T2E1 Report: Quantum Information and Quantum Key Distribution

6.2410 Quantum Engineering Platforms
Daniel Sanango

I. Introduction

In this station, we use a quCR to analyze photon states using a Hanbury Brown-Twiss setup. After this, we used the quCR to perform a Quantum Key Distribution (QKD) experiment to analyze data processing techniques, error identification procedures, and error correction methods.

II. Week 1 Summary

The objective of this laboratory exercise was to measure a second-order correlation function $g^{(2)}(0)$ from a Hanbury-Brown Twiss interferometry setup. Figure 1 demonstrates a schematic of our laboratory setup. Following the paths labeled with APD 1 and APD 2, a laser beam passes through a fiber beamsplitter. The fiber beamsplitter's outputs then go into the APDs, and a quCR interprets the counts on each detector on a user-defined integration time. The quCR also interprets coincidence counts, count values for photons detected by the APDs at specific coincidence windows (set to 30[ns] by the machine).

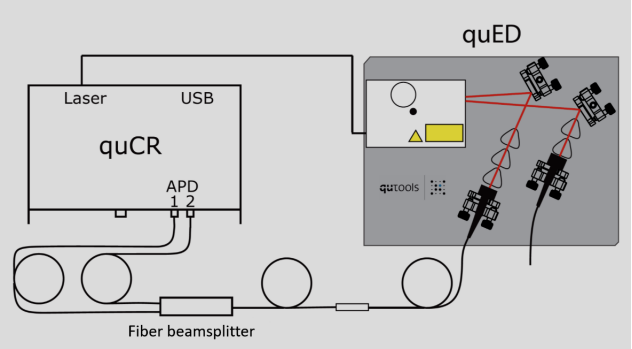

Fig. 1: HBT Setup Schematic [6.2410 Github]

The $g^{(2)}(0)$ function is formally defined as:

$$g^{(2)}(0) = \frac{< \hat{n_1}\hat{n_2} >}{< \hat{n_1} >< \hat{n_2} >} \tag{1}$$

Writing this equation in terms of parameters the quCR provides us, we can write...

$$g^{(2)}(0) = \frac{R_{12}}{R_1 R_2 \Delta_w} \tag{2}$$

Where,...
R_{12} = detector coincidences (cnt/ms)
R_1 = APD 1 count rate (cnt/ms)
R_2 = APD 2 count rate (cnt/ms)
Δ_w = integration time (ms)

We used a Python interface to extract the relevant variables from the quCR. We took numerous samples from the quCR for a time period of 30 seconds and determined a mean, variance, and standard deviation from an integration time of $\Delta_w = 100[ms]$ and $\Delta_w = 1000[ms] = 1[s]$. Table I demonstrates our findings.

$\Delta_w[ms]$	μ	σ^2	σ
100	0.992	0.041	0.204
1000	0.986	0.0059	0.07727

TABLE I: $g^{(2)}(0)$ measurements for various integration times using an HBT setup at laser current = 40[mA]

We see that a lower integration time window increases the measured statistics. This is expected, as shorter time windows preserve more temporal resolution, capturing finer photon behavior. In contrast, longer integration windows tend to average out fluctuations, leading to a reduced variance.

For a single photon source, we would expect zero photon coincidences at the same time. Thus, we would expect the correction function with 0 time delay ($g^{(2)}(0)$) to be about 0. From our gathered data, we see the mean is about 1, meaning this setup does not demonstrate single photon source behavior. At this laser current, it seems to be acting more as a coherent state, as the $g^{(2)}$ function is known to be constant at value 1. This makes sense, as given our laser power settings, we expect numerous photons to pass through the system, thus giving a photon at numerous time delays.

Next, we used a heralded HBT setup to analyze $g^{(2)}(0)$. Figure 2 demonstrates the laboratory setup utilized.

