Major Qualifying Project
Time-Energy Entangled Quantum Key Distribution Without Franson Interferometry

Benjamin Child and David Medich
Worcester Polytechnic Institute

Evan J. Katz and John Lekki
National Aeronautics and Space Administration, Glenn Research Center LCP0

(Dated: April 25, 2019)

Abstract

Traditional encryption protocols are becoming less secure as quantum computing becomes more viable. Quantum Key Distribution(QKD) uses quantum entanglement to distribute provably secure encryption keys. Previous QKD protocols have used polarization-entangled photons that can be easily measured, but cannot be easily transmitted over long distances. This project will use time-energy entanglement which is more challenging to verify but can be easily transmitted over long distances. This project demonstrates Time-Energy entanglement and proposes a method of verifying security independent of Franson interferometry verification.

CONTENTS

ACKNOWLEDGEMENTS

Thank you to Andrew Mendizabal, Alexis Buzzell, Taylor Trottier, Erin Morissette, Bry Voydatch, Nathaniel Mione, and Zoe Mutton for help on my presentation.

Thank you to my parents for supporting me and my interest in science over the course of my life.

Thank you Mr. Blueglass for encouraging me to pursue science and instilling in me an actual work ethic. This paper didn't have a rubric but I tried my best.

Thank you, the hammock in the physics lounge, for providing a place to do 90% of my project and take naps between classes

Thank you, Angela Calvi, for your help troubleshooting my code.

Thank you, Professor Aravind for your assistance and advice on the technical aspects of my project.

Thank you, Dr. John Lekki and Dr. Evan Katz for your mentorship and assistance with this project and my summer work at NASA.

Thank you most of all, Professor Medich for your guidance and mentorship on this project. I will absolutely try to do good things with my life.

I. IMPORTANCE OF QKD

Classical encryption systems use algorithms based on complex prime factorization to secure data. These systems are secure because classical computers are unable to solve these problems in a reasonable amount of time. As quantum computers become more and more viable, this type of encryption is no longer secure. Quantum computers are very adept at solving these types of factorization problems and can undo traditional public key encryption quickly. To maintain the security of sensitive information in the age of quantum computing, encryption methods must adapt. The only provably secure methods of encryption to date rely on hand-delivered encryption keys, such as in One-Time Pad[1], but these methods are not currently feasible for secure high-speed transactions. This leaves Quantum Key Distribution as the next step in secure communications once quantum computing is common. I present a new Quantum Key Distribution method which doubles theoretical efficiency from previous methods.

Quantum Key Distribution is a series of protocols that usess entangled photons to distribute large amounts of random information between two parties. Because the random information is shared securely between these parties, it can be used to encrypt sensitive data which can then be transmitted over classical lines. Photon entanglement is a phenomenon where the states of two photons become highly correlated in a way which violates Bell's Inequalities [2].

Polarization entanglement is the most common type used for QKD[3], in which two photons' polarization states become highly correlated. Measurements of the polarization of these photons along any basis will be correlated, although entirely random. These photons maintain their entanglement even over very large distances[1]. Quantum Key Distribution exploits this by sending the entangled photons to parties who need to encrypt sensitive data. Each party measures their photon's polarization in one of two axes randomly. They then publish which axis they chose, and discard any photons that are measured in different axes. In order to verify security, a small portion of the results are published publicly, and the error rate can be calculated from there. If an eavesdropper is present the entanglement will be broken, error will be introduced to the measurement and the key can be discarded[3].

[1] This is the case in vacuum or any medium through which photon coherence is high. Any interactions constitute ”measurement” and will break entanglement. Free space and fiber optic cabling often approximate these conditions

Once an entangled photon has been measured, the entangled photon is broken. Due to the no cloning theorem, it is impossible for the eavesdropper to recreate that photon's state and send it on to the intended recipient. This method is provably secure because no sensitive data is actually shared until after the security of the key is verified.

Time-Energy(TE) entanglement is a different type of entanglement, but can also be used for QKD. In TE entanglement, photons have highly correlated time of emission and photon energy.[4] A single photon is sent through a crystal known as a "Spontaneous Parametric Down Conversion"(SPDC) crystal. While the photon travels through the crystal, it spontaneously splits into an entangled pair. This type of entanglement is used for QKD by employing measurements of emission time and filtering on the basis of photon energy. The current method of TE QKD uses a type of photon interference measurement known as Franson Interferometry, initially described in Franson et. al[4] and demonstrated by Kwiat et al. [5]. This type of interferometry can be used to distribute random information securely with extremely high data rates[6]. Time-energy entanglement is robust over long distances, and can be transmitted through fiber optic cabling making it preferable to polarization entanglement for earth communications [1].

