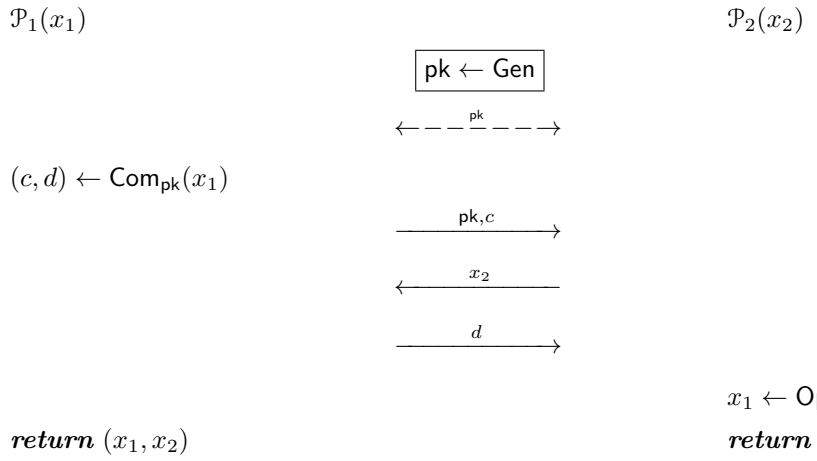
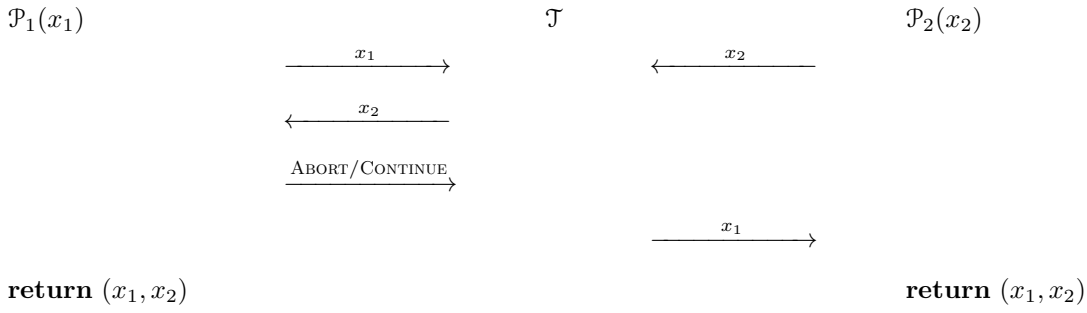
MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

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



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. Prove that there exist an efficient simulator for $\mathcal{P}_2$.

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:



High-level descriptions for simulator constructions. The interaction pattern is somewhat different if the second party $\mathcal{P}_2$ is malicious. Then the corresponding simulator Sim must first provide an input $\hat{x}_2$ to the trusted third party $\mathcal{T}$ who replies x_1. After that the simulator must make $\mathcal{P}_2^*$ to believe that honest party opened an input x_1 and the protocol outcome would be $(x_1, \hat{x}_2)$. As a result, the simulator consists of and input extraction followed by the output equivocation. If the commitment parameters are generated by $\mathcal{P}_1$, we get the the simulator

$\mathsf{Sim}(\phi_2, x_2)$
- $\mathsf{pk} \leftarrow \mathsf{Gen}$
- $\omega_2 \xleftarrow{u} \Omega_2$
- $\hat{x}_2 \leftarrow \mathcal{K}(\phi_2, x_2, \mathsf{pk}, \omega_2)$
- Send $\hat{x}_2$ to $\mathcal{T}$ and store the reply as x_1
- **return** $\mathcal{E}_\ell(\phi_2, x_1, x_2, \hat{x}_2, \mathsf{pk}, \omega_2)$

