Pro Cryptography and Cryptanalysis with C++20

Creating and Programming Advanced Algorithms

Marius Iulian Mihailescu
Stefania Loredana Nita

Apress®

Pro Cryptography and Cryptanalysis with C++20: Creating and Programming Advanced Algorithms

Marius Iulian Mihailescu
Bucharest, Romania

Stefania Loredana Nita
Bucharest, Romania

ISBN-13 (pbk): 978-1-4842-6585-7
ISBN-13 (electronic): 978-1-4842-6586-4
https://doi.org/10.1007/978-1-4842-6586-4

Copyright © Marius Iulian Mihailescu and Stefania Loredana Nita 2021, corrected publication 2021

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.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

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.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Steve Anglin
Development Editor: Matthew Moodie
Editorial Operations Manager: Mark Powers

Cover designed by eStudioCalamar

Cover image by Devin Avery on Unsplash (www.unsplash.com)

Distributed to the book trade worldwide by Apress Media, LLC, 1 New York Plaza, New York, NY 10004, U.S.A. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484265857. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

To our families.

Table of Contents

About the Authors

Marius Iulian Mihailescu, PhD is the CEO of Dapyx Solution Ltd., a company based in Bucharest, Romania. He is involved in information security- and cryptography-related research projects. He is a lead guest editor for applied cryptography journals and a reviewer for multiple publications on information security and cryptography profiles. He has authored and co-authored more than 30 articles for conference proceedings, 25 articles for journals, and four books. For more than six years he has served as a lecturer at well-known national and international universities (University of Bucharest, Titu Maiorescu University, Spiru Haret University of Bucharest, and Kadir Has University, Istanbul, Turkey). He has taught courses on programming languages (C#, Java, C++, Haskell) and object-oriented system analysis and design with UML, graphs, databases, cryptography, and information security. He worked for three years as an IT Officer at Royal Caribbean Cruises Ltd. where he dealt with IT infrastructure, data security, and satellite communications systems. He received his PhD in 2014 and his thesis is on applied cryptography over biometrics data. He holds MSc degrees in information security and software engineering.

Stefania Loredana Nita, PhD is a software developer and researcher at the Institute for Computers of the Romanian Academy. Her PhD thesis is on advanced cryptographic schemes using searchable encryption and homomorphic encryption. At the Institute for Computers, she works on research and development projects that involve searchable encryption, homomorphic encryption, cloud computing security, Internet of Things, and big data. She worked for more than two years as an assistant lecturer at the University of Bucharest where she taught courses on advanced programming techniques, simulation methods, and operating systems. She has authored and co-authored more than 25 workpapers for conferences and journals, and has co-authored four books. She is a lead guest editor for special issues on information security and cryptography such as *Advanced Cryptography and Its Future: Searchable and Homomorphic Encryption.* She has an MSc degree in software engineering and BSc degrees in computer science and mathematics.

About the Technical Reviewer

Doug Holland is a Software Engineer and Architect at Microsoft Corporation. He holds a Master's degree in software engineering from the University of Oxford. Before joining Microsoft, he was awarded the Microsoft MVP and Intel Black Belt Developer awards.

Acknowledgments

We would like to thank our editors for their support, our technical reviewer for his constructive comments and suggestions, the entire team that makes publishing this book possible, and last but not least, our families for their unconditional support and encouragement.