

Contents

Part I Physically Unclonable Functions (PUFs)

Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions	3
Roel Maes and Ingrid Verbauwhede	

Hardware Intrinsic Security from Physically Unclonable Functions	39
Helena Handschuh, Geert-Jan Schrijen, and Pim Tuyls	

From Statistics to Circuits: Foundations for Future Physical Unclonable Functions	55
Inyoung Kim, Abhranil Maiti, Leyla Nazhandali, Patrick Schaumont, Vignesh Vivekraj, and Huaiye Zhang	

Strong PUFs: Models, Constructions, and Security Proofs	79
Ulrich Rührmair, Heike Busch, and Stefan Katzenbeisser	

Part II Hardware-Based Cryptography

Leakage Resilient Cryptography in Practice	99
François-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald	

Memory Leakage-Resilient Encryption Based on Physically Unclonable Functions	135
Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Berk Sunar, and Pim Tuyls	

Part III Hardware Attacks

Hardware Trojan Horses 167
 Mohammad Tehranipoor and Berk Sunar

**Extracting Unknown Keys from Unknown Algorithms Encrypting
 Unknown Fixed Messages and Returning No Results** 189
 Yoo-Jin Baek, Vanessa Gratzner, Sung-Hyun Kim, and David Naccache

Part IV Hardware-Based Policy Enforcement

License Distribution Protocols from Optical Media Fingerprints 201
 Ghaith Hammouri, Aykutlu Dana, and Berk Sunar

Anti-counterfeiting: Mixing the Physical and the Digital World 223
 Darko Kirovski

Part V Hardware Security in Contactless Tokens

**Anti-counterfeiting, Untraceability and Other Security Challenges for
 RFID Systems: Public-Key-Based Protocols and Hardware** 237
 Yong Ki Lee, Lejla Batina, Dave Singelee, Bart Preneel, and
 Ingrid Verbauwhede

**Contactless Security Token Enhanced Security by Using New Hardware
 Features in Cryptographic-Based Security Mechanisms** 259
 Markus Ullmann and Matthias Vögeler

**Enhancing RFID Security and Privacy by Physically Unclonable
 Functions** 281
 Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann

Part VI Hardware-Based Security Architectures and Applications

**Authentication of Processor Hardware Leveraging Performance Limits
 in Detailed Simulations and Emulations** 309
 Daniel Y. Deng, Andrew H. Chan, and G. Edward Suh

Signal Authentication in Trusted Satellite Navigation Receivers 331
 Markus G. Kuhn

On the Limits of Hypervisor- and Virtual Machine Monitor-Based Isolation	349
Loic Duflot, Olivier Grumelard, Olivier Levillain, and Benjamin Morin	
Efficient Secure Two-Party Computation with Untrusted Hardware Tokens	367
Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider	
Towards Reliable Remote Healthcare Applications Using Combined Fuzzy Extraction	387
Jorge Guajardo, Muhammad Asim, and Milan Petković	

Towards Hardware-Intrinsic Security

Foundations and Practice

Sadeghi, A.-R.; Naccache, D. (Eds.)

2010, XVI, 407 p., Hardcover

ISBN: 978-3-642-14451-6