
QKD-Based Secure Chat Room Application

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

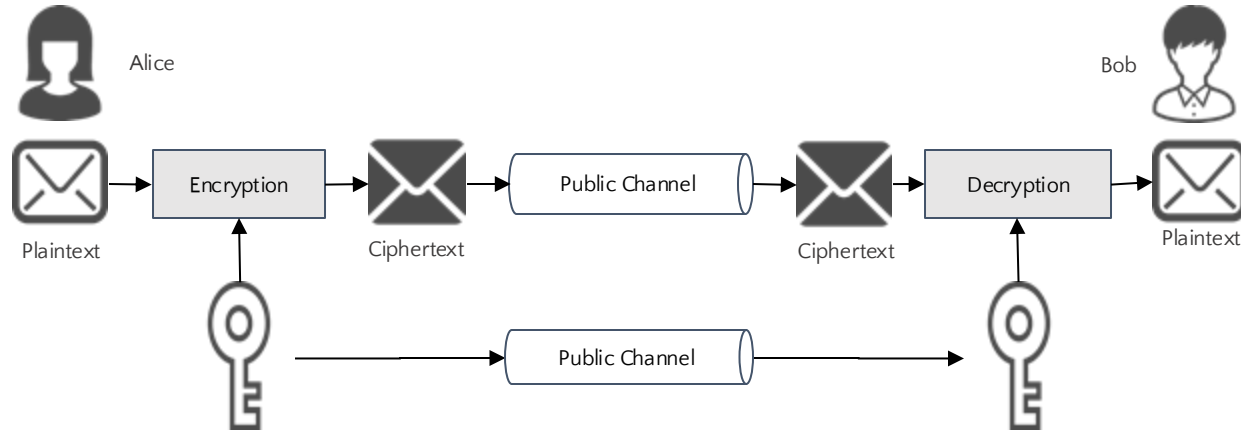
Outline

1. Background of QKD
2. Secure Chat Room Application
 - System Model of Secure Chat Room Application
 - Demonstration
 - Simulation Result of Key Generation

1. Background of QKD

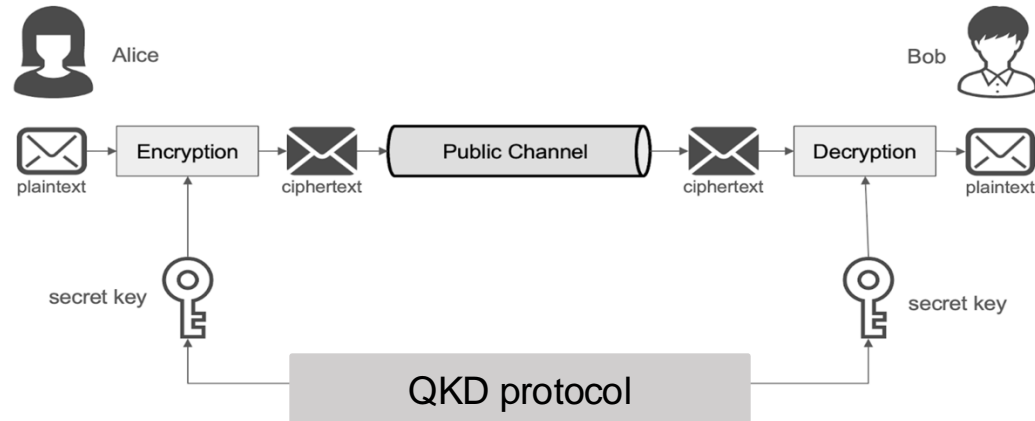
Introduction

- Recent years have seen the proliferation of the Internet, leading to widespread use of various services such as social media and email.
- Cybersecurity risks, including cyber attacks, have been on the rise. For example, traditionally, encryption keys have been exchanged over public channels.
- With the development of quantum computers, there is growing concern that conventional encryption techniques may be broken, thereby increasing the risk of key interception.
- Therefore, a secure key distribution method is becoming increasingly necessary.



QKD (Quantum Key Distribution)

- Quantum Key Distribution (QKD) is a method that utilizes the principles of quantum mechanics to securely generate and share secret key.
- It takes advantage of the fact that when a photon is disturbed, its state changes. This property allows for the detection of any eavesdropping by a third party.

