Quantum Information Processing: from Theory to Practice

Lecture 7: Quantum Key Distribution (QKD)

Maurizio Magarini

Outline

Introduction

- Cryptography refers to the techniques necessary to protect data exchange and guarantee secure communication. Three different names are used interchangeable in the field: cryptography, cryptology, and cryptanalysis.
- Cryptology studies communication over insecure channels and related problems. Cryptography is the process of designing systems to protect and obscure transmitted information, while cryptanalysis deals with techniques for breaking these systems.
- Coding theory is often used to describe cryptography, but this can cause confusion. Actually, it
  - refers to the representation of input information symbols using output symbols called code symbols;
  - covers three fundamental applications[1], which are source compression, data secrecy, and error correction;
- Note that, in any real-world system, error correcting codes are used in conjunction with encryption, since the change of a single bit is enough to destroy the message completely in a well-designed cryptosystem.

[1] In recent decades the term coding theory has been mainly associated with error-correcting codes

Cryptographically Secure Communication

Secure communication using cryptography happens, roughly, in three phases:

1. Authentication refers to the process in which two parties validate the identity of each other to verify they are really the ones who want to communicate with and not somebody else
2. Key generation is used by the parties to encode their messages
3. Data encryption & decryption, which consists in encoding the message and encrypt the data sent to the other party where it will be decrypted

Three Phases

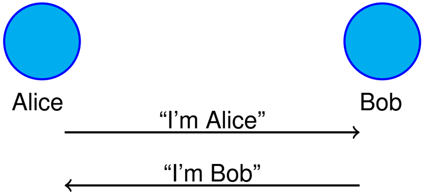
Phase 1: Authentication

Three Phases

Phase 1: Authentication

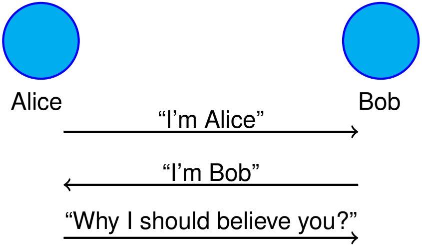
Three Phases

Phase 1: Authentication



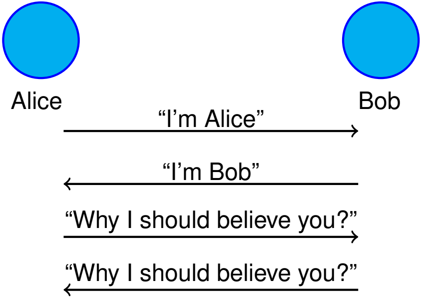
Three Phases

Phase 1: Authentication



Three Phases

Phase 1: Authentication



Three Phases

Phase 1: Authentication

Generally, the message and the procedure how two parties can authenticate each other is:

Three Phases

Phase 1: Authentication

Generally, the message and the procedure how two parties can authenticate each other is:

- Who *are* you? (biometrics)

Three Phases

Phase 1: Authentication

Generally, the message and the procedure how two parties can authenticate each other is:

- Who *are* you? (biometrics)
- What *do* you *have*? (possession)

Three Phases

Phase 1: Authentication

Generally, the message and the procedure how two parties can authenticate each other is:

- Who *are* you? (biometrics)
- What *do* you *have*? (possession)
- What *do* you *know*? (Knowledge)

Three Phases

Phase 1: Authentication

Generally, the message and the procedure how two parties can authenticate each other is:

- Who *are* you? (biometrics)
- What *do* you *have*? (possession)
- What *do* you *know*? (Knowledge)

The last one is quite important!

Three Phases

Phase 1: Authentication

Generally, the message and the procedure how two parties can authenticate each other is:

- Who *are* you? (biometrics)
- What *do* you *have*? (possession)
- What *do* you *know*? (Knowledge)

The last one is quite important!
For communication, we use either a *public key* or a *pre-shared secret*. These can be used as an authentication device.

Three Phases

Phase 2: Key generation

- Alice and Bob need to acquire or make a cryptographyc “key”.
- The key is used for encrypting the message.
- Keys should be changed often to ensure that the data is encrypted in a secure manner.

Three Phases

Phase 3: Data encryption and decryption

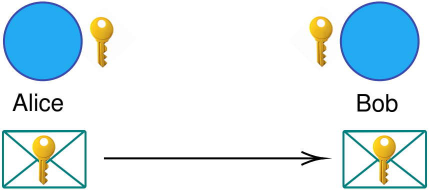
Three Phases

Phase 3: Data encryption and decryption

- Alice encrypts her message with the key.

