4

Quantum Key Distribution

Quantum key distribution protocols are introduced here as the first application of qubits to quantum information processing. Completely secure encryption key can be shared by two parties (Alice and Bob) by making use of quantum resources. This key is used for classical encryption afterward.

4.1 One-Time Pad

A classical encryption system to send a string of n characters $p_1 p_2 \dots p_n$ made of English alphabets is to use an encryption key $k_1 k_2 \dots k_n$, $(0 \le k_j \le 25)$ of the same length, which shifts each character p_j by k_j mod 26. Suppose Alice sends an encrypted message HAL to Bob, which is eavestropped by Eve. Eve tries many different keys to decode the message but she will get many meaningful results. If she tries a key 111, she will get IBM,* while if she tries 588, she will get MIT. This encryption system is totally secure if the key is used only once. If the same key is used more than once, Eve can guess the key by examining candidate decrypted messages. † This is the reason why this cryptosystem is called the "**one-time pad**".

In the following, we use the binary system to make the story simplified and also make it relevant for our purpose. Alice wants to send a message in a form of a bit-string of length n (**plaintext**) to Bob through a public channel. To prevent from being eavesdropped, she encrypts the plaintext with a key, which is another bit-string of the same length, and is supposed to be shared only by Alice and Bob. Let Alice's message be $a_1 a_2 \dots a_n$ $(a_j \in \{0, 1\})$ and the key be $k_1 k_2 \dots k_n$ $(k_j \in \{0, 1\})$. She adds k_j to each a_j bitwise mod 2, which we denote by $a_j \oplus k_j$, namely

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1,\ 1 \oplus 1 = 0.$$

*This is a joke from a movie "2001 A Space Odyssey".

†She can use the fact that "E" appears most frequently in an English plaintext, followed by "A", "T", and "I". Some combinations of alphabets, such as "TH", "EH" and "THE", also appear with high frequencies.

Now an encrypted bit-string of length n (**ciphertext**) has been produced and is sent to Bob through a public channel with possible Eve's eavesdropping. Bob adds the same key bitwise to the ciphertext to recover the plaintext. Alice adds k_j to a_j mod 2 to obtain $c_j = a_j \oplus k_j$ and Bob adds k_j mod 2 to c_j to recover $c_j \oplus k_j = a_j \oplus k_j \oplus k_j = a_j$. Note that $k_j \oplus k_j = 0$ for any k_j. This one-time pad scheme is secure as far as the key is shared only between Alice and Bob and the key is used once and only once.

We can formally define the encryption map E by

$$E : (a, k) \mapsto c = a \oplus k \tag{4.1}$$

and decryption map D as

$$D : (c, k) \mapsto a = c \oplus k. \tag{4.2}$$

Observe that $D(E(a, k)) = D(a \oplus k) = a \oplus k \oplus k = a$.

EXAMPLE 4.1.1. *Let Alice's plaintext be* $a = 1001011011001101$ *and the key be* $k = 1101011101010010$*. Then the ciphertext* c *is* $c = a \oplus k = 0100000110011111$*. Bob adds the same key to the ciphertext as* $c \oplus k = a$ *to recover the plaintext* a*.*

It is possible to share the encryption key between Alice and Bob by using qubits so that Eve's attack can be detected with high precision. Such a scheme is called a **quantum key distribution**, or **QKD** for short. There are several QKD schemes, all of which make use of the fact that Eve's eavesdropping is a measurement of qubits and the qubit state is altered by this action.

QKD is the first practical application of quantum information in this book. QKD devices are manufactured by several companies worldwide and already commercially available [1, 2, 3, 4].

4.2 BB84

The first example of QKD has been proposed by Bennett and Brassard in 1984 and hence this protocol is called **BB84** [5]. The sender Alice and the receiver Bob can detect a possible third party Eve eavesdropping their communications by comparing the sequence of qubits sent and received.

Figure 4.1 shows the BB84 setting, in which Alice sends a qubit-string to Bob through a *unidirectional* quantum channel Q while they can communicate through a *bidirectional* classical channel C, where both Q and C channels may be eavesdropped by Eve.

