course more sophisticated ways of comparing the key than just publishing part of it, called error correction schemes. Some popular choices are the *cascade* protocol or the *low density parity check*.

Remark on the quantum channel: It is important that Alice sends just one photon for each bit. That is, experimentally, not as simple as it sounds, since Alice has to know exactly when a photon was generated and sent, she needs a real *single photon source*. There are still intensive research efforts going on in that direction. Therefore, sources for *weak coherent pulses* are often used at the moment. Here, the photon number per pulse obeys the Poisson distribution.

If Alice sends multiple photons in a pulse, Eve could employ a so called *beam splitter attack*. She intercepts only part of the photons for her measurements. Bob still receives photons directly from Alice and therefore cannot determine the presence of an attacker.

In the case of weak coherent pulses, the average number of photons per pulse has to be taken into account when calculating the security of the protocol. As a rule of thumb, the average photon number has to be smaller than the transmission of the quantum channel (proof of GLLP [1]). However, by using more sophisticated protocols such as the *Decoy state* protocol, the photon number can be increased.

Remark on the classical channel: Alice and Bob can communicate publicly through the classical channel, but they have to be sure that they communicate directly with each other, and Eve does not change the content of their messages. This can be done (cue authentication) using a previously exchanged secret key. So intrusion with ability not only to listen to both channels, but also to send own information there makes the scheme insecure.

Remark on dark counts and error estimation: In the context of the BB84 protocol for Quantum Key Distribution (QKD), the Quantum Bit Error Rate (QBER) refers to the percentage of bits that are received in an erroneous state due to noise, eavesdropping, or imperfections in the transmission channel or detection systems. The QBER in a QKD protocol provides insight into the level of interference or error in the transmission. Ideally, there should be no error in the absence of eavesdropping, which means the QBER should be 0%. However, noise, channel imperfections, or other environmental factors can contribute to errors. So in general QBER can be defined as:

$$QBER = \frac{DetectedErroneousBits}{(DetectedErroneousBits) + (DetctedTrueBits)} * 100\%. \tag{3}$$

Erroneous bits appear either by intrusion of additional photons in the channel or due to a 'dark count' event on detectors. However, even if Bob got a wrong bit, it is not guaranteed that this bit will be considered a detected one. If the polarization basis for this bit was not the same as for Alice, it will be just excluded from key formation anyway. So, only erroneous bits, which will be in a final key are considered as Detected Erroneous Bits.

A higher QBER indicates more noise or potential eavesdropping activity. In the case of BB84, an acceptable QBER is typically around 11% or lower.

If the QBER exceeds this threshold, it could indicate that an eavesdropper is actively intercepting and disturbing the quantum states to gain information about the key. A QBER of 11% is a security

