

**THORLABS**



**QCRY1/M Manual ENG**



0-Jul-17

**THORLABS**

Discovery

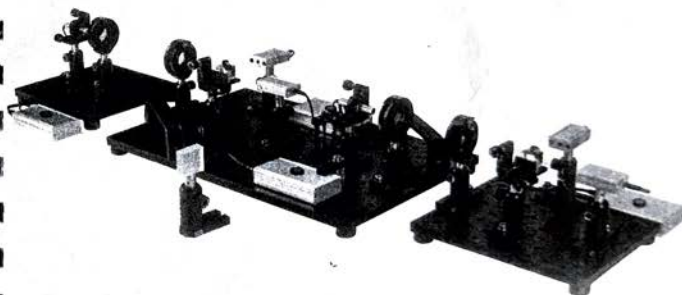
**EDU-QCRY1**

**EDU-QCRY1/M**

**Quantum Cryptography**

**Demonstration Kit**

**Manual**



## Chapter 5 Fundamentals of Quantum Cryptography

This section explains how quantum cryptography works and the steps required to carry it out. It starts with a brief introduction and then explains the one-time pad which turns a message and a key into an encrypted message. This is followed by the generation of the keys, constituting the essential element of quantum cryptography.

The value of quantum cryptography lies in the safety from interception. Section 5.4 discusses how an eavesdropper can be detected using this method.

### 5.1. Introduction

Cryptography describes the encryption of data: that is, rendering a message unrecognizable, ideally making it readable only for the sender and the recipient. This means that the encrypted message is only meaningful if the key to decode it is known. The security of the key is based either on complex underlying algorithms or on practical constraints such as the factorization of large numbers.

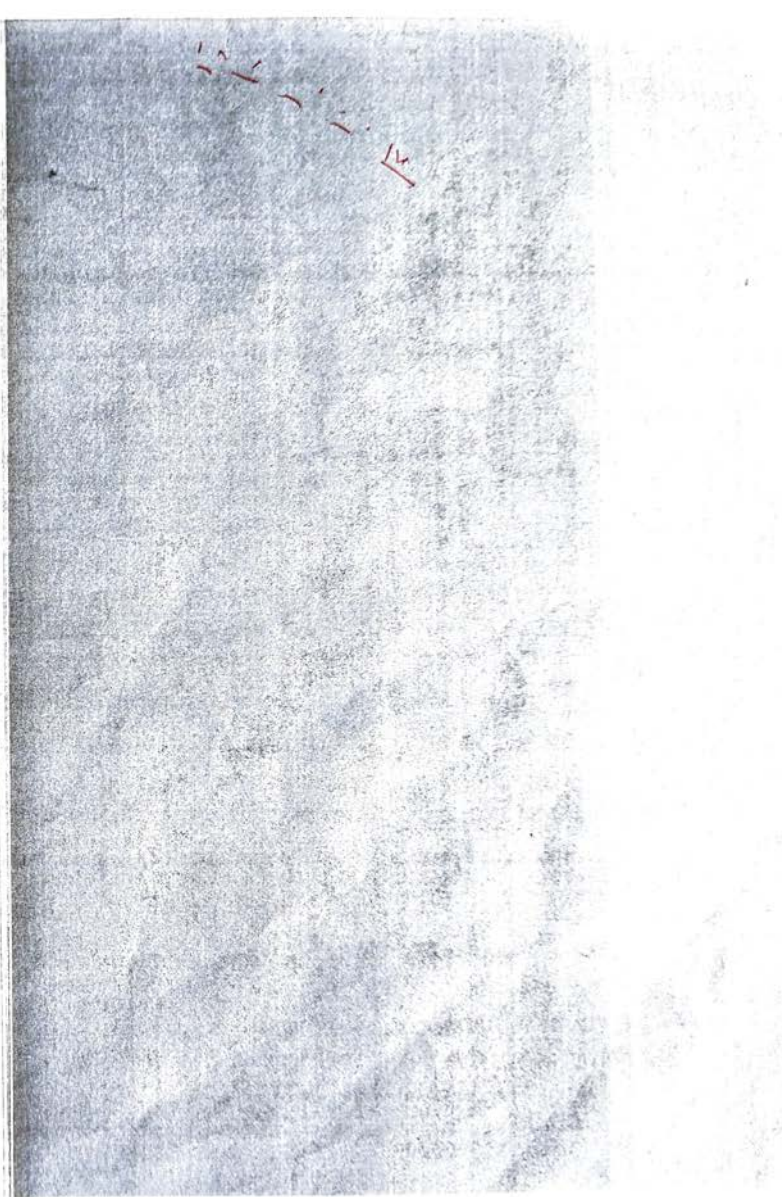
All classical cryptography methods have the disadvantage that one can never be sure that the key will not be "cracked" eventually. This fundamental problem however can be solved with the use of quantum physics. One of the core rules governing quantum physics is that observing the state of a photon or particle simultaneously causes the state to change. This principle, along with true random number generation, is what allows a user to generate a random key that is *known only to the sender and the recipient*. As an added feature, any attempt at interception can theoretically be identified.

There already exist some examples of encryption systems that employ quantum cryptography. These systems are commercially available today, for example at <http://www.idquantique.com/quantum-safe-crypto/>

### 5.2. The One-Time Pad

The one-time pad, also known as a single-use key, is an encryption method that is 100% secure in principle, provided that all requirements are fully met. Quantum physics merely helps meet these requirements, whereas the method itself is a classical encryption technique.

Imagine an encryption key that consists entirely of a perfectly random sequence of 0s and 1s called "bits". Now imagine the message also consists of 0s and 1s. Binary addition of the message and encryption key can be performed to obtain another chain of 0s and 1s which is completely random as well. This results in the encrypted message.





The "calculation rules" that apply for binary addition are as follows:

- $0 + 0 = 0$
- $1 + 0 = 1$
- $0 + 1 = 1$
- $1 + 1 = 0$

When the intended recipient obtains the encrypted message, they will use binary addition on the encrypted message and encryption key. This will then produce the original message.

By way of an example, we can encode the word "Test". Each letter can be translated into a five-digit binary code as shown in the table below (see Chapter 9 for a table that converts alphabet letters to binary code).

Word	T				E				S				T					
Binary word	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1
Key (random)	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0
Encrypted message	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1
Key (as above)	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0
Binary word	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	1	1
Word	T				E				S				T					

If the encrypted message is intercepted, the eavesdropper requires the key in order to decode it. Without the key, the random sequence of zeroes and ones produce complete "gibberish" when converted to a word. This makes the message entirely safe from interception.

To summarize the essential requirements:

1. The key has to be at least as long as the message.
2. The key must only be used once.
3. The key must be completely random.
4. The key must be known only to the sender and the recipient.

Requirement 1 is easy to meet by the sender, who can only encrypt a number less than or equal to the number of available key bits.

Requirement 2 is the responsibility of the sender and recipient, and is easily realized well.

Requirement 3 is difficult to meet upon closer inspection, since every random number generator is ultimately based on an algorithm. This means that random numbers generated by a computer are always merely "pseudo-random". However, quantum physics can be used to solve this problem since it makes true randomness possible. This is discussed in more detail in Section 5.5.

Requirement 4 is problematic as well, since the classical transmission of a key opens up the possibility of intercepting it. This problem too can be solved with quantum physics. The approach to the secret distribution of the key is discussed in the next subsection.

## 5.3. Key Distribution

### 5.3.1. $\lambda/2$ Plate and Data Transmission with One Basis

This subsection is intended to facilitate a better understanding of the experimental setup by briefly running through the process of transmitting data with one basis. Actual quantum cryptography (in the real world and in this analogy experiment) works with two bases, which is described in the next subsection.

A photon is to be used to transmit a "0" or a "1". In this example, the polarization direction is used as the bit: A photon with horizontal polarization is interpreted as a "0", one with vertical polarization as a "1".

So what would an experimental setup look like that can transmit data this way? An example is shown in Figure 2.

