Protocol BB84. The goal of this protocol is to establish a common secret of n bits between Alice and Bob.

1) Alice chooses a data string s of $(4+\delta)n$ bits that are independently selected uniformly at random.

2) Alice chooses a string b of $(4+\delta)n$ symbols over the alphabet $\{\boxplus, \boxtimes\}$ that are independently selected uniformly at random.