ESHAN CHATTOPADHYAY, Cornell University

Non-Malleable Extractors and Codes from Additive Combinatorics

Extractors are algorithms that produce purely random bits from defective sources. Non-malleable extractors generalize extractors in a strong way, and produce random bits even in the presence of adversaries. I will talk about an explicit construction of non-malleable extractors using a sum-product theorem over rings. If time permits, I will discuss applications to non-malleable codes which are an elegant generalization of error-correcting codes.

This is based on joint work with David Zuckerman.