
Contents

| | |
|--|---------------|
| About the authors | xv |
| Acknowledgments | xvii |
| Foreword by Thomas M. Coughlin | xix |
| Foreword by Pradipta Patra | xxi |
| Foreword by Swarup Bhunia | xxiii |
| Foreword by Peter Corcoran | xxv |
| Preface | xxvii |
| List of acronyms | xxxi |
| List of notations | xxxvii |
| | |
| 1 Introduction to IP core protection and hardware-assisted security of consumer electronics | 1 |
| 1.1 Consumer electronics and security perspectives | 1 |
| 1.2 Hardware-assisted security and IP core protection | 3 |
| 1.3 Intellectual property (IP) cores/hardware | 4 |
| 1.3.1 Utility of IP cores in CE devices | 4 |
| 1.3.2 Why security and protection of hardware/IP cores? | 5 |
| 1.3.3 Traditional forms of IP protection not enough? | 6 |
| 1.4 IP core protection and hardware-assisted security of CE device—DSP core | 6 |
| 1.4.1 Security and protection methodologies available for IP core/hardware | 7 |
| 1.4.2 Different IP core protection and hardware-assisted security mechanisms: advantages and disadvantages | 12 |
| 1.4.3 HLS (architectural synthesis) as design backbone for implementing security algorithms for DSP IP cores | 13 |
| 1.5 Hardware-assisted media protection | 15 |
| 1.6 Physical unclonable functions | 16 |
| 1.7 Organization of the book | 17 |
| 1.8 Conclusions | 19 |
| 1.9 Exercises | 19 |
| References | 20 |
| | |
| 2 Security in consumer electronics and internet of things (IoT) | 23 |
| 2.1 Internet of things (IoT) – a broad overview | 23 |
| 2.1.1 IoT – architecture | 25 |
| 2.1.2 IoT – driving technology | 27 |

| | | |
|----------|---|-----------|
| 2.1.3 | IoT – applications | 28 |
| 2.1.4 | IoT – challenges | 30 |
| 2.2 | Security, privacy, IPR in IoT, and consumer electronic systems – a big picture | 31 |
| 2.2.1 | IoT security – attacks and countermeasures | 32 |
| 2.2.2 | Trustworthy consumer electronic systems | 34 |
| 2.2.3 | Hardware-assisted security and protection | 35 |
| 2.2.4 | Different aspects of security and privacy | 37 |
| 2.2.5 | Different aspects of intellectual property (IP), ownership right, or copyright protection | 38 |
| 2.3 | Memory security | 39 |
| 2.3.1 | Memory security attacks | 39 |
| 2.3.2 | Memory security solutions | 40 |
| 2.4 | Radio-frequency identification (RFID) security | 43 |
| 2.4.1 | RFID security attacks | 43 |
| 2.4.2 | RFID security solutions | 44 |
| 2.5 | Near-field communications (NFC) security | 46 |
| 2.5.1 | NFC security attacks | 47 |
| 2.5.2 | NFC security solutions | 48 |
| 2.6 | Smart transportation security | 50 |
| 2.6.1 | Smart car security | 51 |
| 2.6.2 | UAV or drone security | 55 |
| 2.7 | Smart healthcare security | 58 |
| 2.7.1 | Smart healthcare security attacks | 59 |
| 2.7.2 | Smart healthcare security solutions | 60 |
| 2.8 | Firmware | 62 |
| 2.8.1 | Firmware attacks | 62 |
| 2.8.2 | Firmware solutions | 63 |
| 2.9 | Blockchain technology | 64 |
| 2.9.1 | Blockchain – overview | 65 |
| 2.9.2 | Blockchain – application | 66 |
| 2.9.3 | Blockchain as a security framework | 67 |
| 2.9.4 | Blockchain – issues | 68 |
| 2.10 | Conclusions | 69 |
| 2.11 | Exercises | 69 |
| | References | 70 |
| 3 | Trojan security aware DSP IP core and integrated circuits | 79 |
| 3.1 | Introduction | 79 |
| 3.2 | Types of hardware Trojans | 81 |
| 3.2.1 | Trojan features | 81 |
| 3.2.2 | Benefit of Trojan security at higher abstraction level | 84 |
| 3.2.3 | Threat model | 85 |
| 3.3 | Hardware Trojan in a 3PIP module | 86 |
| 3.3.1 | Example of a hardware Trojan | 86 |
| 3.3.2 | Trojan detectability in a 3PIP module at RTL/lower levels | 87 |