Note that the input extractor $\mathcal{K}$ and the output equivocator $\mathcal{E}_\ell$ must share inputs and randomness used by $\mathcal{P}_2^*$ or otherwise we cannot assure that the actions of $\mathcal{P}_2^*$ are consistent between both algorithms. The

consistency is essential for getting a simulation with the right output distribution. If commitment parameters are generated by $\mathcal{P}_2$ then the plumbing between the simulator components changes

$$
\begin{array}{l}
\mathsf{Sim}(\phi_2, x_2) \\
\left[\begin{array}{l}
\omega_2 \xleftarrow{u} \Omega_2 \\
\mathsf{pk} \leftarrow \mathcal{P}_2^*(\phi_2, x_2; \omega_2) \\
\hat{x}_2 \leftarrow \mathcal{K}(\phi_2, x_2, \omega_2) \\
\text{Send } \hat{x}_2 \text{ to } \mathcal{T} \text{ and store the reply as } x_1 \\
\textbf{return } \mathcal{E}_\ell(\phi_2, x_1, x_2, \hat{x}_2, \mathsf{pk}, \omega_2)
\end{array}\right.
\end{array}
$$

but the overall scheme remains the same.

(B) Input extractor for $\mathcal{P}_2$. First note that the input extractor for $\mathcal{P}_2^*$ must work in a black-box manner. The reasoning is analogous to the reasoning given for malicious $\mathcal{P}_1^*$. As $\mathcal{P}_2$ releases its actual input $\hat{x}_2$ only after seeing $c_\circ$ we must provide some sort of commitment during extraction. However, differently form its opponent $\mathcal{P}_2^*$ reply may freely depend on $c_\circ$ and thus the semantics $\hat{x}_2$ is somewhat different – it is the input which can be later successfully combined with the revealed input x_1. This means that the quality of input extraction must be considered together with output equivocation. If commitment parameters pk are generated by the opponent $\mathcal{P}_1$ then the most natural input extraction strategy is following

$$
\begin{array}{l}
\mathcal{K}(\phi_2, x_2, \mathsf{pk}, \omega_2) \\
\left[\begin{array}{l}
(c_\circ, d_\circ) \leftarrow \mathsf{Com}_{\mathsf{pk}}(0) \\
\hat{x}_2 \leftarrow \mathcal{P}_2^*(\phi_2, x_2, \mathsf{pk}; \omega_2) \\
\textbf{return } \hat{x}_2
\end{array}\right.
\end{array}
$$

where we set $\hat{x}_2$ to $\perp$ if $\mathcal{P}_2^*$ refuses to communicate after obtaining $c_\circ$. If commitment parameters pk are generated internally by $\mathcal{P}_2^*$ then the most natural input extraction strategy is following

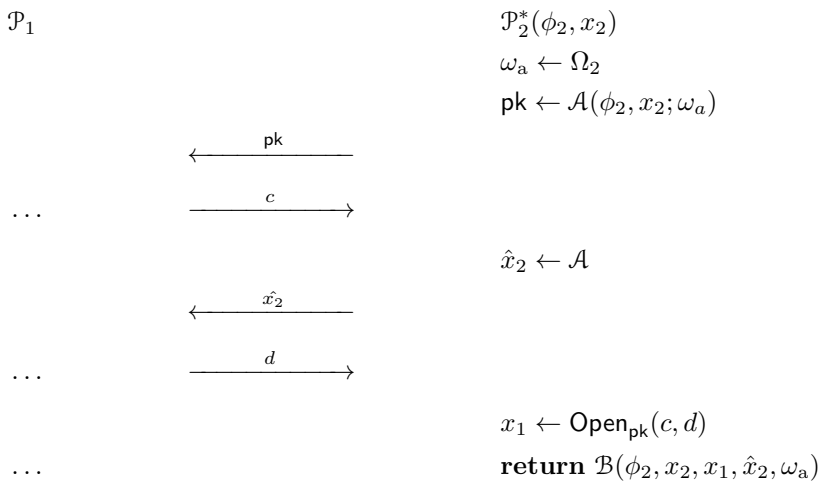
$$
\begin{array}{l}
\mathcal{K}(\phi_2, x_2, \omega_2) \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathcal{P}_2^*(\phi_2, x_2; \omega_2) \\
(c_\circ, d_\circ) \leftarrow \mathsf{Com}_{\mathsf{pk}}(0) \\
\hat{x}_2 \leftarrow \mathcal{P}_2^*(x_2, \phi_2, \mathsf{pk}; \omega_2) \\
\textbf{return } \hat{x}_2
\end{array}\right.
\end{array}
$$

