QKD-Based Secure Chat Room Application

Kaminaga Yuma, Anh T. Pham, Hoang D. Le
Computer Communication Laboratory, The University of Aizu

Outline

1. Background of QKD
2. Secure Chat Room Application

1. Background of QKD

QKD (Quantum Key Distribution)

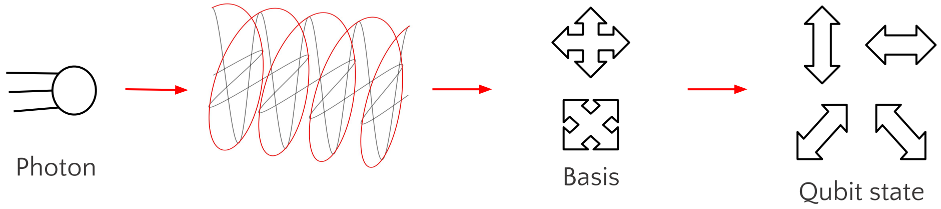
1. QKD can generate and share secure keys by using the polarization of photons (Qubit) and the properties of quantum mechanics.
2. If an eavesdropper attempts to observe a photon, the state of the photon will change, making eavesdropping detectable.

Why is QKD necessary?

It is feared that with the advent of quantum computers, conventional cryptographic methods (such as RSA) will become vulnerable.

What is the Qubit?

Qubit is the information unit of a quantum computer. Instead of being either 0 or 1 like a classical bit, it can have both states in an established proportion.



Bit / Basis	0	1
✥	↕	↔
✕	⤢	⤡

The classical bits, 0 and 1 can be encoded into Qubit using the basis shown on the right table.

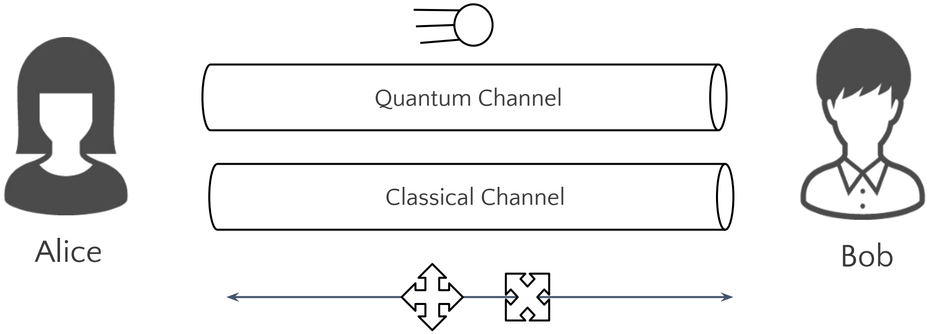
BB84 Protocol

BB84 is the world’s first QKD protocol.

- It uses the polarization of photons to encode information by selecting one of two basis (Rectilinear basis or Diagonal basis).

- Quantum Channel is used to share Qubit and Classical Channel is used to exchange basis information

Basis \ Bit	0	1
✥	↕	↔
⤧	⤢	⤡



Step of The BB84 Protocol

1. Alice randomly generate bits and selects a basis to generate a qubit.
2. Alice sends the generated qubit to Bob using a quantum channel.
3. Bob randomly selects a basis to measure the received qubit.
4. Alice and Bob share over a classical channel which bases they used for their measurements.
5. If the basis is the same, save the bit and use it as the sifted key.

Bit Basis	0	1
✥	⇕	⇔
✕	⤢	⤡

Alice

Bob

Bit	Basis	Qubit		Basis	Qubit	Bit
1	✥	⇔	Match	✥	⇔	1
0	✕	⤢	Mismatch	✥	⇕	0
1	✕	⤡	Match	✕	⤡	1
1	✥	⇔	Mismatch	✕	⤢	0

BBM92 Protocol

BBM92 protocol is essentially an entanglement based version of BB84 protocol

- A third party, Quantum Generator generates photon pairs in a quantum entangled state and uses them to send one to Alice and the other to Bob using the Quantum Channel.
- Classical Channel is used to exchange the basis information as in the BB84 protocol.

