

# Index

## A

- Adaptive filters, 202–204
- Ad hoc on-demand multipath distance vector (AOMDV), 86
- Analog-to-digital converter (ADC), 12
- Analog to residue converters (ARC), 12
- Application-specific integrated circuit (ASIC), 13, 277
- Arithmetic Labeled EXplicit (ALEX)
  - achievements, 375
  - approach, 373–375
- Arithmetic operations, RNS
  - arithmetic channels, 25–26
  - binary-to-RNS conversion, 25
  - RNS-to-binary conversion
    - CRT algorithm, 31–33
    - MRC algorithm, 32–36
- ASIC. *See* Application-specific integrated circuit (ASIC)

## B

- Babai's rounding-off algorithm
  - lattices, 348–349
  - mixed RNS-MRS approach, 353–356
  - RNS arithmetic
    - correction technique, 359–361
    - decryption process, 361
    - fast RNS modular reduction, 358–359
    - Montgomery reduction, 357
    - MRS-based extensions, 357
  - transcription, RNS
    - integer operations, 351
    - Montgomery's modular reduction, 352–353
- Base conversion (BC), 313, 320–322

- BEPPG. *See* Booth encoder and partial product generation (BEPPG)
- Binary Coded Decimal (BCD), 92–94, 102
- Binary Integer Decimal (BID), 99–101, 103
- Binary method algorithm, 327
- Binary number systems, programmable FIR filter design
  - ASIC synthesis results
    - critical path delays, 305, 307
    - EDBNS method, 302
    - gate count vs. number of taps, 306
    - POBS block, 304
    - throughput rate, 305
    - TMCM implementation, 303
  - FPGA synthesis, 307–308
- Bit error rate (BER), 85
- Bit-error-rate (BER), 271
- Bit per symbol (BPS), 85
- Booth-encoded multipliers
  - analyses and discussions
    - high-radix booth encoding vs. simple booth encoding, 141–142
    - NBBE and RBBE, 139–141
    - redundant binary coding efficiency, 142–144
  - booth algorithms, redundant binary multiplier, 116–120
  - converters for RBA interface, 133–134
  - digital multiplication, 114
  - existing RB multipliers, 122–124
  - $N \times N$ -bit RB multipliers, BEPPG, 129–131
  - one-digit BEPPG module, 126–128
  - one-digit RB adder cells, 131–133
  - performance evaluation

