

# Index

## A

Access control, 6, 13, 157, 365, 423  
    restrictions, 364  
Activation mechanism, 120, 123  
Active-layer programming ROM, 266, 271  
Adversary, 6, 16, 110, 118, 172, 174, 183, 194, 198,  
    227, 248, 257, 276, 292, 313, 317, 325,  
    349, 368, 376, 390, 398, 410, 422, 432  
    potential, 112, 137, 351, 375, 422, 432  
Aging, 155, 160, 313–319, 329–333  
Altera, 35, 457  
Analog-to-digital converter (ADC), 142, 301, 459  
Analysis  
    code coverage, 62, 127  
    structural, 71, 128  
Anti-RE techniques, 248, 257, 265, 271–273  
Antifuse memory, 272  
AOI machines, 97  
Application-specific integrated circuit (ASIC), 5, 34,  
    116, 188, 249, 265, 319  
Arbiter PUF, 318  
ARM TrustZone, 366  
Assembly code, 477, 479–483  
Assembly process, 88, 145, 153  
Assets, 276, 313, 349–354, 359, 365, 422, 429–431  
At-speed delay test, 74  
Attack instances, 174, 176, 299, 302  
Attack models, 122, 174, 179, 186, 299, 331, 349, 357,  
    443  
Attack scenario, 174, 299, 364, 420, 430  
Attack surface enumeration, 363  
Attack surfaces, 11, 16, 297, 364  
Attack vectors, 10, 15  
Attackers, 10, 13, 114, 119, 129, 132, 146, 148, 172,  
    174, 176, 178, 183, 187, 195, 200, 204,  
    217, 220, 227, 236, 246, 271, 305, 331,  
    348, 361, 368, 375, 379, 386, 390, 393,  
    430, 435  
Attacks, 2–16, 102, 116, 158, 172–190, 194–217, 221,  
    241, 246, 273–307, 325, 331, 348–357,  
    363, 367, 379–394, 413, 432–445  
    active, 195, 207

    direct memory, 363  
    frequency injection, 335, 340  
    hardware-based, 335, 348  
    invasive, 185, 216, 246, 269, 274, 351, 352  
    key-guessing, 382  
    Meltdown, 15, 442  
    microprobing, 6, 246, 357  
    noninvasive, 186, 194, 210, 216, 223, 246, 248, 269,  
        274, 351  
    passive, 195  
    remote, 350  
    scan-based controllability, 221, 229  
    scan-based observability, 221  
    semiinvasive, 186, 211, 276, 351  
    snooping, 305  
    Spectre, 15, 439, 442  
    successful, 12, 185, 197, 199, 363  
Attacks on FPGA bitstream, 183  
Authentication, 185, 240, 317, 324, 399, 404, 407  
Authentication keys, 185, 236  
Automatic test pattern generation (ATPG), 57, 64, 68,  
    76, 119, 236, 359, 383

## B

Back end of line (BEOL), 134, 277, 314, 379  
Backdoors, 110, 115, 147, 348, 351  
Ball grid array (BGA), 94, 264  
Base address register (BAR), 424  
Bitstream, 180–189, 249, 265, 269, 273, 389–395  
    antireversal, 273  
    reversal, 270  
Board layout, 91  
Bounded model checking (BMC), 128  
Branch Target Buffer (BTB), 440  
Brute-force attacks, 382, 390  
Built-in self-authentication (BISA), 133, 137  
Built-in self-test (BIST), 49, 68, 73, 112, 144  
    logic (LBIST), 73, 74  
    memory (MBIST), 73, 74, 79