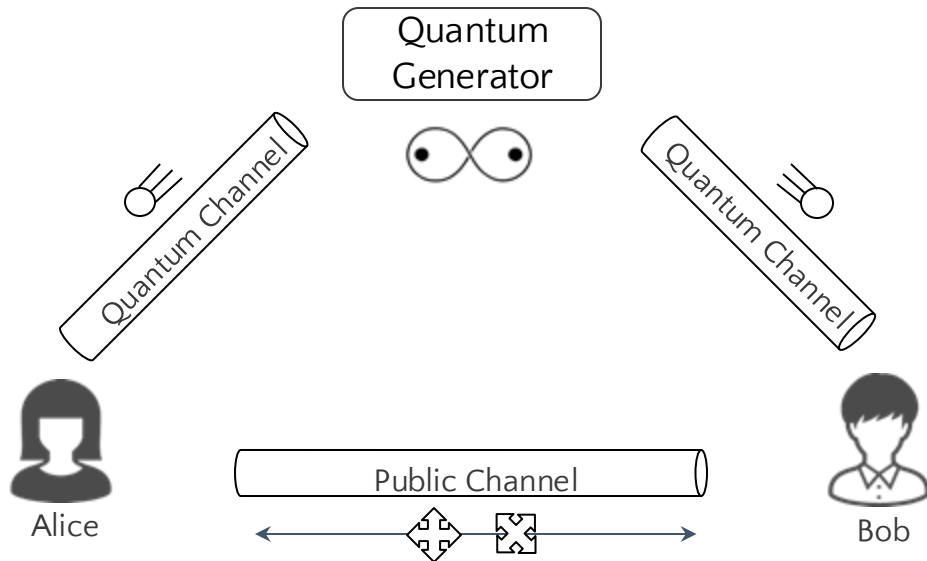


BBM92 Protocol

The BBM92 protocol uses the properties of quantum entanglement to securely generate and share keys.





- 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.

By sending photon pairs in quantum entangled states to Alice and Bob, respectively, there is a strong correlation between the results of both measurements.








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.

Basis \ Bit	0	1
+		
x		



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

System Model of BBM92 Protocol in Secure Chat Room Application

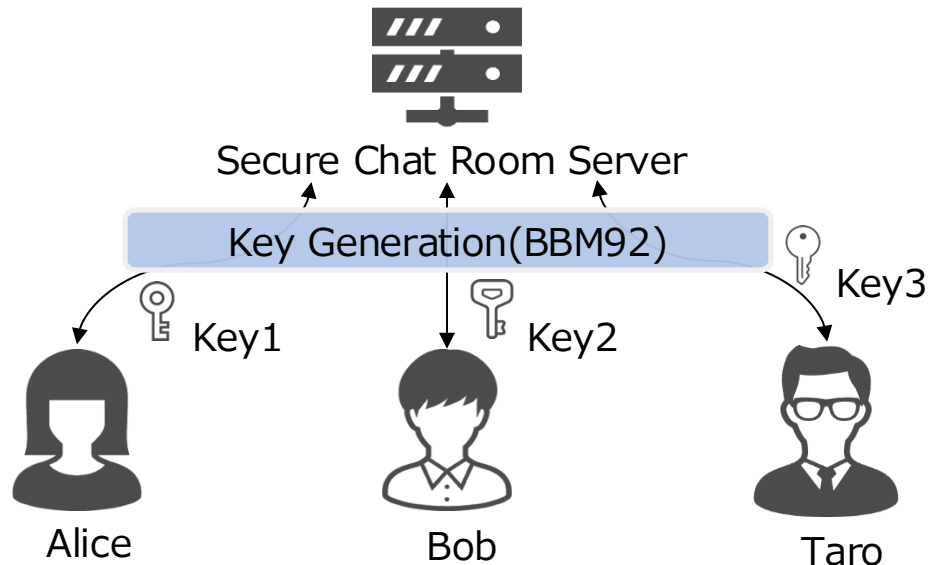
Development of QKD-Chat Application for Multiple Users using BBM92 Protocol

- 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.

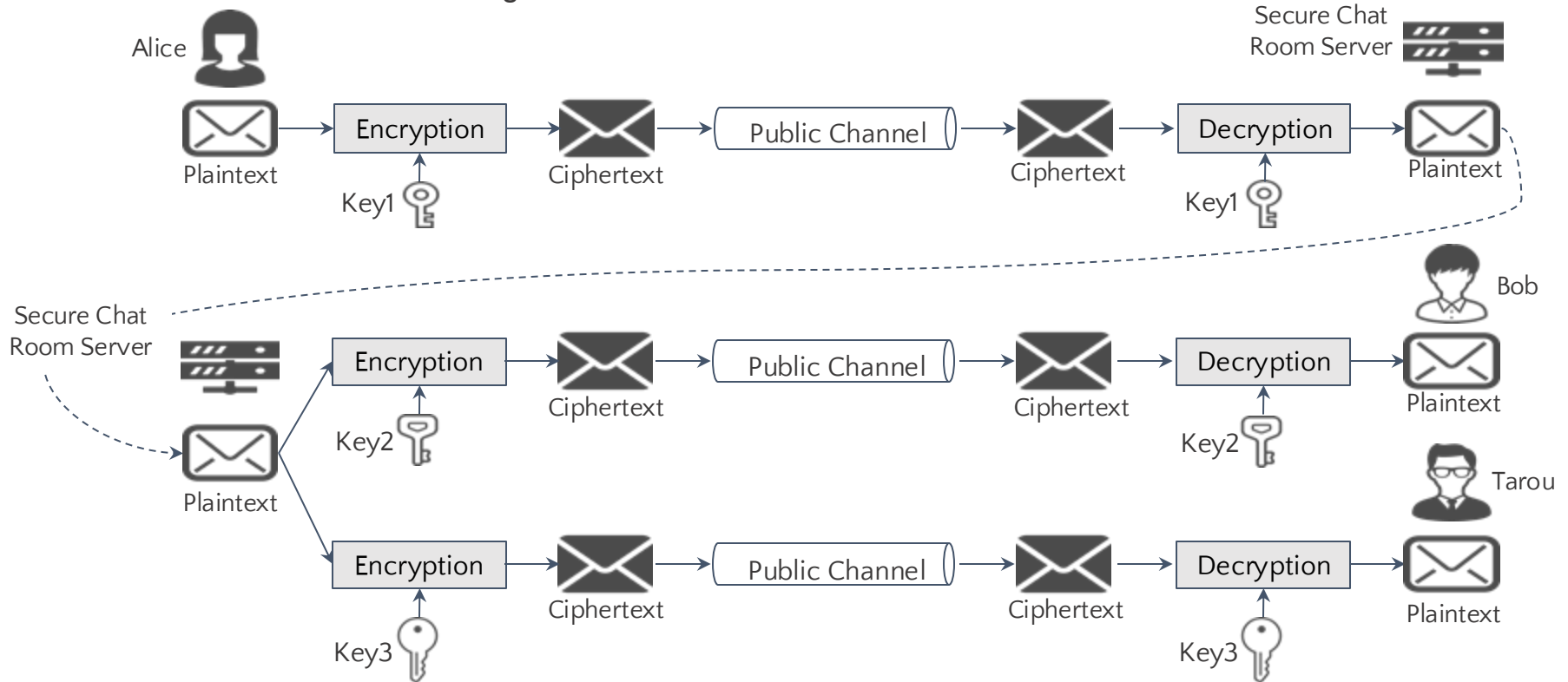
Generate the 168-bit key required for 3DES-CBC using the BBM92 protocol.

