IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 2, July 2022

Design of Low Power Versatile Bit-Serial Multiplier in Finite Field GF (2^m)

Niveditha SR[1], Brunda BS[2], Rohith K[3], Nithyashree R[4], Mrs. Asha R[5]

Students, Department of Electronics and Communication Engineering[1,2,3,4]

Faculty, Department of Electronics and Communication Engineering[5]

Vidya Vikas Institute of Engineering & Technology, Mysuru, Karnataka, India

Abstract: *Finite field arithmetic is the most important component in applications like cryptography, computer algebra and error correcting codes. Versatility is an important property the hardware industry lacks and trying to establish as much as possible. To survive in this booming technological word, the new designs should be of an adjustable one, which processes the versatile property. In this we have proposed an efficient VLSI design for versatile bit-serial multiplier in finite fields GF (2m). The versatile multiplier designed here modifications done by reducing the unwanted switching activity removed by clock gating scheme. Our design provides a solution to the power reduction. The introduced multiplier operates over a variety of binary fields up to an order of 2m. The value of m can vary up to 264 bits. Multiplier is designed using Verilog HDL.*

Keywords: Low power, Versatile, Bit-serial multiplier, Finite field, Galois field

REFERENCES

[1]. El Hadj Youssef Wajih, Guitouni Zied, Machhout Mohsen & Tourki Rached, "Design and Implementation of Elliptic Curve Point Multiplication Processor over GF (2m)", Electronics and Micro-Electronic Laboratory (LEME), Monastir, Tunisia Monastir, 5000, Tunisia, 2018

[2]. Lakshmi Boppanna, "Design and Implementation of a Sequential Polynomial Basis Multiplier over GF(2m)"- Department of Electronics and Communication Engineering, National Institute of Technology-Warangal Warangal, Telangana, 2017

[3]. Sudha Ellison Mathe, "Low-Power and Low-Hardware Bit-Parallel Polynomial Basis Systolic Multiplier over GF(2m) for Irreducible Polynomials"- ETRI Journal, 2017

[4]. Hayssam El- Razouk and Arash Reyhani-Masoleh, "New Bit-Level Serial GF (2m) Multiplication Using Polynomial Basis", Department of Electrical and Computer Engineering Western University London, Canada, 2015

[5]. Lejla Batina, Nele Mentens, Sıddıka Berna Ors, Bart Preneel Katholieke Universiteit Leuven, "Serial Multiplier Architectures over GF(2n) for Elliptic Curve Cryptosystems", ESAT/SCD-COSIC Kasteelpark Arenberg 10 B-3001 Leuven-Heverlee, Belgium Lejl, 2014

[6]. Riddhish Shukla, Kulin Shah, Raj Chaurasia, Sivanatham S, "Study of Bit-Serial Multiplier in Finite Fields GF (2m)", National Conference on Innovative Trends in Science andEngineering (NC-ITSE'16),2014

[7]. Jeng-Shyang Pan, Reza Azarderakhsh, Mehran Mozaffari Kermani, Chiou-Yng Lee, Wen-Yo Lee, Che Wun Chiou, "Low-Latency Digit-Serial Systolic Double Basis Multiplier over GF(2m) Using Sub quadratic, MAY 2014

[8]. I Grasschadi, "A Low power Bit-Serial multiplier for finite field GF(2m)"- Graz University of Technology Institute for Applied Information Processing and Communications Inffeldgasse 16a, A–8010 Graz, Austria,2010

[9]. P. Kitsos,G. Theodoridis, O. Koufopavlou, "An efficient reconfigurable multiplier architecture for Galois field GF(2m)"- VLSI Design Laboratory, Department of Electrical and Computer Engineering, University of Patras, Rio, Patras 26500, Greece,2003

DOI: 10.48175/IJARSCT-5848