Average-Case Fine-Grained Hardness, or: How I Learned to Stop Worrying and Love the Oded

Alon Rosen

We present functions that are hard to compute on average for algorithms running in some fixed polynomial time, assuming widely-conjectured worst-case hardness of certain problems from the study of fine-grained complexity.

We discuss the relevance of such average-case hardness to cryptography and present, as an illustration, an outline of a proof-of-work protocol constructed based on the hardness and certain structural properties of our functions.

Joint work with Marshall Ball, Manuel Sabin and Prashant Nalini Vasudevan