Assume three Chat Room participants



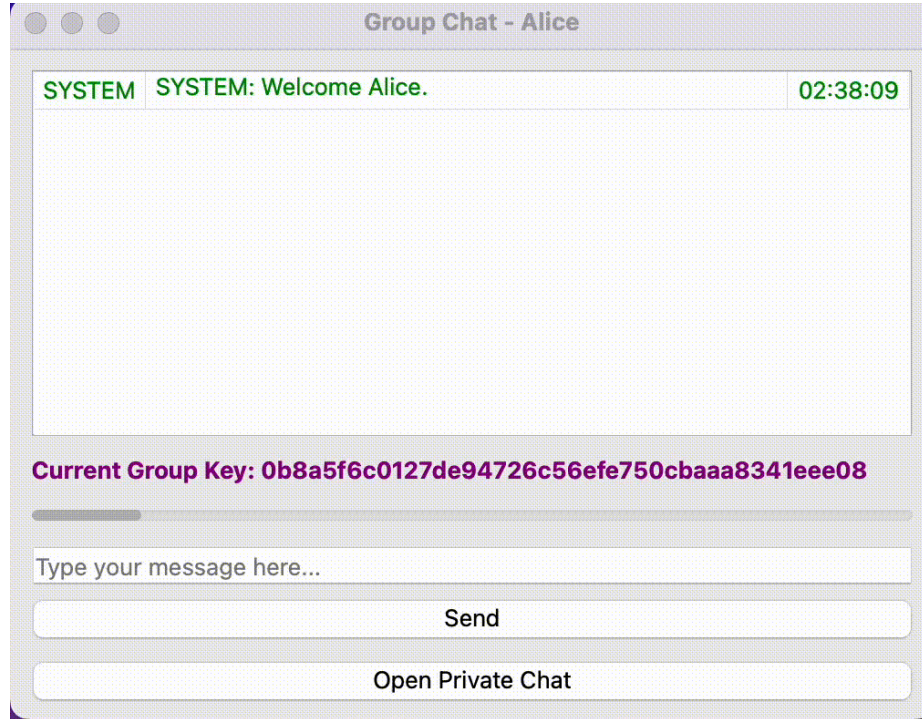
System Model for Sending and Receiving Messages in Secure Chat Room

Assume that Alice sends a message to Bob and Tarou



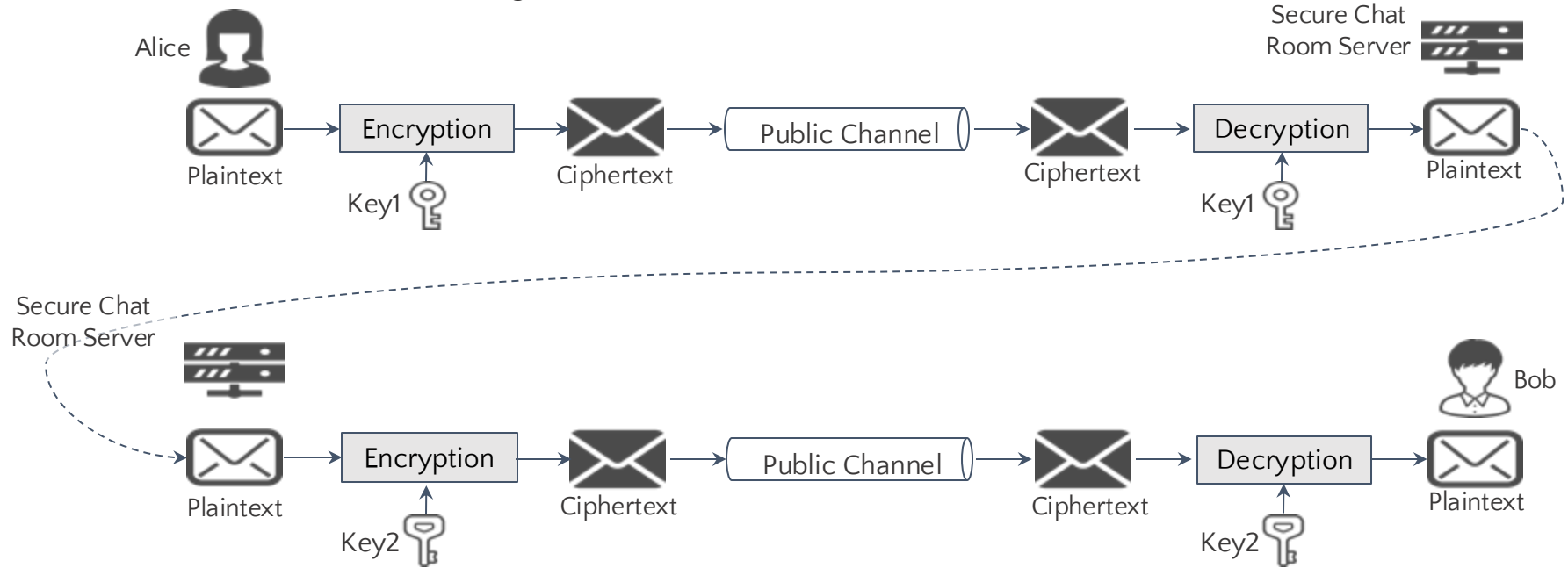
Demonstration of QKD-Based Secure Chat Room Application

Alice, Bob and Taro join the chat room.