To make our discussion concrete, suppose they employ polarized photons as qubits. Let us define four polarized photon states $|e_0\rangle = |\leftrightarrow\rangle, |e_1\rangle = |\updownarrow$

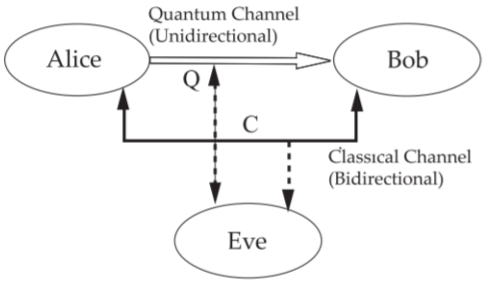

FIGURE 4.1
Quantum key distribution protocol BB84. Q is a unidirectional quantum channel while C is a bidirectional classical channel. Eve might intercepts both channels.

$\rangle, |f_0\rangle = |\swarrow\!\!\!\!\!\nearrow\rangle, |f_1\rangle = |\nwarrow\!\!\!\!\!\searrow\rangle$, where $|f_0\rangle = (|e_0\rangle + |e_1\rangle)/\sqrt{2}, |f_1\rangle = (|e_0\rangle - |e_1\rangle)/\sqrt{2}$. In optics, they are also knows as $|e_0\rangle = |\mathrm{H}\rangle, |e_1\rangle = |\mathrm{V}\rangle, |f_0\rangle = |\mathrm{D}\rangle$, and $|f_1\rangle = |\mathrm{X}\rangle$. Alice encodes 0 and 1 with respect to two bases $B_1 = \{|e_0\rangle, |e_1\rangle\}$ and $B_2 = \{|f_0\rangle, |f_1\rangle\}$ as

$$\begin{array}{lll} \text{Basis } B_1 & 0 \mapsto |e_0\rangle, & 1 \mapsto |e_1\rangle, \\ \text{Basis } B_2 & 0 \mapsto |f_0\rangle, & 1 \mapsto |f_1\rangle. \end{array}$$

Step 1 Alice randomly chooses one of the four polarizations $\{|e_0\rangle, |e_1\rangle, |f_0\rangle, |f_1\rangle\}$ for each photon and sends a photon sequence $|f_1\rangle, |e_0\rangle, |f_0\rangle, \ldots$, for example, to Bob. Bob also chooses a basis B_1 or B_2 randomly and independently of Alice, to measure the polarization of each photon he receives. $4N$ photons must be sent from Alice to Bob to generate a key of bit-length N as will be shown below.

Step 2 After all photons have been sent, Alice and Bob exchange the sequence of the bases B_1/B_2 they employed using the classical communication channel (so Eve might intercept their communication), without disclosing the bits (0/1) Alice sent and Bob received. They will know, as a result, for which photons they employed the same basis. They discard all the cases where they employed different bases since the sent bits and the received bits agree only with probability 1/2 in these cases. For example, suppose Alice sent a photon $|e_0\rangle$ and Bob measures it with B_2 basis. Since the photon he receives is $|e_0\rangle = \frac{1}{\sqrt{2}}(|f_0\rangle + |f_1\rangle)$, his measurement outcome is f_0 or f_1 both with probability 1/2. There are $\sim 2N$ cases that are discarded.

Step 3 Now $\sim 2N$ photons, on average, are correctly transmitted and they share a bit-string of length $\sim 2N$ in their hands. To make sure that no one eavesdrops their quantum channel, they sacrifice N cases chosen randomly from the $2N$ cases with matched bases and exchange N bits (0/1) associated with these N cases over the classical channel. If there are no eavesdroppers operating, they should have the same bits for all the N cases.

Step 4 After verifying they are free from eavesdroppers, they discard these N cases (since the classical channel to exchange the bit-strings may be eavesdropped) and use the remaining N bits to generate a one-time pad key of bit-length N.

