QKD: Fundamentals

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. We will discuss how an eavesdropper can be detected using this method.

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/

References:
- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: The One-Time Pad → 메시지 ⊗ 키값 = 암호화된 메시지

키를 가진쪽 → 암호화된걸 받아서 키값이랑 XOR 연산 → 원래 메시지 게또! 예~~

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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: The One-Time Pad

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

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

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: The One-Time Pad

To summarize the essential requirements: OTP가 안전하게 쓰이려면

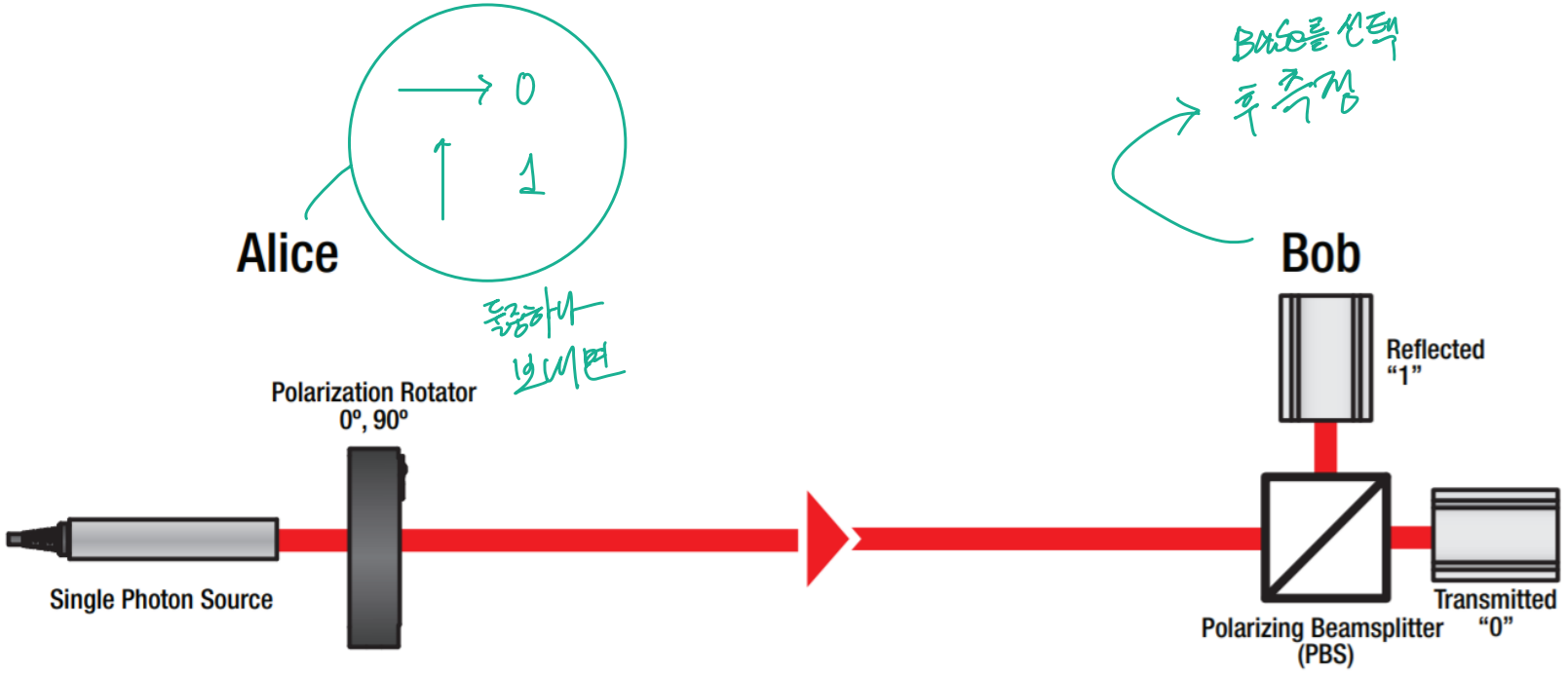
1. The key has to be at least as long as the message. Key는 메시지보다 길어야 → 전체 메시지를 암호화 해야될거 아님
2. The key must only be used once. 키는 일회용, 계속쓰면 패턴이 생겨서 이게 개꿀이라고 할수도
3. The key must be completely random. 그렇지만 그게 쉽진 않으듯, 알고리즘 기반이라 예측될 가능성 有
4. The key must be known only to the sender and the recipient. 이건당연한거지만 고전적 방식은 파훼가 가능해서 문제!!

