

Index

- 2-design, 201
- 2-weight, 45, 155, 324, 327
- (n, m) -function, 24, 30, 51, 71, 113, 127, 186, 268, 313, 344, 348, 369, 415, 437, 476
- (n, m, t) -function, 129, 313
- $[n, k, d]$ -code, 7, 292
- $[n, k, d]_q$ -code, 7
- $\mathbb{Z}$ -bent function, 239
- k -normal function, 105
- k -th order derivative, 39, 159
- k -weakly normal function, 105
- n -variable, 17
- p -ary function, 159
- p -polynomial, 491
- r -th order nonlinearity, 83
- s -th order Kronecker sum, 310
- AB, 370, 478, 479
- absolute indicator, 97
- absolute trace function, 42
- absolute trace representation, 43
- access structure, 147
- address function, 68, 264
- adjoint operator, 63
- Advanced Encryption Standard (AES), 25
- affine disperser, 105
- affine function, 37, 79, 131, 152, 166, 190, 369
- affine invariant, 29, 88, 92, 97, 101, 102, 114, 443
- affine plane, 137, 218, 220
- affinely equivalent, 28, 103, 165, 335
- algebraic attack, 89, 189, 321
- algebraic degree, 35, 40, 63, 91, 99, 102, 151, 190, 202, 213, 222, 242, 251, 259, 287, 318, 321, 337, 476
- algebraic immunity, 91, 127, 321, 344
- algebraic immunity with inputs in E , 464
- algebraic manipulation, 450
- algebraic manipulation detection codes, 450
- algebraic normal form, 31, 39, 103, 213, 248, 375, 476
- algebraic thickness, 103
- almost bent, 119, 370
- almost perfect nonlinear, 137, 371
- ambiguity, 139
- AMD code, 450
- amplitude, 258
- ANF, 31, 90, 128, 174, 195, 200, 292, 320, 335, 353, 359, 441
- annihilator, 91, 127
- APN, 137, 371, 478
- APN exponent, 383
- arithmetic Walsh transform, 57
- asymmetric cryptography, 2
- atomic function, 31
- attacker model, 20, 425
- authentication scheme, 149
- autocorrelation function, 61, 71
- automorphism group, 88
- automorphism group of function, 72, 192
- Ax's theorem, 156
- balanced, 16, 76, 112, 252, 475–477
- balanced incomplete block design, 201
- basic algebraic immunity, 127
- BCH bound, 13, 338, 387
- bent, 80, 370, 449, 476, 477, 479
- bent concatenation bound, 81
- bent concatenation construction, 234
- bent exponents, 230
- bent monomial Boolean univariate functions, 229
- bent₄, 267
- Berlekamp–Massey (BM) algorithm, 21
- best affine approximation, 57
- bias in the output distribution, 134
- big open APN problem, 410
- binary entropy function, 289
- binary expansion, 45
- binary Möbius transform, 33, 37, 353
- binomial AB functions, 397
- binomial APN functions, 405
- bit-probing security, 429, 445
- bivariate APN functions, 409
- bivariate representation, 47, 207, 209, 213, 231, 249, 270, 361
- black box attacker model, 425

558

block cipher, 3
 Boolean functions in dimension n , 17
 Boolean masking, 428, 444, 445, 447
 boomerang uniformity, 141
 bounded moment security model, 429
 Brinkmann–Leander–Edel–Pott function, 408
 butterfly construction, 411, 421