Suppose Eve is in action. After eavesdropping each photon, she immediately sends Bob a photon polarized as her measurement outcome in order to hide her presence. Note that Bob will immediately recognize the presence of Eve from missing photons unless Eve sends some photons to Bob. Eve's basis is different from Alice's with probability 1/2, and she sends Bob the results of her measurement with the same basis as she employed for measurement. Then there exist cases in which the bit (0/1) Alice sends disagrees with the one Bob receives even when they employed the same basis B_1/B_2. This happens with probability 1/4 as is shown now. Suppose both Alice and Bob employed the basis B_1, for example, and Alice sent Bob 0 as $|e_0\rangle$. Eve will use the basis B_1 with probability 1/2, in which case Eve definitely measures e_0 and sends Bob $|e_0\rangle$. Bob, also employing the basis B_1, will measure e_0 with probability 1. If, in contrast, Eve employs basis B_2, which happens with probability 1/2, then Eve measures f_0 or f_1 with probability 1/2 for each photon and sends Bob her result with basis B_2. Then Bob, with basis B_1, will obtain e_0 or e_1 both with probability 1/2. Eventually, Bob obtains 0 (e_0) with probability 3/4 and 1 (e_1) with probability 1/4, even though Alice and Bob employ the same basis. This argument remains true if both Alice and Bob use basis B_2. Suppose $4N$ photons are sent from Alice to Bob. They find their bases agree in $\sim 2N$ cases and discard the remaining $\sim 2N$ cases. By comparing bits (0/1) of N cases randomely chosen from the remaining $2N$ bits, they find approximately $N/4$ bits disagree if Eve is in action, from which they detect there is an eavesdropper operating in the quantum channel. They may try different quantum channels until the security is confirmed.

EXAMPLE 4.2.1. *Suppose the sent and received sequences are*

Alice's basis	B_1	B_2	B_1	B_2	B_2	B_1	B_2	B_1	B_2	B_2	B_1	B_1
Alice's bit	*0*	*1*	*0*	*0*	*1*	*1*	*0*	*1*	*0*	*0*	*1*	*0*
Bob's basis	B_1	B_2	B_2	B_1	B_2	B_2	B_1	B_2	B_1	B_2	B_2	B_1
Bob bit	*0*	*1*	*?*	*?*	*1*	*?*	*?*	*?*	*?*	*0*	*?*	*0*

where ? is randomly chosen from $\{0, 1\}$. *Alice and Bob keep the sequence* $0, 1, 1, 0, 0, \ldots$ *and discard the rest. Half of the kept sequence is exchanged to check the security of the channel and the rest is used to generate a key.*

Suppose Eve eavesdrops their communication. Then their readings may, for example, be

Alice's basis	B_1	B_2	B_1	B_2	B_2	B_1	B_2	B_1	B_2	B_2	B_1	B_1
Alice's bit	*0*	*1*	*0*	*0*	*1*	*1*	*0*	*1*	*0*	*0*	*1*	*0*
Eve's basis	B_1	B_2	B_1	B_2	B_1	B_2	B_1	B_2	B_1	B_2	B_1	B_2
Eve's bit	*0*	*1*	*0*	*0*	*?*	*?*	*?*	*?*	*?*	*0*	*1*	*?*
Bob's basis	B_1	B_2	B_2	B_1	B_2	B_2	B_1	B_2	B_1	B_2	B_2	B_1
Bob bit	*0*	*1*	*?*	*?*	$\underline{?}$	*?*	*?*	*?*	*?*	*0*	*?*	$\underline{?}$

The 5th and 12th bits Bob mesaures may not be the correct ones, even though Alice and Bob employed the same basis.

4.3 B92

Bennett proposed a QKD protocol different from BB84 in 1992, which is now called **B92** [6]. BB84 employs four different polarizations for encoding, while B92 employs two. The setting of B92 is essentially the same as that of BB84 depicted in Fig. 4.1 except that the classical channel can be unidirectional from Bob to Alice.