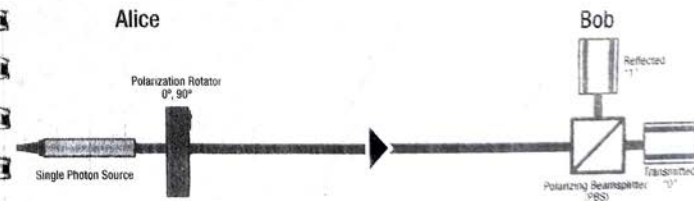


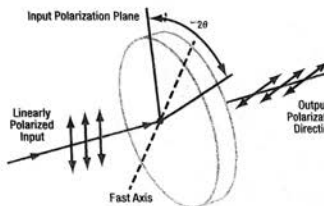
Figure 2 Data Transmission with One Polarization Basis

The sending unit "Alice" consists of a single photon source which is polarized horizontally and a  $\lambda/2$  plate.

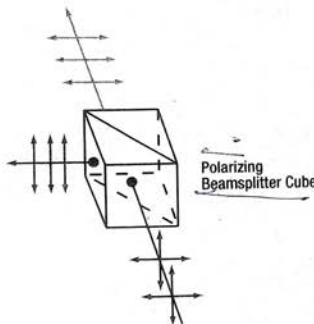
The  $\lambda/2$  plate rotates the polarization of the incident light by double the physical rotation angle of the wave plate. For example, when the wave plate is rotated physically by  $45^\circ$  relative to the incoming polarization, the polarization of the light is actually rotated by  $90^\circ$ . This is why a  $\lambda/2$  plate is also known synonymously as a "polarization rotator".

When we talk about the "0°" and "90°" settings from now on (later "-45°" and "45°"), this angle always refers to the **rotation angle of the polarization** and never the rotation angle of the  $\lambda/2$  plate.

A sketch describing how the  $\lambda/2$  plate operates is shown in the diagram to the right. Light incident on the wave plate is altered such that polarization components not aligned with the fast axis of the birefringent crystal are retarded. For linearly polarized light, the result is that the polarization is rotated by a value twice as large as the rotation of the  $\lambda/2$  plate.



The receiving unit "Bob" consists of a polarizing beamsplitter cube and two detectors. The polarizing beamsplitter cube reflects the vertically-polarized (90°) component of the incident light, while passing the horizontally-polarized (0°) component, as seen in the diagram to the right.



If the polarization state of the light sent by Alice is set to 0°, the photon will pass through the beamsplitter (designated as event "0"). If the wave plate is set to rotate the polarization by 90°, the photon will be reflected by the beamsplitter (designated as event "1").

### 5.3.2. Key Distribution – The Right Way

While the method with one basis (0° or 90°) is sufficient to transfer data from Alice to Bob, it is not able to guarantee safety from interception. A second basis comes into play to accomplish this. In addition to the basis with 0° and 90°, which we will now call the "+ basis", a second basis with -45° and 45° is used. From here on we will call it the "x basis".

Now the setup looks like Figure 3. This is also the setup used for quantum cryptography and for this experiment package.

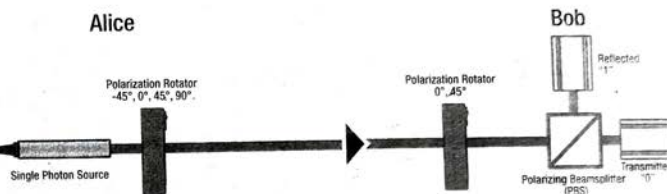


Figure 3 Quantum Cryptography Setup with the Bases + (0° and 90°) and x (-45° and 45°)

Now Alice has to make two *random* decisions for key generation:

- Alice has to select her basis at random, + or x
- Alice has to select a random bit, 0 or 1
  - Selecting 0 with the + basis means the setting 0°
  - Selecting 1 with the + basis means the setting 90°
  - Selecting 0 with the x basis means the setting -45°
  - Selecting 1 with the x basis means the setting 45°

Bob sets his polarization rotator to differentiate between the + and x bases. Accordingly Bob only needs the settings 0° and 45°.

If Bob selected the + basis and Alice sends in the + basis, Bob obtains an unambiguous result; this applies correspondingly if both choose the x basis. But what if Bob chooses a different basis than Alice? The result of choosing a different basis than Alice is that 45° polarized light will be sent to the beamsplitter. For a continuous beam, half is transmitted and half is reflected. However, assuming that only one photon is sent, only one of the two detectors can respond. The detector that responds is then left to chance. If the two bases do not match, Bob will nevertheless measure a signal on one of the two detectors. The probability of detecting the photon on one of the two detectors is 50% respectively.



In the table that follows, the different cases are shown again as an overview.<sup>1</sup>

Alice			Bob				Same basis?
Basis	Bit	Angle	Basis	Angle	Detector "0"	Detector "1"	
+	0	0°	+	0°	100%	0%	Yes
+	1	90°	+	0°	0%	100%	Yes
+	0	45°	+	0°	50%	50%	No
+	1	-45°	+	0°	50%	50%	No
x	0	0°	x	45°	50%	50%	No
x	1	90°	x	45°	50%	50%	No
x	0	45°	x	45°	100%	0%	Yes
x	1	-45°	x	45°	0%	100%	Yes

If Alice were to send a signal comprising of random bits in random bases and Bob analyzed the signal using a random basis – how does this become the key for data transmission?

The answer is that both Alice and Bob will tell each other which BASIS is being used to transmit each bit at a later time. In the last three columns of the table, the result is only unambiguous (100%) when the bases are the same.

In practice, Alice and Bob will go through each of the measurements and only communicate "+" or "x". When the two are different, both discard the measurement. But if both bases are the same, then BOTH know which BIT was transmitted based on the result obtained by Bob's detectors. The bases, not the bits, are ever communicated publicly. Therefore the encryption key is derived from the measurements in which Alice and Bob chose the same basis.

As soon as Alice and Bob have gone through all measurements this way, both are in possession of the (random) key. Now Alice can encrypt the message and send it in the + basis. Bob receives the message in the + basis and is then able to decrypt it.

Section 5.4 expands on this protocol and introduces an eavesdropper into the process. The results of the same exercise have much different results, which allow Alice and Bob to detect the presence of this eavesdropper.

## 5.4. Detection of an Eavesdropper

Let us examine the situation of an eavesdropper "Eve" placed between Alice and Bob. It consists of the same components as Alice and Bob, only in the reverse sequence. This is shown in Figure 4.

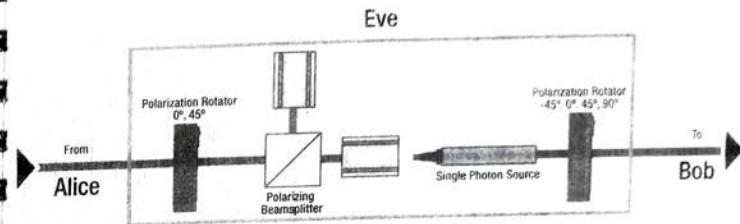


Figure 4 Eavesdropper Eve between Alice and Bob

Eve is placed in a position to measure the light coming from Alice and then attempt to transmit the identical information to Bob. Consider the following two possibilities:

- **Eve chooses the same basis as Alice:** In this case, Eve measures the signal that Alice sends correctly. Therefore, Eve will transmit the correct result to Bob in the same basis that was initially sent by Alice. Now Bob randomly chooses his basis, and once again there are two possibilities:
  - **Bob chooses the same basis as Alice:** Eve has transmitted the signal correctly using the same basis. Thus Bob obtains exactly the polarization state sent by Alice without detecting the presence of Eve.
  - **Bob chooses the other basis:** The basis used to receive the signal is different than the basis of the signal transmitted by Eve. Therefore, one of his detectors will respond at random. However, when Alice and Bob now compare their bases (same result as in the preceding subsection), this measurement is discarded anyway because of the different bases used by Alice and Bob.
- **Eve chooses the wrong basis:** In this case, Eve chooses a basis that differs from the one used by Alice and one of Eve's detectors will respond at random. Therefore, Eve is not able to judge whether she chose the correct basis. When Eve sends her signal to Bob, she will send the bit in the same basis that she received Alice's signal with.