Unfortunately, Franson interferometers are extremely challenging to build, and become unaligned easily [7]. The goal of this project is to demonstrate a Franson interferometer and proposes an alternative to Franson interferometry in TE QKD.

II. ENCRYPTION PROTOCOL

QKD provides two parties with identical strings of random information. One-Time Pad(OTP) encryption uses this to encrypt information later transmitted over classical channels. The encryption protocol uses modular arithmetic as shown in Figure 1. In this example, simple integers are used for both the raw data and the key. Later will be shown an example where images are encrypted using this method. In that case, each pixel value was encrypted the same way. OTP is used because there is no positive verification for correct "guessing". Due to the nature of the encryption, a 10 digit cipher could contain any 10 digit number in existence. The only way to find the correct one is to have the correct key.

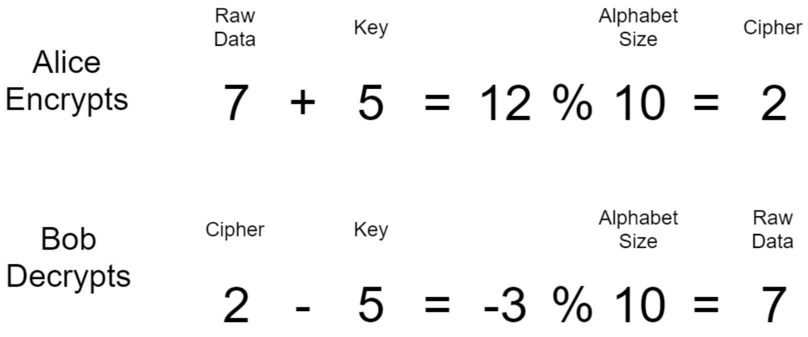

FIG. 1. One-Time Pad encryption uses modular arithmetic

III. QKD PROTOCOL

The key distribution protocol includes three entities: Alice (A) is transmitting a encryption key to Bob (B) with an eavesdropper or noise source Eve (E). While keys can technically be transmitted from a centralized neutral source, this encryption protocol requires Alice to own the entanglement source.

Alice's source will emit two photons with emission uncertainty of $\Delta\tau_1$ and frequency uncertainty $\Delta\nu_1$. Current systems often use SPDC sources as they fit the requirements of this application. However, it is possible to use any source which emits two photons, one of which has an emission time uncertainty much larger than the second. For typical SPDC sources, the emission uncertainty Δ_τ is determined by the length of the crystal [4].

Both Alice and Bob have Single Photon Detectors and timing systems with binning capabilities of $\Delta\tau_2$ such that $\Delta\tau_1 \gg \Delta\tau_2$ with a minimum requirement $\frac{\Delta\tau_1}{\Delta\tau_2} > 2$. For the sake of security, we will assume that Eve has access to a perfect timing system, which allows them to measure the intercept time exactly.

Alice and Bob share a sync pulse which can either be through a classical channel, or an optical pulse through the fiber channel. Eve has access to this sync pulse as well, and compares any intercepted photons to this sync pulse for time tagging purposes. Alice begins by emitting a pair of entangled photons. She separates the photons and observes one. This observation will fall within one sync cycle. The sync cycle is broken down into bins with width $\geq \Delta\tau_2$. Each bin represents one ”letter” of the encryption key alphabet.

A. The Franson Method

In the Franson Method, the second photon is observed by Bob. Both parties send their photons through separated Mach-Zehnder interferometers shown in Figure 2. These interferometers are set up in such a way that there is no single-photon interference observed, typically by a path length difference exceeding 100µm. For the imbalanced Mach-Zehnder systems used in the Franson method, the path length difference is typically large, on the order of several centimeters. After passing through these systems, 3 types of coincidence measurements can be made: long-long(l-l), short-short(s-s), and long-short(l-s). The l-l and s-s cases are indistinguishable and make up 50% of all received photons. The l-s and s-l cases are non-interfering background as the photons travel separate paths. They are easily filtered since there is a large delay in arrival times. This filtering caps efficiency at 50% As one leg of one of the Mach-Zehnder systems is changed in micron-level steps, a sinusoidal change in coincidence counts determines a non-local change in the wave function. This violates Bell's inequality [5] [2] and verifies integrity of the entanglement. Fringe visibility above 50% exceeds the classical limit and is required for this validation. If an eavesdropper had observed any of the photons, the fringe visibility would drop, and both parties would immediately be alerted to the attack.

