

# Contents

1	<b>Introduction</b> .....	1
2	<b>Stream Ciphers</b> .....	5
2.1	Stream Cipher Systems Based on Exclusive-or Operation .....	7
2.2	Finite State Machines and Key Stream Generators .....	8
2.3	The Security of Stream Ciphers .....	10
3	<b>The BAA Attacks on Several Classes of Stream Ciphers</b> .....	13
3.1	Walsh Transforms and Their Properties .....	13
3.2	The Best Affine Approximation of Boolean Functions .....	15
3.3	The BAA Attacks on Two Classes of Stream Ciphers .....	17
4	<b>Measure Indexes on the Security of Stream Ciphers</b> .....	29
4.1	On Correlation-Immune Functions .....	30
4.1.1	From the Energy-Conservation Law and the BAA Attack Viewpoints .....	30
4.1.2	From the Necessity Viewpoint .....	33
4.1.3	From the Loss-and-Gain Viewpoint .....	35
4.2	The Cryptographic Merits and Demerits of Bent Functions .....	41
4.3	Weight Complexity (Sphere Surface Complexity) and Sphere Complexity .....	48
4.4	On the Security of Several Kinds of Key Stream Generators .....	53

4.5	On the Stability of Elementary Symmetric Boolean Functions .....	61
5	<b>The Stability of Linear Complexity of Sequences</b> .....	81
5.1	Linear Complexity and Sequences .....	82
5.1.1	Linear Complexity and Finite Sequences .....	82
5.1.2	Linear Complexity and Periodic Sequences .....	85
5.2	Weight Complexity and Lower Bounds for the Weight Complexity of Binary Sequences with Period $2^n$ .....	88
5.2.1	Weight Complexity $WC_1(s^\infty)$ and Lower Bounds on $WC_1(s^\infty)$ of Binary Sequences with Period $2^n$ .....	89
5.2.2	Weight Complexity $WC_2(s^\infty)$ and Lower Bounds on $WC_2(s^\infty)$ .....	95
5.2.3	Weight Complexity $WC_n(s^\infty)$ and Lower Bounds for $WC_n(s^\infty)$ .....	99
5.3	Lower Bounds on the Weight Complexity of Binary ML-Sequences .....	100
5.4	Lower Bounds on the Linear Complexity of Nonlinear Filtered ML-Sequences Derived from That of Weight Complexity .....	105
5.5	Lower Bounds on the Weight Complexity of Clock-Controlled Binary Sequences .....	108
5.6	A Lower Bound on the Linear Complexity of the Clock-Controlled and Nonlinear-Filtered Binary ML-Sequences .....	117
5.7	Another Approach to the Stability of Linear Complexity of Sequences .....	120
5.7.1	The Relationships Between Weight Complexity and Fixed-Complexity Distance as Well as Sphere Complexity and Variable-Complexity Distance .....	121
5.7.2	Bounds on the VCD of Binary Sequences with Period $2^n$ .....	125

6	<b>The Period Stability of Sequences</b> .....	130
6.1	General Results about Orders of Polynomials and Periods of Sequences .....	131
6.2	Measure Indexes for the Stability of Period and Their Relationships with Weight Complexity and Sphere Complexity .....	135
6.3	The Weight Period and the Autocorrelation Function of Binary Sequences .....	138
6.4	Bounds on the Weight Complexity $WP_k(s^\infty)$ for $1 \leq k \leq 2$ .....	139
6.5	The Period Stability of Binary Sequences with Period $2^n$ .....	143
7	<b>Summary and Open Problems</b> .....	146
7.1	Summary and Open Problems of the stability of Key Streams and Key Stream Generators .....	146
7.2	On the Stability of Source Coding for Binary Additive Stream Ciphers .....	153
<b>Appendices</b>		
A	<b>Massey's Conjectured Algorithm for the Linear Feedback Shift Register Synthesis of Multi-Sequences and Its Applications</b> .....	159
A.1	Massey's Conjectured Algorithm .....	159
A.2	Proof of Massey's Conjectured Algorithm .....	162
A.3	An Application of Massey's Algorithm to Cryptology .....	169
A.4	The Application of Massey's Algorithm to the Determination of Minimal Polynomials .....	172
B	<b>A Fast Algorithm for Determining the Linear Complexity of Sequences over <math>GF(p^m)</math> with Period <math>p^n</math></b> .....	176
<b>Bibliography</b> .....		180