II. Bennett-Brassard Protocol

The first comprehensive protocol for a method of quantum key distribution, now commonly referred to as the BB84 protocol, was introduced by Charles Bennett and Gilles Brassard in 1984 at a conference of computer scientists in Bangalore, India. The protocol relies on bits of information encoded in the polarizations of individual photons that travel along an optical fiber, then employing a parallel classical channel and the limited sharing of secret information to establish a secure quantum key based on the transmission of these photons.

At the start of the process, Alice and Bob establish two parallel channels – one quantum channel by which Alice will transmit polarized photons to Bob, and a classical channel through which Bob will communicate certain parts of his received message back to Alice for confirmation. In modern practice, these two channels take the form of a secure fiber-optic cable and an Internet-based public communication platform. Alice must also set up a device for separating individual photons from a polarized light source, and Bob must attach a single-photon detector to his end of the quantum channel.

Once the channel is established, Alice generates two random strings of bits, one which will serve as the source of the secret key, and the other to determine which bases of polarization she will use for each transmitted photon (either rectilinear or diagonal). For example, if Alice generated the following series of random bits and bases,

0 1 1 0 1 0 0 0 1

D R D D R D R R R

then she would prepare a series of photons polarized in the following states: $|1_D\rangle$, $|2_R\rangle$, $|2_D\rangle$, $|1_D\rangle$, $|2_R\rangle$, $|1_D\rangle$, $|1_R\rangle$, $|2_R\rangle$. In other words, Alice would select photons from her light source which are polarized at 45°, 90°, 135°, 45°, 90°, 45°, 0°, 0°, and 90°, respectively, and then transmit these to Bob one at a time. In later updates to the protocol, including experimental reports, Bennett and Brassard used the photon's circular basis instead of its diagonal basis. Because all three options – rectilinear, diagonal, and circular – are conjugates of each other, it does not matter which two are used.

As Bob receives these photons, he also generates a series of random bases which he will then use to measure each photon in order. If he selects a measuring basis that matches the photon's original polarization basis, then Bob will be able to determine the bit encoded in that particle. However, for each basis he selects which does not match that of the particle's polarization, his observation will cause that photon to randomly align itself in the new measuring basis, effectively destroying the information it carries. At this point, Bob has no way of determining which of his measurements successfully recorded one of Alice's bits.

If Bob received the above photon transmission from Alice, and then selected the following random measurement bases:

R D D D R R D R D

his measurement would result in the following series of bits:

x x 1 0 1 x x 0 x

where “x” stands for a random measurement result. One possible bit string he received could be:

0 1 1 0 1 1 1 0 0

Because Bob has a 50% chance of correctly guessing Alice's polarization basis for any given photon, it stands that, on average, 50% of his received bits will match those originally encoded by Alice.

In the next step of the protocol, Bob uses the public classical channel to disclose certain pieces of information that will determine the accuracy and security of his received message. First, carrying the assumption that Alice transmitted her photons at regularly timed intervals, Bob communicates which photons he in fact received. This will account for data points that are missing for Bob due to experimental error, such as any photons that Bob's detector failed to register. Along with this information, Bob shares the series of bases that he chose to measure Alice's transmission, and Alice checks these agaisnt her randomly selected polarization bases. Based on Alice's response, Bob will then know which of his bits match Alice's and which were the result of a photon randomly realigning itself.

