Studies in Systems, Decision and Control

Volume 375

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

The series "Studies in Systems, Decision and Control" (SSDC) covers both new developments and advances, as well as the state of the art, in the various areas of broadly perceived systems, decision making and control–quickly, up to date and with a high quality. The intent is to cover the theory, applications, and perspectives on the state of the art and future developments relevant to systems, decision making, control, complex processes and related areas, as embedded in the fields of engineering, computer science, physics, economics, social and life sciences, as well as the paradigms and methodologies behind them. The series contains monographs, textbooks, lecture notes and edited volumes in systems, decision making and control spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

Indexed by SCOPUS, DBLP, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at https://link.springer.com/bookseries/13304

Alexandr Alexandrovich Kuznetsov ·
Oleksandr Volodymyrovych Potii ·
Nikolay Alexandrovich Poluyanenko ·
Yurii Ivanovich Gorbenko · Natalia Kryvinska

Stream Ciphers in Modern Real-time IT Systems

Analysis, Design and Comparative Studies

Springer

Alexandr Alexandrovich Kuznetsov
Department of Information
and Communication Systems Security
Faculty of Computer Science
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine

Nikolay Alexandrovich Poluyanenko
Department of Information
and Communication Systems Security
Faculty of Computer Science
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine

Natalia Kryvinska
Department of Information Systems
Faculty of Management
Comenius University
Bratislava, Slovakia

Oleksandr Volodymyrovych Potii
JSC Institute of Information Technology
Kharkiv, Ukraine

Yurii Ivanovich Gorbenko
Department of Information
and Communication Systems Security
Faculty of Computer Science
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine

ISSN 2198-4182 ISSN 2198-4190 (electronic)
Studies in Systems, Decision and Control
ISBN 978-3-030-79769-0 ISBN 978-3-030-79770-6 (eBook)
https://doi.org/10.1007/978-3-030-79770-6

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1 Introduction 1
References 9

2 Criteria and Indices Substantiation of the Stream Cryptoconversion Efficiency 13
2.1 Criteria and Indices of the Stream Cryptoconversions Stability 15
2.1.1 Indices Demonstrating the Parameters of Shift-Registers and of Take-Off Points for Non-Linear Functions and Feedbacks 15
2.1.2 Indices of Stability of Key Initialization Procedure 17
2.1.3 Indices of Stability of a Non-Linear Function (of Non-Linear Conversion Nodes) 18
2.1.4 General Stability Indices 27
2.2 Software and Hardware-Realization Indices 30
2.3 Constructive-Technological Indices 31
2.4 Generalization of Indices and Criteria of Stream Cryptoconversion 31
2.5 Conclusions and Recommendations 34
References 35

3 Analysis of Stream Cryptoconversion Principles 37
3.1 Basic Approaches to Construction and Analysis of SSC and BSC Stream Modes 37
3.2 Formalization of Stream Cryptoconversions by Their General Classification 40
3.3 Conclusions and Recommendations 43
References 44

4 Analysis of Synchronous Stream Cryptoconversions 47
4.1 General Classification of Synchronous Stream Cryptoconversions 47

4.2 Stream Encryption Methods Established on Use of Registers with Steady Motion . . . 47
4.2.1 Synchronous Stream Cryptoconversions with Steady Motion According to the Scheme of the Filter Generator . . . 49
4.2.2 Synchronous Stream Cryptoconversions with Steady Motion According to the Scheme of the Combination Generator . . . 50
4.3 Streaming Encryption Methods Established on the Use of Registers with Unsteady Motion . . . 52
4.3.1 Generator with Control Register “stop-and-go” . . . 52
4.3.2 Generator with Control Register “stop-and-go” with Alternation . . . 53
4.3.3 Two-Way stop-and-go Generator . . . 54
4.3.4 Cascade Generators with Control Registers (Holmann Cascades) . . . 54
4.3.5 Compressor Generator with Control Register . . . 55
4.3.6 Self-Priming Generator . . . 56
4.3.7 Self-Decimated Generator . . . 56
4.3.8 Multi-speed Generator with Internal Product (or with Internal Nonlinear Conversion) . . . 57
4.3.9 Majority Generator . . . 58
4.4 Conclusions and Recommendations . . . 63
References . . . 64

