Quantum distribution key (E91 Protocol)

The important principle on which QKD is based Is the principle of quantum entanglement. It is possible for two particles to become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observation over a classical channel.

The process of communication using entangled states, aided by a classical information channel, is known as quantum teleportation and is the basis of Ekert's protocol.

Let us now go through the procedure of the quantum E91 protocol in the following steps: -

1. Trusted third party that generates quantum particles (Photons), or a channel consisting of a source that emits pairs of spin half particles, in a singlet state.
2. Quantum particles or Qubits should be in Bell state which is:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

3. The Entangled qubits should reach the legitimate users of the channel, say, Alice and Bob.
4. They both perform a random basis, which can be (X and Z gates); to measure their entangled qubits.
5. They record the result of each measurement and use a classical channel to communicate which bases they used (without disclosing the outcomes).

Alice & Bob bits	0	1	1	0	0	0	1	1
Alice Measurement	X	X	Z	Z	X	Z	Z	X
Bob Measurement	X	Z	Z	X	X	X	Z	Z
Different Bases		❌		❌		❌		❌
Shared key	0		1		0		1	

6. They divide the measurement results into two groups:
   1) Where they choose **different** measurement bases.
   2) where they choose the **same** measurement bases, which will be **Shared key**.

   The first group is used to detect whether there is an eavesdropping, by using the correlation coefficient between Alice's bases and Bob's.

   The CHSH inequality is used to experimentally prove Bell's theorem. This theorem asserts that local hidden variable theories cannot account for some consequences of entanglement in quantum mechanics.

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b').$$

Now for $\{|S|<=2\}$ ➡ The Inequality is not violated; therefore, Interception from the adversary.
And for $\{2<|S|<=2\sqrt{2}\}$ ➡ The Inequality Is violated; therefore, no interception, sharing an entangled state, and safe to proceed.

7. After knowing the quantum channel is safe using the first group in step 6, the second group is now can be trusted as key, which in example above is (0101).