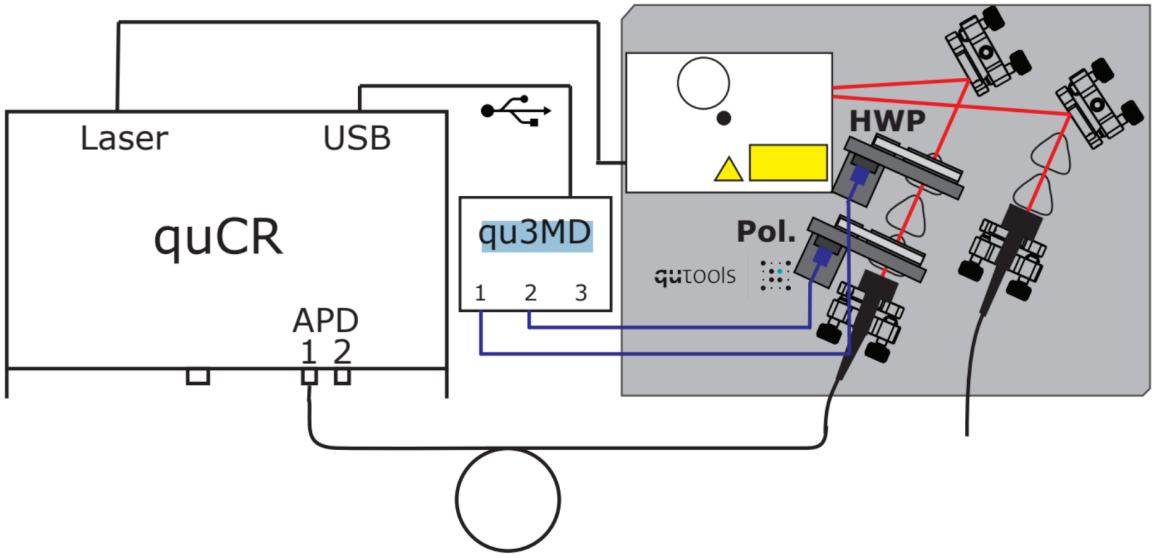


Figure 3: Setup of the BB84 experiment with the motorized stages.

margin; the protocol can still detect eavesdropping and apply error correction and privacy amplification techniques to mitigate the impact.

3 Experimental setup

3.1 General overview

In the labwork one will use the quED-QKD tool, schematically presented in the figure 3. It consists of quCR Control Rack, qu3MD Motor Drive command unit, two Polarizers (Pol.), mirrors and optical couplers. The Control Rack is responsible for data processing, controlling of all the other parts and contains Avalanche Photo Detectors (APD). Consider that in the lab setup we have two polarizers instead of a half wave plate (HWP) in combination with a polarizer as shown in the sketch. From rear panel of it one data cable goes to light source, and a USB cable connected to qu3MD unit, which translates commands to piezo drives of motorized actuators rotating the Polarizers. For data transfer one can disconnect (be sure that the Polarizers are in **zero position**!) qu3MD and connect a USB flash drive to the Rack.

The light source here is a photon pair source, which utilizes Spontaneous Parametric Down Conversion (SPDC) in a nonlinear crystal. The light source is made out of β-Barium-Borate (BBO), a special optical non-linear crystal. A high power UV diode laser at 405 nm wavelength, called the pump laser, is focused in this crystal. If the polarization of the pump beam and the axis of the BBO crystal are matched in a way enabling energy and momentum conservation, some of the pump photons are converted into two lower energy near infrared photons at 810 nm. These down con-verted photons then emerge at opposite sides of a so-called emission cone and form a photon pair (For more information and nice animation visit https://qutools.com/qued/, photon source tab).

3.2 IMPORTANT CHECKLIST FOR THE SETUP

- Do **NOT** turn off the Rack when laser diode is on. Always double check, that laser is off before turning the starting key.
- Do **NOT** disconnect qu3MD from USB port if the Polarizers are not in zero position.
- Always bring the Polarizers to zero position before turning off the setup.

