Papers are presented in chronological order. Electronic versions of all papers are available on my home page (http://www.math.ias.edu/~boaz). Some papers also appear on the Cryptology ePrint and ECCC archives.

Journal papers.


Papers in refereed conferences.


