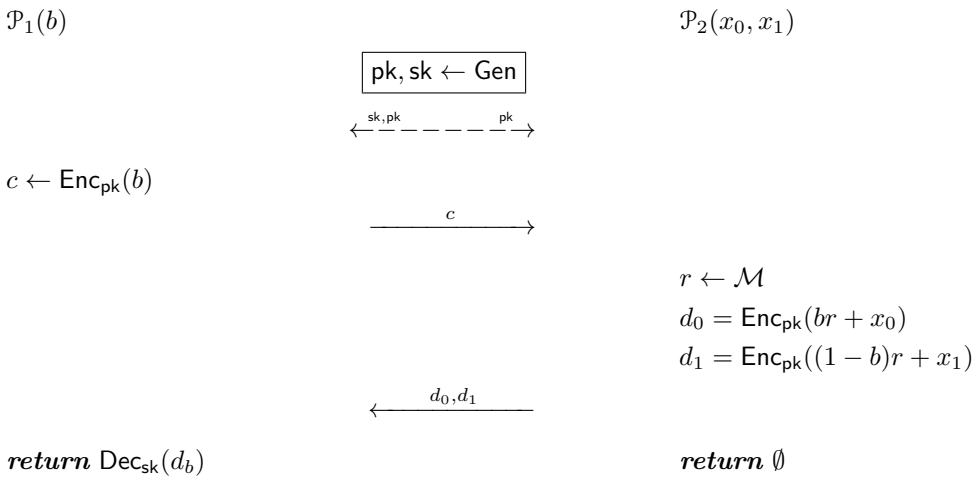
MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Security of against malicious server). *Analyse security of the Aiello-Ishai-Reingold oblivious transfer for additively homomorphic encryption scheme with prime order message space:*



where $b \in \{0,1\}$ and $x_0, x_1 \in \mathcal{M}$ are private protocol inputs and a triple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is an additively homomorphic encryption scheme. The dashed line denotes sub-protocol for fixing the commitment parameters. Prove that there exist an efficient simulator for $\mathcal{P}_2$ if the set of plausible attack goals consists of computationally bounded predicates.

Solution.
Right ideal implementation. As the party $\mathcal{P}_2$ gets no output fairness is acheivable:

(A) Input extractor for $\mathcal{P}_2$.

- Construct input extractor for $\mathcal{P}_2^*$
- Show that outputs of $\mathcal{P}_1$ in real and ideal world coincide.

(B) Output extractor for $\mathcal{P}_2$.

- Construct output equivocator for $\mathcal{P}_2^*$ that achieves 1/2 statistical distance for the joint output distribution ψ_1, ψ_2.
- Show that the construction is tight for unbounded predicates

(C) Output extractor for $\mathcal{P}_2$.

- Show that outputs are computationally indistinguishable for time-bounded predicates