Quiz 10 - COMS E6261: Advanced Cryptography

This week, we had two quizzes: a super fun April Fool's Day quiz, which we hope you enjoyed, and a regular quiz which contained the more reasonable questions from the April Fool's Day Quiz. Here, we include all of the questions, the first four of which are real questions, and the remainder of which were a prank.

Question 1 (real)

Let IS be the following problem: given an integer N that is the product of two primes, a generator $g \in \mathbb{Z}_N^*$, and number $t \in [N]$, compute $g^{2^t} \mod N$.

Assume that there exists a PPT sampler $D(1^n)$ that outputs tuples (N, g, t) such that no PPT solver can output g^{2^t} with non-negligible probability. Then it is known that there exists a hard problem in PPAD $\cap$ PLS.

- ○ True
- ◉ False

Explanation: The premise set up in this question is just the assumption that the Iterated Squaring problem from class is hard-on-average. However, we do *not* know how to construct hard a TFNP problem (let alone PPAD $\cap$ PLS or rSVL) from just this assumption: we need both this *and* an additional assumption about some sort of non-interactive argument for this problem (in particular the normal LWE assumption is enough to construct this latter part).

Question 2 (real)

For any relation S, in the random oracle model, a random function is correlation-intractable for S.

- ○ True
- ◉ False

Explanation: This is true precisely only for any *sparse* relation. If there are many x with non-negligible (greater than 1/poly) fraction of valid y such that $(x, y) \in R$, then the algorithm that keeps trying $(x, h(x))$ will succeed in poly many queries.

Question 3 (real)

Let Gen, Enc, Dec be a CPA secure public-key encryption scheme. Then an encryption $\text{Enc}_{pk}(0^n; r)$ must be indistinguishable from an encryption of $\text{Enc}_{pk}(sk; r')$ of the secret key.

- ○ True
- ◉ False

Explanation: This *may* be the case, but this is an additional property; a PKE scheme with this property is called a *circular* secure PKE scheme. The reason it is not true for *any* PKE scheme is because the definition of security guarantees that encryptions of two strings such as 0^n and 1^n are indistinguishable *over the randomness of Gen* (and other randomness, such as that used by Enc, that of the adversary, etc., but in particular also over the generation of sk) . This would hold even if we modify the Enc to always output sk itself on input sk.

Question 4 (real)

Describe a relation S such that the existence of a Collision-Intractable hash function for S is equivalent to the existence of Collision-Resistant Hash Functions.

Solution/explanation: After the quiz, the instructors realized that there was a problem with how the question! As phrased, it is unclear whether the statement is true. This is because in the definition of Collision-Intractable Hash Functions for a relation S, the hash function H is always applied to one domain element, and the pair $(x, H(x))$ cannot be in S.

"Morally", the answer that we were seeking with this questions was something like this: S has inputs (x_1, x_2) (i.e. parse the input x as a tuple of two strings) and outputs (y_1, y_2). $((x_1, x_2), (y_1, y_2)) \in S$ iff $x_1 \neq x_2$ and $y_1 = y_2$. However, this solution doesn't work since, following the definition of Collision-Intractable Hash Functions, H would be applied to the whole string (x) (i.e. on the "left" side of the relation you'd have something like $H(x_1, x_2)$).

It is unclear whether such a relation might exist anyways (maybe one can construct a CI-intractable hash function whose domain is tuples of strings (x_1, x_2), and use this to construct a regular, one-input CRHF, but unclear how). We've awarded everyone full points on this problem.

Question 5 (prank)

Another route for constructing hard rSVL instances is from #SAT and a way to construct a special kind of unambiguous SNARGs for it.

