Appendix 04
Some Important QKD Protocols

1 BB84

The QKD protocol BB84 is named after the initials of its inventors' last names, Charles Bennett and Gilles Brassard, and the year 1984, when the protocol was published. It is the oldest QKD protocol in existence and is likely also the easiest to understand. At the same time, it contains many elements that are also used in other methods.

However, BB84 is also a discrete-variable scheme. This means that the quantum information is transmitted in clearly separated packets with precisely defined values. In QKD protocols, these packets are always single photons, and in many protocols, including BB84, the quantum information is encoded by the orientation of the polarization direction of these photons. However, there are also other types of encoding (phase encoding, time-slot encoding, path encoding, etc.).

1.1 Alice

1.1.1 Alice's Equipment

Alice generates the quantum information and transmits it. To do this, she needs the following devices:

- A **photon source**. This is a device that generates individual photons with a consistently fixed polarization direction and emits them in a fixed direction. Possible device types for such sources are described in the appendix on hardware components.

- A **cryptographically secure random number generator.** This is a device that generates a random sequence of zeros and ones and must meet certain requirements to prevent Eve from guessing these bit sequences. There is also a separate section on this in the appendix.
- An **electro-optic modulator.** This is a crystal that can rotate the plane of polarization of polarized photons. The exact angle of rotation is set by an electrical voltage applied to the crystal. This angle can therefore be adjusted very quickly and very precisely.

1.1.2 Generation of photons

Every photon generated by the photon source initially has the same polarization direction. Without limiting the generality of the discussion, we assume here that the polarization direction is vertical (direction of oscillation ↕). We define this as corresponding to a polarization angle of 0° (see Fig. 1)

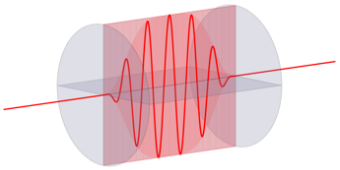
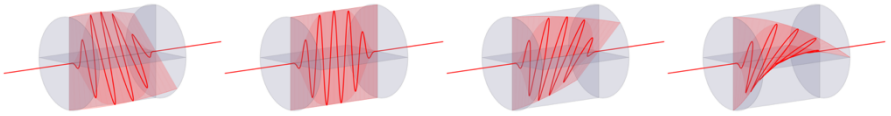


Figure 1: A photon that was generated a short time ago by a single-photon source and is moving along the red line from the front left to the back right. The plane of oscillation is oriented vertically, which corresponds to a polarization angle of 0°.

1.1.3 Encoding the photons

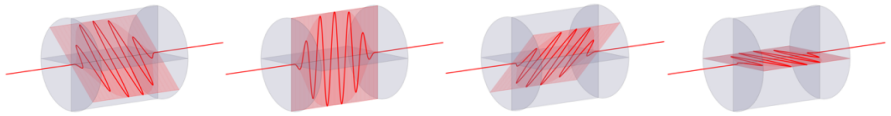
After the photons have left this source, they pass through the electro-optic modulator. This is set to an individual rotation angle for each photon. To control the modulator, Alice uses two bits supplied by the random number generator. One of the two bits is referred to as the "basis," the other as the "value." Together, the basis and value encode the electrical voltage applied to the electro-optical modulator and, consequently, the polarization plane of the photon leaving the modulator.

Figure 2 shows how the polarization plane is rotated in the electro-optical modulator; Figure 3 shows the polarization plane with which the photon continues its path after leaving the modulator. All figures are based on the photon moving from the front left to the back right (i.e., away from the viewer and simultaneously from left to right).



$0° \to -45°$ $0° \to 0°$ $0° \to 45°$ $0° \to 90°$

Figure 2: The electro-optic modulator is a transparent crystal with special optical properties. Depending on the magnitude and polarity of the electrical voltage applied to it, it rotates the plane of polarization of the photons passing through it.



$-45°$	$0°$	$45°$	$90°$
Base bit: 0	Base bit: 1	Base bit: 0	Base bit: 1
Value bit: 0	Value bit: 0	Value bit: 1	Value bit: 1

Figure 3: This is what the polarization planes of four different photons look like after they have left the electro-optic modulator.

The following table provides an overview of how the two bits influence the polarization direction:

Bit 1 "Base"	Bit 2 "Value"	Polarization direction	Symbol for the basis
0	0	⤡ $-45°$	×
	1	⤢ $+45°$	
1	0	↕ $0°$	+
	1	↔ $+90°$	

The symbol for the basis represents the two directions of oscillation possible in the respective basis: In basis 0, the photon oscillates in two mutually orthogonal directions ⤡ and ⤢. Basis 0 is therefore represented by the symbol × . Similarly, the photon oscillates either in the direction ↕ or ↔ when the basis is 1. Therefore, basis 1 is represented by the symbol + .

Alice thus endows each photon she generates with 2 bits of information by rotating the polarization direction. These bits (and thus the polarization directions of successive photons) are purely random. Alice sends the photons prepared in this way to Bob. Figure 4 summarizes the processes at Alice's end.

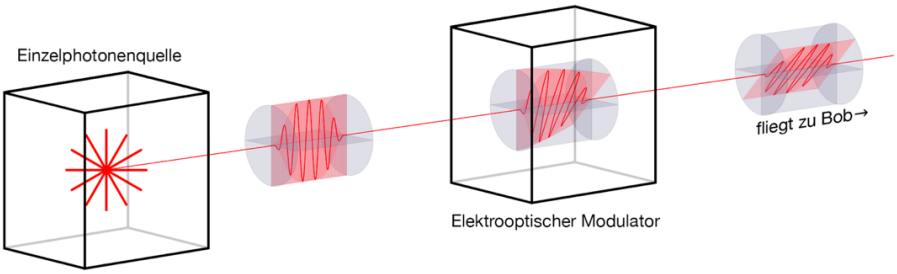


Figure 4: Alice generates a photon, randomly assigns one of four possible polarization states to it, and sends it to Bob.