- Booth-encoded multipliers (*cont.*)  
 numerical simulation results, 136–138  
 RB booth multipliers configurations,  
 134–136  
 RBA and carry-free adding rule, 115–116  
 redundant binary coding interface  
 component, 120–122  
 taxonomy, booth encoders and partial  
 product generators  
 NBBE, 125–126  
 RBBE scheme, 126  
 VLSI performance factors, 114  
 Booth encoder and partial product generation  
 (BEPPG), 123, 124, 126–128
- C**
- Canonical double based number system  
 (CDBNS), 286–288  
 Canonical signed digit (CSD), 282, 285  
 Carry propagate adders (CPAs), 117  
 Carry save adder (CSA), 42, 122, 269, 302  
 Cascade Digit Generation, 150–151  
 CDBNS. *See* Canonical double based number  
 system (CDBNS)  
 Chinese remainder theorem (CRT), 6, 20,  
 31–33, 50, 185, 205, 350, 370  
 hardware-fault tolerance, 341  
 non-modular operations  
 magnitude comparison, 53  
 moduli set, constraints on, 50  
 MOMA, 50, 53  
 performance analysis, 62–63  
 residue-to-binary conversion, 52–53  
 residue representation, 68  
 RNS-to-binary conversion, 317–319  
 Closest vector problem (CVP), 347, 348  
 “Coding overhead,” 188–189  
 Common Subexpression Elimination (CSE),  
 281  
 Common Subexpression Generator (CSG), 288  
 Complex logarithmic number system (CLNS),  
 248  
 Computer networks  
 energy saving and reliability, WSN,  
 376–378  
 MANETs, unicast/multicast routing in  
 (*see* Mobile Ad Hoc Network  
 (MANETs))  
 redundant moduli, 369  
 SDN  
 core fabrics, RNS in, 376  
 unicast/multicast routing and  
 forwarding, 370–372
- Continuous valued number system (CVNS)  
 ADD<sub>b</sub> and ADD<sub>g</sub>, 164–167  
 analog-digits, 150  
 addition, 152–153  
 Cascade Digit Generation, 150–151  
 Modular Digit Generation, 152  
 multiplication algorithm  
 example, 168–168  
 low-resolution environment, 169–171  
 synapse multiplier, VLSI implementation  
 of  
 current-mode circuits, 172–173  
 CVNS registers, 176  
 layout of proposed CVNS multiplier,  
 173–174  
 post-layout simulation results, 173–176  
 sigmoid activation function, 172  
 TSMC CMOS 0.18  $\mu\text{m}$  technology, 171  
 truncated addition  
 ADD<sub>ls</sub> and ADD<sub>ms</sub>, 164–167  
 binary to CVNS conversion, 156  
 lower index digits, 155, 156  
 sliding groups, 157–160  
 truncation signal, 156  
 uniform groups, 161–164  
 two binary operands, addition of  
 binary to CVNS conversion, 153–154  
 CVNS to binary conversion, 155  
 reverse evolution, 155
- Correction algorithms  
 multiple residue digit error detection and  
 arithmetic operation errors, 84  
 base extension approach, 77  
 comparison, 84  
 CRT-based approaches, 83  
 erroneous residue digits, 81  
 flowchart, 79  
 hardware implementation, 78  
 legitimate and illegitimate moduli  
 ranges, 80  
 $m_i$ -projection concept, 79, 80  
 procedure, 83  
 received residue representation, 81  
 redundant moduli, 77  
 scenarios, 82  
 syndrome approach, 84  
 single residue digit error detection  
 arithmetic operations, 76  
 coding theory approach, 74  
 consistency checking method, 71  
 erroneous residue digit, 71  
 error-free residue representation, 72  
 flowchart, 73, 76, 77  
 $m_i$ -projection approach, 74

- $m_i$ -projection method, 73
  - mixed-radix digits, 74
  - modular subtraction, 75
  - residue-to-binary computation, 72
  - syndrome approach, 75
  - Covalent Redundant Binary Booth Encoding (CRBBE), 126, 128, 139, 140, 144
  - Cox–Rower architecture, 39–40, 42–44
  - CRT. *See* Chinese remainder theorem (CRT)
  - CVNS. *see* Continuous valued number system (CVNS)
- D**
- Decimal floating point number system
    - addition
      - adders, 99
      - BCD, 93–94
      - BID, 99–101
      - big shifters, 99
      - DPD, 99–101
      - exponent and sign, 99
      - exponent difference, 97
      - leading zeros, 96–97
      - multiplexers, 99
      - rounding directions, 96
      - significant result, steps for, 98
    - combination and trailing significant field, 94
    - commercial applications, 106–107
    - decimal coding schemes, 92–93
    - division
      - definition, 104
      - designs, 105
      - subtractive and multiplicative methods, 105
    - fused multiply add, 103–104
    - leading zeros, 95
    - multiplication
      - BCD, 102
      - BID multipliers, 103
      - DPD designs, 103
      - significands, 101–102
    - need for, 89–92
    - square root and elementary functions, 105–106
    - verification methods, 106
  - Densely Packed Decimal (DPD), 99–101, 103
  - Design space exploration (DSE)
    - characterization results, 193–195
    - maximum speed corner, 191
    - minimum area corner, 191
    - TCS MADD, 191–192
  - D flip-flops (DFFs), 257, 263
  - Digital signal processing (DSP), 12, 19
    - ASIC platforms, 210–211
    - fault-tolerant RNS, FIR filter
      - CRT block, 205
      - erroneous module, 205
      - hardware implementation, 208–209
      - implementation, 206
      - microelectronic technologies, 205
      - minority voter, 206
      - output converters, 207–208
    - FPGA platforms, 211–212
    - moduli selection
      - “coding overhead,” 188–189
      - criteria for, 187
      - MRC, 187
      - power dissipation, 188
      - RNS base, 188
    - RNS background and notation
      - fault-tolerant techniques, 186
      - input conversion, 185
      - modular multiplication, 183–184
      - output conversion, 185
      - QRNS, 183
    - RNS filters
      - adaptive filters, 202–204
      - DSE, 191–195
      - hardware architecture, 190
      - parallel/serial FIR filter, 196–198
      - polyphase (complex) filter, 198–202
      - real FIR filters, 195–196
      - TCS, 189
      - RNS perspectives, 212–213
  - Digital-to-analog converter (DAC), 12
  - Direct isomorphic transformation (DIT), 183
  - Discrete cosine transform (DCT), 233
  - Discrete fourier transform (DFT), 233
  - Discrete wavelet transform (DWT), 233
  - Distinct multicast routing protocols (DVMRP), 370
  - Double-base coefficient generator (DBCg), 296, 302
  - Double-base product selector (DBPS) block, 288
  - DSE. *See* Design space exploration (DSE)
  - DSP. *See* Digital signal processing (DSP)
- E**
- EDBNS. *See* Extended double based number system (EDBNS)
  - Elementary modular multiplication (EMM), 362
  - Elliptic Curve Cryptography (ECC), 312
    - GF ( $p$ ), 324–326

