



# BB84

## A Quantum Key Distribution Scheme

Mehul Sen  
CSCI - 464 Lightning Talk  
Friday 22nd October 2021

# Quantum Key Distribution (QKD)

QKD is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key, which can then be used to encrypt and decrypt messages.

Note: This is often incorrectly called Quantum Cryptography which is the science of exploiting quantum mechanical properties to perform cryptographic tasks. QKD is the best-known example of a Quantum Cryptographic task.

Example: Alice and Bob come up with a common secret key which they can use to encrypt and decrypt the files shared among each other.

# NIST - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3		Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

# BB84

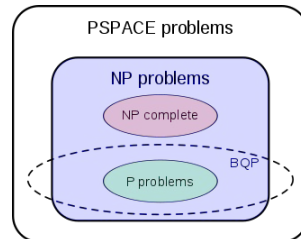
Developed by Charles **B**ennett and Gilles **B**rassard in 1984, it is the first quantum cryptography protocol and is provably secure.

To maintain its security, it relies on two principles of quantum mechanics:

- Heisenberg's Uncertainty Principle : we cannot know both the position and momentum of a particle at quantum level, it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. (No-Cloning Theorem)
- Entanglement : Quantum particles are not always independent of each other and can be entangled, when you measure one particle, the superposition of the other instantly collapses.

It has a complexity of BQP (Bounded-error quantum polynomial time) which is the class of decision problems solvable by a quantum computer in polynomial time.

$$P \subseteq BPP \subseteq BQP \subseteq AWPP \subseteq PP \subseteq PSPACE \subseteq EXP$$



# Quantum Channel

A quantum channel is a communication channel which can transmit quantum information such as the state of qubit.

There are 4 potential qubit states (as covered in class)





$$|\psi_{00}\rangle = |0\rangle,$$

$$|\psi_{10}\rangle = |1\rangle,$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

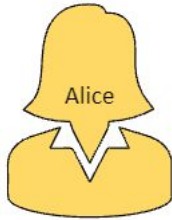
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

BB84 uses pairs of orthogonal states known as Basis:

Basis		0	1
Rectilinear	<b>+</b>		
Diagonal	<b>×</b>		

# BB84 Protocol

- Step 1: Alice chooses a random string of bits.  
Step 2: Alice chooses a random basis to encode each bit with.  
Step 3: Alice encodes the bits using the chosen basis and sends qubit states to Bob through a Quantum Channel

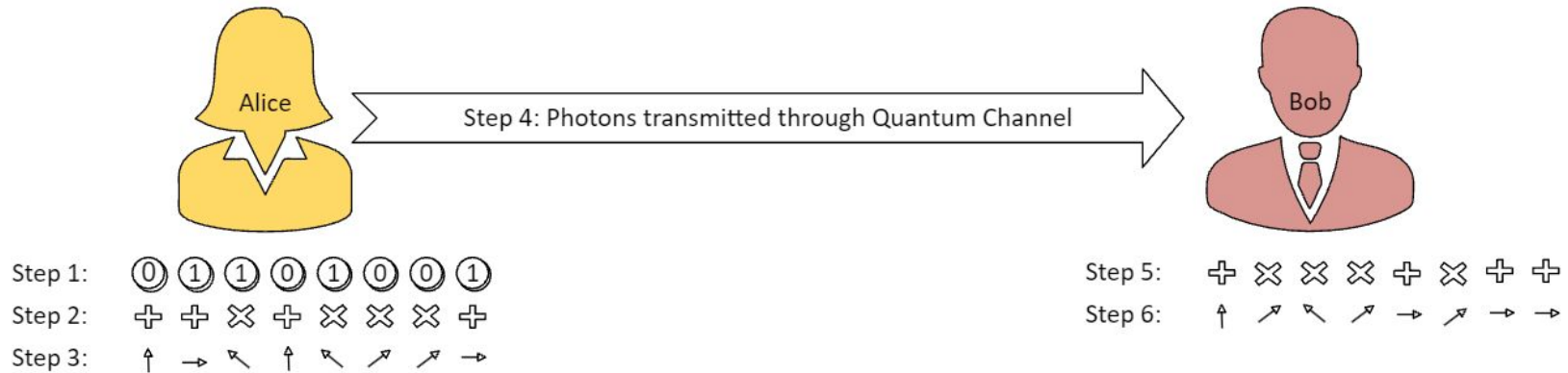


Step 1:	0	1	1	0	1	0	0	1
Step 2:	+	+	×	+	×	×	×	+
Step 3:	↑	→	↖	↑	↖	↗	↗	→

# BB84 Protocol Continued

1

- Step 4: Bob receives the qubit states through the common quantum channel  
Step 5: Bob chooses a random basis to encode each receiving qubit state with.  
Step 6: Bob measures the polarization of the received qubit states.

