

Notations:

a - Number of AD blocks of length 64 bits each