 CAPN, 391, 478
 Carlet–Feng function, 337
 Cayley graph, 70
 CCZ equivalence, 29, 345, 370, 403, 478
 CCZ equivalent, 28, 72, 115, 281, 380, 475
 CCZ invariant, 29, 117, 136, 138, 275, 403
 changing of the guards, 443
 characteristic polynomial, 21
 ciphertext, 1
 classical Singer set, 416
 classify, 27, 478
 cosupport, 201
 code, 5
 code design, 201
 codebook, 34
 codeword, 4
 coding theory, 4
 coincident functions, 37
 collineation, 221
 combiner model, 21, 86, 126, 284
 complementary information set code (CIS), 432
 complete class, 192
 completed Maiorana–McFarland class, 165, 173
 complexity parameters, 103
 component algebraic immunity, 127
 component functions, 40, 112, 115, 122, 268, 272, 274, 278, 345, 369, 414, 439, 493
 componentwise APN, 391, 478
 componentwise Walsh uniform, 414
 composite function, 39, 64, 371
 concatenated code, 9
 confusion, 76
 continuous side-channel attacks, 427
 conventional cryptography, 2
 coordinate functions, 8, 24
 Coron–Roy–Vivek (CRV) method, 434
 correction capacity, 5
 correctness, 437
 correlation attack, 87
 correlation immune, 86, 129, 313
 correlation immunity order, 86
 correlation power analysis, 426
 coset, 7
 coset leader, 7, 43, 79, 475
 Courtois–Meier bound, 92, 469
 covered, 33, 341
 covering radius, 6, 81, 157, 159, 205
 covering radius bound, 80, 118, 133, 269
 covering sequence, 182

Index

CPA, 426
 CPRR method, 435
 crooked, 231, 278
 cryptanalysis, 1
 cryptography, 1
 cryptology, 2
 cryptosystem, 1
 cubic functions, 36, 115, 248
 cubic sums, 177
 CWU, 414
 cyclic code, 12, 155, 215, 245, 249, 262, 326, 341, 387, 446
 cyclic difference set with Singer parameters, 415
 cyclic-additive difference set, 416
 cyclotomic class, 43
 cyclotomic method, 434

 Data Encryption Standard (DES), 25
 DDT, 135
 dealer, 146
 decomposable functions, 232
 decryption, 1
 defining set, 12, 387
 derivative, 38, 52, 61, 67, 81, 98, 275, 414, 476, 477
 derivative imbalance, 138
 Desarguesian spread, 213
 designed distance, 13
 deterministic leak, 426
 Dickson form, 173
 Dickson polynomial, 389, 409, 491
 difference distribution table, 135
 difference set, 197, 448
 difference set design, 201
 difference table, 71
 differential, 134
 differential attack, 134
 differential cryptanalysis, 134
 differential power analysis, 426
 differential spectrum, 135
 differential uniformity, 135, 371
 differentially δ -uniform, 135
 diffusion, 76
 Dillon exponents, 215
 Dillon's functions, 213
 Dirac (or Kronecker) symbol, 55
 direct sum, 232, 265, 297, 341, 362
 direct sum masking, 444
 direct sum of bent functions, 274
 direct sum vector, 363
 distance enumerator, 16, 255
 distance invariant, 255
 distance to linear structures, 101
 distinguisher, 116, 134
 distinguishing attack, 89
 Dobbertin function, 401, 412
 Dobbertin's conjecture, 297
 domain-oriented masking, 444
 double simplex code, 10

