SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Xun Yi • Russell Paulet • Elisa Bertino

Homomorphic Encryption and Applications

Springer

Xun Yi
RMIT University
Computer Science & Info Tech
Melbourne, VIC, Australia

Russell Paulet
Victoria University
Melbourne, VIC, Australia

Elisa Bertino
Computer Science
Purdue University
West Lafayette, IN, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-3-319-12228-1 ISBN 978-3-319-12229-8 (eBook)
DOI 10.1007/978-3-319-12229-8
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014953221

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To our families

Preface

Homomorphic encryption is a form of encryption that allows specific types of computations to be carried out on ciphertext and generate an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.

This is a desirable feature in modern communication system architectures. The homomorphic property of various cryptosystems can be used to create secure voting systems and private information retrieval schemes and enable widespread use of cloud computing by ensuring the confidentiality of processed data.

This book presents the basic homomorphic encryption techniques and their applications. It begins with an introduction of the history of encryption techniques from classical ciphers to secret key encryption and public-key encryption, including secret key encryption and public-key encryption models. It then provides the definition of homomorphic encryption followed by the description of some well-known homomorphic encryption schemes, such as the ElGamal and Paillier encryption schemes. On the basis of the homomorphic encryption concept, this book further introduces the state-of-the-art fully homomorphic encryption concept and describes the fully homomorphic encryption schemes over integers. After that, this book focuses on three applications of homomorphic encryption techniques. The first application introduces an electronic voting scheme on the basis of the ElGamal encryption scheme. The second application deals with nearest neighbor queries with location privacy on the basis of private information retrieval built on the Paillier encryption scheme. The third application discusses private searching on streaming data on the basis of fully homomorphic encryption schemes.

This book is designed to serve as a reference book for undergraduate- or graduate-level courses in computer science or mathematics departments, as a general introduction suitable for self-study (especially for beginning graduate students), and as a reference for students, researchers, and practitioners.

RMIT University, Melbourne, VIC, Australia — Xun Yi
Victoria University, Melbourne, VIC, Australia — Russell Paulet
Purdue University, West Lafayette, IN, USA — Elisa Bertino
September 2014

Acknowledgments

We would like to express our appreciation to Professor Udaya Parampalli (The University of Melbourne, Australia) and Dr. Junzuo Lai (Jinan University, China) for their comments on our book.

Contents