

\mathcal{L}_{pt}

ATTACK() :

$xa \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\}$

$xb := H(xa)$

$xc := H(xa||xb)$

return $xc \stackrel{?}{=} H(xa||xb||xc)$