Homework 2

CSE 208: Advanced Cryptography *(Winter 2017)*

Instructor: Daniele Micciancio

Due: Thursday February 23, in class

In class we defined a *randomized encoding* for a class of functions `F = {f:X -> Y}` by three efficient algorithms `(encode,decode,simulate)` satisfying a correctness condition `decode(encode(f,x,r)) = f(x)`, and a security condition `simulate(f,f(x)) ~ {encode(f,x,r) | r <- R}`.

We also showed how to randomized encodings can be used to build a functional encryption scheme `FE` for the function class `F`, starting from a functional encryption scheme `FE'` for the class of functions `F' = {f'((x,r)) = encode(f,x,r) | f in F}`. Specifically, we proved that if `FE'` is NA-SIM secure, then `FE` is also NA-SIM secure. (See also the GVW12 paper on the course webpage, showing how to expend the proof to AD-SIM security.)

This homework assignment is somehow open ended, in the sense that you won't be told exactly what to prove or not to prove. What you should do is to think about the following questions, come up with your best answer, and then preseting it as your solution.

- Can you prove that if `FE'` is (NA or AD) IND secure, then `FE` is also (NA or AD) IND secure?
- If yes, is it enough assume the randomized encoding is IND secure? (See lecture notes on the webpage for a possible indistinguishability security definition for randomized encorings.)
- If no, can you provide a counterexample showing that the implication is false?
- Again, if no, can you prove the implication for some natural strengthening of IND security?

As the questions in these assignmemnt are left somehow open ended, an important part of your solution is to clearly describe your claim, what you think can or cannot be proved, and exactly what variants of the definions are being used. If you think something is true, but you are not sure how to prove it, you can include your claim in your solution, clearly identifying it as an unproven conjecture.