5 Analysis of Stream Modes for Block Symmetric Ciphers . . . 65
5.1 Electronic Codebook Mode—ECB . . . 65
5.1.1 General Parameters . . . 67
5.1.2 Introducing of Input and Output Data, Internal Modification State . . . 68
5.1.3 Enciphering . . . 69
5.1.4 Deciphering . . . 75
5.1.5 Forming of Cyclic Keys . . . 81
5.2 Counter Mode—CTR . . . 83
5.2.1 General Parameters . . . 85
5.2.2 Enciphering . . . 85
5.2.3 Deciphering . . . 85
5.3 Cipher Feedback Mode—CFB . . . 86
5.3.1 General Parameters . . . 89
5.3.2 Enciphering . . . 89
5.3.3 Deciphering . . . 89
5.4 Cipher Block Chaining—CBC . . . 90
5.4.1 General Parameters . . . 91
5.4.2 Enciphering . . . 92
5.4.3 Deciphering . . . 92

5.5 Output Feedback—OFB 92
5.5.1 General Parameters 95
5.5.2 Enciphering 95
5.5.3 Deciphering 96
5.6 Conclusions and Recommendations 96
References 98

6 Comparison of Stream Modes in Block Symmetric Ciphers 99
6.1 Statistical Researches of the BSC «Kalyna» 100
6.1.1 Statistical Researches of BSC «Kalyna» in the ECB-Mode 100
6.1.2 Statistical Researches of the BSC «Kalyna» in the CTR-Mode 103
6.1.3 Statistical Researches of the BSC «Kalyna» in the CFB-Mode 104
6.1.4 Statistical Researches of the BSC «Kalyna» in the CBC-Mode 104
6.1.5 Statistical Researches of the BSC «Kalyna» in the OFB-Mode 105
6.2 Statistical Researches of BSC AES (FIPS-197) and GOST 28147-89 (DSTU GOST 28147:2009) in Different Using Modes 105
6.3 Comparison of Statistical Security Indices of BSC 106
6.4 Substantiation of Recommendations Concerning BSC-Usage in Various Cryptographic Appliances 107
6.5 Conclusions and Recommendations 108
References 109

7 Analysis of Standardized Algorithms for Streaming Cryptographic Convention, Defined in ISO/IEC 18033-4 111
7.1 General Models of Stream Codes, Defined in ISO/IEC 18033-4 111
7.1.1 Models of Key Stream Generators 111
7.1.2 Output Function Models 112
7.2 Specialized Key Stream Generators 116
7.2.1 MUGI Key Stream Generator 116
7.2.2 *SNOW* 2.0 Key Stream Generator 121
7.2.3 Rabbit Streaming Code 127
7.2.4 *Decim* Key Stream Generator 136
7.2.5 Key Stream Generator *KCipher-2* 144
7.3 Fluid Code Security Levels with ISO/IEC 18033-4 158
7.4 Conclusions and Recommendations 159
References 162

