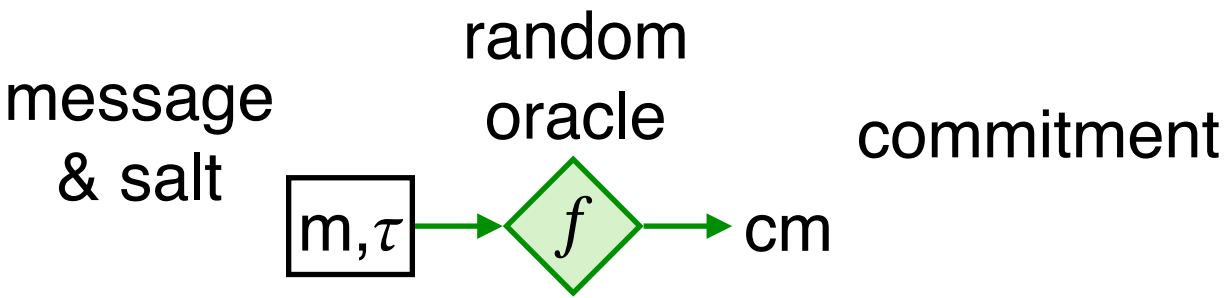
message
& salt
random
oracle
commitment
m,τ
f
cm