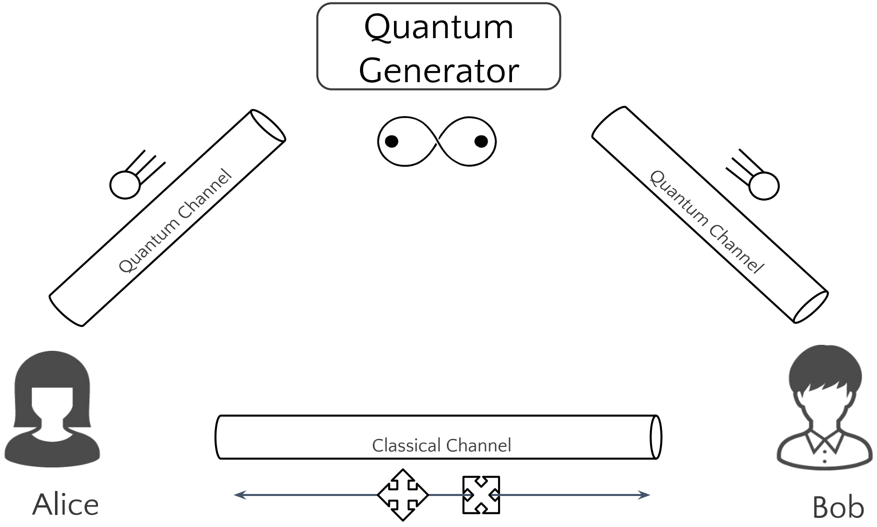
What is Quantum entanglement?

- Quantum entanglement is a phenomenon in which two photons are strongly correlated, and measuring one photon, even if they are far apart, determines the state of the other photon.

E.g.

It means that in a certain entangled state, if one of the photons is measured as 1, then the other will also be 1, and if one is measured as 0, the other will likewise be 0.

Therefore, if Alice and Bob choose the same basis for their measurements, they can predict the other's Qubit state.



Step of The BBM92 Protocol

1. Alice receives one of the entangled photon pairs initially prepared by a third party, and Bob receives the other.
2. Alice and Bob measure the received qubit in a randomly chosen basis
3. Using the classical channel, Alice and Bob tell each other which basis they chose for which position.
4. If the basis is the same, save the bit and use it as the sifted key.

Bit / Basis	0	1
✥	↕	↔
⤧	⤢	⤡

Alice

Basis	Qubit	Bit
✥	↔	1
⤧	⤢	0
⤧	⤡	1
✥	↔	1

Match

Mismatch

Match

Mismatch

Bob

Basis	Qubit	Bit
✥	↔	1
✥	↕	0
⤧	⤡	1
⤧	⤢	0

2. Secure Chat Room Application

Goal of The Study

Development of QKD-Chat Application for Multiple Users using BBM92 Protocol

How do we implement BBM92 protocol?

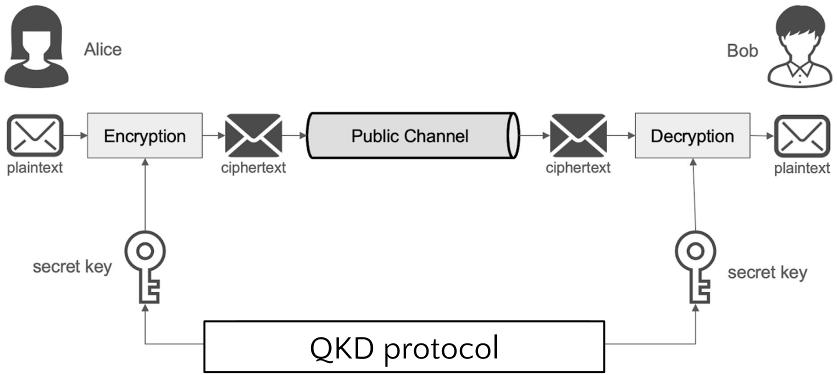
- Using **Qiskit**, a Python library and software development kit for quantum computing by IBM.
- By using Qiskit, you can access IBM Quantum Experience (IQX), which is IBM's cloud-based quantum computing platform.

