INDEX OF TERMS

2013, 2
65537, 2
A5/0, 2
A5/1, 2
A5/2, 3
A5/3, 3
A5/4, 3
Adaptive attack, 3
AEAD (authenticated encryption with associated data) , 3
AES (Advanced Encryption Standard), 4
AES-CCM, 4
AES-GCM, 5
AES-GCM-SIV, 5
AES-NI, 5
AES-SIV, 6
AIM (Advanced INFOSEC Machine), 6
AKA, 6
AKS (Agrawal–Kayal–Saxena), 7
Algebraic cryptanalysis, 7
Alice, 7
All-or-nothing transform (AONT), 7
Anonymous signature, 8
Applied Cryptography, 8
Applied cryptography, 8
ARC4, 8
Argon2, 8
ARX (Add-Rotate-XOR), 9
ASIACRYPT, 9
Asymmetric cryptography, 9
Attack, 9
Attribute-based encryption (ABE), 10
Authenticated cipher, 11
Axolotl, 11
Backdoor, 11
Backtracking resistance, 11
Backward secrecy, 11
Base64, 12
BassOmatic, 12
BB84, 12
bcrypt, 12
Biclique cryptanalysis, 13
BIKE (Bit Flipping Key Encapsulation), 13
BIP (Bitcoin improvement proposal), 13
Bit Gold, 14
Bitcoin, 14
Black, 14
BLAKE, 14
BLAKE2, 14
BLAKE3, 14
Bleichenbacher attack, 15
Blind signature, 15
Block cipher, 16
Blockchain, 16
Blockcipher, 17
Blowfish, 17
BLS (Boneh-Lynn-Shacham) signature, 17
Bob, 18
Boolean function, 18
Boomerang attack, 18
BQP (bounded-error quantum polynomial time), 19
Braid group cryptography, 19
Brainpool curves, 19

Break-in recovery, 20
Broadcast encryption, 20
Brute-force attack, 20
Bulletproof, 20
Byzantine fault tolerance, 21
CAESAR, 21
Caesar’s cipher, 22
CAVP (Cryptographic Algorithm Validation Program), 22
CBC (cipher block chaining), 22
CECPQ (combined elliptic-curve and post-quantum), 22
Cellular automata, 22
Ceremony, 22
Certificate, 23
Certificate authority (CA), 23
Certificate transparency (CT), 23
ChaCha20, 23
CHES (Conference on Cryptographic Hardware and Embedded Systems), 24
CIA, 24
Ciphertext stealing, 24
Clipper, 25
CMVP (Cryptographic Module Validation Program), 25
Code-based cryptography, 25
Commitment, 25
Concurrent zero-knowledge, 26
Consensus protocol, 26
Control word, 26
COPACOBANA (Cost-Optimized PArallel COde Breaker), 26
Cothority (collective authority), 26
Cryptanalysis, 26
Cryptids, 27
Crypto, 27
CRYPTO, 27
Crypto AG, 27
Crypto period, 28
Crypto variable, 28
Crypto wars, 28
Cryptobiosis, 28
Cryptocurrency, 29
Crypto-Gram, 29
Cryptography, 29
Cryptologia, 29
Cryptology, 29
Cryptonomicon, 29
Cryptorchidism, 30
Cryptovirology, 30
CRYPTREC, 30
CSIDH (Commutative Supersingular Isogeny Diffie–Hellman), 30
CTF (capture the flag), 31
Cube attack, 31
Curve25519, 32
Curve448, 32
Cypher, 32
Daemon, 32
Davies–Meyer, 32
Decentralized private computation, 33
Déchiffrer, 33
Décrypter, 33
Deniable encryption, 33
DES (Data Encryption Standard), 33
Dictionary, 34
Dictionary attack, 34
Differential cryptanalysis, 34
Diffie–Hellman, 34
Disclosure, 35
Discrete logarithm problem, 35
Distinguisher, 35
Distributed randomness, 35
Dolev–Yao model, 36
Double ratchet, 36
Dragonfly, 36
DRBG (deterministic random bit generator), 37
DSA (Digital Signature Algorithm), 37
DSS (Digital Signature Standard), 37
DVB-CSA, 38
E0, 38
ECB (electronic codebook), 38
ECC, 38
ECDLP (Elliptic-curve discrete logarithm problem), 39
ECDSA (Elliptic-curve DSA), 39
ECIES (Elliptic-curve IES), 39
Ed25519, 40
EdDSA, 40

