CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-29951-0 — Privacy-preserving Computing
Kai Chen , Qiang Yang
Index
More Information

Index

ABY, 78, 165
ABY^3, 34–35, 164, 180, 181
access structure, 16
activation function, 61
AEGIS, 106
algebraic structure
  group, 42
  lattice, 44
  ring, 43
AMD secure memory encryption, 111
AMD SEV, 106, 111–112
AND gate, 69, 71
application-specific integrated circuit, 187
ARM Cortex-A processor, 108
ARM Cortex-M processor, 109
ARM TrustZone, 107–109
ASIC, *see* application-specific integrated circuit
asymmetric encryption scheme, 37, 45, 64

BatchCrypt, 133–134
BGN scheme, *see* Boneh–Goh–Nissim encryption scheme
bloom filter, 221, 227, 229
Boneh–Goh–Nissim encryption scheme, 47–49
bootstrapping, 49, 50

CART, *see* classification and regression tree
central processing unit, 186
Cheon–Kim–Kim–Song encryption scheme, 38, 53–56, 214
Chinese remainder theorem, 23, 190
chosen ciphertext attack, 39
chosen plaintext attack, 39
circuit privacy, 41
CKKS, *see* Cheon–Kim–Kim–Song encryption scheme
classification and regression tree, 32
closest vector problem, 44
compactness, 40
Conclave, 172–178
convolutional layer, 61
CPU, *see* central processing unit
CryptDB, 158–164
CryptoNets, 60–61

database query, 172–178, 206–209
differential attack, 85
differential privacy, 8, 80–104, 220, 225
  advantages and disadvantages, 103–104
  application, 96–102
  definition, 82–89
  local, 88, 225, 228, 230
  mechanism, 89–93
  property, 93–96
    group privacy, 94
    parallel composition, 95
    post-processing, 93
    sequential composition, 95
differentially private stochastic gradient descent, 100–102, 134
DP, *see* differential privacy
DPSGD, *see* differentially private stochastic gradient descent

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-29951-0 — Privacy-preserving Computing
Kai Chen , Qiang Yang
Index
More Information

(ε, δ)-differential privacy, 87
(ε, δ)-local differential privacy, 88
ε-differential privacy, 86
empirical risk minimization, 98
enclave, 110, 111
entropy function, 17
exponential mechanism, 93

FATE, *see* federated AI technology enabler
FedAvg, *see* federated averaging
federated AI technology enabler, 151–158, 187, 200
federated averaging, 128–129
federated learning, 9, 121–149, 195, 205, 215
  accuracy, efficiency, and privacy tradeoff, 147
  application, 144–147
  cross-device, 122, 125
  cross-silo, 122, 126, 133
  decentralized, 149
  definition, 122–123
  FL-QSAR, 216
  horizontal, 29, 124, 126–134, 205
    and differential privacy, 134
    and homomorphic encryption, 133–134
    and secure aggregation, 131–133
    privacy, 129–134
  security, 126
  transfer, 122, 124
  vertical, 32, 122, 124, 134–139, 206
    linear regression, 137–139, 199
    privacy, 138
field programming gate array, 187
FL, *see* federated learning
FPGA, *see* field programming gate array
free XOR, 75

garbled circuit, 6, 69–79, 212
  advantages and disadvantages, 77
  applications, 77–79
  definition, 69–71
  efficiency, 185
  implementation, 71–77
    AND gate, 72
    general circuits, 73
    optimization, 74–77
    with oblivious transfer, 71
garbled circuits, 166
Gaussian distribution, 91
Gaussian elimination method, 26
Gaussian mechanism, 93
GBDT, *see* gradient boosting decision tree
GDPR, *see* General Data Protection Regulation
General Data Protection Regulation, 122
genome-wide association study, 210
GPU, *see* graphics processing unit
gradient boosting decision tree, 139
graphics processing unit, 186
GWAS, *see* genome-wide association study