Qiskit allows you to manipulate Qubit, design and simulate quantum circuits.

How do we encrypt and decrypt messages?

- DES-CBC is used for message encryption and decryption.

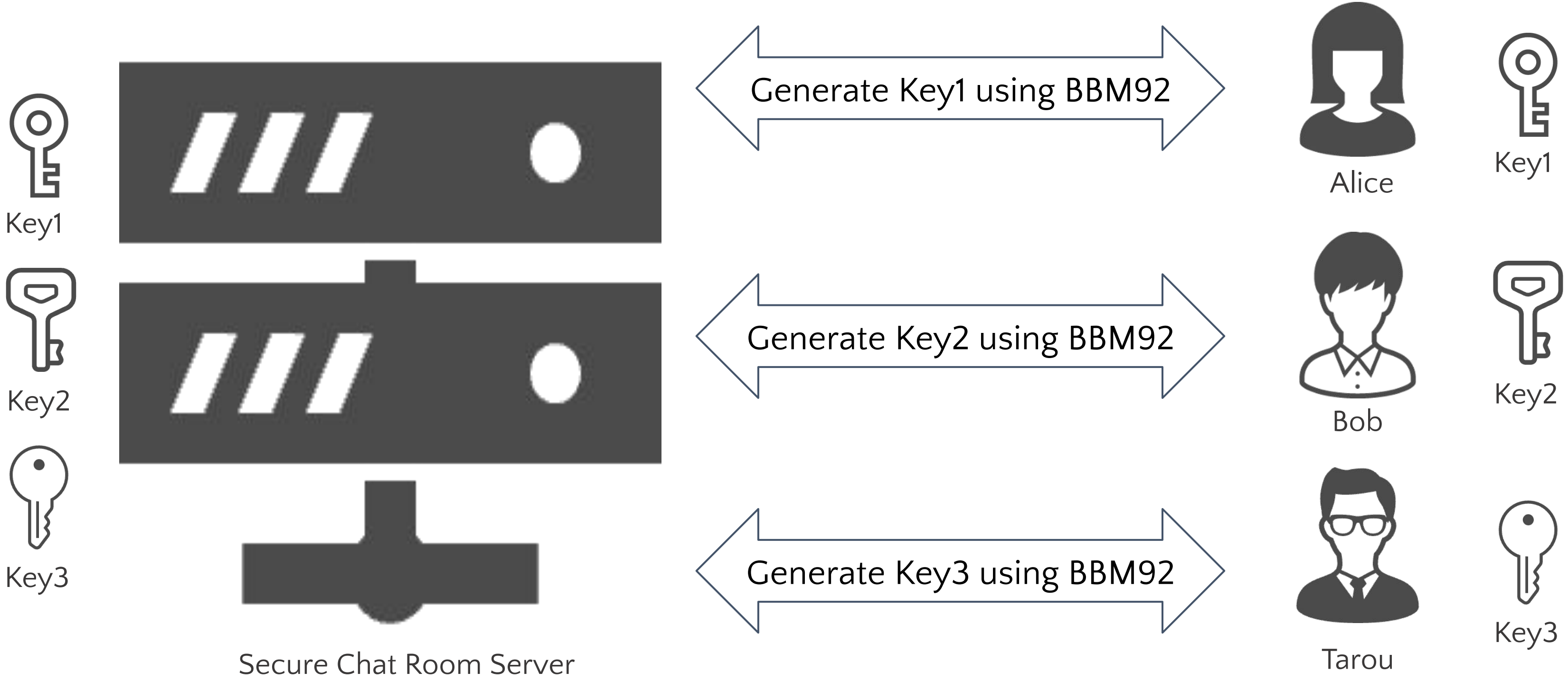
An Example of QKD-Based Chat Application



Generate the 56-bit key required for DES-CBC using the BBM92 protocol.