## C

CAD tools, 112, 144, 348, 354, 357, 376

Camouflaging, 132, 178, 257, 379, 386  
 Capacitance, 32, 99, 122, 272, 401, 410  
 Capacitors, 32, 86, 94, 156, 198, 249, 256, 272, 294, 302  
 Cells  
   camouflaged, 379, 384  
   configurable CMOS, 384  
 Central processing unit (CPU), 41, 42, 142, 420, 424, 438, 456  
 Challenge-response pair (CRP), 159, 317, 331, 339, 407  
 Chip-scale packaging (CSPs), 94  
 Chips  
   faulty, 51, 77, 145  
   unlocked, 159, 383  
 Circuit boards, 40, 82, 252, 405  
 Circuit input-output combinations, 52  
 Circuit probe (CP), 64  
 Circuits, 31, 51–59, 66–73, 86, 90, 94, 99, 111, 113, 122–387, 433, 463  
   reconfigurable, 132  
    $t$ -private, 281, 282  
 Clock cycle, 55, 202, 233, 279, 368  
 Clock grid, 122  
 Clock signals, 29, 71, 120, 122, 210  
 Clock sweeping technique, 161  
 Complex programmable logic device (CPLD), 72, 303, 380  
 Computer numerical control (CNC), 252  
 Computer-aided design (CAD), 7, 49, 111, 144, 276  
 Computing systems, 2–4, 11, 305, 456  
 Concurrent error detection (CED), 133  
 Confidentiality, 6, 121, 157, 223, 275, 356, 366, 423, 430  
 Configurable logic block (CLB), 180, 270  
 Configuration bits, 14, 180, 183, 187  
 Control unit, 227  
 Control vector, 227  
 Controllability, 8, 54, 67, 129, 149, 220, 349, 386  
 Correlation power analysis (CPA), 202  
 Counterfeiting, 6, 150, 163, 276, 297, 312, 398  
 Countermeasures, 10, 13, 125, 179, 203, 207, 210, 212, 223, 235, 275, 312, 335, 349, 367, 384, 431, 444  
   potential, 274  
 Critical information, 6, 12, 128, 183, 197–207, 210, 217, 223, 298, 305, 442  
 Critical traces, 303, 412

Crypto IP, 223, 422, 430  
 Cryptoengine, 115, 240, 423  
 Cryptographic applications, 322  
 Cryptographic devices, 194, 202, 282  
 Cryptographic keys, 14, 172, 269, 273, 283, 316, 328, 365, 423, 441  
 Cryptographic random number, 277  
 Cryptographic systems, 207, 211, 328  
 Cryptomodule, 115, 120, 215, 350, 445

## D

D flip-flop (DFF), 29, 55, 68, 131  
 D-type flip-flop, 68  
 Dangerous Don't-Care States (DDCS), 359  
 Decapsulation, 163, 179, 253, 278  
 Defect level (DL), 49, 51, 77, 92  
 Defect-free chips, 145, 152, 159  
 Defects, 53, 57, 73, 96, 145, 163, 221, 264, 314  
 Delaying, 154, 178, 205, 249, 253, 261, 272  
 Denial of service (DoS), 7, 110, 121, 276, 348, 351, 362, 445  
 Design for anti-counterfeit (DfACs), 313, 329  
 Design houses, 7, 59, 88, 112, 132, 143, 153, 181, 258, 293, 299, 301, 307, 348, 351, 377, 379, 393  
 Design mistakes, 146, 148, 348  
 Design rule check (DRC), 53, 63, 88, 256, 356  
 Design security rule, 353, 428  
 Design security rule check (DSeRC), 353, 362  
 Design specifications, 58, 90, 98, 111, 143, 354, 484  
 Design-for-debug (DfD), 8, 64, 150, 354, 427, 446  
 Design-for-security (DfS), 14  
 Design-for-test (DFT), 8, 49, 61, 67, 112, 134, 144, 149, 157, 220, 227, 348, 354, 362, 401  
 Design-for-trust, 130  
 Destructive reverse engineering, 111, 125, 379  
 Deterministic security requirements, 364  
 Device configuration, 277, 349  
 Device under attack, 197–204, 207, 211, 351  
 Differential electromagnetic analysis (DEMA), 207  
 Differential power analysis (DPA), 185, 200, 215, 221  
 Digital circuits, 27, 57, 67, 252, 257  
 Digital logic, 27, 67, 256  
 Digital signal processing (DSP), 180, 265  
 Direct memory access (DMA), 225, 363, 432  
 DOS architecture, 226  
 Downgrade performance, 120  
 DPA attacks, 200  
 Dummy flip-flops, 228, 236

**E**

Electrical tests, 163  
 Electrically erasable programmable read-only memory (EEPROM), 249, 265, 283, 316, 413, 452, 465  
 Electro-optical frequency modulation (EOFM), 277  
 Electronic design automation (EDA), 57, 157  
 Electronic hardware, 4, 102, 328  
 EM emanation, 205  
 EM signals, 211  
 Embedded system hardware, 41  
 Embedded systems, 40, 265, 305, 320  
 Emerging nanodevices, 336  
 Encrypted bitstream, 182, 185, 269, 389  
 Encryption key, 14, 185, 215, 220, 376, 389, 432, 442  
 Engineering change order (ECO), 133  
 Entropy, 313, 324, 327, 337, 349, 382, 388  
 Equalization techniques, 367  
 Error-correction code (ECC), 208, 322, 333, 407, 437  
 Execution, 14, 179, 194, 203, 207, 365, 368, 380, 423, 440