1.2 Bob

1.2.1 Bob's Equipment

Bob has the following equipment:

- A cryptographically secure **random number generator**, as described for Alice.
- An **electro-optical modulator**. This device is also identical to Alice's modulator.
- A **polarizing beam splitter** (also called a "polarizing cube"). This is a transparent crystal cube. It is positioned so that photons strike one of its sides at a right angle and enter the crystal. Inside the crystal is a separating layer that is tilted at a 45° angle relative to the incoming light beam. Vertically polarized photons (↕) are not deflected by this separating layer. Horizontally polarized photons (↔) are reflected at the separating layer and exit the beam splitter at a right angle to their original direction of travel. (The behavior of photons with other polarizations is described below.)
- Two **single-photon detectors** placed at the two outputs of the polarizing cube. There is a separate section on these devices in the appendix.

Bob receives the photons emitted by Alice. The photons first pass through Bob's electro-optic modulator and then through the polarizing cube. Subsequently, each photon ends up in one of the two detectors (see Figure 5).

To perform a measurement, Bob must first choose one of the two possible bases (× or +). Since he does not know which basis Alice used, the best strategy is to randomly select one of the two bases. With any other strategy, there is a risk that the eavesdropper Eve knows Bob's strategy and measures in the same way as Bob.

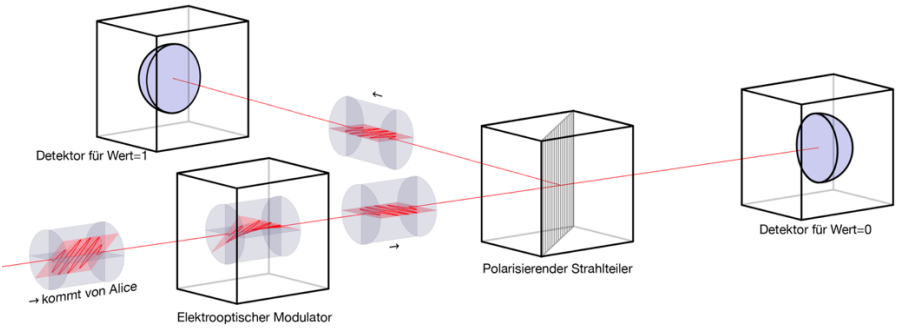


Figure 5: Trajectory of a photon through Bob's apparatus

If Bob's random number generator outputs base bit 0, Bob sets his modulator to rotate the polarization plane of the incoming photons by +45°. In this case, he adds an angle of +45° to the angle that Alice has given the photons. If Bob's random number generator outputs the base bit 1, he instructs the modulator not to change the polarization plane.

After this preprocessing, the photons strike the polarizing cube. 100% of all photons entering the polarizing cube with the polarization direction ↕ (0°) pass straight through and are detected by the photon detector mounted directly behind the polarizing cube. If this detector emits a signal, it means that the value bit was 0. Not a single one of these vertically (↕) polarized photons reaches the other detector.

All photons entering the polarizing cube in the ↔ (90°) direction are reflected at the interface within the cube and, without exception, exit the cube at a right angle to their original direction of travel. They are detected by the side detector, which is responsible for reporting the value 1. Not a single one of these horizontally (↔) polarized photons reaches the detector behind the polarizing cube.

What is interesting now is the behavior of those photons that strike the polar cube in the polarization planes ↘ (-45° or +135°) and ↗ (+45°). For these photons, chance determines their fate. In both cases, exactly 50% of the incoming photons travel straight ahead, thus triggering the rear detector, which reports a value of 0. The other 50% are deflected at a right angle and detected by the side detector, which Bob records as a value of 1.

Something else happens to these photons: those that travel straight ahead are always vertically polarized behind the polarizing cube. Those that are reflected to the side— —are always horizontally polarized after the polarizing cube. This is the reason for the adjective "polarizing" in the name "polarizing beam splitter." Such polarizing cubes impose the fixed polarization plane ↕ (0°) on all photons traveling straight ahead, and the fixed polarization plane ↔ (90°) on all reflected photons. The polarization plane the photons had previously possessed only determines the probability with which the photons take which path. The photons that have already

passed through the polarizing cube thus no longer carry any information about the original basis. While this doesn't bother Bob, it drastically limits the possibilities for the eavesdropper Eve.

From a practical standpoint, the registration of a photon in a detector is what constitutes a measurement, but from a quantum physics perspective, the measurement already takes place in the polarizing cube, precisely at the point where the photon's two potential paths diverge. The fact that not only the direction of flight but also the orientation of the polarization plane changes is, of course, due in this specific case to the specific properties of the oblique interface in the polarizing beam splitter. However, due to very fundamental physical laws, it is impossible to build a device that can measure the orientation of the polarization plane without simultaneously realigning that polarization plane. Although there are beam splitters that do not alter the polarization direction, they do not direct the photons based on the polarization direction but instead select the subsequent path completely at random. Which of the two detectors then clicks is entirely independent of the polarization direction.

1.3 Summary

The following table summarizes what can happen:

Alice				**Bob**				
Direction generated by the source	Choice for base	Choice for value	Direction during transmission	Selection for the base	Effect of modulator	Direction in front of the pole cube	Likely straight ahead	Likely sideways
↕	0	0	↘	0	+45°	↕	100%	0%
↕	0	0	↘	1	± 0°	↘	50%	50%
↕	0	1	↗	0	+45°	↔	0%	100%
↕	0	1	↗	1	± 0°	↗	50%	50%
↕	1	0	↕	0	+45°	↗	50%	50%
↕	1	0	↕	1	± 0°	↕	100%	0%
↕	1	1	↔	0	+45°	↘	50%	50%
↕	1	1	↔	1	± 0°	↔	0%	100%

1.4 Determining the useful bits for the key

The green-highlighted fields clearly show that Bob's detectors provide a clear and unambiguous result only when Bob has randomly selected the same basis as Alice. If Bob made a mistake in choosing the basis, the measurement results from the two detectors are purely random and therefore completely useless.