- Elliptic Curve Cryptography (ECC) (*cont.*)  
 point multiplication, 327  
 RNS application  
   conversion from base  $B'$  to base  $B$ ,  
   335–336  
   hardware architecture, RNSMMM,  
   337–338  
   modular adders and multipliers,  
   334–335  
   RNS bases use, 333  
   RNSMMM algorithm, 333
- Elliptic curve discrete logarithm problem  
 (ECDLP), 324
- Energy-delay product (EDP), 140
- European Logarithmic Processor (ELM), 248
- Exponential diophantine equation (EDE),  
 299–301
- Extended double based number system  
 (EDBNS)  
 binary and CSD representations, 293  
 integer  $c$ , 293  
 power-of- $b$  integers, 296  
 programmable FIR filter design  
   overall design flow, 301–302  
   POBG, 296–298  
   POBS, EDBNS reduction properties  
   and EDE, 299–301  
   transposed form FIR filter, 297  
 search algorithm, 295  
 $w$ -bit integers, 294, 295
- F**
- Fast fourier transform (FFT), 271–272
- Fault-tolerant RNS, FIR filter  
 CRT block, 205  
 erroneous module, 205  
 hardware implementation, 208–209  
 implementation, 206  
 microelectronic technologies, 205  
 minority voter, 206  
 output converters, 207–208
- Fault-tolerant techniques, redundant RNS  
 background and preliminaries  
   residue arithmetic, 68  
   residue-to-binary conversion, 68–69  
   RNS, 66–67  
 correction algorithms  
   multiple residue digit error detection  
   and, 77–84  
   single residue digit error detection and,  
   71–77  
 erroneous residue digits, 71  
 error detection and correction, 85–87
- legitimate and illegitimate ranges, 70  
 motivations, 65–66  
 residue representation, 69
- Field programmable gate arrays (FPGAs), 13,  
 278
- Finite impulse response (FIR) filter  
 ASIC, 277  
 binary number systems  
   ASIC synthesis results, 302–307  
   FPGA synthesis, 307–308  
 conventional number systems, 283–285  
 double-base number system  
   CDBNSs, 286–288  
   design method and examples, 288–292  
   DSP applications and public key  
   cryptography, 285  
   EDBNS (*see* Extended double based  
   number system (EDBNS))  
 implementations  
   area-delay and power-delay complexity,  
   267  
   normalized delay, 268, 270  
   Wallace-tree and carry-save (CSA)  
   structures, 269
- LNS MAC architectures  
 retimed LNS MAC unit, 267  
 single-MAC architecture, 265  
 SNR, 266  
 switching activity, 265  
 two-MAC architecture, 265  
 multiple constant multiplication block,  
 280–281  
 optimization of representation  
   logarithmic representation, 254  
   simulation-based methodology,  
   256–257  
   SNR, 255, 256  
 SDR, 277  
 TCM block, 281–283  
 transpose direct form, 279–280
- Floating point numbers  
 decimal floating point number system (*see*  
   Decimal floating point number  
   system)  
   IEEE 754-2008 standard, 89  
   single/double precision, 89
- Forward converters, 5–7, 11
- Forwarding Group Bitmap (FGB), 373
- Full-Adder (FA) model, 42
- Fused multiply add (FMA), 103–104
- G**
- Graph-dependence (GD) algorithms, 280

