

# Index

## A

Alternant code, [66](#), [84](#)  
Approximate lower triangular, [12](#), [43](#)

## B

Back substitution, [13](#)  
Barrel shift register, [27](#)  
Base-block, [45](#), [52](#)  
BCH code, [66](#)  
Belief propagation, [5](#), [11](#), [92](#)  
BF decoding threshold, [19](#), [94–97](#), [113](#)  
Binary block code, [5](#)  
Binary symmetric channel, [93](#)  
Birthday paradox, [75](#)  
Bit flipping algorithm, [18](#), [93](#)  
Blocks circulant matrix, [24](#)

## C

CCA2-secure conversion, [70](#), [81](#), [98](#), [111](#)  
CFS signature scheme, [84](#), [115](#)  
Check node, [9](#)  
Check node degree distribution, [10](#)  
Circulant matrix, [31](#), [32](#)  
Circulant permutation matrix, [36](#), [42](#)  
Circulants block matrix, [31](#), [42](#)  
Circulants row matrix, [37](#), [43](#), [61](#)  
Code dimension, [5](#)  
Code length, [5](#)  
Concatenated code, [67](#), [83](#)

## D

Decision threshold, [94](#)  
Decoding, [6](#)  
Decoding complexity, [20](#), [41](#), [62](#)

Decryption complexity, [111](#), [114](#)  
Difference family, [44](#), [46](#), [47](#)  
Digital signature, [81](#), [84](#), [115](#)  
Distinguisher, [81](#), [83](#), [85](#)  
Dual code, [99](#)

## E

Edge, [9](#)  
Edge degree distribution, [10](#)  
Edge perspective, [10](#)  
Encoding, [6](#)  
Encoding circuit, [26](#)  
Encoding complexity, [14](#), [37](#), [41](#)  
Encryption complexity, [111](#)  
Encryption rate, [70](#), [92](#)  
Extended difference family, [49](#), [50](#)

## F

Fast polynomial product, [38](#)

## G

Gallager algorithms, [18](#)  
Galois field, [5](#)  
Gaussian elimination, [13](#)  
Generalized birthday algorithm, [85](#)  
Generator matrix, [6](#), [9](#), [12](#), [24](#), [37](#), [68](#), [69](#), [74](#),  
[76](#)  
Gilbert bound, [24](#)  
Goppa code, [66](#), [68](#), [112](#)  
GPT cryptosystem, [84](#)  
GRS code, [66](#), [67](#), [69](#), [71](#), [83](#)

## H

Hamming distance, [6](#)

Hamming weight, **6**  
 Hash algorithm, **85**

## I

IND-CCA, **81**  
 IND-CPA, **81**  
 Information set, **73**  
 Information set decoding, **73**  
 Irreducible Goppa code, **67**  
 Irregular code, **9, 37**  
 Isomorphism between circulant matrices and polynomials, **33**

## K

KKS signature scheme, **84**

## L

LDGM codes, **12**  
 LDPC code, **5, 9**  
 Linear block code, **6**  
 Local cycle, **11, 44**  
 Local girth, **11**  
 Log-likelihood ratio, **16, 93**  
 Log-likelihood ratios sum-product algorithm, **15, 93**  
 Lower triangular form, **12, 43**

## M

McEliece cryptosystem, **65, 67, 91**  
 McEliece decryption, **68**  
 McEliece encryption, **68**  
 MDPC code, **61, 99**  
 MDS code, **73, 75, 83**  
 Min-sum algorithm, **15**  
 Minimum distance, **6, 8, 43**  
 Minimum weight, **6**  
 MRD code, **84**

## N

Niederreiter cryptosystem, **69**  
 Node degree, **9**  
 Node perspective, **10**

## O

One-way security, **81**  
 Orthogonal matrix, **36, 69, 98**  
 Orthogonal vectors, **102**  
 OW-CPA, **81**

## P

Parity bit, **7**  
 Parity-check equation, **7, 9**  
 Parity-check matrix, **8, 28, 37, 42, 67, 69**  
 Permutation matrix, **35**  
 Polynomial product, **38**  
 Private key, **67, 69**  
 Pseudo difference family, **48, 49**  
 Public key, **67, 68, 69, 98, 100**

## Q

QC-LDPC code, **41, 92, 113**  
 QC-MDPC code, **61, 96, 113**  
 Quasi-cyclic code, **13, 23, 41, 84**  
 Quasi-cyclic encoding circuit, **27**  
 Quasi-dyadic code, **84**

## R

Random difference family, **52**  
 Random oracle model, **82**  
 Redundancy, **7**  
 Regular code, **9, 44**  
 RSA system, **112**

## S

Security level, **72, 112, 114**  
 Stopping set, **13**  
 Support, **67**  
 Support splitting algorithm, **82**  
 Symmetric cryptosystem, **84**  
 Syndrome, **8**  
 Systematic code, **7, 9, 27, 29, 70, 82, 98, 99, 111**

## T

Tanner graph, **9**  
 Toom-Cook algorithm, **38**

## V

Variable node, **9**  
 Variable node degree distribution, **10**

## W

Waterfall, **95**  
 Winograd algorithm, **39**  
 Work factor, **72, 73, 75, 78, 104, 106, 112**

## Z

Zero divisor, **33, 35**