Assessment of Developing a High-Speed Area-Efficiency-Based Reversible Adder with Reduced Quantum Cost in VLSI Architecture

[1]B. Thirupathi, [2]R. Srinvias, [3]B. Bhargavendera, [4]Bura Nikitha
[1,2,3]Associate Professor, [4]UG Student, [1,2,3,4]Department of Electronics and Communication Engineering,
Vaageswari College of Engineering, Karimnagar, Telangana, India

ABSTRACT
The three-operand binary adder is the fundamental functional component used in many cryptography and pseudo random bit generator (PRBG) techniques, as well as other applications, to carry out modular arithmetic. The method that is most frequently used to execute three-operand addition is called Carry Save Adder (CS3A). Ripple carry adder is used in carry save adder's last step, which results in a significant critical path delay. In addition, a parallel prefix two-operand adder like the Han-Carlson Adder (HCA) may be utilized for three-operand addition, which greatly decreases the critical path time while increasing area complexity. In order to implement the three-operand binary addition, a novel high-speed and area-efficient adder architecture is developed that uses pre-compute bitwise addition followed by carry prefix computation logic. The effectiveness of the proposed method is designed using Xilinx ISE 14.7
Keywords: Arithmetic Circuits, Three-operand adder, carry Save Adder (CSA), Han-CarlsonAdder (HCA)

Introduction

To minimize this trade-off between area and delay, a new high-speed, area-efficient three- operand adder technique and its efficient VLSI architecture is proposed. New adder architecture is used to perform the three-operand addition in modular arithmetic. The proposed adder technique is a parallel prefix adder. However, it has four-stage structures instead of three-stage structures in prefix adder to compute the addition of three binary input operands such as bit- addition logic, base logic, PG (propagate and generate) logic and sum logic. The logical expression of all these four stages. By implementing in this manner we can reduce the both area as well as delay.

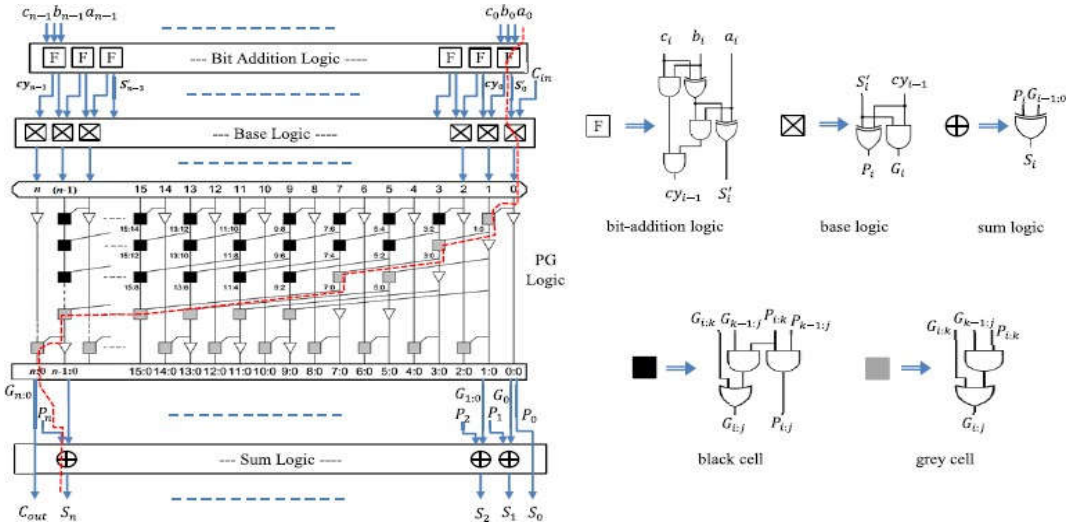


Fig.1. Block Diagram of Proposed Three-operand adder

Related Work

The method most frequently used to execute three-operand binary addition is the carry-save adder. In two phases, it computes the addition of three operands. The array of complete adders makes up the first level. With three binary inputs, ai, bi, and ci, each complete adder simultaneously computes the "carrier" bit and the "sum" bit. The ripple-carry adder, which is the second step, computes the three-operand addition's final n-bit "sum" and one-bit "carry-out" signals. In the ripple-carry stage, the "carry-out" signal is transmitted through the n complete adders. As a result, because bit length is only needed at the very end, the delay grows linearly with bit length. Han-Carlson adder (HCA) may be used to accomplish the three-operand addition in two phases is given in existing method. The detailed architecture of HCA-based three-operand adder (HC3A) is presented in this method. The maximum combinational path delay of HC3A depends on the propagate chain, i.e. the number of black-grey cell stage in the PG logic of Han-Carlson. The HCA-based three-operand binary adder greatly reduces the critical path delay in comparison withthe three-operand carry-save binary adder. However, the area increases with increase of bit length. Hence in carry save adder the critical path delay is more and in HCA-based three-operandadder the area is more while increasing the critical path delay.