**H**

Hardware description language (HDL), 13  
 Homomorphic encryption scheme, 219  
 Horner scheme, 363  
 Hybrid RNS architecture, 203–204

**I**

Image processing  
 digital image and numerical representation, 218  
 edge detection and sharpening filters  
 addition and multiplication of integers, 228  
 binary number system, 221  
 convolution operation, 220  
 data processing, 224  
 frequency and power consumption, 222  
 grayscale images, 220  
 image pixels, 225  
 MATLAB, 225  
 moduli sets, dynamic range for, 222  
 peak signal to noise ratio, 226–227  
 RNS dynamic range., 223  
 simulation results, 224  
 SSIM, 227–228  
 image digitization, 218  
 operations, 219  
 smoothing filters  
 binary number system, 232  
 correct operation, MATLAB, 229  
 division operation, subtraction and multiplication, 231  
 hardware implementation, HDL, 229  
 image denoising and quality improvement, 229  
 noisy images, 231  
 replacement operation, 229  
 reverse conversion operation, 230  
 RNS architectures, 232  
 RNS modulo, 230  
 wavelets  
 construction scheme, 240  
 cryptographic information protection systems, 242  
 Daubechies wavelet Db4, 234  
 DWT, 233  
 finite-field wavelets, 236  
 Fourier transform, 233  
 image filtering scheme, 235  
 mathematic microscopes, 236  
 MATLAB, 234  
 matrix, 239  
 RGB representation, 242

signal processing systems, 243  
 three-level hierarchy wavelet decomposition, 237  
 trivial filterbank, 242

Indirect isomorphic transformation (IIT), 183  
 Instruction Set Architecture (ISA), 20  
 arithmetic and conversion operations, 22  
 32-bit instruction size, 22  
 definition, 22  
 instruction format, 22–23  
 single and multi-cycle instructions, 22–24  
 Integrated Circuit Compiler (ICC), 190  
 Inverse Discrete Fourier Transform (IDFT) unit, 199

**J**

Joint Photographic Experts Group (JPEG), 233

**K**

Karatsuba's algorithm, 364  
 "Kawamura et al.", base conversion, 321–322

**L**

Lagrange's interpolation, 350  
 Lattice-based cryptography (LBC)  
 asymptotic computational efficiency, 346  
 Babai's rounding-off algorithm, 348–349  
 complexity analysis  
 multi-precision approach, 364–365  
 RNS-based approaches, 362–364  
 CPU/GPU, RNS/MRS approach, 365–366  
 general integer lattices, 346  
 hard problems, 346–348  
 key-exchange protocol and RSA, 345  
 mixed RNS-MRS approach, Babai's rounding-off algorithm, 353–356  
 RNS arithmetic, Babai's rounding-off algorithm  
 correction technique, 359–361  
 decryption process, 361  
 fast RNS modular reduction, 358–359  
 Montgomery reduction, 357  
 MRS-based extensions, 357  
 transcription, RNS  
 adapting Babai's rounding-off algorithm, 351–353  
 notations, 350–351  
 trapdoor functions, 349–350  
 Lattice Vector Quantizer, 233  
 Least significant bit (LSB), 121, 257, 283

