Contents

1 Introduction 1

2 Low-Density Parity-Check Codes 5
2.1 Linear Block Codes 5
2.2 Definition of LDPC Codes 9
2.3 LDPC Encoding 12
2.4 Encoding Complexity 14
2.5 Soft-Decision LDPC Decoding 15
2.5.1 Step 1: Initialization 16
2.5.2 Step 2: Left Semi-Iteration 17
2.5.3 Step 3: Right Semi-Iteration 17
2.5.4 Step 4: Decision 17
2.6 Hard-Decision LDPC Decoding 18
2.7 Decoding Complexity 19
References 20

3 Quasi-Cyclic Codes 23
3.1 Generator Matrix of a Quasi-Cyclic Code 24
3.2 Parity-Check Matrix of a Quasi-Cyclic Code 28
3.3 Alternative "Circulants Block" Form 31
3.4 Circulant Matrices and Polynomials 32
3.5 Circulant Permutation Matrices 35
3.6 A Family of QC Codes with Rate $(n_0 - 1)/n_0$ 37
3.7 Low Complexity Encoding of QC Codes 37
3.7.1 Fast Polynomial Product 38
3.7.2 Optimized Vector-Circulant Matrix Product 39
References 39

4 Quasi-Cyclic Low-Density Parity-Check Codes 41
4.1 Codes Based on "Circulants Block" Matrices 42
4.2 Codes Based on "Circulants Row" Matrices 43
4.2.1 Avoidance of Short Length Cycles 44
4.2.2 QC-LDPC Codes Based on Difference Families 46

4.2.3 QC-LDPC Codes Based on Pseudo Difference Families . . . 48
4.2.4 QC-LDPC Codes Based on Extended Difference Families . . . 49
4.2.5 QC-LDPC Codes Based on Random Difference Families . . . 52
4.3 QC-MDPC Codes . . . 61
References . . . 62

5 The McEliece and Niederreiter Cryptosystems . . . 65
5.1 Goppa Codes . . . 66
5.2 The McEliece Cryptosystem . . . 67
5.2.1 Encryption Algorithm . . . 68
5.2.2 Decryption Algorithm . . . 68
5.3 The Niederreiter Cryptosystem . . . 69
5.3.1 Peculiarities of the Niederreiter Cryptosystems . . . 70
5.3.2 Equivalence to the McEliece Cryptosystem . . . 70
5.4 Cryptanalysis of the McEliece and Niederreiter Cryptosystems . . . 71
5.4.1 Brute-Force Attacks . . . 72
5.4.2 Classical Information Set Decoding Attacks . . . 73
5.4.3 Modern Information Set Decoding Attacks . . . 75
5.4.4 Attacks Based on Equivalence Classes . . . 79
5.4.5 High Rate Goppa Codes Distinguisher . . . 80
5.4.6 Message Resend and Related Message Attacks . . . 81
5.4.7 Other Attacks . . . 82
5.5 Variants of the McEliece and Niederreiter Cryptosystems . . . 82
5.6 Code-Based Digital Signatures . . . 84
References . . . 86

6 QC-LDPC Code-Based Cryptosystems . . . 91
6.1 Error Correction Capability of LDPC Codes . . . 92
6.2 Permutation Equivalent Private and Public Codes . . . 96
6.3 Non-permutation Equivalent Private and Public Codes . . . 99
6.4 Attacks to LDPC Code-Based Cryptosystems . . . 101
6.4.1 Density Reduction Attacks . . . 101
6.4.2 Attacks to the Dual Code . . . 103
6.4.3 Information Set Decoding Attacks . . . 106
6.4.4 OTD Attacks . . . 108
6.4.5 Countering OTD Attacks . . . 110
6.5 Complexity . . . 111
6.6 System Examples . . . 112
6.7 Digital Signatures and Symmetric Cryptosystems . . . 114
References . . . 116

Index . . . 119

http://www.springer.com/978-3-319-02555-1

QC-LDPC Code-Based Cryptography

Baldi, M.

2014, XVI, 120 p. 15 illus., Softcover
ISBN: 978-3-319-02555-1