Quiz 3 - COMS E6261: Advanced Cryptography

Question 1

Throughout the quiz, by "hard on average" we will mean exponentially hard against all non-uniform poly-time adversaries, over instances drawn from poly time distributions (this is the same sense of hardness as used for defining most cryptographic primitives).

There exists a relation R in TFNP such that if R is hard-on-average, OWFs exist.

● True

○ False

○ Unknown

Explanation: Take WEAK-PIGEON for example – its hardness-on-average implies existence of CRHF, which in turn implies OWFs.

Question 2

If OWFs exist, there is a relation R in TFNP that is hard-on-average.

○ True

○ False

● Unknown

Explanation: Discussed this as an open problem in class.

Question 3

If OWPs exist, there is a relation R in TFNP that is hard-on-average.

● True

○ False

○ Unknown

Explanation: Take PIGEON for example – we showed this in class.

Question 4

Consider the following attempt to show FACTORING $\in$ PPA.

Given a composite odd integer N, construct the circuit C_N pairing an element x in $\{1, \ldots, N-1\}$ to its inverse x^{-1} mod N (this can be done efficiently, using extended Euclid algorithm), or, if x does not have an inverse (which happens exactly when x is not co-prime to N), C_N pairs it to itself. Since $1 = 1^{-1}$, we have that 1 is paired to itself, which is the definition of being unmatched. A solution is another unmatched element (which must exist since the size of the domain was even to begin with, and we removed 1).

Question 4.1

There exist solutions to this instance of LONELY such that given such a solution, one can factor N.

● True

○ False

Explanation: Any element x that is not co-prime to N is a solution, and $gcd(x, N)$ gives a non-trivial factor of N.

Question 4.2

The above construction reduces Factoring to LONELY.

○ True

● False

Explanation: While some solutions give you a factoring of N, not all do. In particular, -1 (or equivalently $N-1$) is its own inverse, so it is also a solution, but this solution does not help in factoring N.

Question 5

In the following question, any of the three choices will give you full credit, we just want to check:

○ I have a pretty good idea for what topic I want for my project, and what project partner(s) (if any) I'd like to work with.

○ I have some vague sense of which area I might want to explore for my project, and who I'd like to work with (if any)

○ I have no ideas for my project

Note: whatever your answer, we encourage you to contact us and share where you're at. It's a small class, so we can help steer you in a direction that fits your interest, provide resources, etc.