PROPOSED METHOD

In recent years, reversible logic has become a promising technology in the areas of low power VLSI design, nanotechnology, quantum computing and optical computing. The performance and reliability of digital systems which are now implemented using conventional logic gates can be enhanced by the usage of reversible logic gates, which pave for low power consumption and lesser quantum delays, thus increasing the speed of computation. Adder circuits form the fundamental block in the arithmetic and logic unit of processors and other digital logic programmable devices. The performance of a digital system, its speed and throughput depend critically on the way these circuits are designed. Adder circuits are used in the Graphics Processing Unit (GPU) of computers for graphics applications to reduce complexity. Any way to enhance the performance and computational speed of these circuits will pave way for a better ALU. Incorporating the concepts of reversible computing in the design of adder circuits can significantly enhance the performance and speed of operation of digital systems. In this paper, two existing adder designs and a novel design are compared, analyzed. Detailed analysis of reversible logic design parameters, power consumption parameters, and FPGA utilization parameters is carried out.

Over the past few decades, phenomenal growth has been achieved in the design of computers and other digital logic processing devices like mobile phones, calculators, etc. Incorporating several millions of transistors into a single chip has enabled computations and operations to be efficient and fast. However, having very high transistor densities will lead to an increase in power dissipation. Existing technologies like CMOS will reach their boundaries soon as believed by today's researchers. Power dissipation and vulnerability to computing errors are the most important problems associated with the existing technologies. Reversible Logic is believed to be a prominent technology that could alleviate the drawbacks of the existing technologies. Reversible circuits are called lossless circuits, as there is neither energy loss nor information loss. These circuits are very attractive in applications where extremely low power consumption, is needed in areas ranging from communications, low power VLSI (Very Large-Scale Integration) technology, DNA computing to nanotechnology. Furthermore, reversible logic is very useful in quantum computing where the quantum evolution is inherently reversible. Arithmetic circuits such as adders, multipliers, and dividers are the quintessential blocks in a data processing system. Dedicated Adder circuits are required in several Digital Signal Processing applications. Reducing the number of reversible gates required to realize a circuit, quantum costs incurred and garbage inputs/outputs are the focus of research in reversible logic circuit design. In it is depicted that the amount of energy (heat) dissipated for every bit operation that is not reversible is given by KT ln2, where Kis the Boltzmann's constant (1.3807×10-23 JK-1) and T is the operating temperature of the

system. For T equal to the room temperature (300 K), KT ln2 is approximately equals 2.8×10-21 J, which might seem is small but it is no negligible. For example, assuming that all the 1.75 billion transistors in a processor (e.g., Intel i5 core) dissipate heat at a rate equal to the processor's operating frequency (2.5 GHz), then the processor would consume a power of approximately (2.5 x 10^9) x (KT ln2) x (1.75 x 10^9) = 12.258 maw (Assuming that the room temperature is 300K). The loss incurred is not tolerable in the design of ultra-low power consuming devices. Furthermore, Moore's law states that speed and capability of computers can be expected to double every two years, as a result of increases in the number of transistors a microchip can contain. The increase in transistors will lead to further power consumption and power dissipation due to information loss. If this goes on, there will be an intolerable amount of heat dissipationby computer systems. The advent of revolutionary technologies in computing is the need of the hour. One such technology is reversible computing. In 1973, C. H. Bennettconcluded that no energy would dissipate from a system as long as the system was able toreturn to its initial state from its final state regardless of what occurred in between. In it is shown that the theory of reversible computing is based on invertible primitives and composition rules that preserve inevitability and the constraints to be met with deal with both functional and structural aspects of computing processes. The laws of physics won't have an impact on the reduction in the size and quantum behavior of computers as depicted in. Reversible logic can be defined as thermodynamics of information processing. Hence, it is used to reduce the power dissipation by preventing the loss on information. It is shown in that parallel adder/can be extended to design low power Reversible ALUs, Multipliers and Dividers. In, four designs for reversible full-adder circuits and their implementation in CMOS logic and pass transistor logic were presented. A detailed description on reversible computing, quantum implementation of reversible gates, challenges and promising features of reversible logic in. Furthermore, it delineates how reversible logic technology will pave way for achieving ultra-low power computing. Presents a detailed analysis of FPGA utilization parameters and power parameters of reversible logic designs. Two designs of adder circuits using WG gate and DKG gate are proposed in. A serial adder circuit constructed using 8*8 DKG gate and an analysis on reversible logic parameters is carried out in. An 8-bit adder circuit using reversible approach for Xilinx Spartan 3E FPGA is proposed, simulated and synthesized in. In, a novel design of ALU is compared with an existing design. In, three designs using TR, Peres and Feynman gates were proposed and compared those in terms of quantum cost, garbage outputs and gate count.