In those cases where Bob has guessed correctly, his result correlates exactly with the value bits that Alice has randomly set. If Alice has set the value bit to 0, the photon always flies straight through Bob's polar cube (provided he has guessed the basis correctly). If Alice has set the value to 1 (and if Bob has guessed correctly), then the photon reliably always lands in the side detector.

However, at the time of measurement, neither Bob nor Alice nor anyone else knows for which photons Bob guessed the basis correctly. Bob therefore needs information from Alice about which basis she chose for which bit. Consequently, Alice must transmit the sequence of her basis bits to Bob via a classical communication channel. He then compares the received list with the record of his own basis bits and discards all measurement results where he guessed incorrectly, since these results are useless. He knows that the other results correspond exactly to Alice's value bits. Therefore, he interprets these results accordingly and thus arrives at a useful sequence of bits.

So that Alice can also determine which of her value bits are useful and which are useless, she needs Bob's basis bits. So he sends her his basis bits via a classical communication channel, and Alice proceeds exactly as Bob did. If the basis bits match, the corresponding value bit is useful; otherwise, it is not. The sequence of useful bits that Alice receives and the sequence that Bob received are identical. This is illustrated in the following table, which records the temporal sequence of several photons. (For the polar cube, "↰" stands for "sideways reflected" and "↑" for "straight ahead.")

Alice	Base	0	1	1	0	0	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1	0	1	1	0	0	0	1	0	1	1	0	1
	Value	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	0	1	0	1	0	1	1	0	0	1	1
Bob	Base	1	0	1	0	1	1	1	0	1	1	1	0	1	1	0	0	0	1	0	0	1	0	0	1	0	0	1	0	1	0	1	0
	Cube	↰	↑	↑	↑	↰	↰	↑	↰	↑	↰	↑	↑	↑	↰	↑	↰	↑	↰	↰	↑	↰	↰	↰	↑	↰	↑	↰	↰	↑	↰	↑	↑
	Value	1	0	0	0	1	1	0	1	0	1	0	0	0	1	0	1	0	1	1	0	1	1	1	0	1	0	1	1	0	1	0	0
Same value?		✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗

The columns highlighted in green correspond to those photons for which Bob happened to choose the same basis as Alice. Only for these photons can Alice and Bob be certain that Bob measured the correct value bits. In fact, the values are the same in 16 of the 16 cases shown. (✓)

For all other photons, Bob has received a random result that matches Alice's value only in half of all cases. In the table, the values are indeed the same in 8 of these 16 cases (✓), but not in the other 8 cases (✗).

Since Bob and Alice only send each other the base bits, neither of them can determine from the red columns of the table which of these bits have the correct measured value and which have the incorrect one. Therefore, the values of the photons from these columns are useless to both Alice and Bob. These values are therefore discarded by both.

The bit sequence that Alice and Bob now know, but which no one else can know, is shown in the green cells of the two "Value" rows. It is: 0010110100110110.

Note that the first three rows in this table are three random bit sequences, each of which must be generated by a cryptographically secure random number generator.

The fourth row describes the behavior of the polar cube (polarizing beam splitter). It operates strictly deterministically if Bob has guessed Alice's basis correctly. If Bob is wrong, the polar cube also produces a completely random result.

1.5 Eavesdropping Attack: (Eve)

It is often claimed that the quantum channel is eavesdropping-proof, but that is not a correct statement. The quantum channel can be eavesdropped on. However, in doing so, the eavesdropper, referred to as Eve, inevitably alters the polarization directions of 50% of all photons, which is just as inevitably noticed by Alice and Bob.

We first assume that Eve has no access to internal processing steps at either Alice's or Bob's end. In particular, she cannot determine Alice's value bits at all, and she can only determine the basis bits once Alice transmits them to Bob and Eve eavesdrops on this classical communication—that is, after the quantum communication has ended. Eve also only learns Bob's qubit values by eavesdropping on the classical channel once Bob sends them to Alice—that is, likewise only after the quantum communication has ended. At no point does Eve learn which of Bob's two detectors registered an event for which photon.

Eve could, however, measure individual or all photons from the quantum communication, and, as already mentioned, she can fully read the state bits that Alice and Bob send to each other. But that is of no use to her.

Alice assigns each photon an information content of 2 bits (basis and value) by setting the polarization direction. , however, can only read anything useful from every second photon, and what he can read is then only a single bit. Of the bits that Alice produces with her random number generator, only every fourth one arrives at Bob as a useful bit. The chosen method and the quantum nature of the photons do not allow for a better ratio.

Eve now faces the same problem. The best she can do is the following: She measures the photons she receives from Alice in the same way as Bob. Due to the quantum properties of the photons, Eve cannot determine the basis used by Alice. For each photon, she must try to guess the basis, just as Bob does. That is, she first randomly selects a basis and then measures a value in that basis. She then combines the basis and the value in the same way Alice does when sending, and determines the polarization direction of a photon, which she then forwards to Bob, who is supposed to believe it came from Alice.

The problem is that Eve does not know Alice's basis and therefore replaces it with her own. If Eve happens to have chosen the same basis as Alice, the photon she forwards to Bob is indistinguishable from the one Alice sent. Bob will then also choose this basis in 50% of all cases, and Alice, Eve, and Bob will all assign the same value to this photon. Eve will learn of this success as soon as she eavesdrops on Alice and Bob's basis bits.

However, if Eve makes a mistake in choosing her basis, she will inevitably send a photon with the wrong polarization direction to Bob. If Bob also makes a mistake—that is, uses a different basis than Alice (and thus the same as Eve)—then Bob's measurement will match Eve's. But that doesn't matter, because when Alice and Bob later compare their basis bits, they will find that they are different, and Alice and Bob will discard the corresponding value bit, and Eve must do the same.

What is interesting now is the case where Eve is wrong and Bob simultaneously guesses the basis used by Alice correctly. Then Eve will send a photon in the wrong basis to Bob. However, because Bob uses the other basis, he will receive the value bit 1 in 50% of cases and the value bit 0 in 50% of cases, regardless of the value bit that Alice attached to her photon. When Alice and Bob then compare their basis bits, they will find that they have used the same basis bit, and they will consider their own value bit to be valid and include it in the key.