**F**

Fault attacks, 209, 359  
 Fault coverage, 49, 57, 71, 111  
 Fault injection attacks, 149, 196, 207, 210, 215, 283, 348, 357  
 Fault models, 53, 57, 74  
 Fault-injection, 354  
 Faulty ciphertext, 208  
 Field-effect transistors (FETs), 24, 91  
 Filler cells, 127, 133  
 Finite state machine (FSM), 73, 114, 132, 147, 148, 232, 233, 237, 356, 369, 378, 471  
 Firm IP, 59, 111, 143, 152, 173, 378  
 Firmware, 4, 43, 115, 181, 249, 265, 275, 410, 422, 445  
 Flash memory, 41, 265, 273, 316  
 Flip-flops, 29, 53, 69, 120, 161, 220, 227, 236, 282, 430, 433  
 Floating gate (FG), 266  
 Floating gate transistor (FGT), 266  
 Focused ion beam circuit edit (FIBCE), 334  
 Focused ion beam (FIB), 251, 275, 283  
 FPGA devices, 117, 181, 389, 454  
 FPGA (field programmable gate arrays), 5, 34–189, 215, 240, 249, 265–270, 273, 303, 320, 329, 335, 380, 389, 452–471

FPGA vendors, 116, 180–183, 270, 274  
 Front end of line (FEOL), 134, 314, 379  
 Functional test (FCT), 51, 64, 73, 88, 96, 98, 100, 111, 114, 125, 129, 144, 153, 299, 364  
 Fuse controller, 425

**G**

Gate-level, 124, 256, 354, 374, 378  
 Gate-level netlist, 59, 111, 129, 144, 157, 174, 177, 189, 257, 351, 376, 381  
 Gates, 26, 53, 75, 122, 127, 132, 144, 161, 257  
   AND, 226  
   NAND, 257, 385  
   NOR, 257, 385  
   OR, 230  
   XOR, 28, 55, 119, 161, 226, 230, 258, 381, 391  
 Global positioning system (GPS), 42

**H**

Hackers, 220, 224, 228, 233, 269, 293, 348  
 HaHa board, 16, 450–484  
 HaHa platform, 102, 188, 215, 240, 305, 392, 413  
 Hamming distance (HD), 189, 202, 317, 382, 408  
 Hard IPs, 59, 111, 144, 173, 379  
 Hardware, 1, 15, 27, 40, 62, 116, 149, 182, 189, 249, 258, 312, 324, 348, 362, 366, 375, 380, 390, 410, 420, 423, 438  
 Hardware attacks, 10–16, 305, 452  
 Hardware description language (HDL), 34, 61, 143  
   SystemVerilog, 173  
   Verilog, 34, 62, 122, 143, 149, 264, 354, 361, 377, 445, 468  
   VHDL, 34, 143, 377  
 Hardware design, 6, 15, 62, 82, 113, 173, 179, 257, 348, 352, 365, 375  
 Hardware IPs, 128, 172, 188, 374, 381, 393  
 Hardware obfuscation, 374, 381, 386, 391, 392  
 Hardware security, 2, 6, 10, 15, 221  
 Hardware security primitives, 16, 248, 313, 338  
 Hardware Trojan attacks, 6, 131, 174, 292–294, 302, 449  
 Hardware Trojan detection, 111, 125, 131  
 Hardware Trojan insertion, 112, 136, 146, 351  
 Hardware Trojan prevention, 125  
 Hardware Trojan structure, 113  
 Hardware Trojans (HT), 10, 15, 94, 110, 146, 174, 187, 246, 312, 348, 351, 398, 445  
 Hardware Trojans taxonomy, 117  
 Hardware trust, 7, 118, 134

Hardware-firmware-software interaction, 42  
 Hardware/software codesign, 42  
 Hardware/software systems, 362  
 Higher-order side-channel attacks, 203  
 Hot carrier injection (HCI), 160, 315, 333