Requirement 1 is easy to meet by the sender, who can only encrypt a number of bits that is less than or equal to the number of available key bits. Requirement 2 is the responsibility of the sender and recipient, and is easily realizable as 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. 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.

References:
- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Key distribution

This subsection is intended to facilitate a better understanding by briefly running through the process of transmitting data with one basis. Actual quantum cryptography (in the real world) 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”. An example is shown in the figure below.



References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

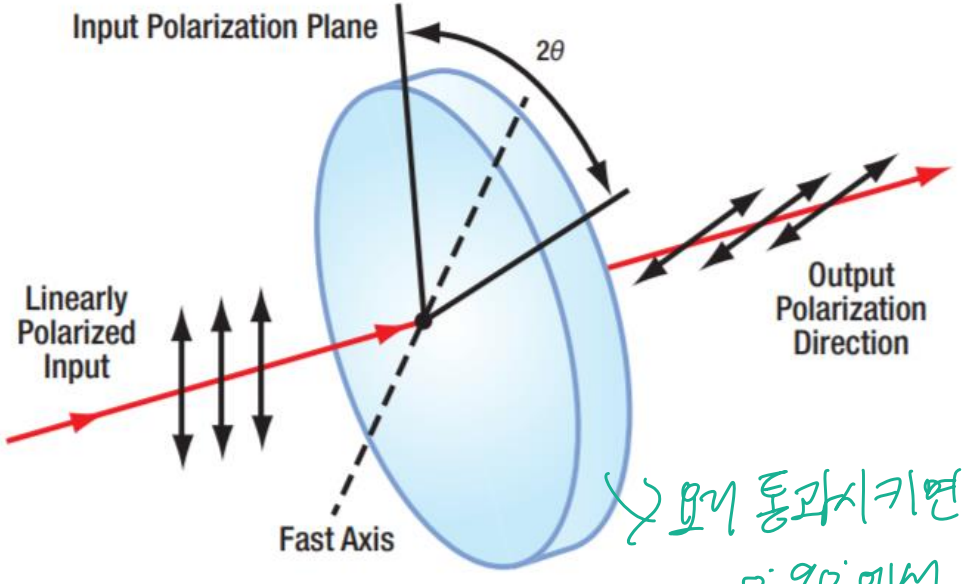
QKD: Key distribution

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° relative to the incoming polarization, the polarization of the light is actually rotated by 90°. 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.

