SPRINGER BRIEFS IN COMPUTER SCIENCE

Xun Yi
Russell Paulet
Elisa Bertino

Homomorphic Encryption and Applications

Springer

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

Chapter 1
Introduction

Abstract Encryption is the process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Encrypted data must be decrypted, before it can be read by the recipient. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers, and pictures. Today's encryption algorithms are divided into two categories: secret key and public key. Secret key encryption schemes use the same key (the secret key) to encrypt and decrypt a message, and public-key encryption schemes use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it, and all of today's encryption algorithms fit within those two categories. This chapter introduces the history of encryption techniques from classical ciphers to secret key encryption and public-key encryption, including secret key and public-key encryption models. It provides some background for homomorphic encryption.

1.1 Classical Ciphers

A cipher is a technique for hiding a message, by which letters of the message are substituted or transposed to other letters, letter pairs, and even many letters. In cryptography, a classical cipher is a type of cipher that was used historically but not now. In general, classical ciphers operate on an alphabet of letters (such as "A–Z") and can be implemented by hand or with simple mechanical devices. They are the most basic types of ciphers and not very secure, especially after new technology was developed. Modern schemes use computers or other digital technology and operate on bits and bytes.

Many classical ciphers were used by well-respected people, such as Julius Caesar and Napoleon, who created their own ciphers which were then popularly used. Many ciphers had their origins in the military and were used for transporting secret messages among people on the same side.

Classical schemes are often susceptible to ciphertext-only attacks, sometimes even without knowledge of the encryption system itself, using tools such as frequency analysis.

Classical ciphers are often divided into substitution ciphers, transposition ciphers, and product ciphers as follows:

X. Yi et al., *Homomorphic Encryption and Applications*, SpringerBriefs in Computer Science, DOI 10.1007/978-3-319-12229-8_1