Quiz 11 - COMS E6261: Advanced Cryptography

Question 1

Last week's presentations concluded a line of papers, one building on the other, that thought about SVL (or rSVL, or in one case PLS) hardness from strong cryptographic assumptions: iO, non-interactive arguments (with additional assumptions), and several others. This quiz will briefly review some of the main takeways from this line of work.

Suppose iO exists. Check all of the classes which are known to contain hard-on-average distributions.

□ TNFP

□ PPP

□ PPAD

□ PLS

□ PPAD ∩ PLS

Explanation: None of the above follow from iO alone – all the results we saw that involved iO required additional assumptions. In fact, iO exists in Algorithmica (ie if P=NP), where none of these classes have hard problems.

Question 2

Suppose sub-exponential iO and OWFs exist. Check each that is known to be true:

☑ injective OWF exist

☑ OWP exist

☑ trapdoor permutations (TDP) exist

☑ TFNP is hard

☑ PPP is hard

☑ PPAD is hard

☑ PLS is hard

☑ PPAD ∩ PLS is hard

Explanation: On one hand, Hugo's presentation showed us how sub-exponential iO and OWFs imply trapdoor permutations, which thereby also imply the first two (injective OWFs and OWP). Separately, we have seen much earlier the construction of SVL hard distributions from subexponential iO and injective OWFs, but as we know the latter follows from the first result in Hugo's presentation, so hardness is implied in every class which we can reduce solving SVL to.

Question 3

In the random oracle model, which of the following classes are known to be hard-on-average?

☑ TFNP

☑ PPP

☑ PWPP

☑ PLS

□ PPAD

□ PPAD ∩ PLS

Explanation: PPP and PWPP are hard in the random-oracle model because a random-oracle implementing a shrinking function (say from n bits to $n-1$) is collision resistant (this is easy to show). On the other hand, Shouqiao showed us that in the ROM, PLS is hard on average (this construction is not so easy). The same is not known for PPAD (we've seen that PPAD is hard in the ROM with additional computational assumptions).

Question 4

Suppose there exists a hard-on-average language L in PSPACE, for which there exist incrementably generatable and verifiable proofs of each state of the computation of the PSPACE machine M deciding L. Which of the following classes are known to be hard-on-average?

☑ PLS

□ PPAD

□ PPAD ∩ PLS

Explanation: As we learnt from Shouqiao's presentation, a hard PSPACE language with such incremental proofs that are *not* necessarily unique gives us hardness in PLS.

Question 5

Suppose that in the previous question, it was also the case that there exists a unique proof for each state of the computation of M. Which of the following classes are known to be hard-on-average?

- ☑ PLS
- ☑ PPAD
- ☑ PPAD ∩ PLS

Explanation: As we learnt originally from Jiaqian's presentation, a hard PSPACE language with such incremental proofs that are also unique (unique proof for each state of computation) gives us a hard SVL instance.