Common mistakes made on hw1

December 23, 2018

The purpose of this document is to list common mistakes. For each mistake I give intuitive explanations of why it is wrong. Notice that in addition to all these mistakes the mistake of "not writing formal solutions" and "skipping parts of the proof", was also pretty common.

1 Question 2

1.1 Proving the Question by induction - 7 pts penalty

This question can’t be proven by induction, because, as we saw in class, the computational/statistical close relation is transitive Only when applied polynomial number of times, but proof by induction supposed to work infinite number of times. For example, one can "proof by induction", that the distributions $H_0 = 0^n$ (i.e. - a single word of only zeroes) and $H_{2n} = 1^n$ are "computationally indistinguishable", by defining $2^n$ Hybrids, such that $H_i$ is distribution that takes $1^n$ with probability $\frac{i}{2^n}$, and else takes $0^n$. Its easy to see that $H_i, H_{i+1}$ are computationally indistinguishable (because they have $\frac{1}{2^n}$ statistical distance), yet one cannot claim that due to the "transitivity of computationally close relation" it holds that $H_0 \approx H_{2^n}$.

1.2 Stating that "computationally close" is fully transitive (without using induction) - 3-5 pts penalty

This is incorrect from the same reason that using induction would be illegal here.

2 Statistical distance Vs Computational distance confusing - 2 pts for each case of confusing

Across questions 2 and 3a,b,c - many computed statistical distance and not computational distance at questions that regarding PRG. Note that when we are talking about PRG, the Statistical distance between $G(U_n)$ and $U_{l(n)}$ will always be non-negligible (why?). Therefore, stating that the statistical
distance between the distributions at question 3a is big is not enough to prove that G is not a PRG. Stating that the statistical distance between $G'(U_n)$ and $U_{p(n)+n}$ is negligible at question 2 is just plain wrong.

3 Question 3

3.1 section a - show that this is not a PRG by using "encryption game challenge" - two points penalty

Some students defined a correct distinguisher, but then, in order to prove that it is indeed distinguishes, they described an "encryption challenge game", in which the distinguisher is given a word that comes w.p. $\frac{1}{2}$ from each distribution and "has to guess right".

This is wrong because in the encryption game, the adversary can choose $m_0, m_1$ to use and still the ciphertext will provide negligible information on which word is taken". This is because we want a "good hiding" For each two words - i.e. in the worst case

In contrast - in the distinguisher game, It might be the case when certain tuples of messages from the two distributions are extremely "hard" or "easy" to distinguish between, and therefore we would like To prove claims on "average" chosing of words.

3.2 section e - claiming that $\Pr[x \leftarrow \{0, 1\}^n, y \leftarrow f(x), x' \leftarrow \{0, 1\}^n : f(x') = y] = \frac{1}{n}$ - 3 pts penalty

This is just wrong. For example - if $f$ is the constant function (i.e.: $\forall x : f(x) = 0^{|\log(n)|}$), then the probability on the left side is exactly 1.

4 Question 4

Most of the students defined a valid candidate: $f(x) = \text{Enc}(x, 0^{2|x|})$, (w.l.o.g. Some used another constant message), and then defined the valid adversary $A'$ to $\text{Enc}$ that will pick messages $m_0 = 0^{2|x|}$ and a random $m_1$, and given $c$ will use $A$ to find $k$ such that $\text{Enc}(k, 0^{2|x|}) = c$, and if $A$ gave a valid key $k$ the adversary will output 0, else it will output 1.

However, in the proof that this adversary works, many mistakes were made:

4.1 Ignore the case in which the challenger chose $b=1$, yet $A$ found a key that "explains" $m_0$ - 12 pts penalty

This is of course a crucial part in analysing the success probability of your distinguisher. In particular, ignoring this case means that given any secure encryption, including one time pad you can prove the existence of OWF.
4.2 State that this case happens with negligible probability without a proof - 10 pts penalty

Again, you have to write your solutions formally and explain why it is negligible. In particular, stating that this case happens with negligible probability without mentioning the secure encryption message/key dimensions, means that given any secure encryption, including one time pad you can prove the existence of OWF.

4.3 Wrongly assume things about A when analysing the success probability of A in this case - 3-5 pts penalty

Many students that tried to bound the case mentioned above, claimed that even if $m_1$ was chosen, and there is a key such that $\text{Enc}(k, m_0) = c$, then the probability that A will find such key is $\frac{1}{p(n)}$ (i.e. equal to the success probability of A to invert f).

This is wrong because you assumed that
$$\Pr[k \leftarrow \text{Gen}, c \leftarrow \text{Enc}(k, m_0), k' \leftarrow A(1^n, c) : \text{Enc}(k', m_0) = c] \geq \frac{1}{p(n)}$$

But you know nothing about the behaviour of A when he gets inputs from a different distribution, i.e. you can’t assume that
$$\Pr[k \leftarrow \text{Gen}, c \leftarrow \text{Enc}(k, m_1), k' \leftarrow A(1^n, c) : \text{Enc}(k', m_0) = c] \geq \frac{1}{p(n)}$$

In particular, A might always return a key such that this equality holds, given that such key indeed exists.