M
DES
DES −1
M
S AB
DES(S AB,M)
S AB