The Naxos protocol

lkA	A's long-term priv. key
g^lkA	A's long-term pub. key
eskA	A's eph. priv. key

I		R
Fresh esk_I		
$ex_I = h1(esk_I, lk_I)$		
$hk_I = g^{ex_I}$	$\xrightarrow{hk_I}$	receive X
		Fresh esk_R
		$ex_R = h1(esk_R, lk_R)$
receive Y	$\xleftarrow{hk_R}$	$hk_R = g^{ex_R}$

$$key = h2(g^{(ex_R)(lk_I)}, g^{(ex_I)(lk_R)}, g^{(ex_I)(ex_R)}, I, R)$$