**I**

IC overbuilding, 174  
 IC testing phase, 118  
 Imaging, 253, 256, 261, 268  
 Implant programming ROM, 266  
 In-circuit test (ICT), 98, 184, 299  
 In-field alteration, 297  
 Inductors, 32, 82, 87, 94, 256  
 Information flow, 13, 42, 258, 359, 423  
 Information flow tracking (IFT), 359  
 Input ports, 130, 360, 470, 481  
 Insertion phase, 117, 123  
 Inspection, 95, 253  
 Instruction register (IR), 237, 297  
 Instruction set architecture (ISA), 380  
 Integrated circuits (ICs), 1, 15, 26  
 Integration, 4, 15, 25, 61, 89, 92, 96, 131, 134, 146, 182, 224, 293, 364  
 Integrator, 58, 111, 172, 178, 224  
 Intel, 24, 180, 303, 440, 442  
 Intel Software Guard Extension (SGX), 366  
 Intellectual properties (IPs), 2, 10, 58, 77, 111, 128, 143, 151, 172, 248, 276, 364, 374, 380, 389, 420–433, 445  
   third party (3PIP), 112, 128, 134, 142, 224  
 Interconnections, 119, 134, 248, 253, 256, 265, 284  
 Invasive fault injection attack, 282  
 IP blocks, 10, 14, 111, 116, 171, 420, 445  
 IP overuse, 151, 159, 185  
 IP owner, 146, 151, 224, 246, 259, 276, 324  
 IP piracy, 6, 15, 151, 158, 174, 176, 380, 390  
 IP-based SoC design, 174

**J**

Joint Test Action Group (JTAG), 12, 72, 100, 117, 121, 184, 223, 238, 260, 264, 292, 297, 457  
   attacks, 240, 297  
   hacks, 238

**K**

Key, 121, 149, 158, 185, 194, 209, 223, 236, 257, 269, 276, 294, 316, 322, 328, 335, 361, 374, 380, 387, 424, 445

Key gates, 158, 381, 384, 389  
 Key sensitizing attacks (KSA), 383, 388  
 Kill switches, 6, 111  
 Kirchhoff's current law (KCL), 33, 44, 230

**L**

Launch-off-capture (LOC), 75  
 Launch-off-shift (LOS), 47, 75  
 Leak information, 121, 125, 196, 204, 306, 367, 439  
 Linear feedback shift register (LFSR), 226–236, 327  
 Lock & Key technique, 231  
 Logic, 27, 54, 67, 72, 121, 127, 172, 227, 299, 320, 375, 390, 420  
   combinational, 29, 132, 230, 236, 266, 378, 381, 386, 388, 433  
   sequential, 29, 223  
 Logic blocks, 35, 257, 266  
 Logic encryption, 389  
 Logic gates, 7, 27, 53, 111, 119, 143, 282, 378, 384  
 Logic locking, 381  
 Logic obfuscation, 132, 158  
 Logic states, 266–273, 337  
 Look-up tables (LUTs), 116, 180, 187, 258, 270, 390

**M**

Malicious system software, 366  
 Manufacturing test, 39, 59, 66, 78, 92, 120, 125, 220, 240  
 Markings, 154, 260  
 Memory, 2, 9, 27, 41, 72, 121, 212, 249, 265, 272, 275, 283, 305, 316, 364, 375, 429, 434, 441  
   kernel, 442  
   main, 380, 436, 441  
 Memory locations, 121, 208, 435, 443  
 Metal-layer programming ROM, 266  
 Microcontroller, 41, 123, 186, 260, 302, 320, 380, 410, 452–482  
 MicroSemi, 172, 180  
 Mobile devices, 36, 305  
 Modchip attack, 303, 307, 413  
 Modchips, 303, 413  
 Modeling attacks, 317, 331  
 Modes  
   normal, 233, 257, 374, 378, 386, 391  
   obfuscated, 257, 378, 387, 391  
 MRAM (magnetic random access memory), 336  
 Multiple input signature register (MISR), 73

**N**

Nanotechnology, 25  
 National Institute of Standards and Technology (NIST), 150  
   test, 318  
 Netlist, 48, 59, 88, 111, 143, 174, 179, 180, 249, 256, 264, 278, 359, 376, 390  
   obfuscated, 382, 388  
 Netlist information, 265  
 Noninvasive attacks, 186, 194, 246, 269, 274, 351

