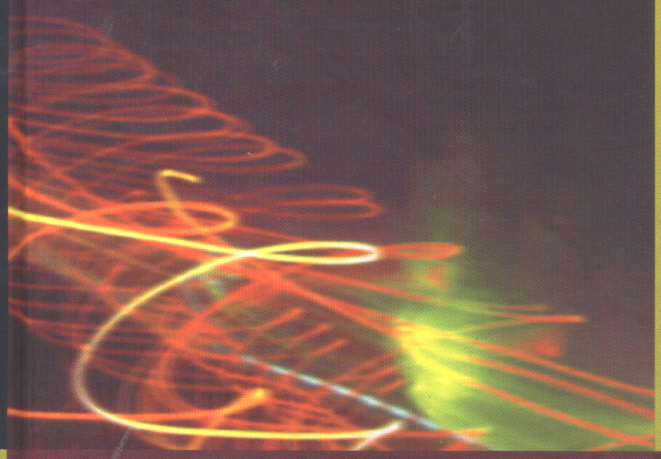
SPRINGER PROFESSIONAL COMPUTING



Darrel Hankerson
Alfred Menezes
Scott Vanstone

Guide to Elliptic Curve Cryptography

Springer

Guide to Elliptic Curve Cryptography

Darrel Hankerson
Alfred Menezes
Scott Vanstone

Guide to Elliptic Curve Cryptography

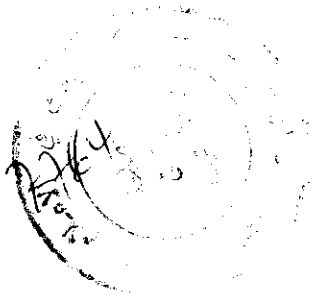
With 38 Illustrations

Springer

Darrel Hankerson
Department of Mathematics
Auburn University
Auburn, AL 36849-5107, USA
hankedr@auburn.edu

Alfred Menezes
Department of Combinatorics and
Optimization
University of Waterloo
Waterloo, Ontario, N2L 3G1 Canada
ajmeneze@uwaterloo.ca

Scott Vanstone
Department of Combinatorics and
Optimization
University of Waterloo
Waterloo, Ontario, N2L 3G1 Canada
savansto@uwaterloo.ca



Library of Congress Cataloging-in-Publication Data
Hankerson, Darrel R.
Guide to elliptic curve cryptography / Darrel Hankerson, Alfred J. Menezes, Scott Vanstone.
p. cm.
Includes bibliographical references and index.
ISBN 0-387-95273-X (alk. paper)
1. Computer security. 2. Public key cryptography. I. Vanstone, Scott A.
II. Menezes, A. J. (Alfred J.), 1965- III. Title.
QA76.9.A25H37 2003
005.8'2-dc22 2003059137

ISBN 0-387-95273-X Printed on acid-free paper.

Printed in the United States of America. (HAM)

9 8 7 6 5 4 3 2

Springer-Verlag is a part of *Springer Science+Business Media*

springeronline.com

Contents