Homework 1

CSE 208: Advanced Cryptography *(Winter 2017)*

Instructor: Daniele Micciancio

Due: Tuesday January 31, in class

Important Disclaimer: Problems 2 and 3 are very similar. I (Daniele) solved only one of them, and it has a relatively simple solution, definitely fair as a homework assignment for this class. So, for fairness, you will receive full credit for solving any 2 of the following 3 problems. You may still solve all three for extra credit, but as I don't know how hard it is, that's entirely optional.

Program Obfuscation

An obfuscator is a probabilistic polynomial time (PPT) program O that on input a boolean circtuit C, outputs an equivalent circuit $C' \leftarrow O(C)$ (written $C \equiv C'$), i.e., a circuit C' such that

- C and C' have the same number of inputs and outputs, and
- for any input x, $C(x) = C'(x)$

We also assume that the size $|C'|$ of the obfuscated circuit depends only on the size of the input circuit $|C|$. (This is without loss of generality, as it can always be achieved by padding, i.e., by adding an appropriate number of "useless" gates to C'.) Recall the definition of black-box (BB) security:

Definition (BB) An obfuscator O achieves black-box (BB) security if for any PPT adversary A, there is a PPT simulator S such that for any circuit C the distributions $A(O(C))$ and $S^C(|C|)$ are computationally indistinguishable, i.e., for any polynomial time distinguisher D, $\Pr\{D(A(O(C)))\} \approx \Pr\{D(S^C(|C|))\}$.

In the above definition A is a program that on input an obuscated circuit, outputs an arbitrary bitstring. We also considered a restricted definition where A is a predicate, i.e., a program that outputs a single bit.

Definition (BB1) An obfuscator O achieves 1-bit black-box (BB1) security if for any PPT predicate A, there is a PPT simulator S such that for any circuit C, $\Pr\{A(O(C))\} \approx \Pr\{S^C(|C|)\}$.

Problem 1: [Barak et al.] quickly dismisses definition BB as too strong to be achieved, and informally claims, as counterexample, that a family of pseudorandom functions cannot be obfuscated because "it cannot be compressed".

Give a formal proof of the above statement, i.e., show that there is no (PPT) obfuscator O satisfying definition **BB**. You may assume the existence of a

family of pseudorandom functions $\{f_k : \{0,1\}^n \to \{0,1\}^n\}_k$ computable by a polynomial sized circtuit $C(k,x)$ that on input an n-bit key k and n-bit value x, outputs $f_k(x)$.

Problem 2: Following [Barak et al.], in class we went to a great length to prove that also the seemingly weaker definition **BB1** is not achievable. In class it was conjectured that definition 1 and definition 2 are equivalent, i.e., if an obfuscator O satisfies **BB1**, then it also satisfies **BB**. If true, this, together with problem 1, would give a much simpler proof that **BB1** is not achievable. In fact, it would be enough to prove the following somehow weaker claim, where you can modify the obfuscator to achieve the stronger definition.

Claim If there is a PPT obfuscator O achieving **BB1**, then there is a PPT obfuscator O' achieving **BB**.

Prove (or disprove) the claim. Notice that the impossibility of achieving **BB1** already shows that the claim is vacuously true because the premise is false. That's not the type of proof we are interested in. You should interpret the question as asking to give a constructive method to transform O into O'.

Problem 3: This is similar to problem 2, but using the definition of best possible obfuscation, as defined by [Goldwasser & Rothblum]. Recall that this definition is similar to **BB**, but with the difference that the simulator is given a circtuit equivalent to C, rather than just black-box access to it.

Definition An obfuscator O achieves best possible security (**BP**) if for any PPT adversary A there is a PPT simulator S such that for any circuits C and C' with $C \equiv C'$ and $|C'| = |O(C)|$, the distributions $A(O(C))$ and $S(C')$ are computationally indistinguishable, i.e., for any polynomial time distinguisher D, $\Pr\{D(A(O(C)))\} \approx \Pr\{D(S(C'))\}$.

Again, we also consider a restricted definition where the adversary is a predicate, i.e., it outputs a single bit.

Definition An obfuscator O achieves 1-bit best possible security (**BP1**) if for any PPT adversary A there is a PPT simulator S such that for any circuits C and C' with $C \equiv C'$ and $|C'| = |O(C)|$, $\Pr\{A(O(C))\} \approx \Pr\{S(C')\}$.

Prove (or disprove) the following claim.

Claim If there is a PPT obfuscator O achieving **BP1**, then there is a PPT obfuscator O' achieving **BP**.