Consider the following #SAT instance on 5 variables $(x_1, x_2, x_3, x_4, x_5)$. How many satisfying assignments does it have?

$$\phi = (x_5 \vee x_3) \wedge (\neg x_1 \vee \neg x_4) \wedge (x_1 \vee \neg x_5) \wedge (x_4 \vee x_3) \wedge (\neg x_3 \vee \neg x_4)$$

Solution: 8

Question 6 (prank)

Select all the satisfying assignments of the #SAT formula (same one as above).

$$\phi = (x_5 \vee x_3) \wedge (\neg x_1 \vee \neg x_4) \wedge (x_1 \vee \neg x_5) \wedge (x_4 \vee x_3) \wedge (\neg x_3 \vee \neg x_4)$$

- ☐ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 0$
- ☐ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 0$
- ☐ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 0$
- ☐ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 0$
- ☑ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 0$
- ☑ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 0$
- ☑ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 0$
- ☑ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 0$
- ☐ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 0$
- ☐ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 1$
- ☐ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 1$

☐ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 1$

☐ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 1$

☑ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 1$

☑ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 1$

☑ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 1$

☑ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 1$

☐ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 1$

☐ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 1$

☐ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 1$

☐ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 1$

☐ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 1$

☐ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 1$

☐ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 1$

☐ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 1$

Question 7 (prank)

Select all the non-satisfying assignments, i.e. such that

$$\phi(x_1, x_2, x_3, x_4, x_5) = 0$$

.

☑ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 0$

☑ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 0$

☑ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 0$

☑ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 0$

☐ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 0$

☐ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 0$

☐ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 0$

☐ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 0$

☑ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 0$

☑ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 0$

☑ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 0$

☑ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 0$

☑ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 0$

☑ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 0$

☑ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 0$

☑ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 0$

☑ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 1$

☑ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 1$

☑ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 1$

☑ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 1$

☐ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 1$

☐ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0, x_5 = 1$

☐ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 1$

☐ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0, x_5 = 1$

☑ $x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 1$

☑ $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 1$

☑ $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 1$

☑ $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1, x_5 = 1$

☑ $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 1$

☑ $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 1$

☑ $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 1$

☑ $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1, x_5 = 1$

Question 8 (prank)

Recall the pebbling game construction covered in class, which is used to reduce an SVL (or rSVL) instance to PPAD. Since we skipped the quiz that week, in this problem we will practice the pebbling construction.

The goal is to place a pebble on tape cell 2^t. Recall that a valid move is one of (1) place a pebble in cell 1, or (2) place/remove a pebble in cell l as long as there is a pebble in cell $l-1$.

Question 8.1

In order to place a pebble in cell number 512, how many pebbles are needed?

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ◉ 9
- ○ 10
- ○ between 10 and 511
- ○ 512
- ○ greater than 512

Question 8.2

To denote a move, we will write a tuple (i, t) for placing pebble i in cell t, and $(i, 0)$ for removing pebble i (from wherever it is). For any large t, the first move will be pebble 1 into cell 1, denoted $(1, 1)$, followed by pebble 2 in cell 2 $(2, 2)$, followed by removing pebble 1 $(1, 0)$, and so on.

List the pebbling moves in order for placing a pebble in cell 512. Since this question will be automatically graded, separate each move by only a single comma (i.e. the string should begin as "(1,1),(2,2),(1,0)...").

Question 9 (prank)

True or False: If one could prove a black-box separation from CLS = PPAD ∩ PLS to rSVL such that in the proof of security the CLS solver A must make all queries to the rSVL oracle before querying the CLS instance, with the exception of the cost function C of the CLS instance (in reduction to PLS) which A can query but only obliviously (no queries to the CLS instance after all rSVL queries have been answered can depend on the initial queries) or equivalently, there exists a simulation of A's execution after given only the rSVL queries and answers, then we obtain a black-box oblivious separation between PPAD and PLS from an additional oracle separation between CLS and the latter classes?

- ○ True
- ○ False

Explanation: This question makes no sense.

