

ltkI

Initiator

FRESH $eskI$
 $exI = h1(eskI, ltkI)$
 $hkl = g^{exI}$

hkl

(X)

(Y)

$kl = h2(<Y^{\sim}ltkI, pkR^{exI}, Y^{exI}, \$I, \$R>)$

ltkR

Responder

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

hkR

$kr = h2(<pkI^{exR}, X^{\sim}ltkR, X^{exR}, \$I, \$R>)$