

Alice

**Initiator**

generate  
random  $x$

$g^x$

$Y$

shared key  
 $K = Y^x$