Alice uses two types of photons for encoding as

$$0 \mapsto |e_0\rangle, \quad 1 \mapsto |f_0\rangle.$$

Alice randomly chooses one of $\{|e_0\rangle, |f_0\rangle\}$ for each photon and sends a photon sequence $|f_0\rangle, |e_1\rangle, |f_0\rangle, |e_0\rangle, \ldots$, for example, to Bob. Bob chooses one of measurement bases $B_1 = \{|e_0\rangle, |e_1\rangle\}$ and $B_2 = \{|f_0\rangle, |f_1\rangle\}$ randomly to measure each photon he receives. The following table shows the relation between Alice's photon state and Bob's measurement outcome. The table also shows the probability of each event to happen.

$(\|a\rangle, \|b\rangle)$	$(\|e_0\rangle, \|e_0\rangle)$	$(\|e_0\rangle, \|e_1\rangle)$	$(\|e_0\rangle, \|f_0\rangle)$	$(\|e_0\rangle, \|f_1\rangle)$
Prob.	1/4	0	1/8	1/8

$(\|a\rangle, \|b\rangle)$	$(\|f_0\rangle, \|e_0\rangle)$	$(\|f_0\rangle, \|e_1\rangle)$	$(\|f_0\rangle, \|f_0\rangle)$	$(\|f_0\rangle, \|f_1\rangle)$
Prob.	1/8	1/8	1/4	0

Here $|a\rangle$ is the photon state Alice sends while $|b\rangle$ is the photon state Bob measures. Note that Bob measures $|e_k\rangle$ if the basis B_1 is employed while $|f_k\rangle$ if the basis B_2 is employed. It is important to recognize that (i) if Bob measures e_1, then Alice has *definitely* sent $|f_0\rangle$, while (ii) if he measures f_1, Alice has *definitely* sent $|e_0\rangle$. Bob can say nothing definite for other cases with the measurement outcomes e_0 and f_0.

Step 1 Alice sends $8N$ photons to Bob. We show below that this is the necessary number of photons to generate a key of bit-length N.

Step 2 Bob tells Alice over a public channel when he measured e_0 and f_0. We find from the above table that there are approximately $8N \times 3/4 = 6N$ such cases among $8N$ photons. They discard these cases and keep $2N$ cases, for which Bob measured e_1 or f_1.

Step 3 For these $2N$ cases, Alice assigns 0 to her e_0 and 1 to her f_0, while Bob assigns 0 to his f_1 and 1 to his e_1. By these assignments, they should share the same bit-string of the average length $2N$. Note that Alice does not send any classical information to Bob in this scheme.

Step 4 To check if Eve is in action, they randomly pick up N bits out of the $2N$ bits obtained in Step 3 and Bob sends these bits to Alice over a public channel. They can use the remaining N bits for encryption key if Alice confirms all N bits are the same as hers. Otherwise, they repeat the same process with a different quantum channel until the security is confirmed.

Let us analyze Eve's action in more details. Suppose that Alice has sent the ith state $|a_i\rangle$ and Eve intercepted the transmission with the basis B_1 or B_2. In her measurements, Eve will have probability 1/2 of getting $|a_i\rangle$, a probability 1/4 of getting a state in $\{|e_0\rangle, |f_0\rangle\} \setminus \{|a_i\rangle\}$, and a probability 1/4 of getting a state in $\{|e_1\rangle, |f_1\rangle\}$. If Eve measures $|e_1\rangle$ or $|f_1\rangle$, she knows for sure that $|a_i\rangle = |f_0\rangle$ or $|e_0\rangle$, respectively. Then Eve should send Bob $|c_i\rangle = |f_0\rangle$ or $|e_0\rangle$, respectively. In other cases, Eve should send Bob her measured state, which is the best action she can take.

Let us estimate the fraction of the N bits sent to Alice, which indicates Eve's presence. Recall that these bits corresponds to Bob's measurement outcomes e_1, f_1. There are two cases that are impossible without eavesdropping, namely (Alice, Bob) $= (|e_0\rangle, |e_1\rangle)$ and $(|f_0\rangle, |f_1\rangle)$. The first case takes place if Alice sends $|e_0\rangle$ and Eve measures it with B_2 basis and measure $|f_0\rangle$, which is sent to Bob who measures it with B_1 basis. Note that if Eve measures $|f_1\rangle$, she will send Bob $|e_0\rangle$ and Bob will definitely measure $|e_0\rangle$. The probability Alice chooses $|e_0\rangle$ is 1/2, the probability Eve chooses B_2 and measure f_0 is 1/4, while the probability Bob chooses B_1 and measure e_1 is 1/4, which results in overall probability of 1/32. Obviously the probability of the second case (Alice, Bob) $= (|f_0\rangle, |f_1\rangle)$ is also 1/32. Therefore, if N bits are sent from Bob to Alice, she finds approximately $N/16$ bits do not match with hers.

