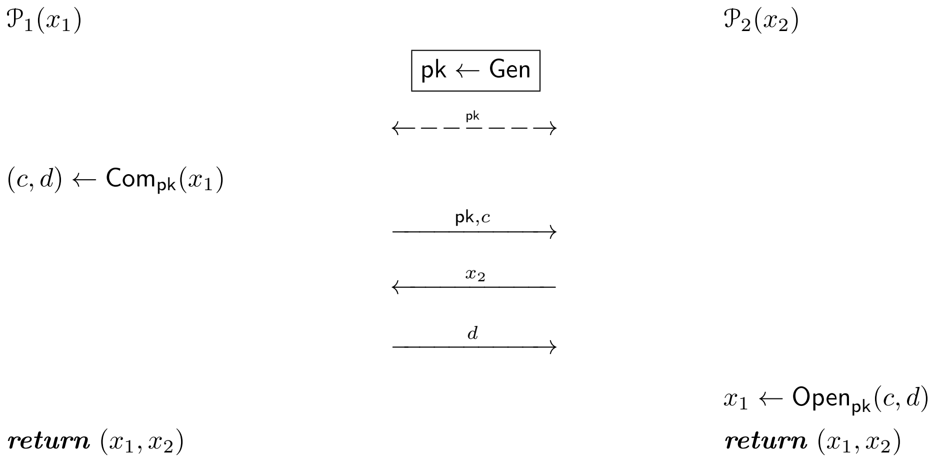
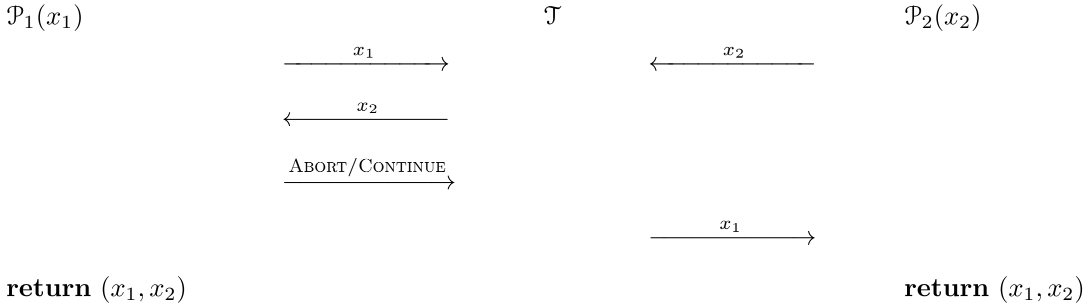
MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Security of simultaneous message exchange protocol). *Analyse security of the following simplistic protocol for simultaneous message exchange*


$\mathcal{P}_1(x_1)$
$\mathcal{P}_2(x_2)$
$\boxed{\mathsf{pk} \leftarrow \mathsf{Gen}}$
pk
$(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(x_1)$
pk, c
x_2
d
$x_1 \leftarrow \mathsf{Open}_{\mathsf{pk}}(c, d)$
return (x_1, x_2)
return (x_1, x_2)

where bits x_1 and x_2 are private protocol inputs and a triple of algorithms $(\mathsf{Gen}, \mathsf{Com}, \mathsf{Open})$ *is a commitment scheme Com with appropriate properties. The dashed line denotes sub-protocol for fixing the commitment parameters. In the following, we assume that the protocol has a trusted setup where parameter generation is done by a trusted third party. Consider security only against static malicious corruption.*

Solution.
RIGHT IDEAL IMPLEMENTATION. As the first party $\mathcal{P}_1$ can refuse to open its input based on the opponents input x_2, we must consider the idealised functionality where the first party $\mathcal{P}_1$ is in the dominant position:



(E) OUTPUT EQUIVOCATION BASED ON TRUSTED SETUP. We can use equivocal commitments to bypass problems in the output equivocation phase. But this leads to a setting with a trusted setup.

- Construct the corresponding simulator for malicious $\mathcal{P}_2$ by modifying the input extraction and output equivocation blocks
- Prove that the corresponding simulator achieves the desired goal. That is, the joint output distributions are identical in the real and ideal world.

(F) INPUT EXTRACTION BASED ON TRUSTED SETUP. The simulation efficiency for a malicious $\mathcal{P}_1^*$ depends on the size of $\mathcal{X}_2$ as the input extractor needs to iterate over all potential inputs x_2 to unlock the commitment. This problem can be bypassed if we use trusted setup with extractable commitment schemes.

- Construct the corresponding simulator for malicious $\mathcal{P}_1$ by modifying the input extraction block so that its efficiency does not depend on the size of $\mathcal{X}_2$.
- Prove that the corresponding simulator achieves the desired goal. That is, the joint output distributions are identical in the real and ideal world.