<table>
<thead>
<tr>
<th>achievability</th>
<th>82</th>
</tr>
</thead>
<tbody>
<tr>
<td>active limited-knowledge adversary</td>
<td>524</td>
</tr>
<tr>
<td>active omniscient adversary</td>
<td>524</td>
</tr>
<tr>
<td>additivity</td>
<td>265, 278</td>
</tr>
<tr>
<td>Ahlswede–Csiszár secret generation, see secret key generation</td>
<td></td>
</tr>
<tr>
<td>algebraic core</td>
<td>371, 374</td>
</tr>
<tr>
<td>dimension</td>
<td>375</td>
</tr>
<tr>
<td>index set</td>
<td>375</td>
</tr>
<tr>
<td>rank</td>
<td>375</td>
</tr>
<tr>
<td>rank loss</td>
<td>375</td>
</tr>
<tr>
<td>alternating CSIT</td>
<td>214</td>
</tr>
<tr>
<td>DN/ND</td>
<td>223</td>
</tr>
<tr>
<td>PD/DP</td>
<td>221</td>
</tr>
<tr>
<td>anchor node</td>
<td>391</td>
</tr>
<tr>
<td>anonymous broadcast messaging</td>
<td>476</td>
</tr>
<tr>
<td>arbitrarily varying channel, 259, 315, 317, 324, 325</td>
<td></td>
</tr>
<tr>
<td>CR-assisted capacity</td>
<td>325</td>
</tr>
<tr>
<td>unassisted capacity</td>
<td>325</td>
</tr>
<tr>
<td>arbitrarily varying wiretap channel, 259, 259, 274, 315, 316, 318, 321, 322</td>
<td></td>
</tr>
<tr>
<td>CR-assisted secrecy capacity</td>
<td>321</td>
</tr>
<tr>
<td>orthogonal</td>
<td>322</td>
</tr>
<tr>
<td>unassisted secrecy capacity</td>
<td>322</td>
</tr>
<tr>
<td>attack vectors</td>
<td>368, 372</td>
</tr>
<tr>
<td>attacks</td>
<td></td>
</tr>
<tr>
<td>active attacks</td>
<td>258, 259</td>
</tr>
<tr>
<td>passive attacks</td>
<td>258, 259</td>
</tr>
<tr>
<td>authentication</td>
<td>390, 396, 424</td>
</tr>
<tr>
<td>channel-based</td>
<td>395</td>
</tr>
<tr>
<td>key-based</td>
<td>394</td>
</tr>
<tr>
<td>keyless</td>
<td>394</td>
</tr>
<tr>
<td>physical-layer authentication, 393</td>
<td></td>
</tr>
<tr>
<td>AVC, see arbitrarily varying channel</td>
<td></td>
</tr>
<tr>
<td>average wasted energy</td>
<td>507</td>
</tr>
<tr>
<td>AWVC, see arbitrarily varying wiretap channel</td>
<td></td>
</tr>
<tr>
<td>backtracking line search</td>
<td>133</td>
</tr>
<tr>
<td>barrier method</td>
<td>132</td>
</tr>
<tr>
<td>battery capacity</td>
<td>509</td>
</tr>
<tr>
<td>beamforming</td>
<td>145</td>
</tr>
<tr>
<td>Berger–Tung coding</td>
<td>91</td>
</tr>
<tr>
<td>Bernoulli source</td>
<td>84, 101</td>
</tr>
<tr>
<td>bin index</td>
<td>82, 91</td>
</tr>
<tr>
<td>binary entropy function</td>
<td>84, 101</td>
</tr>
<tr>
<td>binary erasure fading wiretap channel</td>
<td>232</td>
</tr>
<tr>
<td>binary jamming</td>
<td>70</td>
</tr>
<tr>
<td>binary symmetric channel</td>
<td>84, 101</td>
</tr>
<tr>
<td>binning</td>
<td>82, 91, 94, 99</td>
</tr>
<tr>
<td>biometric authentication</td>
<td>445, 446, 450, 451</td>
</tr>
<tr>
<td>biometric authentication system, 421, 424</td>
<td></td>
</tr>
<tr>
<td>BSC, see binary symmetric channel</td>
<td></td>
</tr>
<tr>
<td>capacity</td>
<td>263</td>
</tr>
<tr>
<td>uncorrelated coding</td>
<td>260, 263, 264, 308</td>
</tr>
<tr>
<td>zero-error</td>
<td>314</td>
</tr>
<tr>
<td>secret common randomness assisted, 277</td>
