IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 4, Issue 1, August 2015)

Polynomial Based Mastrovito Multipliers for FFT Applications for Secure Data Encryption and Decryption

Swarnim Baghel
M. Tech Scholar
Department of Electronics and Communication
Gyan Ganga Institute of Technology and Science,
Jabalpur (M.P.), INDIA
RGPV University, Bhopal (M.P.)
swarnim.baghel@gmail.com

Sunil Shah
Asst. Professor
Department of Electronics and Communication
Gyan Ganga Institute of Technology and Science,
Jabalpur (M.P.), INDIA
RGPV University, Bhopal (M.P.)
sunilshah@ggits.org

Abstract- **At present scenario Polynomial groundwork multipliers re used for the reason that they're fairly simple to design, and offer scalability for the fields of bigger orders. It's used in Cryptographic and FFT purposes for at ease knowledge encryption and decryption which deals with discrete constitution and mathematical arithmetic. In view that it makes use of modular arithmetic operation, it's observed that it has the latency of m cycles. To beat this problem, an effective low latency polynomial multiplier for speedy Fourier transform (FFT) algorithm which is based on Mastrovito structure has been developed. This multiplier makes use of the notion of parallel processing in which multiplication is decomposed into number of impartial models and "pre-computed addition" systems. Our design has been implemented in VHDL, simulated and synthesized utilizing the Xilinx ISE Design Suite 13.2 device for supply voltage levels from 1.2V to 2.5 V. The multiplier is analyzed in terms of pace, subject overhead and reminiscence. The design includes significantly less prolong and field overhead complexities than the present structure.**

Keywords: **FFT, Mastrovito, VHDL, Polynomial basis.**