Question

1:What kind of information that leaked from Cryptographic Devices can be utilized to apply side-channel attack?(list at least 3)

2.In what situation you would choose SPA to attack? And how about DPA?

3.Take the AES-128 algorithm as an example, the key size is 128bit(16bytes K_{i},i=1~16)
Then use DPA to attack AES-128, how many tests do you need for per K_i? And what’s the total number of tests to recover the whole 128bit key?