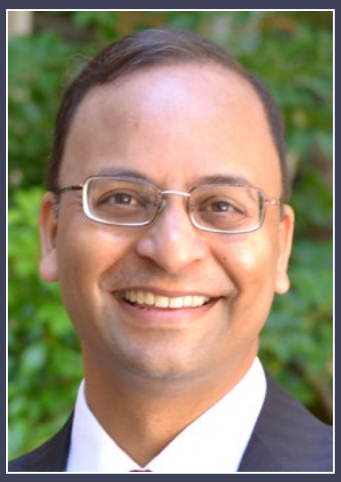
LECTURE SERIES

Mathematical Science Literature

March 23, 2021

5:00pm ET- *Virtually*



Amit Sahai

University of California, Los Angeles

"Indistinguishability Obfuscation: How to Hide Secrets within Software"

At least since the initial public proposal of public-key cryptography based on computational hardness conjectures (Diffie and Hellman, 1976), cryptographers have contemplated the possibility of a "one-way compiler" that translates computer programs into "incomprehensible" but equivalent forms. And yet, the search for such a "one-way compiler" remained elusive for decades.

In this talk, we look back at our community's attempts to formalize the notion of such a compiler, culminating in our 2001 work with Barak, Goldreich, Impagliazzo, Rudich, Vadhan, and Yang, which proposed the notion of indistinguishability obfuscation (iO). Roughly speaking, iO requires that the compiled versions of any two equivalent programs (with the same size and running time) be indistinguishable to any efficient adversary. Leveraging the notion of punctured programming, introduced in our work with Waters in 2013, well over a hundred papers have explored the remarkable power of iO.

We'll then discuss the intense effort that recently culminated in our 2020 work with Jain and Lin, finally showing how to construct iO in such a way that, for the first time, we can prove the security of our iO scheme based on well-studied computational hardness conjectures in cryptography.

This lecture will be held virtually.

Click here to register

HARVARD UNIVERSITY
CENTER OF MATHEMATICAL SCIENCES AND APPLICATIONS

cmsa.fas.harvard.edu/literature-lecture-series/