<sup>1</sup> If slight variations of the table should be found in other implementations of this experiment, this is probably caused by a different polarization of the incident laser. If it is vertical, then the 0° (Alice) and 0° (Bob) make a digital 1.

Because Bob is also randomly choosing his basis, there are two possibilities:

- Bob chooses a different basis than Alice: This measurement is discarded after Alice and Bob compare bases.
- Bob chooses the same basis as Alice: This case produces the error which allows Alice and Bob to detect Eve eavesdropping. Keep in mind that Alice and Bob have confirmed that they sent and received the signal using the same basis, so the measurement is not discarded. However, Eve was eavesdropping in a different basis. This means two random detections took place: Eve in intercepting Alice's signal (because her basis did not match Alice's) and Bob's in receiving the intercepted signal (because his basis did not match Eve's).

In half of the cases the correct detector responds for Bob, so that he receives the same bit which Alice sent. But in the other half of the cases, the other detector will detect the photon. Therefore Bob obtains a different bit than the one sent by Alice.

To summarize: This represents a case where Alice and Bob obtain *different bits with the same bases* (which can never happen without third party interference). Therefore, the test for a spy is simple. After Alice and Bob have compared bases, they choose a certain number of bits with matching bases to compare publicly. If these test bits are identical, then there was no eavesdropper in the system.<sup>2</sup> But if errors are found in approximately 25% of the compared bits, then the communication was intercepted.

Although it may appear that Eve is only discovered only after eavesdropping, this is not the case since only one test encryption key has been generated so far. Even if Eve was eavesdropping (and therefore intercepted a certain number of bits undetected), this is inconsequential since no part of the actual message has been encoded or transmitted.

The individual cases are presented again briefly in a table for an overview. Only the cases where Alice and Bob use the same bases are considered here. The remaining measurements are discarded during the basis comparison process.<sup>3</sup>

Basis used by Alice and Bob	Basis used by Eve	Error?	Bits match for Alice and Bob
++	+	No	100%
++	x	In part	50%
xx	+	In part	50%
xx	x	No	100%

<sup>2</sup> Statistically it is possible for all test bits to be randomly correct. Therefore the sample size of bits must be large enough to ensure that the result is statistically significant.

<sup>3</sup> The 25% error rate can be calculated from the table. If Alice and Bob choose the + basis, then Eve also chooses the + basis in 50% of all cases, which cannot be detected. But in 50% of all cases she chooses the x basis. Furthermore, in 50% of these cases the correct detector responds due to the random chance associated with an incorrect signal transmission. Therefore, the total error rate is  $50\% \times 50\% = 25\%$ .

## 5.5. What Does "Random" Mean?

As described in Section 5.2, the one-time pad requires the completely random selection of the encryption key. This means computer-generated, pseudo-random numbers are not a solution for 100% security. However, quantum physics offers numerous possibilities for true randomness. For example, a photon that hits a 50:50 non-polarizing beamsplitter is transmitted or reflected entirely at random. Half are transmitted and the other half reflected on average, but the "decision" of an individual photon is completely random. While this particular principle applies to photons, many other processes such as radioactive decay are also entirely random.

In practice, we can interpret a photon reflected by the beamsplitter as a binary 0 and a photon transmitted through the beamsplitter as a binary 1. In the case of conventional light incident on two single photodetectors after a beamsplitter, if the intensity on the detectors is the same, then the distribution of hits on the detectors can be considered completely random as well.

Particularly, quantum physics random number generators are a key component of quantum cryptography data networks. Some commercially available options already exist: <http://www.idquantique.com/random-number-generation/>.

## 5.6. What prevents one from simply copying the information?

Consider the scenario where Eve could simply copy the photon carrying the information. In this case, the security of quantum cryptography would be wiped out, since she could send the original photon on to Bob and carry out her measurement on the copied photon. Eve could then intercept the key bits without Alice and Bob detecting the eavesdropping.

However, the exact copying of a quantum physics state is actually impossible. This principle is known as the "no-cloning theorem" which was formulated and proven in 1982. In general, this theorem states that no quantum state can be exactly copied without altering its state. Therefore, Eve could not copy a photon from Alice without altering it, and cannot send an unaltered photon to Bob while keeping a copy for analysis.



## 5.7. Experimental Procedure

The sequence of steps for this experiment are taken from the BB84 protocol. You can find the original publication [here](http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf).

<http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>

The sequence of the BB84 protocol experiment is:

1. Key transmission	<p>Alice chooses a random basis (x or +) and a bit (0 or 1). Bob then randomly chooses his basis (x or +). Both set their wave plates accordingly. Then the photon is sent through the setup (with us, the laser pulse).</p> <p>Bob notes whether he measured a 0 or a 1.</p> <p>Repeat this step many times.</p>
2. Erasing incorrect bases	<p>Alice and Bob go through their measurements and tell each other which bases they chose. They keep the bits measured when bases used by both Alice and Bob were the same. Any others are discarded from the sequence.</p> <p>Note: Only the bases are communicated between Alice and Bob (this can even be done publicly).</p> <p>After comparison, the remaining bits become the secret encryption key between Alice and Bob.</p>
3. Testing for a spy	<p>Alice and Bob publicly compare a sample of the transmitted bits in step 2. If errors exist, this confirms the presence of a spy and the key is erased.</p> <p>However, if no eavesdropper is detected, the test bits are removed and the remaining bits are the final encryption key.</p>
4. Encrypting the message	Using the key generated in step 3, Alice can encrypt the message.
5. Transmitting the message	Alice sends the encrypted message to Bob. This is done publicly.
6. Decrypting the message	Bob decrypts the message with the help of the generated encryption key.

There are additional steps in the protocol, which are not implemented for this experiment.

- Authentication: A few bits are exchanged at the start of communication according to a key established by Alice and Bob in advance. This step allows Alice to authenticate that she is communicating with Bob and not someone else.

If no errors occur then this confirms there is no eavesdropper in the line at the outset. One way to accomplish this step is to save a few bits from a previous communication for authentication in the next communication.

- Error correction: Since no system is perfect and measuring errors always occur, certain algorithms are used for error correction. These algorithms are not discussed here as it is outside the scope of the experiment.

## 5.8. Classical Light Versus Single Photons

The one major difference between this analogous experiment and a true quantum cryptography setup is that genuine safety from interception can only be guaranteed if a single photon source is used. This means the information of a bit has to be transported only by a single photon, since according to Section 5.6 it cannot be copied or measured without changes.

If any classical light source (even weakened lasers) is used instead of a single photon source, then Eve cannot be detected. All that is required to eavesdrop is for Eve to separate a portion of the transmitted light for detection/analysis while sending the remainder to Bob unnoticed.

Because the experiment detailed in this kit uses a pulsed light source (still not a single photon source), it cannot truly be employed as a perfect encryption system. However, the sequence of the protocol is completely identical to a true quantum encryption system.

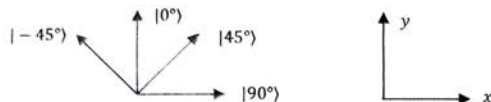
## 5.9. Mathematical Description in Dirac-Notation

Up to here, we described the experiments qualitatively. The preparation of the polarization states and their measurement by Bob (and Eve) are comprehensive parts of the experimental realization. However, every physical theory requires a mathematical description as well. In the following, we cast the experiments into formulas.

A suitable notation must first be found. For polarization states, Dirac's Bra-Ket Notation is an elegant choice. The four polarization states in this experiment are symbolized as

$$|-45^\circ\rangle, |0^\circ\rangle, |45^\circ\rangle, |90^\circ\rangle \quad (1)$$

where  $|0^\circ\rangle$  and  $|90^\circ\rangle$  are the basis states of the + basis and  $|-45^\circ\rangle$  and  $|45^\circ\rangle$  are the basis states of the x basis. The elegance of Dirac's notation lies in the fact that a state can be expressed and processed even if no distinct coordinate system has been chosen.



When a coordinate system has been chosen (to the right,  $xy$ ), the states can be written in vector form as

$$|0^\circ\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |90^\circ\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (2)$$

An important mathematical tool is the scalar product which is performed in the following way<sup>4</sup>

$$\langle 90^\circ | 0^\circ \rangle = (1 \ 0) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \quad (3)$$

The squared absolute value of the scalar product ( $|\langle 90^\circ | 0^\circ \rangle|^2$ ) is a descriptive quantity that represents the probability that a  $0^\circ$ -polarized photon passes through a polarizer oriented in the  $90^\circ$  direction. Naturally, this probability is 0 which is consistent with equation (3).

The states can also be expressed as linear combinations, e.g.,

$$|45^\circ\rangle = \alpha \cdot |0^\circ\rangle + \beta \cdot |90^\circ\rangle \quad (4)$$

Since the scalar product has to be normalized, it is show that

$$1 = |\langle 45^\circ | 45^\circ \rangle|^2 = \alpha^* \alpha \underbrace{\langle 0^\circ | 0^\circ \rangle}_{=1} + \alpha^* \beta \underbrace{\langle 0^\circ | 90^\circ \rangle}_{=0} + \alpha \beta^* \underbrace{\langle 90^\circ | 0^\circ \rangle}_{=0} + \beta \beta^* \underbrace{\langle 90^\circ | 90^\circ \rangle}_{=1} = |\alpha|^2 + |\beta|^2 \quad (5)$$

Due to symmetry it follows that  $\alpha = \beta = 1/\sqrt{2}$ . Therefore, all four states can be expressed as:

$$\begin{aligned} |45^\circ\rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle + \frac{1}{\sqrt{2}} |90^\circ\rangle \\ |-45^\circ\rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle - \frac{1}{\sqrt{2}} |90^\circ\rangle \\ |0^\circ\rangle &= \frac{1}{\sqrt{2}} |45^\circ\rangle + \frac{1}{\sqrt{2}} |-45^\circ\rangle \\ |90^\circ\rangle &= \frac{1}{\sqrt{2}} |45^\circ\rangle - \frac{1}{\sqrt{2}} |-45^\circ\rangle \end{aligned} \quad (6)$$

A vector representation can also be chosen, e.g.,  $|\pm 45^\circ\rangle = (\pm 1/\sqrt{2}, 1/\sqrt{2})^T$ . The probability that a  $0^\circ$ -polarized photon passes a  $45^\circ$  oriented polarizer can now be calculated:

<sup>4</sup> To be precise:  $|\langle a | b \rangle|^2 = \langle a | b \rangle \cdot \langle a | b \rangle^* = \langle a | b \rangle \langle b | a \rangle$ , where  $a^*$  is the complex conjugate of  $a$ .

$$|\langle 45^\circ | 0^\circ \rangle|^2 = \left| \frac{1}{\sqrt{2}} \underbrace{\langle 45^\circ | 45^\circ \rangle}_{=1} + \frac{1}{\sqrt{2}} \underbrace{\langle 45^\circ | -45^\circ \rangle}_{=0} \right|^2 = \frac{1}{2} \quad (7)$$

This means that the probability of a  $0^\circ$ -polarized photon passing a  $45^\circ$  oriented polarizer is 50%.

In the experiment, however, Bob and Eve only decide for a basis to measure in ( $+$  or  $x$ ) and observe which detector responds. The question is how to express that mathematically. In order to do so, operators  $\hat{M}_+$  and  $\hat{M}_x$  are introduced that each describe a measurement in either one or the other basis.

$$\hat{M}_+ = |0^\circ\rangle\langle 0^\circ| - |90^\circ\rangle\langle 90^\circ| \quad (8)$$

$$\hat{M}_x = |45^\circ\rangle\langle 45^\circ| - |-45^\circ\rangle\langle -45^\circ|$$

First, the operator of the  $+$  basis acts on the vertically and horizontally polarized state:

$$\hat{M}_+ |0^\circ\rangle = |0^\circ\rangle\langle 0^\circ | 0^\circ\rangle - |90^\circ\rangle\langle 90^\circ | 0^\circ\rangle = |0^\circ\rangle - |90^\circ\rangle \cdot 0 = |0^\circ\rangle \quad (9)$$

$$\hat{M}_+ |90^\circ\rangle = |0^\circ\rangle\langle 0^\circ | 90^\circ\rangle - |90^\circ\rangle\langle 90^\circ | 90^\circ\rangle = |0^\circ\rangle \cdot 0 - |90^\circ\rangle = -|90^\circ\rangle$$

The result is not too surprising – when the vertical or horizontal state is measured in the  $+$  basis we retrieve the state itself. Note that the observable  $\hat{M}_+$  is the quantity to be measured while the eigenvectors (namely  $|0^\circ\rangle, |90^\circ\rangle$ ) are the possible states of the system.<sup>5</sup> The eigenvalues (namely  $\pm 1$ ) represent the possible outcomes of the measurement. Here,  $+1$  corresponds to the transmission of the photon and  $-1$  corresponds to the reflection (which, in turn, can be interpreted as the phase jump occurring due to the reflection).

The diagonally polarized states behave accordingly when measured in the diagonal basis:

$$\hat{M}_x |45^\circ\rangle = |45^\circ\rangle\langle 45^\circ | 45^\circ\rangle - |-45^\circ\rangle\langle -45^\circ | 45^\circ\rangle = |45^\circ\rangle \quad (10)$$

$$\hat{M}_x |-45^\circ\rangle = |45^\circ\rangle\langle 45^\circ | -45^\circ\rangle - |-45^\circ\rangle\langle -45^\circ | -45^\circ\rangle = -|-45^\circ\rangle$$

The eigenvalue  $-1$  does not correspond to the reflection in our setup, though (since the state  $|-45^\circ\rangle$  corresponds to the transmission and, therefore, Bit 0). This can be understood by noting that we do not tilt the beamsplitter for a measurement in the diagonal basis but instead rotate the incident polarization by means of a  $\lambda/2$ -wave plate at the receiving unit.

What happens, though, when a  $45^\circ$ -polarized photon is measured in the  $+$  basis? In equation (7) it was shown that the transmission probability of this photon through a  $0^\circ$  polarizer can be calculated as 50%. Calculating the state yields a superposition of the  $|0^\circ\rangle$  and  $|90^\circ\rangle$  states:

<sup>5</sup> Reminder: when the equation  $\hat{M}|x\rangle = \chi|x\rangle$  holds for a state  $|x\rangle$  and an operator  $\hat{M}$ , we call  $|x\rangle$  an eigenvector of the operator  $\hat{M}$  with eigenvalue  $\chi$ .



$$\begin{aligned}
 \langle 1, |45^\circ\rangle &= \langle 0^\circ | 0^\circ \rangle \left( \frac{1}{\sqrt{2}} |0^\circ\rangle + \frac{1}{\sqrt{2}} |90^\circ\rangle \right) - \langle 90^\circ | 90^\circ \rangle \left( \frac{1}{\sqrt{2}} |0^\circ\rangle + \frac{1}{\sqrt{2}} |90^\circ\rangle \right) \\
 &= \frac{1}{\sqrt{2}} \langle 0^\circ | 0^\circ \rangle \langle 0^\circ | 0^\circ \rangle + \frac{1}{\sqrt{2}} \langle 0^\circ | 0^\circ \rangle \langle 0^\circ | 90^\circ \rangle - \frac{1}{\sqrt{2}} \langle 90^\circ | 90^\circ \rangle \langle 90^\circ | 0^\circ \rangle \\
 &\quad - \frac{1}{\sqrt{2}} \langle 90^\circ | 90^\circ \rangle \langle 90^\circ | 90^\circ \rangle = \frac{1}{\sqrt{2}} |0^\circ\rangle - \frac{1}{\sqrt{2}} |90^\circ\rangle \\
 \hat{M}_+ | -45^\circ \rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle + \frac{1}{\sqrt{2}} |90^\circ\rangle
 \end{aligned} \tag{11}$$

Similarly, measuring a vertically or horizontally polarized photon in the diagonal basis results in:

$$\begin{aligned}
 \hat{M}_+ |0^\circ\rangle &= \frac{1}{\sqrt{2}} |45^\circ\rangle - \frac{1}{\sqrt{2}} | -45^\circ\rangle \\
 \hat{M}_+ |90^\circ\rangle &= \frac{1}{\sqrt{2}} |45^\circ\rangle + \frac{1}{\sqrt{2}} | -45^\circ\rangle
 \end{aligned} \tag{12}$$

Now we know how the photon states change. In the following, we can mathematically describe the measurements and states for Alice, Bob, and Eve as described in the previous sections.<sup>6</sup> We start with a table describing the situation without Eve. Afterwards, a table presenting the description including Eve is shown.