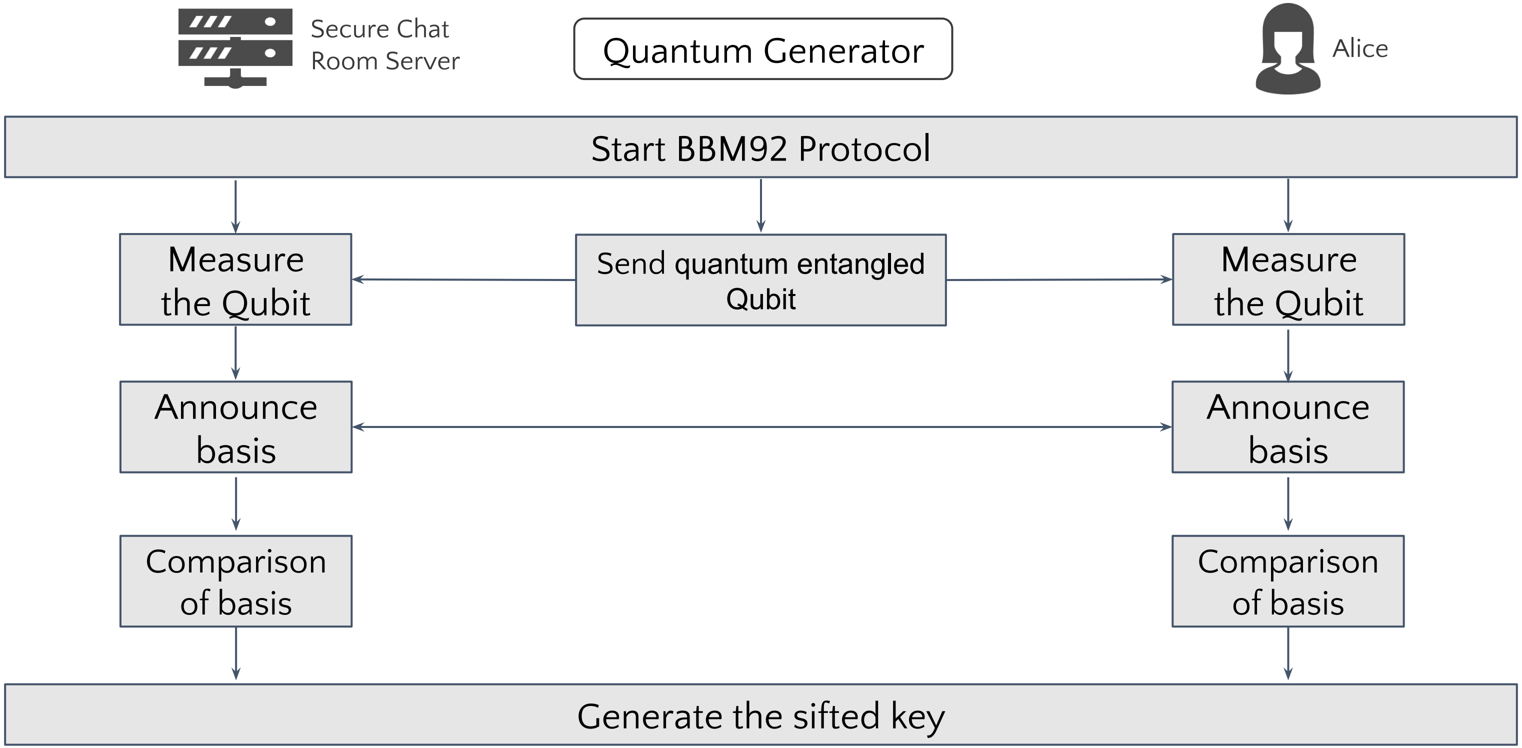
System Model of BBM92 Protocol

Assume three Chat Room participants


Key1
Key2
Key3
Secure Chat Room Server
Generate Key1 using BBM92
Generate Key2 using BBM92
Generate Key3 using BBM92
Alice
Key1
Bob
Key2
Tarou
Key3