Three Phases

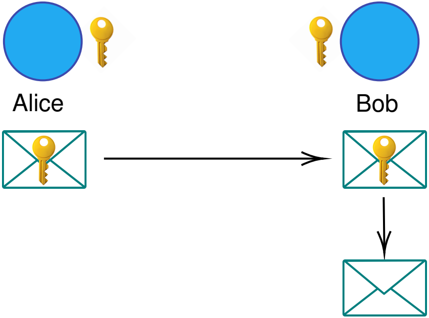
Phase 3: Data encryption and decryption



- Alice encrypts her message with the key.
- She sends it to Bob

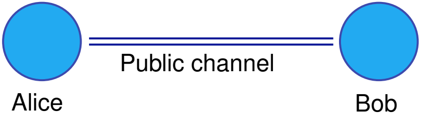
Three Phases

Phase 3: Data encryption and decryption



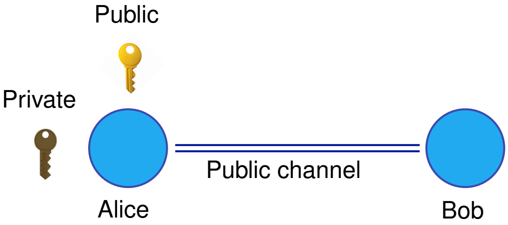
- Alice encrypts her message with the key.
- She sends it to Bob
- Bob uses his generated part of the key to decrypt the message and read it.

Public Key Cryptography



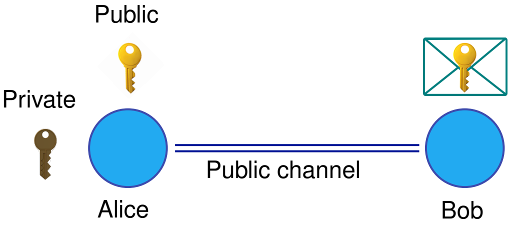
- A way to establish a private key between Alice and Bob is to use a public key channel, where "public" means that anybody can access (not secure channel)

Public Key Cryptography



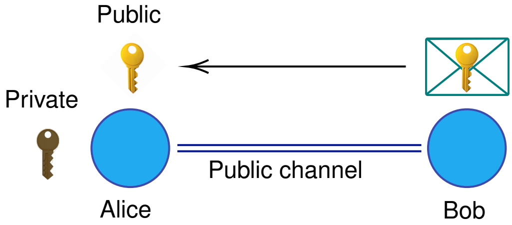
- A way to establish a private key between Alice and Bob is to use a public key channel, where "public" means that anybody can access (not secure channel)
- Alice generates two keys:
  - Public key, which can be revealed to everyone.
  - Private key, which is secret (only she knows it!).

Public Key Cryptography



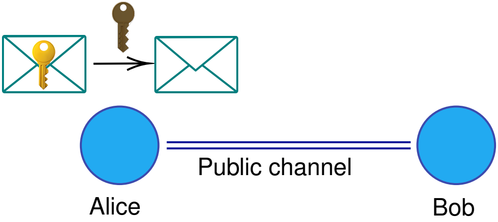
- A way to establish a private key between Alice and Bob is to use a public key channel, where "public" means that anybody can access (not secure channel)
- Alice generates two keys:
  - Public key, which can be revealed to everyone.
  - Private key, which is secret (only she knows it!).
- Alice sends the public key to Bob who uses it to encrypt his message that is then sent back to her.

Public Key Cryptography



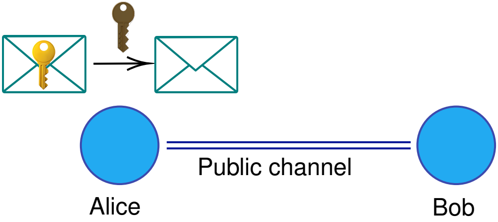
- A way to establish a private key between Alice and Bob is to use a public key channel, where "public" means that anybody can access (not secure channel)
- Alice generates two keys:
  - Public key, which can be revealed to everyone.
  - Private key, which is secret (only she knows it!).
- Alice sends the public key to Bob who uses it to encrypt his message that is then sent back to her.

Public Key Cryptography



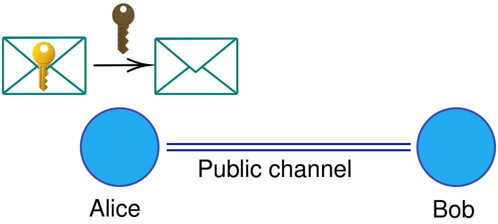
- Alice uses the private key that she did not communicate to decrypt Bob's message.

Public Key Cryptography



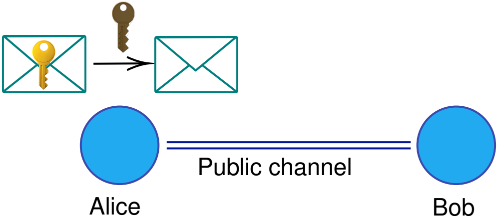
- Alice uses the private key that she did not communicate to decrypt Bob's message.