Given the new setup, we can rewrite $g^{(2)}(0)$ as demonstrated in Equation (3):

$$g^{(2)}(0) = \frac{N_{012} N_0}{N_{01} N_{02}} \tag{3}$$

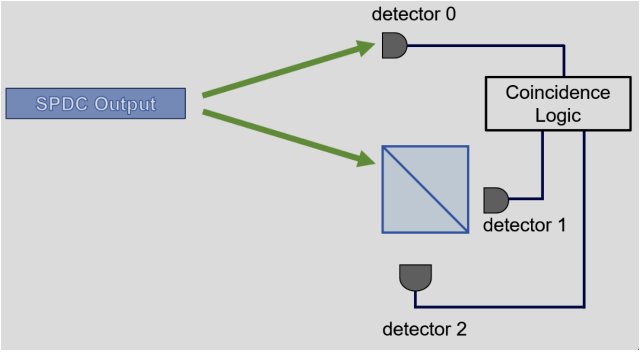

Fig. 2: Heralded HBT Setup Schematic [6.2410 Github]

$\Delta_w[ms]$	μ	σ^2	σ
100	0.134	0.01231	0.11095
1000	0.1269	0.001	0.03175

TABLE II: $g^{(2)}(0)$ measurements for various integration times using a heralded HBT setup at laser current = 40[mA]

Table II demonstrates our statistical calculations for our new setup. Our measured statistics are noticeably smaller than from the unheralded HBT setup in Figure 1. We again see that lower integration time windows yield higher statistics, following the same reasoning from Figure 1's data analysis. The lower mean value implies that there are often not coincidences at time 0. Because of this, I would expect the output state to be a number state at about $n = 1$. Thus, this setup acts moreso as a single-photon source.

III. Week 2 Summary

The objective of this laboratory exercise was to analyze Quantum Key Distribution (QKD) systems and quantum bit error rate methods. Figure 3 demonstrates our optical setup. Alice encodes her basis and bit with a half waveplate, while Bob interprets the basis and bit with a polarizer. The quCR can set waveplate and polarizer angles.

This method closely follows the BB84 protocol, which uses polarization states to define bases and bits. The "+" basis encodes the $|0\rangle$ and $|1\rangle$ states, while the "x" basis encodes the $|D\rangle$ and $|A\rangle$ states. Notably, the "+" basis is a 45 degree rotation from the "x" basis. If the sender, Alice, sends a bit in the "+" basis (say $|1\rangle$), the receiver, Bob, must measure the bit in the correct basis to get a definitive result. If Bob measures in the wrong basis, he will get a random measured bit.

While the quCR offers a simple Python function for setting waveplate and polarizer angles, the internal motors have an internal offset relative to each other. To rectify this, we set the waveplate to 0 degrees and rotated the polarizer until we achieved a maximum count rate value on the quCR. The maximum count rate is used because, logically, when the half waveplate's output polarization enters the polarizer, the maximum output from the polarizer is when the polarizer's polarization axis aligns with the input polarization. Thus, when the half waveplate is at 0 degrees, the polarizer should be set

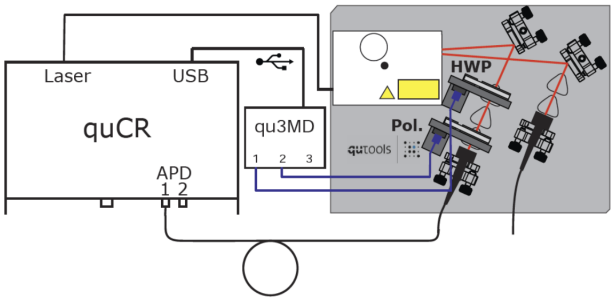

Fig. 3: QKD Setup Schematic [6.2410 Github]

at the desired angle with an additional measured offset. The necessary offset for our setup was $\theta = 31.77\,\text{deg}$.

It is important to note the different effects and, thus, angle settings for the waveplate and polarizer. For half waveplates, light reflects across the slow axis, essentially doubling the input angle. Our given motor code already accounts for this. For a polarizer, light fully transmits when the polarization is parallel to the polarization axis but is fully blocked when the polarization is perpendicular to the polarization axis.