Bob reports the following series of measurement bases:	R D D D R R D R D
(in this case we assume he measured every photon)	
Alice checks against her original basis selections:	D R D D R D R R R
Alice reports back which bases were correct:	- - ✔ ✔ ✔ - - ✔ -
Resulting shared information:	- - 1 0 1 - - 0 -

Bob will then select a random subset of this shared information, the *quantum transmission*, to compare with Alice over the public channel. Bennett and Brassard recommend in their original protocol a subset of one-third. If the above transmission were, say, part of this longer string:

- - 1 0 1 - - 0 - - 1 0 - 0 - 1 - 1 - - - - 1 - 0 - 0 0 1 0 1 - 1 0 - - 1 - 0 - - 1

Bob might share the following bits with Alice to confirm their accuracy:

- - 1 - - - - 0 - - - - - 0 - - - - - - - - 1 - - - - 0 - - - - - 1 - - - - - 0 - - -

If Alice confirms these, then the bits are removed from the shared code, having been sacrificed to public knowledge, and the remaining shared bits become Alice and Bob's secret key: 0 1 1 0 1 1 0 0 1 0 1 0 1 1. They will then use this key as a one-time pad to send an encrypted message between the parties.

The process is then repeated from the beginning for every further message Alice sends to Bob.

If the shared subset of bits reveals inconsistencies, Alice and Bob then know that their quantum channel is subject to either significant technological deficiencies, or else the presence of a third-party eavesdropper (Eve). If Eve has infiltrated the quantum channel and is measuring each of Alice's photons as they pass through the cable (known as an *intercept/resend attack*), she will generate series of bits equivalent to what Bob would have otherwise received, with an average accuracy of 50%. However, for each incorrect basis that Eve chose to measure a qubit, the corresponding photon will arrive at Bob's detector in a random polarization state. If Bob then chooses the correct polarization basis to measure this photon (relative to Alice's chosen basis), and also selects this bit to share with

Alice for confirmation, there will be a 50% chance that the bit does not match Alice's data, thus alerting the two parties to a security breach. The multiple probabilities against Bob's successful detection of Eve stack: a 50% chance that Eve alters a photon by choosing the wrong measuring basis, times a 50% chance that Bob measures this photon with the same basis as Alice, and therefore will not discard it, equalling a 25% chance overall that Eve has altered bits in the quantum transmission. If we assume that the errors which Eve has introduced are spaced out over certain average intervals, then we can also assume that the subset of bits which Bob confirms with Alice over the public channel will likely contain one of these errors. Therefore there is also a 25% chance per photon that Alice and Bob will detect Eve. It becomes imperative for Alice to send enough photons in her original transmission that the number of inconsistencies in the shared key due to interception becomes significant.

In a 1991 update to their protocol, Bennet and Brassard decribed further methods for measuring Eve's influence on the quantum transmission, correcting errors, and then reducing Eve's likelihood of intercepting useful information. These methods, called *error rate analysis*, *information reconciliation*, and *privacy amplification*, rely on non-quantum cryptanalytic and mathematical computer functions such as parity checks and hash functions that take place over the classical channel. The details are beyond the scope of this paper, but can be referenced in the original publication (Bennett, Bessette, Brassard, Salvail, and Smolin 1991).

Following is an example of a possible outcome for eavesdropping on Alice's transmission:

Alice's string of random bits	0 1 1 0 1 0 0 0 1
Alice's random bases	D R D D R D R R R
Eve selects a measuring basis:	R R R R R R R R R
Eve's stolen information (~50% accuracy):	x 1 x x 1 x 0 0 1
all photons are now polarized in a rectilinear basis	
Bob selects the following measuring bases:	R D D D R R D R D

Bob's measurements:		x	x	x	x	1	x	x	x	x
	=	0	1	0	1	1	1	1	0	0

Eve's tampering has caused high inaccuracy within Bob's data

Bob communicates his chosen bases with Alice, who confirms:	-	-	✔	✔	✔	-	-	✔	-
Bob assumes the following information is shared:	-	-	0	1	1	-	-	0	-
Bob communicates a random subset of the key with Alice:			0		1				
Alice alerts Bob to an inconsistency:			✘		✔				

When Alice and Bob report a mismatch for the value of the third qubit in their shared information, they will abort their communications and begin the process again, assuming their privacy has been compromised. In future revisions of BB84, quantum key distribution would still be successful in spite of Eve, using techniques to amplify privacy and reduce Eve's ability to manipulate the transmission.