Development of Secure Chat Application Based Quantum Key Distribution (QKD)

Takihara Yudai, Hoang D. Le, Anh T. Pham
Computer Communication Laboratory, The University of Aizu

Contents

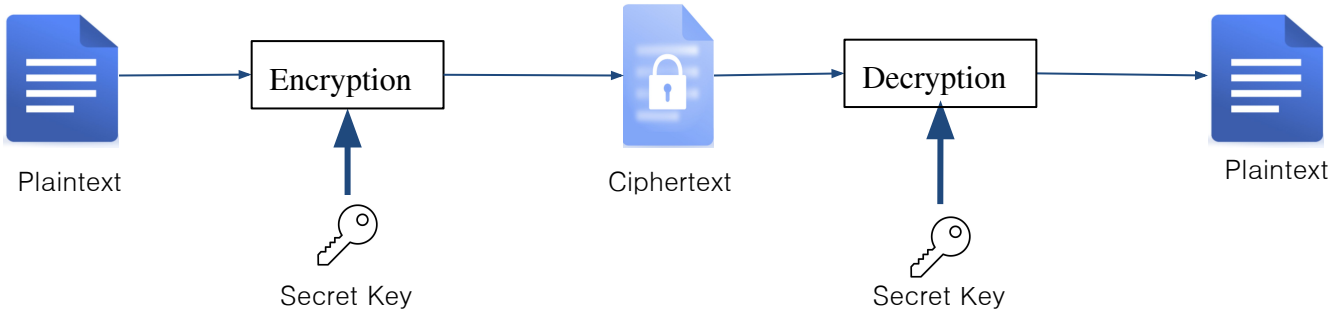
1
Background of QKD

1.1 Security of the Internet

A lot of people use many applications (SNS, Video Streaming, Shopping and Banking ….) on the Internet

>> A high level of security against eavesdropping and surveillance by attackers is required.

1.2. Existing solution

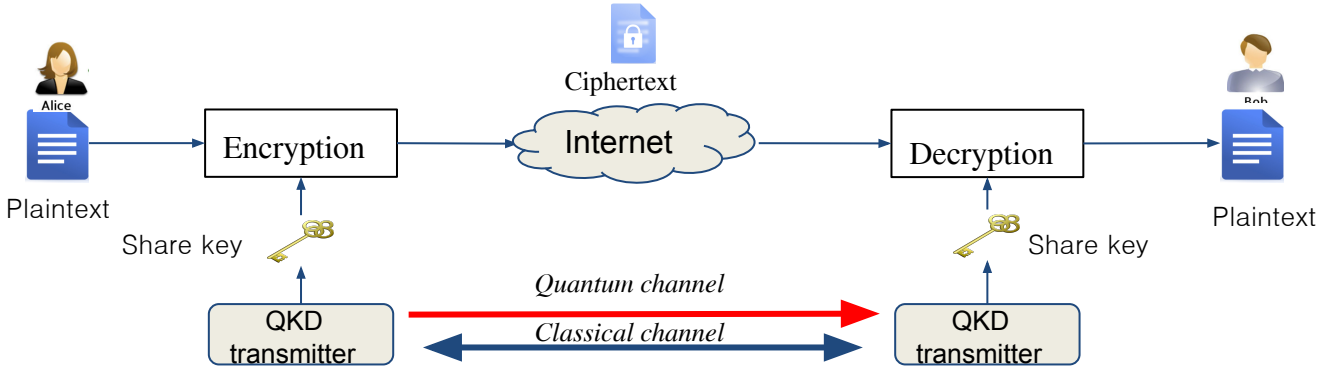


Symmetric Key Distribution is based on Public Key Cryptography(PKC)

However, PKC can be broken by ***Quantum Computers*** (with unusually fast processing speed)

➢ We should have a new Key Distribution System

1.3 Solution Quantum Key Distribution



- A secure communication method that implements a cryptographic protocol involving components of quantum mechanics.
- It enables two parties to produce the shared random secret key known only to them, which then used to encrypt and decrypt messages
- The ability of the legitimate two users to detect the presence of any third party trying to gain knowledge of the key.
- An example: ***BB84 protocol***

