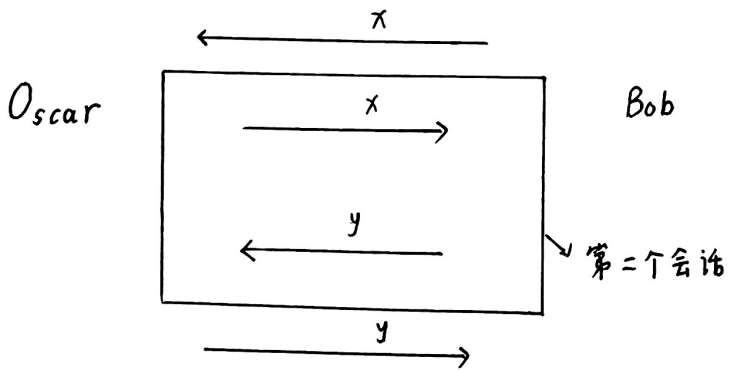
P301 9.7

会遭受并行会话攻击



在第一个会话进行中，Oscar正向Bob模仿Alice，让Bob发送自己x值。然后，他发起第二个会话，主动去识别Bob身份，发送同一个x值给Bob，Bob将x的二次方根y发给了Oscar，然后他再把y发给Bob，这样，他就成功模仿了Alice。