There exist many reversible gates in the literature. Among them 2*2 Feynman gate , 3*3 Fredkin gate, 3*3 Toffoli gate and 3*3 Peres gate is the most referred. The detailed cost of a reversible gate depends on any particular realization of quantum logic. Generally, the cost is calculated as a total sum of 2*2 quantum primitives used. The cost of Toffler gate is exactly the same as the cost of Fredkin gate and is 5. The only cheapest quantum realization of a complete (universal) 3*3 reversible gate is Peres gate and its cost is 4.

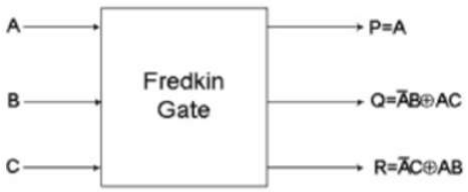


Figure 3: 3*3 Fredkin gate

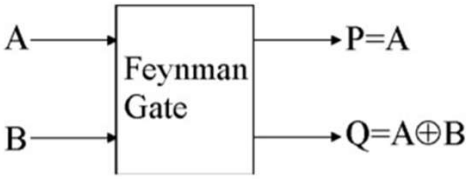


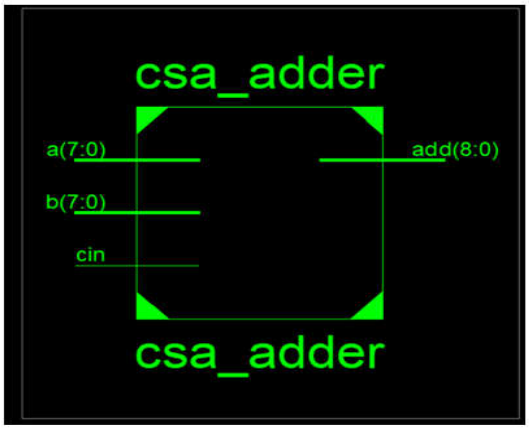
Figure 2: 2*2 Feynman gate

Full adder is the fundamental building block in almost every arithmetic logic circuit. Therefore, a gate that can work singly as a reversible full adder will be beneficial to the development of other complex logic circuits. This gate requires only one clock cycle and produces no extra ra Garbage outputs, that is, it adheres to the theoretical minimum as establish.

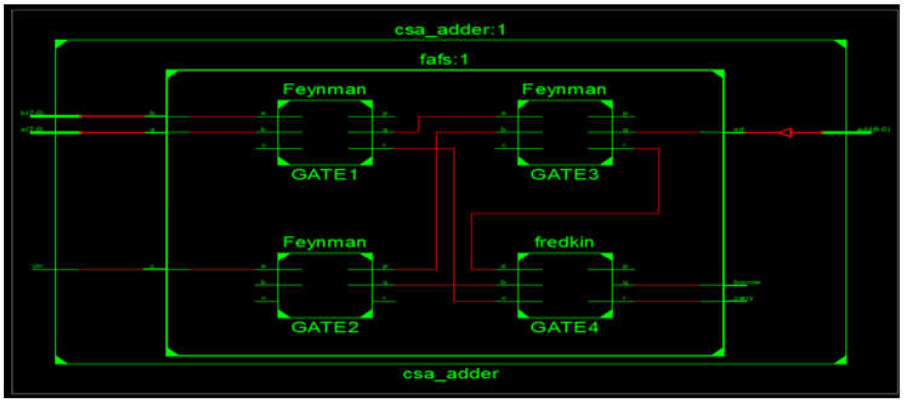
The following demonstrates that the proposed reversible full adder gate is superior to the existing counterparts in terms of hardware complexity, quantum costs, garbage outputs and constant input.