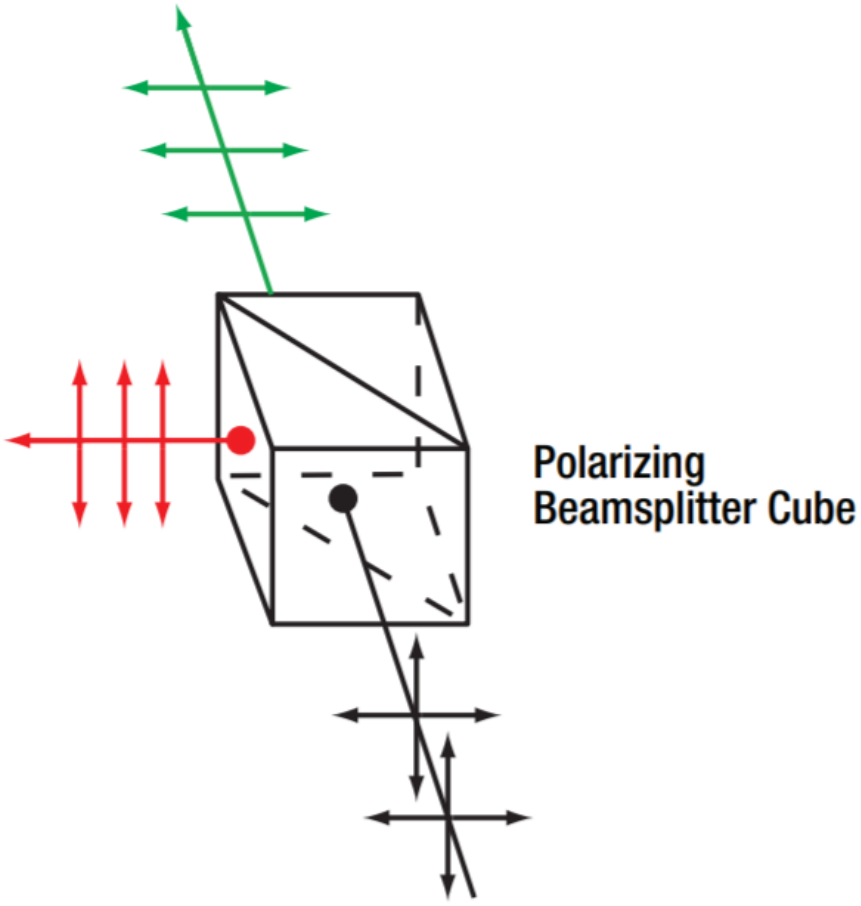


References:
- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Key distribution

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”).



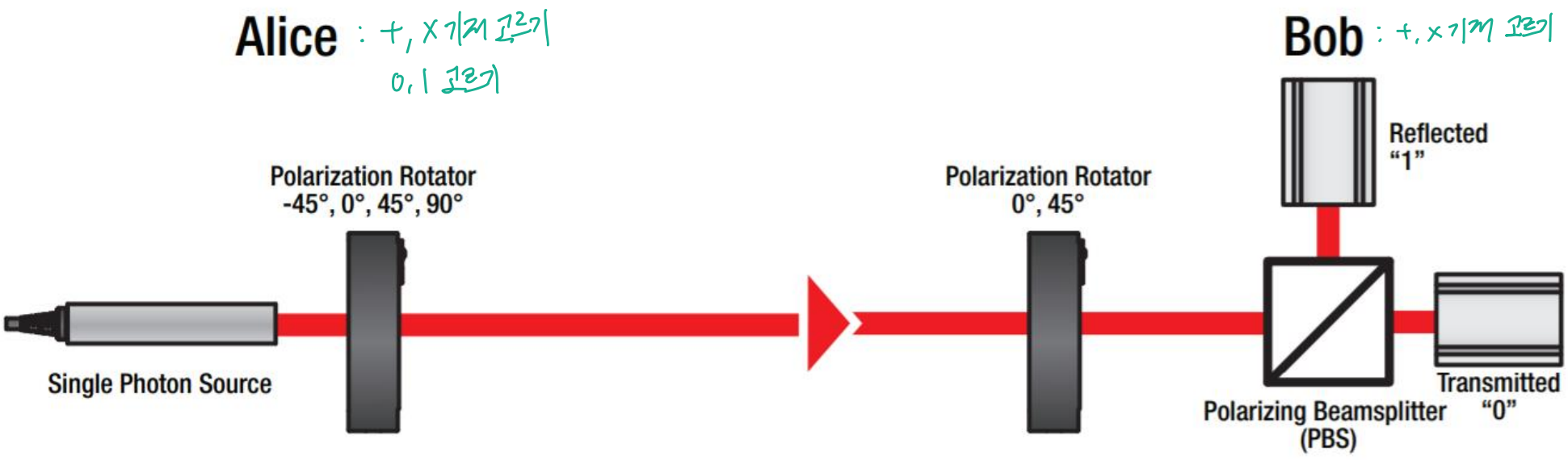
References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: 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 below.

