

# INDEX

## Numbers

3 dB point, 442  
3D printer, 462

## A

abstraction, 123, 403  
AC (alternating current), 37  
AC/DC (Australian rock band), 36  
active shield countermeasure, 21  
Advanced Encryption Standard. *See*  
    AES  
adversarial machine learning, 25  
AES (Advanced Encryption Standard),  
    12, 308–310  
    AES-256, 363–364  
    cipher block chaining (CBC),  
        363–364  
    construction, 309  
    counter with cipher block chaining  
        message authentication code  
        (CCM), 395  
    Indexed Code Block (ICB) mode,  
        410  
    key schedule, 365  
    masked implementation, 407  
    modes of operation, 308  
    power analysis of, 310, 316, 395  
    Rijndael cipher, 308  
aliasing, 440  
alternating current (AC), 37  
analog-to-digital converter (ADC), 66  
anti-tamper mesh, 76  
Apple M1, 172  
arbitrary waveform generator (AWG),  
    460  
Arduino, 160, 192  
Arm Cortex JTAG pinout, 469  
Arm JTAG pinout, 468

artificial neural network (ANN).  
    *See* neural network  
assets, 7, 10, 22  
asynchronous communication, 43  
attackers, 10  
attack resistance, 420  
attacks, 10  
attack surface, 4, 12  
attack tree, 10, 403  
AWG (arbitrary waveform generator),  
    460

## B

BadFET, 461  
balanced logic, 406  
ball grid array (BGA), 91–95, 97, 431  
    flip-chip, 93  
    heat spreader, 94  
    plastic, 93  
    reballing, 432–434  
    thermally enhanced, 93  
bare metal, 7  
baud rate, 47  
BBI (body biasing injection), 184–186  
BBQ lighter, 191  
BGA. *See* ball grid array  
binwalk, 18, 109, 111–117  
bitcoin wallet, 224  
bitrate, 98  
bits per second, 47  
Black Magic Probe, 448  
blinding, 408  
body biasing injection (BBI), 184–186  
boot attestation, 24  
boot configuration, 85  
bootloader, 5, 201, 225, 230, 362, 391,  
    395  
boot ROM code, 5, 20, 201

