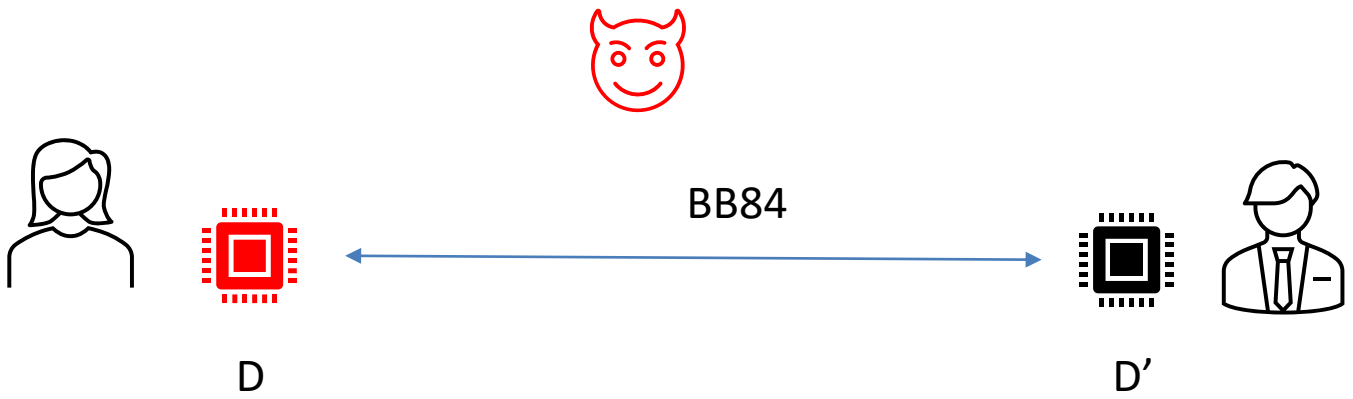
Devices D and D’ implement the BB84 communication protocol. Alice is holding D while Bob is holding D' and they execute the protocol.

Assume that the random number generator (conventional one) used by D is poor so that you may guess its output with probability 2^{-20}. The generator of D' is of the best quality.

Discuss the consequences for the security of the connection: what are the real opportunities for the attacker?



Again, be creative!
Deadline 28.12.22. Submit your solution over MS Teams