**O**

Obfuscated design, 178, 270, 381, 387, 391  
 Obfuscation, 14, 178, 223, 228, 257, 264, 374, 379, 387  
   state space, 386, 391  
 Obfuscation key, 224  
 Obfuscation methods, 382, 388  
 Obfuscation techniques, 257, 377, 384  
 Observability, 8, 14, 54, 65, 131, 149, 220, 422  
 Operating systems (OS), 4, 41, 115, 380, 425, 437, 441  
 Out-of-order execution, 440, 442  
 Output  
   hashed, 323  
   payload, 113  
 Output pins, 70, 477  
 Output ports, 360, 438, 481  
 Output responses, 52, 129, 382  
 Overproduction, 153, 158, 176, 190, 259, 324

**P**

Package test, 145, 153  
 Paths, 10, 53, 74, 83, 160, 187, 279, 318, 331, 360, 386, 401, 406, 411, 424, 433  
 Payload, 113, 114, 120, 183, 187, 391, 437  
 PCB authentication, 399, 414  
 PCB design, 9, 39, 87, 94, 292, 380  
 PCB integrity validation, 411  
 PCB layers, 402  
 PCB life cycle, 87, 95  
 PCB security challenges, 293  
 PCB signature, 399  
 PCB surface, 402  
 PCB tampering attacks, 413  
 PCB-level, 249, 264  
 Peripheral exploitation, 297  
 Phase change memory (PCM), 336  
 Phase-locked loops (PLL), 433, 457, 465

Physical access, 72, 100, 182, 185, 197, 390, 422, 443  
 Physical attacks, 246, 264, 275, 278, 282, 316, 350, 357, 412  
 Physical layout design, 112, 144, 354  
 Physical unclonable functions (PUFs), 16, 160, 258, 312, 316–324, 331–342, 378, 391, 400  
   strong, 317–319, 322, 323, 329, 331, 340  
 Piracy, 10, 152, 173, 188, 189, 257, 297, 303, 374, 380, 389, 392  
 Potential vulnerabilities, 11, 349, 352  
 Power analysis, 199, 211  
 Power analysis attacks, 197, 348  
 Power consumption, 66, 94, 100, 127, 179, 194, 198, 259, 273, 313, 324, 356, 368, 432, 467  
 Power side-channel attack countermeasures, 202  
 Power side-channel attacks, 215, 357, 451  
 Power signals, 198, 211, 367  
 Power supply noise, 48, 74, 314, 324, 327, 332  
 Power traces, 117, 197–202, 211, 402, 439  
 Pre-silicon security, 353  
 Primary inputs (PIs), 55, 351, 385  
 Primary outputs (POs), 220, 222, 386  
 Printed circuit boards (PCBs), 16, 36–40, 49, 82–102, 119, 146, 156, 224, 237, 246, 249, 256, 260–264, 284, 307, 414, 449  
 Probing, 241, 268, 275–280, 316  
 Probing attack fundamentals, 276  
 Probing attack targets, 276  
 Probing attacks, 185, 203, 275, 284, 356  
 Process variations, 48, 160, 281, 313, 325, 337, 434, 455  
 Process-induced variability, 336  
 Processor, 2, 8, 41, 121, 172, 212, 238, 261, 380, 410, 432, 438–445  
 Product security specification (PSS), 427  
 Propagation delay, 30, 300  
 Protected state, 147, 358  
 Prototype test, 39, 92  
 Pseudo-random number generator (PRNG), 325

**R**

Random response network (RRN), 230  
 Random telegraph noise (RTN), 324  
 Randomness, 230, 260, 317, 325, 335, 362, 405  
 Real-time operating system (RTOS), 40  
 Reconfigurable logics, 116, 132  
 Register transfer level (RTL), 59, 111, 119, 143, 157, 186, 257, 269, 351, 376, 428

