Quantum Cryptography BB84

By: Omitted

Date: 12/14/2023

Contents

1 Introduction and Theory

The BB84 protocol takes advantage of the uncertainty principle of quantum mechanics and the idea of incompatible observables to create a secure communication channel that is immune to discreet eavesdropping. The destructive nature of quantum measurements ensures that anyone eavesdropping on more than a few bits will likely be detected. Bits of information are encoded in non-orthogonal polarization states of light: $-45°$, $0°$, $40°$, and $90°$. A sender and receiver can then by means of these polarization states, generate a secure key that can be used to securely encrypt any message they wish to send.

1.1 Classical Polarization of Light

When we think of light in the classical context, we image plane waves traveling in the z-direction. With this there are two orthogonal modes of plane polarization: One with the electric field along the x-direction, and one with the electric field along the y-direction. The direction of the electric field is designated as the direction of polarization.

$$\vec{E}(t) = E_0 \cos(kz - wt)\hat{x}$$

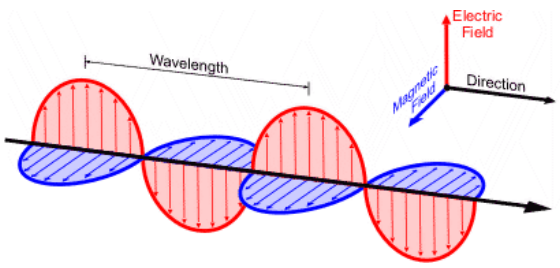

Figure 1: Electromagnetic wave polarized in the x direction.

1.1.1 Interaction with Polarizsers

The transmission axis of a polarizer is defined by the direction of the electric field vector that can be transmitted, without being absorbed. In the classical perspective the light can be decomposed into components orthogonal to and parallel to the transmission axis. The parallel component passes through the polarizer undisturbed, while the ortogonal component is absorbed. Maulus' Law, as shown below, mathematically describes the phenomenon and follows easily from the vector components. Here θ is the angle between the transmis-

sion axis and the incoming polarized light of intensity I_0.

$$I = I_0 \cos^2(\theta)$$

1.1.2 Wave Plates

Wave Plates, also known as retarders, are optical devices that change the polarization of incident light. They accomplish this by slowing polarized light in one axis and allowing polarized light to pass through the other axis un-encumbered. This changes the phase between the two constituent polarization components thus shifting the polarization[4].

A **half-wave plate** serves to shift the slow axis phase by half a wavelength. This has the effect of rotating $\vec{E}$ through 2θ. Where θ is the angle the incoming polarized light makes wit the fast axis.[4]

1.2 The Quantum Perspective

The interaction of a single photon with an optical element like a polarizer is a bit more nuanced than in the classical perspective. A photon cannot be split into orthogonal polarization states, doing so would give you two photons of a lower energy and frequency, so the photon instead must either pass through or be absorbed by the polarizer. So which one is it? Well, we can't be sure unless of course our incident photon is either perfectly aligned or orthogonal to our polarizer.

1.2.1 Probabilistic Nature and Convergence to Malus' Law

The polarization can take any value on a plane perpendicular to the motion of the photon, and as such can be defined in a two-dimensional Hilbert space, shown below.*

`Rectilinear Basis:`

$$|0\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad |90\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1}$$

*The below is in Dirac(aka Bra-ket) notation: https://en.wikipedia.org/wiki/Bra-ket_notation

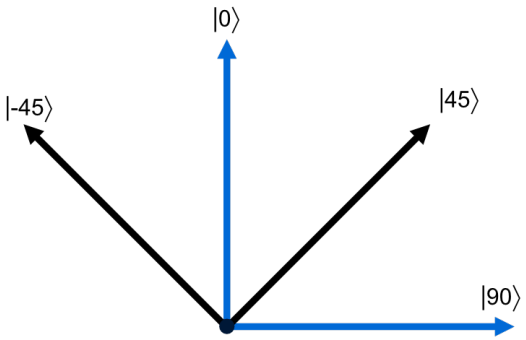

Figure 2: Bases Visualization

`Diagonal Basis:`

$$|-45\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \quad |45\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \tag{2}$$

And any polarization state can be represented as a superposition of the eigen-states, although we of course cannot measure this.

$$|\psi\rangle = a\,|0\rangle + b\,|90\rangle$$
$$|\psi\rangle = \alpha\,|-45\rangle + \beta\,|45\rangle$$

According to the generalized statistical interpretation of quantum mechanics, if we take a measurement on this system it must resolve to one of our measurements eigen-states. This is one of the postulates of quantum mechanics. I.e. if we measure in our rectilinear basis we will get either $|0\rangle$ or $|90\rangle$, and if we measure in our rectilinear basis we will get either $|-45\rangle$ or $|45\rangle$. To generalize this we develop an operator for a polarization measurement at some arbitrary angle γ.[5]

$$P_\gamma \equiv |\gamma\rangle\langle\gamma| = \begin{bmatrix}\sin\gamma\\\cos\gamma\end{bmatrix}\begin{bmatrix}\sin\gamma & \cos\gamma\end{bmatrix} = \begin{bmatrix}\sin^2\gamma & \cos\gamma\sin\gamma\\\cos\gamma\sin\gamma & \cos^2\gamma\end{bmatrix}$$
$$\begin{bmatrix}\sin^2\gamma & \cos\gamma\sin\gamma\\\cos\gamma\sin\gamma & \cos^2\gamma\end{bmatrix}|\psi\rangle = \cdots$$

This operator has eigenvalues 0 and 1, and eigen-states $|\gamma + 90\rangle$ and $|\gamma\rangle$ respectively.[†] And so, if we apply to operator to some state $|\psi\rangle$

Going back to Malus' Law if we have a polerizer at angle γ and we send a light beam polarized at angle ϕ we expect only partial transmission. If we have a photon polarized at some angle ϕ in our rectilinear basis as shown below:

$$|\phi\rangle = \begin{bmatrix} \sin(\phi) \\ \cos(\phi) \end{bmatrix}$$

And if we try to measure this photon with a polarizer at angle γ we expect a probability of transmission of[‡]:

$$\begin{aligned} |\langle\phi|\gamma\rangle|^2 &= (\cos(\phi)\cos(\gamma) + \sin(\phi)\sin(\gamma))^2 \\ &= \left(\frac{\cos(\phi-\gamma) + \cos(\phi+\gamma)}{2} + \frac{\cos(\phi-\gamma) - \cos(\phi+\gamma)}{2}\right)^2 \\ &= \cos^2(\phi-\gamma) \end{aligned}$$

And so, in the limit as we send many photons we have the same result as in Malus' Law, only in this case each photon behaves dichotomously and probabilisticaly, rather than being split like in the classical wave model. The photon must behave probabilistically because non ortohognal polarizations are incompable observables, meaning they share no eigen-states, but our result must be an eigen-state of measurment operator.