However, 50% of the value bits that end up in the key this way are different. Alice and Bob can detect this by, after the key exchange, separating an arbitrary sequence from the received bit string as a test sequence and sending these test sequences to each other. The longer this test sequence is, the more likely it is that Alice and Bob will discover different bits within it. If that is the case, Alice and Bob will know that Eve has been eavesdropping and knows large parts of the key. Then Alice and Bob will discard this key and try again later to generate a shared key.

Event	Proba-bility	Consequence
Bob chooses a different basis than Alice. (Eve's choice is irrelevant here)	50%	Alice and Bob discard the bit, so Eve does too (regardless of which basis Eve chooses).
Alice, Bob, and Eve choose the same base.	25%	Bob and Eve correctly measure the value Alice chose. Eve knows her value is correct. Alice and Bob cannot tell from this bit whether Alice was active.
Bob chooses Alice's base, but Eve chooses the other base, thereby interfering with the bit. Nevertheless, Bob receives the correct value by chance.	12.5%	Alice and Bob have the same bit and use it. This bit provides no indication of Eve's activity. Eve realizes she has measured incorrectly and concludes that she knows nothing about Alice and Bob's bits. She cannot trust her own bit.
Bob selects Alice's base, but Eve selects a different base and interferes with the bit. Bob receives the wrong value by chance.	12.5%	Alice and Bob have different bits. They detect such errors when they compare a sufficiently long segment of the key. In this specific case, Eve realizes that she has measured incorrectly and concludes that she knows nothing about Alice and Bob's bits. She cannot trust her own bit.

1.6 Alice and Bob's Strategy

According to the protocol, 50% of all value bits are discarded because Bob guessed the wrong base for these bits. The other value bits end up in Alice and Bob's key sequences. If Eve does nothing, these bits are always identical, but then Eve has no knowledge whatsoever of these key bits.

If Eve eavesdrops, she can determine the value of half of all the bits that make it into the key (that is, 25% of the transmitted bits) without being noticed.

For the other half of the key bits, Eve knows that what she has measured is a meaningless random result. She cannot trust these bits. Her success rate therefore remains at 50%.

Because of Eve's eavesdropping, 25% of the bits Bob collects in his key are incorrect (that is 12.5% of the transmitted bits).

After completing the described protocol, Alice and Bob must therefore still verify the equality of the received value bits, i.e., their two key sequences. The bits they use for this test cannot be used for encryption later.

If Eve is eavesdropping, each bit in Bob's key has a probability of$p(A = B) = \frac{3}{4}$ that it matches the corresponding bit from Alice. If Alice and Bob perform their equality test using only one bit, they will detect Eve's activity with this probability:

$$p(Eve)_1 = 1 - \frac{3}{4} = \frac{1}{4} = 25\%$$

If they use two bits for the test, both must match at the same time to miss Eve. The probability of detecting Eve is then:

$$p(Eve)_2 = 1 - \left(\frac{3}{4}\right)^2 = \frac{7}{16} = 43{,}75\%$$

In general, for$n$ bits that Alice and Bob use for the test:

$$p(Eve)_n = 1 - \left(\frac{3}{4}\right)^n$$

Although this value never reaches exactly 100%, it approaches this value quite rapidly as the number of bits used (n) increases. Even with a test length of 56 bits (7 bytes), it is more likely to hit the jackpot in the Austrian Lotto 6 out of 45 with just one ticket than to miss Eve's eavesdropping. With 72 bits (9 bytes), only about one in a billion eavesdropping attacks is missed.

Number of bits compared	Number of key exchange operations that must be performed so that at least one of them involves an attack by Eve that goes unnoticed.
56 bits = 7 bytes	$9.921.315 = 9{,}921 \cdot 10^6 \approx 10^7$
72 bits = 9 bytes	$989.894.783 = 9{,}899 \cdot 10^8 \approx 10^9$
128 bits = 16 bytes	$9.821.058.226.344.214 = 9{,}821 \cdot 10^{15} \approx 10^{16}$
1024 bits = 128 bytes	$9{,}655 \cdot 10^{127} \approx 10^{128}$
8000 bits = 1000 bytes = 1 KB	$3{,}235 \cdot 10^{999} \approx 10^{1000}$

With just a few dozen bytes, it is already practically impossible to overlook Eve. If a test sequence of only one kilobyte is used, it is already significantly more likely that unnoticed errors in the hardware or software will result in Eve's eavesdropping attacks going unnoticed.

1.7 What if an attacker is more powerful than Eve?

An attacker could manipulate or infiltrate Alice's or Bob's hardware. This gives them new possibilities:

1.7.1 Intercepting Alice's random number generator

If an attacker can eavesdrop on the output of the random number generator, they know exactly how every single photon Alice sends is polarized. They then don't even need to eavesdrop on the quantum channel. They can easily reconstruct this output of the random number generator based on the electrical voltages used to control the electro-optic modulator. The attacker need only tap into the data flow from the random number generator to the modulator within the device and route it externally to via a secret channel. Another possibility: The varying voltages used to control the modulator generate an electric field there (this is how the modulator works). If this field is strong enough to be measurable outside the device, an attacker does not even need to manipulate the device itself. They need only record and analyze the temporal progression of the electric field strength. However, this is considered unrealistic because the fields are very weak and are masked by stronger fields within the device (e.g., from the power supply).

Of course, an attacker must also intercept the base bits that Bob sends to Alice at the end of the key exchange. If he succeeds in doing so, he obtains exactly the same key that Alice and Bob have generated, without Alice or Bob noticing.

