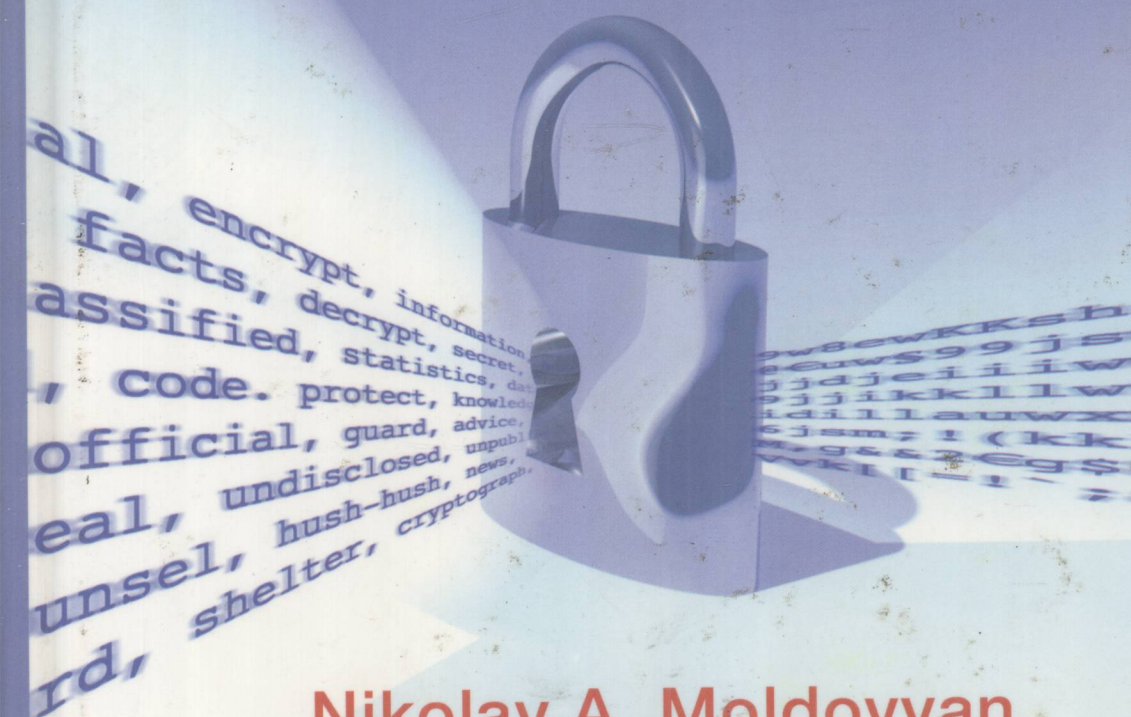


DATA-DRIVEN BLOCK CIPHERS FOR FAST TELECOMMUNICATION SYSTEMS



Nikolay A. Moldovyan
Alexander A. Moldovyan



Auerbach Publications
Taylor & Francis Group

TP309
M717

DATA-DRIVEN BLOCK CIPHERS FOR FAST TELECOMMUNICATION SYSTEMS



Nikolay A. Moldovyan
Alexander A. Moldovyan



E2008000808



Auerbach Publications

Taylor & Francis Group

New York London

CRC Press is an imprint of the

Taylor & Francis Group, an **informa** business

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2008 by Taylor & Francis Group, LLC
Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-5411-8 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC) 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Moldovyan, Nick.

Data-driven block ciphers for fast telecommunication systems / Nikolai
Moldovyan, Alexander A. Moldovyan.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-4200-5411-8 (hardback : alk. paper) 1. Computer security. 2.

Ciphers. 3. Cryptography. I. Moldovyan, Alex. II. Title.

QA76.9.A25M664 2007

005.8--dc22

2007031200

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the Auerbach Web site at
<http://www.auerbach-publications.com>