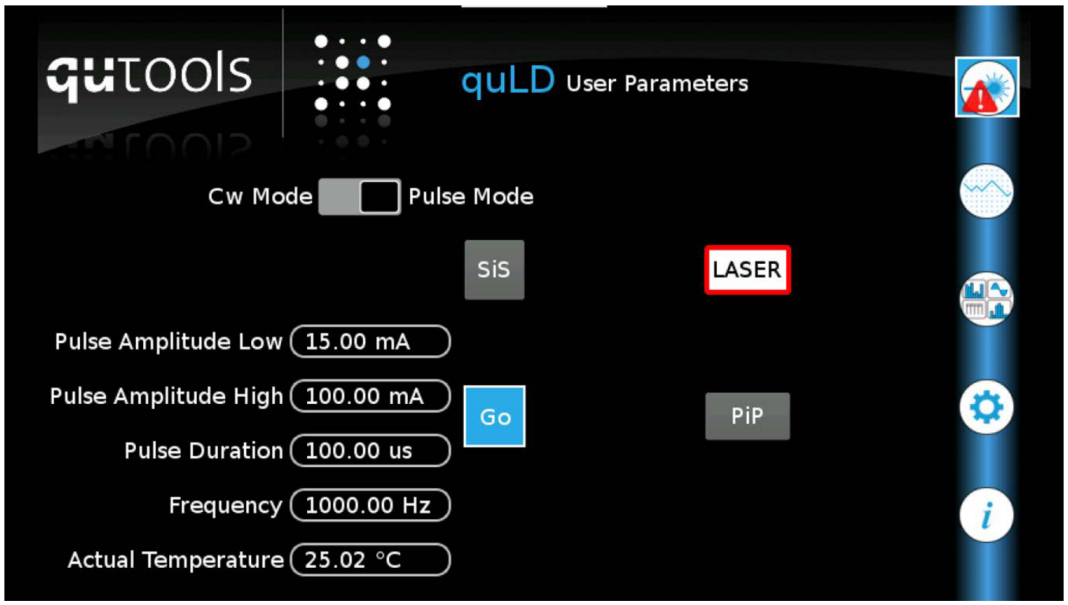


Figure 4: The pulsed laser menu of the quCR control interface.

3.3 Quickstart Manual

With the quED-QKD Add-On, you gain the ability to pulse the pump laser diode, and with that, to generate weak coherent pulses (almost as good as single photons) on the push of a button. Indeed we have a SPDC source, but for a single channel and small number of photons per puls it can be considered as a weak coherent pulse. So, generate pulses, you can simply switch to pulsed mode in the laser tab of the quCR control unit interface, see Fig. 4. You can tweak the following factors:

1. **Pulse Amplitude**: How much current will flow during the pulse.
2. **Pulse Duration**: How long will a single pulse last (together with pulse amplitude, this defines the average photon number per pulse).
3. **Frequency**: How often a pulse will be generated (only applicable if the "'Go"' Button is pressed.

Factor	**Value**
Pulse Amplitude	operating current, see quED datasheet
Pulse Duration	1 μs

Table 3: The settings needed for pulses with approximately a single photon per pulse (on average).

To generate pulses with approximately a single photon per pulse (on average), use the settings in Tab. 3. Please note that you will be detecting much less than a photon per pulse, because of detector and coupling efficiencies. In our case we have the motorized version of the quED-QKD, and the BB84 Experiment can be performed step by step in the BB84 tab of the quCR control interface.

4 Experiments with the quED-QKD

4.1 Weak coherent pulses

4.1.1 Experimental description

To generate and gauge weak coherent pulses, first be sure that the Polarizers are at the same angle position (can be manually adjusted in menu with a gear icon), the HWP inside the source is removed and realign the setup for maximal coincidences. After that, switch to the pulsed laser mode in the laser tab and activate the Picture-in-Picture (PiP) Overlay, such that you can modify the pulse settings