8 Comparative Analysis of Determined Generators for Random Bits, Defined in the Nist Special Publication 800-90A 165

8.1 Analysis and Research of the Main Conversions in DGRB with Using of the Hashing Funcions 169

8.2 Analysis and Research of the Main Conversions in DGRB with Using of Symmetric Ciphering 170

8.3 Analysis and Researches of Main Conversions in DRGB, Based on Numeric-Theoretical Problems 174

8.4 Comparative DGRB-Researches, Defined in the Standard NIST Special Publication 800-90A 175

8.5 Conclusions and Recommendations 178

References 179

9 Analysis of Bitstreamed Cryptographic Conversion Algorithms from the International Project eSTREAM 181

9.1 Analysis of Software-Oriented Stream Ciphers, Recognized as Winners of the International Project eSTREAM 181

9.1.1 Stream Cipher HC-128 182

9.1.2 Stream Cipher Salsa20 186

9.1.3 Stream Cipher SOSEMANUK 195

9.2 Analysis of Hardware-Oriented Stream Ciphers, Recognised as Winners of the International Project eSTREAM 203

9.2.1 Stream Cipher *Grain* 203

9.2.2 Stream Cipher *MICKEY* 212

9.2.3 Stream Cipher *Trivium* 220

9.3 Stream Cipher *CryptMT* Version 3 226

9.3.1 Specification of the Cipher 226

9.3.2 *CryptMT* Cipher Security 235

9.3.3 Comparison of Productivity 237

9.4 Conclusions and Recommendations 238

References 239

10 Analysis of Stream Cryptographic Transfer Algorithms for Light (Less-Resource) Cryptographies Defined in ISO/IEC 29192 241

10.1 Stream Cipher Enocoro 241

10.1.1 Data Structure 241

10.1.2 The General Specification of *Enocoro V2* 244

10.1.3 *Enocoro-128v2* Stream Encryption Specification 247

10.1.4 Data Encryption Using *Enocoro-128v2* 248

10.1.5 Key Stream Statistics Tests 249

10.1.6 Attacks Based on a Compromise of Time-Memory-Data 250

10.1.7 Initialization Vector Recovery Attacks 253
10.1.8 The Maximum Degree of Monomials Test 256
10.2 *RC4* Stream Cipher 259
10.2.1 Specification of the Algorithm 260
10.2.2 *RS4* SSC Security 261
10.2.3 Realization 262
10.3 Conclusions and Recommendations 262
References 263

11 Comparative Research of Fluid Cryptographic Transformation Algorithms 265
11.1 Comparative Studies of Statistical Security of Stream Cryptographic Transformation Algorithms 265
11.1.1 Methods of Analysis of Passing Statistical Tests 268
11.1.2 NIST STS Statistical Test Package 269
11.1.3 Results of Experimental Studies of SSC Statistical Properties Using the NIST STS Statistical Testing Package 272
11.1.4 Characteristics of DIEHARD Statistical Tests 274
11.1.5 Results of Experimental Statistical Studies SSC Properties Using the DIEHARD Package 277
11.2 Comparative Researches of Computing Complexity of the FLOW-Cryptographic Transformation Algorithms 280
11.2.1 The Essence of the Method of Testing Speed Characteristics Stream Ciphers 280
11.2.2 Investigation of the Characteristics of Ciphers on Different Processors 281
11.3 Conclusions and Recommendations 291
References 292

12 Areas of Application for Nonlinear Shift Registers in PRS Generators 295
12.1 Key Issues During the Design of Streaming Encryption Algorithms 295
12.2 General Second-Order NLFSR Model 297
12.3 Research of the Basic Methods of Construction of NLFSR 299
12.3.1 De Bruijn’s Sequence 301
12.3.2 Algorithms for Generating De Bruijn Sequences 303
12.4 Problems of SPS Synthesis and Analysis on the Basis of NLFSR 305
12.5 Cryptographic Stability of NLFSR 307
12.5.1 System of Criteria and Indicators of Cryptographic Evaluation Stability of NLFSR 308
12.5.2 Unconditional Criteria of Cryptographic Stability 309
12.5.3 Conditional Criteria of Cryptographic Stability 310

12.5.4 Estimation of Cryptographic Stability of NLFSR as Filtering or Combining Function 312
12.6 Conclusions 314
References 314