- Registers, 27, 65, 119, 149, 159, 179, 203, 209, 222, 229, 266, 297, 360, 422, 433, 439, 443, 479
  - Lock, 430
  - Sec, 430
  - targeted, 221
- Reliability, 7, 76, 89, 92, 95, 149, 156, 275, 313, 315, 325, 334, 348, 397
- Resistors, 31, 36, 82, 86, 94, 156, 249, 256, 302, 467
- Responses, 64, 73, 125, 205, 221, 229, 240, 316, 322, 331, 338, 379, 424
- Reverse engineering (RE), 12, 154, 173, 185, 189, 211, 246, 249, 255, 260, 267, 278, 297, 352, 385, 398
  - attacks, 102, 173, 188, 189
- Ring oscillator (RO), 131, 162, 319, 327, 340
- Ring-oscillator-based PUF (RO-PUF), 319, 333
- Rogue foundry, 113, 137, 174
- ROM (read-only memory), 121, 142, 160, 249, 265, 271, 275
- Rowhammer attack, 434
- RRAM (resistive random access memory), 336
- S**
  - Sandia controllability observability analysis program (SCOAP), 54, 57
  - Scan cells, 57, 68, 100, 223, 401
  - Scan chains, 14, 66, 69, 149, 220–236, 359, 361, 376, 378, 388, 401
  - Scan design, 68, 230
    - partial, 71
  - Scan flip-flops (SFFs), 68, 236, 362, 379
  - Scan test compression, 70
  - Scan-based attacks, 220–225, 236, 241
  - Scanning electron microscope (SEM), 154, 179, 249, 279
  - Secret key, 115, 121, 147, 187, 194–211, 235, 258, 269, 282, 316, 322, 333, 350, 380
  - Secure boot, 364, 423
  - Secure scan architecture using test key randomization (SSTKR), 236
  - Security
    - design's, 134, 157, 353
    - post-silicon, 349, 362
    - system's, 12
  - Security architecture, 14, 365, 422
  - Security assessment, 14, 349, 358
  - Security assets, 14, 349, 354, 427, 445
  - Security enhancement (SE), 366
  - Security issues, 4, 12, 16, 174, 179, 335, 354, 365, 420, 445
    - system-level, 420, 453
  - Security model, 12
  - Security policies, 6, 207, 214, 423, 427, 445
  - Security policy controller (SPC), 427
  - Security protocol, 240, 348
  - Security threats, 94, 174, 312, 426
  - Security validation, 13, 357, 427, 431
    - early, 427
    - post-silicon, 14, 429
    - pre-silicon, 428
  - Security vulnerabilities, 14, 95, 146, 148, 348, 351
  - Security wrappers, 427
  - Sense-amplified-based logic (SABL), 202
  - Sensitive information, 12, 15, 113, 147, 214, 224, 275, 279, 294, 348, 351, 357, 368, 438, 444
  - Sequential circuit, 29, 117, 378, 387
  - Sequential circuit test generator, 71
  - Shadow chain, 67, 226
  - Side-channel analysis, 6, 197, 204
  - Side-channel attack (SCA), 10, 185, 194–217, 221, 231, 248, 269, 273, 325, 350, 354, 390, 442
    - scan-based, 235
  - Signal integrity (SI), 63, 76
  - Signal-to-noise (SNR) ratio, 367, 452
  - Signatures, 241, 313, 318, 339, 412
  - Simple electromagnetic analysis (SEMA), 207
  - Simple power analysis (SPA), 199, 215
  - Soft IPs, 59, 111, 143, 173, 181, 377
  - Software, 11, 42, 62, 117, 181, 248, 279, 312, 348, 362, 375, 380, 459
    - legitimate system, 366
  - Software attacks, 6, 14, 445
  - Software-induced hardware trojan attacks, 437
  - Software-induced side-channel attack, 439
  - Specification phase, 117
  - Spectre attacks, 439, 442
  - Speculative execution, 440
  - Split manufacturing, 134, 379
  - SRAM (static random-access memory), 187, 269, 282, 320, 432, 476
  - State transition graph (STG), 358
  - Statement hardness, 128, 357
  - Structural tests, 51, 112, 145, 224
  - Structured DFT techniques overview, 67
  - Successful attacks, 204, 349

Supply chain, 9, 16, 116, 146, 153, 159, 182, 223, 241, 259, 313, 351, 374, 393  
 Supply chain attacks, 159, 259  
 Support vector machine (SVM), 125  
 Surface Mount Technology (SMT), 93  
 Switches, 87, 120, 456, 458, 470  
 System assets, 423, 431  
 System clock, 75, 162, 319  
 System controller, 240  
 System execution, 365  
 System initialization, 227  
 System integrators, 59, 112, 145, 292, 351  
 System on chip (SoC), 58, 63, 94, 119, 143, 231, 259, 305, 348, 353, 356, 374, 380, 422, 423, 432, 445  
   design, 112, 144, 151, 159, 172, 259, 351, 420, 427  
   flow, 60, 111, 117  
   rogue, 151  
   integrator, 58, 111, 128, 143, 151, 176, 223, 423  
   security, 423  
   test flow, 63  
   verification flow, 61  
 System security, 4, 172, 197, 240, 348  
 System-level mutual authentication, 410