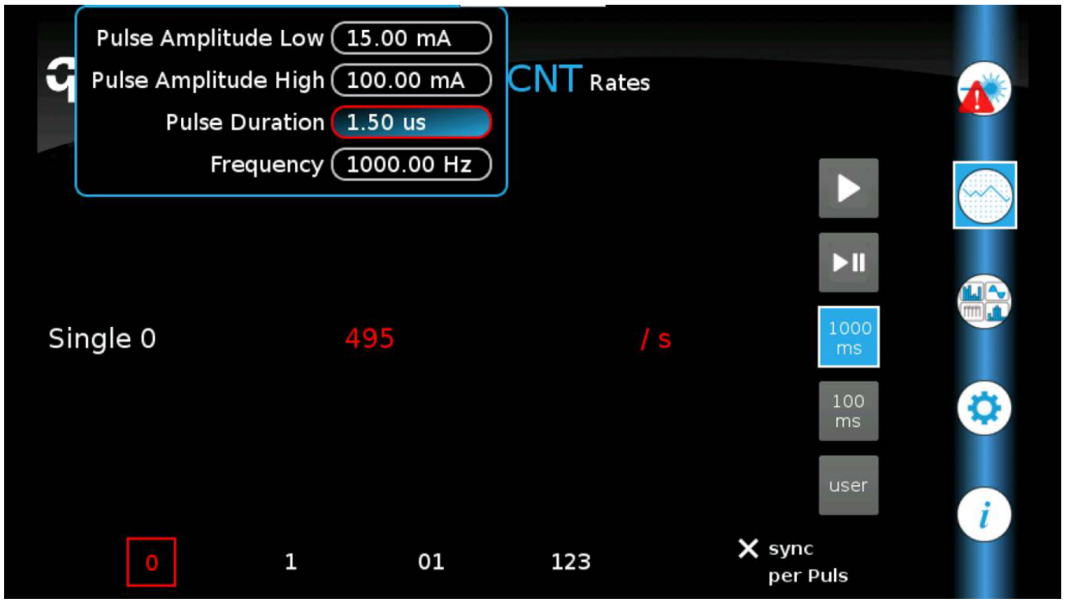


Figure 5: A screenshot of the quCR with the average number of photons per pulse for a given setting.

from anywhere in the quCR software. A single pulse is specified by its amplitude and its duration, and you can modify the frequency with which the pulses are generated.

Switch to the count rate panel to see the signals from the APDs. Please note that (while the *sync* checkbox is active) only counts happening during a laser pulse are displayed, but they are still integrated over the integration interval. So, if you set the frequency to 1000 Hz and the Integration time to 100ms, you can see how many photons are detected during 100 pulses. You can also display the average number of photons *per pulse* if you activate the per pulse checkbox.

The average number of photons per pulse can then be adjusted by changing the pulse duration and the pulse amplitude. You can also try what happens when the laser is switched off.

4.1.2 Measurement example

Here, we set the pulse duration as short as possible such that we still observe pulses with 0.5 photons on average, see Fig. 5. In the Fig. 5 we can see an example of settings for a weak coherent pulse and results of photon number measurement from a detector. In pulse settings we have Frequency of 1000Hz, which means, that each second we send 1000 pulses with specified parameters. In measurement section we see that integration time is 1000 ms and detector is synchronized with source (so it ignores detection events outside of time window, when pulse is expected to come). Detector gives value of 495 'clicks' per second and taking into account the fact that we have 1000 pulses per second, we derive average value of 0.5 photons per pulse.

4.1.3 Didactic Material

1. Why is it of advantage to set the pulse duration as low as possible?
2. Calculate the ratio between pulses with no photon and pulses with one photon and the ratio between pulses with one photon and pulses with two photons for an average photon number of λ.
3. How could one try to measure this effect?

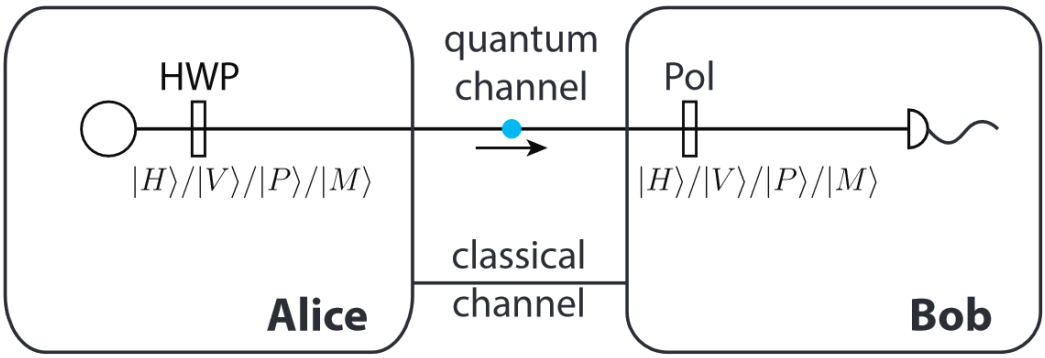


Figure 6: Schematic for the setup of the BB84 experiment with the quED. Instead of a polarizing beam splitter, a polarizer is used.