13 Requirements for Feedback Coefficients, What Should the M-Nlfsr Respond to? 319
13.1 Requirements 1–4 319
13.1.1 Formulation and Substantiation of Requirements 1–4 319
13.1.2 Calculation of the Number of NLFSR that Meet the Requirements 1–4. Empirical Expression for the Calculation of M-NLFSR 326
13.1.3 Conclusions on the Application of Requirements 1–4 330
13.2 Requirements 5–6 331
13.2.1 Formulation and Substantiation of Requirements 5–6 331
13.2.2 Calculation of the Set of NLFSR that Do not Meet the Requirements 1–6 333
13.2.3 Quantitative Evaluation of the Obtained Results 334
13.3 Requirements 7–8 336
13.3.1 Formulation and Substantiation of Requirements 7–8 336
13.3.2 The Method of Calculating the Set of Combinations, that Do not Meet the Requirement 8 340
13.3.3 Inclusion and Exclusion Formula 342
13.3.4 Solve the Problem of Computing a Non-intersecting Set for Small Values of *L* 343
13.3.5 Calculating the Complete Set of Feedback Combinations that Do not Meet Requirement 8 354
13.4 Requirement 9 360
13.4.1 Description Requirements 9 360
13.4.2 Joint Application of Requirement 9 with Other Requirements 363
13.4.3 Quantitative Assessment of the Application of the Requirements 367
13.4.4 Conditions of the Zero Set Truncated by Requirement 9 368
13.4.5 Estimation of Spent Resources (RAM) 370
13.4.6 Estimation of Time Costs 372
13.4.7 Optimization of Pattern Construction 375
13.4.8 Conclusions on the Application of the Requirement 9 375

13.5 Conclusions 376

14 Method of Synthesis M-NLFSR. Hardware and Software Search M-NLFSR Second Order. List M-NLFSR 379

14.1 Development of Mathematical Apparatus Based on Solutions of the System of Linear Equations for Optimization of M-NLFSR Search 379

14.1.1 Restoration of NLFSR in a Known Sequence Using the SLAE Solution 379

14.1.2 Selection of Forming Sequences for Assembly of SLAE 381

14.1.3 Search M-NLFSR Using SLAE 384

14.2 Model with Simplified Formalized Description of Second-Order Nonlinear Feedback 385

14.2.1 Finding M-NLFSR for Large Registers 390

14.2.2 Search Results for M-NLFSR—List of M-NLFSR Dimension from $L = 19$ to $L = 25$ 390

14.3 Search for M-NLFSR with the Use of Hardware Implemented on FPGA 394

14.3.1 M-NLFSR Search Method 395

14.3.2 The Structure of the Hardware and Software 396

14.3.3 Implementation of NLFSR on FPGA 397

14.3.4 FPGA Performance 398

14.3.5 Search Results for M-NLFSR—List of M-NLFSR Dimension from L = 26 to L = 30 402

14.3.6 Conclusions on the Use of FPGA in the Search for M-NLFSR 405

14.4 Search for MRZNZZ with the Application of Parallel Calculation at GPU 406

14.4.1 Use of Parallel Computing Technologies in GPUs 406

14.4.2 GPU Application for Streaming Encryption Systems 409

14.4.3 GPU Application in the Second Stage of M-NLFSR Search Obtained M-NLFSR Dimension L = 31, 32 415

14.5 Conclusions 416

References 418

15 Research of Second-Order Properties of NLFSR. Comparative Analysis of M-NLFSR and M-LFSR 419

15.1 Assessment of Linear Complexity 419

15.2 Assessment of Quadratic Complexity 424

15.3 Estimation of the Amount of the Amount of Two or More Sequences Generated by M-NLFSR 425
15.4 Assessment of Linear and Quadratic Complexity Sum of Sequences 428
15.5 Analysis of the Applicability of Decimation and Properties of Group Addition to M-NLFSR 429
15.6 Study of Statistical Characteristics of prs, Which are Generated M-NLFSR 433
15.6.1 Setting up a Computational Experiment 433
15.6.2 Analysis of Results 435
15.7 Comparison of the Volume of the M-LFSR and M-NLFSR Ensembles for GF(2) and in Field Extensions GF(2^2) 437
15.8 Quantitative Calculation of the set of NLFSR Third and More High Order 442
15.9 Evaluation of M-NLFSR and M-LFSR Productivity in the Software Implementation of the Algorithm 446
15.10 Distribution of Number of Nonlinears Feedback in M-NLFSR 448
15.11 Research of NLFSR as a Filter or Combining Functions 449
15.11.1 Balance 450
15.11.2 The Presence of Prohibitions 450
15.11.3 Correlation Immunity 451
15.11.4 Nonlinearity 452
15.12 Cryptographic Resistance Assessment Model as a Basic Element of Current Symmetric Encryption Schemes. Comparisons by Developed Model of NLFSR and LFSR Assessments 458
15.13 Conclusions on Chap. 15 462
References 464

