EAI/Springer Innovations in Communication and Computing

Series Editor
Imrich Chlamtac, European Alliance for Innovation, Ghent, Belgium

Editor's Note

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

Khairol Amali Bin Ahmad • Khaleel Ahmad
Uma N. Dulhare
Editors

Functional Encryption

Springer

EAI
RESEARCH MEETS INNOVATION

Editors
Khairol Amali Bin Ahmad
National Defence University of Malaysia
Kem, Kuala Lumpur, Malaysia

Uma N. Dulhare
Muffakham Jah College of Engineering and Technology
Hyderabad, Telangana, India

Khaleel Ahmad
Department of Computer Science and Information Technology
Maulana Azad National Urdu University
Hyderabad, Telangana, India

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-60889-7 ISBN 978-3-030-60890-3 (eBook)
https://doi.org/10.1007/978-3-030-60890-3

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

Foreword

Digital security is of utmost importance since half of the world's population uses smartphones. Thus, it touches the lives of common people worldwide. In this digital age, hiding and encrypting important data is one of the major challenges. Functional encryption schemes enhance the security, confidentiality and access control by using the function which allows the sharing of information with authorized people. For newcomers, students from another branch, or researchers who are new and want to understand and learn the basics of functional encryption, the search for any source material that fulfills these demands is often unsuccessful. Most books written on this topic are targeted at those who already possess knowledge of the basics. This can lead to the novice losing interest in this field because they cannot find a book written for them. Thus, this book will satisfy these readers, as it has been written with them in mind.

This is perhaps the first book about functional encryption written specifically for the novice. This book covers functional encryption algorithms and its modern applications in developing secure systems. The latest functional encryption algorithms are explained in a simple and precise manner. Examples are given to solidify the concepts and increase understanding.

This book helps professionals, researchers, scientists, faculty members, research scholars, graduate students, and software developers in the domain of Cryptography/Cybersecurity/Information Security/Software Security/Database Security/Web Security/Wireless Network Security/Cloud Security/Online Transactions/E-Commerce Security/M-Commerce Security for better understanding of the basic concepts and techniques to build functional encryption and various encryption mechanisms such as identity-based encryption (IBE) and attribute-based encryption (ABE) into real-world systems. Those who seek to understand these concepts and techniques will find this book a valuable asset. The editors have edited this book to provide awareness of the methods used for functional encryption in the academic and professional communities.

Riverside, USA — Mohammad Sufian Badar

Preface

Information security is the protection of information systems, hardware, software, and information from damages as well as theft, interruption, or misdirection to any of these resources. In other words, cybersecurity focuses on protecting computers, networks, programs, and data (in use, in rest, in motion) from unauthorized or unintended access, change, or destruction (all aimed for exploitation). It is estimated that 3300 million people are using smart mobile phones globally, which is more than half of the world's population. Hence, digital security is no longer limited to the scholarly community but is now the concern of all users of computers worldwide.

In acknowledging such expansion and needs of information security, this book is aimed to provide awareness of methods used for functional encryption in the academic and professional community. While this book would dwell on the foundations of functional encryption as part of security, it will also focus on contemporary topics for Research and Development.

The chapters cover functional encryption algorithms and its modern applications in developing secure systems, viz. entity authentication, message authentication, software security, cybersecurity, hardware security, Internet of Thing (IoT), cloud security, smart card technology, CAPTCHA, digital signature, and digital watermarking. This book is organized into 15 chapters, i.e., Foundations of functional encryption, Impact of Group Theory in Cryptosystem, Elliptic Curve Cryptography, Hyper Elliptic Curve Cryptography (HECC), XTR algorithm: Efficient and Compact Subgroup Trace Representation, Pairing-based cryptography, NTRU Algorithm: Nth Degree Truncated Polynomial Ring Units, Cocks IBE scheme, Boneh-Franklin IBE, Boneh-Boyen IBE, Sakai-Kasahara IBE, Hierarchical Identity-Based Encryption, Attribute-based Encryption, Extensions of IBE and Related Primitives, Digital Signatures.

Finally, it gives us great pleasure to acknowledge the contributions and supports of many individuals. Indeed, we would like to express our gratitude to all the authors who had contributed in the forms of the submitted chapters without which, the production of this book is not possible. We are also thankful to the team from

Springer for the meticulous service in timely publication of this book. We would like also to thank our college/University for their encouragement and last but not least, we gratefully appreciate the support, encouragement, and patience of our families.

Kuala Lumpur, Malaysia — Khairol Amali Bin Ahmad

Hyderabad, Telangana, India — Khaleel Ahmad

Hyderabad, Telangana, India — Uma N. Dulhare

Contents