1.4 Our Focus: Secure Chat App Based QKD

We want to develop a secure chat application with QKD

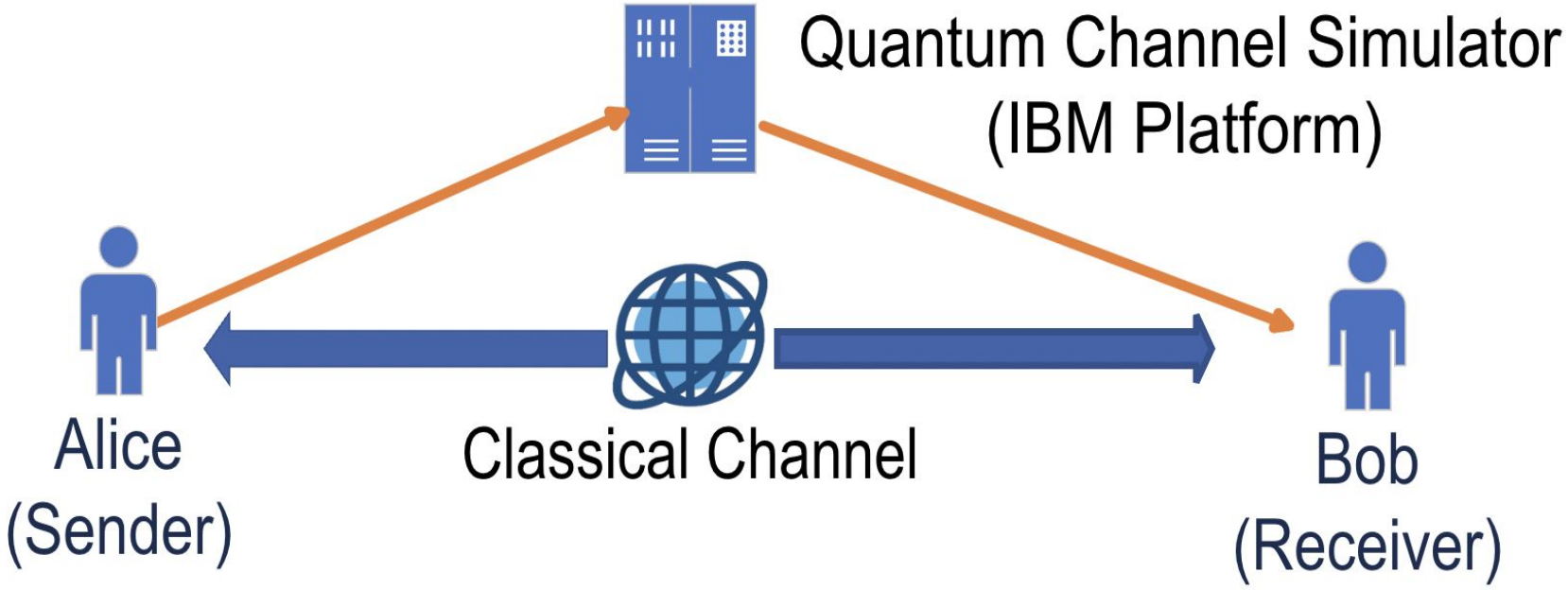
Key point of Chat Application based QKD

1. Simulate quantum states
   Tool that we use: Qiskit, a python library developed by IBM, used to develop chat apps using QKD.
   - ❏ Generate Qubit (the basic unit information for quantum computing.)