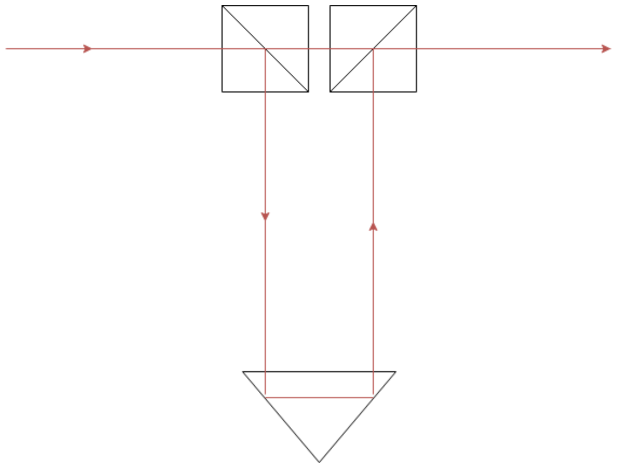

FIG. 2. An unbalanced Mach-zehnder interferometer consists of two beamsplitter cubes and a retroreflector. This system has a large path length difference which prohibits self-interference

IV. METHODOLOGY

QKD requires that the key be the same size as the data being transmitted [1]. In order for Time-Energy systems to be viable, entanglement sources must emit large numbers of photons pairs. These types of sources are known as ”high-brightness”. This project tested a high-brightness source to demonstrate TE entanglement and verify the source for future experimentation.

A. Franson Method

The source used was a periodically poled MgO-doped $LiNbO_3$ (MgO:LN) non-degenerate photon pair source. This source exhibits spontaneous parametric down conversion (SPDC), a non-linear optical response that generates two entangled photons from a single photon. The crystal was pumped with 532nm photons from an Nd:YAG fiber coupled laser. Photon pairs consisted of 794nm and 1614nm photons.

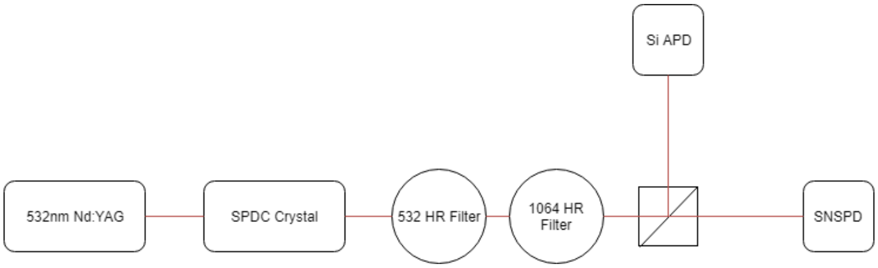

FIG. 3. The sorting optics for the pair detection system

The sorting optics are shown in Figure 3. Two filters are used, one high reflective 532nm filter to remove unconverted pump photons, and one 1064nm filter to remove pump photons from the source laser. A dichroic mirror splits the photons into two beams, one of 794nm photons and one of 1614nm photons. The 794nm photons were measured using a Silicon Avalanche Photodetector (Si APD) calibrated for 800nm. The 1614nm photons were measured using a Superconducting Nanowire Single Photon Detector (SNSPD). The function and calibration of the SNSPD is described in Appendix B. Outputs of these detectors were connected to a time tagging device to measure coincidences.

Preliminary verification of photon entanglement was achieved through direct coincidence counting. Normally distributed coincidences would imply that photon emission times were at least highly correlated, and acted as an equipment test. The preliminary un-adjusted measurements showed maximum true coincidences of 350kHz at an SNR above 1 [8]. This showed photon emission times were at least highly correlated. It is important to note that this does not verify entanglement as no violation of Bell's inequality can be proven. To prove entanglement, an interferometer setup based off of Franson et. al was used.[4] Two separate but nearly identical Mach Zehnder interferometers were built, one for each wavelength of interest. The short path measured approximately 10cm, and the long path approximately 30cm. This ensured that there was no single photon interference while staying within the crystal's coherence length. The retroreflector of the long arm of the 1614nm interferometer was moved using a stepper motor with 0.5nm resolution. 5 microns were scanned with 10nm resolution. Fringe visibility of 58% was observed which is a violation of Bell's inequality [9]. This verified the entanglement of the source.