1.2.2 Projection Operators for Diagonal($\times$) and Rectilinear($+$) Basis

As seen in the previous section orthogonal polarization projections share eigenstates so we can define our basis measurements by the below:[§]

[†]Strictly speaking there are eigen-states of $\lambda = 0 : |\gamma + \frac{\pi}{2}(2n+1)\rangle$ and $\lambda = 1 : |\gamma + \pi n\rangle$ for $n = 1, 2, 3, \ldots$; However, we pick results between $-\pi$ and π

[‡]Via trigonometric product identities

[§]Note that the eigenvalues corresponding to the eigenstates differ between the two definitions

$$P_+ = |0\rangle\langle 0| \quad \textbf{or} \quad P_+ = |90\rangle\langle 90|$$
$$P_\times = |-45\rangle\langle -45| \quad \textbf{or} \quad P_\times = |45\rangle\langle 45|$$

1.2.3 Taking Measurments

If we take a measurement on $|\psi\rangle$ in our rectilinear basis we will get $|0\rangle$ with probability $|a|^2$ and $|90\rangle$ with probability $|b|^2$. And any repeated measurement in this basis will necessarily yield the same result. Likewise, if we take a measurement on $|\psi\rangle$ in our diagonal basis we will get $|-45\rangle$ with probability $|\alpha|^2$ and $|45\rangle$ with probability $|\beta|^2$. And any repeated measurement in this basis will necessarily yield the same result. We can show this using our projection operators:

$$P_\gamma^2 = P_\gamma P_\gamma = |\gamma\rangle\langle\gamma|\,|\gamma\rangle\langle\gamma| = |\gamma\rangle\langle\gamma| = P_\gamma$$

However, if we first measure in the rectilinear basis and determine a state, $|0\rangle$, then take a measurement in the diagonal basis we find that it is equally likely that the photon takes either state in this new basis.

$$|\langle 0|-45\rangle|^2 = \frac{1}{2}; \quad |\langle 0|45\rangle|^2 = \frac{1}{2}$$

In fact, this is true whenever we switch between out two chosen bases. If we call $\{a_i\}$ our set of rectilinear basis vectors, and $\{b_i\}$ our set of diagonal then for all i and j. $i, j \in \mathbb{Z}$: $i, j \in [1, N]$:[¶]

$$|\langle a_i|b_j\rangle|^2 = \frac{1}{N}$$

When this condition is met, the bases are said to be conjugate. And in the words of Bennet and Brassard "... a system prepared in a specific state of one basis will behave entirely ran-

[¶]Where N is the dimensionality of our Hilbert Space, namely 2

domly, and lose all its stored information, when subjected to a measurement corresponding to the other basis." [2]

2 BB84 Protocol

The BB84 protocol consists of a sender, a receiver, and a potential eavesdropper which we will call ALICE, BOB, and EVE respectively. To start, ALICE selects a random basis($+$ or $\times$) then selects a random bit(0 or 1). ALICE encodes this information in a polarized photon, a 90° or 45° photon representing a digital 1 in their respective basis, and a 0° or 135° photon representing a 0 in their respective basis. ALICE repeats this process an arbitrary number of times.

For each photon ALICE sends: BOB independently chooses a basis to measure in and interprets the measurement as a bit. BOB only gets meaningful data if he, by chance, selects the same basis as ALICE since measuring in differing bases will result in a random bit. See section 2.1.

Once ALICE sends all her photons she and BOB can compare the basis they measured each photon in. They decide to discard any measurements with a differing basis, and keep the remaining bits as their one-time-pad. If this process was undisturbed ALICE and BOB should be in agreement over their secret key.

Finally, to determine whether their secret key generation was eavesdropped on they publicly share a a random subset of their secret key(this can be done publicly). If they find that all their shared bits match they can discard those bits, and use the remaining bits as a secure one time pad.

Alice and Bob can now securely use this key as a one time pad to encrypt and decrypt a message.

2.1 Detection of an Eavesdropper

These conjugate bases ensure that any data interception has a noticeable effect. If ALICE and BOB agree to generate a key using polarized photons, they will only be successful if no-one is interfering because measuring these photons is destructive to their state. If ALICE, EVE, and BOB all choose the same basis then all is good and EVE goes undetected. If

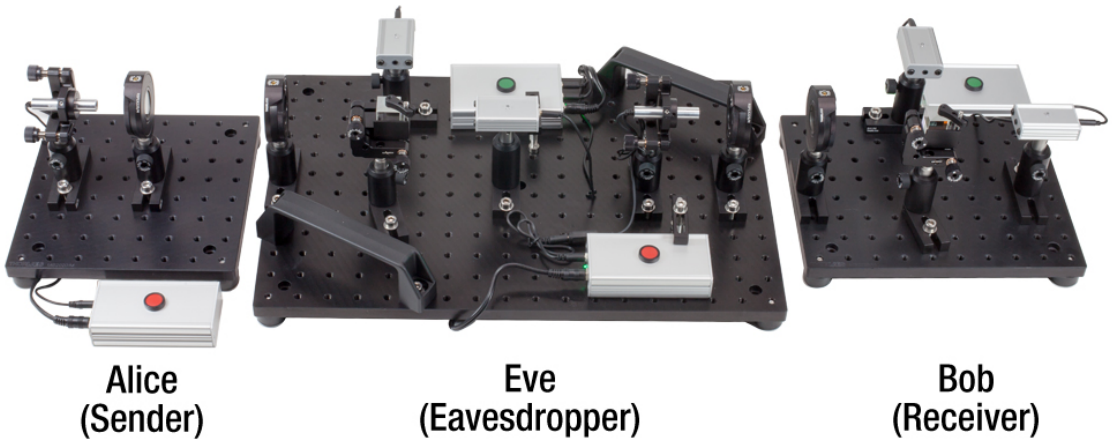

Figure 3: Thorlabs' Quantum Cryptography Analogy Demonstration Kit. Image courtesy of Thorlabs.