Public Key Cryptography



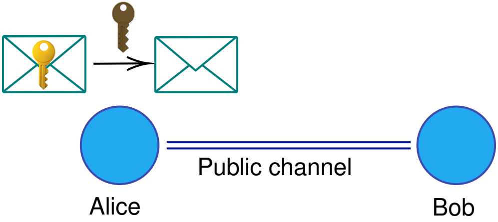
- Alice uses the private key that she did not communicate to decrypt Bob's message.
- In public key cryptography, the public key is used to encrypt the message but it cannot be used to decrypt the message.

Public Key Cryptography



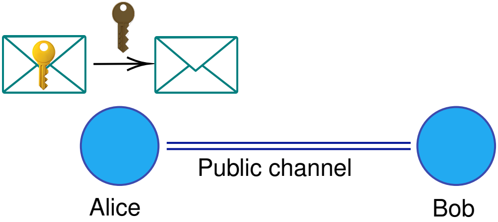
- Alice uses the private key that she did not communicate to decrypt Bob's message.
- In public key cryptography, the public key is used to encrypt the message but it cannot be used to decrypt the message.
- The message can be decrypted only using the private key.

Public Key Cryptography



- Alice uses the private key that she did not communicate to decrypt Bob's message.
- In public key cryptography, the public key is used to encrypt the message but it cannot be used to decrypt the message.
- The message can be decrypted only using the private key.
- Public key cryptography covers all the three requirements, but
  1. is very slow/expensive,
  2. encrypted public message is only computationally secure, meaning that anybody listening to the channel is able, in theory, to break the encryption if, either they have a large amount of computational resources or computational time.

Public Key Cryptography



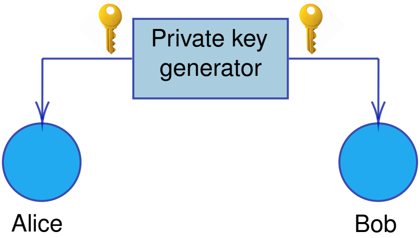
- Alice uses the private key that she did not communicate to decrypt Bob's message.
- In public key cryptography, the public key is used to encrypt the message but it cannot be used to decrypt the message.
- The message can be decrypted only using the private key.
- Public key cryptography covers all the three requirements, but
  1. is very slow/expensive,
  2. encrypted public message is only computationally secure, meaning that anybody listening to the channel is able, in theory, to break the encryption if, either they have a large amount of computational resources or computational time.
- Quantum computers can, in principle, break the encryption with relative ease!

Private Key Cryptography

Alternatively, Alice and Bob can communicate securely via the use of a private key.

Private Key Cryptography

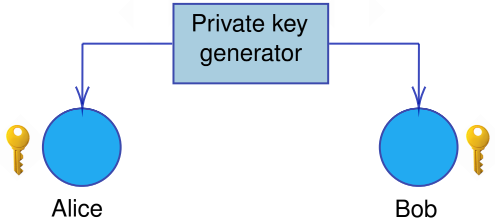
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- A device can generate a private key that is sent both to Alice and to Bob.

Private Key Cryptography

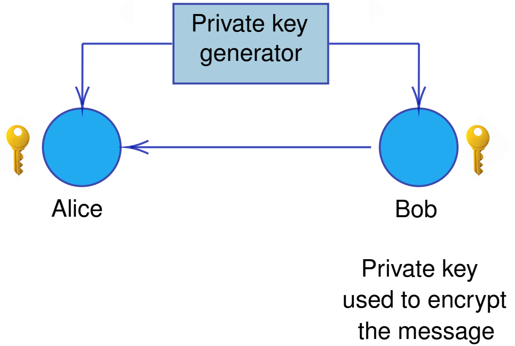
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- A device can generate a private key that is sent both to Alice and to Bob.
- Now Alice and Bob share some correlated secret key they only know and use to encrypt their messages

Private Key Cryptography

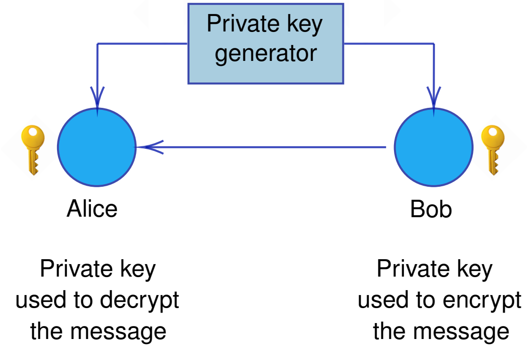
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- A device can generate a private key that is sent both to Alice and to Bob.
- Now Alice and Bob share some correlated secret key they only know and use to encrypt their messages
- For example, Bob encrypts his message and sends it to Alice