<td></td>
</tr>
<tr>
<td>with public side information, 268, 277</td>
<td></td>
</tr>
<tr>
<td>zero error</td>
<td>264</td>
</tr>
<tr>
<td>causal disclosure</td>
<td>59, 68</td>
</tr>
<tr>
<td>CCDF</td>
<td>234</td>
</tr>
<tr>
<td>cellular model</td>
<td>333, 334, 340, 343, 357</td>
</tr>
<tr>
<td>channel</td>
<td>184</td>
</tr>
<tr>
<td>$K$-user</td>
<td>195</td>
</tr>
<tr>
<td>orthogonal</td>
<td>270, 285</td>
</tr>
<tr>
<td>broadcast</td>
<td>184</td>
</tr>
<tr>
<td>interference</td>
<td>184</td>
</tr>
<tr>
<td>multi-access</td>
<td>184</td>
</tr>
<tr>
<td>multi-antenna</td>
<td>184, 189</td>
</tr>
<tr>
<td>relay</td>
<td>184</td>
</tr>
<tr>
<td>X-channel</td>
<td>187</td>
</tr>
<tr>
<td>channel enhancement</td>
<td>232</td>
</tr>
<tr>
<td>channel resolvability</td>
<td>165, 166, 170</td>
</tr>
<tr>
<td>channel state information</td>
<td>184</td>
</tr>
<tr>
<td>alternating</td>
<td>195</td>
</tr>
<tr>
<td>causal</td>
<td>185</td>
</tr>
<tr>
<td>mixed</td>
<td>186</td>
</tr>
<tr>
<td>no</td>
<td>190</td>
</tr>
<tr>
<td>perfect</td>
<td>185</td>
</tr>
<tr>
<td>channel state information at transmitter, 203, 231</td>
<td></td>
</tr>
<tr>
<td>alternating CSIT</td>
<td>214</td>
</tr>
<tr>
<td>delayed CSIT</td>
<td>203</td>
</tr>
<tr>
<td>homogeneous CSIT</td>
<td>203</td>
</tr>
<tr>
<td>hybrid CSIT</td>
<td>203</td>
</tr>
<tr>
<td>no CSIT</td>
<td>203</td>
</tr>
<tr>
<td>perfect CSIT</td>
<td>203</td>
</tr>
</tbody>
</table>
Index

555
code, 274–277, 319, 321
CR-assisted code, 275–277, 284, 290, 291, 296, 298, 321
private/public, 275
shared randomness assisted code, 274, 275, 296
unassisted code, 319
uncorrelated code, 260, 262, 274, 276, 286, 296
coding scheme at helper, 93
decode and reencode, 93, 95, 96
forwarding, 93, 94, 96
common goal game, 514
common randomness, 262, 265, 267, 268, 270, 271, 277–279, 286, 296, 300, 303, 320
competitive privacy, 511
game theoretic formulation, 513
pricing, 514
compound channel, 120, 263, 276, 291
compound source, 365
compound wiretap channel, 267, 279, 291
concentrator node, 391
continuity, 282
capacity, 270, 278, 279, 282, 284, 307
cooperative jamming, 141, 148, 149, 152–154, 157–159, 161, 162, 178
countably infinite support, 27, 41
coupling, 234
covariance matrix, 112, 118
full-rank, 110, 113, 115, 118
optimal, 110, 112, 114, 116, 119, 122, 128–131
rank of, 113
rank-1, 113, 114
CR, see common randomness
CSI, see channel state information
CSIT, see channel state information at transmitter
cut-set bound, 337, 343, 344, 346, 348, 350, 351, 357
cyber-physical system, 499
dark bit masking, 373, 377
data processing inequality, 96
database
multiple databases, 504
multiple queries, 504
database attributes
public (revealed) and private (hidden), 501
database model, 500
decode, 186
interference alignment, 185
noise injection, 186
zero-forcing, 186
degraded, 233
degrees of freedom, 181, 196
secure, 204
generalized, 189, 196
secure, 184
derandomization, 303
deterministic cipher, 22