ALICE, and BOB choose a different basis than EVE then the key will include an random bit bit. If ALICE and BOB choose different bases then the resulting bit is irrelevant as it will be discarded anyway. The result is 25% of the generated key will be incorrect in the limit as the key length gets very large. Practically it will be some significant portion of "Alice's" key will not match "Bob's" key.

Below are all possible measurement steps that a photon may undergo in the proposed system notice.[‖]

Without an Eavesdropper

$$|0\rangle \to P_+ |0\rangle \qquad |90\rangle \to P_+ |90\rangle$$
$$|0\rangle \to P_\times |0\rangle \qquad |90\rangle \to P_\times |90\rangle$$
$$|-45\rangle \to P_+ |-45\rangle \qquad |45\rangle \to P_+ |45\rangle$$
$$|-45\rangle \to P_\times |-45\rangle \qquad |45\rangle \to P_\times |45\rangle$$

[‖] `What ALICE Sends` $\to$ `What EVE Measures` $\to$ `What BOB Measures`

With an Eavesdropper

$$|0\rangle \to P_+ |0\rangle \to P_+P_+ |0\rangle \qquad |90\rangle \to P_+ |90\rangle \to P_+P_+ |90\rangle$$

$$|0\rangle \to P_+ |0\rangle \to P_\times P_+ |0\rangle \qquad |90\rangle \to P_+ |90\rangle \to P_\times P_+ |90\rangle$$

$$|0\rangle \to P_\times |0\rangle \to P_\times P_\times |0\rangle \qquad |90\rangle \to P_\times |90\rangle \to P_\times P_\times |90\rangle$$

$$|0\rangle \to P_\times |0\rangle \to P_+P_\times |0\rangle \qquad |90\rangle \to P_\times |90\rangle \to P_+P_\times |90\rangle$$

$$|-45\rangle \to P_+ |-45\rangle \to P_+P_+ |-45\rangle \qquad |45\rangle \to P_+ |45\rangle \to P_+P_+ |45\rangle$$

$$|-45\rangle \to P_+ |-45\rangle \to P_\times P_+ |-45\rangle \qquad |45\rangle \to P_+ |45\rangle \to P_\times P_+ |45\rangle$$

$$|-45\rangle \to P_\times |-45\rangle \to P_\times P_\times |-45\rangle \qquad |45\rangle \to P_\times |45\rangle \to P_\times P_\times |45\rangle$$

$$|-45\rangle \to P_\times |-45\rangle \to P_+P_\times |-45\rangle \qquad |45\rangle \to P_\times |45\rangle \to P_+P_\times |45\rangle$$

2.2 Encryption and Decryption

Once you have a secret bit key and have verified your key generation has not been disturbed it is fairly easy to encrypt and encrypt a message. Your message can only be as long as your key, but also should be a multiple of your character encoding system. UTF-8, for example, is a standard where each character is represented as 8 bits, but you could also choose 5 bit characters since there are $2^5 = 32$ unique combinations that can represent every letter in the English language and some special characters.

Once you have a message encoded in your format all you must do to encrypt your message is perform a **BITWISE XOR** operation between your key and your message. Go through your message and key bit by bit and note a 0 if both bits are the same and a 1 otherwise. To unencrypt follow the same process but with the encrypted message and the key. Table.1 shows the process of encrypting and encrypting a message.

Message (UTF-8)	S	E	C	R	E	T
Unencrypted Bits	01010011	01000101	01000011	01010010	01000101	01010100
Key	10000011	10010101	10010000	01011111	10001100	10010011
Encrypted Bits	11010000	11010000	11010011	00001101	11001001	11000111
Decrypted Bits	01010011	01000101	01000011	01010010	01000101	01010100
Decrypted (UTF-8)	S	E	C	R	E	T

Table 1: Example encryption with message "SECRET" and one time pad(key) given in table.

2.3 No Cloning Theorem

Why can't an eavesdropper just make a copy of an incoming photon, measuring one in an attempt to steal some information and passing the other along to remain inconspicuous?

Assume someone claims to have some method $\mathcal{M}$ which can take some desired particle state $|\psi\rangle$ and another particle state $|X\rangle$ and return two particles in the desired state. Where $|\psi\rangle$ is an arbitrary linear combination of base states $|A\rangle$ and $|B\rangle$.

$$|\psi\rangle\,|X\rangle \xrightarrow{\mathcal{M}} |\psi\rangle\,|\psi\rangle$$

Now we try to clone our base states, and we're successful

$$|A\rangle\,|X\rangle \xrightarrow{\mathcal{M}} |A\rangle\,|A\rangle \quad |B\rangle\,|X\rangle \xrightarrow{\mathcal{M}} |B\rangle\,|B\rangle$$

What if we try to clone a more complex state, we suspect that:

$$\begin{aligned}(\alpha\,|A\rangle + \beta\,|B\rangle)\,|X\rangle &\xrightarrow{\mathcal{M}} (\alpha\,|A\rangle + \beta\,|B\rangle)\,(\alpha\,|A\rangle + \beta\,|B\rangle) \\ &= \alpha^2\,|A\rangle\,|A\rangle + \beta^2\,|B\rangle\,|B\rangle + \alpha\beta\,|A\rangle\,|B\rangle + \beta\alpha\,|B\rangle\,|A\rangle\end{aligned}$$

But, $(\alpha\,|A\rangle + \beta\,|B\rangle)\,|X\rangle = \alpha\,|A\rangle\,|X\rangle + \beta\,|B\rangle\,|X\rangle$, and:

$$\alpha\,|A\rangle\,|X\rangle + \beta\,|B\rangle\,|X\rangle \xrightarrow{\mathcal{M}} \alpha\,|A\rangle\,|A\rangle + \beta\,|B\rangle\,|B\rangle$$

So, we could only hope to be successful in our cloning if the quantum system that we want to clone is in a pure base state[5].

2.4 The use of pulses rather than photons

This demonstration uses laser pulses rather than singular photons since it would be much more expensive to send singular photons, and the photons would likely not make it to its destination without being scattered.

So, the no cloning theorem does not strictly apply to this setup as one could simply split the beam measuring half for themselves and sending the other on its way. However, the protocol itself is unchanged.

