

Contents

Part I Basics

- 1 Modular Integer Arithmetic for Public-Key Cryptography** 3
Tim Güneysu and Christof Paar
- 2 Introduction to Side-Channel Attacks** 27
François-Xavier Standaert

Part II Cryptomodules and Arithmetic

- 3 Secret Key Crypto Implementations** 45
Guido Marco Bertoni and Filippo Melzani
- 4 Arithmetic for Public-Key Cryptography** 63
Kazuo Sakiyama and Lejla Batina
- 5 Hardware Design for Hash Functions** 79
Yong Ki Lee, Miroslav Knežević, and Ingrid M.R. Verbauwhede

Part III Design Methods for Security

- 6 Random Number Generators for Integrated Circuits and FPGAs** ... 107
Berk Sunar and Dries Schellekens
- 7 Process Variations for Security: PUFs** 125
Roel Maes and Pim Tuyls

Part IV Applications

8 Side-Channel Resistant Circuit Styles and Associated IC Design Flow	145
Kris Tiri	
9 Counteracting Power Analysis Attacks by Masking	159
Elisabeth Oswald and Stefan Mangard	
10 Compact Public-Key Implementations for RFID and Sensor Nodes ..	179
Lejla Batina, Kazuo Sakiyama, and Ingrid M.R. Verbauwhede	
11 Demonstrating End-Point Security in Embedded Systems	197
Patrick Schaumont, Eric Simpson, and Pengyuan Yu	
12 From Secure Memories to Smart Card Security	215
Helena Handschuh and Elena Trichina	
Index	235



<http://www.springer.com/978-0-387-71827-9>

Secure Integrated Circuits and Systems

Verbauwhede, I.M.R. (Ed.)

2010, X, 246 p. 92 illus., Hardcover

ISBN: 978-0-387-71827-9