This is necessary to prove entanglement in sources of this nature but has several drawbacks. Primarily, these Franson interferometers are challenging to build and maintain. Extreme precision is required to balance the interferometers, which is challenging when the systems are separated by long distances. Additionally, nm size steps in prism location are required to verify visibility. While possible in a laboratory setting, applying this system in an application with vibration or large changes in temperature is challenging. Attempts have been made to create a fiber-only system[7][1] using fiber heating to increase path length, but many of the existing challenges remain. These drawbacks mean that Franson interferometry is challenging with current technologies.

B. Proposed Method

I propose a new method of key distribution which does not employ Franson Interferometry. In order to verify key integrity without Franson interferometry, a monochrometer is employed. Here, Bob sends the photons he receives from Alice through a monochrometer with a bandwidth of $\Delta\nu_b$ where

$$\Delta\nu_b = \frac{1}{4\pi\Delta\tau_1} \tag{1}$$

This makes use of Heisenberg uncertainty. Franson et. al. discuss a two-level system, from which two photons are emitted. The first state has a lifetime of τ_1 and the second has lifetime of τ_2 where $\tau_1 \gg \tau_2$. Franson states the uncertainty of the emission time of the photon pair is initially τ_1, but when one photon is observed the wave function collapses nonlocally, and thus the time of emission of the other photon is immediately known to within τ_2. This two level system is interchangeable with SPDC sources[5]. Because the time uncertainty is defined by the crystal, it is much larger than the binning capability of the timing system. Because time uncertainty is large, the energy can be known very accurately. It is important to note that not all sources will take full advantage of this, so sources that have a very small known bandwidth are needed.

Since information is sent as single photon packets, Eve can not simply be a passive observer. Any photons she absorbs will be removed from the set that Bob measures, and he can then see that the integrity of the encryption has been compromised. To avoid this, Eve absorbs and re-emits the photons she receives as quickly as possible, hoping to pass them off as the originals. Assuming a worst-case scenario, she receives the photons at the beginning of every bin and has the full bin width to re-emit the imposter photon. Since the imposter photon has a much smaller time uncertainty, the energy uncertainty must be large. This increase in energy uncertainty is an increase in bandwidth, and imposter photons can therefore be filtered out easily using the monochrometer. All original photons pass through the monochrometer without issue.

Assuming that the sync pulse travels the same distance as the entangled photon, or that the difference in travel time is known, Bob will receive the second entangled photon and bin it in the same "letter" as Alice. Alice and Bob then take turns verifying the integrity of a subset of their key over the classical channel. This verification is simple, requiring one party to state the time stamp of the sync pulse of a certain letter of the key. The other party will then respond with the letter they received during that sync cycle. As long as this verification is successful to the degree required by the encryption algorithm (typically no greater than 20% noise)[6], both parties can be sure that the keys are secure and shared only between themselves.

C. Protocol Security

This key distribution protocol is proven secure against both passive AND active eavesdropping attempts. Passive security is relatively simple and is based entirely off of the single-photon nature of the key distribution. Since the parties are verifying both ways across a public channel, if Eve is passively eavesdropping, she is observing the photons and Bob will therefore not receive them. This verification ratio then ensures that if Bob is losing enough photons for Eve to gain any usable information, Alice and Bob can both tell stop transmission. Additionally, only random data is being distributed, not the actual sensitive information. The sensitive data is only encrypted and transmitted after key integrity has been verified.

Preventing against active eavesdropping is of course harder. With traditional polarization-entangled QKD, the random basis of the measurement acts as a barrier for the re-emission of the photons. The eavesdropper may re-emit a photon polarized correctly in the basis she measures in, but that photon will not share a state with the other photon, meaning that if Bob measures it in a different basis he will get the wrong answer. Without the Franson interferometers, we are not measuring in randomized bases. In order to ensure security in the case of an active eavesdropper we add a monochrometer with bandwidth $\Delta\nu_b$. The increased energy uncertainty of imposter photons means that they are filtered by the monochrometer, and the error rate properly reflects the number of true photons received.