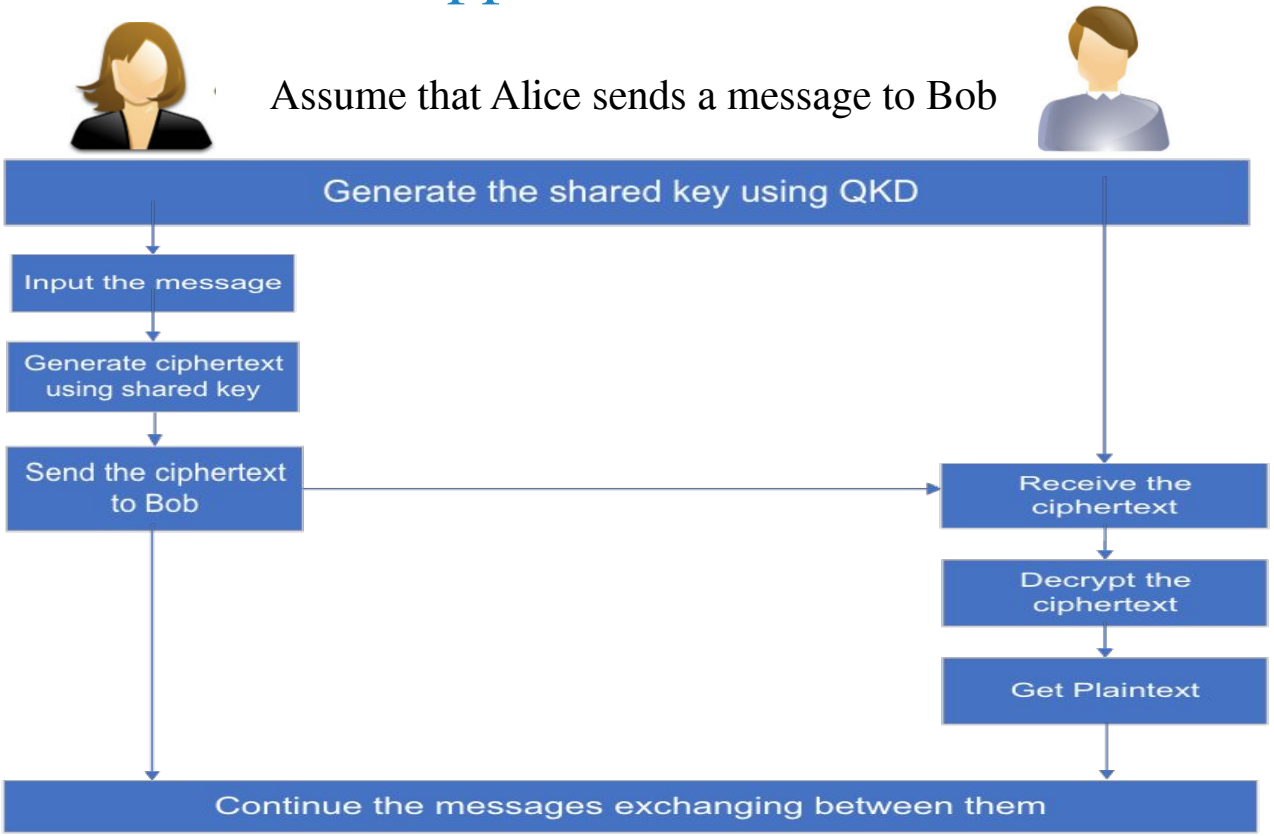
2. Implement a secure chat application
   At the sender, encrypt the text using **one-time pad (OTP)** with the shared key
   Decrypt the ciphertext at the receiver

2
System Description

2.1 QKD System model with IBM Platform



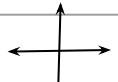
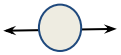
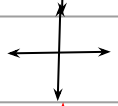
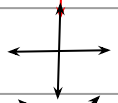
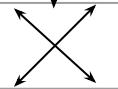
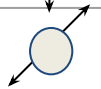
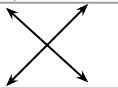
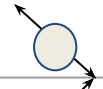
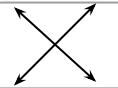
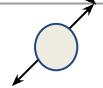
2.2 Flowchart of Chat Application

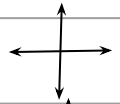
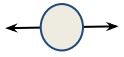
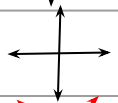
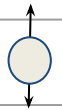
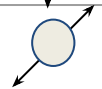
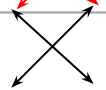
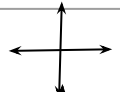
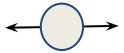
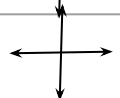
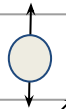
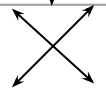
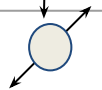