**DATA-DRIVEN BLOCK
CIPHERS FOR FAST
TELECOMMUNICATION
SYSTEMS**

OTHER TELECOMMUNICATIONS BOOKS FROM AUERBACH

Architecting the Telecommunication Evolution: Toward Converged Network Services

Vijay K. Gurbani and Xian-He Sun
ISBN: 0-8493-9567-4

Business Strategies for the Next-Generation Network

Nigel Seel
ISBN: 0-8493-8035-9

Chaos Applications in Telecommunications

Peter Stavroulakis
ISBN: 0-8493-3832-8

Context-Aware Pervasive Systems: Architectures for a New Breed of Applications

Seng Loke
ISBN: 0-8493-7255-0

Fundamentals of DSL Technology

Philip Golden, Herve Dedieu, Krista S Jacobsen
ISBN: 0-8493-1913-7

Introduction to Mobile Communications: Technology,, Services, Markets

Tony Wakefield, Dave McNally, David Bowler, Alan Mayne
ISBN: 1-4200-4653-5

IP Multimedia Subsystem: Service Infrastructure to Converge NGN, 3G and the Internet

Rebecca Copeland
ISBN: 0-8493-9250-0

MPLS for Metropolitan Area Networks

Nam-Kee Tan
ISBN: 0-8493-2212-X

Performance Modeling and Analysis of Bluetooth Networks: Polling, Scheduling, and Traffic Control

Jelena Mistic and Vojislav B Mistic
ISBN: 0-8493-3157-9

A Practical Guide to Content Delivery Networks

Gilbert Held
ISBN: 0-8493-3649-X

Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications

Yan Zhang, Honglin Hu, and Masayuki Fujise
ISBN: 0-8493-8036-7

Security in Distributed, Grid, Mobile, and Pervasive Computing

Yang Xiao
ISBN: 0-8493-7921-0

TCP Performance over UMTS-HSDPA Systems

Mohamad Assaad and Djamel Zeghlache
ISBN: 0-8493-6838-3

Testing Integrated QoS of VoIP: Packets to Perceptual Voice Quality

Vlatko Lipovac
ISBN: 0-8493-3521-3

The Handbook of Mobile Middleware

Paolo Bellavista and Antonio Corradi
ISBN: 0-8493-3833-6

Traffic Management in IP-Based Communications

Trinh Anh Tuan
ISBN: 0-8493-9577-1

Understanding Broadband over Power Line

Gilbert Held
ISBN: 0-8493-9846-0

Understanding IPTV

Gilbert Held
ISBN: 0-8493-7415-4

WiMAX: A Wireless Technology Revolution

G.S.V. Radha Krishna Rao, G. Radhamani
ISBN: 0-8493-7059-0

WiMAX: Taking Wireless to the MAX

Deepak Pareek
ISBN: 0-8493-7186-4

Wireless Mesh Networking: Architectures, Protocols and Standards

Yan Zhang, Jijun Luo and Honglin Hu
ISBN: 0-8493-7399-9

Wireless Mesh Networks

Gilbert Held
ISBN: 0-8493-2960-4

AUERBACH PUBLICATIONS

www.auerbach-publications.com

To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401

E-mail: orders@crcpress.com

Dedicated to the memory of our father,
Andrey Alexander Moldovyan(u),
who always supported us in our creative affairs.

Preface

Among different directions of applied cryptography, the cipher design based on the data-driven operations (DDOs) is, by comparison, poorly represented in the published and available literature. The RC5 and RC6 block ciphers based on data-dependent rotations (DDR) are well known, but many other DDO-based ciphers are known only to a small number of readers. The first application of the DDOs as a main cryptographic primitive relates to RC5 [56] and encryption algorithms based on data-dependent subkey selection [32]. The DDO are implemented with so-called controlled operation boxes (COBs), the most known type of which is represented by permutation networks (PNs). The PNs have been well studied in the field of telephone switching systems and parallel computations (1950–1980), see for example [4, 11, 68]. However, the first application of PNs in cryptalgorithm design relates to 1992 [53], where PNs have been applied to perform key-dependent bit permutations. Only about ten years later were the PNs used to perform data-dependent permutations. Dependence of the bit permutations on input data has imparted a new quality to PNs as a cryptographic primitives and solved some principal problems connected with key-dependent permutations. New applications of PNs have been requested to investigate new properties of PNs. In this area differential and linear characteristics of PNs have been studied and the notions of the PN order and switchable PNs have been introduced.

The next step of the development of the DDO-based cipher design relates to generalization of PNs connected with introducing the controlled substitution–permutation networks (CSPNs) constructed using the minimum size controlled elements. It has been shown that ciphers based on the PNs and CSPNs, implementing DDOs of different types, provide fast encryption and low implementation cost in hardware.

One can currently read papers devoted to different particular items on DDOs as a cryptographic primitive, however there is no published work introducing the DDO-based design as an individual section of the applied cryptography. Because the DDO-based ciphers represent an essential interest for application in the fast telecommunication systems and mobile networks, we have found that summarizing the known results in one book to be both reasonable and important.