Alice		Bob		
State	Basis, Bit	Chosen Basis	State	Measured Bit
0°⟩	+, 0	+	$\hat{M}_+  0^\circ\rangle =  0^\circ\rangle$	0
		×	$\hat{M}_\times  0^\circ\rangle = \frac{1}{\sqrt{2}}  45^\circ\rangle - \frac{1}{\sqrt{2}}   -45^\circ\rangle$	0 or 1
90°⟩	+, 1	+	$\hat{M}_+  90^\circ\rangle = - 90^\circ\rangle$	1
		×	$\hat{M}_\times  90^\circ\rangle = \frac{1}{\sqrt{2}}  45^\circ\rangle + \frac{1}{\sqrt{2}}   -45^\circ\rangle$	0 or 1
45°⟩	×, 1	+	$\hat{M}_+  45^\circ\rangle = \frac{1}{\sqrt{2}}  0^\circ\rangle - \frac{1}{\sqrt{2}}  90^\circ\rangle$	0 or 1
		×	$\hat{M}_\times  45^\circ\rangle =  45^\circ\rangle$	1
-45°⟩	×, 0	+	$\hat{M}_+   -45^\circ\rangle = \frac{1}{\sqrt{2}}  0^\circ\rangle + \frac{1}{\sqrt{2}}  90^\circ\rangle$	0 or 1
		×	$\hat{M}_\times   -45^\circ\rangle = -  -45^\circ\rangle$	0

- ☒ Bases of Alice & Bob Identical → Bit can be Used as Key Bit  
☐ Bases of Alice & Bob Not Identical → Measurement is Discarded

<sup>6</sup> Note that all calculations could also be performed in the vector representation. The state's representation was described above. The operator's representations are matrices, namely  $\hat{M}_+ =$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \hat{M}_\times = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

## Chapter 6 Examples

## 6.1. Encryption Protocol without Eve (Two Letters)

Step 1: Alice and Bob randomly select their bases, and Alice also selects her bits

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	X	X	+	X	+	+	+	X	X	+	X	X	+	+	X	+	X	X
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit																		

Step 2: Alice sends the bits in the chosen basis and Bob records the bits he measures. During Bob's measurements, he uses the bases chosen randomly by him. Bob will then interpret Alice's transmission as in the example below. Please note that in cases where the bases do not match, a 0 or 1 bit result is selected at random.

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

Alice		Eve		Bob	
Basis Bit	State	Basis	State	State	Measured Bit
+, 0	$ 0^\circ\rangle$	+	$M_x  0^\circ\rangle =  0^\circ\rangle$	$ 0^\circ\rangle$	0
		x	$M_x  0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$		0 or 1
		+	$M_x  45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $M_x  -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	$ 45^\circ\rangle$ or $ -45^\circ\rangle$	0 or 1
		x	$M_x  45^\circ\rangle =  45^\circ\rangle$ or $M_x  -45^\circ\rangle =  -45^\circ\rangle$		1
+, 1	$ 90^\circ\rangle$	+	$M_x  90^\circ\rangle = - 90^\circ\rangle$	$ 90^\circ\rangle$	1
		x	$M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$		0 or 1
		+	$M_x  45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $M_x  -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	$ 45^\circ\rangle$ or $ -45^\circ\rangle$	0 or 1
		x	$M_x  45^\circ\rangle =  45^\circ\rangle$ or $M_x  -45^\circ\rangle =  -45^\circ\rangle$		1
x, 1	$ 45^\circ\rangle$	+	$M_x  45^\circ\rangle = \frac{ 0^\circ\rangle +  90^\circ\rangle}{\sqrt{2}}$	$ 0^\circ\rangle$ or $ 90^\circ\rangle$	0
		x	$M_x  45^\circ\rangle =  45^\circ\rangle$	$ 45^\circ\rangle$	1
		+	$M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$		0 or 1
		x	$M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$		1
x, 0	$ -45^\circ\rangle$	+	$M_x  45^\circ\rangle = \frac{ 0^\circ\rangle -  90^\circ\rangle}{\sqrt{2}}$	$ 0^\circ\rangle$ or $ 90^\circ\rangle$	0
		x	$M_x  45^\circ\rangle =  45^\circ\rangle$	$ 45^\circ\rangle$	1
		+	$M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$		0 or 1
		x	$M_x  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$		1

- Bases of Alice & Bob & Eve Identical → Eve is Not Noticed
- Bases of Alice & Bob Not Identical → Measurement is Discarded Anyway
- Bases of Alice & Bob Identical; Bits are Incidentally Identical, Eve is Not Noticed
- Bases of Alice & Bob Identical; Bits Incidentally Differ → Eve is Uncovered



Step 3: Alice and Bob exchange their bases ("I have +" or "I have x"). Both Alice and Bob will note which of the transmitted bits were sent using the same basis (see below).

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	X	X	+	X	+	+	+	X	X	+	X	X	X	+	+	X	+	X
Bit	1	0	0	1	1	0	0	1	1	0	1	0	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	X

The resulting key generated by the two of them is: "0 1 1 0 0 1 0 0 0 1". Both know this key even though they have only exchanged their bases.

Step 4: Alice encrypts two letters with the key that was just generated. Read the binary representation of Q and M from the alphabet table, then perform binary addition on the first and second rows, see Chapter 9 for reference tables.

Letter	Q				M			
Data Bit	1	0	0	0	0	1	1	0
Key Bit	0	1	1	0	0	1	0	0
Encrypted Bit	1	1	1	0	0	1	1	0

Step 5a: Alice sends the encrypted message using the + basis (0° to indicate 0 and 90° to indicate 1). She therefore selects the following angle settings in the sequence below:

90°, 90°, 90°, 0°, 0°, 90°, 90°, 90°, 0°, 90°

Step 5b: Bob receives Alice's transmission using the + basis as well (reflected light = 1, transmitted light = 0). Bob will record the following received bits:

Received Bit	1	1	1	0	0	1	1	1	0	1
--------------	---	---	---	---	---	---	---	---	---	---

Step 6: Bob then uses the encryption key to decode the message (binary addition first and second lines)

Received Bit	1	1	1	0	0	1	1	1	0	1
Key Bit	0	1	1	0	0	1	0	0	0	1
Data Bit	1	0	0	0	0	0	1	1	0	0
Letter	Q					M				

## 6.2. Encryption Protocol with Eve

The process of generating the key is discussed again here, but this time with Eve who is eavesdropping. Her presence is discovered by comparing test bits.

Step 1: Alice, Bob and Eve randomly select their bases, and Alice also randomly selects bits to send.