2.3 BB84 protocol

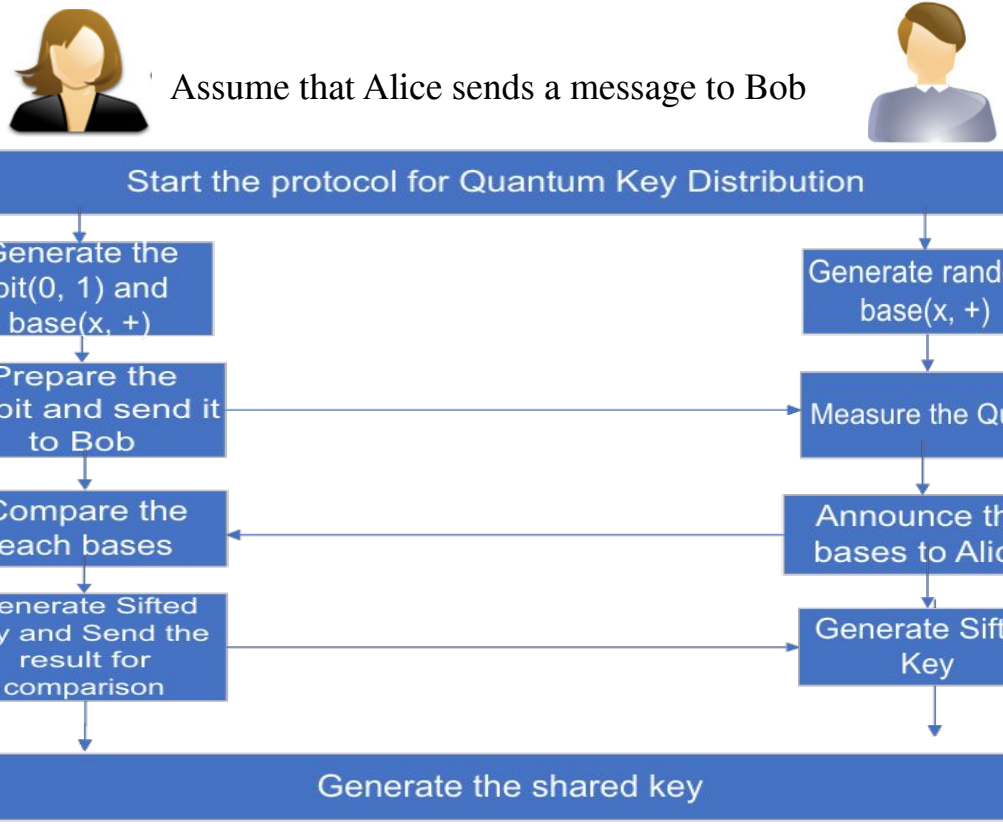
Alice

Bob

Bit	Base	Qubit State
0		
1		
0		
1		
0		
1		
0		

Base	State	outcome(bit)	sifted key
		0	0
		1	1
		0	*Bit is discarded*
		1	*Bit is discarded*
		0	*Bit is discarded*
		1	*Bit is discarded*
		0	0