1.7.2 Manipulation of Alice's Random Number Generator

It is conceivable that an attacker, either as part of a supply chain attack during the device's manufacture or through subsequent manipulation, could replace the originally intended cryptographically secure random number generator with a deterministic generator that produces an infinitely long, precisely predictable bit sequence—in other words, one that produces no randomness at all. This manipulated random number generator could even continue to produce bit sequences that pass every practically feasible statistical test for randomness, so that Alice cannot detect a malfunction in her device using such tests. (For example, the decimal places of almost all irrational numbers pass all tests for randomness, even though they are strictly deterministic.)

But the moment the attacker intercepts the sequence of base bits that Alice sends to Bob, he knows 50% of the output of the random number generator he has manipulated. Using appropriate mathematical methods, he will then be able to

determine the exact state of the random number generator, which subsequently allows him to reconstruct the sequence of value bits as well. If he also gains possession of the base bits that Bob sends to Alice, he can use them to determine the entire key generated by Alice and Bob without having measured a single photon and without having been noticed by Alice or Bob.

1.7.3 Monitoring the activity of the detectors in Bob's device

The two photon detectors built into Bob's device generate electrical pulses whose sequence corresponds to the sequence of the measured value bits. If an attacker manages to tap these pulses directly from the device or determine them from the outside by measuring changes in field strength, they have Bob's value bit sequence. Together with the two base bit sequences from Alice and Bob, they can determine the entire key without attracting anyone's attention and without ever having measured a single photon.

1.7.4 Eavesdropping on Bob's Random Number Generator

Bob uses his random number generator to produce only a sequence of base bits. It is precisely this sequence that he sends to Alice via an insecure channel at the end of the key exchange, meaning Eve comes into possession of this sequence anyway. At first glance, it therefore seems as though she gains nothing by eavesdropping on something she will find out later anyway.

However, this sequence of basis bits would be of use to her precisely if she learns each bit of the sequence early enough—namely, while the photon is still on its way from Alice to Bob. For if Eve already knows Bob's bit at that point, she can use the same basis when measuring the photon that Bob will also use. She then makes exactly the measurement that Bob would make, and then sends a photon to Bob that is polarized in such a way that Bob receives the same value bit as Eve when he measures it. In this way, Eve and Bob arrive at an exactly identical sequence of value bits. Because Eve and Bob have also used identical basis bits, it never happens that Alice and Bob have the same basis bits but different value bits. In this case, Eve does have to measure photons, but her activity still goes unnoticed.

1.7.5 Manipulation of Bob's random number generator

The manipulation can be carried out in the same way as with Alice. If Bob does not transmit all of his collected base bits to Alice at the end of the photon transmission, as has always been described so far, but instead sends the bits individually or in

small packets to Alice while she is still sending him further photons, Eve can draw conclusions about the state of the random number generator from the transmitted base bits. Alice and Bob choose this approach at least whenever they are exchanging keys over a longer period of time. This is because they will not send photons for many months or years and only then transmit the corresponding basis bits when they dismantle their equipment; rather, they will transmit the photons in short sessions, and only milliseconds or seconds later will they transmit the corresponding basis bits over the public channel, while the photons for the next session are already on their way.

If an attacker has intercepted enough qubits, they can predict the subsequent sequence exactly starting at a certain point. As soon as the attacker can predict Bob's qubits, they can use this to perform their measurements on the photons, as described earlier. Although the attacker must measure photons, they still do not attract attention.

1.8 Photon Number Splitting Attack (PSN Attack)

One possible attack on the BB84 protocol (and also on many other prepare-and-measure protocols) deserves special attention here:

For practical reasons, attenuated lasers are almost always used as photon sources. These devices do not emit photons at fixed time intervals, but rather follow a Poisson distribution. The intervals are roughly as irregular as the time intervals between people walking along a sidewalk. There are sometimes large gaps between two consecutive people, but it also occasionally happens that two people walk right next to each other. For the BB84 protocol, this means that time is divided into small time slots, and that there are time slots containing no photons at all, time slots with exactly one photon, and time slots with multiple photons. Alice then sets a measurement basis and value bit for each time slot that applies to the entire time slot, and is thus prepared for the case that there is indeed a photon in this time slot that adopts these settings and flies to Bob. Bob then determines for each time slot whether there was at least one photon at all, and if that is the case, he measures all photons in that time slot together.

For the protocol to be efficient, it would be best if all time windows contained photons, but then there would also be many time windows containing 2 or more photons, and Eve could then carry out her PSN attack, which consists of these 3 steps:

- Eve must identify which time slots contain two or more photons.
- Eve must spatially separate the photons from this time window. She forwards at least one photon to Bob and directs at least one other photon

into a photon storage device. The photon forwarded to Bob (and left unchanged) ensures that Bob and Alice do not notice Eve's attack.

- Eve stores the diverted photon in a photon memory without measuring it. She waits patiently until Alice and Bob publish their measurement bases at the end of all measurements, and only then does Eve measure the stored photon, because only then does she know in which basis she must measure it.

If Eve does all this, she can reliably read all the bits of the key that were transmitted in multi-photon pulses without being detected. (To increase her relative yield, she could also block all single-photon pulses, but this drives up the overall attenuation, which in turn causes the key to be reduced too much during error correction and privacy amplification, so that Eve gains nothing from it.)

To prevent Eve from stealing photons from multi-photon pulses, it is important to avoid such multi-photon pulses. And that is why the laser intensity is usually set so low that most time slots contain no photons at all. For if, on average, only one in ten time slots contains a photon (if, on average, a pedestrian crosses a line on the sidewalk only once every 10 seconds), then only one in a hundred time slots contains 2 or more photons (it only happens once every 100 seconds that 2 or more pedestrians cross the line in the same second). However, such multi-photon pulses cannot be completely avoided. But with the Docoy states, there is at least one way to set a trap for Eve. (See2)

In any case, this approach by Eve is the assumption in the security model. However, all three steps are difficult to implement in practice:

1.8.1 Step 1: Detecting that a pulse contains two or more photons.

This is not feasible with currently publicly known technologies. There are attempts to solve this problem in the laboratory, but these attempts have not been very successful so far. The equipment required for this is highly susceptible to interference, inefficient, and does not function at the wavelengths used in QKD protocols. For this reason, there are only simulations of PNS attacks, but no real-world demonstrations of feasibility.