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	X	X	+	X	+	+	+	X	X	+	X	X	X	+	+	X	+	X
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit																		

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	X	X	+	+	X	+	+	+	X	X	X	X	+	X	+	X	+	+

Step 2: Alice then sends the bits using her selected basis and Bob records the bits he measures. However, in this scenario, Eve is between Alice and Bob and selects her basis randomly as well (either 0° and 45°). If Eve's basis matches the one chosen by Alice, Eve will transmit the correct bit. If Eve selected the incorrect basis, she will transmit a random bit based on her interpretation of Alice's signal (0 or 1). Bob, however will record the bit that he receives from Eve. The measurements performed by Eve and Bob will appear as in the table below (Eve's measurements are shown for explanatory reasons, but are generally hidden from both Alice and Bob<sup>7</sup>):

Eve		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis		X	X	+	+	X	+	+	+	X	X	X	X	+	X	+	X	+	+
Bit		1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Bob		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis		+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit		1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

In the tables below, the same set of data measurements is presented but with all events determined by random chance highlighted in green. Green measurements in the first table indicate random events produced between Alice and Eve, while green measurements in the second table indicate random events produced between Eve and Bob.

In either case, neither Eve nor Bob know whether their measurement was randomly generated.

Eve		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis		X	X	+	+	X	+	+	+	X	X	X	X	+	X	+	X	+	+
Bit		1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Bob		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis		+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit		1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

<sup>7</sup> Similar to the experiment without Eve, the measurements where the bases do not match are random.

Step 3: At this point, Alice and Bob exchange the bases used for transmitting and receiving ("I have +°" or "I have X°"). They highlight the measurements where the bases match.

Alice		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis		X	X	+	X	+	+	+	X	X	+	X	X	X	+	+	X	+	X
Bit		1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis		+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit		1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

Step 4: Now Alice and Bob compare the bits for which their bases matched (the ones circled in red)

Alice:	0	1	1	0	0	1	0	0	0	1
Bob:	0	1	0	0	0	0	0	0	0	0

As seen above, there are differences between the two bit sequences – these are circled in blue. The errors occurred three times out of ten, which is close to the expected 25%.<sup>8</sup> The presence of errors in this test string alerts Alice and Bob to the presence of an eavesdropper and the protocol would be abandoned at this point.

<sup>8</sup> There is no system underlying the numbers chosen here. The fact that Bob has so many zeroes is therefore pure chance. Furthermore, the combination of "Alice=1, Bob=0" three times for the incorrect pairs is random. When the random events marked in green are chosen differently, the bits compared by Alice and Bob also change correspondingly.

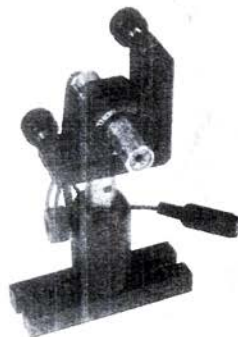


## Chapter 7 Setup and Adjustment

### 7.1. Component Assembly

Screw the RDF1 feet onto all breadboards. To do this, use the 1/4"-20 x 1/2" (M6 x 12 mm) screws to secure four feet to the bottom of each breadboard.

Take a BA1(M) base and screw one of the PH1.5 (PH40/M) post holders to it using a 1/4"-20 x 3/8" (M6 x 10 mm) screw. Insert a TR1.5 (TR40/M) post and screw the KM100 to it (see illustrations below). Insert the CPS635R-C2 laser into the AD11NT adapter ring which is secured in the KM100.



Take a BA1S(M) base and screw one of the PH2 (PH50/M) post holders to it. Insert a TR2 (TR50/M) post and screw the AT1(M) adjustment aid to it.



Take a BA1(M) base and screw one of the PH2 (PH50/M) post holders to it. Insert a TR2 (TR50/M) post. Remove the set screw from the TR2 (TR50/M) post using a hex key. Then screw the sensor unit (pictured below) to the post using the thread adapters. Carry out these steps for all 4 sensors.

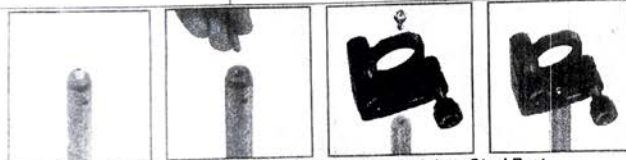


Figure 5 Mounting a KM100 to a Ø1/2" Stainless Steel Post

Now set up the two beamsplitters. Use the UPH2 (UPH50/M) universal holder and a TR2 (TR50/M) post. Remove the set screw from the post with a hex key. Attach a TR2 (TR50/M) post. Remove the set screw from the post with a hex key. Attach the PM3(M) supporting arm as shown in Figure 6. Use protective gloves to pick up the PBS201 and insert it in the orientation shown in photos below. It is secured by tightening the screw in the supporting arm. Verify the correct orientation (lettering on the bottom, edge correct).

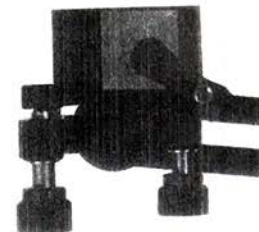


Figure 6 Mount PBS201 Beamsplitter to Kinematic Platform

#### ATTENTION

Avoid touching the  $\lambda/2$  plates with bare hands. Wearing gloves during assembly is strongly recommended. Only grasp the edge of optical components in order to avoid touching the surface with bare fingers.

Install the  $\lambda/2$ -plates. First, screw a PH1.5 (PH40/M) post holder onto a BA1(M) base. Screw a TR1.5 (TR30/M) post into the RSP1X225(M)-ALICE indexing rotation mount (see image to the right). Unscrew the retaining ring by using the included SPW606 spanner wrench. Insert the  $\lambda/2$ -plate and lock it in place with the retaining ring. Repeat the steps for all 4 rotation mounts. Two of the mounts are engraved with 0° and 45° markings while the other two rotation mounts are engraved with four markings (-45°, 0°, 45°, and 90°). The procedure for aligning these rotation mounts is described in Section 7.3.



## 7.2. Electronics

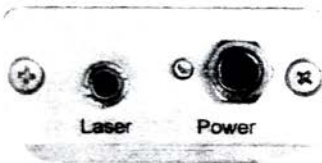
### 7.2.1. Power Supply

The power supply included in this kit is designed to provide a stabilized 5 V. Select the correct plug for your region and insert it in the jack on the power supply.



### 7.2.2. Laser Electronics

In addition to the connection for the power supply, the laser electronics box<sup>9</sup> only has an input for the laser. An adapter cable is included to connect the laser electronics with the CPS635R-C2 laser module.



The laser electronics control unit features a fire button that is used to switch between pulse mode and continuous wave mode (see picture to the right). Hold the fire button down for 2 seconds to switch the laser to continuous wave mode. Pressing the fire button briefly ends the continuous wave mode so that short pulses are sent. The output of the laser is visible when a piece of paper is held in front of the laser. A green LED on the side of the laser electronics control unit indicates that it is ready for use.



<sup>9</sup> Use the supplied power supply for operation. A user-supplied power unit must be a stabilized power supply with 5 V and min. 0.5 A (2.5 W) with a 5.5/2.1 mm power socket (positive terminal inside).

### 7.2.3. Sensor Electronics

The sensor electronics have a connection for the power supply and two sensor inputs. A sensor can be plugged into either of the two sensor ports. Ensure that the sensors are connected to the electronics box prior to inserting the power supply.

The sensor electronics box is equipped with a green button that is used to switch between "adjustment mode" and "measuring mode". These modes determine how the sensor LEDs respond when a laser pulse is received by both sensors simultaneously.

In adjustment mode, the LED on the side of the box lights up yellow. When light of equal intensities is received by both sensors, the blue LEDs on both sensor will light up.

In measuring mode, the LED on the side of the box lights up green. When light of equal intensities is received by both sensors, one of the two blue LEDs (randomly selected) lights up. This effect simulates the "decision" of the single photon which is transmitted or reflected with 50% probability on the beamsplitter.



