

Index

A

- Active learning, 43–46, 48, 74
- Analytical camouflaging security analysis, 72, 117, 124
- AND-tree
 - camouflaging strategy, 69–72
 - decomposability characterization, 57–58
 - general circuits, 54–55
 - input bias, 55–57
 - original netlist detection, 59–62
 - removal attack, 64–66
 - security analysis, 52–54
 - stochastic greedy insertion, 62–64

B

- Back-end-of-line (BEOL)
 - FEOL, 3
 - globalized supply chain, 2
 - interconnections, 9
 - iterative strategy, 23
 - nodes, 35
 - security, 29

C

- Challenge-response pairs (CRPs), 4, 99, 100, 109, 111, 112

E

- Execution and simulation (ESG)
 - amplification, 109
 - computation algorithms, 100

- lower bound, 106–108
- PPUFs, 4, 98, 103–106, 136
- simulation model, 5, 112–114
- upper bound, 108–109
- verifier's task, 109

F

- Fault attack
 - cross-level framework, 117
 - cryptographic modules, 97
 - flow, 119
 - gate-level, 127–128
 - IP integrity issues, 4
 - PPUF design, 5
 - RTL-level, 127
 - SSF, 121
 - system vulnerability, 4, 116
 - valuation framework, 135
- Finite state machine (FSM), 116, 117, 120, 122
- Full chip camouflaging, 136

H

- Hardware Trojan
 - BEOL, 2
 - fabrication time, 9
 - FEOL, 2
 - globalized supply chain, 1, 2
 - insertion, 17
 - Moore's law, 1
 - PUF and PPUF, 4
 - split manufacturing, 3

I

- IC camouflaging technique
 - active learning, 44–45
 - AND-tree (*see* AND-tree)
 - arms race evolution, 40–42
 - cell design
 - discussion, 50–52
 - generation strategy, 68–69
 - STF-type, 49–50
 - XOR-type, 48–49
 - contributions, 43–44
 - effectiveness, 74
 - fabrication-level techniques, 3, 39
 - SAT-based attack strategies, 5, 40
 - security
 - analysis, 45–48
 - level, 43
 - state-of-the-art techniques, 66–67
 - structural and functional impact, 72–74
- Importance sampling
 - analytical analysis, 129
 - attack parameters, 121
 - effectiveness, 129
 - gate-level, 127–128
 - RTL-level
 - fault attack simulation, 127
 - golden simulation, 126–127
 - strategy, 117
 - system pre-characterization, 122–126, 131
- Intellectual property (IP) design
 - globalization, 135
 - integrity
 - issues, 4
 - and privacy, 1–4
 - privacy, 39
 - protection, 135
 - violations, 1, 3
- IP privacy and integrity violations
 - hardware, 1–4
 - reverse engineering, 39
 - semiconductor supply chain, 135

K

- k-isomorphism, 18–20

L

- Lagrangian relaxation algorithm
 - minimum-cost flow transformation, 26–28
 - multiplier update, 28–29

M

- Mixed-integer linear programming (MILP)
 - formulation
 - coefficients, 36
 - dummy wires and gates, 21
 - FEOL layer generation, 10, 21–25
 - LR-based algorithms, 32
 - minimum-cost flow transformation, 28, 31
- Monte Carlo evaluation framework
 - experimental results, 128–131
 - FSM, 116
 - motivation, 117–118
 - problem formulation
 - attack model, 119
 - holistic fault injection modeling, 120
 - system security factor, 120–121
 - SSF, 117

P

- PPUF design
 - basic building block, 103–106
 - crossbar
 - placement, 111
 - structure, 110–111
 - ESG, 98, 99, 109
 - execution and simulation, 98
 - experimental results
 - ESG, 112–114
 - simulation model, 112–114
 - input challenge pre-pruning, 111–112
 - lower bound, 106–108
 - Max-flow problem, 100–102
 - model-building attack resilience, 115
 - MOS transistors, 98
 - protocol, 99–100
 - signal delay, 102–103
 - statistical evaluation, 114–115
 - topology, 103–106
 - upper bound, 108–109
 - verification, 114
 - verifier's task, 109
- Provably secure
 - IC camouflaging (*see* IC camouflaging technique)
 - SAT-based reverse engineering attack, 5

R

- Register-transfer level (RTL), 123, 126–127, 129, 130

- Reverse engineering
 - arms race, 3, 41
 - black-box functional circuit, 80
 - camouflaging
 - cells, 39
 - connections, 40
 - de-camouflaging iterations, 91
 - FEOL and BEOL, 9
 - IP design (*see* Intellectual property (IP) design)
 - wave-pipelining, 77

- S**
- SAT-based attack
 - active learning, 48
 - camouflaging cells, 76
 - clique-based obfuscation, 42
 - de-camouflaging complexity, 54
 - security guarantee, 40
 - timingSAT algorithm, 135
- Simultaneous cell and wire insertion, 10, 12, 21
- Split manufacturing
 - attack model of untrusted foundries, 11
 - dummy cells, 10
 - experimental setup, 31
 - fabrication technology, 135
 - FEOL
 - generation strategy comparison, 31–34
 - layers, 9
 - friendly physical design, 135
 - k-security realization, 18–20
 - motivation, 11–12
 - overhead and framework parameters, 36
 - physical proximity examination, 34–36
 - refinement technique, 10
 - security analysis, 13–18
 - state-of-the-art, 12–13
- Statistical attack space, 5, 112, 114, 115
- System security factor (SSF)
 - accuracy and attack parameter, 131
 - comparison, 130
 - illegal transition, 121
 - pre-characterization procedure, 117
 - radiation-based attacks, 129
 - system vulnerability, 117

- T**
- Timing-based camouflaging, 76–77
 - high-entropy, 93
 - motivating example, 78–79
 - traditional strategy, 93–94
- TimingSAT
 - algorithm, 135
 - attack efficiency, 42
 - discussion, 87
 - efficiency, 88
 - input query, 81–84
 - key post-processing, 86–87
 - netlist simplification, 84–86
 - performance, 89
 - runtime dependency, 88–90
 - scalability issue, 75
 - TU insertion, 80–81
 - unrolling time frames, 90–92
- Trojan prevention
 - hardware, 10
 - insertion, 9
 - k-secure layout refinement, 29–30
 - Lagrangian algorithm (*see* Lagrangian relaxation algorithm)
 - MILP-based FEOL generation, 21–25
 - security and efficiency, 135