2.5 The probability of key length

Alice and Bob have a 50% chance to pick the same base to measure in, or they will fail and pick differing bases. This means that the number of times they pick matching bases should follow a binomial distribution.

A binomial distribution has a mean of $\mu = pN$ and a variance of $\sigma^2 = Npq$. So when sending N "photons" we expect a key length of $\frac{1}{2}N$ and a variance of $\frac{N}{4}$.

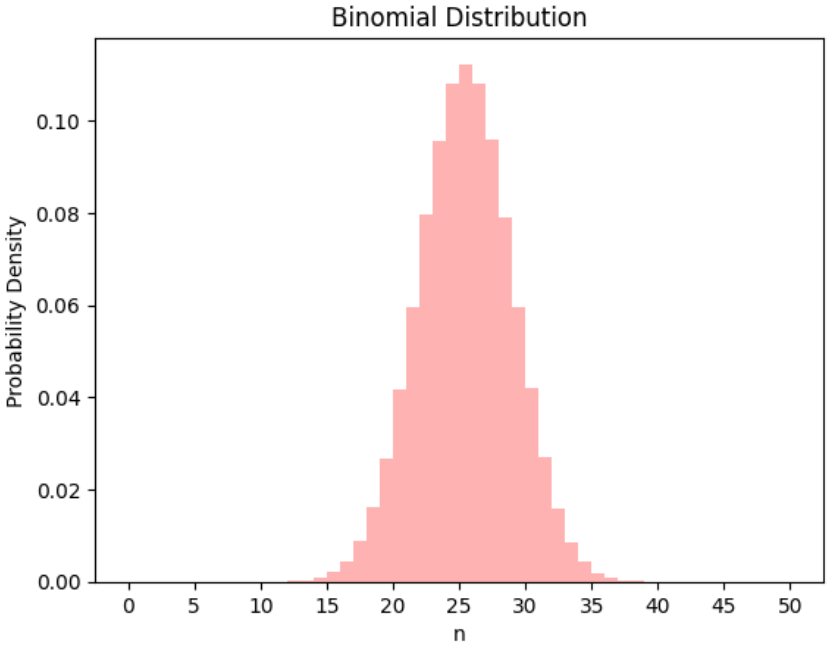

Figure 4: Simulating Alice and Bob picking 50 random bases 1million times. The distribution, as expected, is a binomial distribution with N=50 and p=0.5.

3 Operation

3.1 Setup

Each laser should be setup to lase at a 0° polarization with no waves plates present. And the wave plates offset should be set so that when at 0° the incident laser light is uneffected.

The waveplates are used to rotate the polarization to the selected basis. The angles chosen are such that when the pulse arrives at the beam splitter in will be in either a $|0\rangle$, $|90\rangle$ or some equal superposition of those two states i.e $|45\rangle$ or $|-45\rangle$. See Fig.5 for more in depth look at the wave plate rotations, but the gist is when measuring in the correct basis you will receive a pure $|0\rangle$ or $|90\rangle$ leading to a deterministic measurement, if you are measuring in the incorrect basis you will receive an equal superposition(parallel or anti parallel to $|45\rangle$ or $|-45\rangle$) leading to a probabilistic measurement. Of course, we are using laser pulses rather than photons, so the random measurement is not a result of a quantum process, but of a pseudo-random number generator..

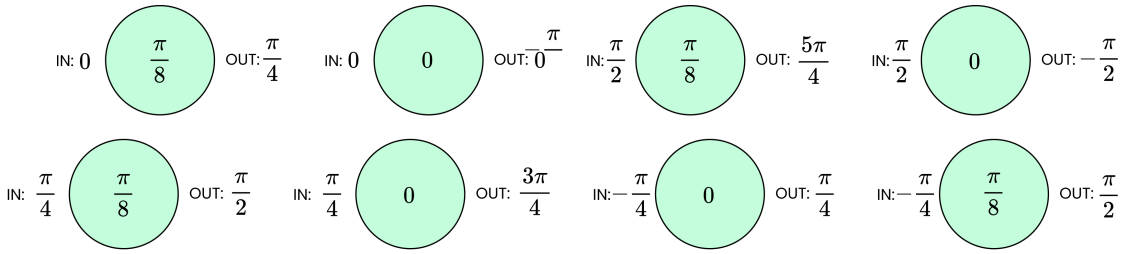

Figure 5: Wave plate Inputs and Outputs at Various Angles

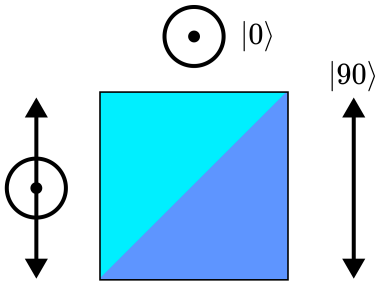

Figure 6: Beam splitter behavior where 0 and 90 are the S and P polarizations of the splitter.

3.2 Modified Operation

3.2.1 Arduinos

> "Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing."

Each ALICE, BOB, and EVE have there own Arduino that acts as their brain. They are responsible for keeping track of incoming and outgoing bits, and directing the other hardware.

To send a pulse we simply toggle the voltage on one of our output pins temporarily to 5V. A C++ function that does this is shown below. digitalWrite, and delayMicro are functions built into Arduino.

To determine if we received a digital 1 or 0 we continuously check our analog inputs that are connected to our two photometer outputs. If either of these inputs goes above some threshold voltage we start reading a pulse. The bit corresponding to the input with the larger maximum within the pulse time is recorded. If the maxima are within some small threshold then a random bit is recorded.

3.2.2 ELL14 - Rotation Mount: SM1 Threaded

Motorized rotation mount to hold the waveplates. Can be controlled by the Arduinos via the ELLB bus controller and the included communications protocol talked about below. More information about this device can be found at the link below.

https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=12829&pn=ELL14

3.2.3 ELLB - Bus Distributor/ Communication Protocol

This interfaces the ELL14 with our Arduinos via the TX and RX pins. More information can be found at: https://www.thorlabs.com/Software/Elliptec/Communications_Protocol/ELLx%20modules%20protocol%20manual_Issue7.pdf.

