



* s is a random scalar of size about 376-bit in the experiment