A Review of Quantum Key Distribution Protocols

Claire Yang

Contents

Abstract

Cryptography is a field of applications that provide secure communication to users in the presence of third parties. It is used to protect information transferred across telecommunications networks, as well as residing in files and databases. Nowadays, the widely used cryptography approaches include public key cryptography and private key cryptography , but both of them face some challenges. Quantum Key Distribution (QKD) addresses these challenges by using quantum properties to exchange secret information. In this paper two popular QKD protocols, BB84 and E91 and their principles are shown.

1 Traditional key distribution approaches

1.1 Public key cryptography

Pubic key cryptography, also called **asymmetric** cryptography, involves two separate keys, one for the sender and the other for the receiver.

The biggest property of public key cryptography is its security relies on **One-way hash function** [2], which means that it should be easy to generate a code given a message, but virtually impossible to generate a message given a code. For example, it is easy to calculate the product of two large prime numbers, but much harder to factor the product to derive the primes. This means that the security of public key distribution is guaranteed by the calculation complexity of certain types of functions, so it can be threatened by the weak random number generators, advances to CPU power, new attack strategies, and the emergence of quantum computers.

1.2 Private key cryptography

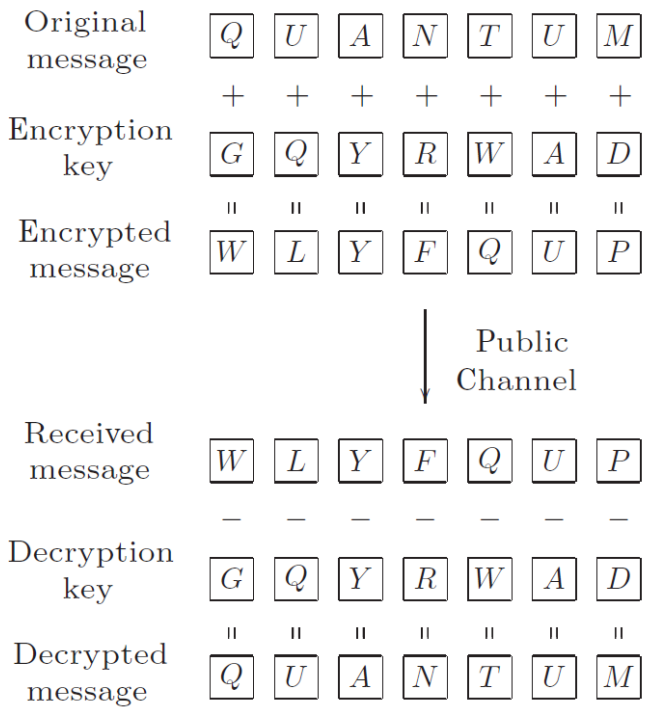

Figure 1: An example for encryption and decryption

Private key cryptography is also called **symmetric** cryptography, which involves one shared secret key for both sender and receiver. Figure 1 is an example for the encryption and decryption of a

message. The sender encrypts the message by adding a random key bits, and the receiver decrypts by subtracting the same key bits.

Private key cryptography also has its drawback. It is relatively difficult to securely distribute the key, because the shared secret key must be delivered beforehand and carefully guarded until use, otherwise it can be copied without disturbing the sender and receiver [1].

2 Quantum key distribution

Quantum key distribution (QKD) are protocols which are provably secure, by which **private key bits** can be created between the sender and the receiver over a public channel and a quantum channel [1] [3]. During the transmission of quantum bits (qubits) from the sender to the receiver, a third party, the eavesdropper, cannot gain any information without disturbing the state of qubits.