## T

Target device, 120, 198, 205, 238  
 Target wires, 277  
 Targeted Trojans, 132  
 Test chips, 134, 240  
 Test circuits, 67, 74, 246  
 Test compression, 70  
 Test control (TC), 221, 230  
 Test cost, 49, 70  
 Test coverage, 57, 78, 113  
 Test cycles, 70, 77, 235  
 Test data input (TDI), 72, 237  
 Test data output (TDO), 73, 237  
 Test enable (TE), 68, 75, 230  
 Test key, 230–236  
 Test mode, 66, 100, 221, 230, 233, 275, 350  
 Test mode select (TMS), 73, 237  
 Test patterns, 53, 75, 228, 234  
 Test responses, 73, 224, 236, 293  
 Test security controller (TSC), 232  
 Test vector leakage assessment (TVLA), 204  
 Test/debug, 14  
 Testability, 54, 57, 71, 149, 220

Testers, 57, 73, 99, 129, 238  
 Testing techniques, 129, 362  
 Third-party vendors, 88, 112, 128, 143, 152, 390, 453  
 Threat modeling, 10, 223, 299, 365, 376, 428, 431  
 Through-hole technology (THT), 40, 93  
 Timing attacks, 211  
 Timing attacks countermeasures, 212  
 Trace impedance variations, 399, 409  
 Transistors, 5, 24, 35, 54, 119, 127, 256, 266, 271, 277, 314, 329, 354  
 Transition delay faults (TDF), 53, 74, 227  
 Transitions, 69, 92, 147, 207, 354, 367, 378, 386, 392, 471  
 Transmission electron microscope (TEM), 154, 251, 268  
 Trojan attacks, 7, 10, 133, 301, 356, 374, 391, 449  
   possible, 115, 299  
 Trojan circuits, 111, 119  
 Trojan detection, 111, 112, 118, 125, 133, 362, 391, 452  
 Trojan insertion, 14, 118, 121, 129, 354, 356, 390  
 Trojan payload, 438  
 Trojan-free circuit, 111, 113, 125  
 Trojan-insertion analysis (TIA), 359  
 Trojans, 111–148, 174, 187, 294, 302, 357, 390, 392, 427, 437  
   triggered, 120, 127  
 True random number generator (TRNG), 16, 233, 259, 312, 324, 328, 335  
 Trust, 15, 115, 131, 146, 152, 159, 312  
 Trust benchmarks, 122  
 Trust issues, 2, 7, 14, 150, 353, 393  
 Trusted execution environment (TEE), 6, 365, 446  
 Trustworthy computing, 133

## U

Unauthorized access, 6, 11, 172, 348, 349, 422, 445  
 Unique signatures, 160, 337, 399, 410  
 Untrusted design, 6, 134, 293, 301, 393  
 Untrusted foundry, 116, 134, 151, 176, 187, 301, 348, 374  
 Untrusted IPs, 422, 429  
 Unused circuit identification (UCI), 127  
 User-defined registers (UDRs), 237

## V

Value-added reseller (VAR), 182  
 VeriTrust, 130  
 Very large scale integration (VLSI), 49, 385

Vias, 36, 248, 261, 379, 402  
Vulnerabilities, 3, 12–16, 102, 146, 157, 176, 181,  
238, 247, 270, 292, 298, 313, 348,  
352–364, 380, 382, 428, 431, 444  
Vulnerability factor for fault-injection (VFFI), 356

## **W**

Wafer final test (WFT), 64  
Wafer test, 63, 145, 153  
Watermarking techniques, 159

Wave dynamic differential logic (WDDL), 202  
Weak PUFs, 317, 340  
Wearable health monitors, 3  
Wrong key, 374, 378, 381

## **X**

X-ray imaging, 163, 249, 296  
X-ray inspection, 98  
Xilinx, 35, 155, 180, 270