INDEX

Actel, 133
Advanced encryption standard (AES), 291–315, 319, 329–331
affine transformation, 297–298
architecture comparison, 312–314
byte substitution and its inverse, 295–296
composite field arithmetic, 302–304
hardware implementation, 300–314
integrated-BOX (I-BOX), 306–310
isomorphic mapping, 303–304
key expansion, 294, 299–300, 310–311
loop-unrolled architectures, 301
mix columns and its inverse, 298–299
multiplicative inverse calculation, 296–297
processing unit, 342–343
round key step, 299–300
S-BOX, 302–304
shift rows and its inverse, 295
state array, 294
very high speed designs, 305–314
efficient merging techniques, 306–312
AES, see Advanced encryption standard
Altera, 130
ALU, see Arithmetic logical unit
Anton architecture, 72–77
interaction subsystem, 72–74
pairwise point interaction modules, 74–75
performance, 77
subsystem, 75–77
AP, see Application processor
Application processor (AP), 273
Arithmetic logical unit (ALU), 8
Base band processor (BP), 273
Basic local alignment search tool (BLAST), 170
BLAST, see Basic local alignment search tool
Bluetooth, 265
classic, 265–266
comparison with Zigbee, 265
healthcare device profile, 271
low energy (LE), 265–266
BP, see Base band processor
CGRA, see Multimedia-oriented reconfigurable array,
course-grained reconfigurable architectures
CLB, see Field-programmable gate arrays, configurable logic block
Commercial off-the-shelf (COTS), 174
COTS, see Commercial off-the-shelf
Cryptography, 291. See also Advanced encryption standard
eccentric curve, 292, 319–320
arithmetic, 325–328
microinstructions, 347
processing unit, 335–337
symmetric-key, 291
Data encryption standard (DES), 292. See also Advanced encryption standard; Cryptography
DCU, see Quantum Monte Carlo, distance computation unit
DES, see Data encryption standard
Design space exploration (DSE), 139
DIGIPS/W, see Processor, performance, Dhrystone giga-instructions per second per watt
Digital video port (DVP), 108–109
DPR, see Field-programmable gate array(s), dynamic partial reconfiguration
DSE, see Design space exploration
DVFS, see Dynamic voltage and frequency scaling
DVP, see Digital video port
Dynamic power management, 39
Dynamic voltage and frequency scaling (DVFS), 95
EC, see Cryptography, elliptic curve
ECC, see Error-correcting code
Electronic device interoperability, 259–272
Elliptic curve cryptography, see Cryptography, elliptic curve
Error-correcting code (ECC), 213, 228, 244
Extended Euclidean algorithm, 297
FAST, see Field-programmable gate array(s), emulation techniques, accelerated simulation technologies
Fault-resilient 3D-Noc, 240–242
4N-First model, 242–250
restriction checks, 244–246
router architecture, 248–250
valid path selection, 246–248
Fault-tolerant (FT), 240
Field-programmable gate array (FPGA), 127, 185
architecture, 128–129
bioinformatics, 170
compared to application-specific integrated circuit, 127
compared to integrated circuit, 127
configurable logic block, 128–129
dynamic partial reconfiguration, 130–131
challenges of use, 131
emulation techniques, 140–144
accelerated simulation technologies, 142
AISIC implementation, 146–147
fast NoC topology selection, 148
MADNESS project, 144–146
multicore processor, 144–146
reconfigurable emulators, 147–161
runtime reconfigurable, 147, 152–154
worst-case configuration, 157
worst-case configuration synthesis algorithm, 157–161
worst-case topology, 148–152
flash-based, 133
intellectual property blocks, 129
memory management units, 135
MS/MS, 176–180
database search engine, 177–178
performance, 180
processor architecture, 178–180
protein database encoding, 176
search engine, 176–180
operating system support, 135
software support, 133–135
spacetime architecture, 132
SRAM-based, 130–133
challenges of use, 131–132
synthesis and design tools, 134–135
AutoESL Auto Pilot, 134
C-to-gates, 134
HandelC, 134
HardwareC, 134
LegUp compiler, 134
OpenCL, 134–135
SpecC, 134
SystemC, 134
Verilog, 134
very high-level design language, 134
FIFO, see First in, first out
Finite field, 292–293, 321
addition, 293
arithmetic, 321–329
Galois, 292–293
multiplication, 293
First in, first out (FIFO), 86, 178
Floating point unit (FPU), 8
FPGA, see Field-programmable gate array
FPU, see Floating point unit
FT, see Fault-tolerant

Galois field, 292–293
GIPS, see Processor, performance, giga-instructions per second
GP, see 3D graphics processor, geometry processor
GPU, see Graphics processor unit(s)
Graphics processing unit(s), 66, 273. See also 3D graphics processor, graphics processor unit architecture
force computation, 69–72
NVIDIA Fermi, 66–69

Hardware-based prototyping/emulation approaches, 140
Hardware description language (HDL), 146
HDL, see Hardware description language
HDP, see Bluetooth, healthcare device profile
High-performance computing (HPC), 170
High-speed image sensors, 107
HPC, see High-performance computing

iBRIDGE, 107–108
iBRIDGE-BB
applications, 118–123
architecture, 109–110
configuring, 110
hardware implementation, 116–118
operation, 110–116
clock generator, 116
internal blocks, 112–116
memory, 114–116
sensor control, 112–114
performance, 118–123
IEEE 802.15.1, 264–265
IEEE 802.15.4, 264–265

Instruction set architecture (ISA), 7. See also Processor, architecture, reduced instruction set computing