These cases should be compared with the following experiment. Suppose one places a polarization plate that polarizes an unpolarized light to horizontal direction. The second plate polarizes light vertically. If the second plate is placed after the first, there should be not light passing through them. This corresponds to the case $|e_0\rangle \nrightarrow |e_1\rangle$ and $|f_0\rangle \nrightarrow |f_1\rangle$. If the third polarization plate making angle $\pi/4$ to the horizontal line is inserted between the first

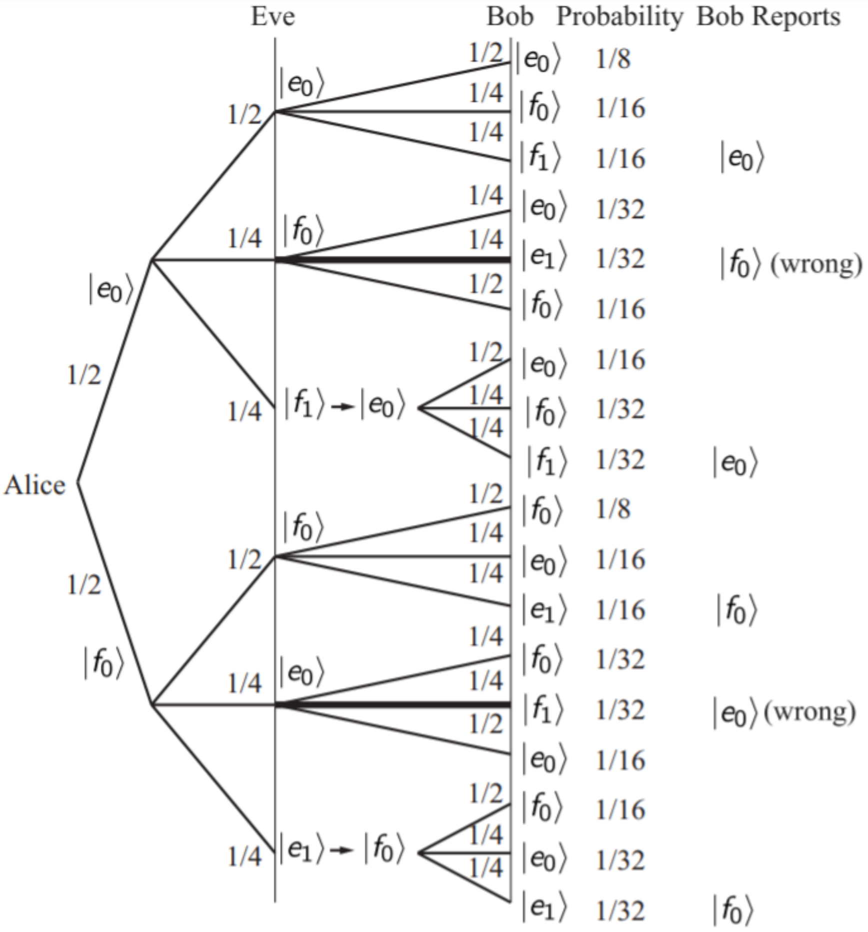

FIGURE 4.2
Probability distribution of Bob's measurement outcomes when Eve is in action. The fractional number attached to each line corresponds to the branching probability while the state shows the projected state after measurement. When Eve measures f_1 (e_1), she replaces it by $|e_0\rangle$ ($|f_0\rangle$), respectively, and send it to Bob. The bold line denotes the case by which Alice can detect an eavesdropper.

and the second plates, then 1/8 of the incoming light propagates through the three plates. Eve's measurement with B_2 basis plays the rôle of the third polarization plate, which opens the channel that leads to forbidden propagation ($|e_0\rangle \to |e_1\rangle$ above and $|\leftrightarrow\rangle \to |\updownarrow\rangle$ here) in both cases.