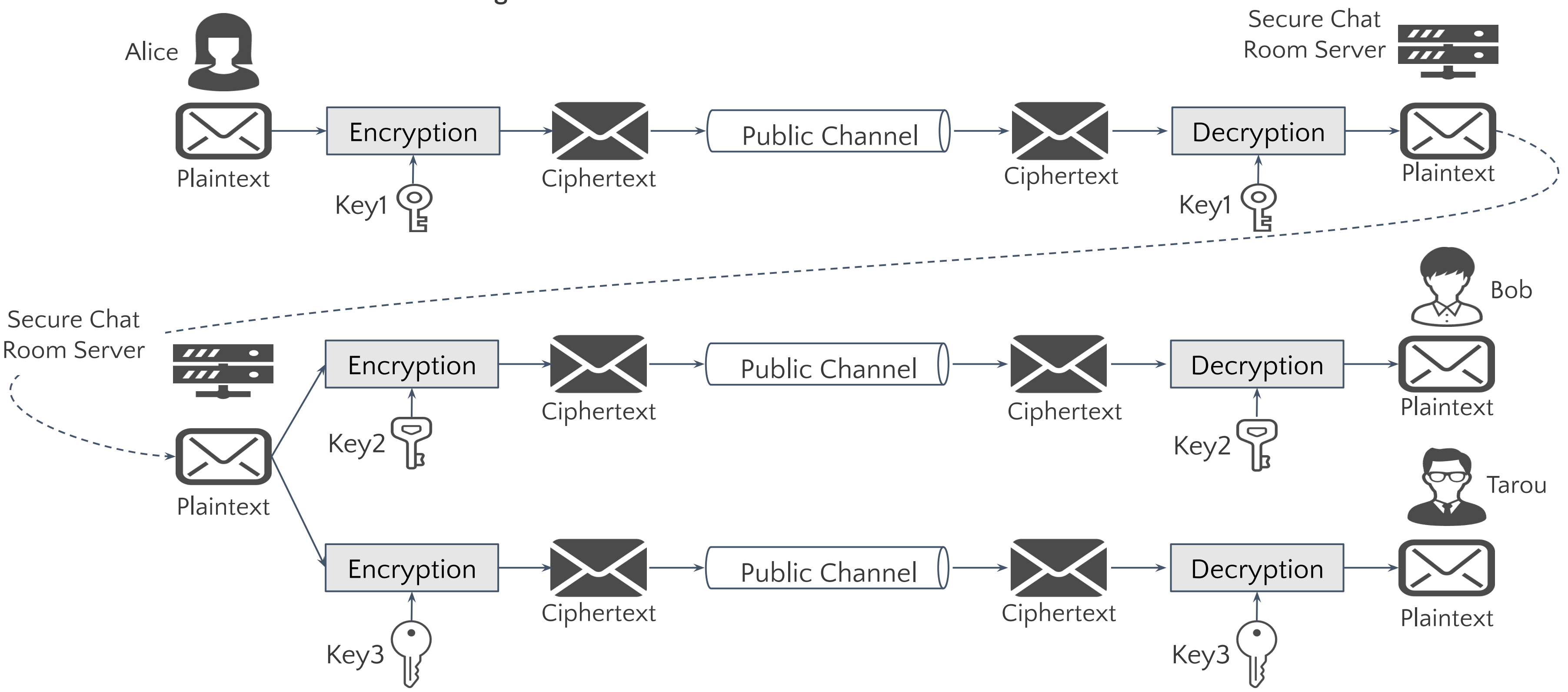
Flowchart of The BBM92 Protocol

Assume that the Secure Chat Room Server and Alice generate sifted key by BBM92 protocol