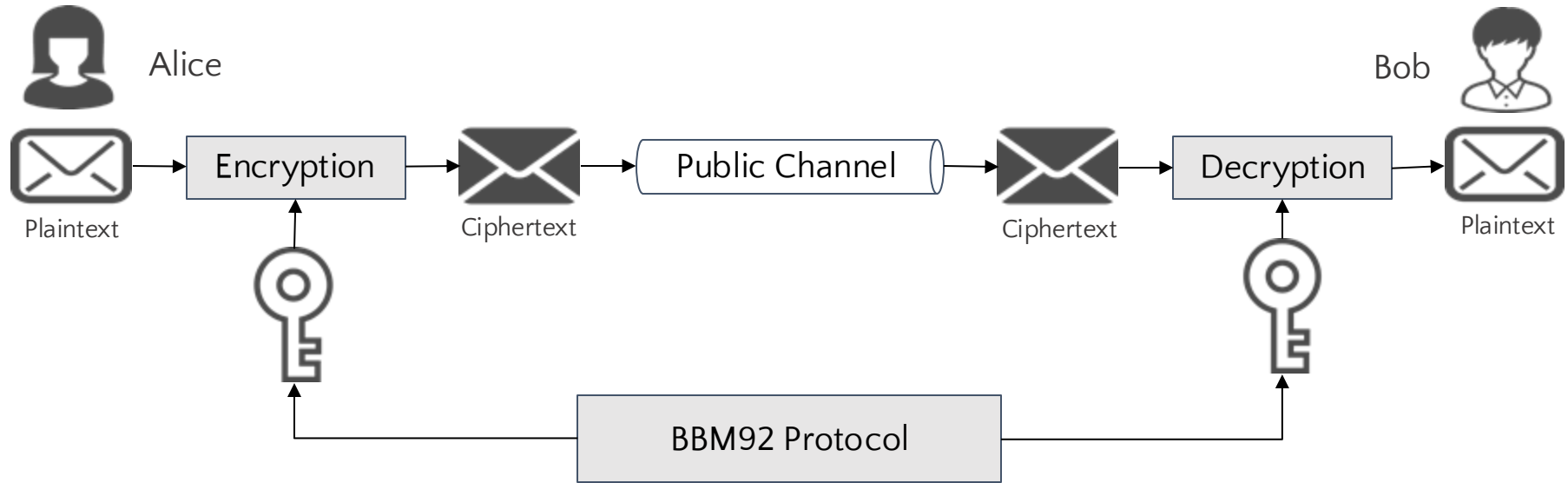
System model of Private Chat Mode at the Last Seminar

