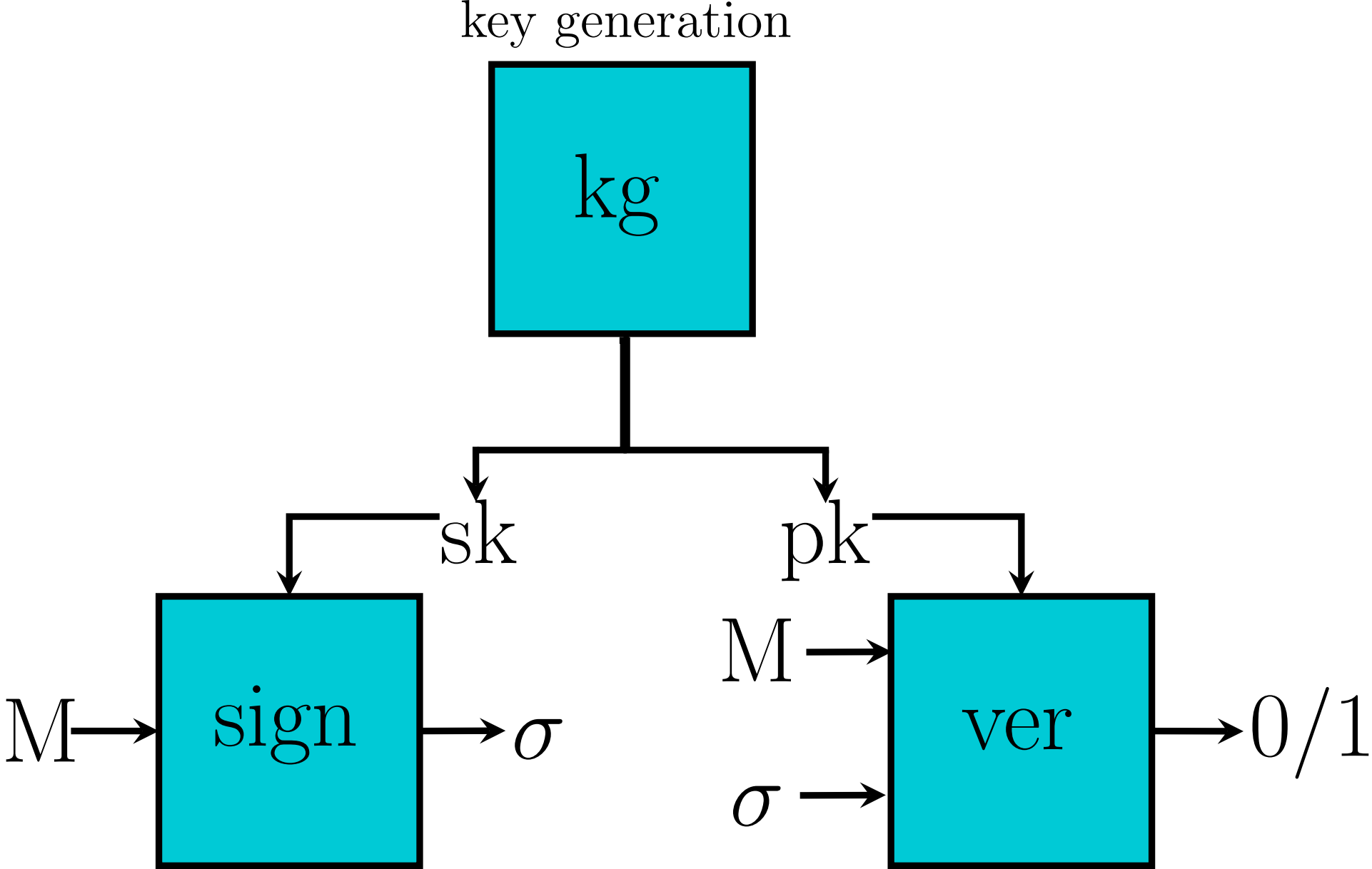
key generation
kg
sk
pk
M
sign
σ
M
σ
ver
0/1