boundary scan, JTAG, 56, 106–108,  
447–448

brick, 8

## C

CAN (control area network), 447

capacitance, 38

carrier PCB, 92

CBC (Cipher Block Chaining). *See* AES,  
cipher block chaining

CC (Common Criteria), 31, 420–422

chain of trust, 6

challenge-response protocol, 410

chip-invasive attacks, 18

chip scale packaging (CSP), 94

ChipSHOUTER, 176, 236, 461

ChipWhisperer, 454, 459, 464

ChipWhisperer-Lite, 167, 218, 269, 366,  
454, 459

ChipWhisperer-Nano, 196, 269, 284,  
454

ChipWhisperer-Pro, 456, 459

chosen inputs, 333

circuits, 36

Cisco Trust Anchor attack, 76

CLKSCREW, 13

clock fault injection. *See* glitching, clock

clocking for communications, 43

code read protection, 195, 203

common clock, 44

Common Criteria (CC), 31, 420–422

Common Vulnerability Scoring System  
(CVSS), 31

Common Weakness Scoring System  
(CWSS), 31

comparison, unsafe, 122, 248

compiler optimization, avoiding, 418

compression, trace, 341, 355

conditional leakage averaging, 326

conferences, 423

constants, nontrivial, 411

constant time, 404

control flow integrity, 415

controller area network (CAN), 447  
CAN bus, 55

correlation power analysis (CPA),  
311–319, 348, 369

calculation, 315

hypothetical, 315

leakage model, 315, 373

on AES-256, 364

correlation traces, 315, 348

countermeasures, 10, 26, 325, 402  
avoiding compiler optimization,  
418

balanced logic, 406

branchless code, 405

bypassability, 417

constant time, 404

constant time compare, 404

control flow integrity, 415

decoy operations, 409

double-checking, 414

dual-rail logic, 406

fault canary, 416

fault counter, 416

infective computing, 409

leakage-resistant protocol, 410

masking, 407

noise addition, 406

nontrivial constants, 411

randomized array access, 409

side channel, 325

square-and-multiply-always, 409

strength, 417

timing randomization, 405, 409,  
414

unique status variables, 413

unstable clock, 406

CPA. *See* correlation power analysis

CRC (cyclic redundancy check),  
366–367, 415

critical path, 149

crystal, 82–84, 103, 154, 393

crowbar, 163–168, 195

crypto libraries, 410

crypto test, 134

CSP (chip scale packaging), 94

current, 36

CVSS (Common Vulnerability Scoring  
System), 31

CWSS (Common Weakness Scoring  
System), 31

cyclic redundancy check (CRC),  
366–367, 415

## D

- data bus, 294
- data bus drivers, 294
- data rate, 43
- datasheets, 77
- DC (direct current), 37
- deallocated memory, 390
- debug, 58–59, 448–449, 467
- decapsulation, 178
- decoupling capacitors, 100
- decoy operations, 409
- deep learning, 326, 355
- depackaging, 178
- desoldering, 429–431
- device labels, 73
- DFA (differential fault analysis), 121, 215–221
- die markings, reading, 88
- difference of means (DoM), 303–306, 377
- differential amplifier, 339
- differential cluster analysis, 326
- differential fault analysis (DFA), 121, 215–221
- differential power analysis (DPA), 293, 301, 374, 377
  - implemented in Python, 305
  - using with XOR, 374–376
- differential probe, 268, 339
- differential signaling, 45
- digital logic power consumption, 295
- digital oscilloscope, 65–69
- direct current (DC), 37
- disclosure, 33–34
- distinguisher, 282
- DMM, 64, 426
- DoM (difference of means), 303–306, 377
- double-checking, 414
- double loop, glitching, 191
- DPA. *See* differential power analysis
- DRAM hammering, 13
- dual-rail logic, 406
- dump test, register or memory, 133

## E

- EAL (evaluation assurance level), 421
- ECB (Electronic Code Book), 308
- ECC (elliptic curve cryptography), 117
  - blinding, 408
  - power analysis of, 258
- ECDSA (Elliptic Curve Digital Signature Algorithm), 258
- EEPROM, 4, 51
- electromagnetic analysis (EMA), 335
- electromagnetic fault injection. *See* EMFI
- electromagnetic probe, 335, 457
  - building, 335
  - chip-scale, 459
  - package-size, 457
  - preamplifier, 458
- Electronic Code Book (ECB), 308
- elliptic curve cryptography. *See* ECC
- Elliptic Curve Digital Signature Algorithm (ECDSA), 258
- embedded clock, 44
- embedded multimedia cards (eMMCs), 53, 110
- Ember Trace pinout, 470
- EMFI (electromagnetic fault injection), 171–178, 191–194, 223, 236, 461
  - architectures, 175
  - coils, 173, 177
  - coupled drive, 175
  - direct-drive, 175
  - effects of shielding, 172
  - high- and low-side drive, 175
  - permanent damage, 177
- EM-FI Transient Probe tool, Riscure, 461
- eMMCs (embedded multimedia cards), 53, 110
- EMVCo, 420
- enlightenment, 419
- entropy, 112
- error correcting codes, 412
- Ethernet, 63, 447
- evaluation assurance level (EAL), 421
- exploitation phase, 8, 30–31
- external interfaces, 3
- extracting firmware, 109

## F

FaceDancer, 452  
Farad (unit), 38  
fault canary, 416  
fault counter, 416  
fault detection, 416  
fault injection. *See* glitching  
fault primitive, 132  
fault response, 416  
fault sensitivity analysis, 154  
fault sensor, 416  
fault simulation, 418  
Federal Communications Commission Identifier (FCC ID), 72  
FIB (focused ion beam), 21  
filtering, trace, 352  
FIPS 140-3, 421  
firmware, 109, 395  
    analysis, 111  
    entropy, 112  
    extraction, 111  
    signature, 116  
    update, 395  
firmware re-hosting, 17  
first-order attacks, 407  
FiSim, 419  
flash, 110, 452, 467  
flash memory, 4  
Flashrom, 453  
flip-chip, 93  
flux, 429  
focused ion beam (FIB), 21  
frequency filtering, 353  
FTDI, 445, 448, 452  
fuses, 5, 117  
fuzzing, 17