In addition, we changed the laser setting from CW mode to pulsed mode. QKD relies on single photon transmission, as if non-single photon sources were used, an eavesdropper could split the light with a beamsplitter and interpret the split light without interrupting the light arriving to Bob. The laser frequency was set such that, with a 100[ms] integration time window, we got mostly 1 count, with an occasional fluctuation to 0 counts.

Once this was accomplished, we sent a key through our QKD system. Alice and Bob's basis and bit selections were randomly generated and interpreted as the necessary angles for the half waveplate and polarizer. After we obtained our data, we performed a bit sifting process. The following criteria were enforced:

1. If the bases match, keep the bit. Otherwise, throw it out
2. If the measured bit is 1, keep the bit. Otherwise, throw it out.

Criteria 1 was used because, in the typical BB84 procedure, Alice and Bob share their bases and keep bits associated with matching bases. This allows them to create a basis key without actually revealing any bit information to eavesdroppers.

Criteria 2 was used because of the greater error sources active when using the 0 bit. For instance, the quCR has a known error rate of 30% for QKD analyses. In addition, photon absorption during the waveguiding process and fiber coupling process to arrive at the quCR default to a detection of 0 photons, meaning most errors are associated with the 0 bit.

Further components also contribute towards imperfect data. Imperfect polarizations setups, for instance, could count as the inverse bit instead of the expected bit. With numerous measurements, even with a 1 degree deviation in Bob's polarizer angle, uncertainty in measurement is small but nonzero. Dark

counts can also contribute to uncertain measurements, as the wrong bit may be reported by chance from environmental and device factors.

We gathered 200 bit and basis pairs. Out of these 200, 11 matched both criteria. It is important to note that, because of our small sample size, we are likely to make claims that are not statistically backed. Having only 11 matched criteria somewhat makes sense, as we expect only 50% of bases to match between Alice and Bob. After that, considering the errors described above, we expect more 0 bits to be detected than 1 bits.

To analyze the quantum bit error rate (qBER) of our sifted bits, we first have Alice and Bob reveal a certain length of their bits over a classical channels. Because Eve can also obtain this data, the revealed bits are thrown out after sharing, giving Eve no additional information about the QKD system. Using our sifted bits, we achieved a 0% error rate. This is likely because of our small sample size, as BERs are typically expected to be between 5%-10%. It is likely that we simply got lucky in getting no errors. Simulating a 10% error rate, however, we do get around a 10% error as expected. This was done with an applied bit-flipping vector with assigned flipping probability.

Another error identification and correction method is through a Hamming matrix. Partitioning our sifted bits into groups of 7, we can multiply our bits by a pre-determined matrix to identify and correct errors. The advantage of this method is that the time complexity is more ideal for larger datasets. We again achieved a BER of 0%, most likely because of our small sample size. Simulating a 10% error rate, however, we do get around a 10% error as expected. This was done with an applied bit-flipping vector with assigned flipping probability. This also allows Alice and Bob to reveal a minimum amount of information to eavesdroppers, preventing too much information about their setup from becoming public.

One way to improve SKR is to use a more efficient single-photon detector. For instance, superconducting nanowire detectors, known as SNSPD's, have lower dark counts and higher detection efficiency. With these parameters, photon sources can be interpreted much faster and with greater precision. Although SNSPD's have greater precision, they are also required to operate at cryogenic temperatures, increasing implementation costs and system size.

Once the BER is known, one can determine if an eavesdropper is present by noting variations in the BER.

To amplify privacy, we can then remove the last 3 bits of each of the 7-bit chunks. This eliminated an eavesdropper's gained information about Alice and Bob's key since, without the full 7-word chunk, no useful information can be interpreted.

IV. Conclusion

In conclusion, we have demonstrated methodologies for analyzing autocorrelation functions and interpreting quantum key distribution encryption methods. By measuring the autocorrelation function, we can determine the photon state of a given laser system. QKD offers a non-classical method of encryption that is difficult to intercept because of an eavesdropper's inability to interpret a quantum state without disturbing it. QKD is extremely useful in secure communications, as it provides greater levels of information security than current classical communication methods.