EKMS (Electronic Key Management System), 40
Electronic codebook, 41
ElGamal, 41
Elligator, 41
Elliptic curve, 41
Elliptic-curve cryptography, 42
Encipherment, 42
End-to-end encryption (E2EE), 42
Enigma, 43
Entropy, 43
ePrint, 44
Erathosthenes’ sieve, 44
eSTREAM, 44
Ethereum, 44
Eurocrypt, 45
Eve, 45
E-voting, 45
Factoring problem, 45
Feedback shift register, 46
Feistel network, 46
Fialka (Фиалка), 46
Fiat–Shamir, 46
FIPS 140-2, 47
FIPS 140-3, 47
Forgery, 48
Formal verification, 48
Format-preserving encryption, 48
Forward secrecy, 48
FOX, 49
FSE (Fast Software Encryption), 49
Fully homomorphic encryption, 49
Functional encryption, 49
Future secrecy, 50
Fuzzy extractor, 50
Generalized birthday problem, 50
GNFS (General Number Field Sieve), 51
GOST, 51
Grain, 51
Gröbner basis, 51
Group signature, 51
Grover’s algorithm, 52
Hardcore predicate, 52
Hash function, 52
Hash-based cryptography, 53
Heartbleed, 53
Hedged signature, 53
HFE (Hidden Field Equations), 54
HMAC (Hash-based MAC), 54
Homomorphic encryption, 54
HPC (Hasty Pudding Cipher), 54
HSM (hardware security module), 55
HTTP/3, 56
Hyperelliptic-curve cryptography, 56
IACR (International Association for Cryptologic Research), 56
IDEA (International Data Encryption Algorithm), 56
IDEA NXT, 57
Identity-based encryption, 57
IES (Integrated Encryption Scheme), 57
Impatient saboteur, 57
Impossibility, 57
Impossible differential attack, 57
IND-CCA, 58
IND-CPA, 58
Indelibility, 58
Indifferentiability, 58
Indistinguishability, 59
Indistinguishability obfuscation (iO), 59
Information-theoretic security, 59
INT-CTXT, 60
Invisible signature, 60
IOTA, 60
IPES (Improved Proposed Encryption Standard), 60
IPSec, 60
ISO standard, 61
Isogeny-based cryptography, 61
Journal of Cryptology (JoC), 61
KASUMI, 61
Keccak, 62
KeeLoq, 62
KEM (key encapsulation mechanism), 62
Kerberos, 62
Kerckhoffs’ principles, 63
Key derivation function (KDF), 64
Key escrow, 65

Key management, 66
Key wrapping, 66
Kleptography, 66
Known-key attack, 66
Kupyna (Купина), 66
Laconic zero-knowledge proof, 66
Lai–Massey, 67
Lamport signature, 67
Lattice-based cryptography, 68
Le Chiffre, 68
Leakage-resilient cryptography, 68
Learning with errors (LWE), 68
Length extension attack, 69
Length-preserving encryption, 69
LFSR (linear feedback shift register), 70
Lightweight cryptography, 70
Linear cryptanalysis, 70
Linkability, 70
LM hash, 70
Luby–Rackoff, 71
Lucifer, 71
MAC (message authentication code), 71
MAGENTA, 72
Malleability, 72
Manger attack, 72
Man-in-the-middle, 72
MASH (Modular Arithmetic Secure Hash), 73
McEliece encryption scheme, 73
MD4, 73
MD5, 73
MDC (Message Digest Cipher), 73
MDC-2 (Modification Detection Code 2), 73
Meet-in-the-middle, 73
Merkle puzzle, 74
Merkle tree, 74
Merkle–Damgård construction, 74
Mersenne twister, 74
Message franking, 75
Miller–Rabin, 75
MINERVA, 75
Mining, 75
Misuse resistance, 75
Mixnet, 76
MQV (Menezes–Qu–Vanstone), 77
Multicollision, 77
Multi-party computation (MPC), 77
Multivariate cryptography, 77
NBS (National Bureau of Standards), 77
NESSIE (New European Schemes for Signatures, Integrity, and Encryption), 78
"New Directions in Cryptography", 78
NFSR (nonlinear feedback shift register), 79
NIST (National Institute of Standards and Technology), 79
NIZK (non-interactive zero-knowledge), 80
Noekeon, 80
Noise, 80
Nonce, 80
Non-committing encryption, 81
Non-outsourceability, 81
Non-slanderability, 81
NSA (National Security Agency), 81
NT hash, 81
NTRU (*N*th degree Truncated polynomial Ring Units), 82
Null cipher, 82
OAEP (Optimal Asymmetric Encryption Padding), 82
Oblivious key management system (OKMS), 82
Oblivious PRF (OPRF), 83
Oblivious RAM (ORAM), 83
Oblivious transfer, 83
Obscurity, 83
OCB (offset codebook mode), 84
One-time pad, 84
One-way function, 84
Onion-AE, 84
OPAQUE, 84
OpenSSL, 85
Oracle, 85
OTR (Off-the-Record), 86
Padding oracle attack, 86
Paillier cryptosystem, 87