| | | |
|----------|--|------------|
| 3.4 | Selected Trojan security approaches | 88 |
| 3.4.1 | Trojan security approaches for DSP cores | 88 |
| 3.4.2 | Trojan security approach for combinational/sequential circuits | 94 |
| 3.5 | Trojan security aware DSP IP core | 95 |
| 3.5.1 | Definition | 96 |
| 3.5.2 | Goal | 96 |
| 3.5.3 | Formulation | 97 |
| 3.5.4 | Models | 97 |
| 3.6 | Design process of Trojan secured DSP IP core | 99 |
| 3.6.1 | Deriving the CDFG of a DSP core | 99 |
| 3.6.2 | Generating the DMR of the CDFG | 108 |
| 3.6.3 | Trojan secured scheduling of DMR CDFG | 108 |
| 3.7 | Analysis of case studies/test cases | 113 |
| 3.7.1 | DSP applications and system setup for the case studies | 113 |
| 3.7.2 | Security analysis | 114 |
| 3.7.3 | Design cost analysis | 115 |
| 3.7.4 | Comparative perspectives | 116 |
| 3.8 | Conclusion | 117 |
| 3.9 | Exercises | 118 |
| | References | 119 |
| 4 | IP core and integrated circuit protection using robust watermarking | 123 |
| 4.1 | Introduction | 123 |
| 4.2 | Selected watermarking approaches | 124 |
| 4.3 | Design process of watermarked IP core/hardware | 128 |
| 4.3.1 | Problem formulation | 128 |
| 4.3.2 | Design process of single-phase watermarked IP core/hardware | 129 |
| 4.3.3 | Design process of triple-phase watermarked IP core/hardware | 148 |
| 4.3.4 | Desired properties of IP core watermark | 161 |
| 4.3.5 | Possible cases of dishonest claim of IP core/hardware ownership and its resolution | 162 |
| 4.4 | Analysis on case studies | 163 |
| 4.4.1 | Security analysis of triple-phase watermark for DSP IP cores | 163 |
| 4.4.2 | Design cost analysis of triple-phase watermark for DSP IP cores | 164 |
| 4.5 | Conclusion | 166 |
| 4.6 | Exercises | 168 |
| | References | 169 |
| 5 | Symmetrical protection of DSP IP core and integrated circuits using fingerprinting and watermarking | 171 |
| 5.1 | Introduction | 171 |
| 5.1.1 | Background on watermark and fingerprint | 173 |