However, it cannot be ruled out that intelligence agencies have already developed such devices, or that they will do so soon.

1.8.2 Step 2: Splitting a photon

This is easily accomplished with a standard non-polarizing beam splitter, but it requires that Step 1 works. However, this simple method has a catch: With 2 photons

in the pulse, the desired result—"1 photon to Bob, 1 photon to Eve"—occurs only in 50% of all cases. In 25% of all pulses, both photons end up with Bob (in which case Eve gains nothing because she has nothing to measure), and in the remaining 25%, both photons end up in Eve's memory, meaning that Bob cannot then perform a measurement, and these photons are guaranteed not to contribute to the key. There are approaches to improve this 50% success rate, but splitting a photon is the problem that causes Eve the least trouble.

1.8.3 Step 3: Storing the diverted photon

A lot of money is currently being invested in the development of such quantum storage devices, because they are also needed for optical computers, for example, and there has already been considerable progress in this area. However, according to currently publicly available information, devices of a quality that would be acceptable to Eve are not yet in sight. The devices currently available require cryogenic cooling and can only store individual photons with half-lives ranging from microseconds to milliseconds. Eve, however, must store millions of photons in order to be able to read them out selectively, and nothing of the sort is currently in sight.

But here, too, it cannot be ruled out that someone in a secret lab is already much further along.

2 BB84 with Decoy States

This is an extension of the BB84 protocol that incorporates a method enabling the detection of PNS attacks. To achieve this, so-called decoy states are utilized.

The photon stream emerging from the laser in Alice's device must be significantly attenuated anyway in order to be usable. Typically, the average photon count is around 0.1, meaning that approximately 100 photons are randomly distributed across 1,000 time slots. And this value applies (as an average) to all time slots.

When using decoy states, the following variation is introduced:

One specifies that, for example, 70% of all time slots are to be treated as signal pulses, and the remaining 30% as decoy pulses, and one randomly determines for each pulse which category it should belong to. Then one selects a specific average photon number for the signal pulses (e.g., 0.2) and attenuates the laser light for these pulses by this factor. The decoy pulses differ from the signal pulses only in their average photon number. For these, the laser is attenuated so that, on average, only 0.05 photons are contained per pulse.

The next step in Alice's device is then the electro-optical modulator, which imposes a specific polarization direction on the time window, and the rest is the same as in the "normal" BB84. Bob measures the polarization directions in the time windows without knowing whether these time windows are signal or decoy time windows. He only finds this out after all measurements are complete, because Alice then announces it via the public channel.

The key point here is that Eve, too, cannot know which pulses are signal pulses and which are decoy pulses. In particular, however, the proportion of multi-photon pulses in the signal pulses is different (in the example: higher) than in the decoy pulses. Eve, however, steals only individual photons from these multi-photon pulses, which means nothing other than that she specifically attenuates multi-photon pulses. And in doing so, Eve attenuates the signal pulses differently (in the example: more strongly) than the decoy pulses.

Another important point is Bob's device: The detectors cannot detect all photons. But when 2 (or more) photons are contained in a single pulse, the detectors "click" with a higher probability than with single-photon pulses. Although Bob cannot tell from a detector click whether it has detected 1 photon or 2 photons, by specifically reducing the number of photons in multi-photon pulses, Eve reduces the detector activity in Bob's device. And she does this to a greater extent for the signal pulses than for the decoy pulses.

Alice and Bob know from their agreement what proportion of the time slots are decoy pulses. (In the example: 30%) Therefore, if Eve is present, Bob would also have to make measurements (detector clicks) that belong to decoy pulses in 30% of all cases, because the fiber optic cable attenuates both types of pulses to exactly the same degree. However, if Bob finds that, for example, 35% or 45% of his measurements correspond to decoy pulses, he knows that someone has attenuated the signal pulses significantly more than the decoy pulses, and that can only have been Eve. If Alice and Bob discover such deviations in their statistical analysis, they can therefore assume that Eve has been eavesdropping, and they can respond accordingly.

3 E91 (Entanglement)

Once you understand the BB84 protocol, it quickly becomes clear that the randomness required in the final key material has absolutely nothing to do with the fact that quantum physics was involved in the key derivation process. The specific values of the individual bits in the key come exclusively from random number generators, which are potentially insecure. Yet one of the strengths of quantum physics is precisely the ability to generate true, guaranteed unpredictable randomness, and this actually happens in the BB84 protocol even with Bob's

polarizing beam splitter, if Bob uses a different measurement basis than Alice. In that case, the photon's polarization direction does not match the alignment of the polarizing cube, and the photon randomly selects one of the two possible paths according to quantum physics. However, this guaranteed randomness is not utilized in the BB84 protocol.

In the E91 protocol, published in 1991 by Arthur Eckert, a different approach is taken that ensures the randomness in the final key is guaranteed by quantum physics.

3.1 The Sender

In BB84, there were two parties, Alice and Bob, who wanted to generate a shared key, and Eve, who wanted to eavesdrop on this key. In the E91 protocol, however, there is a third party: the sender. The sender generates the quantum information and sends it to Alice and Bob, who in the E91 protocol act (almost) exactly the same as in the " " and also have exactly the same equipment. It is permissible for Alice (or Bob) to be identical to the sender. This has no impact on the security of the protocol. In practice, however, this is generally avoided because it would reduce the bridgeable distance. It is better for the bridgeable distance if the sender is physically located between Alice and Bob.

It is also permitted for the eavesdropper Eve to be identical to the transmitter. This, too, has no impact on the security of the protocol because the transmitter does not possess any usable information. In the E91 protocol, one does not need to trust the transmitter.

3.2 Entangled photon pairs

There are materials that can occasionally split a single photon entering the material with high energy into two photons, each of which continues on its way in different directions with half the original energy. However, from the perspective of quantum physics, the two photons produced are still a single quantum particle, but one that is simultaneously present at two different locations, each with a 50% probability. And this single particle, which is now traveling in two different directions at the same time, has only a single specific quantum state (e.g., a specific polarization direction) that cannot be individually assigned to either of its two spatially separated manifestations. This is called an entangled quantum state.