dining cryptographer networks, 477
discrete $p$-dispersion problem, 458
discrete memoryless source, 55
distortion, 84, 87, 88
Hamming, 61, 84, 101
logarithmic loss, 73, 87, 88, 90, 94, 95
measure of utility, 501
quadratic, 88, 90
distributed storage system, 522
file reconstruction, 522
node repair, 522
exact repair, 523
functional repair, 523
eavesdropper, 79, 258, 259, 524
isotropic, 120–123, 125
negligible, 125
omnidirectional, 110, 127
weak, 110, 117–119
elimination of correlation, 173
encryption, 95
end-user privacy, 97, 98
energy efficiency, 404, 407
energy harvesting and storage, 506
energy harvesting rate, 508
energy management unit, 506
enrollment, 424
enrollment biometric sequence, 423, 427, 430, 439
entropy, 78, 195, 376, 501
conditional, 78, 98
relative, 273
entropy power inequality, 88
EPI, see entropy power inequality
EPS, see error-free perfect secrecy system
equivocation
measure of privacy, 501
rate, 73, 78, 97
erasure probability, 84, 101
error
error-free, 22
average error, 262, 275, 279, 289, 296, 298, 305
maximal error, 264
zero error, 264
error correcting code, 363, 452, 453, 470
error-free perfect secrecy system, 25
false acceptance exponent, 421, 422, 424, 428, 431, 439
maximum achievable, 425, 431
achievable, 424, 427, 431, 439
false acceptance rate, 421, 422, 424, 427
false alarm, 397, 398, 402
false rejection rate, 421, 424, 427, 431
FAR, see false acceptance rate
feedback, 187
Index

fixed-basis design, 462
Fourier–Motzkin elimination, 348
PRR, see false rejection rate
game theory, 513
payoff function, 513
Gaussian source, 88, 90
generalized likelihood ratio test, 397
global maximization, 131
GLRT, see generalized likelihood ratio test
graphical equivalence, 461
Grassmann graph, 457
hash function, 370, 373
Hasse diagram, 458
Hausdorff distance, 273
helper data, 363, 370
capacity, 368
leakage, 364, 370
rate, 368, 386
helper data generation
code-offset fuzzy extractor, 378, 386
comparison, 385
complementary IBS (C-IBS), 383, 386
fuzzy commitment, 377, 386
index-based syndrome coding (IBS), 380, 386
parity construction, 379, 386
syndrome construction, 378, 386
systematic low leakage coding (SLLC), 379, 386
helper message, 430, 439
Henchman problem, 62, 70
hierarchical model, 333–337, 357
high SNR, 115–118, 122, 123, 125, 126
homogeneous CSIT, 203, 205
DD, 203, 206, 208, 213, 216, 224
NN, 203, 206, 216, 217
PP, 203, 205, 216, 217
hybrid CSIT, 203, 211
DN, 211, 212
PD, 211
PN, 211
hypothesis testing, 16
impostor authentication sequence, 423, 424, 427, 430
impostor strategy, 433, 434, 436, 437
information density, 165, 168
information diagrams, 38
information leakage rate, 78, 81
information theoretic security, 181
initial key requirement, 24
Internet of Things, 390
cellular IoT, 399
IoT, see Internet of Things
isotropic signaling, 110, 131
jammer, 258, 259
joint privacy leakage, 454
joint security, 454
key consumption
excess, 32
expected, 24, 31
minimal expected, 37–44
minimizing, 30
key regeneration, 57