### 7.3. Adjusting the Laser and $\lambda/2$ -Plates

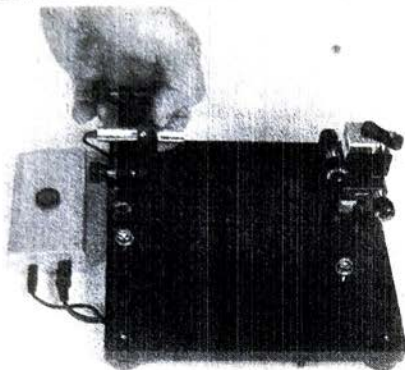
Before performing the experiment, the polarization plane of the laser and the orientation of the  $\lambda/2$ -plates need to be aligned.

- First, place the laser and the beamsplitter on one of the breadboards.
  - Hold the fire button down for 2 seconds so the laser switches to continuous wave mode. This makes adjustment much easier.

**WARNING**

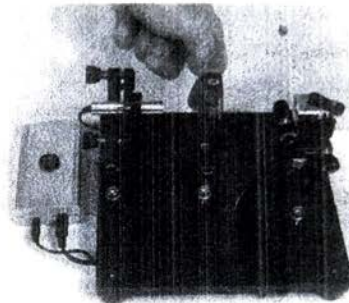
The laser module is a class 2 laser. Although no protective eyewear is required to operate class 2 lasers, do not look directly into the beam or into scattered light.





1. Use the AT1/M height adjustment tool to ensure that the laser runs parallel to the tabletop. Adjust the laser tip/tilt using the adjusters on the KM100 mount, if necessary. To ensure the best alignment, use the AT1/M adjustment tool alternating between close and far distances from the laser during the alignment process.
2. Position the laser and beamsplitter such that light reflected off the beamsplitter surface is at a 90° angle from the incoming beam.
3. Now the laser is turned in its holder, rotating the polarization of the laser. While the laser does not have full linear polarization, it has a predominant direction. Slightly loosen the screw that clamps the adapter ring in the kinematic holder. Rotate the laser using the adapter ring. In order to keep it from sliding away, one should put pressure onto the adapter ring from the front with two fingers. Now use a sheet of paper to observe the laser intensity reflected by the beamsplitter cube. It should distinctly decrease and increase again during rotation. You are looking for the setting with the lowest intensity on the reflected path.
4. Continue turning the laser until the intensity of the light reflecting off the beamsplitter is **minimal** and screw down the laser in this position.
5. Take the entire assembly (laser and holder) out of the setup and repeat the previous steps using the other laser. After this process, both lasers should be horizontally polarized.

- Place the rotation mount (Item # RSP1X225(M)-ALICE) with the  $\lambda/2$  between laser and beamsplitter, with the engraved dial face facing the laser.
- Loosen the screw at the top of the rotation mount for continuous movement.



- Rotate the  $\lambda/2$  plate and observe the reflected intensity. The intensity will vary with the rotation angle. Look for the orientation with the lowest reflected intensity.
- Once you've found the angle which minimizes the intensity of the reflected light, engage the indexing mode by tightening the screw at the top of the rotation mount.
- Take the rotation mount out of the setup and re-align the dial face. To do this, loosen the two small screws on the face of the mount. Rotate the dial face until the "0" mark is aligned with the small mark at the centered top part of the mount as shown in the photo below. The wave plate should not rotate during this step. Tighten the two screws on the face plate to secure the dial face.



- Repeat the previous steps with all rotation mounts and wave plates.

#### 4. Setup for Alice and Bob

Alice and Bob should face each other at a distance of about 60 cm. For best performance, set up the two breadboards up as parallel as possible.

- Set up Alice (laser and the  $\lambda/2$  plate) on the small breadboard. The rotation mount should be centered on the breadboard. The holder is engraved with markings "45, 0, 45, 90°" facing the laser. Set Alice's laser to continuous mode (hold the red button down for 2 seconds).
- On the other breadboard (Bob), set up the other  $\lambda/2$  plate directly at the edge of the breadboard. This wave plate holder is engraved with "0, 45°" markings. The markings should point away from Alice.
- Place one of the two sensors at the other end of Bob's breadboard (opposite the wave plate holder). Roughly align the position of the sensor so that the laser is incident on the detector.
- Place the beamsplitter in between Bob's wave plate holder and detector. It should be as close to perpendicular to the beam as possible.
- The second sensor should be placed such that:
  - Laser light from Alice that is reflected by the beamsplitter is incident on this detector. The sensors should be placed such that the entrance is perpendicular to the incident light.
  - The distance between both detectors and the beamsplitter is equal.

The setup should now look as follows:

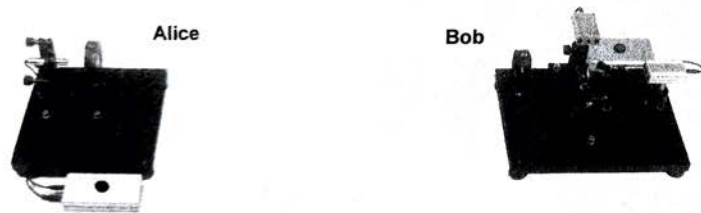


Figure 7 Alice and Bob

#### Fine-Tuning the Alignment

- Set the sensor electronics to adjustment mode (the side LED lights up yellow).
- Set both polarization rotators to 0° and press the fire button. The blue LED on the sensor in the path of the laser should light up. If this is not the case, check:
  - That the sensor is actually perpendicular to the beam.
  - That the laser is incident on the opening in front of the detector in the sensor.

- That the sensor is at the correct height.
- That the laser light is centered on the hole in the sensor module.

If difficulties are encountered, have one user continue sending pulses with the laser while the other aligns the sensor.

When this sensor is configured correctly align the other sensor in the setup.

- Set the  $\lambda/2$  plate of Alice to 90° on the scale (Bob stays at 0°). Now the LED on the other sensor (reflected from the beamsplitter) should light up when a pulse is sent from Alice.
- The tip/tilt of the beamsplitter cube can be adjusted to align the reflected beam with this sensor.

Repeat these alignment steps with other polarization rotation combinations:

For example, using polarizer rotation settings of 45° and -45° on Alice and a 0° setting on Bob, both sensor LEDs should light up. This is because the light is split by the beamsplitter and half of the total incident light reaches each sensor. If the expected behavior (indicated in the tables below) does not occur, continue alignment of the sensors. Alternatively, confirm that the sensors are in adjustment mode, i.e., the side LED on the sensor electronics is lit up yellow.

Overall one has to test 8 cases, all of which have to work before starting the experiment.<sup>10</sup>

Alice	Bob	Which LED lights up	Bit
-45°	0°	Both	Random
0°	0°	Transmitted	0
45°	0°	Both	Random
90°	0°	Reflected	1

Alice	Bob	Which LED lights up	Bit
-45°	45°	Transmitted	0
0°	45°	Both	Random
45°	45°	Reflected	1
90°	45°	Both	Random

Once all cases are verified, set the sensor electronics to measuring mode (LED changes from yellow to green).

All eight cases must perform correctly, otherwise the experiment will not produce the correct results. Chapter 11 contains a troubleshooting guide for additional help with aligning the sensors and lasers.

**Important:** The setup should not be moved during the experiment. Leaning on the table may cause the laser and sensors to become misaligned.

<sup>10</sup> The bit value has also been added to the table for assistance. Random events will cause both LEDs to light up if the sensor electronics are in adjustment mode. If the sensor electronics are in measuring mode, only one random LED will light up.



## 7.5. Adding Eve

To add Eve as an eavesdropper to the setup, place the large breadboard between the breadboards of Alice and Bob. In this scenario, Eve is intended to intercept transmissions from Alice to Bob, so avoid making changes to Alice and Bob and align Eve within the setup.

Attach the BBH1 handles onto the breadboard of Eve. This makes it possible to add and remove Eve quickly.

Install Eve's receiver. The setup is the same as aligning Bob's receiver described in Section 7.4. Test to verify that all 8 cases are aligned correctly. Then set the sensor electronics from adjustment mode back to measuring mode.

Set up Eve's transmitter. Eve's transmitting laser should be aligned to hit each of Bob's sensors (depending on polarization). Use alignment mode on Eve's laser to aid alignment. Verify that all 8 transmission cases work between Eve's transmitter and Bob, and then switch Eve's laser back to measuring mode.

