1 Pseudorandom generators and commitment schemes

The questions below ask you to "check the limits" of PRGs – show that $\mathsf{P} \neq \mathsf{NP}$ is necessary for their existence, and show that they must have large enough seed, and cannot be secure against *all* algorithms (i.e., they can only be secure against efficient algorithms).

Question 1. *Prove that if the PRG conjecture is true, then* $\mathsf{P} \neq \mathsf{NP}$.

Question 2. *Prove that there is no pseudorandom generator secure against algorithms running in exponential time. That is, for every polynomial-time algorithm G that gets a seed of length $\ell(n) < n$ and outputs n bits, there is an (inefficient) algorithm A that $1/2$-distinguishes $G(\mathbf{u}_\ell)$ from the uniform distribution.*

Question 3. *Prove that there is no pseudorandom generator with seed length $\ell(n) = O(\log n)$. That is, for every polynomial-time algorithm G that gets a seed of length $O(\log n)$ and outputs n bits, there is another polynomial-time algorithm A that $1/2$-distinguishes $G(\mathbf{u}_\ell)$ from the uniform distribution.*[1]

In class we saw a specific construction of a commitment scheme, based on the PRG conjecture. The next question tests your understanding of it, as well as your understanding of the basic requirements from a commitment scheme.

Question 4. *Consider the commitment scheme shown in class, and modify it in the following way: instead of the receiver choosing a random $r_0 \in \{0,1\}^n$, the committer is allowed to choose r_0 and send it to the receiver. (In particular, there is no a-priori guarantee that a malicious committer would actually choose r_0 at random.) What would happen? Which of the requirements from a commitment scheme would be violated? Prove your answer.*

[1] In fact, you can even replace $1/2$ with 0.99.