

# Intellectual Property Protection in VLSI Designs

Theory and Practice

Gang Qu  
Miodrag Potkonjak

KLUWER ACADEMIC PUBLISHERS

# Contents

List of Figures	ix
List of Tables	xv
Acknowledgments	xix
<b>1. DESIGN SECURITY: FROM THE POINT OF VIEW OF AN EMBEDDED SYSTEM DESIGNER</b>	<b>1</b>
1 Introduction	1
2 Intellectual Property in Reuse-Based Design	2
2.1 The Emergence of Embedded Systems	2
2.2 Intellectual Property Reuse-Based Design	4
2.3 Intellectual Property Misuse and Infringement	8
3 Constraint-Based IP Protection: Examples	9
3.1 Solutions to SAT	10
3.2 FPGA Design of DES Benchmark	12
3.3 Graph Coloring and the CF IIR Filter Design	13
4 Constraint-Based IP Protection: Overview	16
4.1 Constraint-Based Watermarking	16
4.2 Fingerprinting	17
4.3 Copy Detection	18
5 Summary	19
<b>2. PROTECTION OF DATA AND PRIVACY</b>	<b>23</b>
1 Network Security and Privacy Protection	23
2 Watermarking and Fingerprinting for Digital Data	26
3 Software Protection	29
4 Summary	31

<b>3. CONSTRAINT-BASED WATERMARKING FOR VLSI IP PROTECTION</b>	<b>35</b>
<b>1 Challenges and the Generic Approach</b>	<b>36</b>
1.1 Overview	36
1.2 Watermark Embedding Procedure	37
1.3 Signature Verification Procedure	37
1.4 Credibility of the Approach	38
1.5 Essence of Constraint Addition	39
1.6 Context for Watermarking	40
1.7 Requirements for Effective Watermarks	41
<b>2 Mathematical Foundations for the Constraint-Based Watermarking Techniques</b>	<b>41</b>
2.1 Graph Coloring Problem and Random Graphs	42
2.2 Watermarking Technique #1: Adding Edges	43
2.3 Watermarking Technique #2: Selecting MIS	47
2.4 Watermarking Technique #3: Adding New Vertices and Edges	52
2.5 Simulation and Experimental Results	53
2.5.1 Numerical Simulation for Techniques # 1 and # 2	53
2.5.2 Experimental Results	54
<b>3 Optimization-Intensive Watermarking Techniques</b>	<b>58</b>
3.1 Motivation	58
3.2 SAT in EDA and SAT Solvers	61
3.3 Watermarking in the Optimization Fashion	63
3.4 Optimization-Intensive Watermarking Techniques for SAT Problem	64
3.4.1 Adding Clauses	65
3.4.2 Deleting Literals	66
3.4.3 Push-out and Pull-back	67
3.5 Analysis of the Optimization-Intensive Watermarking Techniques	69
3.5.1 The Correctness of the Watermarking Techniques	69
3.5.2 The Objective Function	70
3.5.3 Limitations of the Optimization-Intensive Watermarking Techniques on Random SAT	72
3.5.4 Copy Detection	75
3.6 Experimental Results	76
<b>4 Summary</b>	<b>78</b>

<b>4. FINGERPRINTING FOR IP USER'S RIGHT PROTECTION</b>	<b>81</b>
1 Motivation and Challenges	81
2 Fingerprinting Objectives	83
2.1 A Symmetric Interactive IP Fingerprinting Technique	83
2.2 General Fingerprinting Assumptions	84
2.3 Context for Fingerprinting in IP Protection	85
2.4 Fingerprinting Objectives	85
3 Iterative Fingerprinting Techniques	87
3.1 Iterative Optimization Techniques	87
3.2 Generic Approach	88
3.3 VLSI Design Applications	90
3.3.1 Partitioning	91
3.3.2 Standard-Cell Placement	91
3.3.3 Graph Coloring	92
3.3.4 Satisfiability	94
3.4 Experimental Results	95
4 Constraint-Based Fingerprinting Techniques	101
4.1 Motivation, New Approach, and Contributions	102
4.2 Generic Constraint-Addition IP Fingerprinting	103
4.3 Solution Creation Techniques	105
4.3.1 Solution post-processing	108
4.4 Solution Distribution Schemes	110
4.5 Experimental Results	111
5 Summary	114
<b>5. COPY DETECTION MECHANISMS FOR IP AUTHENTICATION</b>	<b>117</b>
1 Introduction	117
2 Pattern Matching Based Techniques	119
2.1 Copy Detection in High-Level Synthesis	120
2.2 Copy Detection in Gate-Level Netlist Place-and-Rout	122
2.3 Experimental Results	123
3 Forensic Engineering Techniques	125
3.1 Introduction	125
3.2 Forensic Engineering for the Detection of VLSI CAD Tools	126
3.2.1 Generic Approach	126
3.2.2 Statistics Collection for Graph Coloring Problem	128
3.2.3 Statistics Collection for Boolean Satisfiability Problem	131
3.2.4 Algorithm Clustering and Decision Making	132

3.3	Experimental Results	134
4	Public Detectable Watermarking Techniques	137
4.1	Introduction	137
4.2	Public-Private Watermarking Technique	140
4.2.1	Watermark Selection and Embedding	141
4.2.2	Watermark Detection and Security	142
4.2.3	Example: Graph Partitioning	143
4.3	Theory of Public Watermarking	144
4.3.1	General Approach	144
4.3.2	Public Watermark Holder	145
4.3.3	Public Watermark Embedding	149
4.3.4	Public Watermark Authentication	150
4.3.5	Summary	151
4.4	Validation and Experimental Results	152
4.4.1	FPGA Layout	152
4.4.2	Boolean Satisfiability	153
4.4.3	Graph Coloring	155
5	Summary	157
6.	CONCLUSIONS	159
	Appendices	163
	VSI Alliance White Paper (IPPWP1 1.1)	163
	References	173