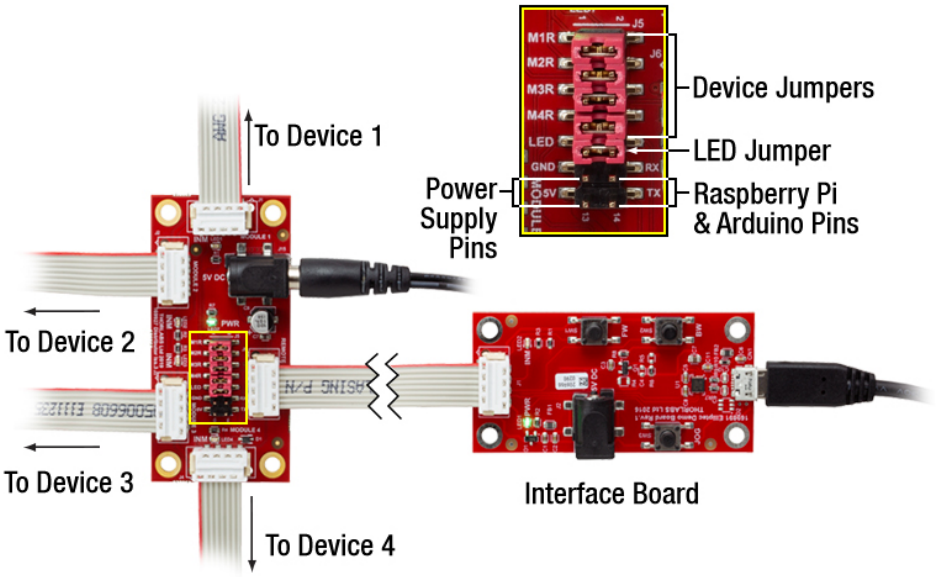

Figure 7: ELLB Bus Controller Layout.

3.2.4 Layout

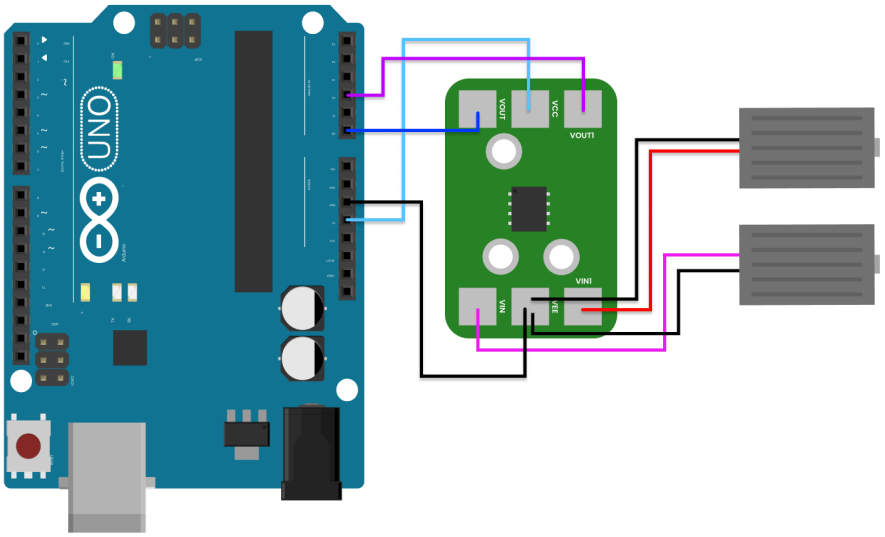

Figure 8: Diagram showing how the photometers connect to the Arduino via a single supply inverting amplifier using a LM358 low power dual operational amplifier. Not to scale.

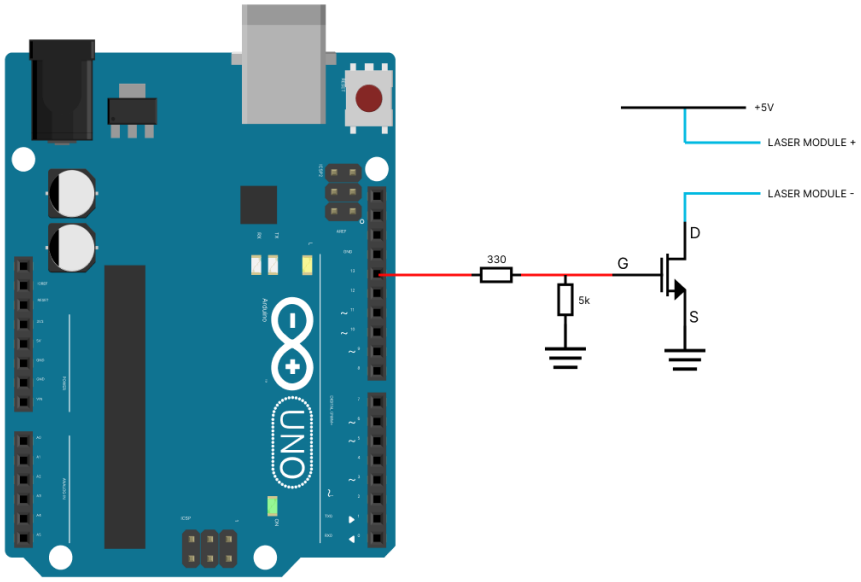

Figure 9: Diagram showing how the Arduino switches the laser on and off using a MOSFET (IRLZ44N).

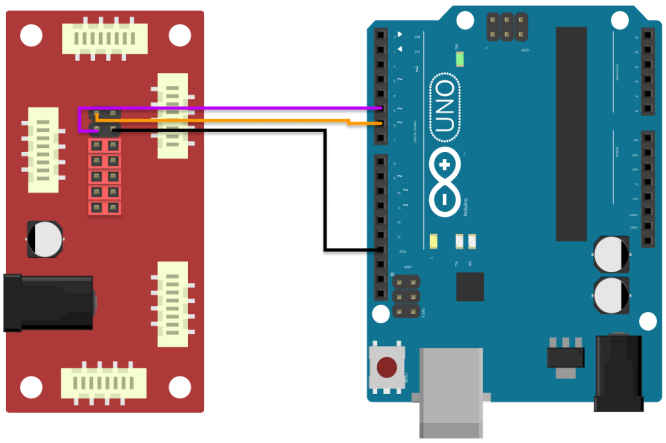

Figure 10: Diagram showing how the Arduino connects to the ELLB. Not to scale. It is really connected through a logic level converter between the Arduino's 5V logic and the Bus' 3V3 logic. Pins 5 and 6 are designated in the Arduino's programming to be the software RX and TX pins respectively.

