eman ta zabal zazu

Universidad del País Vasco Euskal Herriko Unibertsitatea

UNIVERSIDAD DEL PAÍS VASCO
FACULTAD DE INFORMÁTICA

Practical work

BB84 algorithm

Justinas Bliujus

jbliujus001@ikasle.ehu.eus

2025

Contents

1. FIRST SECTION

1.1. The task

The task is to understand what the BB84 algorithm achieves, how it works and implementing it in Qiskit.

1.2. The algorithm principles

The algorithm tries to solve the following problem: how do you securely share the key in advance.

BB84 quantum protocol is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984.

The classical example involves Alice and Bob sharing information. Protocol requires one qubit at a time. Let’s say Alice creates two random classical bits a and b. Alice uses them to perform transformations on the qubit as shown in Figure 1.

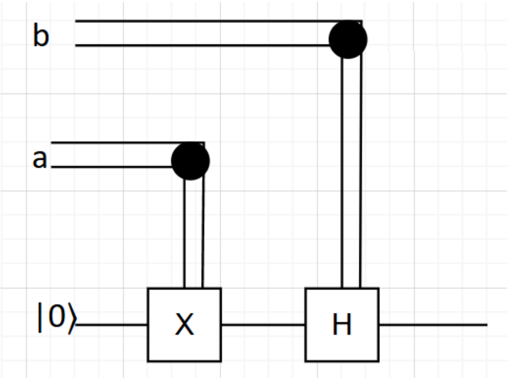


Figure 1

The bit a is used to control Pauli-X gate, meaning if a = 1 the gate is applied, otherwise it is not applied. Another bit b is used to control Hadamard gate. If b = 1, Hadamard is applied, otherwise it is not applied.

After applying the two control operations, the qubit state can have four possibilities as in Table 1:

Table 1

a	b	$|\psi\rangle$
0	0	$|0\rangle$
0	1	$|+\rangle$
1	0	$|1\rangle$
1	1	$|-\rangle$

Then, Alice sends the qubit to Bob. Bob also creates a random bit, let’s call it b’. Bob uses b’ to control another Hadamard gate (Figure 2), which increases the number of possibilities to eight (Table 2).

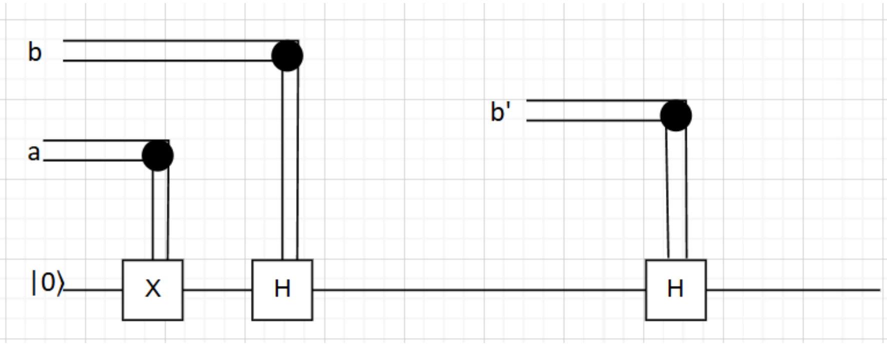


Figure 2

Table 2

a	b	b’	|ψ’⟩
0	0	0	|0⟩
0	0	1	|+⟩
0	1	0	|+⟩
0	1	1	|0⟩
1	0	0	|1⟩
1	0	1	|–⟩
1	1	0	|–⟩
1	1	1	|1⟩

Then Bob performs a measurement in standard basis as shown in Figure 3.

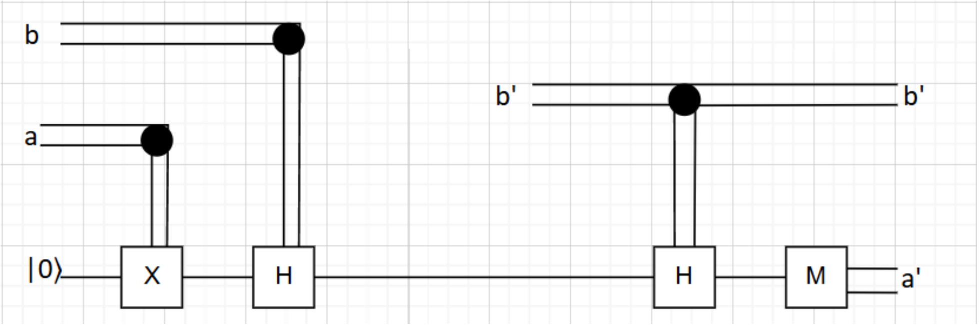


Figure 3

The outcome of the measurement is 0 or 1, which is a classical bit. Then Bob announces that he measured the qubit. Then Alice sends over classical bit b to Bob, so that Bob could compare b to his b’ (Figure 4) and announces to Alice if they are equal or not. This part is not confidential.

