Quiz 1 - COMS E6261: Advanced Cryptography

1 Question 1

Suppose Collision-Resistant Hash Functions (CRHF) exist. Which of the possible worlds could we possibly be in, given what we currently know?

- ☐ Algorithmica
- ☐ Heuristica
- ☐ Pessiland
- ☑ Minicrypt
- ☑ Cryptomania
- ☑ Obfustopia

Explanation: If CRHF exist then OWF exist, so the first three worlds are not possible (in all of them there are no OWF). The other worlds are all possible, as far as we know: KA (key agreement) and iO (indistinguishability obfuscation) may or may not exist if CRHF exist.

2 Question 2

Suppose C is a class that for each n contains only two circuits: one that maps every n bit input to 0^n, and one that maps every n bit input to 1^n. Then it's easy to construct a indistinguishability obfuscator for C.

- ◉ True
- ○ False

Explanation: iO has a requirement of indistinguishability only on the obfuscation of two circuits with identical functionality. Since in this class C there are no two circuits of identical functionality, the condition holds vacuously, so one could just have the "obfuscator" be the identity function, mapping any circuit to itself. Of course, this is not an interesting class — the power of iO comes from iO for richer classes of circuits, that have more than one implementation for the same functionality.

3 Question 3

Let $F : \{0,1\}^n \to \{0,1\}^m$ be a OWF (one-way function). Consider the following search problem: given a uniform $y \in \{0,1\}^m$, find an x such that $F(x) = y$. Check all that necessarily apply:

- ☑ This search problem is in FNP
- ☐ This search problem is in TFNP
- ☐ This search problem is hard (up to negligible success probability) for any poly time algorithm

Explanation: Since F is efficiently computable, one can efficiently verify whether a given solution x is indeed a preimage of y, hence the problem is in FNP. It is not necessarily in TFNP since F is not necessarily onto. It is not necessarily hard, since the OWF hardness is with respect to a uniformly chosen input x. For example, say that we have some OWF $F' : \{0,1\}^k \to \{0,1\}^k$ and we define $F : \{0,1\}^{2k} \to \{0,1\}^{k+1}$ as follows: $F(0^k||x) = 0||x$ and $F(x_1||x_2) = 1||F'(x_2)$ if $x_1 \neq 0^k$. This F is still a OWF, but if we choose y uniformly at random, with probability $1/2$ it begins with a 0 and thus is easy to invert.

4 Question 4

Let $F : \{0,1\}^n \to \{0,1\}^n$ be a OWP (one-way permutation). Consider the following search problem: given a uniform $y \in \{0,1\}^n$, find an x such that $F(x) = y$. Check all that necessarily apply:

- ☑ This search problem is in FNP
- ☑ This search problem is in TFNP
- ☑ This search problem is hard (up to negligible success probability) for any poly time algorithm

Explanation: Since F is a permutation, it must be onto, so every instance y must have a preimage (solution), hence it's in TFNP. It is also hard, since being a permutation, the distribution of choosing y uniformly at random is the same as choosing x uniformly at random and then applying F — this is hard based on the one-way property.

5 Question 5

If TFNP = FP, which of the following do we NOT know is necessarily true?

- ○ Given an integer, one can efficiently find its prime factorization.
- ○ Given a circuit with less outputs than inputs, one can efficiently find a collision.
- ◉ Given a satisfiable SAT formula on n variables, one can efficiently find a satisfying assignment.
- ○ Given a language in NP $\cap$ coNP, one can efficiently decide membership in the language.

Explanation: All but the third problem are in TFNP — every instance is guaranteed to have a solution, and a solution is easy to verify. Thus, if TFNP=FP, all these questions are efficiently solvable. The third bullet is the only one here that is not in TFNP (as far as we know), so we cannot apply the same argument. Indeed, given a formula, we do not know how to efficiently check whether or not it has a satisfying assignment, so the relation is not in TFNP (if we insist that the relation only has satisfiable formulas, we do not know how to efficiently verify it, and if we allow any formula, the relation is not total).

Note: It is an open problem whether TFNP=NP implies that P=NP (hence we do not know the third bullet to be true).

6 Question 6

Which of the following relations/ search problems are in FNP? (we phrase the first two as relations and the last two as search problems). Select all that apply.

- ☑ The set of (N, p) where N is a positive integer and p is a non-trivial factor of N
- ☑ The set of (N, p) where N is a positive integer and p is a prime number that divides N
- ☑ Given a circuit $C : \{0,1\}^{n+1} \to \{0,1\}^n$ output a pair $x_1 \neq x_2$ such that $C(x_1) = C(x_2)$
- ☑ Given circuits $C_1 : \{0,1\}^n \to \{0,1\}^n$ and $C_2 : \{0,1\}^n \to \{0,1\}^n$ find an $x \in \{0,1\}^n$ such that $C_1(x) = C_2(x)$

Explanation: In all cases, given a proposed solution, it is easy to efficiently verify it (multiplying, dividing, checking primality, and applying a given circuit on a given input are all efficiently computable), so all are in FNP.

7 Question 7

Which of the following relations/ search problems (same as in the previous question) are total? Select all that apply.

- ☐ the set of (N, p) where N is a positive integer and p is a non-trivial factor of N
- ☑ the set of (N, p) where N is a positive integer and p is a prime number that divides N
- ☑ Given a circuit $C : \{0,1\}^{n+1} \to \{0,1\}^n$ output a pair $x_1 \neq x_2$ such that $C(x_1) = C(x_2)$
- ☐ Given circuits $C_1 : \{0,1\}^n \to \{0,1\}^n$ and $C_2 : \{0,1\}^n \to \{0,1\}^n$ find an $x \in \{0,1\}^n$ such that $C_1(x) = C_2(x)$

Explanation: The first relation is not total since for a prime N there's no non-trivial factor. The second is total since every integer N has a prime that divides it. The third is total since every circuit that has a shorter output than input, must map two inputs to the same output, by the pigeonhole principle. The last is not total since there are pairs of circuits C_1, C_2 that do not give the same output on any input (e.g., say C_1 always outputs 0 and C_2 always outputs 1).

8 Question 8

I have looked over the class webpage https://dmitropolsky.github.io/teaching/6261/

9 Question 9

The WEAK PIGEON in class had (check all that apply):

- ☑ Broken wing
- ☐ Broken leg
- ☑ A tear

Explanation: This question was meant to check whether you attended lecture and give some advantage to those who did (but looking at the lecture notes on the webpage also gives the answer). We expect people to attend, unless there's an excellent reason not to (e.g., you're traveling to a conference to present your work, you are sick, etc). We aim to put all necessary materials on the class webpage, for people to review.