3) For all $k \in \{1, \ldots, (4+\delta)n\}$, Alice sends the data bit s_k encoded in the basis b_k to Bob.

4) Bob selects for each incoming photon a basis from the set $\{\boxplus, \boxtimes\}$, independently and uniformly at random, and measures the photon in that basis. He records the basis that he has chosen and the measurement outcome.

5) Alice publicly announces the string b.

6) Alice and Bob discard all bits from s where Bob measured in the wrong basis. With high probability, there are at least $2n$ bits left. They repeat the protocol if that is not the case. They keep $2n$ bits.