Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

THREE OPERAND BINARY ADDER OF LOW POWER AND HIGH SPEED VLSI ARCHITECTURE

ASHA CN,
Dept. of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore

JAYALAXMI H,
Dept. of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore

SAPNA KUMARI C,
Dept. of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology, Bangalore

NAGAPUSHPHA KP
Dept. of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore

Abstract

Addition is one of the most vital and initial operations among all arithmetic operations and is utilized in many of the mathematical equations. In digital world, the addition operation can be performed by several adders. These adders produce carries with preferred power and delay. One of the most basic functional units for performing modular arithmetic in different cryptography and PRBG (pseudorandom bit generator) algorithms is Three-operand binary adder. Because of ripple-carry stage, the Carry save three-operand Adder (CS3A) has long propagation delay. In addition, a parallel prefix two-operand adder (PP2A) like HCA (Han-Carlson) is used in the addition of three-operands. Hence new higher speed and less power adder architecture is presented in this paper using the pre-computing bitwise addition follow by carry-prefix computation logic for performing binary addition of three operands that can consume less power and low area and adder delay is drastically reduced to O(log2 n). The ISE Xilinx 14.7 software is used for simulation and synthesizing these processes. The simulation results of presented adder will represent that it will have less power dissipation, lesser area and less delay compared to CS3A adder. More over the presented adder will achieve least PDP (power-delay-product) and ADP(area-delay-product) than previous three-operand adder methods.

Keywords: Carry Save Adder (CSA), Three-operand binary adder, VLSI architecture, Han-Carlson adder (HCA), low power, and high speed.

I. INTRODUCTION

In arithmetic operations, one of the most essential components is Adders. In digital circuits, binary adders are utilized in subtraction, addition and Floating point consequently, the adders become as fundamental elements, however optimization of their tasks is the most tough task in digital architectures. The computer arithmetic algorithms have been developed n-bit adders delay and lower limits on area; generally the former can differ linearly with the size of adder and the latter has an O (log2 (n)) behaviour. The implementation of cryptography algorithms on the hardware is essential for achieving optimal performance of system by maintaining the system physical security. Often the modular arithmetic like modular multiplication, addition and exponentiation is utilized for arithmetic operations in different cryptography methods [2]. Therefore, the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

cryptography algorithm performance is relying on congruential modular arithmetic operation effective implementation. Montgomery algorithm is the most effective technique for the implementation of modular exponentiation and multiplication and its critical operations depends on the binary addition of three operands. The binary addition of three-operands is a fundamental arithmetic operation in LCG (Linear Congruential Generator) based PRBG like CLCG (Coupled CLCG) [3, 4], CVLCG (Variable input LCG) and MDLCG (Modified Dual LCG). Among all the LGGs based and earlier PRBG techniques, the MDCLG is highly random and most secured PRBG technique.

The RCA (Ripple Carry Adder) can require linear number of gates [5], where as quick adders like Prefix Adders, CLA (Carry Look-Ahead Adders), etc. has logarithmic delays. These boundaries are indicating that often no effective adder is designed with sub-logarithmic delay; besides unreliable adders are implementing with sub-logarithmic delays. The unreliable adders can be utilized in cryptographic attacks; the reliable adders can be building with unreliable adders while adding error-detecting and correcting techniques [6].

The binary addition of three-operand is performed using one 3-operand adder or 2 two-operand adder. The CS3A is the widely adopted and area efficient method for performing the binary addition of three-operand in modular arithmetic utilized in PRBG techniques and cryptographic algorithms [7]. For shortening the delay of critical path, a PP2A like HCA is utilized for performing the addition of three-operand [8]. Hence the development of an effective VLSI architecture is essential for performing the binary addition of three-operand with minimal hardware resources. Thus a new area-effective and high speed adder is presented with pre-computing bit wise addition follow by carry-prefix computation logic for performing addition of three-operand that can significantly consume less gate area by reducing the propagation delay compared to CS3A.

Increasing market demands of battery-powered portable consumer electronics is one of the factors that drive the demand of low power chips. The requirement of lighter, durable and smaller electronic products indirectly results low consumption of power. In most of the portable systems, the life of battery will be emerging as a product differentiator. As a largest and heaviset element in several portable systems, the batteries won't have same growth in rapid density than electronic circuits. The power dissipation major source is gaining importance in these higher performance battery-powered digital systems like cell phones, laptops, individual digital assistants, etc. In these systems one of the major concerns is low consumption of power, since it can directly affect the performance through affecting the life span of battery. As a active and rapidly growing filed, the low power VLSI design become crucial in these scenarios. Though, reducing the frequency of clock is only feasible at the architecture level and basically frequency is considered as constant at circuit level for satisfying the requirements of speed. Certain basic logic requirements to implement the design of low power circuits are stated as follows:

• Reduction of Switched Capacitance

• Reduction of Switching Activity