| | | |
|----------|---|------------|
| 5.1.2 | Threat model | 173 |
| 5.1.3 | Benefits of protection at higher abstraction | 173 |
| 5.2 | Fundamentals of IP core protection | 174 |
| 5.2.1 | Overview on non-symmetric IP core protection techniques | 174 |
| 5.2.2 | Overview on symmetric IP core protection techniques | 175 |
| 5.3 | Symmetrical IP core protection for DSP core | 175 |
| 5.3.1 | Problem formulation | 177 |
| 5.3.2 | Symmetrically protected design—area evaluation model | 177 |
| 5.3.3 | Symmetrically protected design—delay evaluation model | 177 |
| 5.3.4 | Symmetrically protected design—cost evaluation function | 177 |
| 5.3.5 | Encoding rules of buyer fingerprint and seller watermark for DSP IP cores | 178 |
| 5.3.6 | Multi-variable signature embedding process | 180 |
| 5.3.7 | Signature detection process | 181 |
| 5.3.8 | Desirable properties of signature | 182 |
| 5.4 | Case study of symmetrical IP core protection | 182 |
| 5.4.1 | Demonstration of fingerprinting constraints embedding process | 183 |
| 5.4.2 | Demonstration of watermarking constraints embedding process | 186 |
| 5.5 | Analysis of case studies for DSP cores | 187 |
| 5.5.1 | Analysis of embedding cost, security metric on DSP Cores symmetrical protection | 188 |
| 5.5.2 | Comparative study between symmetrical and non-symmetrical technique | 190 |
| 5.6 | Conclusion | 194 |
| 5.7 | Exercises | 194 |
| | References | 195 |
| 6 | Computational forensic engineering for resolving ownership conflict of DSP IP core | 199 |
| 6.1 | Introduction | 199 |
| 6.1.1 | Overview of forensic engineering | 200 |
| 6.2 | Computational FE technology | 202 |
| 6.3 | IP core feature extraction algorithms | 204 |
| 6.3.1 | Feature extraction rules | 204 |
| 6.3.2 | IP core validation | 213 |
| 6.3.3 | Important characteristics of customized CFE | 214 |
| 6.4 | Analysis on case studies | 214 |
| 6.4.1 | Results of the customized CFE approach | 215 |
| 6.5 | Conclusion | 222 |
| 6.6 | Exercises | 222 |
| | References | 223 |

| | | |
|----------|---|------------|
| 7 | Structural obfuscation of DSP cores used in CE devices | 227 |
| 7.1 | Introduction | 227 |
| 7.1.1 | Threat model | 230 |
| 7.1.2 | Benefits of providing security at higher design abstraction level | 230 |
| 7.2 | Obfuscation for IP core protection—a broad view | 231 |
| 7.2.1 | Code obfuscation techniques | 231 |
| 7.2.2 | Logic obfuscation techniques | 231 |
| 7.2.3 | Structural obfuscation techniques | 232 |
| 7.3 | Compiler transformation-driven structural obfuscation | 233 |
| 7.3.1 | Formulation and evaluation models | 235 |
| 7.3.2 | Multistage high-level transformation techniques | 236 |
| 7.4 | Low-cost structural obfuscation for DSP IP core | 242 |
| 7.4.1 | Overview on PSO | 242 |
| 7.4.2 | Movement of particle | 242 |
| 7.4.3 | Terminating condition of PSO | 243 |
| 7.5 | A case study for multistage structural obfuscation | 243 |
| 7.6 | Analysis of case studies | 246 |
| 7.6.1 | Result of multistage structural obfuscation | 246 |
| 7.6.2 | Comparative study and discussion | 248 |
| 7.7 | Conclusion | 250 |
| 7.8 | Exercises | 251 |
| | References | 251 |
| 8 | Functional obfuscation of DSP cores used in CE devices | 255 |
| 8.1 | Introduction | 255 |
| 8.2 | Attack scenarios and threat model | 256 |
| 8.2.1 | Possible attack scenarios | 256 |
| 8.2.2 | Threat model | 259 |
| 8.3 | Selected functional obfuscation approaches | 260 |
| 8.4 | Design of functionally obfuscated DSP core | 262 |
| 8.4.1 | Formulation | 262 |
| 8.4.2 | Low-cost obfuscation method for DSP core | 262 |
| 8.5 | Security of functionally obfuscated DSP core design | 266 |
| 8.5.1 | Keyspace | 266 |
| 8.5.2 | Security analysis | 267 |
| 8.5.3 | Countermeasures against attacks | 267 |
| 8.6 | Optimization engine for functional obfuscation of DSP cores | 273 |
| 8.6.1 | Particle encoding | 273 |
| 8.6.2 | Particle fitness | 273 |
| 8.6.3 | Updating particle | 274 |
| 8.7 | Analysis of case studies | 275 |
| 8.7.1 | Security analysis | 275 |
| 8.7.2 | Overhead analysis | 277 |