16 Stream Symmetric Cipher “Strumok” 467
16.1 Justification of the Mathematical Structure of the Cipher 467
16.1.1 Justification of General Requirements for the Key System Perspective Symmetric Stream Cipher for Post-Quantum Application 468
16.1.2 General Cipher Parameters 470
16.1.3 Substantiation of the Mathematical Structure of the Stream Symmetric Cipher “Strumok” 472
16.1.4 Init Internal State Initialization Function 474
16.1.5 Next State Function *Next* 475
16.1.6 Key Stream Function *Strm* 477
16.1.7 Function of Finite Automaton *FSM* 477
16.1.8 Nonlinear Substitution Function *T* 477
16.2 Substantiation of the Main Cryptographic Elements of the Stream Symmetric Cipher “STRUMOK” 479

16.2.1 Rationale for Fast Execution of Nonlinear Substitution Operation 479
16.2.2 Substantiation of Fast Execution of Multiplication Operation on α^{-1} in Arithmetic of Field GF (2^{64}) 482
16.2.3 Algorithm for Fast Execution of Multiplication Operation by α^{-1} in Arithmetic of the GF Field (2^{64}) 482
16.2.4 Substantiation of Fast Execution of Multiplication Operation by α^{-1} in Arithmetic of the GF Field (2^{64}) 483
16.2.5 Algorithm for Fast Execution of Multiplication Operation by α^{-1} in Arithmetic of Field GF(2^{64}) 484
16.3 Evaluation of «STRUMOK» Cipher Speed 485
16.3.1 Substantiation of the Method of Research of the Speed of Streaming Cryptoconversion 486
16.3.2 Comparative Studies of the Speed of Streaming Cryptoconversion 488
16.3.3 Comparison with AMD FX6300 SixCoreProcessor 3.50 GHz 502
16.4 Substantiation of Flow Characteristics Symmetric Encryption by Stability/Complexity Ratio 504
16.4.1 Estimate the Number of Operations and the Minimum Amount of Memory, Required for the Implementation of the Cipher "Strumok" 505
16.4.2 Substantiation of the Characteristics of the Cipher "Strumok" in Terms of Stability/Complexity 508
16.5 Conclusions in this Chapter 510
References 514

17 Conclusions 517
References 527

Appendix A 529

Appendix B 533

Appendix C 537

Appendix D 551

Appendix E 555

Symbols, Signs, Units, Abbreviations and Terms

AS	Automated system
ANF	Algebraic normal form
BSC	Block symmetric cipher
MT	Mersenne twister
GOST 28147	Standard encryption using BSC
PRSG	Pseudorandom sequence generator
DRBG	Deterministic random bit generator
IS	Information system
IT	Information technology
ITS	Information telecommunication system
«Кalyna»	Symbol for BSC, determined by State Standard of Ukraine 7624:2014
CIP	Cryptographic information protection
CI	Correlation immunity
CP	Cryptographic protocol
DC	Distribution criterion
M-sequence	Pseudorandom sequence, which is formed by LFSR or NLFSR, which has the maximum possible period at a given value of the register size and corresponds to the properties De Bruijn sequence
M-NLFSR	Nonlinear-feedback shift register, generating M-sequence
M-LFSR	Linear-feedback shift register, generating M-sequence
PRS	Pseudorandom sequence
PLIC	Programmable logic integrated circuit
De Bruijn sequence	De Bruijn sequence of element order from binary field $GF(2)$ is a sequence of the period, in which different L-processions appear only once
SSC	Symmetric stream cipher
SE	Stream encryption
SFMT	Simple fast Mersenne twister