3.2.5 Commands

All commands are sent over the Arduino's serial port and will be terminated by a new line.

To send commands over the serial ports you should install the Arduino IDE from https://www.arduino.cc/en/software.

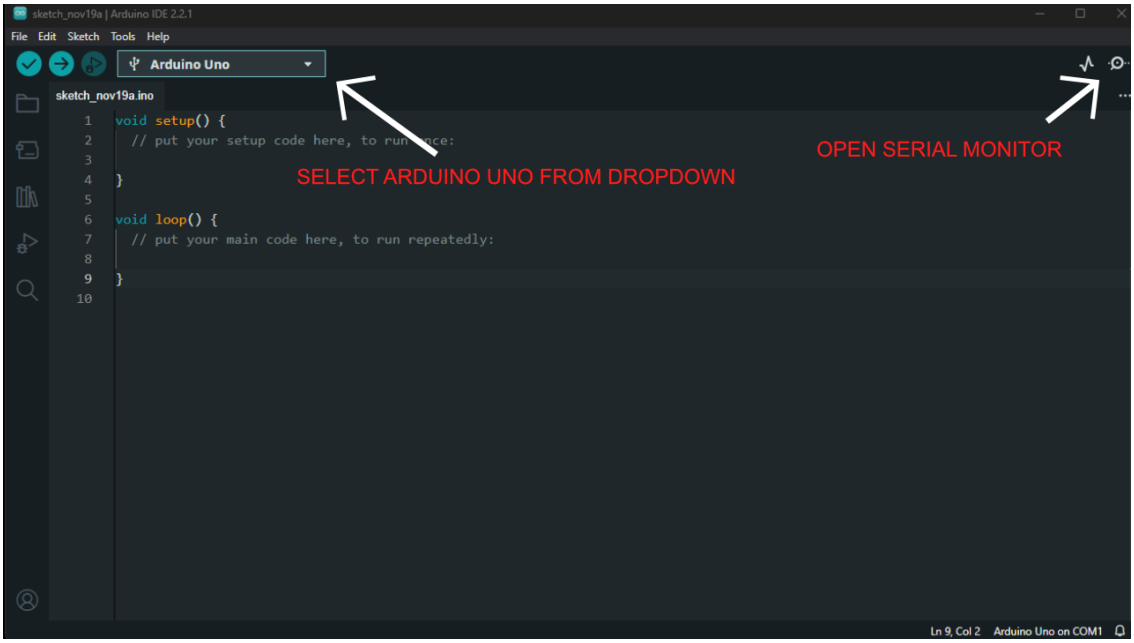

Figure 11: What You See When first Opening Arduino IDE. Plug into ALICE/BOB's Arduino and select Arduino UNO from the drop down in the top left of the application. Next Open the Serial Monitor via the magnifying glass icon in the upper right hand corner.

SEND 1 PULSE

`TX: "F1"`

Send one laser pulse of duration 1ms. Random Base will **not** be selected or recorded.

SEND 8 PULSE

`TX: "F8"`

Send one laser pulse of duration 1ms with a 1ms delay between pulses. Random Bases will **not** be selected or recorded. Commands entered while sending will be ignored.

SEND 32 PULSES

`TX: "F32"`

Each pulse is of duration 1ms with a 1ms delay between pulses. Random Bases will **not** be selected or recorded. Commands entered while sending will be ignored.

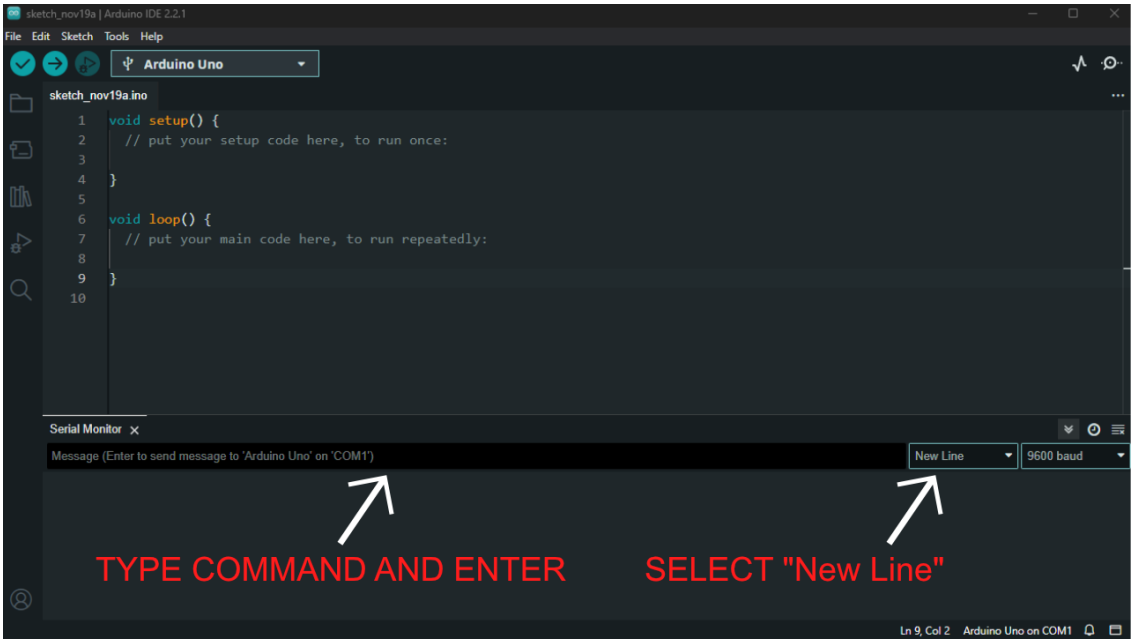

Figure 12: Arduino IDE Serial Monitor. Select "New Line" to automatically end all entered Serial Data with a new line character. Ensure the baud rate is on 9600.

CLEAR BASE/BIT HISTORY

`TX: "CMR"`

Clear history of send bits and the base they were sent in. This data is stored in an array and can hold a maximum of 256 bits. It is recommended to clear before every message. This will be automatically cleared if the limit is reached, but will be printed over serial first.

PRINT SENT/RECEIVED HISTORY

`TX: "PHS"`

Outputs history in {basis}, {bit} comma separated value format. Basis is 'R' or 'D' for rectilinear and diagonal respectively.