- DPA, 426
 DSM, 444
 dual code, 8, 17, 146
 dual distance, 16, 88, 162, 284, 292, 314, 432
 dual function, 197
 dual-bent vectorial function, 269
- EA equivalent, 28, 219, 281, 359, 394, 404
 EA invariant, 29, 36, 40, 79, 192, 275
 edges, 70
 encryption, 1
 equivalent codes, 8
 error detecting/correcting codes, 4
 error vector, 9
 eSTREAM Project, 22
 exact repair problem, 146
 exceptional, 404
 expander graph, 468
 extended code, 6, 380
 extended propagation criterion, 97, 319
 extended Walsh spectrum, 55, 71
 extended Walsh transform, 244
 extension of Maiorana–McFarland type, 235
- FAA, 93, 291, 344
 fast algebraic attack, 93, 190, 284, 291, 321, 335, 338
 fast algebraic complexity, 94, 322
 fast algebraic immunity, 94, 321
 fast correlation attack, 78, 194, 244
 fast Fourier–Hadamard transform, 53
 fast Möbius transform, 33
 fault injection attack, 427
 feedback coefficients, 21
 feedback polynomial, 20
 feedback shift register, 23
 Feistel cipher, 26, 112, 423
 FHE, 453
 FIA, 427
 filter model, 22, 89, 126
 filter permutator, 454
 flat, 36
 FLIP cipher, 454
 Fourier–Hadamard spectrum, 53
 Fourier–Hadamard support, 53
 Fourier–Hadamard transform, 53, 117, 132, 306
 Frobenius automorphism, 42, 222, 487
 fully homomorphic encryption, 453
- general affine group, 155
 generalized correlation attack, 131
 generalized degree, 48
 generalized nonlinearity, 132
 generalized partial spread, 242
 generator matrix, 7
 generator polynomial, 12
 Gleason theorem, 16
 glitches, 436
- global avalanche criterion, 97
 Gold AB functions, 394
 Gold APN functions, 400
 Gold Boolean functions, 206
 Goldreich’s function, 468
 Goldreich’s pseudorandom generator, 468
 Golomb–Xiao–Massey characterization, 87, 286, 363
 Gowers inverse conjecture, 473
 graph, 7, 34, 39, 40, 51, 71, 72, 136, 275, 388
 graph algebraic immunity, 127
 graph theory, 70
 gray box attacker model, 425
 group algebra, 152, 403
 guess and determine, 96
- Hadamard difference set, 197
 Hamming bound, 6
 Hamming code, 8, 13, 155, 379
 Hamming distance, 5, 27
 Hamming distance leakage model, 426
 Hamming weight, 4, 27, 112, 130, 154, 180, 195, 215, 285, 303, 475, 477, 479
 Hamming weight leakage model, 426
 hexadecimal, 417
 hexanomial APN functions, 408
 hidden weight bit function, 343, 477
 higher-order differential attack, 114
 higher-order nonlinearity, 83, 114
 higher-order side-channel attack, 427
 HO-SCA, 427
 homogeneous function, 201, 209, 248
 HWBF, 343
 hybrid symmetric-FHE encryption, 453
 hyper-bent function, 244, 246, 272, 338, 477
 hypergraph, 70
 hyperoval, 219
 hyper-nonlinearity, 338, 477
- ideal autocorrelation, 416
 idempotent function, 248, 360
 imbalance, 114, 268
 indicator, 51, 58, 71, 103, 127, 154, 181, 275, 345, 375, 416, 432, 448
 indirect sum, 233, 235, 265, 300
 influence of variable, 68
 information bits, 7
 information protection, 17
 information set, 161, 314, 328, 432
 initial functions, 209
 inner product, 37, 58, 61, 160, 164, 166, 209, 213
 inner product masking, 446
 interpolation attack, 142
 inverse Fourier–Hadamard transform formula, 59, 65, 88
 inverse function, 85, 137, 317, 324, 400, 401, 412, 417, 423, 433, 442, 479
 inverse Walsh transform formula, 59, 65, 71, 109, 380, 438

IPM, 446
ISW algorithm, 430

Jacobi symbol, 177

Kasami AB functions, 394
Kasami APN functions, 400, 478
Kasami exponents, 230
Kasami function, 418
Kasami–Welch functions, 394
Kerdock code, 254, 477
key scheduling algorithm, 24
keystream, 3, 19, 344, 454
Kloosterman sums, 188
Knuth–Eve method, 434
Krawtchouk polynomial, 355
Kronecker sum, 309

last round attack, 134
LCD, 446
LCP, 445
leakage, 425
leakage squeezing, 431
leakage trace, 427
level of the covering sequence, 182
LFSR, 20
line ovals, 220
linear attack, 115
linear code, 7
linear complementary dual, 446
linear complementary pair, 445
linear complexity, 21, 77
linear exact repairing code, 428
linear feedback shift register, 20
linear invariant, 29
linear kernel, 99, 383
linear leakage model, 426
linear secret sharing scheme, 146, 450
linear span, 21
linear structure, 99
linearized polynomial, 46
linearly equivalent, 28, 99, 134, 337, 400
local pseudorandom generator, 467
log-alog, 75
lookup table, 30
Lucas’ theorem, 487

m-sequence, 21, 77, 383, 490
MacWilliams’ identity, 15
Maiorana–McFarland, 165, 263, 293
Maiorana–McFarland original class, 209
Maiorana–McFarland vectorial functions, 167
majority function, 335, 468
masked version of function, 428
masking, 428
masking complexity, 433
masking order, 428
masks, 428