LFSR	Linear-feedback shift register
NLFSR	Nonlinear-feedback shift register
NLFSR of the second order	NLFSR, in function of which's feedback the nonlinearity of second order only is used, i.e., the product amounts to not more as two tiles of the given register
NLFSR *r*-order	NLFSR, in function of which's feedback the nonlinearity of *r*-order is used, i.e., the product from *r* tiles of the given register
FA	Finite-state automaton
SBC	Symmetric block conversion
SLAE	System of linear algebraic equation
SAC	Strict avalanche criterion
SCC	Symmetric cryptographic conversion
SISC	System of information stream conversion
«Strumok»	Identification code of the stream cipher fixed by DSTU 8845:2019
LAT	Linear approximation table
DDT	Difference distribution table
AES	Advanced Encryption Standard
ASIC	Application-specific integrated circuit
CBC	Cipher block chaining (BSC application mode: cipher block chaining)
CCM	Counter with cipher block chaining message authentication code (BSC application mode: counter with cipher block chaining message authentication code)
CFB	Cipher feedback (BSC application mode: prohibition with feedback after the cipher text)
CMAC	Symmetric key block cipher-based message authentication code (BSC application mode: elaboration of a message authentication code)
CPU	Central processing unit (central processor)
CryptMT	Software-oriented stream cipher
CTR	Counter mode (BSC application mode: prohibition)
Decim	Bit stream cipher
DES	Data Encryption Standard
DIEHARD	Testing methodology for research of statistical security of contemporary cryptography algorithms
ECB	Electronic codebook (BSC application mode: simple substitution)
Enocoro	Hardware-oriented bit stream cipher
eSTREAM	International project for detection of new bit stream ciphers, usable for wide application, organized by European Union
FIPS-197	Deciphering standard with BSC usage
FPGA	Field-programmable gate array

FSM	Finite-state machine
GCM and GMAC	Galois/Counter Mode and Galois Message Authentication Code (BSC application mode: elaboration of a message authentication code with prohibition and without prohibition)
GPU	Graphics Processing Unit (graphic processor)
Grain	Hardware-oriented bit stream cipher
HC-128	Software-oriented bit stream cipher
KCipher-2	SSC, stream symmetric cipher
KW	Key wrapping (BSC application mode: key ciphering)
LEs	Logic elements (logic elements in FPLD (field-programmable logic device))
MICKEY	Hardware-oriented bit stream cipher
MUGI	Stream cipher
NESSIE	New European Schemes for Signatures, Integrity, and Encryption
NIST	National Institute of Standards and Technology
NIST STS	NIST Statistical Test Suite (modality of testing for research of statistical security of contemporary cryptoalgorithms)
OFB	Output feedback (BSC application mode: inhibition with feedback after enciphering keystream)
Permutation	Transposition
Rabbit	Bit stream cipher
RC4	Software-oriented bit stream cipher
RFID	Radio frequency identification
Salsa 20	Software-oriented bit stream cipher
ShiftBytes	Line shift modification
SNOW 2.0	Stream cipher
SOSEMANUK	Software-oriented bit stream cipher
SSL	Secure socket layer (cryptographic protocol, which ensures an establishing of a secure connection between client and server)
SubBytes	Modification of a substitution
Substitution	Substitution
TLS	Transport layer security (cryptographic protocol, which enables a secure data sending into Internet)
Trivium	Hardware-oriented bit stream cipher
WEP	Wired Equivalent Privacy (algorithm for assuring of Wi-Fi network security)
WPA	Wi-Fi Protected Access (security protocol for protection of wireless networks)
XTS	XOR encrypt XOR (XEX) tweakable block cipher (BSC application mode: index linked replacing)
$\oplus$	Operation of the logic exclusive OR (XOR)

&	Operation of the logic AND (AND)
¬	Operation of the logic negation (NOT)
>>	Right shift of indicated number of bits operator
<<	Left shift of indicated number of bits operator
>>>	Cyclic right shift of indicated number of bits operator
<<<	Cyclic left shift of indicated number of bits operator