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:

Prover		**Verifier**
w	x	
		pick $e \in_U \{0,1\}^t$, $(a,e,z) \leftarrow S(x,e)$
	$\xleftarrow{a,a'}$	pick ρ_V, $a' \leftarrow P'((x,a),(e,z);\rho_V)$
pick $e' \in_U \{0,1\}^t$	$\xrightarrow{e'}$	
unless $V'(x,a,a',e',z')$, abort	$\xleftarrow{z'}$	$z' \leftarrow P'((x,a),(e,z),e';\rho_V)$
pick $e_2 \in_U \{0,1\}^t$, $(a'_P,e_2,z'_P) \leftarrow S'((x,a),e_2)$		
pick ρ_P, $a_P \leftarrow P(x,w;\rho_P)$	$\xrightarrow{a_P,a'_P}$	
	$\xleftarrow{e_V}$	pick $e_V \in_U \{0,1\}^t$
$e_1 \leftarrow e_V \oplus e_2$		
$z_P \leftarrow P(x,w,e_1;\rho_P)$	$\xrightarrow{z_P,z'_P,e_2}$	$e_1 \leftarrow e_V \oplus e_2$
		$V(x,a_P,e_1,z_P) \wedge V'(x,a,a'_P,e_2,z'_P)$

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.