master key, 24
Mattson–Solomon polynomial, 44
maximal odd weighting, 153
maximum correlation with respect to I , 101
maximum distance separable, 6, 14
maximum length sequence, 21, 383
maximum likelihood decoding, 6
McEliece’s theorem, 13, 65, 156
MCM polynomial, 400
MDS, 6, 9, 14, 147, 162, 446
Menon design, 201
message, 4
metric complements, 191
minimal code, 149
minimal codeword, 148
minimum degree, 41
minimum distance, 5
Möbius transform over integers, 49
modeled leakage, 426
modified derivatives, 266
modified planar, 269
monomial bent, 229
monomial Boolean (multivariate) function, 363
monomial Boolean (univariate) function, 66
monomial vectorial function, 383
monotone, 363
monovariate attack, 425
Müller–Cohen–Matthews polynomial, 400
multidimensional Walsh transform, 74
multinomial APN functions, 231, 406
multioutput Boolean function, 24
multiparty computation, 146, 436, 453, 454
multipermutation, 129
multiplicative inverse permutation, 400

naive bound, 243
near-bent, 119, 178, 262
nega-bent, 191, 267
NFSR, 23, 475
Niho functions, 395
NNF, 47, 156, 195, 326, 352
nodes, 70
noisy leakage model, 429
noncompleteness, 439
nonhomomorphism, 111
noninterference, 430
nonlinearity, 79, 117, 369, 475, 478, 479
nonlinearity profile, 83
nonlinearity with inputs in E , 459
nontrivial covering sequence, 182
nonzeros of the cyclic code, 12
Nordstrom–Robinson code, 254
normal basis, 248
normal extension, 253
normal function, 105
numerical degree, 48, 67, 69, 70, 201, 287, 356, 475
numerical normal form, 47, 199, 286
Nyberg’s bound, 423, 478

- ODSM, 446
- one-way function, 2, 467
- one time pad, 19
- orphan, 159, 262
- orthogonal array, 86
- orthogonal direct sum masking, 446
- orthogonal space, 58
- oval polynomial, 219
- pair of metrically regular sets, 191
- parity check bits, 7
- parity check matrix, 8
- parity check polynomial, 78
- parity code, 5
- Parseval’s relation, 60, 61, 68, 79, 118, 258
- partial bent functions, 258
- partial spread, 212
- partial spread class, 212
- partially defined, 37
- partially-bent function, 256
- perfect algebraic immune, 322
- perfect code, 6
- perfect nonlinear, 135, 193, 449, 477, 478
- perfect robust code, 448
- permutation, 10
- permutation equivalent, 28
- permutation invariant, 29, 48, 88, 102
- physical attack, 427
- plaintext, 1
- planar, 269
- plateaued, 258–261, 264, 275, 279, 283, 382, 391, 393
- plateaued with single amplitude, 140, 274, 372
- player, 146
- Poisson summation formula, 58, 65, 87, 106, 200, 286, 364
- polar representation, 168, 271, 340, 351
- polynomial masking, 436
- polynomial representation of codeword, 12
- power bent, 229
- power function, 24, 72, 134, 161, 263, 278, 324, 478
- preferred cross-correlation, 384
- PRG, 19
- primary construction, 209, 263, 270, 282, 291, 336, 417, 479
- primitive element, 11, 44, 155, 168, 336, 378, 405, 477, 487
- primitive length, 12
- private-key cryptography, 2
- probing security model, 428
- projective equivalence, 221
- projective plane, 219
- propagation criterion, 97, 319
- pseudo-Boolean, 17, 37, 256, 377, 445
- pseudoplanar, 269
- pseudorandom generator, 19, 86, 321, 467
- pseudorandom sequence, 19
- public-key cryptography, 2
- punctured code, 6, 155, 162
- puncturing at position i , 6
- quadratic bound, 81
- quadratic function, 36, 64, 85, 99, 103, 107, 115, 165, 172, 177, 223, 257, 393, 441, 475, 478
- quadrinomial APN functions, 405
- qualified coalition, 147
- radical, 152, 171
- random local function, 467
- rank of β_f , 171
- Rayleigh quotient, 199
- realization, 437
- rectangles, 239
- reduced cipher, 115, 134
- redundancy, 5
- Reed–Muller code, 23, 37, 65, 80, 151, 154, 328, 341, 475, 477
- Reed–Solomon code, 14, 45, 151
- relative difference set, 197
- resiliency order, 86
- resilient, 86, 129, 284, 313, 356, 433, 468, 477
- reversed Dickson polynomial, 389
- robust code, 448
- rotating S-box masking, 432
- rotation symmetric, 248, 292, 360
- Rothaus construction, 233
- Rothaus’ bound, 200
- round key, 24
- rounds, 24
- RS code, 14
- S-box, 24, 112, 127, 129, 134, 369, 475
- S-box of the AES, 417
- Sarkar et al.’s bound, 287
- Sarkar–Maitra’s divisibility bound, 287
- SCA, 425
- SCV bound, 118
- second-order bent function, 257
- second-order covering sequence, 193
- second-order Poisson summation formula, 62, 65, 365
- secondary construction, 144, 209, 211, 232, 251, 266, 273, 297, 317, 362, 442, 457, 478
- secret sharing scheme, 145, 428
- self-dual bent function, 198, 476
- semi-bent function, 178, 262, 268
- semidirect sum, 234
- sensitive variable, 426
- sequences, 383
- session key, 2
- Shannon effect, 103
- sharing, 145
- shifted bent, 267
- shortened code, 6
- side-channel attacks, 425
- Sidelnikov–Chabaud–Vaudenay, 118

