

Design an High Performance Novel Reversible Multiplier

¹PODETI SIRISHA, ²P. BALA KRISHNA, ³S. KISHORE BABU

¹M.Tech – Scholar, ²Assistant Professor, ³Head Of The Department,

1,2,3.Department Of ECE, Vikas Group Of Institutions, Nunna, Krishna District

Abstract-Increasing demand for reduction in power dissipation in digital computer system has leads to new mode of computation for digital design giving birth to reversible computing. Its main aim is low power dissipation in logical elements but can have some other advantages like error prevention and data security. In present-day, reversible logic has bring out to be an optimistic computing model having applications in low power CMOS, nanotechnology, quantum computing and DNA computing. A high performance processor of elliptic curve cryptography (ECC) over GF by using polynomial presentation. It has three finite field (FF) RISC cores and to achieve instruction-level parallelism use main controller with pipeline, so that one can get largely parallelized algorithm for elliptic curve point. The main focus of this study involves two primary design implementations. First one reversible gate design and second one multiplier design using reversible gates. Here in this manuscript we implemented a 8*8 reversible gate design called "NSG". The total project is implemented in Xilinx 14.7 ISE with Spartan 3E family.

Keywords: Reversibility, NSG, Constant Input, Garbage Output, ALU.

I. INTRODUCTION

Energy loss is a very important factor in modern VLSI design. Irreversible hardware computation results in energy dissipation due to information loss. R.Landauer has shown that for irreversible logic computations, each bit of information lost generated $KT \ln 2$ joules of heat energy, where K is Boltzmann’s constant and T is the temperature at which computation performed. Reversible logic circuit does not have loss of information and reversible computation in a system can be performed only when the system consists of reversible gates. C.H.Bennet showed that $KT \ln 2$ energy dissipation would not occur if the computation is carried out in a reversible way.

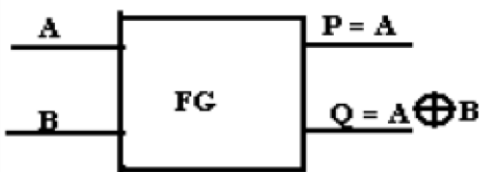


Fig 1. Block Diagram of Feynman Gate

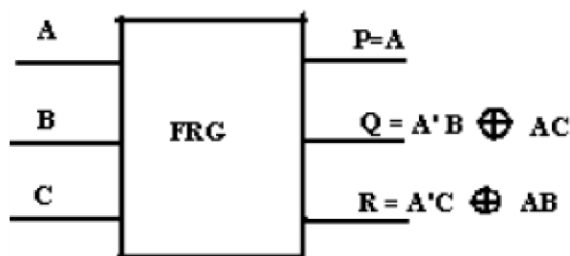


Fig 1. Block Diagram of Fredkin Gate

Reversible logic is very crucial for the construction of low power, low loss computational designs which are very essential for the design process of arithmetic circuits used in quantum computation, Nano-technology and other low power digital circuits.

Lately, quite a few researchers have been paying their attention on the design, simulation and synthesis of proficient reversible logic circuits. The vital reversible gates [3] used for reversible logic synthesis are Feynman Gate and Fredkin gate [3, 4].

Reversible logic is emergent and drawing attention in the recent past due to its uniqueness i.e. less heat dissipating characteristics. It has been proved that any Boolean function can be implemented using reversible gates. The NS Gate [5] i.e. "NSG" can singly be implemented in all logical Boolean operations. Reversible logic has publicized possibilities to have widespread purpose in upcoming emerging promising technologies such as quantum computing, optical computing, quantum dot cellular automata in addition to ultra-low power VLSI circuits, DNA computing to generate zero power rakishness under ideal conditions.

In Proposed system, there exists a design of multiplier and adder units by number of reversible gates. In This design, we are using only one reversible gate called NSG gate. By using this gate number of operations will be performed by only single gate and the garbage outputs also minimized. In this paper, we are also proposed a 8-bit MAC unit. MAC unit is an inevitable component in many digital signal processing (DSP) applications involving multiplications and/or accumulations. MAC unit is used for high performance digital signal processing systems. The DSP applications include filtering, convolution, and inner products. Most of digital signal processing methods use nonlinear functions such as discrete cosine transform (DCT) or discrete wavelet transforms (DWT).

Because they are basically accomplished by repetitive application of multiplication and addition, the speed of the

multiplication and addition arithmetic determines the execution speed and performance of the entire calculation. The multiplier and adder unit will be designed by NSG gate and accumulator unit will be designed by using Sayem gate [6], Feynman gate and Fredkin gate.

The simulation output is verified using Xilinx ISE 13.2 and the model graph results verified using Modelsim software.

II. EXISTED SYSTEM

To get different elliptic curve arithmetic algorithms we use point scalar multiplication which is also known as ECC operation. As the program executed on crypto processor is fixed to a certain type of elliptic curve arithmetic algorithm, we can accelerate the system performance by using a customized operation. There are some ECC point multiplication which has an advantage of reducing FF inversion operation. The most commonly used FFS are prime fields GF (p) and binary fields GF (2^m). They both provide the same level of security. Now discussing about algorithms used in implementation of FF arithmetic instructions. The algorithms are parallel field reductions, world level finite field multiplier, FF square, double square and FF inversion.