Private Key Cryptography

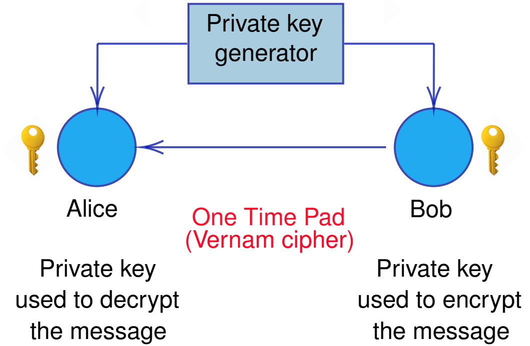
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- A device can generate a private key that is sent both to Alice and to Bob.
- Now Alice and Bob share some correlated secret key they only know and use to encrypt their messages
- For example, Bob encrypts his message and sends it to Alice
- Alice uses her part of the secret key to decrypt it and read the message

Private Key Cryptography

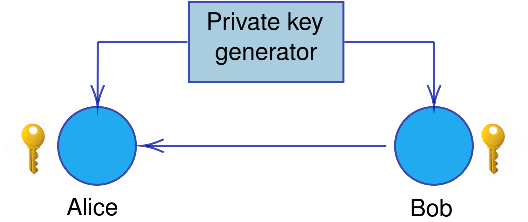
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- A device can generate a private key that is sent both to Alice and to Bob.
- Now Alice and Bob share some correlated secret key they only know and use to encrypt their messages
- For example, Bob encrypts his message and sends it to Alice
- Alice uses her part of the secret key to decrypt it and read the message
- This is known as “One Time Pad” (Vernam Cipher)

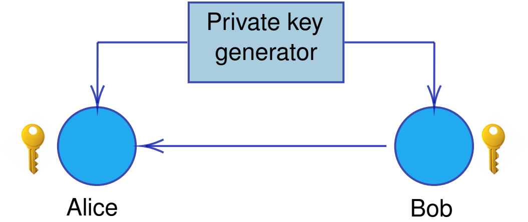
Private Key Cryptography

Alternatively, Alice and Bob can communicate securely via the use of a private key.



Private Key Cryptography

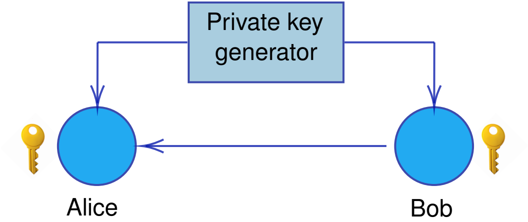
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- Secure if the private key is used only once!

Private Key Cryptography

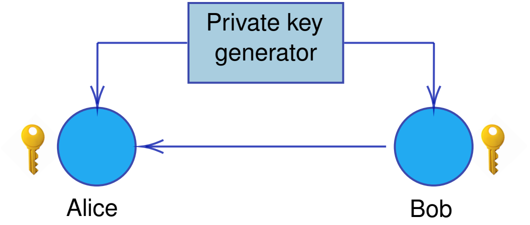
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- Secure if the private key is used only once!
- So, if Bob has a message of n bits that he is trying to send to Alice, he requires a private key that is at least n bits long and once he uses that private key to encrypt his message he cannot use it again. If he has some other thing to say to Alice, he cannot use it again.

Private Key Cryptography

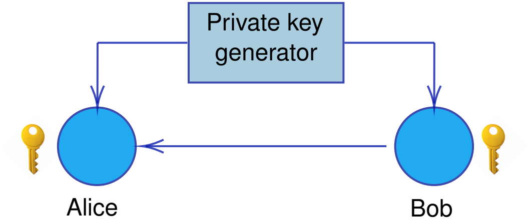
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- Secure if the private key is used only once!
- So, if Bob has a message of n bits that he is trying to send to Alice, he requires a private key that is at least n bits long and once he uses that private key to encrypt his message he cannot use it again. If he has some other thing to say to Alice, he cannot use it again.
- If Bob has some other thing to say to Alice, they require a completely new and fresh private key to guarantee security.

Private Key Cryptography

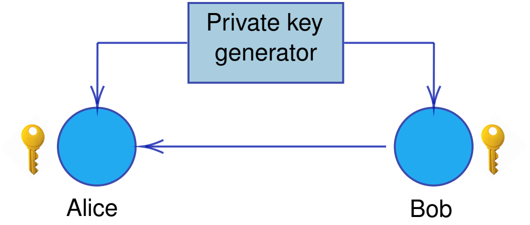
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- Secure if the private key is used only once!
- So, if Bob has a message of n bits that he is trying to send to Alice, he requires a private key that is at least n bits long and once he uses that private key to encrypt his message he cannot use it again. If he has some other thing to say to Alice, he cannot use it again.
- If Bob has some other thing to say to Alice, they require a completely new and fresh private key to guarantee security.
- Requires a large amount of key bits.

Private Key Cryptography

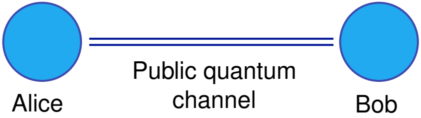
Alternatively, Alice and Bob can communicate securely via the use of a private key.