2.1 Classification

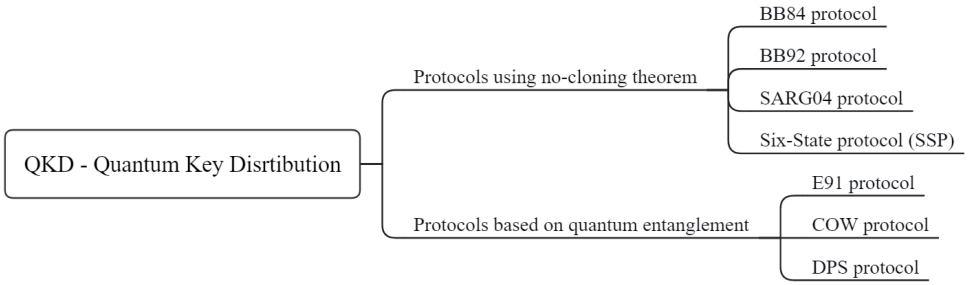

Figure 2: Different types of QKD protocols

As is shown in Figure 2, we can divide QKD protocols into two categories, based on the different principles they use, no-cloning theorem and quantum entanglement.

2.1.1 No-cloning theorem

The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state. When quantum information is transmitted in a channel, it is impossible for a third party to copy and steal information without interfering with the original quantum information. It is the basis for quantum information theory and quantum cryptography.

Here is the mathematical proof of why a qubit cannot be copied:

If a copy procedure exists, we can use a notation U to stand for the copy transformation, thus the copy procedure can be represented by[1]:

$$U|\psi\rangle_A|0\rangle_B = |\psi\rangle_A|\psi\rangle_B \tag{1}$$

where the $|\psi\rangle_A$ is the qubit to be copied, and $|0\rangle_A$ is an empty qubit register initialized with zero.

The copy transform U should work for $|\psi\rangle_A$ with any value, including:

$$\begin{cases} when\ |\psi\rangle_A = |0\rangle_A, U|0\rangle_A|0\rangle_B = |0\rangle_A|0\rangle_B \\ when\ |\psi\rangle_A = |1\rangle_A, U|1\rangle_A|0\rangle_B = |1\rangle_A|1\rangle_B \end{cases} \tag{2}$$

This should also work for the Hadamard basis $|+\rangle_A$ (the Hadamard transform is described detailedly in part 2.2.1):

$$when\ |\psi\rangle_A = |+\rangle_A, U|+\rangle_A|0\rangle_B = |+\rangle_A|+\rangle_B = \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix} \tag{3}$$

[1]Bra–ket notation is a standard notation for describing quantum states, which is also known as Dirac notation. Ket ($|\cdot\rangle$) is typically represented as a column vector. Bra ($\langle\cdot|$) is the conjugate transpose of ket with the same label, which is typically represented as a row vector.

If we use Equation 2 to calculate the left-hand side of Equation 3, we can find out that:

$$U|+\rangle_A|0\rangle_B = U\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)\cdot|0\rangle_B \tag{4}$$

$$= \frac{1}{\sqrt{2}}(U|0\rangle_A|0\rangle_B + U|1\rangle_A|0\rangle_B) \tag{5}$$

$$= \frac{1}{\sqrt{2}}(U|0\rangle_A|0\rangle_B + U|1\rangle_A|1\rangle_B) \tag{6}$$

$$= \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} \tag{7}$$

It is obvious that Equation 3 and Equation 7 have different result, even though their left-hand side is the same. This means that our initial hypothesis, a qubit can be copied, is wrong. Thus, a qubit cannot be copied.

2.1.2 Quantum entanglement

Another principle that QKD can be based on is the principle of quantum entanglement. Quantum entanglement occurs when pairs or groups of qubits stay in special states that the quantum state of each qubit cannot be described independently, but must be described for the system as a whole. This is true regardless of the distance between the entangled qubits.

2.1.3 Another way for classification

There is another way for classifying the QKD protocols, which is to divide them into discrete-variable protocols and continuous-variable protocols [4].

The first approach is discrete-variable protocol, which encodes quantum information in discrete variables and uses single photon detectors to measure the received quantum states. Both BB84 and E91 protocols introduced in Part 2.2 and Part 2.3 are discrete-variable protocols.

The second approach is continuous-variable protocols, which is to encode the quantum information onto the amplitude and phase quadratures of a coherent laser, and then measure it by the receiver using homodyne detectors. Example protocols include Silberhorn (2002) and Grangier (2003). We will not introduce this approach in detail in this article.