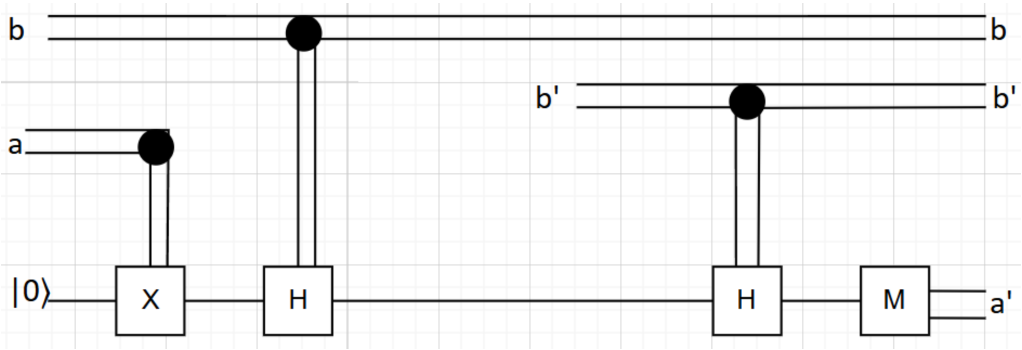


Figure 4

Whenever b and b' are equal, the state of the qubit is identical with the classical bit a. So, when Bob measures the qubit in the standard basis, it is guaranteed that a' is identical to a of Alice. Because of this Alice and Bob can ignore the cases where b and b' are different. The remaining four possibilities are as follows in Table 3.

Table 3

a	b	b'	|ψ'⟩
0	0	0	|0⟩
0	1	1	|0⟩
1	0	0	|1⟩
1	1	1	|1⟩

Meaning if their b and b' are equal, their a and a' are also equal. They use this as one bit in their shared key. They repeat this multiple times. In the end they should have identical keys.

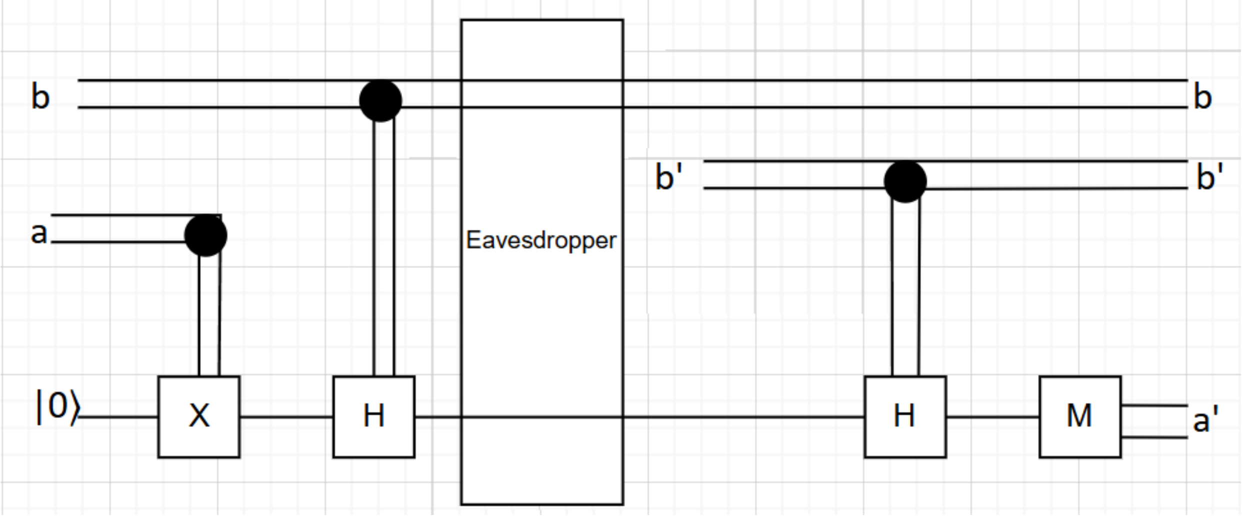
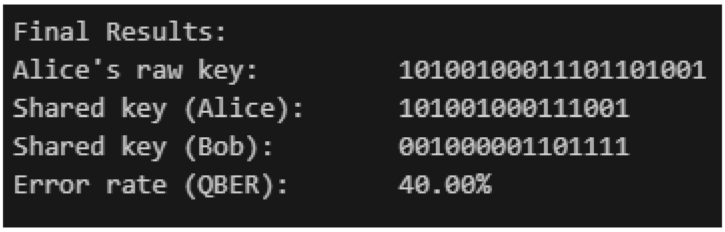


Figure 5

If in between there is an eavesdropper (Figure 5): to extract information, the eavesdropper would have to perform a measurement on the qubit. It changes the quantum state. He could try measuring in the suitable basis, but he cannot always do that, because there are four possible states |+⟩, |−⟩, |1⟩, |0⟩. For example, if he measures in the standard basis, but the qubit is in the plus or minus state, the state of the qubit is disturbed. Since transformations on the side of Alice are random, there is always disturbance if there is an eavesdropper and then it is no longer true that if b is equal to b’, a will also be equal to a’. To secure the communication Alice and Bob create the shared key. They make it sufficiently long, then take a sample of certain digits to compare. If compared digits are different, it is evidence of a presence of an eavesdropper, and they can stop communicating to not give out information.

