

**DESIGN AND IMPLEMENTATION
OF
REORDERED NORMAL BASIS
FINITE FIELD MULTIPLIER
USING
NP DOMINO LOGIC**

DR. K. RAGINI

Professor

Department of Computer Science & Engineering
G. Narayanamma Institute of Technology and
Science (For women), Hyderabad, Telangana, IN

DESIGN AND IMPLEMENTATION OF REORDERED NORMAL BASIS FINITE FIELD MULTIPLIER USING NP DOMINO LOGIC

Copyright© : Dr. K. Ragini
Publishing Rights© : VSRD Academic Publishing
A Division of Visual Soft India Pvt. Ltd.

ISBN-13: 978-93-91462-71-0
FIRST EDITION, JULY 2023, INDIA

Printed & Published by:
VSRD Academic Publishing
(A Division of Visual Soft India Pvt. Ltd.)

Disclaimer: The author(s) / Editor(s) are solely responsible for the contents compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Author(s) or Editor(s) or Publishers to avoid discrepancies in future.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Publishers & Author.

Printed & Bound in India

VSRD ACADEMIC PUBLISHING
A Division of Visual Soft India Pvt. Ltd.

REGISTERED OFFICE

154, Tezab mill Campus, Anwarganj, KANPUR–208003 (UP) (IN)
Mb:9899936803, Web: www.vsrdpublishing.com, Email: vsrdpublishing@gmail.com

MARKETING OFFICE

340, FF, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI–400053 (MH) (IN)
Mb:9956127040, Web: www.vsrdpublishing.com, Email: vsrdpublishing@gmail.com

PREFACE

Finite field arithmetic circuits are a core part for implementing some cryptographic systems and Reed-Solomon codes. For efficient hardware implementation of finite field arithmetic units, the use of a normal basis is advantageous. A high-speed power-efficient VLSI implementation of a finite field multiplier in Galois Field (2^m) is proposed. In this book, a Reordered Normal Basis (RNB) finite field multiplier is implemented using NP domino logic. This multiplier uses RNB, which is the type-II Optimal Normal Basis (ONB), to perform multiplication. The Critical Path Delay (CPD) is influenced by the XOR-AND-XOR (XAX) module of the Serial-In Parallel-Out (SIPO) RNB multiplier. Hence, this block is designed in various logic styles, including static CMOS logic, pseudo NMOS logic, domino keeper logic, and NP domino logic. Both the 5-bit and 11-bit SIPO multipliers are designed using these logic styles. The Mentor Graphics tool is used to design the multiplier using the full-custom design. The 45nm technology is used in the Mentor Graphics tool. The major goal is to determine the optimum logic style that meets the VLSI optimisation requirements like the area, multiplication delay, CPD, power dissipation, Area-Delay Product (APD), and Power-Delay Product (PDP). When compared to other logic styles, the delay and area of the multiplier employing NP domino logic are lower, whereas the power dissipation is similar to other domino logic styles. Also, the architectures of Serial-In Serial-Out (SISO), Parallel-In Serial-Out (PISO), SIPO, and Parallel-In Parallel-Out (PIPO) multipliers were implemented to analyse their efficiencies in terms of design parameters.

 Author

CONTENTS

CHAPTER 1: INTRODUCTION	1
1.1. INTRODUCTION.....	1
1.2. OBJECTIVES	2
1.3. REQUIREMENTS	3
1.4. FORMULATION OF THE PROBLEM	3
1.5. LITERATURE SURVEY	4
1.6. ORGANIZATION OF WORK.....	5
1.7. CONCLUSION.....	6
CHAPTER 2: RNB MULTIPLICATION PROCESS	7
2.1. INTRODUCTION.....	7
2.2. MULTIPLICATION OVER GF (25)	8
2.3. MULTIPLICATION OVER GF (211).....	10
2.4. CONCLUSION.....	13
CHAPTER 3: DIFFERENT LOGIC STYLES USED TO IMPLEMENT XAX MODULE	14
3.1. STATIC DESIGN STYLE	15
3.2. DYNAMIC DESIGN STYLE.....	18
3.3. CONCLUSION.....	21
CHAPTER 4: CLASSIFICATION OF REORDERED NORMAL BASIS MULTIPLIERS USING VARIOUS LOGIC STYLES.....	23
4.1. CLASSIFICATION OF MULTIPLIERS.....	23

4.2.	SERIAL-IN PARALLEL-OUT RNB MULTIPLIER.....	24
4.3.	PARALLEL-IN PARALLEL-OUT RNB MULTIPLIER	52
4.4.	SERIAL-IN SERIAL-OUT RNB MULTIPLIER.....	59
4.5.	PARALLEL-IN SERIAL-OUT RNB MULTIPLIER.....	62
4.6.	CONCLUSION.....	64

CHAPTER 5: MENTOR GRAPHICS TOOL 65

5.1.	STEPS TO CREATE SCHEMATIC IN TANNER EDA TOOL.....	65
5.2.	STEPS TO CREATE SYMBOL IN TANNER EDA TOOL.....	72
5.3.	STEPS TO CREATE TEST BENCH IN TANNER EDA TOOL	72

CHAPTER 6: RESULTS AND DISCUSSIONS..... 79

6.1.	5-BIT SISO RNB MULTIPLIER	80
6.2.	5-BIT PISO RNB MULTIPLIER	81
6.3.	5-BIT SIPO RNB MULTIPLIER	82
6.4.	5-BIT PIPO RNB MULTIPLIER.....	86
6.5.	11-BIT SIPO RNB MULTIPLIER	90
6.6.	COMPARISON OF DESIGN PARAMETERS OF 5-BIT RNB MULTIPLIERS	96
6.7.	COMPARISON OF DESIGN PARAMETERS OF 11-BIT RNB MULTIPLIERS	99

CHAPTER 7: CONCLUSIONS..... 100

CHAPTER 8: REFERENCES..... 101