Stream Ciphers and Number Theory

Thomas W. CUSICK

State University of New York at Buffalo

Cunsheng DING

The National University of Singapore

Ari RENVALL

University of Turku



1998

ELSEVIER

Amsterdam – Lausanne – New York – Oxford – Shannor



Contents

LI	rrelace			
1	Intr	oducti	ion	1
	1.1	Applie	cations of Number Theory	1
	1.2	An Ou	Itline of this Book	5
2	Stre	eam C	iphers 1	1
	2.1	Stream	n Cipher Systems	.1
		2.1.1	Additive Synchronous Stream Ciphers	.3
		2.1.2	Additive Self-Synchronous Stream Ciphers	4
		2.1.3	Nonadditive Synchronous Stream Ciphers	4
		2.1.4	Stream Ciphering with Block Ciphers	6
		2.1.5	Cooperatively Distributed Ciphering	8.
	2.2	Some		21
		2.2.1		22
		2.2.2		23
	2.3	Crypte	ographic Aspects of Sequences	25
		2.3.1	-	25
		2.3.2		29
		2.3.3	Correlation Functions	1
		2.3.4	Sphere Complexity and Linear Cryptanalysis 3	2
		2.3.5		5
	2.4	Harmo		6
	2.5			10
3	Pri	nes, P	rimitive Roots and Sequences 4	3
	3.1	Cyclot	tomic Polynomials	13
	3.2			4
	3.3		•	17
	3.4			60
	3.5		· · · · · · · · · · · · · · · · · · ·	55

X Contents

	3.6	Prime	s, Negord and Sequences	58
	3.7		Powers, Primitive Roots and Sequences	
	3.8		Products and Sequences	
		3.8.1	Binary Sequences and Primes	
		3.8.2	Ternary Sequences and Primes	
	3.9	On Cr	yptographic Primitive Roots	65
	3.10		Complexity of Sequences over Z_m	67
			and its Cryptographic Importance	75
4	Сус	lotomy	y and Cryptographic Functions	77
	4.1		tomic Numbers	77
	4.2	Cyclot	omy and Cryptography	
		4.2.1	Cyclotomy and Difference Parameters	
		4.2.2	Cyclotomy and the Differential Cryptanalysis	
		4.2.3	Cryptographic Cyclotomic Numbers	
	4.3		ographic Functions from Z_p to Z_d	
		4.3.1	The Case $d=2$	
		4.3.2	The Case $d=3$	85
		4.3.3	The Case $d = 4 \ldots \ldots \ldots \ldots \ldots$	86
		4.3.4	The Case $d = 5 \ldots \ldots \ldots \ldots \ldots$	87
		4.3.5	The Case $d = 6$	89
		4.3.6	The Case $d = 8 \ldots \ldots \ldots \ldots \ldots$	89
		4.3.7	The Case $d = 10 \ldots \ldots \ldots \ldots$	
		4.3.8	The Case $d = 12 \dots \dots \dots \dots$	
	4.4	Crypto	ographic Functions from Z_{pq} to Z_d	
		4.4.1	Whiteman's Generalized Cyclotomy and Cryptography .	
		4.4.2	Cryptographic Functions from Z_{pq} to $Z_2 \ldots \ldots$	
		4.4.3	Cryptographic Functions from Z_{pq} to Z_4	
	4.5	Crypto	ographic Functions from Z_{p^2} to Z_2	104
	4.6		ographic Functions Defined on $GF(p^m)$	
	4.7	The O	rigin of Cyclotomic Numbers	107
5	Spe		•	113
	5.1	Sophie	Germain Primes and Sequences	
		5.1.1	Their Importance in Stream Ciphers	
		5.1.2	Their Relations with Other Number-theoretic Problems	
		5.1.3	The Existence Problem	
		5.1.4	A Search for Cryptographic Sophie Germain Primes	
	5.2	Tcheb	ychef Primes and Sequences	
		5.2.1	Their Cryptographic Significance	
		5.2.2	Existence and Search Problem	118
	5.3		Primes of Form $k \times 2^n + 1$ and Sequences	
	5.4	Primes	s of Form $(a^n - 1)/(a - 1)$ and Sequences	123

Contents XI

		5.4.1 Mersenne Primes and Sequences					
		5.4.2 Cryptographic Primes of Form $((4u)^n - 1)/(4u - 1)$ 126					
		5.4.3 Prime Repunits and their Cryptographic Values 127					
	5.5	$n! \pm 1$ and $p# \pm 1$ Primes and Sequences					
	5.6	Twin Primes and Sequences over $GF(2)$ 129					
		5.6.1 The Significance of Twins and their Sexes 130					
		5.6.2 Cryptographic Twins and the Sex Distribution 131					
	5.7	Twin Primes and Sequences over $GF(3)$					
	5.8	Other Special Primes and Sequences					
	5.9	Prime Distributions and their Significance					
	5.10	Primes for Stream Ciphers and for RSA					
6	Diff	erence Sets and Cryptographic Functions 139					
	6.1	Rudiments of Difference Sets					
	6.2	Difference Sets and Autocorrelation Functions					
	6.3	Difference Sets and Nonlinearity					
	6.4	Difference Sets and Information Stability					
	6.5	Difference Sets and Linear Approximation					
	6.6	Almost Difference Sets					
	6.7	Almost Difference Sets and Autocorrelation Functions 153					
	6.8	Almost Difference Sets, Nonlinearity and Approximation 154					
	6.9	Summary					
7	Difference Sets and Sequences 157						
	7.1	The NSG Realization of Sequences					
	7.2	Differential Analysis of Sequences					
	7.3	Linear Complexity of DSC (ADSC) Sequences 161					
	7.4	Barker Sequences					
8	Bina	ary Cyclotomic Generators 167					
	8.1	Cyclotomic Generator of Order 2k					
	8.2	Two-Prime Generator of Order 2					
	8.3	Two-Prime Generator of Order 4					
	8.4	Prime-Square Generator					
	8.5	Implementation and Performance					
	8.6	A Summary of Binary Cyclotomic Generators					
9	Ana	alysis of Cyclotomic Generators of Order 2 199					
	9.1	Crosscorrelation Property					
	9.2	Decimation Property					
	9.3	Linear Complexity					
	9.4	Security against a Decision Tree Attack					
	0.5						