V. SIMULATION

A simulation of the proposed monochrometer system was created in python to demonstrate the security (Appendix A). This simulation used PNG images as sample data to encrypt. The image was first turned into an array of pixel values. The photon pairs were then generated using Python's random function. This function uses pseudo random numbers and is not sufficient for actual cryptography, but is good enough for this demonstration. Each photon pair is given a value between 1 and 10, and a wavelength. In reality, each photon pair would consist of two timings and two wavelengths, but it is assumed Alice has negligible losses due to having the source. The photon wavelength is a random value within the wavelength uncertainty.

In a true QKD application, the wavelength is not uniformly distributed within the uncertainty. While the time and energy uncertainties are theoretically step functions, real optics are rarely so linear. For this application however this assumption is suitable.

The key is then transmitted to Bob, at which point eve is able to disrupt it. Assuming for security that eve collects every lost photon up to a given noise level, she re-emits each.

At this point, photon wavelength of the imposter photons is calculated using the new time uncertainty.

For the sake of security, we assume a worst-case scenario in which Eve receives each photon at the beginning of the bin, and takes the entire bin width to re-emit the imposter photon. This gives her the maximum possible time uncertainty and the most wavelength precision. After all photons have been recorded, Alice and Bob compare a subset of their photons. The error rate is calculated, and the key is rejected if it is above 20%.

The image is then encrypted using the accepted key. Each pixel is defined by 4 values: Red, Green, Blue, and Opacity. Each of these values is an 8-digit decimal ranging between 0 and 1. One-Time Pad encryption was employed using a 10^8 digit alphabet for convenience. Python's modular arithmetic handling required a modulation about 1.000000001 to avoid errors with values of 1 and 0.

VI. RESULTS

A. Franson Interferometry

The Fringe visibility was 58%, shown in Figure 4. This exceeds the classical limit of 50%, proving that the source is a valid entanglement source. The measured maximum of 350kHz with an SNR above 1 means that this source is a valid high-brightness source.

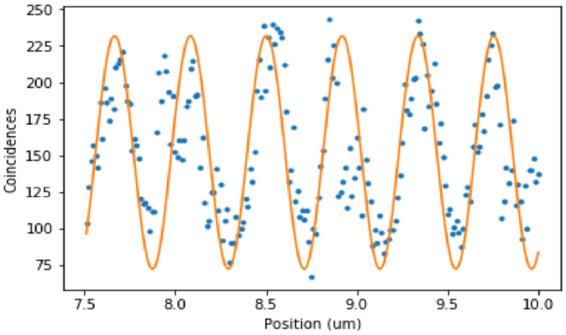

FIG. 4. Fringe visibility is shown exceeding 50%, violating Bell's inequality[9]

This verification means that this high-brightness, low SWaP source is suitable for space applications, and shows promise in future space-based applications.

B. Proposed Monochrometer Method

The simulation was used to verify encryption integrity in high and low error scenarios. The first, shown in Figure 5 used an error rate of 17% and a worst-case scenario in which all error was due to Eve. Bob was able to measure a noise level of 16.6%, showing that almost all imposter photons were filtered out. The following images are visual representations of the encryption process, and the "Bob" image shows the fidelity of Bob's key. The proof of the security is that at higher error rates, Bob's image loses fidelity. If Eve's imposter photons were able to pass through the monochrometer, Bob's image would look exactly like the original. The fact that Bob loses every photon that Eve gains shows that the monochrometer is accurately filtering the imposter photons.

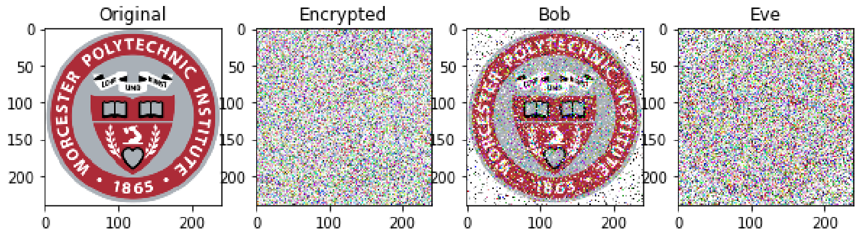

FIG. 5. These images were encrypted using an error rate of 17%. A phantom of the image can be seen in the Eve image, however the 20% error cited includes key obfuscation.