- Secure if the private key is used only once!
- So, if Bob has a message of n bits that he is trying to send to Alice, he requires a private key that is at least n bits long and once he uses that private key to encrypt his message he cannot use it again. If he has some other thing to say to Alice, he cannot use it again.
- If Bob has some other thing to say to Alice, they require a completely new and fresh private key to guarantee security.
- Requires a large amount of key bits.
- Remaining question: How do we distribute the private key?

Protocol

- The BB84 is a QKD protocol where Alice and Bob communicate through a public quantum channel as well as their public classical channel.



- Alice generates two n-bit strings:

$$a = a_1\, a_2\, \ldots\, a_n$$
$$b = b_1\, b_2\, \ldots\, b_n$$

- Alice creates a quantum state according to these bit strings as described in the following.

Encoding

- From each two bits from *a* and *b* Alice generates one qubit.
- The whole state Alice creates is given by

$$|\psi\rangle = \bigotimes_{k=1}^{n} |\psi_{a_k b_k}\rangle \qquad \begin{array}{ll} |\psi_{00}\rangle = |0\rangle\,, & |\psi_{01}\rangle = |+\rangle \\ |\psi_{10}\rangle = |1\rangle\,, & |\psi_{11}\rangle = |-\rangle \end{array}$$

- It can be seen that the bit coming from the bit string *b* determines the basis of the encoding:
  - If $b = 0$ she prepares the qubit in the Z basis (computational basis);
  - If $b = 1$ she prepares the qubit in the X basis (Hadamard basis).
  - Then a_k chooses which state from the basis she prepares.
- Note that the encoded states are not orthogonal

$$\langle\psi_{00}|\psi_{01}\rangle = \frac{1}{\sqrt{2}},$$

which means that the states are not perfectly distinguishable.

Encoding

What does it mean to be distinguishable?

- Consider the two orthogonal states

$$|\psi_{00}\rangle = |0\rangle \quad |\psi_{10}\rangle = |1\rangle$$

  and measure them in the Z basis.
- In this case they are orthogonal and we can perfectly distinguish them:
  - The measure of $|\psi_{00}\rangle = |0\rangle$ always gives $+1$
  - The measure of $|\psi_{10}\rangle = |1\rangle$ always gives -1
- The two states can always be distinguished!
- Also true for $|\psi_{01}\rangle = |+\rangle$ and $|\psi_{11}\rangle = |-\rangle$ when measured in the X basis.

Encoding

What does it mean to be distinguishable?

- Consider now the two non-orthogonal states

$$|\psi_{00}\rangle = |0\rangle \quad |\psi_{01}\rangle = |+\rangle$$

and measure them in the Z basis.

- In this case we have that the measure of
  - $|\psi_{00}\rangle = |0\rangle$ always gives $+1$, which is fine
  - $|\psi_{01}\rangle = |+\rangle$ gives $+1$ in 50% of the cases and -1 in the other 50%. If we get -1 we can say that we know the state is $|+\rangle$ but if we get $+1$, we are unsure whether the state is $|+\rangle$ of $|0\rangle$.
- In this sense, the states are not-distinguishable.
- Measuring in the X basis does not help.
- There is no measurement basis that perfectly distinguishes these states!

Encoding example

Consider an example when $n = 5$.

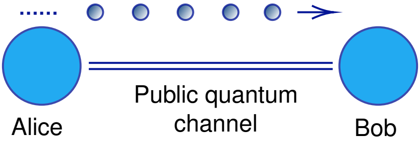
$$\left|\psi_{a_k b_k}\right\rangle \qquad \begin{array}{ll} |\psi_{00}\rangle = |0\rangle\,, & |\psi_{01}\rangle = |+\rangle \\ |\psi_{10}\rangle = |1\rangle\,, & |\psi_{11}\rangle = |-\rangle \end{array}$$

Alice's operations

string a	0	1	1	0	1
string b	1	1	0	0	1
basis	X	X	Z	Z	X
encoded qubits	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$

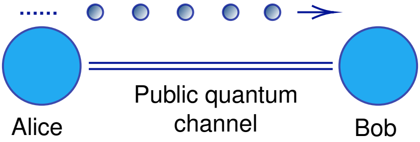
Bob's measurements

Alice sends the encoded qubits to Bob over the quantum public channel.



Bob's measurements

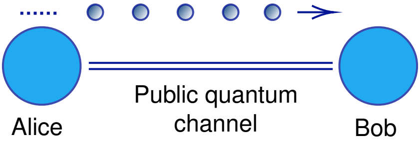
Alice sends the encoded qubits to Bob over the quantum public channel.



- Bob receives the qubits.

