

Table of Contents

1.	Introduction	1
2.	Stream Ciphers	5
2.1.	Theoretical versus Practical Security	8
2.2.	The Key Stream Generator	11
2.3.	The Synchronization (Problem) of Stream Ciphers	14
3.	Algebraic Tools	17
3.1.	Finite Fields and Polynomials	17
3.2.	Linear Feedback Shift Registers (LFSRs) and Sequences ..	24
3.3.	Minimal Polynomial and Traces	26
4.	Random Sequences and Linear Complexity	31
5.	Nonlinear Theory of Periodic Sequences	54
5.1.	Nonlinear Operations on Phases of a Sequence with Irreducible Minimal Polynomial	59
5.2.	Nonlinear Operations on Sequences with Distinct Minimal Polynomials	92
5.3.	Correlation-Immunity of Memoryless Combining Functions	114
5.4.	Summary and Conclusions	135
6.	Multiple Speed: An Additional Parameter in Secure Sequence Generation	142
6.1.	The Simulated Linear Feedback Shift Register	144
6.2.	A Random Number Generator Suggested by a Linear Cipher Problem	152
6.2.1.	The Random Sequence Generator	154
6.2.2.	Analysis of the Random Sequence Generator	155
6.2.3.	Extensions and Comments	161
7.	The Knapsack as a Nonlinear Function	163
7.1.	The Significance of the Knapsack for Secrecy Systems ..	165
7.2.	Addition is a Cryptographically Useful Function	182
7.3.	The Knapsack in $GF(2)$ -Arithmetic	188

8.	The Hard Knapsack Stream Cipher	192
8.1.	System Description	193
8.2.	Analysis of the Knapsack Stream Cipher	194
8.3.	Conclusions and Design Considerations	203
8.4.	Simulation Results of Small Scale Knapsack Stream Ciphers	204
9.	Nonlinear Combining Functions with Memory	209
9.1.	Correlation Immunity	209
9.2.	The Summation Principle	217
9.3.	Summary and Conclusions	227
	Literature References	231
	Glossary	237
	Index	241