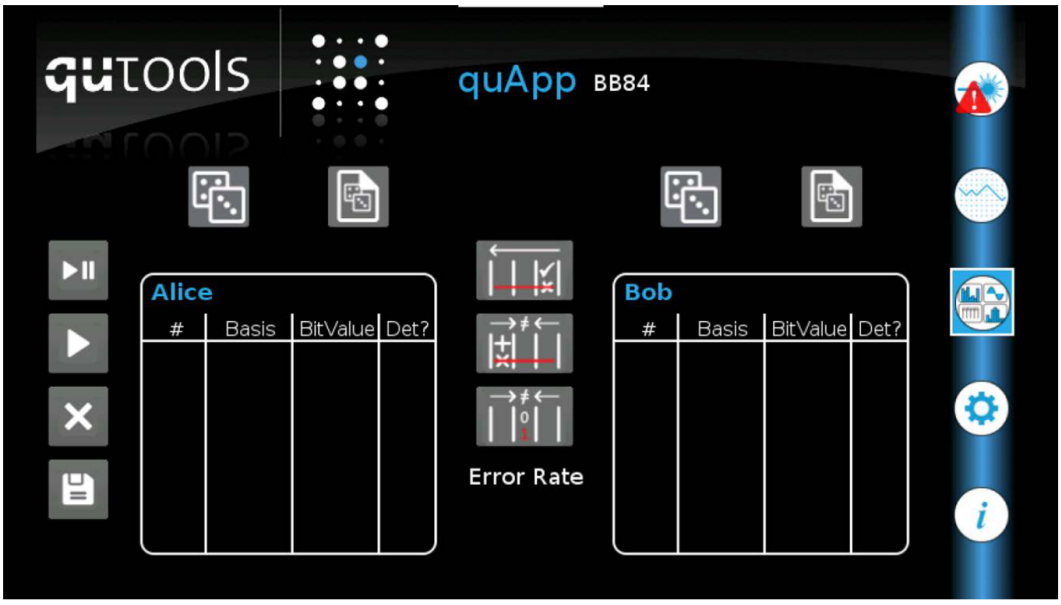


Figure 7: The BB84 tab is made for an semi-automated key exchange with the motorized version.

4.2 Quantum Key Distribution: The BB84 Protocol

4.2.1 Experimental description

Set up the source The source should be set up without the (inner) half waveplate inserted, such that only horizontally polarized photons will be produced. Perform a short alignment of your beam (with screws on mirrors and fiber coupler) to maximize the count rate in the left arm of the quED. The right arm will not be used in this experiment.

Weak coherent pulses Then, set up the number of photons per pulse as described in 4.1 Weak coherent pulses. In practice, the more photons per pulse are sent, the less secure the protocol will be against an attack. But, with less photons per pulse, one needs more pulses to transmit a secret key, limiting the key rate. Since the coupling and detection of photons in the quED has an efficiency of approximately 10%, the actual number of photons per pulse is ten times that of the detected number. For a secure protocol, less than 1 actual photons per pulse should be sent, meaning less than 0.1 should be detected. Though, you might want to turn this number up a bit (to about one detected per pulse) such that a reasonable key rate can be reached, sacrificing security.

Performing an experiment Be careful that a polarizer is used in Bob's Setup instead of a polarizing beam splitter, see Fig. 6. Then switch to the BB84 Tab in the quAPP menu, see Fig. 7. In

this tab, you can run through every step of the BB84 protocol:

1. Alice and Bob need randomly chosen measurement bases and bit values. The randomness can either be mathematically produced (a) or loaded from a file (b). These files can e.g. be produced by hand or with the random number generator tab if you have the quED-HBT Add-On. It is recommended to produce them by built-in tool (dice button).

2. The actual key exchange over the quantum channel can be done run by run (a), or continuously (b). The motors will be set to the angles specified by base and bit value automatically, after which a single pulse specified by the values in the laser tab will be released. On Bob's side, it will be noted if the respective pulse led to a detection event.

3. All operations over the classical channel can be done using the buttons in the middle of the two tables:

   (a) The first button is for communicating which runs led to an detection event. On the first push, the detections are communicated to Alice and all experiment runs without a detection event are marked for deletion. The second push removes them from the tables, while the third push will remove the detected column.

   (b) The second button is for comparing the bases. Like the first button, it can be pressed multiple times, toggling the different states: 1) Bases are communicated, differing ones are marked for deletion. 2) These are removed. 3) The whole column is removed.

