

Contents

Preface	xv
Abbreviations & Notations	xix
List of tables	xxi
List of figures	xxiii
Introduction	1
1 Preliminaries	5
1.1 Basics of quasigroups and loops	5
1.1.1 Morphisms	9
1.1.2 String transformations based on quasigroup	12
1.1.3 Quasigroup as a vector valued Boolean functions	15
1.2 Basics of coding theory	18
1.2.1 Some special types of error-correcting codes	21
1.3 Basics of cryptography	23
1.3.1 Multivariate equations and multivariate polynomials based digital signature scheme	25
2 Error-detecting codes based on T-quasigroup	29
2.1 General check digit system	31
2.2 Check equation using field \mathbb{F}_{p^n}	33
2.3 Check equation using group \mathbb{F}_p	39
2.4 Comparative analysis and applications	42
2.4.1 ISBN code	42
2.4.2 Check digit system to detect an ineligible cheque	43
2.4.3 Social security number	44
3 MDS codes based on orthogonality of quasigroups	47
3.1 Recursive derivatives and orthogonality of quasigroups	48

3.2	Orthogonal system of k -ary operations	50
3.3	MDS code	62
4	Symmetric encryption scheme based on quasigroup	67
4.1	Enumeration of Latin squares and a string transformation based on quasigroups	74
4.2	Symmetric encryption scheme based on quasigroup	77
4.2.1	Key generation process	77
4.2.2	Encryption process	77
4.2.3	Decryption process	79
4.3	Security analysis	81
4.3.1	Unbalanced Feistel transformation	82
4.3.2	Randomness testing	84
4.3.3	Avalanche criterion	84
4.4	Analysis of the scheme	88
5	Digital signature scheme based on multivariate quadratic quasigroups	91
5.1	Multivariate quadratic quasigroups over finite field	94
5.1.1	Existential unforgeability under chosen-message attack	96
5.2	Construction of central map using multivariate quadratic quasigroup	97
5.2.1	Generation of private-key	98
5.2.2	Generation of public-key	98
5.2.3	Signature scheme	100
5.3	Security analysis	102
5.3.1	Resistance against good-key attack	108
5.4	Operating characteristics	110
	Conclusion and future research directions	113
	Bibliography	117
	List of publications	129