

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

Fresh esk_I

$$ex_I = h1(esk_I, lk_I)$$

$$hk_I = g^{ex_I}$$

receive Y

R

receive X

Fresh esk_R

$$ex_R = h1(esk_R, lk_R)$$

$$hk_R = g^{ex_R}$$

$\xrightarrow{hk_I}$

$\xleftarrow{hk_R}$

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