+ 기계와 x 기계 두개 써야 좋은



References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Key Distribution – The Right Way

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
    - o Selecting 0 with the + basis means the setting 0°
    - o Selecting 1 with the + basis means the setting 90°
    - o Selecting 0 with the x basis means the setting -45°
    - o 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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Key Distribution – The Right Way

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
x	1	45°	+	0°	50%	50%	No
x	0	-45°	+	0°	50%	50%	No
+	0	0°	x	45°	50%	50%	No
+	1	90°	x	45°	50%	50%	No
x	1	45°	x	45°	**100%**	0%	Yes
x	0	-45°	x	45°	0%	**100%**	Yes

같은 기계를 사용한 값만 쓰였다

다른게 사용 → 반반이라 버림

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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Detection of an Eavesdropper

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

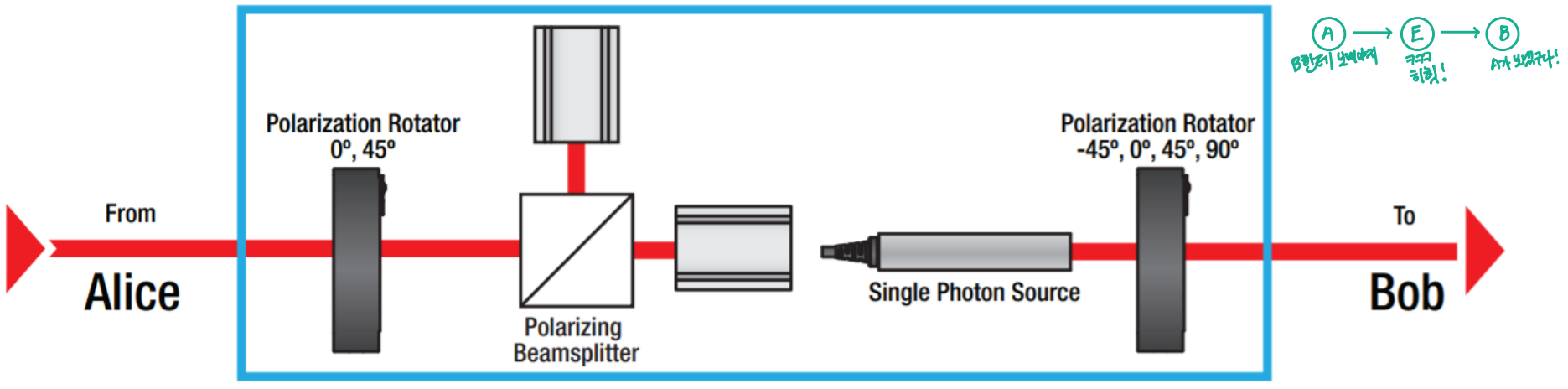


Figure 4 Eavesdropper Eve between Alice and Bob

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Detection of an Eavesdropper

E, 앨리스랑 같은 basis 선택 → 정확해요!

B, A랑 같은 basis → 문제 X

B, A랑 다른 " → 어차피 찾다버릴거임

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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Detection of an Eavesdropper

E≠A → E→B 과정에서 오류 발생

- 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.

  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. 갖다버려
  - 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). → 같은 basis인데 왜 측정값이 다르지? → 어브?!

    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.

References:
- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Detection of an Eavesdropper

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.[2] 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.[3]

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

A=E일땐 문제×

A≠E일때 문제

[2] 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.

[3] 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% x 50% = 25%.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: What Does “Random” Mean?

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/.

References:
- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change,” 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: What prevents one from simply copying the information?

photon 복사해서 갖고갈수 있어요? 쓸모없는데 아님?

→ LL 안됨, 노클로닝

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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Other Steps

There are additional steps in the protocol,

- 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 vary by quantum channels.

