Preface

These are the proceedings of CaLC 2001, the first conference devoted to cryptography and lattices. We have long believed that the importance of lattices and lattice reduction in cryptography, both for cryptographic construction and cryptographic analysis, merits a gathering devoted to this topic. The enthusiastic response that we received from the program committee, the invited speakers, the many people who submitted papers, and the 90 registered participants amply confirmed the widespread interest in lattices and their cryptographic applications.

We thank everyone whose involvement made CaLC such a successful event; in particular we thank Natalie Johnson, Larry Larrivee, Doreen Pappas, and the Brown University Mathematics Department for their assistance and support.

March 2001 Jeffrey Hoffstein, Jill Pipher, Joseph Silverman

Organization

CaLC 2001 was organized by the Department of Mathematics at Brown University. The program chairs express their thanks to the program commitee and the additional external referees for their help in selecting the papers for CaLC 2001. The program chairs would also like to thank NTRU Cryptosystems for providing financial support for the conference.

Program Commitee

- Don Coppersmith <dcopper@us.ibm.com>
  IBM Research
- Jeffrey Hoffstein (co-chair) <jhoff@math.brown.edu>, <jhoff@ntru.com>
  Brown University and NTRU Cryptosystems
- Arjen Lenstra <arjen.lenstra@citicorp.com>
  Citibank, USA
- Phong Nguyen <Phong.Nguyen@ens.fr>
  ENS
- Andrew Odlyzko <amo@research.att.com>
  AT&T Labs Research
- Joseph H. Silverman (co-chair) <jhs@math.brown.edu>, <jhs@ntru.com>
  Brown University and NTRU Cryptosystems

External Referees

Ali Akhavi, Glenn Durfee, Nick Howgrave-Graham, Daniele Micciancio

Sponsoring Institutions

NTRU Cryptosystems, Inc., Burlington, MA <www.ntru.com>