2.2 Protocol based on no-cloning theorem: BB84

BB84 protocol is the one of the best-known QKD protocols published by Bennett and Brassard in 1984, which was originally described using photon polarization states to transmit the information [5]. The BB84 protocol has a different way of generating and distributing the key, compared with traditional private key cryptography methods. Before introducing this process in Part 2.2.2, we can first have a look at the two bases, diagonal basis and rectilinear basis, and the Hadamard transform.

2.2.1 The two bases and Hadamard transform

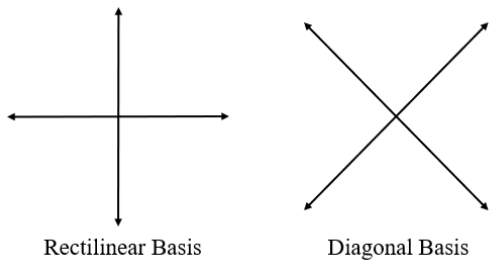

Figure 3: The two bases used in BB84 protocol

basis \ binary 0 or 1	0	1
rectilinear basis (+)	$\uparrow$ (90°)	$\rightarrow$ (0°)
diagonal basis ($\times$)	$\nearrow$ (45°)	$\nwarrow$ (135°)

As is shown in Figure 3 and the table above, we can encode the binary 0 and 1 according to different bases. And for the BB84 protocol, it uses two bases, the rectilinear basis and diagonal basis. Thus each qubit $|\psi\rangle_{ab}$ can be in one of the four states (a is to determine between binary 0 and 1, and b is to determine between the bases):

$$\begin{cases} |\psi\rangle_{00} = |0\rangle \\ |\psi\rangle_{10} = |1\rangle \\ |\psi\rangle_{01} = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |\psi\rangle_{11} = |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases} \tag{8}$$

The state $|0\rangle$ can be written as vector $\begin{bmatrix}1\\0\end{bmatrix}$, and the state $|1\rangle$ can be written as vector $\begin{bmatrix}0\\1\end{bmatrix}$. What is more, the Hadamard gate can be denoted by matrix $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$. Thus we have:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}) \Rightarrow |0\rangle \xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle \tag{9}$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}(\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}) \Rightarrow |1\rangle \xrightarrow{H} \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle \tag{10}$$

which means that we can obtain the $|+\rangle$ and $|-\rangle$ states through $|0\rangle$ and $|1\rangle$ states respectively using the Hadamard transform. And state $|+\rangle$ and $|-\rangle$ are in a superposition of staying at 0 and 1 at the same time. If we measure one of the two states, there is a 50% chance of getting 0, and 50% chance of getting 1.

We can then discuss the inverse Hadamard transform:

$$H^{-1} = \frac{1}{-\frac{1}{2}-\frac{1}{2}}\begin{bmatrix}-\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = H \tag{11}$$

thus if we want to do an inverse Hadamard transform to a qubit, it is equivalent to do Hadamard transform to it.

2.2.2 Generation and distribution of the shared secret key

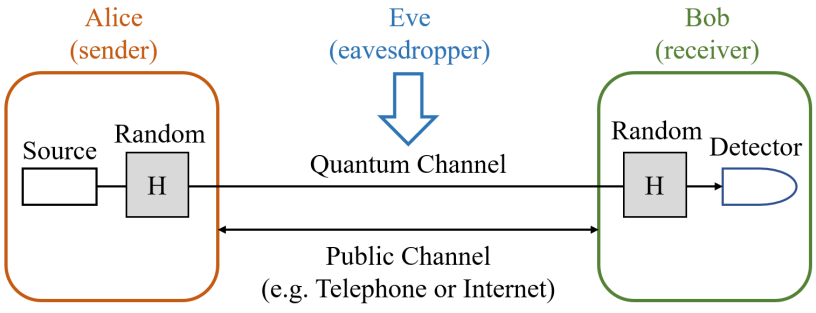

Figure 4: The structure of BB84 protocol

The structure of BB84 protocol is shown in Figure 4, and it can be divided into several steps:

Step 1. The sender, Alice, randomly generate an initial bit key sting a with length k, and generate the initial qubit key string according to a.

