

ltkR

**Responder**

X

FRESH eskR  
 $exR = h1(eskR, ltkR)$   
 $hkR = g^{exR}$

hkR

$kR = h2(\langle pkl^{exR}, X \sim ltkR, X^{exR}, \$l, \$R \rangle)$