Pairing, 87
Pairing-based cryptography, 87
PAKE (password-authenticated key exchange), 88
Paradigm, 88
Password hash function, 88
PBKDF2 (Password-Based Key Derivation Function 2), 89
PCT (Private Communications Technology), 89
PEP (Plaintext equivalence proof), 89
Perfect forward secrecy, 89
Permutation-based cryptography, 90
PES (Proposed Encryption Standard), 91
PET (Plaintext equivalence test), 91
PFS, 91
PGP (Pretty Good Privacy), 91
Photuris, 91
Picnic, 92
PKC, 92
PKCS (Public Key Cryptography Standards), 92
Poly1305, 93
Polynomial complexity, 93
Post-compromise security, 93
Post-quantum cryptography, 93
Post-quantum RSA, 94
Prediction resistance, 94
Preimage, 94
PRESENT, 95
PRIMES, 95
Privacy-preserving, 96
Private information retrieval (PIR), 97
Proof of burn, 98
Proof of catalytic space, 98
Proof of human work, 98
Proof of replication, 98
Proof of reserve, 99
Proof of security, 99
Proof of sequential work, 99
Proof of space, 99
Proof of spacetime, 99
Proof of stake, 100
Proof of storage, 100
Proof of useful work, 100
Proof of work, 100
Provable security, 100
Provably secure, 100
Proxy re-encryption, 101
Pseudo-random, 101
Pseudorandom function (PRF), 101
Pseudorandom number generator (PRNG), 101
Pseudorandom permutation (PRP), 102
Public-key cryptography, 102
PUF (physically unclonable function), 102
Puncturable encryption, 102
Puncturable pseudorandom function (PPRF), 102
Quantum computer, 103
Quantum cryptography, 103
Quantum encryption, 103
Quantum key distribution, 103
Quantum signature, 103
QUIC (Quick UDP Internet Connections), 104
Rabin cryptosystem, 104
Rainbow tables, 104
Random bits, 104
Random oracle, 104
Randomness, 105
Range proof, 105
RC4, 105
RC5, 105
RC6, 106
Real world, 106
Real World Crypto (RWC), 106
Rectangle attack, 106
Related-key attack, 107
Research papers, 107
Revocation, 108
Rijndael, 108
Ring signature, 108
RIPEMD-160, 108
Rivest–Shamir–Adleman, 108
ROBOT (Return Of Bleichenbacher's Oracle Threat), 109
ROS, 109
RSA, 109

Rubber-hose cryptanalysis, 109
Rumba20, 109
SAEP (Simplified OAEP), 110
Salsa20, 110
Sandwich attack, 110
S-box, 110
Scalar, 111
sci.crypt, 111
Scrambler, 111
scrypt, 111
Searchable encryption, 111
secp256k1, 112
Secret sharing, 112
Security, 112
Security proof, 112
Semantic security, 112
Serious Cryptography, 113
Serpent, 113
SHA-0, 113
SHA-1, 113
SHA-2, 113
SHA-3, 113
SHA-3 competition, 114
SHACAL, 114
Shamir's secret database, 114
Shor's algorithm, 114
SHS (Secure Hash Standard), 115
Side channel, 115
Side-channel attack, 115
Sigaba, 115
Signal protocol, 116
Signature, 116
Signcryption, 117
SIKE (Supersingular Isogeny Key Encapsulation), 117
SIMECK, 117
SIMON, 117
SipHash, 117
SIV-AES, 117
Skipjack, 118
Slide attack, 118
SM, 119
Smart contract, 119
Snake-oil, 119
SNARK (succinct non-interactive argument of knowledge), 119
SNIP (secret-shared non-interactive proof), 120
SNOW 3G, 120
Solitaire, 121
SPECK, 121
SPEKE (Simple Password Exponential Key Exchange), 121
SPHINCS, 121
Sponge function, 121
SRP (Secure Remote Password), 122
SSH (Secure Shell), 122
SSL (Secure Socket Layer), 122
STARK (scalable transparent arguments of knowledge), 122
Steganography, 123
Stream cipher, 123
Substitution-permutation network (SPN), 123
Suck, 124
Sugar beet auctions, 124
Suite A, 124
SUPERCOP, 125
Superpolynomial complexity, 125
SVP (shortest vector problem), 125
Symmetric-key cryptography, 125
TCC, 126
Test vectors, 126
Threefish, 126
Threshold encryption, 126
Threshold secret-sharing, 126
Threshold signature, 127
Time AI, 127
Time-lock encryption, 127
Time-lock puzzle, 127
Timing attack, 128
TLS (Transport Layer Security), 128
Tor, 129
Traitor tracing, 129
Transfinite cryptography, 129
Trapdoor, 130
Triple DES, 130
Trivium, 131
True random number generator (TRNG), 131
Trusted third party, 131
Tweakable block cipher, 131

Twitter, 131
Twofish, 131
Undeniable signature, 132
Universal composability, 132
Universal hash function, 132
Updatable encryption, 133
Verifiable delay function (VDF), 133
Verifiable random function (VRF), 133
Verifiable unpredictable function (VUF), 134
Vigenère cipher, 134
VSH (Very Smooth Hash), 134
Wallet, 134
Watermarking, 134
White-box cryptography, 135
Winternitz signature, 135
WireGuard, 135
X25519, 136
X3DH, 136
XMSS (eXtended Merkle Signature Scheme), 137
XOF (extendable output function), 137
XOR, 137
XOR encryption, 137
Zerocash, 137
ZKP (zero-knowledge proof), 137
ZRTP, 138