

Cambridge University Press

052160415X - Advances in Elliptic Curve Cryptography

Edited by Ian F. Blake, Gadiel Seroussi and Nigel P. Smart

Copyright Information

[More information](#)

London Mathematical Society Lecture Note Series. 317

# Advances in Elliptic Curve Cryptography

Edited by

Ian F. Blake

*University of Toronto*

Gadiel Seroussi

*Hewlett-Packard Laboratories*

Nigel P. Smart

*University of Bristol*



**CAMBRIDGE**  
UNIVERSITY PRESS

Cambridge University Press

052160415X - Advances in Elliptic Curve Cryptography

Edited by Ian F. Blake, Gadiel Seroussi and Nigel P. Smart

Copyright Information

[More information](#)

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE  
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS  
The Edinburgh Building, Cambridge CB2 2RU, UK  
40 West 20th Street, New York, NY 10011-4211, USA  
477 Williamstown Road, Port Melbourne, VIC 3207, Australia  
Ruiz de Alarcón 13, 28014 Madrid, Spain  
Dock House, The Waterfront, Cape Town 8001, South Africa

<http://www.cambridge.org>

© Cambridge University Press 2005

This book is in copyright. Subject to statutory exception  
and to the provisions of relevant collective licensing agreements,  
no reproduction of any part may take place without  
the written permission of Cambridge University Press.

First published 2005

Printed in the United Kingdom at the University Press, Cambridge

*Typeface* Times 10/12 pt.    *System* L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub> [AU]

*A catalog record for this book is available from the British Library.*

*Library of Congress Cataloging in Publication Data*

Advances in elliptic curve cryptography / edited by Ian F. Blake, Gadiel Seroussi, Nigel P. Smart.

p. cm. – (London Mathematical Society lecture note series ; 317)

Includes bibliographical references and index.

ISBN 0-521-60415-X (alk. paper)

1. Computer security. 2. Public key cryptography. I. Blake, Ian F.

II. Seroussi, G. (Gadiel), 1955– III. Smart, Nigel P. (Nigel Paul), 1967– IV. Series.

QA76.9.A25A375 2004

005.8–dc22 2004054519

ISBN 0 521 60415 X paperback