The second, shown in Figure 6 used an error rate of 1% and the same worst-case scenario. Bob's measured error rate was 0.9%, again showing that almost all imposter photons were filtered.

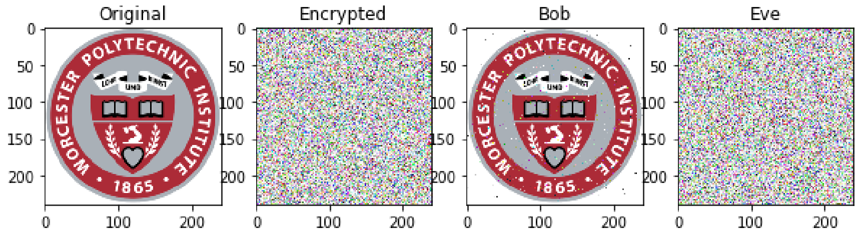

FIG. 6. These images were encrypted using an error rate of 1%. No phantom can be seen in Eve's image, but some pixels are lost.

The third, shown in Figure 7 used an error rate of 0.01%. Bob's measured error rate was 0.012%. This is interesting as it is higher than the induced error for the first time. This implies that (i) high error rates result in the highest percentage of false positives and (ii) the introduction of the monochrometer increases random loss even when the bandwidth is smaller than the monochrometer.

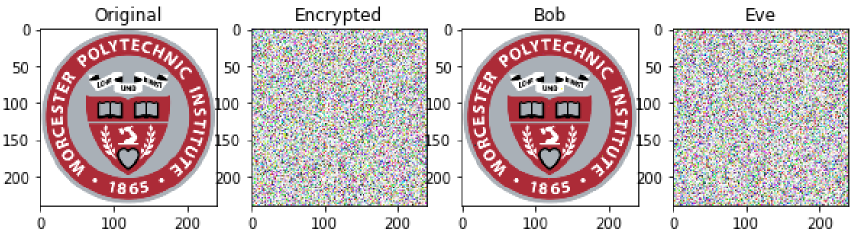

FIG. 7. These images were encrypted using an error rate of 0.01%. No phantom can be seen and almost no pixels are lost.

VII. CONCLUSION

The simulation of the monochrometer method demonstrates the viability of non-franson time-energy quantum key distribution. This circumvents the sensitivity of Franson Interferometers while maintaining the benefits of TE entangled photons for QKD. The monochrometer method had a theoretically low induced error, and the total error was almost entirely attributed to photons lost pre-monochrometer. This stands in contrast to the Franson method which has a minimum photon loss of 50% due to discarding the l-s and s-l photons. Since keys in QKD must be the same size as the data being transmitted, increase in data rates is the primary goal of new QKD systems. This method doubles the amount of photons that are used and is limited primarily by the deadtime and saturation points of the single photon detectors.

[1] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Physical Review Letters **98** (2007), 10.1103/physrevlett.98.060503.

[2] J. Brendel, E. Mohler, and W. Martienssen, Europhysics Letters (EPL) **20**, 575580 (1992).

[3] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 711 (1984).

[4] J. D. Franson, Physical Review Letters **62**, 22052208 (1989).

[5] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, Physical Review A **47** (1993), 10.1103/physreva.47.r2472.

[6] N. Gisin and R. Thew, Nature Photonics **1**, 165171 (2007).

[7] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, and et al., New Journal of Physics **17**, 022002 (2015).

[8] E. J. Katz, B. Child, I. R. Nemitz, B. E. Vyhnalek, T. D. Roberts, A. Hohne, B. M. Floyd, J. Dietz, and J. D. Lekki, Free-Space Laser Communications XXXI (2019), 10.1117/12.2508736.

[9] I. R. Nemitz, J. Dietz, E. J. Katz, B. E. Vynhalek, B. Child, B. M. Floyd, and J. D. Lekki, Nonlinear Frequency Generation and Conversion: Materials and Devices XVIII (2019), 10.1117/12.2509849.

