1. Alice chooses a sequence of $(4+\delta)n$ uniformly random information bits $a = (a_i)$ and a sequence of $(4+\delta)n$ instruction bits $b = (b_i)$.
2. Alice encodes a_i using states $|0\rangle$ and $|1\rangle$ if $b_i = 0$, and using states $|+\rangle$ and $|-\rangle$ if $b_i = 1$, and sends them to Bob.
3. Bob chooses a sequence of $(4+\delta)n$ uniformly random decoding bits $c = (c_i)$ and measures the received qubits in the base $\{|0\rangle, |1\rangle\}$, if $c_i = 0$, and in the base $\{|+\rangle, |-\rangle\}$, if $c_i = 1$.
4. Bob then publishes the sequence c and Alice publishes the sequence b.
5. Alice and Bob choose $2n$ indexes for which $b_i = c_i$, and for which the value measured by Bob should be a_i. There are enough such indexes with a high probability controlled by the number δ.
6. Uniformly randomly, Alice and Bob then choose half of these indexes to publicly verify that they are really equal. This gives them an idea of the degree of distortion that can be expected

7. If the expected violation rate is acceptable, they use the remaining bits as a shared key (they can correct the corrupted bits using a self-correcting code mechanism).

DENSITY

$\cancel{\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle}$

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

~~PURE~~

MIXED

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|+\rangle\langle +| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$|-\rangle\langle -| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

PROB →

$$C_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}$$

$$C_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} 3/4 & -1/4 \\ -1/4 & 1/4 \end{pmatrix}$$