However, such an entangled state is not stable. As soon as one of the two manifestations interacts with something else and thereby reveals its quantum state, the connection between the two photons—which have now effectively become

individual—disappears, and each of them has a precisely defined state, with the states of the two photons then being exactly opposite. In the case of polarization, this means that the planes of oscillation are at right angles to each other. (Note: It is also possible that these individual states are exactly the same, which in the case of polarization means that the planes of oscillation are identical. Whether equality or opposition occurs depends on the method used to create the entangled state. This is therefore strictly deterministic and, in the practical implementation of the E91 protocol, always known in advance. For several reasons, which would take too long to list here, one very often chooses a version of entanglement in which the two photons are exactly anticorrelated.)

3.3 Alice and Bob

In the E91 protocol, Alice and Bob are exactly the same (except for one small detail that will be mentioned later). Both are receivers, and they each receive one photon from the same entangled photon pair. The equipment used by both corresponds to what was described for Bob in the BB84 protocol. Although Alice and Bob still need a random number generator, its output is used only to set the measurement basis, i.e., during the selection process. In E91, the bits in the final key do not originate from either of the two random number generators, but are the result of genuine quantum physical randomness.

When Alice measures a photon, she first sets the measurement basis. For this, she needs her random number generator. However, she must now choose between 3 different measurement bases. Two of these correspond to the measurement bases that Bob could already choose from in the BB84 protocol. To set the third basis, a 22.5° rotation must be performed in the electro-optical modulator; this third basis thus lies exactly between the two already known ones. (See Figure 1.)

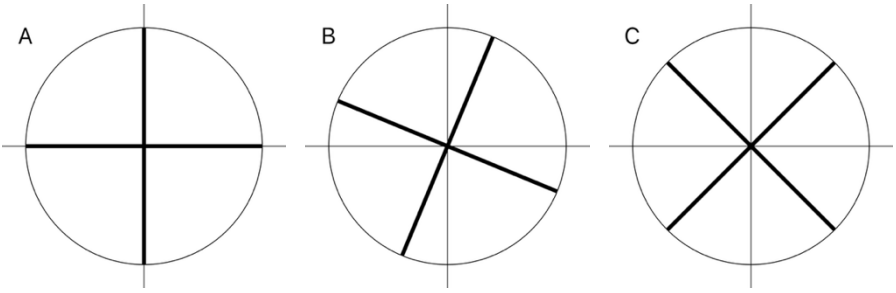


Figure 1: The three measurement bases in the E91 protocol. Base A was called "+ " in the BB84 protocol, base C was called "× " there, and base B is a new addition in the E91 protocol.

After that, the photon enters the polarizing beam splitter, and at precisely this moment, the previously undetermined polarization direction of the Alice entanglement state of the entangled photon is fixed. And there are only two possibilities: Either the photon travels straight through the polarizing cube and is then vertically polarized (↕), or it is reflected to the side and is then horizontally polarized (↔). However, due to entanglement, the quantum state of the Bob-measurement of this entangled photon is also determined at the exact same moment. This state is exactly the opposite of what Alice measures.

So if Bob now chooses the same measurement basis as Alice, he must necessarily measure exactly the opposite of what Alice has just measured. Bob thus inverts his measured bit (this is the only difference between Alice and Bob), and both arrive at identical value bits if they happen to use the same measurement basis. The difference from BB84, however, is that in BB84, Alice (more precisely: her random number generator) determined the value of this measured bit, whereas in the E91 protocol, no one specifies this in advance. The specific value is only determined at the time of measurement and, if the E91 protocol is carried out correctly, is neither predictable nor influenceable.

If Bob chooses basis A and Alice chooses basis C (or vice versa), then although one of them again determines the oscillation direction of the partner's photon through their own measurement, the partner measures this oscillation direction in a basis that is rotated exactly 45° relative to the other, thereby obtaining a completely random result.

An interesting case arises, however, when one of them chooses basis B and the other chooses one of the other two bases. In this case, both measure identical bit values with a probability of approximately 14.6%, but opposite values with a probability of 85.4%. (The value 14.6% is the result of the square of the sine of the angle:$\sin(22{,}5°)^2 = 0{,}14646..$.) Since Alice and Bob still do not know exactly what the other has measured in this case, they discard these results as well; that is, these measurement results are not included in the key generation. However, these measurement results are very useful for something else: they can be used to determine whether Eve has been eavesdropping.

3.4 Eve

Eve knows that Alice and Bob always insert a bit into their key whenever they have used identical measurement bases, and in this case, when measuring entangled photons, they always measure exactly opposite polarization directions. So Eve does the following: She takes complete control of the transmission system, but instead of sending entangled photon pairs, she always generates two unentangled photons, to which she applies a polarization direction known to her using a random number

generator; specifically, she always polarizes Bob's photon rotated by 90° compared to the one she sends to Alice. She selects these directions at random and notes them down. The problem, however, is that Alice and Bob's measurements are now independent of each other due to the lack of entanglement.

If Alice and Bob have chosen the same measurement basis, and if Eve has randomly aligned the two photons such that their polarization planes correspond exactly to the two planes of this measurement basis, then Alice and Bob do indeed measure opposite polarization planes, and after Bob has inverted his bit, Alice and Bob also have the same bit value in this case—one that was, however, predetermined by Eve.

But Eve does not know in advance which measurement bases Alice and Bob will choose, so it can happen that Eve polarizes the photons in the two directions ↕ and ↔, but Alice and Bob both measure in basis C (corresponding to× in BB84), and then, with unentangled photons, each of the four possibilities 00, 01, 10, 11 is equally likely (where the first digit is the bit measured by Alice and the other by Bob). Something similar, though somewhat less pronounced, happens if Eve specifies a different angle. When Alice and Bob later compare their keys, they will therefore find a very high error rate.