## G

G-code, 462  
GDB (GNU Debugger), 448  
Glasgow Interface Explorer, 446  
Glib jocks quiz nymph to vex dwarf, 115  
Glitch Amplifier, Riscure, 461  
glitch delay, 128  
glitching, 119, 147, 189, 223, 236  
    body biasing injection (BBI), 184–186  
    causes of, 151–154

clock, 126, 135, 138, 148–157, 459  
crowbar, 163–168, 195  
electromagnetic. *See* EMFI (electromagnetic fault injection)  
laser. *See* LFI (laser fault injection)  
memory corruption, 390  
optical, 178–184, 461  
parameter search, 131, 142–145, 239, 242  
plotting results, 144  
reading beyond array end, 227  
reset, 393  
sensitive operations, 122, 190  
spark gap, 193  
tools, 126, 189  
triggering, 129–130, 186–187, 191, 200, 204  
voltage, 158–171, 195, 210, 460  
glitch length, 128  
GlobalPlatform TEE certification, 421  
global success rate (GSR), 327  
GNU Debugger (GDB), 448  
GreatFET, 446

## H

Hamming distance (HD), 318  
Hamming weight (HW), 297  
harmonics, 346, 353  
hash-based message authentication code (HMAC), 404  
hash table (HTAB), 388  
heat map, 338  
heat spreader, 94, 172  
Hello World, 219  
henry (unit), 38  
H-Field probe. *See* electromagnetic probe  
higher-order attacks, 407–408  
high impedance, 41  
hill-climbing algorithm, 144  
hot air gun, 431  
hypervisor, 388

## I

icWaves, Riscure, 456  
IDA (interactive disassembler), 124, 228  
identification phase, 8, 30, 31

IEEE 802.15.4, 394  
impedance, 37  
inductance, 38  
Industry Canada (IC) code, 74  
infective computing, 409  
initialization vector (IV), 374  
input correlation, 348  
instruction synchronization barrier  
(ISB), 130  
intellectual property (IP) blocks, 3  
interactive disassembler (IDA), 124, 228  
inter-IC interface (I2C), 50–53  
    addressing, 51  
    EEPROM, 51  
intermediate correlation, 348  
ISO 17825, 422  
ISO 19790, 421  
IV (initialization vector), 374

## J

jitter. *See* noise, temporal  
Joint Hardware Attack Subgroup  
(JHAS), 421  
Joint Interpretation Library (JIL),  
31, 420  
Joint Test Action Group (JTAG), 16,  
56–59, 79–80, 106–108, 120,  
232, 447–449  
    for reverse engineering, 106, 448  
Joules (unit), 38  
JTAGulator, 447  
jumper, 101

## K

kernel, 389  
key enumeration, 262, 300  
key zeroization attack, 410  
known-key analysis, 349

## L

Langer EMV, 458  
leakage model, 315, 318  
leakage-resistant protocol, 410  
LFI (laser fault injection), 178, 461  
    front- and backside, 180, 462  
    preparation, 178  
    wavelength, 181, 462  
linear regression, 326

LNA (low noise amplifier), 458  
logic analyzer, 69, 443  
logic levels, 39  
logic thresholds, 40  
loop termination checking, 415  
loop test, 132  
low noise amplifier (LNA), 458  
LPC microcontroller, 195  
LUNA, 451

## M

magnetic probe. *See* electromagnetic  
    probe  
Manchester encoding, 44  
marking code for small parts, 78  
masking, 407  
master key, 394  
memcmp, 404  
memory copy test, 133  
memory interfaces, 60  
memory protection, 231  
message blinding, 408  
metastability, 151  
microarchitectural attacks, 14  
microcontroller data bus, 294  
microscope, 435  
    USB, 436  
mini-grabber, 453  
misalignment, 353  
modchips, 392  
modular exponentiation, 254–256, 409  
multimedia card (MMC), 53  
multimeter  
    measuring continuity with, 65  
    measuring voltage with, 64  
multiplexor, 159, 210  
mutual information analysis, 326

## N

neural network, 355–357  
noise addition, 406  
noise, amplitude, 324  
noise, temporal, 325  
noninvasive attacks, 18, 236  
nontrivial constants, 411  
nonvolatile memory, 3  
normalization, trace 352

