PROTECTING INFORMATION

For many everyday transmissions, it is essential to protect digital information from noise or eavesdropping. This undergraduate introduction to error correction and cryptography is unique in devoting several chapters to quantum cryptography and quantum computing, thus providing a context in which ideas from mathematics and physics meet. By covering such topics as Shor's quantum factoring algorithm, this text informs the reader about current thinking in quantum information theory and encourages an appreciation of the connections between mathematics and science.

Of particular interest are the potential impacts of quantum physics: (i) a quantum computer, if built, could crack our currently used public-key cryptosystems; and (ii) quantum cryptography promises to provide an alternative to these cryptosystems, basing its security on the laws of nature rather than on computational complexity.

No prior knowledge of quantum mechanics is assumed, but students should have a basic knowledge of complex numbers, vectors, and matrices.

Susan Loepp is an Associate Professor of Mathematics in the Department of Mathematics and Statistics at Williams College. Her research is in commutative algebra, focusing on completions of local rings.

William K. Wootters, a Fellow of the American Physical Society, is the Barclay Jermain Professor of Natural Philosophy in the Department of Physics at Williams College. He does research on quantum entanglement and other aspects of quantum information theory.

"The authors have combined the two 'hot' subjects of cryptography and coding, looking at each with regard to both classical and quantum models of computing and communication. These exciting topics are unified through the steady, consistent development of algebraic structures and techniques. Students who read this book will walk away with a broad exposure to both the theory and the concrete application of groups, finite fields, and vector spaces."

– Ben Lotto, *Vassar College*

Protecting Information

From Classical Error Correction to Quantum Cryptography

SUSAN LOEPP
Williams College

WILLIAM K. WOOTTERS
Williams College

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521827409

First published 2006

Printed in the United States of America

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

Library of Congress Cataloging in Publication Data

Loepp, Susan.
Protecting information : from classical error correction to quantum cryptography /
Susan Loepp, William K. Wootters.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-521-82740-9 (hardback)
ISBN-10: 0-521-82740-X (hardback)
ISBN-13: 978-0-521-53476-5 (pbk.)
ISBN-10: 0-521-53476-3 (pbk.)
1. Quantum computers. 2. Computer security. I. Wootters, William Kent. II. Title.
QA76.889.L64 2006
004.1 – dc22 2006002404

ISBN-13 978-0-521-82740-9 hardback
ISBN-10 0-521-82740-X hardback

ISBN-13 978-0-521-53476-5 paperback
ISBN-10 0-521-53476-3 paperback

Dedicated to
Leona and Franzie,
Dorothy and Franzie,
and Adrienne, Mary, and Nate