- Logarithmic Maximum A Posteriori (Log-MAP) algorithm, 248
  - Logarithmic number system (LNS)
    - base optimization, 252–254
    - basics of, 250–252
    - circuits design
      - LNS adder/subtractor organization, 257, 258
      - LUT subsystem, 258–261
      - sub-LUT selection strategies, 261–263
    - data representation, 247
    - design methodology, 249–250
    - and FFT, 271–272
    - FIR filters
      - implementations, 267–270
      - LNS MAC architectures, 263–267
      - optimization of representation, 254–257
    - look-up tables, 248
    - power dissipation, 249
    - schemes, 272–273
    - symbol-by-symbol Log-MAP algorithm, 248
  - Look-up tables (LUTs)
    - control signals, 301
    - input converters, 185
    - LUT subsystem
      - active sub-LUT, 260
      - complexity reduction, 261
      - design-space exploration, 261
      - LSBs, 259
      - memory subsystem, 258
      - MSBs, 259
      - stored values, 259
    - sub-LUT selection strategies, 261–263
  - Low-Density Parity Check (LDPC), 248
- M**
- Maximum likelihood decoding (MLD), 80
  - Maximum likelihood estimation (MLE), 339
  - Mentor Graphics LeonardoSpectrum, 303
  - Minimal signed digit (MSD), 284, 285
  - Mitchell's algorithm (MA), 248
  - Mixed-radix conversion (MRC), 6, 20, 31–36, 185
    - hardware-fault tolerance, 340
    - non-modular operations, 50–52, 62–63
    - residue representation, 68
    - RNS-to-binary conversion, 319–320
  - Mixed radix system (MRS), 24, 319, 351
  - Mobile Ad Hoc Network (MANETs), 370
    - ALEX
      - achievements, 375
      - approach, 373–375
    - CRT, 372
      - efficient routing protocol, 372
    - Modular Digit Generation, 152
    - Modular multiplication and-accumulation (MMAC) units, 40–41, 43–44
    - Monte Carlo simulation, 173, 175–176
    - Montgomery modular multiplication (MMM), 312, 328
    - Most significant bits (MSBs), 6, 121, 194, 257
    - Most significant digit (MSD), 120
    - Moving Picture Experts Group (MPEG), 233
    - MRC. *See* Mixed-radix conversion (MRC)
    - Multicast Channel-specific Identifier (MCID), 374
    - Multicast Routing Table (MRT), 370
    - Multi-operand modular adders (MOMA), 50, 53
    - Multiple constant multiplication (MCM), 278, 280–281
    - Multiple-Valued-Logic (MVL), 149
    - Multiply-and-accumulate (MAC), 114, 197, 202, 332
- N**
- NBBE. *See* Normal binary Booth encoding (NBBE)
  - New Chinese Remainder Theorem I (New-CRT-I), 31
  - New Chinese Remainder Theorem II (New-CRT-II), 31
  - Newton-Raphson iterations, 106
  - Newton's interpolation, 351
  - Non-modular operations in RNS
    - core functions, magnitude comparison, 50
    - CRT
      - magnitude comparison, 53
      - moduli set, constraints on, 50
      - MOMA, 50, 53
      - performance analysis, 62–63
      - residue-to-binary conversion, 52–53
    - diagonal function, 50, 57–58
      - coefficients, property of, 56
      - diagonal modulus, characterization of, 54–55
      - integers, 53–54
      - labels of diagonals, 53–54
      - monotonicity, 56–57
      - performance analysis, 62–63
    - mixed-radix conversion process, 50–52, 62–63
    - quotient function, 50–51
      - binary representations of  $X$ , 62
      - labels of diagonals, 58–59

- magnitude comparison, 62
- not relatively prime moduli, 61–62
- pairwise relatively prime moduli, 59–61
- performance analysis, 62–63
- residue-to-binary conversion, 62
- residue-to-binary conversion, 50
- Normal binary Booth encoding (NBBE), 125–126