| | | |
|-----------|--|------------|
| 8.7.3 | Comparative analysis | 279 |
| 8.8 | Conclusion | 282 |
| 8.9 | Exercises | 283 |
| | References | 283 |
| 9 | Obfuscation of JPEG CODEC IP core for CE devices | 287 |
| 9.1 | Introduction | 287 |
| 9.2 | Overview of JPEG compression and decompression | 289 |
| 9.2.1 | DCT-based JPEG image compression process | 290 |
| 9.2.2 | DCT-based JPEG image decompression process | 293 |
| 9.3 | Design process of structurally obfuscated JPEG IP core | 293 |
| 9.3.1 | Threat model, problem formulation, and optimization framework | 293 |
| 9.3.2 | Constructing non-obfuscated DFG for JPEG compression | 294 |
| 9.3.3 | Generating structurally obfuscated JPEG compression IP core | 296 |
| 9.3.4 | Generating structurally obfuscated JPEG decompression IP core | 298 |
| 9.4 | Implementation of JPEG CODEC IP core | 299 |
| 9.4.1 | Designing obfuscated JPEG compression IP core | 299 |
| 9.4.2 | Designing obfuscated JPEG decompression IP core | 302 |
| 9.4.3 | End-to-end JPEG CODEC through designed hardware/IP core | 302 |
| 9.5 | Analysis on case studies | 308 |
| 9.6 | Conclusion | 312 |
| 9.7 | Exercises | 312 |
| | References | 313 |
| 10 | Advanced encryption standard (AES) and its hardware watermarking for ownership protection | 317 |
| 10.1 | Introduction | 317 |
| 10.2 | AES algorithm | 318 |
| 10.2.1 | Overview of AES | 318 |
| 10.2.2 | AES algorithm—description and custom hardware design | 318 |
| 10.3 | AES digital watermarking | 326 |
| 10.3.1 | AES watermark encoding | 327 |
| 10.3.2 | Process of embedding watermark in AES | 329 |
| 10.3.3 | Signature detection | 329 |
| 10.4 | Case study of a watermarked AES hardware | 330 |
| 10.5 | Conclusion | 330 |
| 10.6 | Exercises | 334 |
| | References | 334 |

| | |
|---|------------|
| 11 Hardware approaches for media and information protection and authentication | 337 |
| 11.1 IP Protection—a broad overview | 337 |
| 11.1.1 Digital rights management | 338 |
| 11.1.2 Copyright protection of multimedia—a brief history | 339 |
| 11.1.3 Hardware versus media protection | 342 |
| 11.2 General framework for copyright protection | 343 |
| 11.2.1 The encoder | 343 |
| 11.2.2 The decoder | 344 |
| 11.2.3 The comparator | 344 |
| 11.3 Types of digital watermarks | 344 |
| 11.3.1 Spatial versus frequency domain watermarking | 345 |
| 11.3.2 Based on multimedia objects | 345 |
| 11.3.3 Based on human perception | 346 |
| 11.3.4 From applications point of view | 346 |
| 11.3.5 Based on embedding techniques | 347 |
| 11.3.6 Hardware-based watermarking systems | 347 |
| 11.4 Applications of digital watermarks | 347 |
| 11.4.1 Copyright protection | 347 |
| 11.4.2 Ownership assertion | 348 |
| 11.4.3 Authentication and integrity verification | 348 |
| 11.4.4 Fingerprinting | 348 |
| 11.4.5 Usage control | 348 |
| 11.4.6 Broadcast monitoring | 348 |
| 11.4.7 Content labeling | 349 |
| 11.4.8 Misappropriation detection | 349 |
| 11.4.9 Anti-counterfeiting | 349 |
| 11.4.10 UAV safety | 349 |
| 11.4.11 Medical signals authentication | 350 |
| 11.5 Desired characteristics of watermarks | 350 |
| 11.5.1 Perceptibility | 350 |
| 11.5.2 Robustness | 350 |
| 11.5.3 Tamper resistance | 351 |
| 11.5.4 Bit rate | 351 |
| 11.5.5 Modifiability, multiplicity, cascadability, and orthogonality | 351 |
| 11.5.6 Scalability | 351 |
| 11.5.7 Unambiguity and universality | 352 |
| 11.5.8 Pixel alteration and human intervention | 352 |
| 11.5.9 Reliability | 352 |
| 11.5.10 Blindness | 352 |
| 11.5.11 Security | 353 |
| 11.5.12 Real-time operation | 353 |
| 11.5.13 Cost and complexity | 353 |
| 11.5.14 Energy consumption | 353 |

