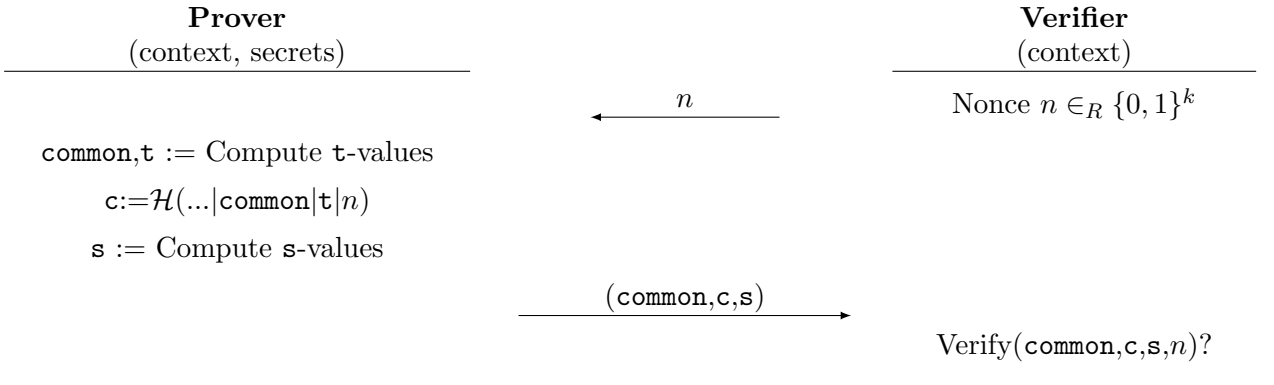
Prover
(context, secrets)
Verifier
(context)
n
Nonce $n \in_R \{0,1\}^k$
common,t := Compute t-values
c:=$\mathcal{H}$(...|common|t|n)
s := Compute s-values
(common,c,s)
Verify(common,c,s,n)?