Public Key Cryptography from Different Assumptions

Boaz Barak and Avi Wigderson

Abstract
We construct a new public key encryption based on two assumptions:

1. One can obtain a pseudorandom generator with small locality by connecting the outputs to the inputs using any sufficiently good unbalanced expander.

2. It is hard to distinguish between a random graph that is such an expander and a random graph where a (planted) random logarithmic-sized subset $S$ of the outputs is connected to fewer than $|S|$ inputs.

The validity and strength of the assumptions raise interesting new algorithmic and pseudorandomness questions, and we explore their relation to the current state-of-art.