| | | |
|-----------|--|------------|
| 11.5.15 | Integrability | 354 |
| 11.5.16 | Characteristics specific to a watermark | 354 |
| 11.6 | Technical challenges for watermarking | 355 |
| 11.6.1 | Properties of visual signals | 356 |
| 11.6.2 | Properties of the human visual system | 357 |
| 11.6.3 | How much watermark signal to add and where? | 357 |
| 11.6.4 | Spread spectrum communications | 358 |
| 11.7 | Hardware-based approaches for watermarking | 358 |
| 11.7.1 | Image watermarking hardware systems | 359 |
| 11.7.2 | Video watermarking hardware systems | 372 |
| 11.7.3 | Secure better portable graphics (SBPG) | 378 |
| 11.7.4 | Trust cam | 379 |
| 11.8 | Dynamic watermarking in smart car or UAV | 381 |
| 11.9 | Medical signals authentication | 382 |
| 11.10 | Side-channel information leakage attacks and countermeasures | 383 |
| 11.10.1 | An encryption hardware | 383 |
| 11.10.2 | Side-channel analysis attacks | 384 |
| 11.10.3 | Side-channel attack countermeasures | 387 |
| 11.11 | Attacks on watermarks and watermarking systems | 388 |
| 11.11.1 | Removal and interference attacks | 389 |
| 11.11.2 | Geometric attacks | 389 |
| 11.11.3 | Cryptographic attacks | 389 |
| 11.11.4 | Protocol attacks | 389 |
| 11.12 | Limitations of watermarks and watermarking | 390 |
| 11.13 | Conclusion | 391 |
| 11.14 | Exercises | 391 |
| | References | 392 |
| 12 | Physical unclonable functions (PUFs) | 403 |
| 12.1 | Introduction | 403 |
| 12.2 | PUF: Principle | 406 |
| 12.3 | Properties or characteristics of PUFs | 407 |
| 12.3.1 | Uniqueness | 407 |
| 12.3.2 | Reliability (correctness) | 409 |
| 12.3.3 | Randomness (uniformity) | 409 |
| 12.3.4 | Correlation (bit aliasing) | 409 |
| 12.3.5 | Power consumption | 410 |
| 12.3.6 | Speed | 410 |
| 12.4 | Classification of PUFs | 410 |
| 12.4.1 | Device-based PUFs | 411 |
| 12.4.2 | Security-based PUFs | 411 |
| 12.5 | Ring oscillator-based PUFs | 412 |
| 12.6 | Reconfigurable or dynamic PUFs | 415 |
| 12.7 | SRAM-based PUF | 419 |
| 12.8 | Memristor-based PUFs | 420 |

| | |
|---------------------------------------|------------|
| 12.9 Diode-based PUF | 424 |
| 12.10 Carbon-based PUFs | 426 |
| 12.10.1 CNT-based PUF | 427 |
| 12.10.2 Graphene-based PUF | 428 |
| 12.11 Microprocessor-based PUF | 429 |
| 12.12 Magnetic PUF | 430 |
| 12.13 Practical implementation of PUF | 432 |
| 12.14 PUF: case study applications | 433 |
| 12.15 PUF: issues | 438 |
| 12.16 Conclusion | 440 |
| 12.17 Exercises | 440 |
| References | 441 |
| Appendix A | 447 |
| Appendix B | 459 |
| Index | 493 |