KKT conditions, 110, 112, 114, 117, 132, 133, 136, 137
Kullback–Leibler divergence, 87, 273
layered coding, 82, 83, 99
layered signaling, 232
legitimate authentication sequence, 423, 424, 427, 430
linear codes, 371
linear measurement model, 511
local statistical equivalence property, 213
locally repairable codes, 521
lossless compression, 53
low SNR, 119, 120, 123, 125, 126
MBR, see minimum bandwidth regenerating
MIMO, 109, 110, 116, 122, 128, 131
minimax optimization, 133
minimum bandwidth regenerating, 523
minimum storage regenerating, 523
MISO, 110, 113
missed detection, 397–400
MSR, see minimum storage regenerating
multi-stage game, 514
infinite window, 514
multiple antennas, 232
multiple biometric systems, 447, 450
multiple key capacity region, 333, 334, 336, 337, 341–344, 346, 348–352, 357, 358
mutual information, 78, 81, 273, 370, 375, 376, 507
Nakagami-m fading, 232
Nash equilibrium, 514
network lifespan, 403–406, 414
networked secure source coding, 77–103
under a reconstruction privacy, 96
with a helper, 85
one-sided, 86, 90
two-sided, 89, 91
with an intermediate node, 92
Newton method, 132–135
number of channel uses, 24
minimal number, 45
omniscience, omniscience scheme, 334, 337
one-norm distance, 272
one-time pad, 29, 45, 53
partition code, 39, 40
passive adversary, 524
phasor measurement units, 500
physical layer security, 77, 183, 266
physical unclonable function
  analogy to source model, 370
  arbiter PUF, 363
  ring oscillator (RO) PUF, 363
  SRAM PUF, 363
PIN model, 333, 334, 352, 357
PM codes, see product-matrix codes
PMUs, see phasor measurement units
postprocessing matrix, 370, 371, 383, 385
preprocessing matrix, 370, 371, 381, 385
primal/dual method, 133
prisoner’s dilemma, 514
privacy, 445, 447, 449, 450, 453–455, 457
privacy leakage, 421, 422, 439
achievable, 439
privacy leakage rate, 439
privacy protection, 421, 422
privacy–security pair, 439
quantization, 440
random binning, 334, 338–340, 345
randomized encoding, 260, 276, 306
rate splitting, 94
rate–distortion theory, 59, 68
rate–distortion=equivocation region, 99, 100, 503
rate–distortion=leakage region, 82, 86, 88, 89, 94, 95
rate-constrained authentication, 427
real interference alignment, 153
complex-field extension, 155
reconstruction, 100
causal, 100
memoryless, 100
regional transmission organizations, 511
relaxation, 464, 465
reliability information, 370
residual secret randomness, 24, 31
resiliency capacity, 525
reverse water-filling, 506
same marginal property, 232
sanitized database, 502
secrecy capacity, 111–114, 116, 117, 121, 122, 127, 135, 183, 265, 277, 432, 525
bound, 119, 121
uncorrelated, 267, 268, 277, 279, 291
secrecy criterion, 276
effective secrecy, 4, 15
maximum strong secrecy, 276
mean secrecy, 276, 277
mean strong secrecy, 276
perfect secrecy, 21, 53
strong secrecy, 3, 143, 148, 159, 160, 173, 175, 267, 276, 277, 286, 300
weak secrecy, 3, 143, 149, 204
secret common randomness, 268, 277, 279
secret key, 333–335, 337–340, 342, 345, 348, 351, 358, 359