Prove the following facts

- If the commitment is perfectly hiding then the protocol output y_1 of $\mathcal{P}_1$ is the same in the real and ideal world. Note that the output is completely determined by the values $(\phi_2, x_2, \omega_2, x_1)$ and thus can be considered as a deterministic function $y_1(\phi_2, x_2, \omega_2, x_1)$.
- Analyse what changes if we consider the setting with computationally hiding commitments where pk is provided by $\mathcal{P}_1$. Show that corresponding distributions must be computationally indistinguishable. How is the corresponding time-bound connected to the running-time of the extractor.
- Show that if the number of possible input values $\mathcal{X}_2$ is small then the computational distance and statistical distance are equivalent, i.e., likelihood ratio test is efficient.

(C) Limited form of output equivocation for $\mathcal{P}_2$. Although the simulator using the input extractor $\mathcal{K}$ can perfectly match the output distribution of honest $\mathcal{P}_1$, we need to show closeness of the joint output distribution. This is straightforward for a limited class of malicious adversaries $\mathcal{P}_2^*$ that consist of two

algorithms $\mathcal{A}$ and $\mathcal{B}$ with isolated states that are sequentially combined



For such adversaries, the output equivocator is following

$\mathcal{E}(\phi_2, x_1, x_2, \hat{x}_2, \mathsf{pk}, \omega_2)$
- Split ω_2 into ω_a and ω_b
- **return** $\mathcal{B}(\phi_2, x_2, x_1, \hat{x}_2, \omega_a; \omega_b)$

The randomness splitting is trivial if algorithms $\mathcal{A}$ and $\mathcal{B}$ have explicit description of the number f used random bits. If this is implicit, we can split the randomness by running $\mathcal{A}$ with ω_2 and set ω_b as the list of unused bits. Thus, the randomness splitting step is relatively efficient.

- Prove that if the commitment is perfectly hiding and the adversary has the structure described above then the joint output distributions in the real and ideal world are identical.
- Interpret the result. For which kind of security goals the malicious adversary $\mathcal{P}_2^*$ might obtain a significant gain is speed or in success. For that note that an isolated adversary $\mathcal{B}$ might completely restore the state of $\mathcal{A}$ is we additionally give him the randomness used to create the commitment decommitment pair (c, d). Are the class of neglected security goals relevant in the practice.

(D) Complete output equivocation for $\mathcal{P}_2$. To protect against all attack goals, we need equivocation algorithm works for malicious adversaries without structural restrictions. Let $\ell \in \mathbb{N}$ be a parameter determines a tradeoff between efficiency and quality of simulation. Then the following algorithm

$\mathcal{E}_\ell(\phi_2, x_1, x_2, \hat{x}_2, \mathsf{pk}, \omega_2)$
- For $i \in \{1, \ldots, \ell\}$ do
  - $(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(x_1)$
  - $x_2^* \leftarrow \mathcal{P}_2^*(x_2, \phi_2, \mathsf{pk}; \omega_2)$
  - if $x_2^* = \hat{x}_2$ then **return** $\mathcal{P}_2^*(d)$
- **return** Fail

performs rejection sampling over all possible protocol runs with the opponents input x_1 and $\mathcal{P}_2$ reply $\hat{x}_2$ and thus gets the desired output distribution when $\mathcal{E}$ does not fail.

Prove the following facts

- Assume that if the commitment is perfectly hiding and let $\hat{x}_2$ be the actual input fixed by the input extractor. Estimate the probability that $\mathcal{E}_\ell$ returns Fail as a function of probability $p(\hat{x}_2) = \Pr[\mathcal{K} = \hat{x}_2]$.
- Let $\mathcal{X}_2$ be the set of all potential inputs for $\mathcal{P}_2$ compute the maximal failure probability when $\hat{x}_2$ is sampled by $\mathcal{K}$.
- Prove that the statistical difference between joint output distributions is equal to the probability that $\Pr[\mathcal{E}_\ell = \mathsf{Fail}]$.
- Interpret results. How does the efficiency depend on desired statistical distance
- What changes if the commitment is only computationally hiding.