Question 10 (prank)

An important problem that is known to be PLS complete is that of finding pure Nash equilibrium in network coordination games. To answer the following question, you don't have to know the exact definition of this problem, only the fact that it is equivalent to ITER. You can also use the following lemma:

Lemma 3.1 (Röglin [2008]). *Let $X \in \mathbb{R}^d$ be a vector of d independent random variables where each X_i has density bounded by ϕ. Let $\alpha_1, \ldots, \alpha_r$ be r linearly independent vectors in $\mathbb{Z}^d$. then the joint density of $(\langle \alpha_i, X \rangle)_{i \in [r]}$ is bounded by ϕ^r, and for any given $b_1, b_2, \ldots \in \mathbb{R}$ and $\epsilon > 0$,*

$$\Pr\left[\bigwedge_{i=1}^{r} \langle \alpha_i, X \rangle \in [b_i, b_i + \epsilon]\right] \leq (\phi\epsilon)^r \tag{2}$$

Now, suppose the following holds:

Let $\mathcal{E}$ be the event in the probability statement, that is, $\bigwedge_{i=1}^{r} \langle \alpha_i, X \rangle \in [0, 0 + \epsilon]$. If $\mathcal{E}$ does not hold, and the sequence is indeed an improving one, then at least one of the improvements must be at least ϵ. If $\mathcal{E}$ does not hold for *any* sequence of $\Omega(n)$ moves, then we can bound the running time of the iterative algorithm by

$$\frac{n}{\epsilon} \cdot \left(\max_{\sigma} \Phi(\boldsymbol{\sigma}) - \min_{\sigma} \Phi(\boldsymbol{\sigma})\right)$$

Then we can certainly conclude that (select all that apply):

- ☐ PLS is hard
- ☐ PLS is easy
- ☐ PLS = PPAD

Explanation: This question also makes no sense.

Question 11 (prank)

Last week's presentation was based off a paper with many important authors.

Please select the authors from below, being careful to avoid decoy names. Since some names are not-unique and appear twice, each name appears twice in the options as well with a suffix 1/2 or 2/2. If there is only one author with that name, then select only the *first* of the two options (1/2)

- ☑ Canetti (1/2)
- ☐ Canetti (2/2)
- ☐ Cannoli (1/2)
- ☐ Cannoli (2/2)
- ☑ Chen (1/2)
- ☐ Chen (2/2)
- ☐ Christ (1/2)
- ☐ Christ (2/2)
- ☐ Homlgren (1/2)
- ☐ Homlgren (2/2)
- ☑ Holmgren (1/2)
- ☐ Holmgren (2/2)
- ☑ Lombardi (1/2)
- ☐ Lombardi (2/2)
- ☐ Mitropolsky (1/2)
- ☐ Mitropolsky (2/2)
- ☐ Naor (1/2)
- ☐ Naor (2/2)
- ☑ Rothblum (1/2)
- ☑ Rothblum (2/2)
- ☐ Malkin (1/2)
- ☐ Malkin (2/2)
- ☑ Wichs (1/2)

☐ Wichs (2/2)

☐ Vlatakis Gkaragkounis (1/2)

☐ Vlatakis Gkaragkounis (2/2)

Question 12 (prank)

Let G be a Lie group and ℓ be prime, and consider the natural ring homomorphism $H^*_{sing}(BG;\mathbb{Z}/\ell) \to (BG^\delta;\mathbb{Z}/\ell)$ from the $\mathbb{Z}/\ell$-singular cohomology of the classifying space BG of the topological group G to the $\mathbb{Z}/\ell$-singular cohomology of the classifying space BG^δ of the discrete group G^δ underlying G. This is an isomorphism.

○ True

○ False

Explanation: Unknown! Milnor's conjecture, big open problem in Lie algebras

Question 13 (prank)

Recall the paper that showed that TFNP is hard on average in Pessiland (lecture 5). Consider the names of the authors:

Question 13.1

sixteenth letter of second author's first name:

$\boxed{A}$

Question 13.2

first letter of first author's last name:

$\boxed{P}$

Question 13.3

eleventh letter of second author's last name:

$\boxed{R}$

Question 13.4

sixteenth letter of second author's last name:

$\boxed{I}$

Question 13.5

sixth letter of first author's first name:

$\boxed{L}$

Question 13.6

third letter of first author's first name:

$\boxed{F}$

Question 13.7

twelveth letter of second author's first name:

$\boxed{I}$

Question 13.8

first letter of first author's first name:

$\boxed{R}$

Question 13.9

fourth letter of first author's last name:

$\boxed{S}$

Question 13.10

third letter of second author's first name:

$\boxed{T}$