achievable rate, 367, 368
agreement, 366
capacity, 368, 386
generation, 93, 95, 422, 430, 431
rate, 368, 386, 422, 432
secret-based authentication with privacy protection, 439
secret-based biometric authentication, 430, 431
secret-based biometric authentication with privacy protection, 439
secure sketch, 451, 452
secure triangular source coding, 92
security, 445, 447, 449, 450, 453–455, 457
sensor networks, 516
separation scheme, 531
Shannon cipher system, 52
Shannon’s additivity problem, 265
Shannon’s fundamental bound for perfect secrecy, 21–22
shared randomness, 260, 265, 277, 284
side information, 78, 79, 81, 83, 85, 86, 89, 91–93, 95–97, 100
causal, 100
coded, 85, 86, 89, 91
common, 91, 93, 95
degraded, 83, 95, 96
pattern, 92
signaling efficiency, 405
Slepian–Wolf coding, 91, 434
Slepian–Wolf condition, 345, 347, 348, 351, 357
<table>
<thead>
<tr>
<th>Index</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>smart grid</td>
<td>template protection, see privacy protection</td>
</tr>
<tr>
<td>definition, 499</td>
<td>topology, 181, 192</td>
</tr>
<tr>
<td>motivation, 499</td>
<td>fixed, 192</td>
</tr>
<tr>
<td>smart meter, 504</td>
<td>total variation distance, 272</td>
</tr>
<tr>
<td>Markov chain model, 508</td>
<td>transformational equivalence, 461</td>
</tr>
<tr>
<td>privacy concerns, 504</td>
<td>typical sequences, 426, 434</td>
</tr>
<tr>
<td>smart meter privacy</td>
<td>typical set, 288</td>
</tr>
<tr>
<td>active control approach, 506</td>
<td>typicality, 288</td>
</tr>
<tr>
<td>source coding approach, 505</td>
<td></td>
</tr>
<tr>
<td>smart meters, 500</td>
<td></td>
</tr>
<tr>
<td>social networks, 516</td>
<td>unified algebraic description, 370</td>
</tr>
<tr>
<td>source node, 391</td>
<td>unknown and varying eavesdropper channel, 173</td>
</tr>
<tr>
<td>spreading of signals, 261</td>
<td></td>
</tr>
<tr>
<td>statistical equivalence property, 210</td>
<td></td>
</tr>
<tr>
<td>stealth, 4, 16</td>
<td></td>
</tr>
<tr>
<td>stochastic control, 506</td>
<td>variable length coding, 56</td>
</tr>
<tr>
<td>stochastic decoder, 53, 98</td>
<td>variational distance, 165, 166, 170, 173</td>
</tr>
<tr>
<td>stochastic encoder, 53</td>
<td></td>
</tr>
<tr>
<td>stochastic order, 232</td>
<td></td>
</tr>
<tr>
<td>convex order, 232</td>
<td></td>
</tr>
<tr>
<td>increasing convex order, 232</td>
<td></td>
</tr>
<tr>
<td>usual stochastic order, 232</td>
<td></td>
</tr>
<tr>
<td>storage rate, 427, 428</td>
<td></td>
</tr>
<tr>
<td>achievable, 427</td>
<td>water-filling, 110, 115, 116, 123, 128, 130</td>
</tr>
<tr>
<td>subspace codes, 450</td>
<td>WF, see water-filling</td>
</tr>
<tr>
<td>super-activation, 278, 283, 285, 286, 308, 316, 323</td>
<td>wireless sensor network, 392</td>
</tr>
<tr>
<td>superposition coding, see layered coding</td>
<td>worst-case measures, 454</td>
</tr>
<tr>
<td>syndrome, 451</td>
<td>zero-forcing, 110, 129</td>
</tr>
<tr>
<td></td>
<td>ZF, see zero-forcing</td>
</tr>
</tbody>
</table>