Subject index

Note: Page numbers in bold refer to figures and tables.

achievability proof, **26**
  channel coding, 30
  channel model, 162
  coded cooperative jamming, 285
  cooperative jamming, 276
  distributed source coding, 35
  Gaussian broadcast channel with confidential messages, 179
  Gaussian source model, 191
  source coding, 27
achievable rate, 25, 26, 34, 38, 42, 60, 79, 116, 118, 137, 145, 272
advantage distillation, 136–143
  capacity, **137**, 138
  protocol, 136
  rate, 137
AEP, *see* asymptotic equipartition property
AES, 248
application layer, 254
asymptotic equipartition property
  conditional, 20
  joint, 19
  strong, 19
  weak, 21
  weak joint AEP, 22
authentication, 251, 252, 264
  unconditional, 252
AWGN, *see* Gaussian channel

base of logarithm, 15
BEC, *see* binary erasure channel
binary erasure channel, 7, **25**, 32, 53, 65, 84, 85, 90, 222, 223, 228, 229
binary symmetric channel, **25**, 32, 62, 65, 84, 85, 90, 136, 222, 230, 233, 244
binning, 92
block cipher, 248
broadcast channel with confidential messages, 78–103
  Gaussian, 177–190
broadcast channel, 40–44
brute-force attack, 249
BSC, *see* binary symmetric channel

chain rule
  entropy, 16
  mutual information, 16
channel
  broadcast, *see* broadcast channel
  code, *see* code
  discrete memoryless, *see* discrete memoryless channel
  Gaussian, *see* Gaussian channel
  less capable, *see* less capable channel
  multiple-access, *see* multiple-access channel
  noisier, *see* noisier channel
  ordered, 222
  physically degraded, *see* physically degraded channel
  stochastically degraded, *see* stochastically degraded channel, 229
  two-way wiretap, *see* two-way wiretap channel
  weakly symmetric, 63, **63**, 65, 106
  wiretap, *see* wiretap channel
channel capacity
  Gaussian channel, 32
channel coding theorem, 29
channel capacity, 26
channel estimation, 264
Chebyshev's inequality, **14**, 170, 171, 228
Chernov bounds, **14**
code, 26, 37, 41, 59, 68, 79, 91, 105, 272
  linear, *see* linear code
codebook, 26
coded cooperative jamming, **273**, 283–289
coherence interval, 194, **194**, 200, 203, 207
computational security, 248–251
concave, **17**
conditional mutual information, **16**
conditioning does not increase entropy, 16
confidentiality, 251
converse proof, **26**
  broadcast channel with confidential messages, 98

Downloaded from https://www.cambridge.org/core. Bibliotheque Mathematiques Recherche - Chevaleret, on 10 Apr 2020 at 10:31:14, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511977985

channel coding, 31
channel model, 163
cooperative jamming, 277
degraded wiretap channel, 76
distributed source coding, 36
Gaussian broadcast channel with confidential messages, 179
multiple-access channel, 40
source coding, 28
source model, 127
wiretap channel with rate-limited feedback, 166
convex, **17**
convex hull, **38**, 75, 96
cooperative jamming, 10, **273**, 275–283
coset coding, 224
with dual of LDPC codes, 228–229
coset code, 218, 224
coset coding, 225
cross-over probability, 25
crypto lemma, 53, 56, 107, 120, 141

data-processing inequality, **17**, 32, 60, 76, 77, 85, 128, 130
degraded wiretap channel, 58
example, 65
digital signature, 252
discrete memoryless channel, 25
discrete memoryless source, **25**, 33, **59**
distributed source coding, 33
DMC, *see* discrete memoryless channel
DMS, *see* discrete memoryless source
dual code, 218
dummy message, 69, 92, 103, 286

eavesdropper's channel, 58, 79
entropy
binary entropy function, **15**
chain rule, 16
collision entropy, 149
conditional entropy, 15
differential entropy, 18
joint entropy, 15
min-entropy, 150
Rényi entropy, 151
Shannon entropy, **15**
entropy–power inequality, **18**, 181
equivocation, 5, **50**, 59, 79
erasure probability, 25
exponential-integral function, **202**, 206, 208
extractor, **159**, 160

fading
block fading, 194, 203–206
ergodic fading, 194–203
quasi-static fading, 194, 206–210, 244
fading coefficient, **194**
fading gain, **194**
Fano's inequality, **17**, 29, 31, 51, 69, 76, 92, 98, 123, 127, 132, 138, 145, 163, 169, 205, 277, 286
feedback
rate-limited, 105
secure, 105
full secrecy, *see* secrecy condition
functional dependence graph, **22**, 102

generator matrix, 218
GPRS, 258
GSM, 258

hash functions, 250

IETF, 255
integrity, 251
intrinsic conditional information, 130
reduced, 133
IP, 247
IPSec, 256