3.5 Bell test

But something else happens as well: The probabilities that Alice and Bob will measure the same or opposite bit values are altered by Eve's activity not only when Alice and Bob choose the same basis, but they also change in all other possible basis combinations. When Alice and Bob perform a key exchange, these probabilities (i.e., predictions about the future) become relative frequencies (i.e., statements about reality), and from this, a metric can be calculated that is incorporated into the so-called Bell test. This metric can reach a maximum value of 2.828 (more precisely:$2 \cdot \sqrt{2}$), but it can only be greater than 2.0 if the photons measured by Alice and Bob were entangled. If this metric is less than 2.0, then Alice and Bob were fed unentangled photons, and they abort the key exchange.

3.6 Alternative Strategies by Eve

Another strategy for Eve would be not to manipulate the source at all, but instead to measure the photons from Bob's photon stream. This allows Eve to know the exact polarization of the photons traveling to Alice, and she generates photons that match this exactly, which she sends to Bob. But the result is then exactly the same: the two

photons are not entangled, and Alice and Bob notice this because their measurement results no longer correlate as they would with entangled photons.

Eve could instead entangle two photons she has prepared herself. That is certainly possible, but it does not benefit Eve. For if Eve creates the entanglement in such a way that Alice and Bob do not notice that Eve was involved, then Eve possesses absolutely no information about what Alice and Bob will actually measure. That is precisely the intended state of the E91 protocol: The creator of the entanglement has no information whatsoever about the polarization directions of the individual photons, because these two individual directions are indeterminate. Only the state of the overall system is known: the two directions are at right angles to each other. Exactly how the individual photons oscillate is only determined during the measurement, and is an unpredictable random outcome.

Eve would therefore need a third photon herself, one that is entangled with the other two, in the hope that this third photon will reveal which result Alice and Bob received after they had carried out their measurements. Entanglement involving 3 photons is certainly possible. In that case, there is a system with 3 components, of which only the overall state is physically real, but none of the 3 components has a concrete individual manifestation of this state. The problem here, however, is this: If one measures one of the three particles, one learns only the exact state of the measured particle. The other two remain entangled with each other and no longer have any connection to the first particle measured. If one then measures one of these two remaining particles, one knows the state of the measured particle and the third remaining particle, but neither of these two correlates with the first. If Eve measures first, she learns nothing about the results that Alice and Bob obtain. If Alice measures first, Eve's photon is indeed entangled with Bob's, and Eve thereby learns what Bob will measure or has already measured, but this result is completely independent of Alice's result. Alice and Bob will, with some probability, detect a quantum bit error, and they will determine from the Bell index that their photons were not entangled. (Note: The actual physical conditions are a bit more complex than depicted here, primarily because there are different types of three-particle entanglements that react differently to the measurement of a single particle. But the fact remains that Eve's activity is reliably detected in a three-particle entanglement involving Alice and Bob, and that Eve can learn very little of practical use in the process.)

3.7 Ways to Attack E91

At first glance, everything seems perfect: Eve has no way to measure or manipulate the photons without being detected, and even the source of randomness for the bits in the final key is purely quantum-physical in E91. Nevertheless, this protocol is also vulnerable to attack.

3.7.1 Monitoring the detector activity of one side

This works the same way as in the BB84 protocol. In the E91 protocol, it is sufficient for the attacker to eavesdrop on the detector activity at just one of the two receivers. He records these measurement results, and when Alice and Bob share their measurement bases with each other, he discards all results from unequal bases. The results that one party has obtained when the bases are the same match exactly with the results of the other party, and what the other party has measured in all other cases does not enter the key and is therefore irrelevant to the attacker.

3.7.2 Manipulation of both random number generators

Let us assume that an attacker succeeds in replacing the cryptographically secure random number generator originally intended for use in both Alice's and Bob's devices with a strictly deterministic pseudorandom number generator that outputs the decimal places of the circular numberπ or the square root of a non-square natural number ($\sqrt{2}$,$\sqrt{3}$,$\sqrt{5}$, ...). Without knowledge of the underlying irrational number, the output of such a pseudorandom number generator cannot be distinguished from the output of a cryptographically secure random number generator. If the hardware swap went unnoticed, no one would be able to detect later that the bit sequences have been manipulated. But the attacker, of course, knows the respective irrational number and thus knows the complete infinitely long bit sequence that the pseudorandom number generator will generate in advance.

When Alice and Bob perform a key exchange, they subsequently share the measurement bases via the public channel. However, these are precisely the bits that the pseudorandom number generator has produced. If the attacker has obtained a sufficiently long bit sequence by eavesdropping on the public channel, they know exactly which decimal place of the irrational number the pseudorandom number generator is currently at, and they therefore know which bits are next in line. From this point on, the attacker knows exactly when Alice and Bob will set which measurement bases.

The attacker now prepares an individual photon stream for Alice, and another that matches Bob's individual random sequence exactly. In doing so, the attacker always uses exactly the same measurement basis in which the respective recipient will measure the photons. And in this measurement basis, he selects a value bit of his choice. Because both Alice and Bob are now guaranteed to always measure in exactly the measurement basis in which the photon is actually oscillating, the photon always arrives at the polarizing cube either exactly vertically or exactly horizontally polarized, and is reflected or transmitted there in a precisely predictable manner. It never happens that the photon strikes the polarizing cube at an oblique angle and is then deflected in one of the two directions by quantum mechanical chance.

The attacker thus has full control over what Alice and Bob will measure, and he can supply them with exact bit sequences that both will then interpret as perfectly entangled photon pairs, and in this way he can dictate any bit sequence for their shared key, without Alice and Bob becoming suspicious.

3.7.3 Intercepting the Random Number Generators

If the attacker cannot manipulate the random number generators but manages to intercept the electrical signal with which the random number generator in the receiver controls the electro-optical manipulator—and if he succeeds in doing so for both devices—then he can proceed exactly as if he had manipulated the random number generators. He simply has less time to prepare the photons he generates accordingly.