4.4 E91

BB84 and B92 use a string of single qubits. It is also possible to use entangled pairs for QKD. Here we introduce a protocol, known as **E91**, which was proposed by Ekert in 1991 [6]. Another protocol BBM92, also making use of entanglement, will be introduced in the next section.

E91 is based on the very property of entanglement: It violates the Bell inequality. The third party prepares an entangled state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|e_0\rangle|e_1\rangle - |e_1\rangle|e_0\rangle).$$

Then the first qubit is sent to Alice while the second to Bob. They share an entangled state $|\Psi^-\rangle$ if there are no eavesdroppers acting.

Suppose Eve intercepts a photon sent to Bob. She measures the qubit with an arbitrary basis and sends Bob a photon in the state Eve measured. Suppose Eve used a basis $\{|\epsilon_0\rangle = (\cos(\theta/2), e^{i\phi}\sin(\theta/2))^t, |\epsilon_1\rangle = (-\sin(\theta/2), e^{i\phi}\cos(\theta/2))^2\}$ for her measurement. Since $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|\epsilon_0\rangle|\epsilon_1\rangle - |\epsilon_1\rangle|\epsilon_0\rangle)$ up to unphysical overall phase for any θ and ϕ, the state after the measurement is either $|\epsilon_0\rangle|\epsilon_1\rangle$ or $|\epsilon_1\rangle|\epsilon_0\rangle$. Note that both of them are tensor product state and hence satisfies the Bell inequality. It is impossible to eavesdrop the qubit sent to Bob without disentangling $|\Psi^-\rangle$.

Step 1 A third party (it may be Alice as well) prepares $9N/2$ entangled photon pairs $|\Psi^-\rangle$ and sends the first photons to Alice and the second photons to Bob.

Step 2 Alice and Bob measure photons they possess one by one by choosing one of the following bases independently and randomly;

$$\begin{array}{r}\text{Alice}: \text{vec}a_1, \text{vec}a_2, \text{vec}a_3 \\ \text{Bob}: \text{vec}b_1, \text{vec}b_2, \text{vec}b_2,\end{array} \tag{4.3}$$

where $\text{vec}a_i$ is a unit vector making angle $\alpha_1 = 0, \alpha_2 = \pi/4, \alpha_3 = \pi/2$ from the horizontal axis, while $\text{vec}b_j$ is another unit vector making angle $\beta_1 = \pi/4, \beta_2 = \pi/2, \beta_3 = 3\pi/4$ from the horizontal axis in the xy-plane.

Step 3 Alice and Bob exchange the list of their measurement axes over a classical channel after all photons are measured. They keep the data for which they used the common axis for measurement, namely those corresponding to $(\mathrm{vec}a_2, \mathrm{vec}b_1)$ and $(\mathrm{vec}a_3, \mathrm{vec}b_2)$ out of 9 combinations $\{(\mathrm{vec}a_j, \mathrm{vec}b_k)\}$. There are approximately N such cases, for which Alice's and Bob's measurement outcomes are anti-correlated; if Alice measures e_0, Bob will measure e_1 and *vice versa*. The other 7 combinations are used to detect eavesdroppers.

Step 4 Alice and Bob check the CHSH variant of the Bell's inequality, see below. The photons they keep could be disentangled by possible eavesdropping if the inequality is satisfied, in which case they use other quantum channels until they confirm the security of the channels. Once they confirm the security, they use the n bits corresponding to the common axis measurements to generate a key of length N.