Step 2. Alice randomly generate a rotation string b with the same length as a, to determine which basis should each bit of a be encoded in. Do random rotation to the initial qubit key string according

to b, which means to do **Hadamard transform** to qubits where the basis is chosen as diagonal basis ($\times$), and do nothing if the basis is chosen as rectilinear basis ($+$). The bases and Hadamard transform is introduced in Part 2.2.1.

Step 3. Now transform the rotated qubit key string through a **quantum channel**. Here the eavesdropper Eve may intercept the qubits.

Step 4. After the transformation of the rotated qubit key string, the receiver Bob randomly generate a bit string b' with length k. Do random rotation in another direction to the rotated qubit key string according to b', which means to do **inverse Hadamard transform** to qubits where the basis is chosen as diagonal basis ($\times$), and do nothing if the basis is chosen as rectilinear basis ($+$). The bases and inverse Hadamard transform is introduced in Part 2.2.1.

Step 5. Bob measures the qubits, and get a final bit key string.

Step 6. Alice and Bob exchange their bit sting b and b' to each other through a **public channel**, e.g. telephone, Internet. For all $i \in [1, k]$ where $b[i] = b'[i]$ (Alice and Bob choose the same basis), there must be $a[i] = a'[i]$, otherwise it means that a third party Eve has been eavesdropping. We keep all the $a[i] = a'[i]$ as the shared secret key. According to probability, the average length of the shared secret key is $\frac{k}{2}$, which is half of the length of a, a', b and b' [2].

1	Sender (Alice)	Initial bit key string a		0	1	1	0	1	0	0	1
		Initial qubit key string		$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
2		Randomly Hadamard transform	Random rotation string b	0	0	1	0	1	1	1	0
			Rotation basis	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$+$
		Qubit key string to be transmitted	Dirac notation	$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\|1\rangle$
			Direction	↑ 90°	→ 0°	↖ 135°	↑ 90°	↖ 135°	↗ 45°	↗ 45°	→ 0°
3	Quantum Channel										
4	Receiver (Bob)	Qubit key string after transmission		$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\|1\rangle$
		Randomly inverse Hadamard transform	Random rotation string b'	0	1	1	1	0	1	0	0
			Rotation basis	$+$	$\times$	$\times$	$\times$	$+$	$\times$	$+$	$+$
		Final qubit key string		$\|0\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\|1\rangle$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\|1\rangle$
5	Final bit key string a' after measurement			0	0 or 1	1	0 or 1	0 or 1	0	0 or 1	1
6	Shared secret key			0		1			0		1

Figure 5: An example for the process of BB84 protocol, which is consistent with the the steps introduced above

Now the sender Alice and the receiver Bob have the same shared secret key. They can then encrypt and decrypt the message they want to send. The encryption and decryption process is the same with traditional private key cryptography, which is introduced in Part 1.2.

There are some other QKD protocols which are also based on the no-cloning theorem, but use different kinds of bases, for example BB92, SARG04 and Six-State protocol [3].

2.2.3 The eavesdropper

Then we would like to discuss why the eavesdropper, Eve, can be detected. During the way Alice sending qubits to Bob, Eve can intercept the qubits. But she does not know which basis Alice choose, and her measurement can destroy the quantum state. Eve does not know when or when not to rotate to recreate the qubits. Thus she may send all qubits without rotation to Bob, hoping to get the rotation 50% correct.

After Bob receives the key from Eve, Alice and Bob can randomly select part of their keys to compare publicly. If the two parts are not the same, they can detect the eavesdropping of Eve. Otherwise they are confident that Eve did not eavesdrop. The longer the key bits compared, the more likely they can detect Eve. Finally, Alice and Bob throw away the part of the key bits they compared, because these bits are now publicly known and not safe, and encrypt and decrypt the message with the left key bits.

