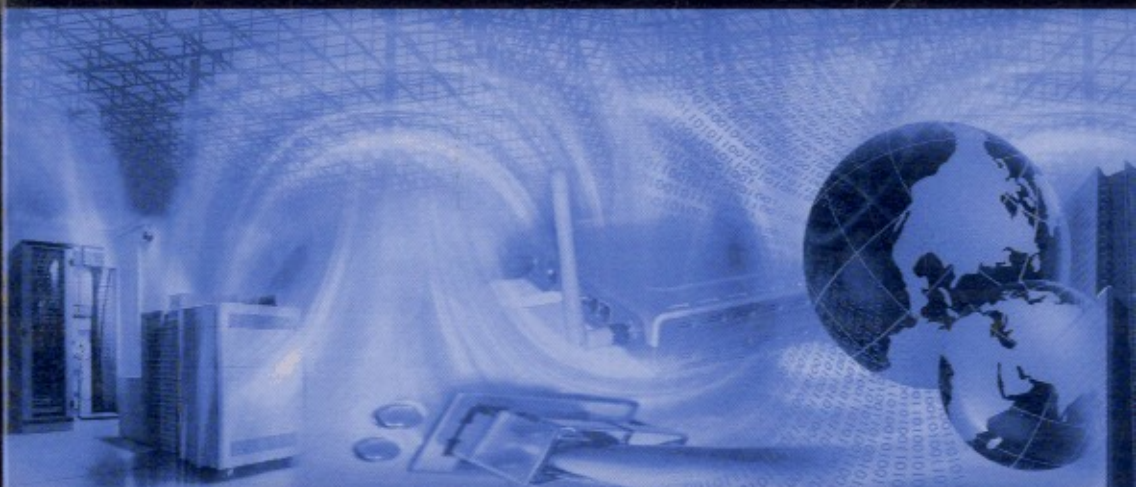


WIRELESS SECURITY AND CRYPTOGRAPHY

Specifications and Implementations



Edited by
NICOLAS SKLAVOS
XINMIAO ZHANG



CRC Press
Taylor & Francis Group

Table of Contents

Chapter 1

Overview of Cryptographic Primitives for Secure Communication.....	1
<i>Palash Sarkar</i>	

Chapter 2

Introduction to Communication Security.....	29
<i>Vesna Hassler</i>	

Chapter 3

Efficient VLSI Architectures for the Advanced Encryption Standard Algorithm	45
<i>Xinmiao Zhang</i>	

Chapter 4

Hardware Design Issues in Elliptic Curve Cryptography for Wireless Systems	79
<i>Apostolos P. Fournaris and O. Koufopavlou</i>	

Chapter 5

Efficient Elliptic Curve Cryptographic Hardware Design for Wireless Security	153
<i>Lo'ai A. Tawalbeh and Çetin Kaya Koç</i>	

Chapter 6

Cryptographic Algorithms in Constrained Environments	177
<i>Vincent Rijmen and Norbert Pramstaller</i>	

Chapter 7

Side-Channel Analysis Attacks on Hardware Implementations of Cryptographic Algorithms	213
<i>Siddika Berna Örs, Bart Preneel, and Ingrid Verbauwhede</i>	

Chapter 8

Security Enhancement Layer for Bluetooth.....	249
<i>Panu Hämäläinen, Marko Hännikäinen, and Timo D. Hämäläinen</i>	

Chapter 9

WLAN Security Processing Architectures..... 275

Neil Smyth, Maire McLoone, and John V. McCanny

Chapter 10

Security Architecture and Implementation of the Universal Mobile
Telecommunication System 295

Paris Kitsos and Nicolas Sklavos

Chapter 11

Wireless Application Protocol Security Processor: Privacy,
Authentication, and Data Integrity..... 315

Nicolas Sklavos

Chapter 12

Binary Algorithms for Multiplicative Inversion 341

Erkay Savas

Chapter 13

Smart Card Technology..... 363

Martin Manninger

Index..... 389