In this book we present the most interesting results on the DDO boxes topologies, classification of the controlled elements, DDO-based ciphers, and fast software-oriented encryption algorithms using the data-driven subkey section as a main primitive. Prior to this book a major portion of these results have been available only in Russian literature.

Acknowledgments

We are grateful to the editorial board of *The Computer Science Journal of Moldova* for permission to use the material previously published in our papers. These include: 1994, volume 2, pp. 269–282; 2000, volume 8, pp. 270–283; 2003, volume 11, pp. 292–315; 2005, volume. 13, pp. 84–109; 2005, volume 13, pp. 268–291.

We also thank the co-authors of our papers and the authors of other papers, reports, and books cited for their contributions to the development of data-driven block ciphers, the subject of this book.

Introduction

Block data encryption is the most widely used cryptographic transformation in computer and telecommunication systems. The security of ciphers should be based on the secrecy of a small portion of information called a *key*. All other details of cryptosystems are considered as known elements. Moreover, ciphers should be secure against known and chosen text attacks as well as against different side channel attacks. If we mention encryption algorithm, then first of all we have in mind security requirements. Substitution-permutation and Feistel's networks represent conventional designs of block ciphers. Controlled operations have been unsuccessfully tried over a long term as the main cryptographic primitive in cipher design. Recently, they have been proposed to perform variable transformation, i.e., data-dependent (DD) operations (DDOs). This has given birth to a new direction in fast cryptography oriented to cheap hardware implementation. Such application of the controlled operations lead to designing the data-driven ciphers providing significant reduction of hardware implementation costs to relatively conventional designs. The implementation efficacy estimated using different comparison models increases by a factor up to 10 against AES candidates and other conventional ciphers. The data-driven ciphers are very attractive while embedding security mechanisms in constrained environments. Therefore, the data-driven ciphers are extremely interesting for usage to support the successful solution of security problems while deploying ad hoc and sensor networks.

Histories, different types, and topologies of the DDO boxes are considered in this book. Detailed attention is paid to design, properties, and application of the DD permutations (DDPs). Several DDP-based ciphers are considered concerning security and implementation items. Topologies of the controlled substitution-permutation networks (CSPNs) that are built up using small-size controlled elements (CEs) as standard building block are considered. The notion of the order of the CSPN is explained. The classification of CEs corresponding to different types is described. Reversible CSPNs representing a new cryptographic primitive and their designs are discussed. Application of the CSPNs as DDOs is illustrated by examples of several ciphers with 64- and 128-bit data block. A feature of the ciphers is the use of very simple key scheduling providing high performance in case of frequent change of keys.

About the Authors

Nikolay A. Moldovyan, Ph.D., is an honored inventor of the Russian Federation (2002), Prof. Doctor (2001), a chief researcher with the Specialized Center of Program Systems “SPECTR,” and a professor with the Saint Petersburg State Electrotechnical University. His research interests include computer security and cryptography. He has authored or co-authored more than 60 patents and 250 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981). He can be contacted at: nmold@cobra.ru.

Alexander A. Moldovyan, Ph.D., is a Prof. Doctor (2005), a director with the Specialized Center of Program Systems “SPECTR,” and a professor with the State University for Waterway Communications (Saint Petersburg, Russia). His research interests include information assurance, computer security, and applied cryptography. He has authored or co-authored more than 45 patents and 180 scientific articles, books, and reports. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (1996). He can be contacted at: ma@cobra.ru.

Abbreviations

AES	advanced encryption standard
ASIC	application specific integrated circuit
BF	Boolean function
BPI	bit permutation instruction
CBC	cipher block chaining
CE	controlled element
CFB	cipher-feedback
CLB	configurable logic block
COS	controlled operational substitution
CP	controlled permutation
CPB	controlled permutation box
CPI	controlled permutation instruction
CPU	central processing unit (processor)
CSPN	controlled substitution-permutation network
CTPO	controlled two-place operation
DC	differential characteristic
DCA	differential cryptanalysis
DDO	data-dependent operation (data-driven operation)
DDP	data-dependent permutation (data-driven permutation)
DDR	data-dependent rotation
DDSS	data-dependent subkey selection
DFA	differential fault analysis
DFF	D Flip-Flop
DSS	digital signature scheme
ECB	electronic codebook
FG	functional generator
FPGA	field programmable gate array
FT	final transformation
IV	initialization vector
LC	linear characteristic
LCA	linear cryptanalysis