Bob's measurements

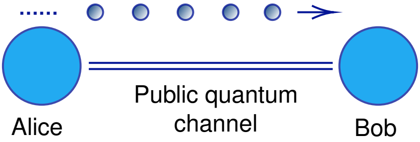
Alice sends the encoded qubits to Bob over the quantum public channel.



- Bob receives the qubits.
- He does not know at this time what these states are because Alice did not share the secret bit string *b*.

Bob's measurements

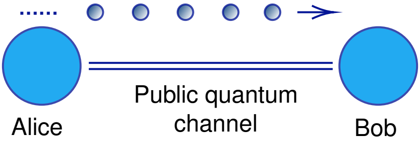
Alice sends the encoded qubits to Bob over the quantum public channel.



- Bob receives the qubits.
- He does not know at this time what these states are because Alice did not share the secret bit string b.
- The secret bit string b contains information about the preparation basis.

Bob's measurements

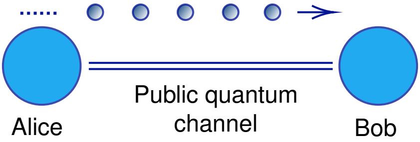
Alice sends the encoded qubits to Bob over the quantum public channel.



- Bob receives the qubits.
- He does not know at this time what these states are because Alice did not share the secret bit string b.
- The secret bit string b contains information about the preparation basis.
- Bob only knows that he is receiving qubits that can be any of the four possible states: $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$.

Bob's measurements

Alice sends the encoded qubits to Bob over the quantum public channel.

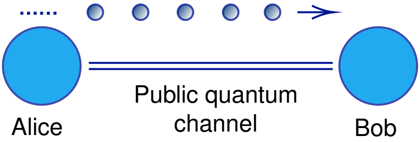


- Bob receives the qubits.
- He does not know at this time what these states are because Alice did not share the secret bit string b.
- The secret bit string b contains information about the preparation basis.
- Bob only knows that he is receiving qubits that can be any of the four possible states: $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$.
- Bob generates his own random bit string:

$$b' = b'_1 \, b'_2 \, \ldots \, b'_n$$

Bob's measurements

Alice sends the encoded qubits to Bob over the quantum public channel.



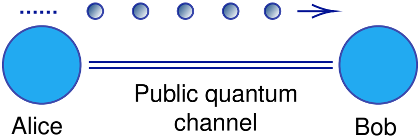
- Bob receives the qubits.
- He does not know at this time what these states are because Alice did not share the secret bit string b.
- The secret bit string b contains information about the preparation basis.
- Bob only knows that he is receiving qubits that can be any of the four possible states: $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$.
- Bob generates his own random bit string:

$$b' = b'_1\, b'_2\, \ldots\, b'_n$$

- He measures the received qubits according to b'

Bob's measurements

Bob measures the qubits to produce bit string a'.



If $b'_k = 0$, Bob measures in the Z basis.

If $b'_k = 1$, Bob measures in the X basis.

This allows Bob to generate his own random bit string a'

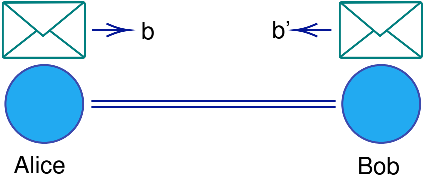
According to the kth measurement:

If kth outcome is $+1$, then $a'_k = 0$.

If kth outcome is -1, then $a'_k = 1$.

New key

Alice and Bob announce the strings b and b' over a public channel.



When $b_k = b'_k$, keep the bits a_k, a'_k.
When $b_k \neq b'_k$, discard the bits a_k, a'_k.

This produces new shorter keys $\bar{a}$, $\bar{a}'$ such that

$$\bar{a} = \bar{a}'$$

Now they are sharing a key they can use in the next step, which is encryption of the data!

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1
string b	1	0	1	1	0
basis	X	Z	X	X	Z
encoded qubits	$\vert -\rangle$	$\vert 0\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 1\rangle$
string b'	1	1	1	0	0
Bob's basis	X	X	X	Z	Z
string a'	1	$0/1$	0	$0/1$	1

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1
string b	1	0	1	1	0
basis	X	Z	X	X	Z
encoded qubits	$\lvert - \rangle$	$\lvert 0 \rangle$	$\lvert + \rangle$	$\lvert - \rangle$	$\lvert 1 \rangle$
string b'	1	1	1	0	0
Bob's basis	X	X	X	Z	Z
string a'	1	$0/1$	0	$0/1$	1

Alice

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1
string b	1	0	1	1	0
basis	X	Z	X	X	Z
encoded qubits	$\lvert - \rangle$	$\lvert 0 \rangle$	$\lvert + \rangle$	$\lvert - \rangle$	$\lvert 1 \rangle$
string b'	1	1	1	0	0
Bob's basis	X	X	X	Z	Z
string a'	1	$0/1$	0	$0/1$	1