Jensen's inequality, **17**, 150, 153, 180, 181
joint AEP, 39, 44

kernel, **187**, 226
key-distillation strategy, 113, 115, 278

LDPC, *see* low-density parity-check code
leakage, **50**, 59, 92, 116, 195, 272
less capable channel, **87**, 88, 90
linear code, 218, 224
coset, *see* coset code
dual, *see* dual code
syndrome, *see* syndrome
link layer, 256
local randomness, **59**, 67, 68, 79, 91, 103, 105, 113, 115, 136, 144, 272, 278, 285
low-density parity-check codes, 217–223
message-passing, 220–222, 232–233
threshold, 222
LTE, 259

main channel, 58, 79
Markov chain, **17**
Markov's inequality, **13**, 160, 173
multiple-access channel, 37–40, 284, 285
mutual information, **16**
chain rule, 16

near-field communication, 260
network coding, 293
Byzantine attacks, 306
linear, 296
passive attacks, 303
protocols, 299
vulnerabilities, 302

Downloaded from https://www.cambridge.org/core. Bibliotheque Mathematiques Recherche - Chevaleret, on 10 Apr 2020 at 10:31:14, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511977985

network error correction, 306
network information theory, 33
network layer, 255
NIST, 250
noisier channel, **86**, 88–90, 104, 106

one-time pad, 5, 52, 249, 273, 289, 290
one-way communication, 116, 119, 121, 145, 154
optical communication, 257
OSI Reference Model, 253
outage probability, 208

parity-check matrix, 218
perfect secrecy, *see* secrecy condition
physically degraded channel, **84**, 88, 108, 165
privacy amplification, 148–162, 243
  extractor, *see* extractor
  universal hash function, *see* universal hash functions
public-key cryptography, 249

quantization, 127, 147

random binning, **27**, 35, 123
random coding, **30**, 39, 42, 65, 68, 90, 91, 285
rate–equivocation region
  broadcast channel with confidential messages, **79**, 80
  degraded wiretap channel, **60**, 61
  wiretap channel, **80**, 81
reconciliation, 143–148, 231–242
  binary source, 231–234
  capacity, 145
  continuous random variables, 147
  direct reconciliation, **147**, 155
  efficiency, 147
  Gaussian source, 239–242
  multilevel reconciliation, 235–239
  protocol, **144**, 154, 161, 232, 235, 243
  rate, 145
  reverse reconciliation, **147**, 157
RFID, 259
RSA, 249

secrecy-capacity region
  broadcast channel with confidential messages, 81
  Gaussian broadcast channel with confidential messages, 179
secrecy capacity, 6
  Gaussian wiretap channel, 185
  wireless channel, 196, 204, 208
  wiretap channel, **60**, 62, 168
secrecy condition
  full secrecy, **60**, 61, 65, 68, 70, 80, 91
  perfect secrecy, 3, **5**, 49–53, 55, 60, 117, 227, 305
  strong secrecy, 55, 166
  weak secrecy, 55, 166
secret-key agreement, 112–176
  channel model, 114, 278
  Gaussian source model, 190
  source model, 113
secret-key agreement, 262
secret-key capacity
  channel model, **162**, 166, 277
  source model, **118, 119**, 138, 158
secure channel codes, 261
security services, 248, 251
selection lemma, **14**, 27–29, 31, 36, 72, 94, 126, 288
Shannon's cipher system, 4, 49
side information, 37
Slepian–Wolf code, 34
Slepian–Wolf region, 34
source
  code, *see* source code
  discrete memoryless, *see* discrete memoryless source
source coding, 27
source code, 25, 34
source coding theorem, 26
source coding with side information, 37
spread spectrum, 257
SSL, 255
stochastically degraded channel, **84**, 85, 88, 90, 178, 196
stochastic encoder, 59
strategy, *see* key-distillation strategy
stream cipher, 249
strong secrecy, *see* secrecy condition
strong secrecy capacity
  wiretap channel, **61**, 168
strong secret-key capacity
  channel model, **162**, 166
  source model, **118**, 158
superposition coding, **42**, 66, 91–93
symmetric encryption, 248
syndrome, 218, 232

Tanner graph, 218, 219
TCP, 247
time-sharing, 40, 276, 282, 290
transport layer, 255
two-way communication, 116
two-way wiretap channel, 105, 270–275
  Gaussian, 270
typical set
  consistency, 19
  jointly typical set, 19

Downloaded from https://www.cambridge.org/core. Bibliotheque Mathematiques Recherche - Chevaleret, on 10 Apr 2020 at 10:31:14, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511977985

typical set
- jointly weak typical set, 21
- strong typical set, 18
- weak typical set, 21

UMTS, 259
universal families of hash functions, **152**, 252

variational distance, **15**, 74, 159, 160
Vernam's cipher, 5, 52

weak secrecy, *see* secrecy condition
wiretap channel, 6, 49
- binary erasure, 54, 90, 223–231
- binary symmetric, 90, 244
- complex Gaussian, 185
- degraded, **58**
- type II, 227, 305

wiretap code, 6

X.800, 253

Downloaded from https://www.cambridge.org/core. Bibliotheque Mathematiques Recherche - Chevaleret, on 10 Apr 2020 at 10:31:14, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511977985