Sidon set, 386, 388
Siegenthaler bound, 285, 469
sign function, 55
simplex code, 8, 13, 155, 381
simplified ANF vector, 353
simplified value vector, 352
Singer set, 389, 416
Singleton bound, 6, 452
slices, 456
slide attack, 142
source vectors, 4
spectral complexity, 109
spectral immunity, 96, 327
sphere covering bound, 7
sphere-packing bound, 6
splitting field, 13, 485
spread, 212
statistical distance, 429
Stickelberger theorem, 156
stream cipher, 3
stretch, 468
strict avalanche criterion, 97
strongly plateaued, 274, 278
subfield trace representation, 43
substitution box, 24
substitution permutation network, 26
sum-free set, 388
sum-of-squares indicator, 97, 288
supplementary subspaces, 62, 212
support of function, 27
support of vector, 27
switching, 402, 407
symmetric Boolean function, 206, 244, 322, 328, 335, 352, 477
symmetric cryptography, 2
symplectic matrix, 171, 199
synchronous, 20
syndrome, 9, 10
systematic, 7, 149, 161, 314, 448, 451
systematic form, 147
systematic generator matrix, 7

T-function, 26
Tarannikov et al.'s construction, 300
three-valued almost optimal, 262
three-valued functions, 258

threshold function, 358
threshold implementation, 437, 478
threshold secret sharing schemes, 147
TI, 437, 478
Titsworth relation, 61
trace form, 43
transmission rate, 6, 449
triangular function, 363, 455
trinomial APN functions, 408
triple construction, 228, 388
truth table, 30, 152, 166, 298, 361
Tu–Deng function, 339
two-weight code, 149

uniformity (of TI), 440
uniformly packed code, 10, 381
uniformly robust code, 448
unitary transformation, 266
univariate attack, 425
univariate representation, 42, 142, 214, 221, 231, 271, 476
unrestricted code, 7, 23, 83
unrestricted nonlinearity, 131
usual inner product, 8, 15, 37, 53, 117, 165, 190, 307

vectorial bent₄ functions, 274
vectorial Boolean functions, 24
Vernam cipher, 19
vertices, 70

Walsh functions, 53, 109
Walsh spectrum, 55, 71
Walsh support, 55, 71
Walsh transform, 55, 71
weakly APN, 383
weight distribution, 14
weight enumerator, 14
weightwise almost perfectly balanced, 459
weightwise perfectly balanced, 457
Weil's bound, 188
Welch functions, 395
Wiener–Khinchine formula, 61
worst error-masking probability, 447, 448

zero-difference 2-balanced, 394
zeros of the cyclic code, 12