SEND 32 PULSES W/ RANDOM BASES

`TX: "R32"`

Each pulse is of duration 1ms with a 1ms delay between pulses. Random Bases **will** be selected and recorded. Will rotate wave plate between pulses. Commands entered while sending will be ignored.

SEND 64 PULSES W/ RANDOM BASES

`TX: "R64"`

Each pulse is of duration 1ms with a 1ms delay between pulses. Random Bases **will** be selected and recorded. Will rotate wave plate between pulses. Commands entered while sending will be ignored.

SET BASIS $0°$

`TX: "S000"`

ELL14 to $0°$

Angle definitions are within the code that can be found in the appendix. They should be adjusted to align the device. They are near the top and defined as "#define $DEGREE\_\{0, 45, 90, N45\}$" or "#define $SEGREE\_\{0, 45, 90, N45\}$" (for eve which has two sets of definitions).

SET BASIS $90°$

`TX: "S090"`

ELL14 to $45°$

SET BASIS $45°$

`TX: "S045"`

ELL14 to $22.5°$

SET BASIS $-45°$

`TX: "S315"`

ELL14 to $67.5°$

START ALIGNMENT

`TX: "STA"`

Continuously lase.

END ALIGNMENT

`TX: "ENA"`

End continuous lase.

MOVE RELATIVE 1

`TX: "MR1"`

Move relative and return position so you can update the 0° angle in the code.

MOVE RELATIVE 2

`TX: "MR2"`

Smaller move relative and return position so you can update the 0° angle in the code.

Change Address to 1

`TX: "CAT1"`

Only on Eve change any ELL14 that is connected to address 1. Eve's receiving ELL14 should be 0. Eve's outgoing ELL14 should be 1.

Change Address to 1

`TX: "CAT0"`

Only on Eve change any ELL14 that is connected to address 0. Eve's receiving ELL14 should be 0. Eve's outgoing ELL14 should be 1.

4 Alignment With the Arduino Setup

Use the MR1 and MR2 commands to find the correct zero location for the wave plates. Update the zero angle and the others in the code. The correct zero angle is one what is aligned with the polarization of the laser. STA will start continuously lasing so you can see the effects of the beam splitter. ENA ends the continuous lase.

5 Standard Procedure

5.1 Alignment

1. Setup ALICE and BOB in series, leaving room for EVE in between
2. Ensure that all equipment is connected properly, and set the green boxes to alignment mode. If done properly the LED indicator on the back will be orange.
3. Press and hold the red button on ALICE to set the laser to continuous mode.

4. Set ALICE's waveplate to $|0\rangle$ and BOB's waveplate to $|45\rangle$

5. Move, rotate, lower, or raise any equipment on ALICE or BOB such that the laser passing through the beam splitter lands in the eye of both photometers. Try to keep all equipment square.

6. If done properly the LED's on both photometers will light up at the same time when a pulse is sent in different bases

7. Now, place EVE in between ALICE and BOB. Set sets EVE's first basis to 45, and EVE's second basis to 0

8. Move, rotate, lower, or raise any equipment on EVE such that ALICE's laser lands in the eye of both EVE's photometers and EVE's laser both BOB's photometers

5.2 Generate a key without EVE

1. Set up Alice and Bob so that they face each other at a large distance.

2. Follow the alignment to adjust the ALICE and BOB.

3. Alice and Bob randomly select their bases, and Alice also selects her bit.

4. Alice sends the bits in the chosen basis and Bob records the bits he measures.

5. During Bob's measurements, uses the bases chosen randomly to interpret Alice's transmission. (if the bases do not match, a 0 or 1 bit result is selected at random)

6. Alice and Bob exchange their bases, find and record the same key when they have same basis.

5.3 Generate a key with EVE

1. Follow the Alignment to set up Alice, Bob and EVE.

2. Alice, Bob and Eve randomly select their bases, and Alice randomly selects bits to send.

3. Alice then sends the bits using her selected basis and Bob records the bits he measures.

4. Eve is between Alice and Bob and selects her basis randomly as well (either 0° and 45°)

5. If Eve's basis matches the one chosen by Alice, Eve will transmit the correct bit.

6. If Eve selected the incorrect basis, she will transmit a random bit based on her interpretation of Alice's signal (0 or 1).

7. Bob will record the bit that he receives from Eve.

8. Alice and Bob exchange the bases used for transmitting and receiving. They highlight the measurements where the bases match.

9. Now Alice and Bob compare the bits for which their bases matched. We get two lines bits of Alice and Bob.

10. There are differences between the two bits sequence. We will find that these two sets of numbers are not identical, and their error rate will be infinitely close to 25%.

5.4 Example Key Generation

Alice Sends		BOB MEASURES		COMPARE BASES	KEY
D	0	R	1	✗	-
R	0	D	0	✗	-
D	1	D	1	✓	1
R	0	R	0	✓	0
D	1	R	1	✗	-
D	0	R	0	✗	-
D	0	D	0	✓	0
R	1	D	1	✗	-
D	0	D	0	✓	0
R	0	D	1	✗	-
R	1	D	1	✗	-
D	1	D	1	✓	1
D	0	R	1	✗	-
D	0	R	1	✗	-
R	0	R	0	✓	0
R	1	R	1	✓	1

Table 2 continued from previous page

Alice Sends		BOB MEASURES		COMPARE BASES	KEY
R	0	R	0	✓	0
D	1	R	1	✗	-
D	0	D	0	✓	0
D	0	R	1	✗	-
R	1	D	1	✗	-
R	0	D	1	✗	-
D	1	D	1	✓	1
D	0	R	1	✗	-
D	1	R	0	✗	-
D	0	D	0	✓	0
D	0	R	0	✗	-
R	1	R	1	✓	1
D	0	D	0	✓	0
R	0	R	0	✓	0
R	1	R	1	✓	1
R	1	D	0	✗	-
D	1	R	0	✗	-
R	1	R	1	✓	1
R	0	R	0	✓	0
D	0	D	0	✓	0
R	1	D	0	✗	-
D	0	R	0	✗	-
D	1	R	0	✗	-
R	1	R	1	✓	1
D	1	D	1	✓	1
D	0	R	0	✗	-
D	1	D	1	✓	1
D	1	D	1	✓	1
D	1	R	1	✗	-
R	1	D	1	✗	-
R	0	D	0	✗	-
D	0	D	0	✓	0
D	1	D	1	✓	1
D	0	D	0	✓	0

