

Notations:

p - Number PT or CT blocks of length 64 bits each

