ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: On Statistically Secure Obfuscation with Approximate Correctness

Author: Christina Brzuska, Technische Universität Hamburg-Harburg

Goldwasser and Rothblum (TCC '07) prove that statistical indistinguishability obfuscation (iO) cannot exist if the obfuscator must maintain perfect correctness (under a widely believed complexity theoretic assumption: $NP \not\subseteq SZK \subseteq AM \cap coAM$). However, for many applications of iO, such as constructing public-key encryption from one-way functions (one of the main open problems in theoretical cryptography), approximate correctness is sufficient. It had been unknown thus far whether statistical approximate iO (saiO) can exist.

We show that saiO does not exist, even for a minimal correctness requirement, if $NP \not\subseteq AM \cap coAM$, and if one-way functions exist. A simple complementary observation shows that if one-way functions do not exist, then average-case saiO exists. Technically, previous approaches utilized the behavior of the obfuscator on evasive functions, for which saiO always exists. We overcome this barrier by using a PRF as a ``baseline'' for the obfuscated program.

We broaden our study and consider relaxed notions of security for iO. We introduce the notion of correlation obfuscation, where the obfuscations of equivalent circuits only need to be mildly correlated (rather than statistically indistinguishable). Perhaps surprisingly, we show that correlation obfuscators exist via a trivial construction for some parameter regimes, whereas our impossibility result extends to other regimes. Interestingly, within the gap between the parameters regimes that we show possible and impossible, there is a small fraction of parameters that still allow to build public-key encryption from one-way functions and thus deserve further investigation.

This is joint work with Zvika Brakerski and Nils Fleischhacker.