Alice

Bob

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1	Alice
string b	1	0	1	1	0	
basis	X	Z	X	X	Z	
encoded qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	
string b'	1	1	1	0	0	Bob
Bob's basis	X	X	X	Z	Z	
string a'	1	$0/1$	0	$0/1$	1	

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1	Alice
string b	1	0	1	1	0	
basis	X	Z	X	X	Z	
encoded qubits	$\vert-\rangle$	$\vert 0\rangle$	$\vert+\rangle$	$\vert-\rangle$	$\vert 1\rangle$	
string b'	1	1	1	0	0	Bob
Bob's basis	X	X	X	Z	Z	
string a'	1	$0/1$	0	$0/1$	1	

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1	Alice
string b	1	0	1	1	0	
basis	X	Z	X	X	Z	
encoded qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	
string b'	1	1	1	0	0	Bob
Bob's basis	X	X	X	Z	Z	
string a'	1	$0/1$	0	$0/1$	1	

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1	
string b	1	0	1	1	0	Alice
basis	X	Z	X	X	Z	
encoded qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	
string b'	1	1	1	0	0	
Bob's basis	X	X	X	Z	Z	Bob
string a'	1	$0/1$	0	$0/1$	1	

Encoding example

Consider the case when $n = 5$

string a	1	0	0	1	1	Alice
string b	1	0	1	1	0	
basis	X	Z	X	X	Z	
encoded qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	
string b'	1	1	1	0	0	Bob
Bob's basis	X	X	X	Z	Z	
string a'	1	$0/1$	0	$0/1$	1	
	✓	✗	✓	✗	✓	

Summary

1. Alice generates random n-bits strings a, b.
2. Alice encodes each bit a_k in the Z basis if $b_k = 0$, and in the X basis if $b_k = 1$.
3. Alice sends the quantum state to Bob.
4. Bob measures each qubit in Z or X basis at random.
5. Alice and Bob discard qubits where Bob measured in different basis than Alice prepared.
6. Results of measurements where Alice's and Bob's bases agree are used as a secret key.

Summary

1. Alice generates random n-bits strings a, b.
2. Alice encodes each bit a_k in the Z basis if $b_k = 0$, and in the X basis if $b_k = 1$.
3. Alice sends the quantum state to Bob.
4. Bob measures each qubit in Z or X basis at random.
5. Alice and Bob discard qubits where Bob measured in different basis than Alice prepared.
6. Results of measurements where Alice's and Bob's bases agree are used as a secret key.

This protocol works under ideal conditions.

Summary

1. Alice generates random n-bits strings a, b.
2. Alice encodes each bit a_k in the Z basis if $b_k = 0$, and in the X basis if $b_k = 1$.
3. Alice sends the quantum state to Bob.
4. Bob measures each qubit in Z or X basis at random.
5. Alice and Bob discard qubits where Bob measured in different basis than Alice prepared.
6. Results of measurements where Alice's and Bob's bases agree are used as a secret key.

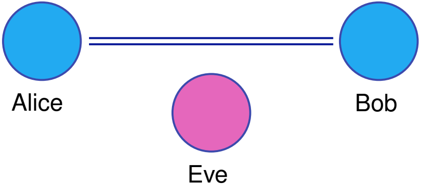
This protocol works under ideal conditions.

What happens when Eve tries to eavesdrop?

Introducing the eavesdropper

Eve wants to discover the secret key.

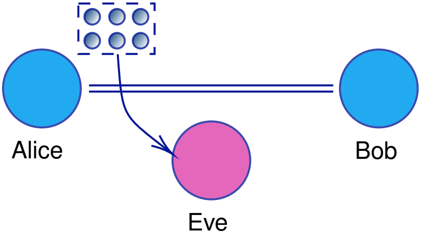
Can Eve copy and resend the qubits to Bob?



Introducing the eavesdropper

Eve wants to discover the secret key.

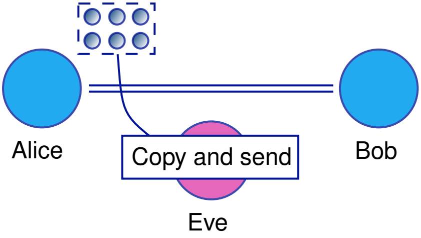
Can Eve copy and resend the qubits to Bob?



Introducing the eavesdropper

Eve wants to discover the secret key.

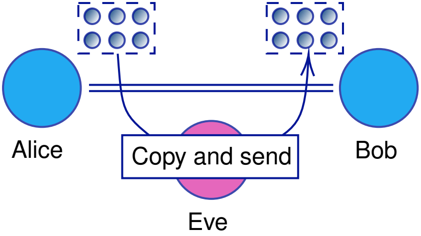
Can Eve copy and resend the qubits to Bob?



Introducing the eavesdropper

Eve wants to discover the secret key.