Appendix A: Code

```
import numpy as np
#np.set_printoptions(threshold=np.nan)
import pandas as pd
import random as rand
import matplotlib.pyplot as plt
import matplotlib.image as mpimg
import math as math

c = 3*10**8
alph  = 10
crylen = 10 #length of the crystal in mm
wl = 800 #wavelength of the 2ndary photon
bintime = 10**-12
monochrom = 10**-4 #monochrometer slit width
alice = ([])
eve = ([])
bob = ([])
crysk = 1 #The probability that a pair will be produced
noise = 6 #The probability that a photon pair will be intercepted
img = mpimg.imread('WPI_logo.PNG')
imgshape = img.shape
enc = np.zeros(imgshape)
dec = np.zeros(imgshape)
eveim = np.zeros(imgshape)
plt.imshow(img)
plt.show()
awl = {}
bwl = {}

def photonwl(sigmax, wlcent):
    temp = (wlcent**2)/(4* math.pi *c*sigmax)
    return(rand.uniform(wlcent-temp,wlcent+temp))

#Generates the random key
i = 0
for i in range(img.size):
    alice.append(round(rand.uniform(0,1),8))
    awl[i] = photonwl(crylen ,wl)



#Encrypts the image using the key
i=0
for x in range(img.shape[0]):
    for y in range(img.shape[1]):
        for z in range(img.shape[2]):
            enc[x,y,z] = round(((img[x,y,z] + alice[i])%1.00000001),8)
            i+=1

plt.imshow(enc)
plt.show()

#disrupts key
i=0
for i in range(len(alice)):
    if rand.randint(1,noise) ==1:
        eve.append(alice[i])
        bob.append(alice[i])
        bwl[i] = photonwl(c*bintime,wl)
    else:
        eve.append(round(rand.uniform(0,1),8))
        bob.append(alice[i])
        bwl[i] = awl[i]
    i+=1

i=0
y = 0
tot = 0
for i in range(len(bwl)):
    if i<len(bwl):
        if abs(bwl[i]-wl)<monochrom:
            y+=1
            tot+=1
        else:
            tot+=1
    i+=5

print(1-(y/tot))
if 1-(y/tot) < 0.2:
    #decrypts the alice image using the key
    i=0
    for x in range(img.shape[0]):
        for y in range(img.shape[1]):
            for z in range(img.shape[2]):
                if(abs(bwl[i]-wl)>monochrom):
                    dec[x,y,z] = round(((enc[x,y,z]
                    round(rand.uniform(0,1),8))%1.00000001),8)
                else:
                    dec[x,y,z] =
                    round(((enc[x,y,z] - bob[i])%1.00000001),8)
                i+=1
    plt.imshow(dec)
    plt.show()


    # decrypts the eve image using the key
    i=0
    for x in range(img.shape[0]):
        for y in range(img.shape[1]):
            for z in range(img.shape[2]):
                eveim[x,y,z] = round(((enc[x,y,z] - eve[i])%1.00000001),8)
                i+=1
    plt.imshow(eveim)
    plt.show()
else:
    print('Too␣much␣noise␣to␣verify␣security')
```

Appendix B: SNSPD

The efficiency setup for the 4-channel Quantum Opus SNSPD is shown in Figure 8. In order to measure channel efficiency, a 1600nm fiber coupled CW laser was filtered and attenuated and connected to a 4-way fiber splitter. Splitter attenuation was measured using the same 1600nm laser and a traditional bucket photodetector, and all outputs were found to be equivalent. Each output of the splitter was then run through polarization controllers and connected to each channel of the SNSPD. The outputs were connected to a 4 channel oscilloscope, and photon flux was compared. The highest efficiency channel was then used for all future measurements.

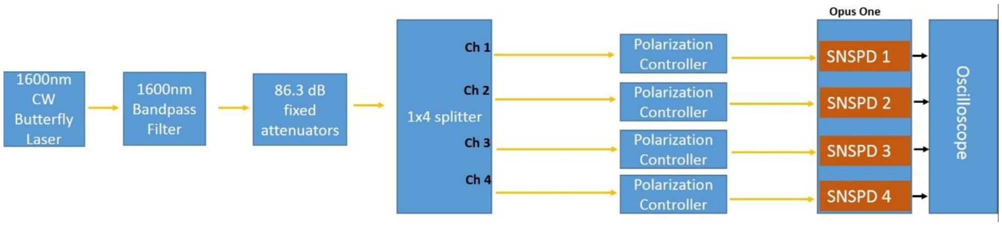

FIG. 8. SNSPD channel efficiency measurements [8]