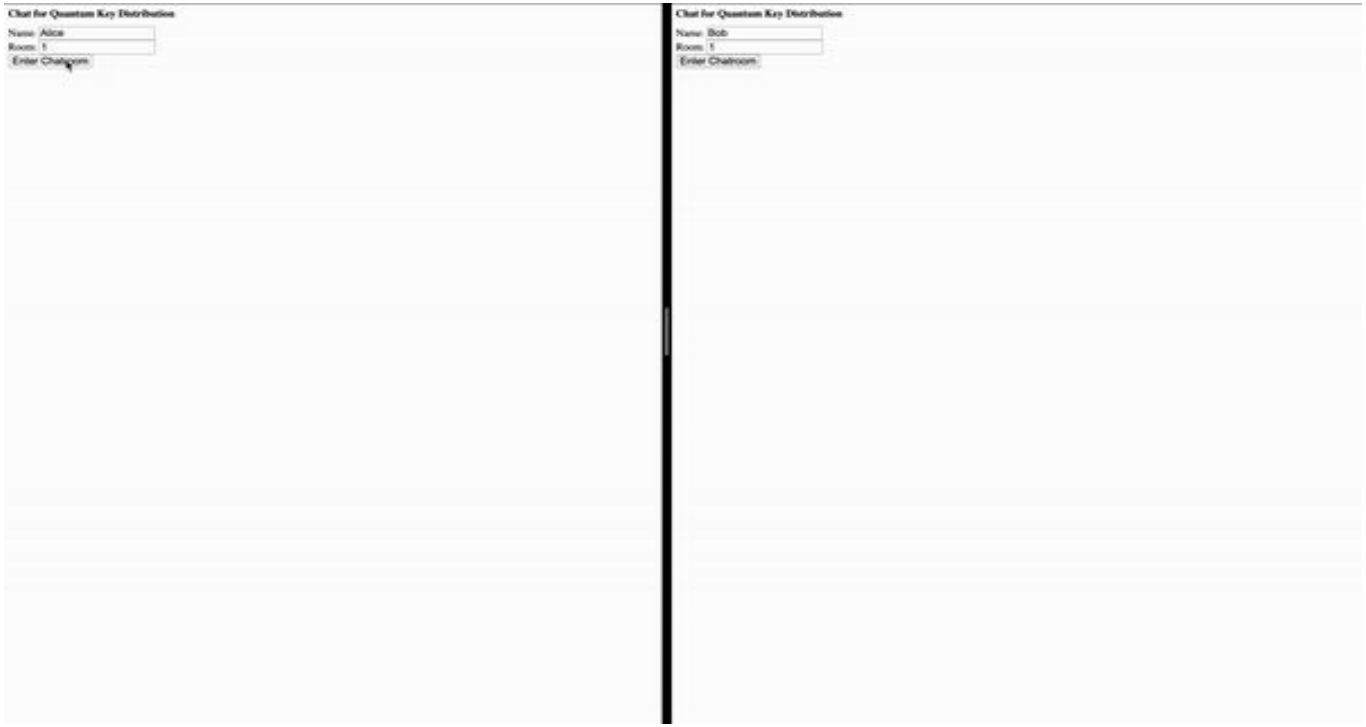
2.4 Flowchart of QKD



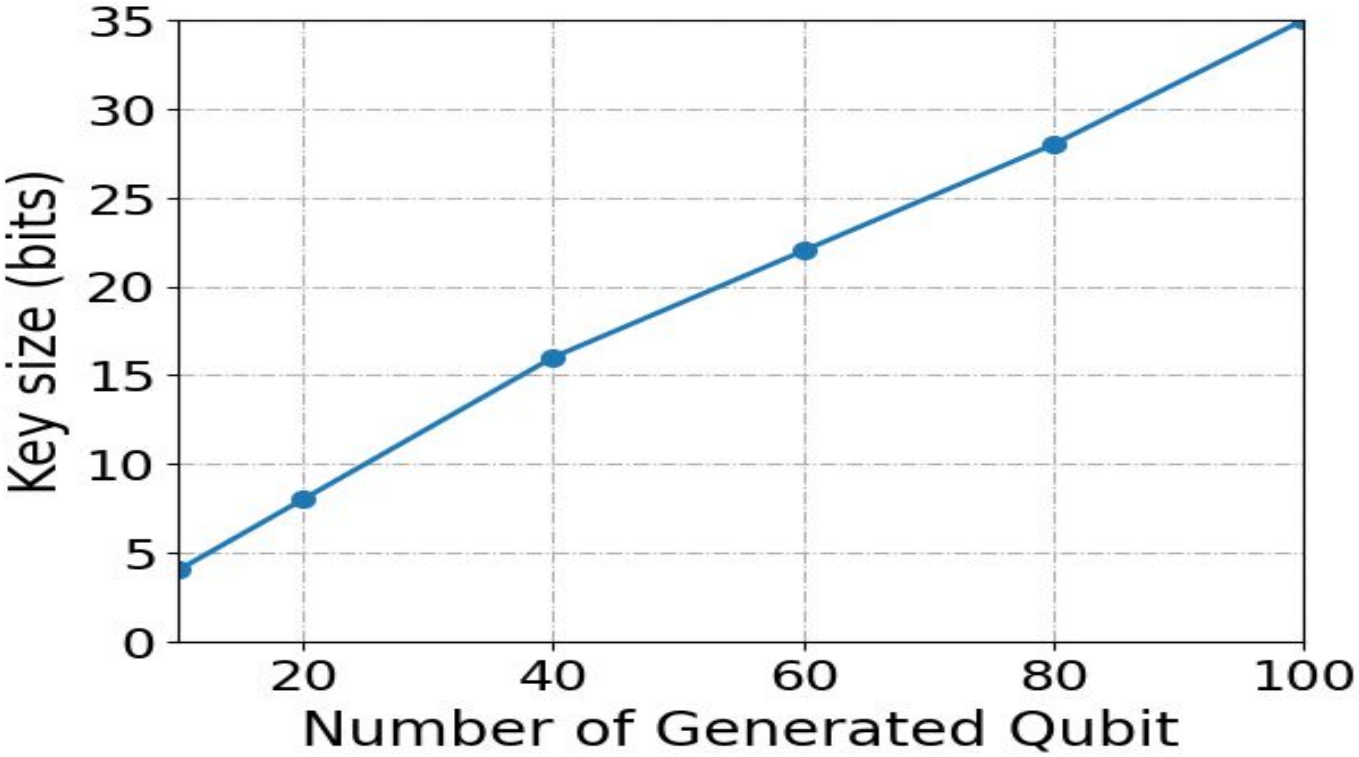
3

Demonstration

Demonstration of the chat application



Number of Generated Qubit vs Key size (bits)



Thank you for your attention!