Intermittent faults, 240
Interposer card, 279
IONTOL, see Tolerance of the precursor ions
ISA, see Instruction set architecture

k-means clustering algorithm, 283, 287

Lattice Semiconductor, 132
Mass spectrometry (MS), 169
MD, see Molecular dynamics
MIPS, see Processor, performance, million instructions per second
MMU, see Field-programmable gate array(s), memory management units
Molecular dynamics (MD), 62–63
Molecular mechanics, 63–65
MORA, see Multimedia-oriented reconfigurable array
MS, see Mass spectrometry
MS/MS, see Tandem mass spectrometry
Multicore chip, 187
RP-1, 40–43
RP-2, 43–47
Multimedia-oriented reconfigurable array (MORA), 213, 223–234
architectures, 223–227
coarse-grained reconfigurable architectures, 225
reconfigurable cell, 230–234
rollback impact on throughput, 232–234
rollback mechanism, 230–232
rollback scheme, 227

NBTI, see Negative bias temperature instability
Negative bias temperature instability (NBTI), 240
Network-on-chip (NoC), 240, 274
NoC, see Network-on-chip

OCP-IP, see Open Core Protocol International Partnership Association
Open Core Protocol International Partnership Association (OCP-IP), 280–281
Open Systems Interconnection (OSI), reference model, 259, 261–263
layers, 262–263
protocol stack, 262
Operating system task level, 276
OSI, see Open Systems Interconnection

Permanent faults, 239
Pipeline, 185, 188
computation, 185
decentralized tag-based control, 189
issues in tracking data, 188
phase coherent, 187, 191–204
dynamically configurable, 191–204
prototype implementation, 204–208
resource allocation, 200
phase tag control, 195–200
tags, 189–190, 195
PMU, see 3D graphics processor, system power management, power management unit
Pollack’s rule, 6
Presilicon system performance analysis, 273–288
cache hit rate analysis, 281
high-level software description, 276–278
audio power consumption example, 284–285
methodologies, 275–283
stochastic traffic generator, 282–283
GPU traffic characterization example, 287–288
transaction trace file, 278–282
cache analysis example, 285–286
virtual platform, 281
PRNGs, see Random number generators, pseudo
Processor architecture
CISC, 7
reduced instruction set computing, 5, 7
SH Processor, 5–7
SuperH, 5
superscalar, 8–9

performance, 1–5
Dhrystone giga-instructions per second, 1
Dhrystone giga-instructions per second per watt, 1
giga-instructions per second, 1
million instructions per second, 1
ProtoFlex, 143
QMC, see Quantum Monte Carlo
Quantum Monte Carlo (QMC), 77–82
architecture, 79–80
distance computation unit, 81
WF kernel, 78
Radiation-hardened reconfigurable array, 212, 223
RAMP, see Research accelerator for multipole processor
Random number generators (RNGs), 333, 344–345
pseudo, 333,
true, 333, 344
RC, see Reconfigurable cell
RE, see 3D graphics processor, rendering engine
Read-to-write ratio, 282
Reconfigurable cell (RC), 213. See also under Multimedia-oriented reconfigurable array
Reconfigurable computing platform, 174–176
Reconfigurable processor, 333–350
Research accelerator for multipole processor (RAMP), 141
Research In Motion (RIM), 274
Rijndael cipher, 293–300. See also Advanced encryption standard
RIM, see Research In Motion
RISC, see Processor, architecture, reduced instruction set computing
RNGs, see Random number generators
RP-X, 54–57
SEEs, see Soft errors, single event error
SEU, see Single event upset
SH-3, 34–40
SH-X
branch prediction, 13–15
FPU, 20–29
architecture, 21–24
performance, 29–33
pipeline, 26
microarchitecture, 11
performance, 17–20
power efficiency, 15–17
superpipeline, 12–13

SH-X2
frequency enhancement, 33
multicore architecture, 34
power efficiency, 34

SH-X4
address space extension, 52–54
core specification, 48
ISA, 49–52
SiliconBlue Technologies, 132
Single event upset (SEU), 131, 211–236
tolerance techniques, 213–223
decoupled ground bus, 218–223
differential cascode voltage swing logic, 215–218
latch design, 214–215
radiation-hardened, 212

Smartphone
hacking, 279
software architecture, 276
Socket transaction language (STL), 280–281

Soft errors
mitigation, 213
single event error, 211
single error upset, 211; see also Single event upset

Soft processors, 186
Statistical traffic characterization, 282
STL, see Socket transaction language
Systolic array, 186

Tabula, 132
Tandem mass spectrometry, 169, 171
protein identification, 171–174
FPGA, 173–176
3D graphics processor
game processor, 89–91
graphic module design, 88–89
implementation, 99–100
rendering engine, 92–95
unified multifunction unit, 90–91
vertex cache, 91–92
geometry transformation, 90–91
graphic processor unit, 85
pipeline, 86
rendering engine, 85
RISC, 88–89; see also Processor,
arithmetic, reduced instruction set computing
system architecture, 86–88
system power management, 95–99
multipole power-domain management, 95–99
power management unit, 98–99
3D-IC, see Three-dimensional integrated circuit
Three-dimensional integrated circuit (3D-IC), 239
3D turn model, 242–243
TMR, see Triple modular redundancy
Tolerance of the precursor ions, 179
Triple modular redundancy (TMR), 213
TRNGs, see Random number generators, true

Universal serial bus (USB), 263
USB, see Universal serial bus

VHDL, see Field-programmable gate array(s), synthesis and design tools, very high-level design language
VP, see Presilicon system performance analysis, virtual platform

Wave function (WF), 78
WCC, see Field-programmable gate array(s), emulation techniques, worst-case configuration
WCT, see FPGA emulation techniques, worst-case topology
WF, see Wave function

Xilinx, 130
X!Tandem, 171

ZigBee, 264–265
collection with Bluetooth, 265