**O**

- Output Port Bitmap (OPB), 371
- Output Port Index (OPI), 371

**P**

- Parallel-prefix computations, 3
- Parallel/serial FIR filter, 196–198
- Partially redundant biased Booth encoding (PRBBE), 126
- Partial product generator (PPG), 125
- Peak signal to noise ratio (PSNR), 226–227
- Polyphase (complex) filter
  - clock gating, 200
  - complex TCS, 199
  - EXP-3, 200, 201
  - EXP-4, single serial complex filter, 202
  - IDFT unit, 199
  - operational frequency, 201
  - power dissipation, 200
  - QRNS base, 199
  - structure, 201
- Power-of- $b$  generator (POBG), 296–298
- Power-of- $b$  selector (POBS), 299–301
- Processors, RNS
  - architecture, 20–22
  - arithmetic operations
    - arithmetic channels, 25–30
    - binary-to-RNS conversion, 25
    - RNS-to-binary conversion, 31–36
  - control units
    - global control unit, 36
    - multi-cycle operations, condensed micro-code for, 36–37
    - relative co-prime numbers, 37–38
- ISA, 20
  - arithmetic and conversion operations, 22
  - 32-bit instruction size, 22
  - definition, 22
  - instruction format, 22–23
  - single and multi-cycle instructions, 22–24

- state-of-the-art analysis
  - Cox–Rower architecture, 39–40, 42–44
  - MMAC units, uRNS, 40–41, 43–44
  - RDSP, 38–39
  - TTA approach, 40

## Public-key cryptography

- ECC
  - GF ( $p$ ), 324–326
  - point multiplication, 327
- residue arithmetic
  - binary-to-RNS conversion, 314–316
  - CRT, 311
  - cryptosystem designs, 312
  - mathematical background, 312–314
  - modular multiplication, 312
  - RNS-to-binary conversion, 316–322

## RNS application

- ECC, 333–338
- RSA, 330–332
- RNS modular multiplication, 328–330

## RSA

- digital signatures, 324
- encryption/decryption, 323
- key establishment, 323
- RSA-CRT
  - digital signature operation, 338
  - fault-infective techniques, 339
  - hardware-fault tolerance, 340, 341
  - modulus expansion, 339
  - safe-error concept, 339

**Q**

- Quadratic Residue Number System (QRNS), 183
- Quality of Service (QOS), 375

**R**

- RB full adders (RBFA), 131
- RB partial products (RBPP), 124
- Reconfigurable modulo (RM) adder, 335
- Reconfigurable modulo (RM) multiplier, 335
- Reduced Instruction Set Computer (RISC), 39
- Redundant binary adders (RBAs), 114
- Redundant binary Booth encoding (RBBE), 119, 125
- Redundant binary representation, booth-encoded multipliers
  - analyses and discussions
    - high-radix booth encoding vs. simple booth encoding, 141–142
    - NBBE and RBBE, 139–141

