

SpringerBriefs in Computer Science

Series Editors

Stan Zdonik

Shashi Shekhar

Jonathan Katz

Xindong Wu

Lakhmi C. Jain

David Padua

Xuemin (Sherman) Shen

Borko Furht

V.S. Subrahmanian

Martial Hebert

Katsushi Ikeuchi

Bruno Siciliano

Sushil Jajodia

Newton Lee

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

ISBN 978-3-319-12228-1

DOI 10.1007/978-3-319-12229-8

Springer Cham Heidelberg New York Dordrecht London

ISSN 2191-5776 (electronic)

ISBN 978-3-319-12229-8 (eBook)

Library of Congress Control Number: 2014953221

© Xun Yi, Russell Paulet, Elisa Bertino 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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
Victoria University, Melbourne, VIC, Australia
Purdue University, West Lafayette, IN, USA
September 2014

Xun Yi
Russell Paulet
Elisa Bertino

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

1	Introduction	1
1.1	Classical Ciphers	1
1.1.1	Substitution Ciphers	2
1.1.2	Transposition Ciphers	3
1.1.3	Product Ciphers	5
1.2	Secret Key Encryption	7
1.2.1	Secret Key Encryption Model	7
1.2.2	Data Encryption Standard	8
1.2.3	Advanced Encryption Standard	11
1.3	Public-Key Encryption	14
1.3.1	Public-Key Encryption Model	14
1.3.2	RSA	16
1.3.3	Rabin Public-Key Encryption	20
1.3.4	Public-Key Cryptography Standards	22
	References	24
2	Homomorphic Encryption	27
2.1	Homomorphic Encryption Definition	27
2.2	Goldwasser–Micali Encryption Scheme	29
2.3	ElGamal Encryption Scheme	32
2.4	Paillier Encryption Scheme	36
2.5	Boneh–Goh–Nissim Encryption Scheme	41
	References	46
3	Fully Homomorphic Encryption	47
3.1	Fully Homomorphic Encryption Definition	47
3.2	Overview of Fully Homomorphic Encryption Schemes	49
3.3	Somewhat Homomorphic Encryption Scheme over Integers	50
3.3.1	Secret Key Somewhat Homomorphic Encryption	50
3.3.2	Public-Key Somewhat Homomorphic Encryption	54
3.4	Fully Homomorphic Encryption Scheme over Integers	58
3.4.1	Squashed Encryption	58

- 3.4.2 Bootstrappable Encryption 63
 - 3.4.3 Implementation 64
 - References 65
- 4 Remote End-to-End Voting Scheme 67**
 - 4.1 Introduction 67
 - 4.2 Remote End-to-End Voting 70
 - 4.2.1 Participating Parties..... 70
 - 4.2.2 Basic Remote Voting Scheme 70
 - 4.2.3 General Remote Voting Scheme 74
 - 4.2.4 Voter Reference Refresh..... 76
 - 4.3 Conclusion and Discussion 78
 - References 78
- 5 Nearest Neighbor Queries with Location Privacy 81**
 - 5.1 Introduction 81
 - 5.2 Private k Nearest Neighbor Queries 84
 - 5.2.1 Security Model..... 84
 - 5.2.2 Private kNN Queries Without Data Privacy 87
 - 5.2.3 Private kNN Queries with Data Privacy 89
 - 5.2.4 Private kNN Queries Based on POI Type 91
 - 5.2.5 Private Cloaking Region..... 94
 - 5.3 Performance Analysis..... 96
 - 5.3.1 Protocol Performance..... 96
 - 5.3.2 Performance Comparison 97
 - 5.4 Conclusion and Discussion 97
 - References 98
- 6 Private Searching on Streaming Data 101**
 - 6.1 Introduction 101
 - 6.2 Overview of Private Searching on Streaming Data..... 103
 - 6.3 Preliminaries 106
 - 6.3.1 Integer Addition with FHE 106
 - 6.3.2 Integer Comparison with FHE 107
 - 6.3.3 Binary Linear Codes..... 107
 - 6.4 Definitions 108
 - 6.5 Private Threshold Query Based on Keyword Frequency 111
 - 6.5.1 Disjunctive Threshold Query..... 111
 - 6.5.2 Conjunctive Threshold Query 115
 - 6.5.3 Complement Threshold Query 118
 - 6.5.4 Generic Threshold Query..... 121
 - 6.6 Performance Analysis..... 122
 - 6.7 Conclusion and Discussion 124
 - References 125