## O

- Ohm's law, 37, 267
- one-time-programmable (OTP) fuses, 4
- open collector, 43
- open drain, 43
- OpenOCD, 448, 468
- OpenSSH, 122
- oscilloscope, 65–68, 266–267, 273–274, 339–341, 437–442
  - AC coupling, 66, 273
  - aliasing artifacts, 440
  - bandwidth, 66, 441
  - input sensitivity, 453
  - memory depth, 439
  - PC attached, 453
  - probes, 65, 68
  - sample rate, 439, 455
  - trigger out, 443
- output correlation, 348
- over-the-air (OTA), 395

## P

- parallel bus, 59–61
- partial guessing entropy (PGE), 328–329
- partial success rate, 327
- patents, 75
- PCB. *See* printed circuit board
- PCI Express (PCIe), 63, 449
- Pearson's correlation coefficient, 312
- PGE (partial guessing entropy), 328–329
- phase-locked loop. *See* PLL
- Philips Hue, 393
- PhyWhisperer-USB, 234, 451
- PicoEVB, 449
- PicoScope, 453
- Piñata, 464
- PIN code check, 246–252, 404
- PKCS#1 v1.5 padding, 219
- plastic quad flat pack (PQFP), 89
- Platform Security Architecture (PSA), 421
- PlayStation 3 hypervisor attack, 388–391
- PLL (phase-locked loop), 154–155
  - PLL bypass, 391

- power analysis, 204, 245, 265, 297, 395
  - hardware implementation leakage model, 319
  - initiating encryption, 332
  - leakage assumption, 301
  - leakage model, 315, 318
  - measurement tools, 453
  - metrics, 326
  - signal processing for, 257
  - without prior knowledge, 331
- power consumption, 38
  - data dependent, 297
- power management IC (PMIC), 84, 105, 162, 164
- PowerPC JTAG pinout, 469
- power rails, 165
- power supply, 437
- practical lab
  - Arduino glitching, 190
  - BBQ lighter, 191
  - differential fault analysis, 215–222
  - differential power analysis, 361
  - ECDSA (Elliptic Curve Digital Signature Algorithm), 258
  - power consumption simulation, 299–300
  - Raspberry Pi glitching, 164–171
  - read protection bypass, 194–214
  - RSA fault attack, 215–222
  - SPA attack, 275–284
- printed circuit board (PCB)
  - components, 98–101
  - mapping, 101–108
  - modifying, 434
  - photographing, 436
  - power planes, 105
  - reverse engineering, 102
  - tracing, 81, 104
- printer cartridges, 362
- processor (central processing unit or CPU), 2
- program counter control, 133
- PSA (Platform Security Architecture), 421
- pulldown, 42
- pullup, 42
- push-pull, 42

## Q

quad flat no-lead (QFN), 91, 95, 95–96  
quad flat pack (QFP), 90  
quantization error, 67  
quantum attacks, 301

## R

randomized array access, 409  
read-only memory. *See* ROM  
reference designator, 103  
remote boot attestation, 24  
removal alloy, 432  
reset, target, 129  
resistance, 37  
resistor, 100  
resynchronization, 353, 371  
ringing, 45  
Riscure Glitch Amplifier, 461  
Riscure icWaves, 456  
Riscure Spider, 460  
Riscure VC Glitcher, 460  
ROM (read-only memory), 4  
    patching, 5  
root of trust, 5  
rotary tool, 434  
Rotating S-boxes Masking (RSM), 407  
Rowhammer attack, 13  
RS-232, 47  
RSA, 117, 215, 409  
    blinding, 408  
    CRT (Chinese Remainder  
    Theorem), 215, 220  
    MBED-TLS, 219, 256  
    power analysis of, 254, 256  
    windowing implementation, 256