hash function, 221, 227, 229
hash table, 153
HE, *see* homomorphic encryption
heterogeneous computing, 185
histogram counting, 97
homomorphic encryption, 8, 33, 36–62, 80, 133–134, 138, 142, 154, 161, 198
  advantages and disadvantages, 55–57
  applications, 57–62
  definition, 36–41
  efficiency, 184
  fully, 41, 49–52
  leveled, 41, 52–55
  partially, 41, 45–46
  somewhat, 41, 47–49
homomorphism
  additive, 26, 45, 46, 48, 175, 181
  multiplicative, 27, 45, 175
  strong, 40, 49

I.I.D., *see* independent and identically distributed
independent and identically distributed, 140
inference, 128, 136
instant randomized response, 228
Intel SGX, 106, 109–111, 166

join encryption, 161

L_1-sensitivity, 90
Lagrangian interpolation method, 22
Laplace distribution, 91
Laplace mechanism, 91, 230
lattice-based fully homomorphic encryption, 50–52
learning with error, 53
linear regression, 137, 215
LWE, *see* learning with error

MesaTEE, 164–171
moments accountant method, 102

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-29951-0 — Privacy-preserving Computing
Kai Chen , Qiang Yang
Index
More Information

MPC, *see* secure multiparty computation
multiplication triples, 67

noisy max, 98

oblivious transfer, 63–68, 71, 165
  1-out-of-k, 64, 65
  1-out-of-2, 63, 64
  correlated, 65
  definition, 63–64
  efficiency, 185
  implementation, 64–67
  random, 65
order-preserving encryption, 160

PaddleFL, 164
PaddlePaddle, 164
Paillier encryption scheme, 45–46, 154, 187, 189
parallelism, 186, 188
permanent randomized response, 228
Permute-and-Point, 75
Pivot algorithm, 32–34
pooling layer, 61
privacy-preserving computing, x–xii
  case studies, 194–232
  future opportunities, 12, 233–237
  history, 6–9
  platforms and cases, 11–12
  taxonomy, 3–6
privacy-preserving computing platform, 150–193
  efficiency, 184, 237
private set intersection, 135, 154, 195–198, 202
PrivPy, 178–183
public key encryption scheme, *see* asymmetric encryption scheme

query counting, 96

randomized response, 82–84, 90, 227
RAPPOR, 90, 227
residue class, 46
ring learning with error, 54
Rivest–Shamir–Adelman encryption scheme, 45, 154, 195
RSA scheme, *see* Rivest–Shamir–Adelman encryption scheme

SEAL, 56
secret sharing, 6, 13–35, 133, 154, 165, 181
  (t, n)-threshold scheme, *see* Shamir's scheme
  advantages and disadvantages, 29
  applications, 29–35
  arithmetic, 165
  based on Chinese remainder theorem, 23–24
  Blakley's scheme, 25–26
  Brickell's scheme, 24–25
  computational, 18
  definition, 16–19
  dynamic scheme, 21
  efficiency, 185
  general access structure, 20
  generalized self-shrinking sequence, 22
  homomorphism, 26–28
  multiresolution filtering, 21
  multisecret scheme, 20
  multispan scheme, 20
  quantum scheme, 21
  Shamir's scheme, 22–23, 27, 174
  statistical, 18
  threshold scheme, 19, 31, 133
  verifiable scheme, 21
  visual scheme, 21
secure aggregation, 30, 131–133
secure multiparty computation, x, 6, 34, 63, 79, 172, 212
semantic security, 39
semihonest, 130, 135, 180
shortest vector problem, 44
sparse vector technique, 93
Sun Tzu's theorem, *see* Chinese remainder theorem

TEE, *see* trusted execution environment
transfer learning, 139–140
trusted computation base, 106
trusted execution environment, 8, 105–120
  application, 116–120
  definition, 106
  implementation, 107–113
  vulnerability, 113–115

© in this web service Cambridge University Press & Assessment www.cambridge.org