Indistinguishability Obfuscation from Well-Founded Assumptions

Huijia (Rachel) Lin ✉ 🏠
Paul G. Allen School of Computer Science & Engineering,
University of Washington, Seattle, WA, USA

Abstract

Indistinguishability obfuscation, introduced by Barak et al. [Crypto 2001], aims to compile programs into unintelligible ones while preserving functionality. It is a fascinating and powerful object that has been shown to enable a host of new cryptographic goals and beyond. However, constructions of indistinguishability obfuscation have remained elusive, with all other proposals relying on heuristics or newly conjectured hardness assumptions. In this work, we show how to construct indistinguishability obfuscation from the subexponential hardness of three well-founded assumptions. We prove the following.

▶ **Theorem 1** (Informal). *Assume sub-exponential hardness for the following:*

- *the Learning Parity with Noise (*LPN*) assumption over general prime fields $\mathbb{F}_p$ with polynomially many* LPN *samples and error rate $1/k^\delta$, where k is the dimension of the* LPN *secret, and $\delta > 0$ is any constant;*
- *the existence of a Boolean Pseudo-Random Generator (*PRG*) in* NC^0 *with stretch $n^{1+\tau}$, where n is the length of the* PRG *seed, and $\tau > 0$ is any constant;*
- *the Decision Linear (*DLIN*) assumption on symmetric bilinear groups of prime order.*

Then, (subexponentially secure) indistinguishability obfuscation for all polynomial-size circuits exist.

As a corollary, all cryptographic goals that can be achieved using indistinguishability obfuscation can now be achieved assuming the above three assumptions. This includes fully homomorphic encryption, functional encryption, multiparty non-interactive key-exchange, succinct garbled random access machine, and many others.

This is joint work with Aayush Jain (UCLA and NTT Research) and Amit Sahai (UCLA).

2012 ACM Subject Classification Theory of computation → Cryptographic primitives

Keywords and phrases Cryptography, indistinguishability obfuscation

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2021.4

Category Invited Talk

41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2021).
Editors: Mikołaj Bojańczyk and Chandra Chekuri; Article No. 4; pp. 4:1–4:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany