

# Homomorphic Encryption for Financial Cryptography

V. Seethalakshmi · Rajesh Kumar Dhanaraj ·  
S. Suganyadevi · Mariya Ouaisa  
Editors

# Homomorphic Encryption for Financial Cryptography

Recent Inventions and Challenges

### *Editors*

V. Seethalakshmi  
Department of Electronics  
and Communication Engineering  
KPR Institute of Engineering  
and Technology  
Coimbatore, Tamil Nadu, India

S. Suganyadevi  
Department of Electronics  
and Communication Engineering  
KPR Institute of Engineering  
and Technology  
Coimbatore, Tamil Nadu, India

Rajesh Kumar Dhanaraj  
Symbiosis Institute of Computer Studies  
and Research (SICSR)  
Symbiosis International (Deemed  
University)  
Pune, India

Mariya Ouaisa   
Institute Specializing in New Information  
and Communication Technologies  
Moulay Ismail University  
Meknes, Morocco

ISBN 978-3-031-35534-9      ISBN 978-3-031-35535-6 (eBook)  
<https://doi.org/10.1007/978-3-031-35535-6>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are solely and exclusively licensed 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.

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.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This book offers to get insights regarding the efficient utilization of Homomorphic Encryption for Financial Cryptography in confidentiality, phishing, anonymity, object and user identity protection. In an era where there is a greater emphasis on privacy, owing mostly to rules such as General Data Protection Regulations (GDPR), the notion of Homomorphic Encryption (HE) has a lot of potential for real-world applications across a wide range of sectors. Homomorphic Encryption is a new technique that can help organizations protect their customers' privacy without affecting their capacity to obtain insights from their data. Homomorphic Encryption allows to evaluate or modify encrypted data without disclosing it to anyone. The possibilities provided by Homomorphic Encryption are nearly limitless.

Homomorphic Encryption enables enterprises to safely use cloud computing and storage services. It eliminates the need for users to choose between data security and usability. Organizations can use HE to exchange sensitive business data with other parties without disclosing the data or the results of the calculation to them. This may hasten cooperation and creativity while limiting the possibility of sensitive information being exposed. HE can enable organizations in highly regulated areas, like health care and finance, to outsource research and analytical services without fear of non-compliance.

This edited book aims to bring together leading academic researchers, scientists and research scholars to exchange and share their experiences and research results on all aspects of Homomorphic Encryption for Financial Cryptography. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends and concerns as well as practical challenges encountered and solutions adopted in the field of Homomorphic

Encryption for Financial Cryptography as a solution to increase the security of the data.

Coimbatore, India  
Pune, India  
Coimbatore, India  
Meknes, Morocco

V. Seethalakshmi  
Rajesh Kumar Dhanaraj  
S. Suganyadevi  
Mariya Ouaisa

# Contents

<b>Introduction to Homomorphic Encryption for Financial Cryptography</b> .....	1
Rajesh Kumar Dhanaraj, S. Suganyadevi, V. Seethalakshmi, and Mariya Ouaisa	
<b>A Survey on Homomorphic Encryption for Financial Cryptography Workout</b> .....	13
M. Siva Sangari, K. Balasamy, Habib Hamam, S. Nithya, and S. Surya	
<b>Improved Login Interface Algorithm for Financial Transactions Using Visual Cryptographic Authentication</b> .....	29
N. Sugirtham, R. Sherine Jenny, R. Sudhakar, S. Vasudevan, and Irfan Khan Tanoli	
<b>Securing Shared Data Based on Homomorphic Encryption Schemes</b> ...	53
K. Renuka Devi, S. Nithyapriya, G. Pradeep, R. Menaha, and S. Suganyadevi	
<b>Challenges and Opportunities Associated with Homomorphic Encryption for Financial Cryptography</b> .....	85
S. Finney Daniel Shadrach, A. Shiny Pershiya, A. Shirley Stevany Faryl, K. Balasamy, and K. Chiranjeevi	
<b>Homomorphic Encryption-Based Cloud Privacy-Preserving in Remote ECG Monitoring and Surveillance</b> .....	107
V. Seethalakshmi, S. Suganyadevi, S. Nithya, K. Sheela Sobana Rani, and Gokul Basavaraj	
<b>Enhancing Encryption Security Against Cypher Attacks</b> .....	125
R. Naveenkumar, N. M. Sivamangai, A. Napoleon, and S. Sridevi Sathyapriya	

**Biometric-Based Key Generation Using AES Algorithm  
for Real-Time Security Applications ..... 157**  
S. Sridevi Sathya Priya, N. M. Sivamangai, R. Naveenkumar,  
A. Napoleon, and G. Saranya

**Financial Cryptography and Its Application in Blockchain ..... 181**  
V. Sathya, Sridhar Chandrasekaran, and Govindasamy Madhaiyan

**Algorithmic Strategies for Solving Complex Problems in Financial  
Cryptography ..... 207**  
Vani Rajasekar, K. Venu, Vandana Sharma, and Muzafer Saracevic

**Various Attacks on the Implementation of Cryptographic  
Algorithms ..... 221**  
P. Kanaga Priya, R. Sivaranjani, K. Thangaraj, and Naif Alsharabi

**A Survey on Private Keyword Sorting and Searching  
Homomorphic Encryption ..... 259**  
S. Nithya, V. Seethalakshmi, G. Vetrichelvi, M. Siva Sangari,  
and Gokul Basavaraj

**Multivariate Cryptosystem Based on a Quadratic Equation  
to Eliminate the Outliers Using Homomorphic Encryption Scheme ..... 277**  
M. Janani, R. Jeevitha, R. Jaikumar, R. Suganthi, and S. Jhansi Ida