References:
- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: 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

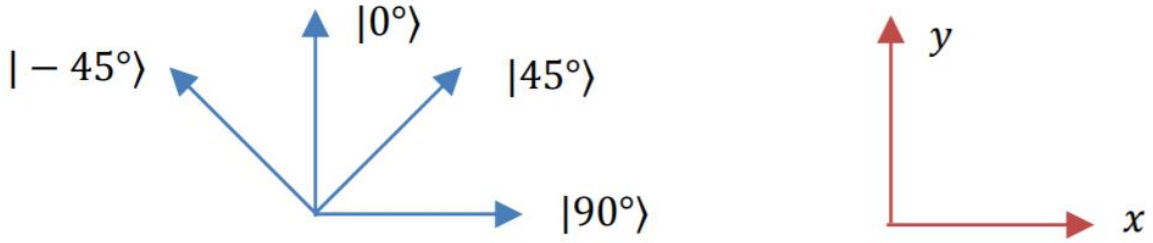
$$|-45°\rangle,\ |0°\rangle,\ |45°\rangle,\ |90°\rangle \qquad (1)$$

where $|0°\rangle$ and $|90°\rangle$ are the basis states of the + basis and $|-45°\rangle$ and $|45°\rangle$ 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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation



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

$$|0°\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \quad |90°\rangle = \begin{pmatrix}1\\0\end{pmatrix} \tag{2}$$

An important mathematical tool is the scalar product which is performed in the following way[4]

$$\langle 90°|0°\rangle = \begin{pmatrix}1 & 0\end{pmatrix} \cdot \begin{pmatrix}0\\1\end{pmatrix} = 0 \tag{3}$$

0°가 90°로 발견될 확률

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

$|\langle a|b\rangle|^2$ ⇒ b가 a로 발견될 probability

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

$$|45°\rangle = \alpha \cdot |0°\rangle + \beta \cdot |90°\rangle \tag{4}$$

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

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

$$1 \overset{!}{=} |\langle 45°|45°\rangle|^2 = \alpha^*\alpha \underbrace{\langle 0°|0°\rangle}_{=1} + \alpha^*\beta \underbrace{\langle 0°|90°\rangle}_{=0} + \alpha\beta^* \underbrace{\langle 90°|0°\rangle}_{=0} + \beta\beta^* \underbrace{\langle 90°|90°\rangle}_{=1} = |\alpha|^2 + |\beta|^2 \tag{5}$$

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

$$\begin{aligned} |45°\rangle &= \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle \\ |-45°\rangle &= \frac{1}{\sqrt{2}}|0°\rangle - \frac{1}{\sqrt{2}}|90°\rangle \\ |0°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|-45°\rangle \\ |90°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle - \frac{1}{\sqrt{2}}|-45°\rangle \end{aligned} \tag{6}$$

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

[4] *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.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

$$|\langle 45°|0°\rangle|^2 = \left|\frac{1}{\sqrt{2}}\underbrace{\langle 45°|45°\rangle}_{=1} + \frac{1}{\sqrt{2}}\underbrace{\langle 45°|-45°\rangle}_{=0}\right|^2 = \frac{1}{2} \tag{7}$$

This means that the probability of a 0°-polarized photon passing a 45° 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 $\widehat{M}_+$ and $\widehat{M}_\times$ are introduced that each describe a measurement in either one or the other basis.

$$\begin{aligned}\widehat{M}_+ &= |0°\rangle\langle 0°| - |90°\rangle\langle 90°| \\ \widehat{M}_\times &= |45°\rangle\langle 45°| - |-45°\rangle\langle -45°|\end{aligned} \tag{8}$$

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

$$\begin{aligned}\widehat{M}_+ |0°\rangle &= |0°\rangle\langle 0°|0°\rangle - |90°\rangle\langle 90°|0°\rangle = |0°\rangle - |90°\rangle \cdot 0 = |0°\rangle \\ \widehat{M}_+ |90°\rangle &= |0°\rangle\langle 0°|90°\rangle - |90°\rangle\langle 90°|90°\rangle = |0°\rangle \cdot 0 - |90°\rangle = -|90°\rangle\end{aligned} \tag{9}$$

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

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 $\widehat{M}_+$ is the quantity to be measured while the eigenvectors (namely $|0°\rangle, |90°\rangle$) are the possible states of the system.[5] The eigenvalues (namely ± 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 interpretated as the phase jump occurring due to the reflection).