Table 2 continued from previous page

Alice Sends	BOB MEASURES	COMPARE BASES	KEY

Table 2: Manually generated key process with no eavesdropper. We obtained a key length of 25 bits out of the 50 photons we sent. This is close to the 50% that we expect. Alice's and Bob's keys matched

N	Alice Sends	Eve Measures	Bob Measures	Compare	Key A	Key B	Inaccuracies
1	R 1	D 1	R 0	✓	1	0	✗
2	D 0	D 0	D 0	✓	0	0	
3	D 1	R 1	D 0	✓	1	0	✗
4	R 1	D 1	D 1	✗	-	-	
5	R 1	R 1	R 1	✓	1	1	
6	D 1	D 1	R 0	✗	-	-	
7	R 0	R 0	D 1	✗	-	-	
8	R 0	R 0	R 0	✓	0	0	
9	R 0	D 0	R 0	✓	0	0	
10	R 0	R 0	R 0	✓	0	0	
11	R 0	D 1	D 1	✗	-	-	
12	R 1	R 1	R 1	✓	1	1	
13	R 1	R 1	D 0	✗	-	-	
14	R 1	R 1	D 1	✗	-	-	
15	R 0	R 0	D 0	✗	-	-	
16	D 1	R 0	R 0	✗	-	-	
17	R 0	D 0	D 0	✗	-	-	
18	R 0	R 0	R 0	✓	0	0	
19	D 1	R 1	R 1	✗	-	-	
20	R 1	D 1	D 1	✗	-	-	
21	D 0	D 0	R 0	✗	-	-	
22	D 1	R 1	R 1	✗	-	-	
23	R 1	R 1	D 1	✗	-	-	
24	R 1	R 1	D 1	✗	-	-	
25	R 1	R 1	R 1	✓	1	1	
26	R 1	R 1	D 0	✗	-	-	
27	R 0	D 1	R 1	✓	0	1	✗
28	R 0	D 0	R 1	✓	0	1	✗
29	D 1	D 1	D 1	✓	1	1	

N	Alice Sends		Eve Measures		Bob Measures		Compare	Key A	Key B	Inaccuracies
30	R	0	D	1	D	1	✗	-	-	
31	D	1	R	1	D	1	✓	1	1	
32	D	0	R	1	D	0	✓	0	0	
33	R	1	D	1	R	1	✓	1	1	
34	R	0	D	1	R	1	✓	0	1	✗
35	R	1	D	1	D	1	✗	-	-	
36	R	1	R	1	R	1	✓	1	1	
37	R	0	D	1	R	1	✓	0	1	✗
38	R	0	D	1	R	1	✓	0	1	✗
39	D	0	D	0	R	0	✗	-	-	
40	R	0	R	0	D	1	✗	-	-	
41	D	0	R	1	D	1	✓	0	1	✗
42	D	0	R	1	R	1	✗	-	-	
43	D	1	D	1	R	0	✗	-	-	
44	D	1	R	0	D	1	✓	1	1	
45	R	0	R	0	R	0	✓	0	0	
46	D	1	D	1	D	1	✓	1	1	
47	D	1	R	1	R	1	✗	-	-	
48	R	0	R	0	R	0	✓	0	0	
49	R	1	D	1	R	1	✓	1	1	
50	R	0	D	0	R	1	✓	0	1	✗
51	D	0	R	1	D	1	✓	0	1	✗
52	D	0	D	0	R	0	✗	-	-	
53	D	1	R	1	R	1	✗	-	-	

Table 3: Manually generated key process with no eavesdropper. We obtained a key length of 28 bits out of the 53 photons we sent. This is close to the 50% that we expect. However, Alice's and Bob's keys do not match; 10 bits of there 28bit key are incorrect (36%). This leads Alice and Bob to conclude that there was an eavesdropper.

6 Experimentation

6.1 Confirming Expectations

Send 32 bits in each polarization basis measure half in the correct polarization state that you know and the other in the conjugate basis.

Using Serial Commands:

1. Ensure BOB in in manual mode.
2. Clear the history on ALICE and BOB
3. Manually set the ALICE's and BOB's waveplate angle.
4. Send 32 pulses in the base/bit configuration you setup
5. Collect BOB's received data
6. Compare to what you expect

6.2 Generate a key without EVE present

ALICE should communicate with BOB that a message will be sent, both will clear their logs. ALICE and BOB begin generating a key.

1. Ensure BOB is in automatic mode.
2. Clear the history on ALICE and BOB
3. Send 64 bits in random basis'
4. Collect ALICE's and BOB's data
5. Compare base and bit strings to determine a one-time-pad

6.3 Generate a key with with EVE present

Place EVE in between ALICE and BOB and try to generate a new key following the previous steps.

A Code

Code for each Arduino can be found here on GitHub in the 'main' branch: https://github.com/seambr/bb84-lab-automation. To upload to the Arduinos plug into the respective Arduinos via usb, open each .ino file named alice, bob, and eve in the Arduino IDE and hit upload in the top left.

References

[1] Stephen Wiesner. "Conjugate Coding". In: ACM SIGACT News 15.1 (1983), pp. 78–88. DOI: 10.1145/1008908.1008920.

[2] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: Theoretical Computer Science 1 (Dec. 1984), pp. 175–179. DOI: 10.1016/j.tcs.2014.05.025.

[3] Charles H. Bennett, Gilles Brassard, and Artur K. Ekert. "Quantum Cryptography". In: Scientific American 267.4 (1992), pp. 50–57. ISSN: 00368733, 19467087. URL: http://www.jstor.org/stable/24939253 (visited on 09/11/2023).

[4] Eugene Hecht. "Polarization". In: Optics. Addison-Wesley, 2010, pp. 325–379.

[5] David J. Griffiths and Darrell F. Schroeter. Introduction to quantum mechanics. Third edition. Cambridge ; New York, NY: Cambridge University Press, 2018. ISBN: 978-1-107-18963-8.

[6] Chankyun Lee, Ilkwon Sohn, and Wonhyuk Lee. "Eavesdropping detection in BB84 quantum key distribution protocols". In: IEEE Transactions on Network and Service Management 19.3 (2022), pp. 2689–2701. DOI: 10.1109/tnsm.2022.3165202.