To examine the CHSH inequality, they use the following observables

$$Q = \sigma_z \otimes I_2, R = \sigma_x \otimes I_2, S = -I_2 \otimes \frac{\sigma_z - \sigma_x}{\sqrt{2}}, T = I_2 \otimes \frac{\sigma_z - \sigma_x}{\sqrt{2}}$$

and evaluate the expectation values $E(QS), E(RS), E(RT)$ and $E(QT)$ to check the inequality

$$|E(QS) + E(RS) + E(RT) - E(QT)| \leq 2$$

is satisfied or not. If the state $|\Psi^-\rangle$ is intact, they should have

$$E(QS) = \langle \Psi^- | QS | \Psi^- \rangle = -\frac{1}{2}(0, 1, -1, 0)\left[\sigma_z \otimes \frac{\sigma_z + \sigma_x}{\sqrt{2}}\right](0, 1, -1, 0)^t = \frac{1}{\sqrt{2}}.$$

Similarly they evaluate

$$E(RS) = E(RT) = -E(QT) = \frac{1}{\sqrt{2}},$$

from which they obtain

$$|E(QS) + E(RS) + E(RT) - E(QT)| = 2\sqrt{2} > 2.$$

If, on the other hand, the state they share is $|\Xi\rangle = |e_0\rangle|e_1\rangle$, for example, because of eavesdropping, they have

$$\langle \Xi | QS | \Xi \rangle = -\langle \Xi | QT | \Xi \rangle = \frac{1}{\sqrt{2}}, \quad \langle \Xi | RS | \Xi \rangle = \langle \Xi | RT | \Xi \rangle = 0,$$

from which they find the CHSH inequality is satisfied as

$$|E(QS) + E(RS) + E(RT) - E(QT)| = \sqrt{2} < 2.$$

BB84 and B92 employ a string of single qubit states. There can be a security problem if a single photo source produces multiple photons, which allows for eavesdropping without being recognized by Alice and Bob by stealing a part of photons. It should be also noted that E91 protocol does not require random number generators, which might lower the security of single-photon based QKD. Note that randomness in E91 is built in Nature.

4.5 BBM92

Bennett, Brassard and Mermin proposed a QKD protocol making use of entangled states, which is now known as BBM92 [8]. This protocol is regarded as a natural extension of BB84 to entangled states.

Suppose Alice generates many two-qubit states of the form

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|e_0\rangle|e_0\rangle + |e_1\rangle|e_1\rangle)$$

and keeps the first qubits while the string of the second qubits is sent to Bob. They measure qubits they possess one by one. They should share a common bit-string such as $00101101\ldots$, where e_0 is mapped to 0 while e_1 is mapped to 1. Of course we know this protocol is too naïve. Eve may intercepts qubits sent to Bob and measure them with $B_1 = \{|e_0\rangle, |e_1\rangle\}$ basis and sends the result to Bob. Then Alice, Bob and Eve share the same bit-string and confidentiality will be lost.

To overcome this problem, we employ the same strategy as that of BB84 and B92; we introduce two measurement bases B_1 and $B_2 = \{|f_0\rangle, |f_1\rangle\}$. Let us note that $|\Phi^+\rangle$ is also written as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|f_0\rangle|f_0\rangle + |f_1\rangle|f_1\rangle).$$

If both Alice and Bob employ the measurement basis B_1, they will obtain the identical outcome e_0 or e_1 while if both of them employ the measurement basis B_2, they will obtain identical outcome f_0 or f_1. If they employ different measurement bases, their measurement outcomes are random. For example, if Alice employs B_1 basis while Bob employs B_2 basis and Alice obtains e_0, Bob's outcome will be f_0 or f_1 both with probability $1/2$.

Step 1 To generate a one-time pad key of bit-length N, Alice generates $4N$ pairs $|\Phi^+\rangle$, keeps the first qubits and sends Bob the second qubits.

Step 2 They choose measurement basis independently and randomly, after which they measure $4N$ qubits in their possession.

Step 3 They exchange the measurement bases they employed upon each measurement over a classical channel while keeping the measurement outcomes secret.

Step 4 They discard the $\sim 2N$ cases, for which they employed different measurement bases, while keeping $\sim 2N$ measurement outcomes with the same measurement bases. They assign 0 to e_0 and f_0 and 1 to $|e_1$ and f_1 to generate a one-time pad key of bit-length $\sim 2N$.

The following example with $4N = 8$ illustrates the above protocol.