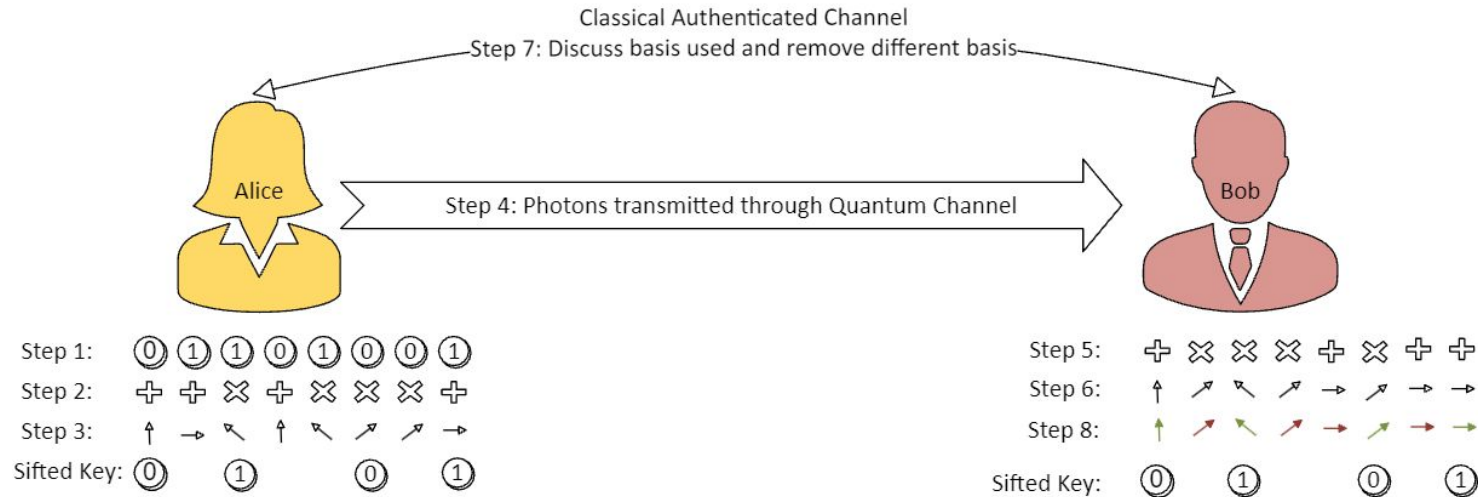


# BB84 Protocol Continued

2

Step 7: After receiving the qubit states, Bob and Alice discuss their chosen basis over a classical channel, removing the different basis.

Step 8: Resulting shared secret is the **Sifted Key** which they can be used to encrypt and decrypt data.





# Security of BB84

Each randomly chosen basis by Bob has a 50% likelihood of being correct and 50% likelihood of being incorrect. The size of the sifted key would be roughly half of the initially used bits.

In the event that Eve tries to intercept the quantum channel between Alice and Bob, since she cannot make identical copies of the qubits, she would have to communicate individually with Alice, and then with Bob. This would mean that Bob's likelihood of choosing the same basis as Alice will be reduced to 25% with the probability of being incorrect becoming 75%. With this they can easily detect if their communication is being intercepted.

One drawback for BB84 is that the bits chosen by Alice have to be random, if not, Eve is able to imitate Alice and successfully conduct a MITM attack.

# References

[https://en.wikipedia.org/wiki/Quantum key distribution](https://en.wikipedia.org/wiki/Quantum_key_distribution)

[https://csrc.nist.gov/csrc/media/publications/nistir/8105/final/documents/nistir\\_8105\\_draft.pdf](https://csrc.nist.gov/csrc/media/publications/nistir/8105/final/documents/nistir_8105_draft.pdf)

<https://en.wikipedia.org/wiki/BB84>

<https://youtu.be/44G9UuB2RWI>

<https://cryptography.fandom.com/wiki/BB84>



# Questions?