XII Contents

		9.5.1	Linear Complexity Analysis
		9.5.2	Balance Analysis
		9.5.3	Correlation Analysis
		9.5.4	Differential Analysis
10	Non	binary	Cyclotomic Generators 223
			h-Order Cyclotomic Generator
			Complexity
			prelation Property
			ation Property
			Behind the Cyclotomic Generators
11	Gen	erator	s Based on Permutations 231
	11.1	The C	ryptographic Idea
			tations on Finite Fields
	11.3	A Gen	erator Based on Inverse Permutations
	11.4	Binary	Generators and Permutations of $GF(2^n)$
		11.4.1	APN Permutations and their Properties
			Quadratic Permutations with Controllable Nonlinearity 241
			Permutations of Order 3
			APN Permutations of Order $n-1$
			Permutations of Order $n-2$
		11.4.6	Permutations X^d with $d = 2^m - 1 \dots 246$
		11.4.7	APN Permutations via Crosscorrelation Function 246
		11.4.8	Other Power Functions with Good Nonlinearity 251
			Choosing the Linear Functions
	11.5	_	Key Generators and their Problems 251
	•		Cyclic-Key Generators
			Several Specific Forms: An Overview 254
	11.6	A Gen	erator Based on Permutations of Z_m
12	-		Partitions and Cryptography 265
	12.1	Quadra	atic Partition and Cryptography 266
			$+y^2$ and $p = x^2 + 4y^2$
			$+2y^2$ and $p = x^2 + 3y^2$
			$+ ny^2$ and Quadratic Reciprocity
			$+7y^2$ and Quadratic Forms
			$+15y^2$ and Genus Theory
			$+ny^2$ and Class Field Theory
	12.8	Other	Cryptographic Quadratic Partitions 283

13 Group Characters and Cryptography 28	7
13.1 Group Characters	37
13.2 Field Characters and Cryptography	39
13.2.1 Field Multiplicative Characters: Most Used Ones 29	1
13.2.2 Field Additive Characters: Most Used Ones 29	13
13.3 The Nonlinearity of Characters	9
13.3.1 The Nonlinearity of Multiplicative Characters 29	9
13.3.2 The Nonlinearity of Additive Characters	O
13.4 Ring Characters and Cryptography	
13.5 Group Characters and Cyclotomic Numbers	
14 P-Adic Numbers, Class Numbers and Sequences 30	7
14.1 The 2-Adic Value and 2-Adic Expansion	7
14.2 A Fast Algorithm for the 2-Adic Expansion	
14.3 The Arithmetic of $Q_{[2]}$ and $Z_{[2]}$.3
14.4 Feedback Shift Registers with Carry	8
14.5 Analysis and Synthesis of FCSRs	
14.6 The 2-Adic Span and 2-RA Algorithm	
14.7 Some Properties of FCSR Sequences	
14.8 Blum-Blum-Shub Sequences & Class Numbers	
15 Prime Ciphering Algorithms 34	.7
15.1 Prime-32: A Description	17
15.2 Theoretical Results about Prime-32	2
15.3 Security Arguments	54
15.4 Performance of Prime-32	7
15.5 Prime-32 with a 192-Bit Key	7
15.6 Prime-64	7
16 Cryptographic Problems and Philosophies 35	9
16.1 Nonlinearity and Linearity	ç
16.2 Stability and Instability	
16.2.1 Stability and Diffusion	
16.2.2 Stability of Local Nonlinearities and Differences 36	
16.2.3 Correlation Stability and Pattern Stability 36	
16.2.4 Mutual Information Stability	
16.3 Localness and Globalness	
16.4 Goodness and Badness	
16.5 About Good plus Good	
16.6 About Good plus Bad	
16.7 About Bad plus Good	
16.8 Hardware and Software Model Complexity	73

Appendices 3			
More About Cyclotomic Numbers A.1 Cyclotomic Numbers of Order 7	. 377 . 378 . 378		
Cyclotomic Formulae of Orders 6, 8 and 10	383		
Finding Practical Primes	389		
List of Research Problems			
Exercises			
List of Mathematical Symbols			
Bibliography			
	More About Cyclotomic Numbers A.1 Cyclotomic Numbers of Order 7 A.2 Cyclotomic Numbers of Orders 9, 18 A.3 Cyclotomic Numbers of Order Eleven A.4 On Other Cyclotomic Numbers A.5 Behind Cyclotomic Numbers Cyclotomic Formulae of Orders 6, 8 and 10 Finding Practical Primes List of Research Problems Exercises List of Mathematical Symbols		

Contents

429

XIV

Index