[2]Note that as Claude Shannon discovered, to make it safe, the length of the shared secret key must be at least the same as the length of message. For one-time pad, we use a key as long as the message.

2.3 Protocol based on quantum entanglement: E91

E91 protocol was published by Ekert in 1991 [6], and it uses the entangled pairs of qubits (photons). These qubit pairs can be created by the sender Alice, the receiver Bob, or some source separate from both of them.

2.3.1 Create entanglement

Just now in Part 2.2.1 we discussed the Hadamard gate, which can be used to create superposition on a qubit. Then we would like to use another quantum gate, controlled-NOT (CNOT) gate, and add another qubit to create the entanglement between two qubits. This process is shown in Figure 6.

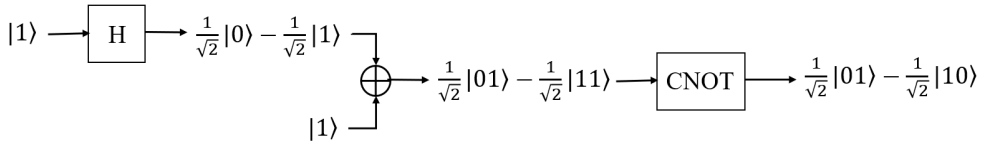

Figure 6: The process of creating entanglement using two $|1\rangle$ quantum states, the Hadamard gate and the CNOT gate.

After acting the CNOT gate on a pair of qubits, if the first qubit is $|0\rangle$, it will do nothing; however, if the first qubit is $|1\rangle$, it will flips the second qubit.

This quantum state $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$ that we get after CNOT gate is one of the Bell States. The Bell states are four specific maximally entangled quantum states of two qubits. The other three Bell states are created in a similar way as is shown in Figure 6, but using different input qubits. All Bell states are:

$$\begin{cases} |\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \\ |\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \\ |\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \\ |\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \end{cases} \tag{12}$$

where $\otimes$ stands for the tensor product. It is defined as:

$$|\psi\rangle_A \otimes |\psi\rangle_B = \begin{bmatrix} \alpha_A \\ \beta_A \end{bmatrix} \otimes |\psi\rangle_B = \begin{bmatrix} \alpha_A \otimes |\psi\rangle_B \\ \beta_A \otimes |\psi\rangle_B \end{bmatrix} = \begin{bmatrix} \alpha_A\alpha_B \\ \alpha_A\beta_B \\ \beta_A\alpha_B \\ \beta_A\beta_B \end{bmatrix} \tag{13}$$

with $|\psi\rangle_A = \begin{bmatrix} \alpha_A \\ \beta_A \end{bmatrix}$ and $|\psi\rangle_B = \begin{bmatrix} \alpha_B \\ \beta_B \end{bmatrix}$.

2.3.2 The process of E91 protocol

As we discussed above, in order to implement E91 protocol, entangled pairs of qubits must be created by Alice, Bob, or even a trusted third-party source. Here we suppose that a third-party source Charlie create the qubit pairs.

The E91 protocol relies on two properties of entanglement. Firstly, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they will always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarization. However the particular results are completely random, it is impossible for Alice to predict if and Bob will get vertical polarization or horizontal polarization.

Secondly, any attempt at eavesdropping by Eve will destroy these correlations in a way that Alice and Bob can detect.

References

[1] Nielsen M A, Chuang I. Quantum computation and quantum information[M]. 2002.

[2] Stallings W. Network Security Essentials: Applications and Standards, 4/e[M]. Pearson Education India, 2000.

[3] Hitesh Singh, D.L. Gupta, A.K Singh. Quantum Key Distribution Protocols: A Review[J]. IOSR Journal of Computer Engineering, 2014

[4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution[J]. Reviews of modern physics, 2009, 81(3): 1301.

[5] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theor. Comput. Sci., 2014, 560(P1): 7-11.

[6] Ekert A K. Quantum cryptography based on Bell's theorem[J]. Physical review letters, 1991, 67(6): 661.