Ex 2.

1. $L \in BPP \Rightarrow \exists$ polytime decider $D \Rightarrow$ Verifier can check $x \in BPP$ itself
2. decide $x \in L$ via D defined as follows
   - let $(\pi, r) \leftarrow S(x)$, sample random s, output $b \leftarrow \text{Verifier}(\pi, b)$

   claim: $x \in L$, then $\Pr[D(x) = 1 \geq \frac{2}{3}]$

   as honest proofs verify due to completeness w.h.p., and π is ind. from honest proof

   claim: if $x \in L$, then $\Pr[D(x) = 1 \leq \frac{1}{3}]$

   as otherwise the prover P that outputs simulated proofs can break soundness
3. ROM is not captured by the setting we consider
4. verifier deterministic $\Rightarrow$ prover can collapse rounds into a NIZK $\lightning$ ex. 2

Ex 3.

1. Alice $\quad\quad\quad$ Bob

   $b \in \{0,1\}$

<u>commit:</u>

$\xleftarrow{\quad r \quad}$ $\quad r \leftarrow \{0,1\}^{3\lambda}$

$s \leftarrow \{0,1\}^{\lambda}$

$t \leftarrow G(s)$

$z_b \leftarrow t \oplus b \cdot r$ $\quad \xrightarrow{\quad z_b \quad}$

<u>open:</u>

$\xrightarrow{\quad s, b \quad}$ check $G(s) \oplus b \cdot r = 1$?

hiding: t hides $b \cdot r$

binding: Alice needs to output s, s' s.t.

$G(s) = z$ and $G(s') = z \oplus r$

$\Rightarrow G(s) \oplus G(s') = r \in \{0,1\}^{3n}$

there are 2^{2n} pairs (s, s') but 2^{3n} choices for r

$\Rightarrow \Pr_{r \leftarrow \{0,1\}^{3n}}[\exists s, s' : G(s) \oplus G(s') = r] \leq 2^{-n}$

2. $pp \leftarrow \text{Setup}(1^\lambda)$ is the function description
   - $F_{pp}(b, r) := \text{Com}_{pp}(b; r)$

   assume $\exists \mathcal{A}$ that breaks OWF property
   - sample $b \leftarrow \{0,1\}$, r
   - set $c = \text{Com}_{pp}(b; r)$
   - let $(b', r) \leftarrow \mathcal{A}(c)$

     if $b = b' \rightarrow$ can use to break hiding

     if $b \neq b' \rightarrow$ can use to break binding

Note: ex. 1 is from an old exam, so it is a good exercise for the preparation (without solutions).