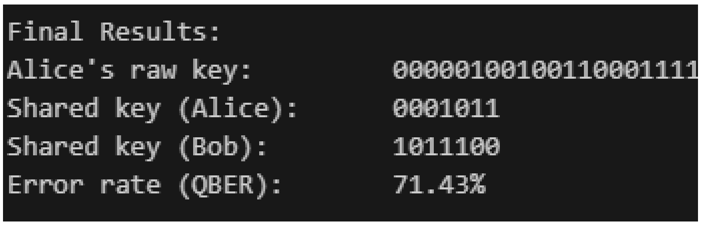
1.3. Simulating the algorithm

The algorithm was implemented in python and using Qiskit, according to the algorithm principles explored earlier. Running the simulation 5 times with the eavesdropper being present, while transmitting 20 qubits gives following results as shown in Figure 6 to Figure 10:



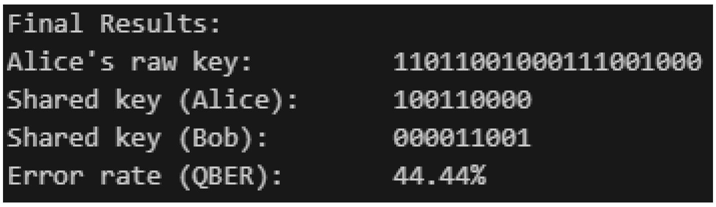
```
Final Results:
Alice's raw key:        10100100011101101001
Shared key (Alice):     101001000111001
Shared key (Bob):       001000001101111
Error rate (QBER):      40.00%
```

Figure 6



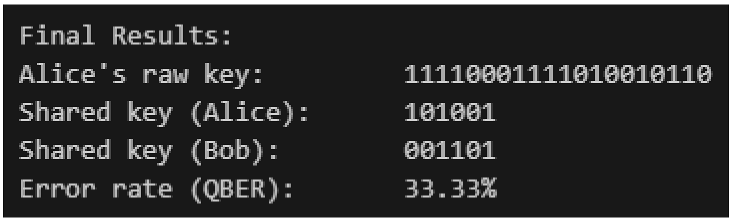
```
Final Results:
Alice's raw key:        00000100100110001111
Shared key (Alice):     0001011
Shared key (Bob):       1011100
Error rate (QBER):      71.43%
```

Figure 7



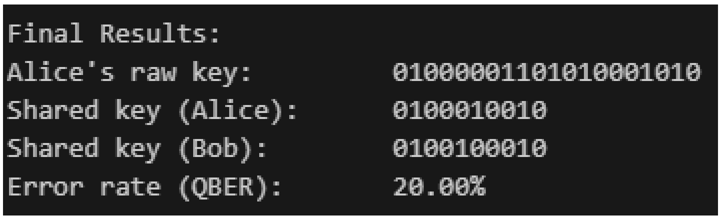
```
Final Results:
Alice's raw key:        11011001000111001000
Shared key (Alice):     100110000
Shared key (Bob):       000011001
Error rate (QBER):      44.44%
```

Figure 8



```
Final Results:
Alice's raw key:        11110001111010010110
Shared key (Alice):     101001
Shared key (Bob):       001101
Error rate (QBER):      33.33%
```

Figure 9



```
Final Results:
Alice's raw key:        01000001101010001010
Shared key (Alice):     0100010010
Shared key (Bob):       0100100010
Error rate (QBER):      20.00%
```

Figure 10

We have chosen the threshold of the noise as 11%. The Minimum disturbance detected was 20%. Meaning every time eavesdropper was detected.

1.4. Conclusions

The BB84 protocol successfully demonstrates how quantum mechanics can be used to establish a secure key between two parties while detecting any eavesdropping attempts. The key takeaway from the simulation and theoretical analysis are as follows:

- The protocol enables Alice and Bob to share an identical key without prior exchange of a secure channel. The randomness of quantum states ensures security.
- Any attempt by an eavesdropper to measure the qubits inevitably disturbs their state, leading to detectable changes in the shared key. This fundamental principle of quantum mechanics ensures that Alice and Bob can verify whether their communication has been compromised.
- By setting a threshold for acceptable errors (11% in the simulation), Alice and Bob can decide whether to proceed with the key or discard it due to potential eavesdropping. In the simulation, the eavesdropper was detected in all five runs, confirming the effectiveness of this detection method.
- Practical Implications – BB84 provides the idea that quantum key distribution could be an alternative to classical encryption methods in securing communications.

1.5. References

Asif, Quantum Key Distribution and BB84 Protocol, 2021, *Medium*. https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5

Improbable Matter, BB84 Quantum Key Distribution Protocol, 2021, *YouTube*. https://www.youtube.com/watch?v=V3WzH2up7Os&t=603s

Attachment 1. Code implementation.

https://github.com/JustinasBliujus/BB84