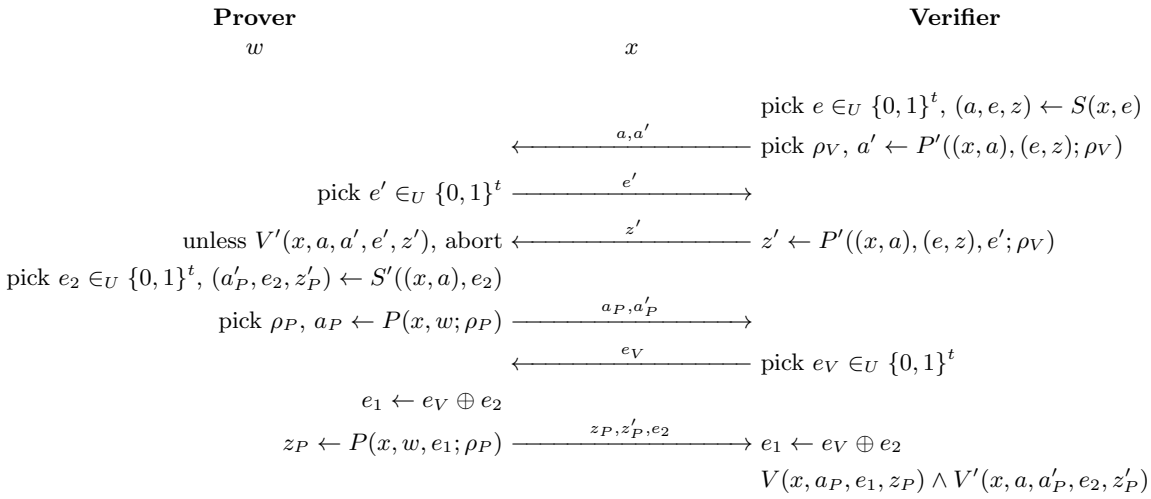
2 ZKPoK from Sigma

We consider a relation $R(x, w)$ defining a language for which we have a Σ protocol (P, V) over a challenge set $\{0,1\}^t$ with accepting predicate $V(x, a, e, z)$, Σ-simulator S, and Σ-extractor E. We define a relation $R'((x, a), (e, z))$ to hold on instance (x, a) with witness (e, z) if $V(x, a, e, z)$ is accepting. We assume that R' also has a Σ protocol (P', V') over the same challenge set $\{0,1\}^t$ with accepting predicate $V'(x, a, a', e', z')$, Σ-simulator S', and Σ-extractor E'. We consider the following protocol:



Q.1 In the first part of the protocol, recognize and isolate a commitment on the value e and a proof of knowledge of a valid opening of this commitment. Fully describe the commitment scheme. Fully describe the proof of knowledge.

Q.2 In the second part of the protocol, recognize a proof of knowledge of either w for $(R(x, w)$ or (e, z) for $R'((x, a), (e, z))$.

Q.3 Show that the protocol is complete and runs in polynomial time $\mathsf{poly}(t, |x|)$ (where $|x|$ is the length of x) for the verifier.

Q.4 Show that the protocol is zero-knowledge by constructing a black-box simulator.

Q.5 Construct a knowledge extractor for this protocol to prove that it is a zero-knowledge proof of knowledge for R.