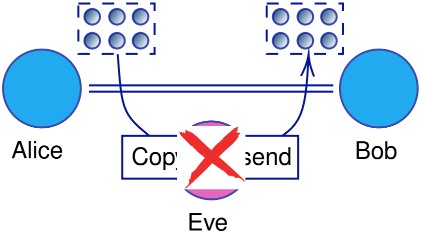
Can Eve copy and resend the qubits to Bob?



Introducing the eavesdropper

Eve wants to discover the secret key.

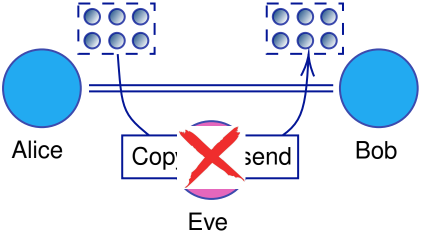
Can Eve copy and resend the qubits to Bob?



Introducing the eavesdropper

Eve wants to discover the secret key.

Can Eve copy and resend the qubits to Bob?



> No-cloning theorem does not allow Eve to replicate Alice's quantum states.

Eavesdropper detection

Eve has to measure the quantum states.

Eavesdropper detection

Eve has to measure the quantum states.

Without access to Alice's preparation basis, Eve has to guess the basis of measurement.

Eavesdropper detection

Eve has to measure the quantum states.

Without access to Alice's preparation basis, Eve has to guess the basis of measurement.

$\rightarrow$ qubits sent by Alice may be get **disturbed**!

Eavesdropper detection

Eve has to measure the quantum states.

Without access to Alice's preparation basis, Eve has to guess the basis of measurement.

$\rightarrow$ qubits sent by Alice may be get **disturbed**!

Example:

Alice's basis	X	Z	X	X
Eve's basis	X	X	Z	X
Disturbance	No	Yes	Yes	No

Eavesdropper detection

Eve has to measure the quantum states.

Without access to Alice's preparation basis, Eve has to guess the basis of measurement.

$\rightarrow$ qubits sent by Alice may be get **disturbed**!

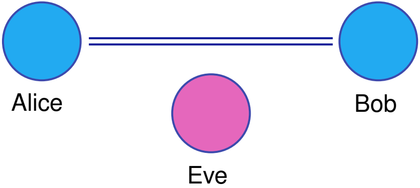
Example:

Alice's basis	X	Z	X	X
Eve's basis	X	X	Z	X
Disturbance	No	Yes	Yes	No

When Eve guesses wrong, the basis is changed!

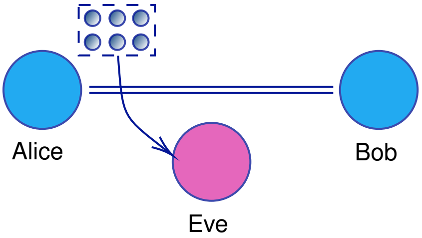
Eavesdropper detection

Eve's measurements disturb the qubits.



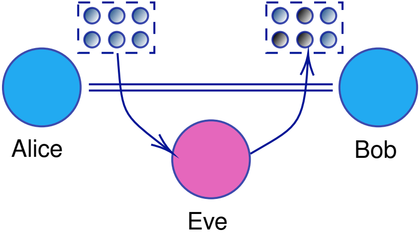
Eavesdropper detection

Eve's measurements disturb the qubits.



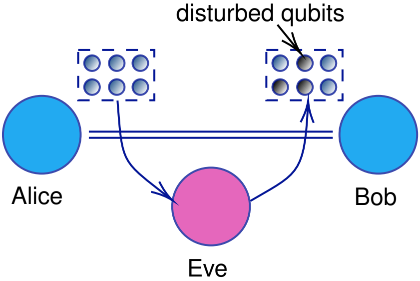
Eavesdropper detection

Eve's measurements disturb the qubits.



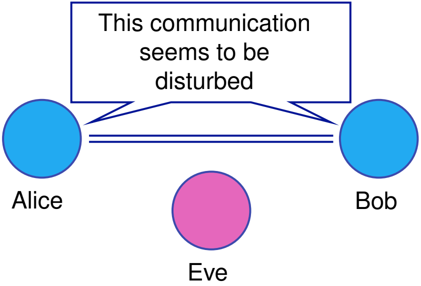
Eavesdropper detection

Eve's measurements disturb the qubits.



Eavesdropper detection

Can Alice and Bob detect the existence of Eve?



In one qubit system, the probability that the eavesdropper is detected is $1/4$ in ideal case.

- Eve chooses different basis from Alice's bases . . . $1/2$
- Bob chooses the same basis as Alice's bases . . . $1/2$

  $\rightarrow$ In both the two cases, Alice and Bob can detect the existence of Eve with probability $1/4$

Eavesdropper detection

In an n qubit system, the probability that Alice and Bob can successfully detect Eve is

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

When $n = 25$ the probability goes to 0.999.