LUA	loop unrolling architecture
MDA	microprocessor design architecture
MDC	manipulation detection code
MAC	message authentication code
NL	nonlinearity
OFB	output-feedback
PA	pipelined architecture
PN	permutation network
RAM	random access memory
RCO	reversible controlled operations
RDDO	reversible data-dependent (data-driven) operations
SCO	switchable controlled operation
SDDO	switchable data-dependent operation (data-driven operation)
SDDP	switchable data-driven permutation
SPN	switchable permutation network
TT	truth table
VBP	variable bit permutation
VLSI	very large scale integration

Notations Used in the Book

- $[x]$ denotes the integer part of x
- $\{0,1\}^g$ denotes the set of all binary vectors $U = (u_1, u_2, \dots, u_g)$, where $\forall i \in \{1, \dots, g\} \ u_i \in \{0,1\}$
- (X, Y) denotes concatenation of the vectors X and Y
- $X \oplus Y$ denotes the bitwise XOR (EXCLUSIVE-OR) operation of the two vectors X and Y ; $X, Y \in \{0,1\}^g$
- $X \ggg k$ or $X \ggg^k$ (or $X^{>k}$) denotes to-right rotation of the word X by k bits
- $X \lll k$ or $X \lll^k$ (or $X^{<k}$) denotes to-left cyclic rotation of the word $X = (x_1, \dots, x_{32})$ by k bits, i.e., $\forall i \in \{1, \dots, 32 - k\}$ we have $y_i = x_{i+k}$ and $\forall i \in \{33 - k, \dots, 32\}$ we have $y_i = x_{i+k-32}$.
- $\varphi(U)$ denotes Hamming weight of binary vector U ; $\varphi(U)$ is equal to the number of nonzero components of U , i.e., $\varphi(U) \stackrel{\text{def}}{=} \sum_{i=1}^g u_i$
- $X \otimes Y$ denotes bitwise AND operation of the two vectors X and Y ; $X, Y \in \{0,1\}^g$. For $c \in \{0,1\}$ and $X \in \{0,1\}^g$, we define $Y = cX$ where $y_i = cx_i \ \forall i \in \{1, \dots, g\}$
- \emptyset denotes a reserved two-place operation
- $\varphi'(U)$ denotes the parity of $\varphi(U)$, i.e., $\varphi'(U) \stackrel{\text{def}}{=} \varphi(U) \bmod 2$
- “ \leftarrow ” or “ $=$ ” denotes assign operation
- \bullet denotes the binary scalar product $c = A \bullet X = \varphi'(A \otimes X)$, $c \in \{0,1\}$
- $F_1 || F_2$ denotes the cascade of the F_1 and F_2 transformation boxes, i.e., $F_1 || F_2(X_1, X_2) = (F_1(X_1), F_2(X_2))$
- $F \circ S$ denotes superposition of F and S transformations
- “ $+_z$ ” denotes modulo 2^z addition of words (for example, the expression $j \leftarrow W \bmod 2^{11}$ is equivalent to the expression $j \leftarrow Z +_{11} 0$)
- “ $-_z$ ” denotes modulo 2^z subtraction
- $\langle Z \rangle$ denotes the average value of the variable Z
- $\#\{z_1, z_2, \dots\}$ denotes the number of elements in the set $\{z_1, z_2, \dots\}$
- $a|b$ denotes that number a divides number b

Contents

Preface.....	xi
Acknowledgments	xiii
Introduction.....	xv
About the Authors	xvii
Abbreviations	xix
Notations Used in the Book	xxi
1 Short Introduction to Cryptography.....	1
1.1 Symmetric Cryptosystems	1
1.1.1 Basic Notions	1
1.1.2 Additive Ciphers.....	5
1.1.3 Application in Telecommunications and Computer Systems.....	8
1.1.4 Block Ciphers.....	12
1.1.5 Controlled Operations as a Cryptographic Primitive.....	21
1.1.6 Construction Scheme Variants of Iterated Ciphers Based on Data-Dependent Operations	26
2 Permutation Networks as Primitive of Data-Driven Ciphers.....	31
2.1 Design of the Permutation Networks.....	31
2.2 Linear Characteristics of the Controlled Permutations	37
2.3 Differential Characteristics	40
2.4 Cobra-H64: A 64-Bit Block Cipher Based on Variable Permutations.....	46
2.4.1 Specification of the Encryption Algorithm.....	46
2.4.1 Security Estimation.....	53
2.5 DDP-64: Pure DDP-Based Cipher	57
2.5.1 Description of the Encryption Algorithm	59
2.5.2 Security Estimation.....	62
2.6 Conclusions	67