SIMULATION RESULTS

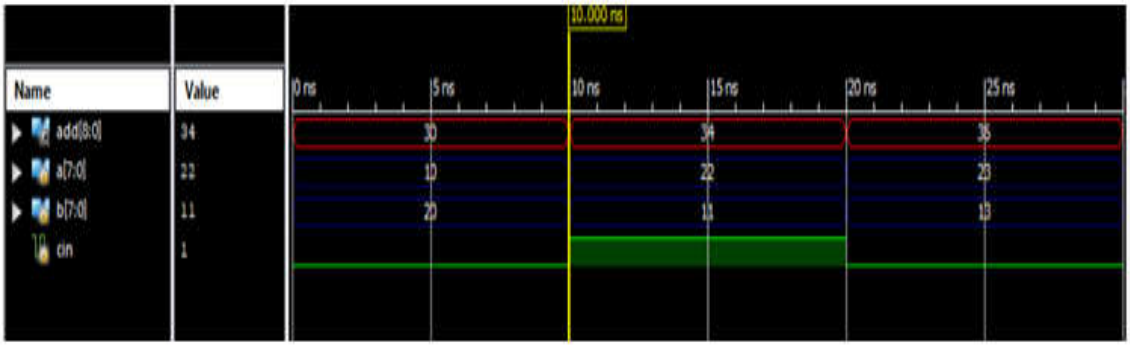
RTL



INTERNAL BLOCK DIAGRAM



SIMULATION RESULTS



CONCLUSION

A high-speed area-efficient adder technique and its VLSI architecture is proposed to perform the three operand binary addition for efficient computation of modular arithmetic used in cryptography and PRBG applications. The proposed three-operand adder technique is a parallel prefix adder that uses four-stage structures to compute the addition of three input operands. The novelty of this proposed architecture is the reduction of delay and area in the prefix computation stages in PG logic and bit-addition logic that leads to an overall reduction in critical path delay, area-delay product (ADP) and power-delay product (PDP). For the fair comparison, the concept of hybrid Han-Carlson two-operand adder is extended to develop a hybrid Han-Carlson three- operand adder (HHC3A) topology. The same coding style adopted in proposed adder architecture is extended to implement the HHC3A, HC3A and CS3A using Verilog HDL. Further, all these designs are synthesized using commercially available 32nm CMOS technology library to obtain the core area, timing and power for different word size. From the physical synthesis results, this is clear that the proposed adder architecture is 3 to 9 times faster than the corresponding CS3A adder architecture. Moreover, a sharp reduction in area utilization, timing path and power dissipation can be observed in the proposed adder as compared to the HC3A adder. A new quantum cost efficient reversible full adder gate in nanotechnology. This gate requires only clock cycle and can be used to synthesize any arbitrary Boolean functions thereforeuniversal. The hardware complexity offered by this gate is less than the existing reversible full adder gates. The quantum realization cost of this gate is only 8. This gate is readily available for use in nanotechnology since its quantum implementation is given in NMR technology.

REFERENCES

1. M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal, and Y. M. Jang, “FPGA implementation of high-speed area-efficient processor for elliptic curve point multiplication over prime field,” IEEE Access, vol. 7, pp. 178811–178826, 2019.
2. Z. Liu, J. GroBschadl, Z. Hu, K. Jarvinen, H. Wang, and I. Verbauwhede, “Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things,” IEEE Trans. Comput., vol. 66, no. 5, pp. 773–785, May 2017.
3. Z. Liu, D. Liu, and X. Zou, “An efficient and flexible hardware implementation of the dual- field elliptic curve cryptographic processor,” IEEE Trans. Ind. Electron., vol. 64, no. 3, pp. 2353–2362, Mar. 2017.
4. B. Parhami, Computer Arithmetic: Algorithms and Hardware Design. New York, NY, USA: Oxford Univ. Press, 2000.
5. P. L. Montgomery, “Modular multiplication without trial division,” Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.
6. S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu, “Low-cost high-performance VLSI architecture for montgomery

modular multiplication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 24, no. 2, pp. 434–443, Feb. 2016.

7. S.-R. Kuang, J.-P. Wang, K.-C. Chang, and H.-W. Hsu, "Energy-efficient high-throughput montgomery modular multipliers for RSA cryptosystems," IEEE Trans. Very Large Scale Integr.(VLSI) Syst., vol. 21, no. 11, pp. 1999–2009, Nov. 2013.
8. S. S. Erdem, T. Yanik, and A. Celebi, "A general digit-serial architecture for montgomery modular multiplication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 5, pp. 1658–1668, May 2017.
9. R. S. Katti and S. K. Srinivasan, "Efficient hardware implementation of a new pseudo- random bit sequence generator," in Proc. IEEE Int. Symp. Circuits Syst., Taipei, Taiwan, May 2009, pp. 1393–1396.
10. A. K. Panda and K. C. Ray, "Modified dual-CLCG method and its VLSI architecture for pseudorandom bit generation," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 66, no. 3, pp. 989–1002, Mar. 2019.