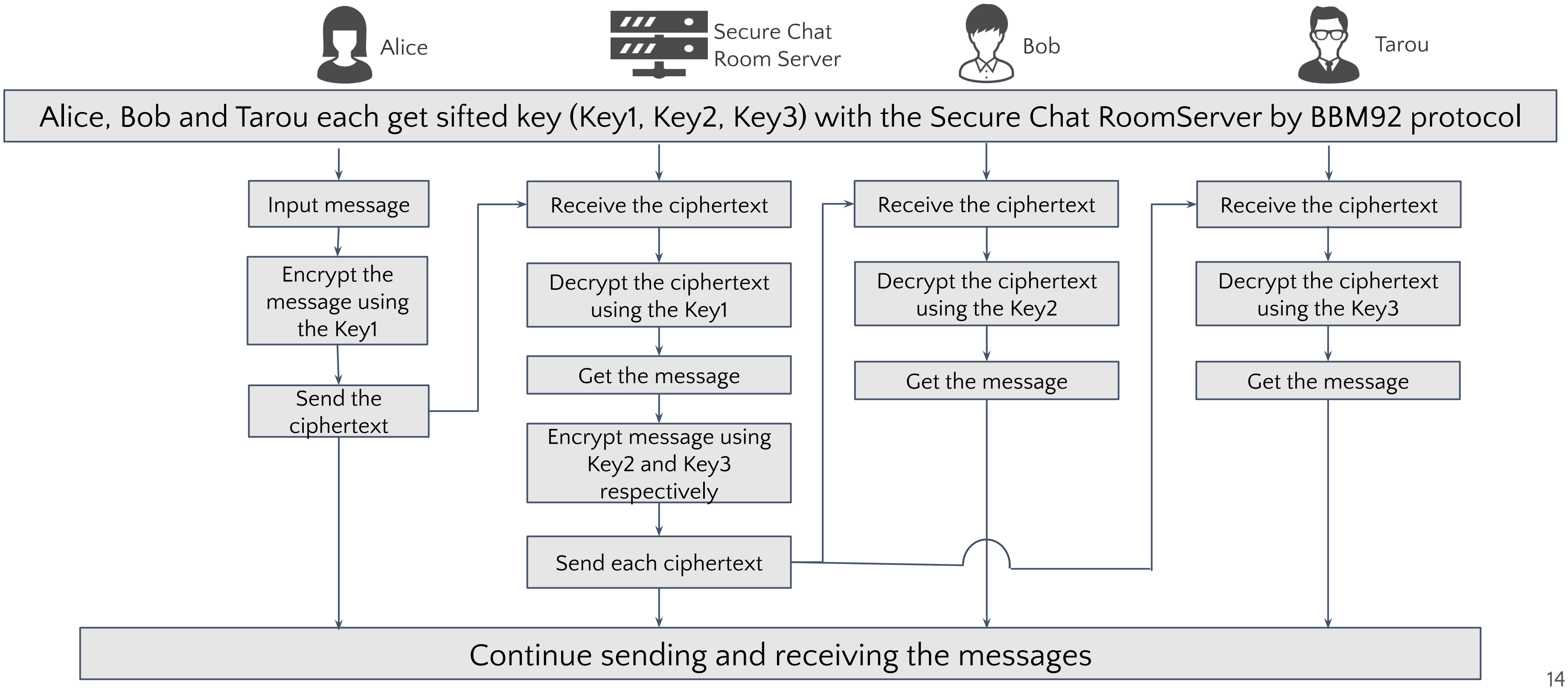
System Model for Sending and Receiving Messages in Secure Chat Room

Assume that Alice sends a message to Bob and Tarou



Flowchart of QKD-Based Secure Chat Room Application

Assume that Alice sends a message to Bob and Tarou



Alice

Secure Chat Room Server

Bob

Tarou

Alice, Bob and Tarou each get sifted key (Key1, Key2, Key3) with the Secure Chat RoomServer by BBM92 protocol

Alice:

- Input message
- Encrypt the message using the Key1
- Send the ciphertext

Secure Chat Room Server:

- Receive the ciphertext
- Decrypt the ciphertext using the Key1
- Get the message
- Encrypt message using Key2 and Key3 respectively
- Send each ciphertext

Bob:

- Receive the ciphertext
- Decrypt the ciphertext using the Key2
- Get the message

Tarou:

- Receive the ciphertext
- Decrypt the ciphertext using the Key3
- Get the message

Continue sending and receiving the messages

Demonstration of QKD-Based Secure Chat Room Application

Demonstration of The Single Chat Mode

Thank you for listening!