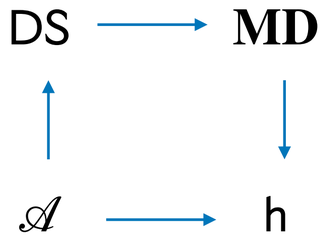
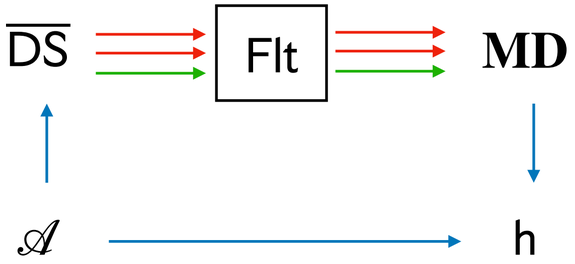


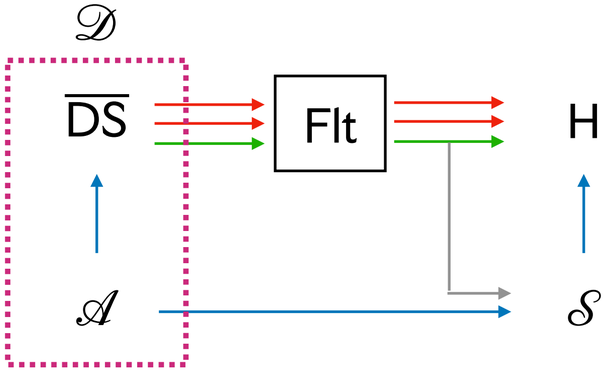
Target Setting
Scheme DS uses $\mathbf{MD}[h]$
Adversary has access to h
We want to show UF security

Recasting to use a filter

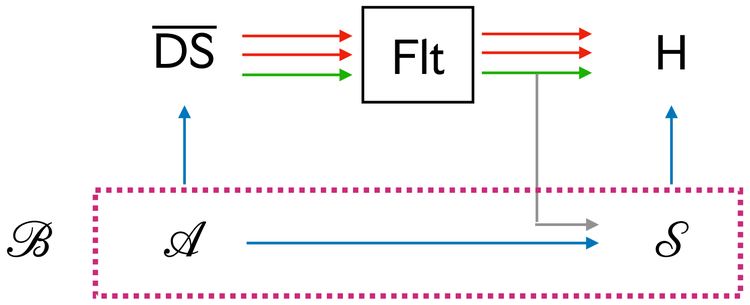


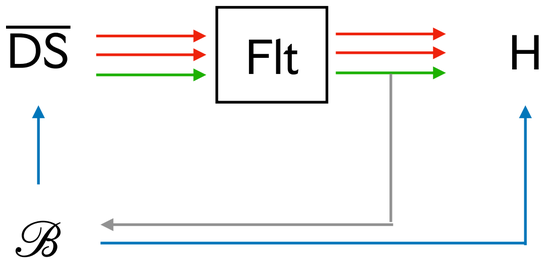
Scheme $\overline{\text{DS}}$ uses filter Flt, which calls $\mathbf{MD}[h]$
Filter has two private ports and one public port
Adversary has access to h
We want to show fUF security

Use fIndiff of MD under this filter



$\mathbf{MD}[h]$ is replaced with a random oracle H
h is replaced with a simulator $\mathscr{S}$ that calls H
Public-port filter queries are provided to $\mathscr{S}$
Dotted box represents the fIndiff distinguisher $\mathscr{D}$





Regroup

$\mathscr{A}$, $\mathscr{S}$ are merged into a fUF adversary $\mathscr{B}$
Public-port filter queries are provided to $\mathscr{B}$, allowing it to run $\mathscr{S}$

Use ideal-model security

Prove fUF security of $\overline{\text{DS}}$ in this setting, where H is a random oracle.