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

$$\widehat{M}_\times |45°\rangle = |45°\rangle\langle 45°|45°\rangle - |-45°\rangle\langle -45°|45°\rangle = |45°\rangle$$
$$\widehat{M}_\times |-45°\rangle = |45°\rangle\langle 45°| - 45°\rangle - |-45°\rangle\langle -45°| - 45°\rangle = -|-45°\rangle \quad (10)$$

The eigenvalue -1 does not correspond to the reflection in our setup, though (since the state $|-45°\rangle$ 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.

Transmission in PBS = '0'
Reflection in PBS = '1'

[5] *Reminder: when the equation $\widehat{M}|x\rangle = \chi\,|x\rangle$ holds for a state $|x\rangle$ and an operator $\widehat{M}$, we call $|x\rangle$ an eigenvector of the operator $\widehat{M}$ with eigenvalue χ.*

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

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

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

$$\widehat{M}_+ |-45°\rangle = \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle$$

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

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

$$\widehat{M}_{\times}\,|0°\rangle = \frac{1}{\sqrt{2}}|45°\rangle - \frac{1}{\sqrt{2}}|-45°\rangle$$
$$\widehat{M}_{\times}\,|90°\rangle = \frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|-45°\rangle \qquad (12)$$

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.[6] We start with a table describing the situation without Eve. Afterwards, a table presenting the description including Eve is shown.

[6] *Note that all calculations could also be performed in the vector representation. The state's representation was decribed above. The operator's representations are matrices, namely* $\widehat{M}_{+} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $\widehat{M}_{\times} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

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

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

References:

- D.L.D Lowndes, "Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change," 10.2014.
- Quantum Cryptography, Thorlabs manual

QKD: Mathematical Description in Dirac-Notation

Alice		Eve			Bob		
Basis, Bit	State	Basis	State	State Sent	Basis	State	Measured Bit
$+,0$	$\|0°\rangle$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	$\|0°\rangle$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
					$\times$	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
		$\times$	$\hat{M}_\times \|0°\rangle = \frac{\|45°\rangle}{\sqrt{2}} - \frac{\|-45°\rangle}{\sqrt{2}}$	$\|45°\rangle$ or $\|-45°\rangle$	$+$	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ or $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1 0 or 1
					$\times$	$\hat{M}_\times \|45°\rangle = \|45°\rangle$ or $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	1 0
$+,1$	$\|90°\rangle$	$+$	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	$\|90°\rangle$	$+$	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	1
					$\times$	$\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
		$\times$	$\hat{M}_\times \|90°\rangle = \frac{\|45°\rangle}{\sqrt{2}} + \frac{\|-45°\rangle}{\sqrt{2}}$	$\|45°\rangle$ or $\|-45°\rangle$	$+$	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ or $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1 0 or 1
					$\times$	$\hat{M}_\times \|45°\rangle = \|45°\rangle$ or $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	1 0
$\times,1$	$\|45°\rangle$	$+$	$\hat{M}_+ \|45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} - \frac{\|90°\rangle}{\sqrt{2}}$	$\|0°\rangle$ or $\|90°\rangle$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$ or $\hat{M}_+ \|90°\rangle = -\|90°\rangle$	0 1
					$\times$	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ or $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1 0 or 1
		$\times$	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	$\|45°\rangle$	$+$	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
					$\times$	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	1
$\times,0$	$\|-45°\rangle$	$+$	$\hat{M}_+ \|-45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} + \frac{\|90°\rangle}{\sqrt{2}}$	$\|0°\rangle$ or $\|90°\rangle$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$ or $\hat{M}_+ \|90°\rangle = -\|90°\rangle$	0 1
					$\times$	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ or $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1 0 or 1
		$\times$	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	$\|-45°\rangle$	$+$	$\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
					$\times$	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	0

- Bases of Alice & Bob & Eve Identical → Eve is Not Noticed
- Bases of Alice & Bob Not Identical → Measurement is Discarded Anyway
- 0/1 Bases of Alice & Bob Identical; Bits are Incidentally Identical, Eve is Not Noticed
- 0/1 Bases of Alice & Bob Identical; Bits Incidentally Differ → *Eve is Uncovered*