New Frontiers in Cryptography

Khaled Salah Mohamed

New Frontiers in Cryptography

Quantum, Blockchain, Lightweight, Chaotic and DNA

Springer

Khaled Salah Mohamed
A Siemens Business
Fremont, CA, USA

ISBN 978-3-030-58995-0 ISBN 978-3-030-58996-7 (eBook)
https://doi.org/10.1007/978-3-030-58996-7

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

Dedicated to the memory of my grandfather and grandmother.

Preface

Today, cryptography plays a vital role in every electronic and communication system. Everyday, many users generate and interchange large amount of information in various fields through internet, telephone conversations and e-commerce transactions. In modern system-on-chips (SoCs), cryptography plays an integral role in protecting the confidentiality and integrity of information. This book provides comprehensive coverage of various cryptography topics, while highlighting the most recent trends such as quantum, blockchain, lightweight, chaotic and DNA cryptography. Moreover, this book covers cryptography primitives and their usage and applications and focuses on the fundamental principles of modern cryptography such as stream ciphers, block ciphers, public key algorithms and digital signatures. The readers will build a solid foundation in cryptography and security. This book presents the fundamental mathematical concepts of cryptography. Moreover, this book presents hiding data techniques such as steganography and watermarking. Besides, it provides a comparative study of the different cryptographic methods that can be used efficiently to solve security problems. This book discusses modern cryptography and data hiding techniques. This includes:

- *Stream ciphers, block ciphers, public key algorithms and digital signatures*.
- *Quantum cryptography*: Quantum cryptography uses physics to develop a cryptosystem completely secure against being compromised without the knowledge of the sender or the receiver of the messages.
- *Blockchain cryptography*: Blockchain is a distributed database that allows direct transactions between two parties without the need for an authoritative mediator. Blockchain cryptography is a way to encapsulate transactions in the form of blocks where blocks are linked through the cryptographic hash, hence forming a chain of secured blocks.
- *Lightweight cryptography*: Lightweight cryptography works between the tradeoffs of security, cost, and performance and is focused at devices and systems on edge.
- *Chaotic cryptography*: Many strong ciphers have been applied widely, such as DES, AES and RSA. But most of them cannot be directly used to encrypt

real-time embedded systems because their encryption speed is not fast enough and they are computationally intensive. So, chaotic cryptography is suitable for real-time embedded systems in terms of performance, area and power efficiency.

- *DNA cryptography*: DNA cryptography is a promising and rapid emerging field in data security. DNA cryptography may bring forward a new hope for unbreakable algorithms. DNA cryptology combines cryptology and modern biotechnology.
- *Steganography*: Steganography is the art of hiding the existence of a message between sender and intended recipient. It hides secret messages in various types of files such as text, images, audio and video.
- *Watermarking*: Watermarking is embedding some information within a digital media so that the digital media looks unchanged. This is useful for copy protection.

Fremont, CA, USA Khaled Salah Mohamed

Contents