Lecture Notes in Computer Science 2146
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Joseph H. Silverman (Ed.)

Cryptography and Lattices

International Conference, CaLC 2001
Providence, RI, USA, March 29-30, 2001
Revised Papers

Springer

Volume Editor

Joseph H. Silverman
Brown University, Mathematics Department - Box 1917
Providence, RI 02912, USA
E-mail: jhs@math.brown.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Cryptography and lattices : international conference, revised papers / CaLC 2001, Providence, RI, USA, March 29 - 30, 2001. Joseph H. Silverman (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2146)
ISBN 3-540-42488-1

CR Subject Classification (1998): E.3, F.2.1, F.2.2, G.1, I.1.2, G.2, K.4.4

ISSN 0302-9743
ISBN 3-540-42488-1 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, date conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN 10840224 06/3142 5 4 3 2 1 0

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

External Referees

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

Sponsoring Institutions

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

Table of Contents