A revised version of Chapters 1,2,4 appears in the paper "On the Security of Modular Exponentiation with Application to the Construction of Pseudorandom Generators" by Oded Goldreich and Vered Rosen. This paper has been posted to ePrint, and can be retreived from the URL http://eprint.iacr.org/2000/.

ISSN 1433-8092