The laser and sensor electronics box can be attached to the breadboard using a CL3/M clamp. This makes it easier to take out Eve. As shown in the photo to the right, each clamp utilizes two screws. The 1/4"-20 x 1.25" (M6 x 30 mm) cap screw to the far right adapts the clamp to the needed height, while the closer 1/4"-20 x 2" (M6 x 45 mm) cap screw secures the clamp to the breadboard.



The finished setup of Eve looks as follows:

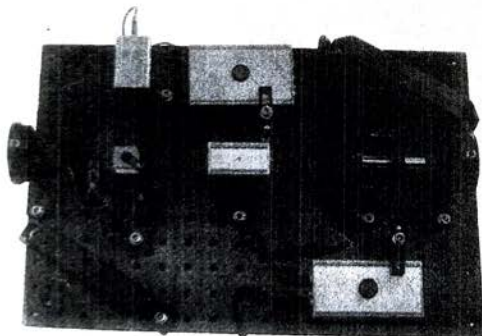


Figure 8 Eve

## Chapter 8 Experiment

The experiment is divided into three sections:

- **Section 8.1:** Generating a key with a length of at least 20 bits
- **Section 8.2:** Encryption and transmission of a 4-letter word
- **Section 8.3:** Installation of Eve and detection of an eavesdropper

In order to complete the exercises, the user should be familiar with the encryption principles outlined in Chapter 5. Detailed examples are presented in Chapter 6, illustrating the entire process with and without Eve. A sample measurement protocol can be found in Chapter 9.

### 8.1. Key Generation

**Exercise 1:** Set up Alice and Bob so that they face each other at a large distance (leave enough space to place Eve between Alice and Bob). Using the guidelines in Chapter 7, align Alice and Bob so that all 8 transmission cases produce reproducible results. During this step, the sensor electronics should be in adjustment mode (the LED indicator is yellow).

**Execution:** See Chapter 7 for setup instructions. A basic schematic is shown in Figure 3 and a photo of the complete setup is shown in Figure 7. The possible transmission cases are outlined in Section 7.4.

**Exercise 2:** Alice and Bob randomly select their bases and Alice also selects random bits for transmission. Chapter 9 provides a 52-bit measuring protocol. Fill in the bits and bases that Alice will use to transmit her signal and the bases that Bob will use for detection.

**Execution:** This corresponds to step 1 in the example described in Section 6.1. The protocols can be found in Chapter 9.

**Exercise 3:** Transmit Alice's bits in the bases chosen in Exercise 2. Bob notes the bits he receives.

**Execution:** This corresponds to step 2 in the example described in Section 6.1. Alice and Bob have to generate a key that is at least 20 bits long. We recommend a transmission sequence of at least 52 bits for this purpose. Because of the random component in generating a key, a longer transmission is more likely to achieve the 20 matching bases for the encryption key. During this step, the sensor electronics should be in measurement mode (the LED indicator is green).

To summarize the choice of bases used in transmission, if Alice:

- Selects 0° then she sends a 0 in the "+" basis.
- Selects 90° then she sends a 1 in the "+" basis.
- Selects -45° then she sends a 0 in the "x" basis.
- Selects 45° then she sends a 1 in the "x" basis.

Alice and Bob transmit the bits according to the table prepared in Exercise 2. Alice sends her bit and Bob notes his measurement (reflected = 1, transmitted = 0).

**Exercise 4:** Alice and Bob publicly exchange the bases used for each measurement. They then erase any measurements where the bases do not match. The remaining measurements/bits form the complete encryption key.

*Execution:* This corresponds to step 3 in the example detailed in Section 6.1. Alice and Bob exchange their bases ("I have chosen + or "I have chosen x") and mark any measurements with matching bases. The corresponding bits form the encryption key.

If 52 measurements are not enough to generate a 20 bit encryption key, then the transmission should be repeated with more measurements until a 20 bit key is generated.

## 8.2. Encryption and Transmission of a Four-Letter Word

**Exercise 5:** Encrypt Alice's message (4 letters) using the key that was generated.

*Execution:* The procedure is described in step 4 of Section 6.1 and also in Section 5.2.

**Exercise 6:** Transmit the encrypted message from Alice to Bob.

*Execution:* Transmission of the actual message is done entirely in one basis. Alice sends her encrypted bits (0° for 0, 90° for 1). Alice and Bob do not change the basis for data transmission. This corresponds to steps 5a and 5b in Section 6.1.

**Exercise 7:** Decrypt the bits received by Bob to find Alice's message.

*Execution:* This process is the same as described in Section 5.2 and corresponds to step 6 in Section 6.1.

## 8.3. Adding Eve and Detection of Eavesdropping

**Exercise 8:** Place Eve between Alice and Bob, and set both sensor electronics to adjustment mode (LED lights up yellow). Adjust Eve's receiver so that all 8 transmission cases work with Alice. Then, adjust Eve's transmitter so that all 8 transmission cases work with Bob. Return to measurement mode for both sensor electronics (LED lights up green).

*Execution:* The adjustment is performed as described in Chapter 7 (also see Figure 4 and Figure 8). The goal should be to align Eve without disturbing the setups for Alice and Bob, since the eavesdropper has no influence on the sender and receiver. Then set the sensor electronics to measurement mode.

**Exercise 9:** Fill out the table for Eve, which determines the random choice of the + or the x basis. Random bases are also needed Alice and Bob again, and random bits should be chosen by Alice for transmission.

*Execution:* There are two methods for implementing this step. In an ideal scenario where the users are isolated from each other, Eve could just choose a basis spontaneously and transmit the measured result. However, because users are in the same room, the physical act of changing a basis leads to a non-random bias for Eve's operator. Choosing random bases at the start of the sequence prevents this bias from interfering with the results of the experiment. A sample table of bases for Eve to use can be found in Chapter 9. Keep in mind that Eve's operator does not have to record any data.

An example is also provided in Step 1 of Section 6.2.

**Exercise 10:** Send Alice's first bit using the basis chosen in the previous exercise. Eve chooses her first basis (randomly chosen in Exercise 9). She receives a bit which she relays to Bob using the same basis. Bob records the bit he receives. This is performed for all 52 bits/bases in the sequence.

*Execution:* Alice and Bob use the same procedure as in Exercise 3. Eve receives the signal from Alice using the randomly chosen basis from Exercise 9. Then she transmits her measurement (using the same basis). This exercise corresponds to step 2 of Section 6.2.

**Exercise 11:** Alice and Bob publicly exchange their bases for each measurement. They then erase the measurements in the sequence where the bases do not match.

*Execution:* Similar to Exercise 4, Alice and Bob compare their bases and eliminate bits where the bases used do not match. The remainder forms the bit sequence that is used to test for an eavesdropper. This exercise corresponds to step 3 in Section 6.2.

**Exercise 12:** Compare Alice's and Bob's results from exercise 11.

*Execution:* Because of Eve's eavesdropping and transmitting bits using a random basis (not necessarily identical to Alice), the bit sequences recorded by Alice and Bob should contain errors (bits that do not match). The presence of these errors is what allows Alice and Bob to detect the presence of an eavesdropper. This is different than the result from Exercise 4, where Alice and Bob should obtain the same result. This exercise corresponds to step 4 in Section 6.2.



## Chapter 9 Measuring Protocols

This section contains the measuring protocols for Alice, Bob and Eve.

In order to make them easy to print, each of them is on one page (the manual is also available as a free download at [discovery.thorlabs.com](http://discovery.thorlabs.com)).

Then you find the table with the encoding of the alphabet using 5 bits per letter.

### Measuring protocol for key generation – ALICE

[illegible][illegible][illegible]

**Generated Key:**

Angle setting (reminder)	Basis +	Basis x
Bit 0	0°	-45°
Bit 1	90°	45°

**Table for encryption of the message – Alice**

[illegible]

■ Data Bit = letter in binary form, 4 x 5 Bit