## S

SAD (sum of absolute differences), 288,  
    353, 371, 456  
SAKURA Project, 463  
Saleae, 444  
sampling rate, 67, 341  
SASEBO Project, 463  
scalar multiplication, 259  
schematics, 77  
Schneier's law, 419  
SDIO (Secure Digital Input/Output), 53

search strategy

    big to small, 143  
    divide and conquer, 143  
    exercising patience, 144  
    intelligent search, 144  
    interval, 142  
    nesting, 142  
    random, 142  
    small to big, 143  
second-order attacks, 407  
secure boot, 391  
Secure Digital card (SD card), 53, 111  
Secure Digital Input/Output (SDIO), 53  
security labs, 421  
security nihilism, 8, 419  
security objectives, 10  
SEGGGER J-Link, 449  
self-clocking, 44  
serial communications, 46–48, 445  
    baud rate, 47  
    for triggering, 445  
serial interface, high speed, 61  
Serial Peripheral Interface (SPI),  
    48–50, 445, 452  
    flash, 110, 452, 467  
Serial Wire Debug (SWD), 16, 469  
shunt resistor, 210, 267, 273, 334  
side channel, 245–246  
    countermeasures, 325  
    power. *See* power analysis  
    timing. *See* timing attack  
signature, 116  
silkscreen, 103  
simple power analysis. *See* SPA  
small outline integrated circuit (SOIC),  
    89, 96, 452, 467  
    clip adapter, 452  
small outline no-lead (SON), 91  
small outline package (SOP), 89  
smartphone glitching, 194  
SMD. *See* surface-mount device  
SoC. *See* System-on-Chip  
power supply, 165  
soldering, 431  
soldering iron, 427–429  
    plating, 428  
solder mask, 104  
solder spheres, 433

- source synchronous clock, 44
- SPA (simple power analysis), 253
  - applying to RSA, 254–257
- spectrogram, 345
- spectrum analysis, 345
- SPI (Serial Peripheral Interface), 48–50, 445, 452
  - flash, 110, 452, 467
- Spider, Riscure, 460
- sportsball, 9
- square-and-multiply algorithm, 409
- squinting at traces, 282
- straps, 15, 16, 101
- sum of absolute differences (SAD), 288, 353, 371, 456
- surface-mount device (SMD)
  - ball grid arrays, 91
  - leaded packages, 88
  - leadless packages, 91
  - marking code, 78
  - rework, 431
- SWD (Serial Wire Debug), 16, 469
- switching-based injector, 159
- symbols, communication, 39
- synchronous communication, 44
- synchronous sampling, 67, 342, 455
- System-on-Chip (SoC), 2, 164
  - power supply, 165

## T

- TAs (trusted applications), 6
- target, laboratory, 463–465
- target, resetting, 129
- TEE (trusted execution environment), 5
- TEMPEST, 246
- template attack, 326
- test leads, 426
- test points, 101
- test vector leakage assessment (TVLA), 349–352, 422
- thin quad flat pack (TQFP), 89, 96
- thin SON (TSOP), 91
- thin SOP (TSOP), 89
- timing attack, 246–252, 257–258, 384, 404
- timing randomization, 405, 409, 414

- timing violation, 150–154
- Total Phase Beagle 480, 450
- trace, 67
  - compression, 341, 355
  - filtering, 352
  - normalization, 352
  - visualization, 344
- transistor-transistor logic (TTL), 40
- Trezor One, 224
- trigger, 68, 445, 456
- tristate, 42
- trusted applications (TAs), 6
- trusted execution environment (TEE), 5
- t-test, 349–350
- TTL (transistor-transistor logic), 40
- TTL serial, 47
- TVLA (test vector leakage assessment), 349–352, 422

## U

- unicorn, 8
- unique status variables, 413
- Universal Asynchronous Receiver/Transmitter (UART), 46
- Universal Serial Bus (USB), 62, 226–227
  - direct firmware upgrade (DFU), 109
  - Human Interface Device (HID), 62
  - from Python, 233
  - sniffer, 229, 233, 242, 450
  - triggering on, 233
- unstable clock, 406
- USB isolator, 192
- USB On-The-Go (OTG), 62

## V

- VC Glitcher, Riscure, 460
- vias, 102
- visualization, trace, 344
- volatile keyword, 418
- volatile memory, 2
- voltage, 36
- voltage glitching, 158–171, 195, 210, 460
- voltage regulators, 105
- voltmeter, 64



## **W**

wafer-level CSP (WLCSP), 94  
weaponize, 392  
wide small outline no lead (WSON), 91,  
95, 467

## **X**

Xbox 360 attack, 391–393, 405  
XY scanning, 462  
XTAL. *See* crystal

## **Z**

Zigbee Light Link, 394