   (c) The third button is simulating an error correction protocol, with which an attacker can also be identified. Again, the three states can be toggled, this time regarding errors in the bit values.

   (d) The Quantum Bit Error Rate (QBER) is shown beneath the buttons and can be used to determine how much information an attacker could have about the key.

4. The tables can also be cleared (a) and saved (b) as a csv file, if a flash drive is inserted in USB slot.

4.2.2 Experimental Tasks

1. **Statistical analysis** Perform 10 measurements by 100 bits. After each measurement save your data on a flash drive. You can use data filtering features before saving (first and second buttons) or do a filtering of the data on your own later. It is not suggested to use automatic error correction protocol, because it will simulate a real implementation and so, some of erroneous bits can still be presented in your final data. Afterwards, do 1 measurement, but now for 1000 bits. Random generation can take a quite long time, up to 5 minutes, so do not worry if it looks like it lagged, just wait. Again save the data. Calculate Quantum Bit Error Rate for the first 10 measurements, find its average and 90% confidence interval for the value (write down the equation, which you use for a confidence interval calculation, be careful, that you have done only 10 measurements and this will be reflected in your calculations via a coefficient). Compare it to QBER of one long 1000 bit measurement. What conclusion can you derive?

2. **Source influence analysis** Chose a sufficient number of bits, it is suggested to take a number from a 250-500 interval. For one chosen number of bits perform measurements for 5 different diode currents, while other parameters are the same. Make a note about average number of photons per pulse and save a data table. For each current repeat your measurement at least 3 times. Do the same measurements for 5 different pulse lengths (again, repeat measurement at least 3 times). Plot dependence of QBER with respect to diode current, pulse length. Do not forget to present 90% confidence interval on your plots. What do you see from this graphs?

3. **Long transmission channel analysis** To simulate a long transmission line one can insert a ND filter between Alice and Bob. For this lab you have a set of 4 filters with Optical Density (OD) values of 0.2, 0.3, 0.5, and 4.0. Filters in this lab are ones from Thorlabs: UV Fused Silica Metallic ND Filters (https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=3193). Perform at least 3 measurements for each of the filters. Save your data after each measurement.

Use the data from manufacturer to get a transmission value for your wavelength and recalculate transmission value into effective length of an optical fiber if it has loss of 0.2 dB/km. Plot dependence of QBER with respect to length of a fiber together with 90% confidence interval. Comment on the plot.

4.2.3 Didactic Material

1. How can one improve the efficiency?
2. How can the basis choice at Bob's be made really (quantumly) random?
3. What is the simplest attack on such a system? What is the special problem of the system? (Hint: Think about authentication.)

5 Calculation tasks

1. In a real communication scenario Alice sends a photon to Bob, who is 250 km away, via a fiber line. The fiber has a loss rate of 4% per km.
   (a) Find the loss coefficient β in that fiber, where β is a loss coefficient per kilometer from equation for photon rate attenuation ($n = n_0 e^{-\beta L}$), where n_0 is initial photon rate and n is a photon rate after propagation for L km distance.
   (b) What fraction of the photons sent by Alice will reach Bob.
2. Assuming that Alice has a perfect single-photon source and Bob is measuring with a HWP and PBS, sketch the photon transfer rate and the secret bit rate as functions of the distance and estimate the maximum possible secure communication distance given the following parameters (as a condition for secure channel use QBER$\leq$11%):
   (a) photon loss in the fiber communication line: $\beta = 0.05 km^{-1}$
   (b) emission rates of Alice's source: $n_0 = 2 \times 10^7$ and 2×10^{10} photons per second
   (c) quantum efficiency of the photon detectors: $\eta = 0.1$
   (d) frequency of dark events that are synchronized with Alice's photons in each of Bob's detectors: $f_d = 10 s^{-1}$
3. Solve task 2 also for experimental setup restriction with two polarizers instead of HWP and PBS on Bob's side and compare your results.
4. Comment on limitations of the performed experiment when compared with task 2.

References

[1] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.