3	Data-Driven Primitives and Ciphers Based on Controlled Substitution–Permutation Networks	69
3.1	Advanced DDP-Like Primitives and Their Classification	70
3.1.1	Elementary Controlled Substitutions	70
3.1.2	Classification of the $F_{2/1}$ Boxes	72
3.1.3	Subset of the $U_{2/1}$ Boxes with One Linear Output	74
3.2	Controlled Elements Suitable to Field Programmable Gate Array (FPGA) Implementation	77
3.3	Symmetric Topologies	83
3.4	Properties of the CSPNs Based on Elements $F_{2/1}$ and $F_{2/2}$	89
3.4.1	Nonlinearity and Avalanche Properties of the DDP-Like Boxes	90
3.4.2	Using the Generating Functions	92
3.5	Data-Driven Ciphers Based on CSPNs	96
3.5.1	Block Cipher Eagle-128	96
3.5.2	DDO-64: A DDO-Based Cipher with 64-Bit Data Block	100
3.5.3	Updating the Known DDP-Based Ciphers	103
3.6	Conclusions	105
4	Switchable Data-Dependent Operations	107
4.1	Representation of the CP Boxes as a Set of Pairs of Mutually Inverse Modifications	107
4.1.1	Topologies of the First Order	107
4.1.2	Topologies of the Higher Orders	112
4.2	Reversible DDO Boxes	115
4.2.1	SDDO Boxes with Symmetric Topology	118
4.2.2	Hardware Efficient SDDOs	119
4.2.3	General Design of the SDDO Boxes of Different Orders	120
4.2.4	The RCO Design Based on CE with Mutual Inverse Modifications	123
4.3	Block Ciphers with Switchable DDOs	126
4.3.1	Updating the DDP-Based Block Ciphers	126
4.3.2	Hawk-64: A Cipher Based on Switchable Data-Driven Operations	129
4.4	Designs of the Bit Permutation Instruction for General Purpose Processors	133
4.4.1	Design of the BPI for Cryptographic Applications	135
4.4.2	Design of the BPI for Non-Cryptographic Applications	136
4.4.3	Architecture of the Universal BPI	139

4.5	Hardware Implementation Estimation of the Data-Driven Ciphers	141
4.5.1	Hardware Implementation Approaches and Architectures	141
4.5.2	Hardware Implementations of the DDP-Based Ciphers	144
4.5.3	Hardware Implementations of the DDO-Based Ciphers	144
4.5.4	Hardware Implementation Estimations of the Ciphers Based on Switchable DDOs	147
4.5.5	Hardware Implementation Efficacy Comparison	148
4.6	On-Fly Expansion of the Secret Key	152
4.7	Conclusions	155
5	Data-Driven Ciphers Suitable for Software Implementation	157
5.1	A Class of Ciphers Based on Data-Dependent Subkey Selection	157
5.2	Flexible Software Encryption Systems	160
5.3	Examples of Algorithm Realization	161
5.3.1	Flexible 128-Bit Cipher ($d = \delta = 8; b = 32; w = 4$)	161
5.3.2	The DDSS-Based Cipher with 64-Bit Input Data Block ($d = \delta = 8; b = 32; w = 2$)	162
5.3.3	The DDSS-Based Cipher with 128-Bit Input Data Block ($d = \delta = 8; b = 32; w = 4$)	163
5.4	General Characterization of the DDSS-Based Algorithms	163
5.5	Advanced DDSS-Based Ciphers	165
5.5.1	Algorithm 1: DDSS-Based Cipher with Fixed Operations	166
5.5.2	Algorithm 2: Flexible Advanced DDSS-Based Cipher	167
5.6	A Model for Security Estimation	168
5.7	A DDSS-Based Cipher with Flexible Input Data Block Size	170
5.7.1	Design Criteria	171
5.7.2	Local Notations	171
5.7.3	Transformation Algorithms	172
5.8	Conclusions	175
	References	177
	Index	183