Alice's basis	B_1	B_2	B_1	B_1	B_2	B_2	B_1	B_2
Alice's outcome	e_0	f_1	e_0	e_1	f_0	f_0	e_1	f_1
Bob's basis	B_2	B_2	B_1	B_2	B_1	B_2	B_1	B_1
Bob's outcome	f_0	f_1	e_0	f_1	e_1	f_0	e_1	e_0
Code generated		1	0			0	1	

Now they share the common key "1001".

To detect eavesdropping, they sacrifice randomly chosen N bits from the bit-string of length $2N$. Suppose Eve intercepts qubits sent to Bob and measures them with randomly chosen basis B_1 or B_2. After Eve's measurement, the qubits are not entangled any more. If she employs B_1 basis, the state after measurement is either $|e_0\rangle|e_0\rangle$ or $|e_1\rangle|e_1\rangle$ while if she employs B_2 basis, the state after the measurement is either $|f_0\rangle|f_0\rangle$ or $|f_1\rangle|f_1\rangle$. Suppose both Alice and Bob used B_1 basis while Eve used B_2 basis for measurement. Suppose Eve measured the photon first. Then the state before Alice's and Bob's measurements is either $|f_0\rangle|f_0\rangle$ or $|f_1\rangle|f_1\rangle$, and hence their measurement outcomes are e_0 or e_1 independently and randomly with equal probability. When Alice and Bob employ the same basis, Eve might employ a different basis with probability 1/2, in which case Alice and Bob will have different bit 0 or 1 with probability 1/2. This means that among N bits broadcast, there are $N/4$ bits on average, where the bits disagree even though they used the same basis. Now Eve's eavesdropping is detected.

The following example with $4N = 8$ illustrates this.

Eve's basis	B_2	B_1	B_2	B_2	B_2	B_1	B_1	B_2
Eve's outcome	f_0	e_0	f_1	f_0	f_1	e_0	e_1	f_1
Alice's basis	B_1	B_2	B_1	B_1	B_2	B_2	B_1	B_2
Alice's outcome	?	?	?	?	f_1	?	e_1	f_1
Bob's basis	B_2	B_2	B_1	B_2	B_1	B_2	B_1	B_1
Bob's outcome	f_0	?	?	f_0	?	?	e_1	?
Code generated		?	?			?	1	

Alice obtains the same outcome with Eve's if and only if they employ the common basis. It is also true for Bob and Eve. Otherwise, the outcome is random as shown with a symbol "?" in the table above. The three parties share the same outcome if and only if all of them employ a common basis. In the table above, there are four cases in which Alice and Bob shared the common basis. However, their outcomes are independently random in three cases out of four.

Above, we assumed Eve makes measurement first among the three. In fact, the order does not matter at all. Either Alice or Bob may measure their qubit first to disentangle the pair. Suppose both Alice and Bob employ the basis B_1 and Eve employs B_2. Alice measures her qubit first to project $|\Phi^+\rangle$ to

$|e_0\rangle|e_0\rangle$, for example. Now Eve intercepts the second qubit and measures it to produce either $|f_0\rangle$ or $|f_1\rangle$. In both cases, Bob will obtain e_0 and e_1 randomly with equal probability upon measurement of his qubit even thought Alice and Bob employ the same measurement basis.

4.6 Note and open problems

In this section, we illustrate how to use the quantum properties on no-cloning theorem, measurements, and entanglement to design secured private quantum key distribution schemes. One may extend these properties to design other efficient and secure quantum key distribution schemes. For example, one may use the idea of setting up a POVM $\{Q_1, \ldots, Q_{m+1}\}$ associated with $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ so that Bob will know for sure that $|\psi_j\rangle$ is sent to him if he gets the measurement of Q_j for $j = 1, \ldots, m$ (see Example 3.4.3). A careful choice of $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ will yield an efficient and secure quantum key distribution scheme.

References

[1] http://www.magiqtech.com/

[2] https://www.toshiba.co.jp/qkd/en/products.htm

[3] https://www.idquantique.com/

[4] https://www.quintessencelabs.com/

[5] C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conf. Comp., Systems and Signal Processing **175** (1984).

[6] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[7] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[8] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).