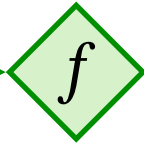


message
& salt

m, τ

random
oracle



commitment

cm