Assume that Alice sends a message to Bob



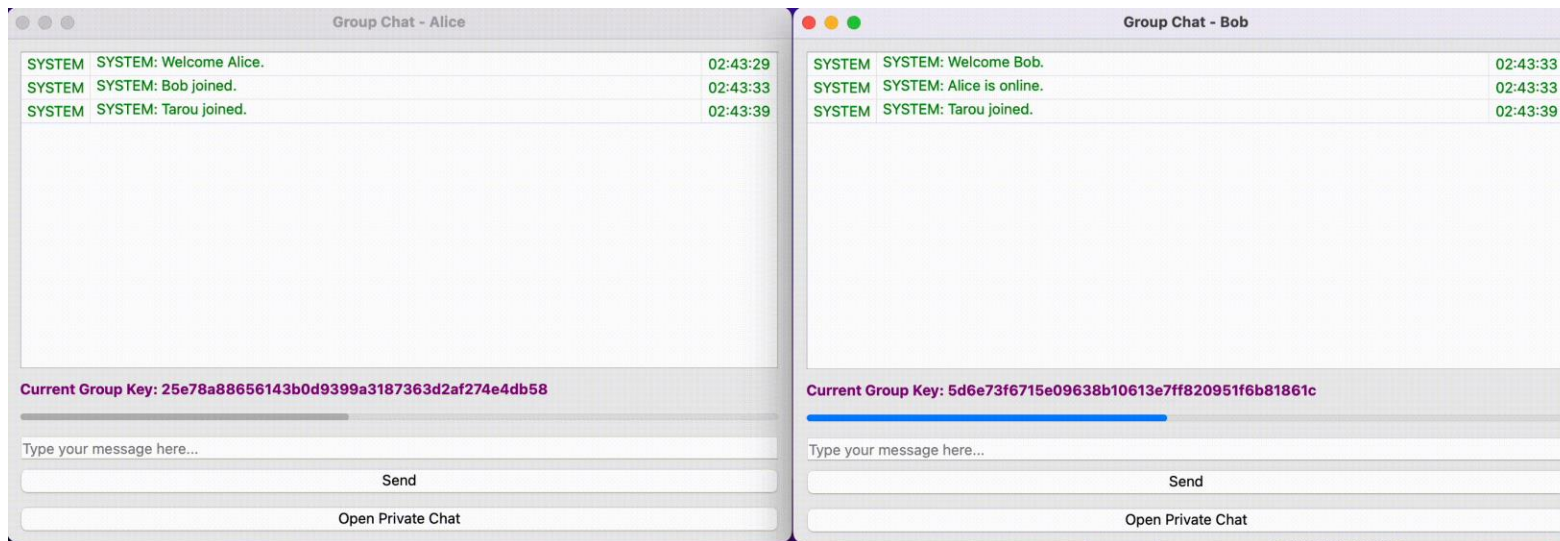
System model of Private Chat Mode

Assume that Alice sends a message to Bob

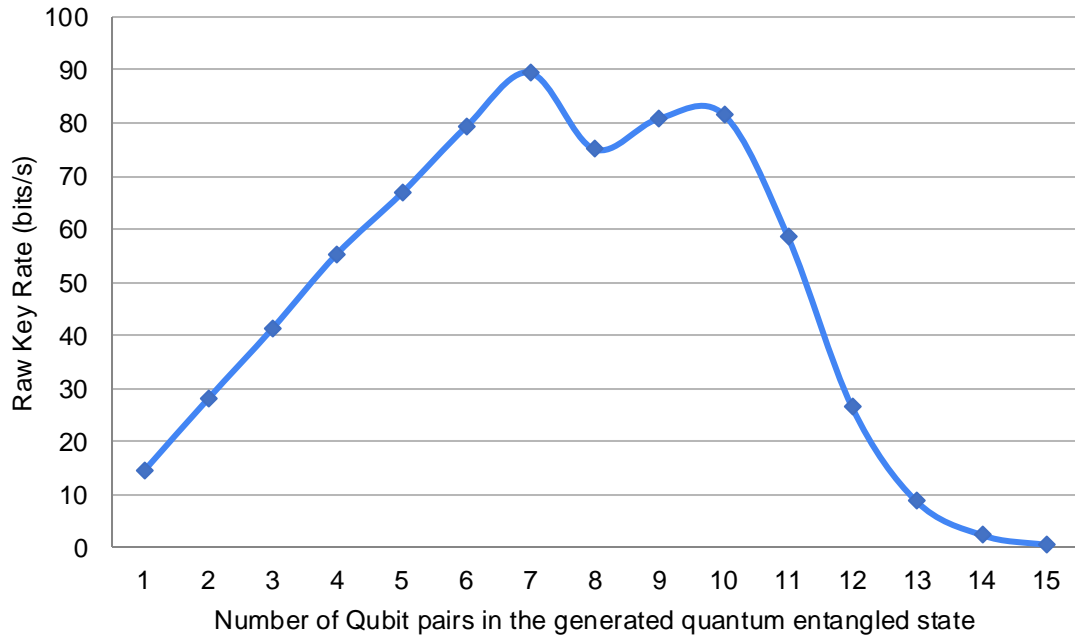


Demonstration of Private Chat Mode

Alice and Bob begin single chat.



Raw Key Rate for generating a 168-bit key



Thank you for listening!