

Contents

1	Introduction and Preview	1
1.1	Introduction	1
1.1.1	Trust and Security in a Modern World	1
1.1.2	Information Security and Cryptology	3
1.1.3	Physical Security and Roots of Trust	5
1.2	Preview	6
1.2.1	Introducing Physically Unclonable Functions	6
1.2.2	Book Outline	8
2	Physically Unclonable Functions: Concept and Constructions	11
2.1	Introduction	11
2.1.1	The PUF Concept	11
2.1.2	Chapter Goals	12
2.1.3	Chapter Overview	13
2.2	Preliminaries	13
2.2.1	Conventions on Describing PUFs	13
2.2.2	Details of a PUF Experiment	15
2.2.3	PUF Response Intra-distance	16
2.2.4	PUF Response Inter-distance	18
2.3	Terminology and Classification	20
2.3.1	“PUFs: Physical(ly) Unclon(e)able Functions”	20
2.3.2	Non-electronic, Electronic and Silicon PUFs	22
2.3.3	Intrinsic and Non-intrinsic PUFs	23
2.3.4	Weak and Strong PUFs	25
2.4	Intrinsic PUF Constructions	25
2.4.1	Arbiter PUF	26
2.4.2	Ring Oscillator PUF	30
2.4.3	Glitch PUF	34
2.4.4	SRAM PUF	35
2.4.5	Latch, Flip-Flop, Butterfly, Buskeeper PUFs	38
2.4.6	Bistable Ring PUF	40

2.4.7	Mixed-Signal PUF Constructions	40
2.4.8	Overview of Experimental Results	42
2.5	PUF Extensions	45
2.5.1	POKs: Physically Obfuscated Keys	45
2.5.2	CPUFs: Controlled PUFs	45
2.5.3	RPUFs: Reconfigurable PUFs	46
2.5.4	PPUFs: Public PUFs and SIMPL Systems	47
2.6	Conclusion	47
2.6.1	Overview of PUF Constructions	47
2.6.2	Insight into PUF Constructions	48
3	Physically Unclonable Functions: Properties	49
3.1	Introduction	49
3.1.1	Motivation	49
3.1.2	Chapter Goals	50
3.1.3	Chapter Overview	50
3.2	A Discussion on the Properties of PUFs	51
3.2.1	Constructibility and Evaluability	51
3.2.2	Reproducibility	52
3.2.3	Uniqueness and Identifiability	53
3.2.4	Physical Unclonability	54
3.2.5	Unpredictability	55
3.2.6	Mathematical and True Unclonability	56
3.2.7	One-Wayness	57
3.2.8	Tamper Evidence	57
3.2.9	PUF Properties Analysis and Discussion	58
3.2.10	Discussion on PUF Properties	64
3.3	Formalizing PUFs	65
3.3.1	Earlier Formalization Attempts	66
3.3.2	Setup of the Formal Framework	69
3.3.3	Definition and Expansion of a Physical Function	70
3.3.4	Robustness of a Physical Function System	73
3.3.5	Physical Unclonability of a Physical Function System	74
3.3.6	Unpredictability of a Physical Function System	76
3.3.7	Discussion	78
3.4	Conclusion	79
4	Implementation and Experimental Analysis of Intrinsic PUFs	81
4.1	Introduction	81
4.1.1	Motivation	81
4.1.2	Chapter Goals	82
4.1.3	Chapter Overview	83
4.2	Test Chip Design	83
4.2.1	Design Rationale	83
4.2.2	Design Requirements	84
4.2.3	Top-Level Architecture	85

4.2.4	PUF Block: Arbiter PUF	86
4.2.5	PUF Block: Ring Oscillator PUF	87
4.2.6	PUF Block: SRAM PUF	87
4.2.7	PUF Blocks: D Flip-Flop PUF, Latch PUF and Buskeeper PUF	88
4.2.8	Power Domains	89
4.2.9	Implementation Details	90
4.3	Experimental Uniqueness and Reproducibility Results	91
4.3.1	Evaluation of Delay-Based PUFs	91
4.3.2	PUF Experiment: Goals, Strategy and Setup	93
4.3.3	Experimental PUF Uniqueness Results	94
4.3.4	Experimental PUF Reproducibility Results	97
4.4	Assessing Entropy	105
4.4.1	Adversary Models and Basic Entropy Bounds	105
4.4.2	Entropy-Bound Estimations Based on Experimental Results	109
4.4.3	Modeling Attacks on Arbiter PUFs	110
4.5	Conclusion	114
4.5.1	Summary of PUF Behavior Results	114
5	PUF-Based Entity Identification and Authentication	117
5.1	Introduction	117
5.1.1	Motivation	117
5.1.2	Chapter Goals	118
5.1.3	Chapter Overview	119
5.2	PUF-Based Identification	119
5.2.1	Background: Assigned Versus Inherent Identities	119
5.2.2	Fuzzy Identification	120
5.2.3	Identification Performance for Different Intrinsic PUFs	125
5.3	PUF-Based Entity Authentication	129
5.3.1	Background: PUF Challenge-Response Authentication	129
5.3.2	A PUF-Based Mutual Authentication Scheme	131
5.3.3	Authentication Performance of Different Intrinsic PUFs	137
5.4	Conclusion	139
6	PUF-Based Key Generation	143
6.1	Introduction	143
6.1.1	Motivation	143
6.1.2	Chapter Goals	144
6.1.3	Chapter Overview	144
6.2	Preliminaries	145
6.2.1	Secure Sketching	145
6.2.2	Randomness Extraction	146
6.2.3	Fuzzy Extractors	149
6.3	A Soft-Decision Secure Sketch Construction	150
6.3.1	Motivation	150

6.3.2	Soft-Decision Error Correction	151
6.3.3	Soft-Decision Secure Sketch Design	153
6.3.4	Implementation Results on FPGA	155
6.4	Practical PUF-Based Key Generation	155
6.4.1	Motivation	155
6.4.2	Practical Key Generation from a Fuzzy Source	156
6.4.3	Comparison of Key Generation with Intrinsic PUFs	160
6.4.4	A Full-Fledged Practical Key Generator Implementation	161
6.5	Conclusion	167
7	Conclusion and Future Work	169
7.1	Conclusions	169
7.2	Future Work	171
	Appendix A Notation and Definitions from Probability Theory and Information Theory	173
A.1	Probability Theory	173
A.1.1	Notation and Definitions	173
A.1.2	The Binomial Distribution	175
A.2	Information Theory	175
A.2.1	Basics of Information Theory	175
A.2.2	Min-entropy	177
	Appendix B Non-intrinsic PUF(-like) Constructions	179
B.1	Optics-Based PUFs	179
B.1.1	Optical PUF	179
B.1.2	Paper-Based PUFs	181
B.1.3	Phosphor PUF	181
B.2	RF-Based PUFs	182
B.2.1	RF-DNA	182
B.2.2	LC PUF	182
B.3	Electronics-Based PUFs	182
B.3.1	Coating PUF	182
B.3.2	Power Distribution Network PUF	183
B.4	More Non-intrinsic PUFs	183
B.4.1	CD-Based PUF	183
B.4.2	Acoustical PUF	183
B.4.3	Magstripe-Based PUF	184
	References	185

Physically Unclonable Functions
Constructions, Properties and Applications

Maes, R.

2013, XVII, 193 p. 28 illus., Hardcover

ISBN: 978-3-642-41394-0