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

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.*)

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