Quantum Key Distribution

Description:

Quantum key distribution (QKD) aims to distribute a key to two parties across an unsecured channel. We can use this protocol to detect if an eavesdropper has tried to read communications between the parties, with a good probability if long messages are sent.

[A step-by-step guide can be found here with a more detailed description:](https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html)

1. Alice generates a random array of bits.
2. Alice generates a random array of basis.
3. Alice encodes the bits using the generated basis into qubits.
4. Alice sends the encoded qubits to bob across the unsecured channel.
5. Bob generates a random array of basis.
6. Bob decodes (measures) the qubits using the random basis he generated.
7. Alice and Bob share the basis they used.
8. Where the bits in pair of basis matches, we keep the (decoded for Bob or original for Alice) value of the key.
9. We share a sample of this key across the unsecured channel, if they match and they are of a good length, it is unlikely that anyone has copied the key.

Why this works:

If Eve – an eavesdropper – tries to copy or measure the encoded qubits, she will have to also use a randomly generated array of basis.

A fundamental rule of quantum computing is that we cannot copy a qubit that is in an arbitrary quantum state. In other words, to be able to copy a qubit, we need to have prior knowledge on the state of the qubit, which Eve does not have.

Eve also cannot measure the qubits and send them over to Bob, as the qubits are encoded in different basis, and if we try to measure a qubit using the wrong basis, we will collapse the superposition. Changing the state of the qubits that arrive to Bob.

Properties that I have tested (same order they appear in the code):

* Alice’s randomly generated message is an array of 1’s and 0’s
* Alice’s randomly generated message is equal to the length specified, in the parameter for the function
* The length of the encoded message (array of encoded qubits) is the same length as the array of bits/basis to encode
* The encoded message array contains objects of type QuantumCircuit
* The encoded message array does not contain QuantumCircuits that have more than 3 quantum gates in them
* The encoded message array does not contain QuantumCircuits that use gates other than Barrier, X and H
* A message that has been decoded is the same length as the encoded message array/original random bit array/basis
* A message that has been decoded (measured) is an array of 1’s and 0’s
* An encoded message that is decoded with the same basis array that it was encoded by, should return an array of the exact original bits that were used to encode the array.
* Two encoded messages, decoded with their original basis are return equal outputs
* The output key length with never be larger than length of original bits
* The two generated keys should be equal
* The Keys that have been generated at the end is an array of 1’s and 0’s