- Redundant binary representation, booth-encoded multipliers (*cont.*)
  - redundant binary coding efficiency, 142–144
- booth algorithms, redundant binary multiplier, 116–120
- converters for RBA interface, 133–134
- digital multiplication, 114
- existing RB multipliers, 122–124
- $N \times N$ -bit RB multipliers, BEPPG, 129–131
- one-digit BEPPG module, 126–128
- one-digit RB adder cells, 131–133
- performance evaluation
  - numerical simulation results, 136–138
  - RB booth multipliers configurations, 134–136
- RBA and carry-free adding rule, 115–116
- redundant binary coding interface
  - component, 120–122
- taxonomy, booth encoders and partial product generators
  - NBBE, 125–126
  - RBBE scheme, 126
- VLSI performance factors, 114
- Redundant Residue Number System (RRNS), 186, 205
- Reed–Solomon (RS) codes, 85
- Residue arithmetic
  - binary-to-RNS conversion, 314–316
  - CRT, 311
  - cryptosystem designs, 312
  - mathematical background, 312–314
  - modular multiplication, 312
  - RNS-to-binary conversion
    - base conversion, 320–322
    - CRT, 316–319
    - MRC, 319–320
- Residue digital signal processor (RDSP), 38–39
- Residue number system (RNS), 49–50
  - abilities, 3, 13
  - applications, 3–4
  - approach in (*see* Lattice-based cryptography (LBC))
  - components, 4
  - computer networks (*see* Computer networks)
  - CVNS (*see* Continuous Valued Number System (CVNS))
  - DSP (*see* Digital signal processing (DSP))
  - dynamic range, 4
  - image processing (*see* Image processing)
  - non-modular operations (*see* Non-modular operations in RNS)
  - processor design (*see* Processors, RNS)
  - properties, 4
  - public-key cryptography (*see* Public-key cryptography)
  - structure
    - arithmetic-friendly moduli sets, 4
    - conversion-friendly moduli sets, 4
    - extended moduli sets, 5
    - forward converters, 5–7
    - magnitude comparators, 6, 7
    - modulo adders and multipliers, 6, 7
    - overflow detection, 6, 7
    - prime moduli sets, 5
    - reverse converters, 6, 7
    - scaling, 6, 7
    - sign detection, 6, 7
    - special moduli sets, 4, 6
  - teaching methodology, 9
    - application, embedded systems design, 12
    - ASIC/FPGA implementation, 13
    - basic concepts, 10
    - courses, 8
    - forward converter, 11
    - hard RNS operations, 12
    - modular adders and multipliers, 10–11
    - phases, 8
    - reverse converters, 11–12
- Residue Number System Product Code (RNS-PC), 186
- Reverse converters, 6, 7, 11–12
- Reverse Evolution, 155
- Ripple-carry adder (RCA), 10, 11
- Rivest-Shamir-Adleman-system (RSA)
  - digital signatures, 324
  - encryption/decryption, 323
  - key establishment, 323
- RNS. *See* Residue number system (RNS)
- Round to Nearest with ties Away from zero (RNA), 96
- Round to Nearest with ties to Even (RNE), 96
- Round To Negative (RTN), 96
- Round To Positive (RTP), 96
- Round To Zero (RTZ), 96
- Round trip time (RTT), 376
- Rower architecture, 39–40
- RRNS. *See* Redundant Residue Number System (RRNS)
- RSA. *See* Rivest-Shamir-Adleman-system (RSA)



**S**

- Scalar-pair vectors routing and forwarding (SVRF), 370–372
- Shenoy and Kumaresan's technique, 358
- Shortest vector problem (SVP), 346–348
- Signal-to-noise ratio (SNR), 85, 249, 255, 266
- Signed digit (SD) representation, 284
- Signed-Power-of-Two (SPT), 284
- Single event upset (SEU), 205
- Single instruction multiple data (SIMD), 366
- Six-Moduli RRNS (6 M-RRNS), 85, 86
- Software-defined network (SDN), 370–372
- Software defined radio (SDR), 277
- Structural SIMilarity index (SSIM), 227–228
- Synapse multiplier, CVNS
  - current-mode circuits, 172–173
  - CVNS registers, 176
  - layout of proposed CVNS multiplier, 173–176
  - post-layout simulation results, 173–176
  - sigmoid activation function, 172

- TSMC CMOS 0.18  $\mu\text{m}$  technology, 171
- Synopsys Design Compiler, 136

**T**

- Time-multiplexed multiple constants multiplication (TMCM), 281–283
- Transport triggered architecture (TTA), 40
- Triple modular redundancy (TMR), 205
- Two's complement system (TCS), 66, 189, 204

**W**

- Wallace-tree, 269
- Watermarking algorithms, 219
- Weighted number system, 6
- Wireless sensor network (WSN), 369, 376–378

**X**

- Xilinx Virtex-E FPGA, 211–212