Architecture and implementation: The actual architecture consists of a main controller, three cores, interconnection and register files. To store the middle results we use registers files of each core. To store the middle results we use registers files of each core. To the prefix Ai stands for signals in core i. The Ai-z and Ai-x are special registers to store zi and xi in algorithm. Ai-G is only general register. The dash lines in each core are the interconnection and by pass results from local ALU. Rx, Ry and R2 are interconnections from the main controller for accessing x, y and b. The address of data path is divided into two levels. The first level has a high priority and uses five most significant bits. The second level consists of three least significant bits. The second level consists of three least significant bits. These least significant bits used to decode register data paths. The address of the third bit form least significant bits in one if the second level is valid which represent a special register. The change the address of least significant bit we can perform swap operation between special registers. See A1-X and A1-Z are accessed to X2 and Z2 instead of X1 and Z1 at the end of loop in core which is similar with core 3. Therefore a swap operation exists by default. Swap1 and swap2 are two swap signals which are generated from the main controller of swap logic. The function of swap1 is to swap special registers by changing the address of least significant bits and that of swap2 is to swap by pass data.

Five stage pipeline and data flow: The five stage pipeline is a modified structure of four stage pipeline. We need to add a data loading stage between executing and instruction of decoding from register files so that one can load data.

III. PROPOSED DESIGN

In this paper, a 4 * 4 one through reversible gate called NS gate "NSG" is projected. The proposed reversible NSG gate is shown in Figure.3.1. The corresponding truth table of the gate is shown in Table I. It can be established from the Truth

Table that the input pattern analogous to a particular output pattern can be exclusively determined [5]. The invented NSG gate can perceive all Boolean logical operators. The input d, c, b and a are termed as input terminal 1, 2, 3 and 4 respectively and the output are termed as output 1, output 2, output3 and output 4 respectively from first to last of the paper.

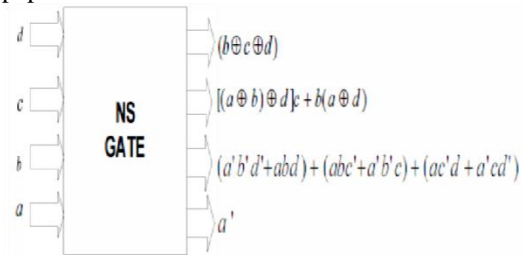


Fig 3.1 Proposed Reversible NS Gate

As mentioned above, MAC unit consist of multiplier, adder and register/accumulator. In this paper, we used 8 bit modified Reversible NS multiplier. The MAC inputs are obtained from the memory location and given to the multiplier block. This will be useful in 8 bit digital signal processor. The input which is being fed from the memory location is 8 bit.

Since the bits are huge and also ripple carry adder produces all the output values in parallel, PIPO register is used where the input bits are taken in parallel and output is taken in parallel. The output of the accumulator register is taken out or fed back as one of the input to the ripple carry adder. The above figure 2.1 shows [8] the basic architecture of MAC unit. The figures 3.2 shows the 8X8 NS multiplier.

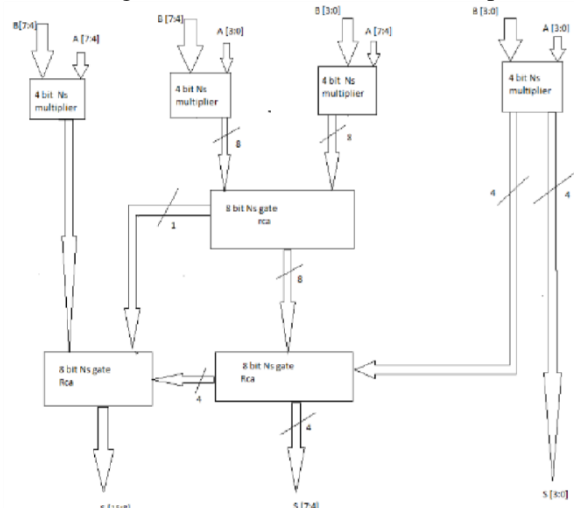


Fig 3.2 Multiplier architecture

IV. RESULTS

The Reversible MAC unit simulated and synthesized using the Xilinx Design Suit14.7 with device family as spartan3E and device Xc3s100e5vq100. The simulation Results are verified by using Modelsim simulator i.e. given the input values are multiplier of a = 00110011 (51) and b = 00011110 (30) and get the final output is final_out = 0000101111110100 (3060). The Figure 4.1 shows the model graph of Reversible MAC unit and Table I shows the comparison of conventional and Reversible MAC units.

In the below table-I observe the number of (Look Up Tables) LUT’s used in the general MAC unit is 214 which is higher than that of Reversible MAC unit. Here area occupied by the General MAC unit is higher than that of Reversible MAC unit. In reversible Mac unit, the multiplier we used was designed by using only one reversible gate called as NS gate. So area occupied by reversible multiplier is low when comparing with normal multiplier used in general MAC unit. And also the delay produced by general Mac unit is very high when comparing with Reversible MAC unit.

Name	Value	0.999,994 ps	0.999,995 ps	0.999,996 ps	0.999,997 ps	0.999,998 ps	0.999,999 ps
q[3:0]	0000000000000000			0000000000000000			
q[4:0]	0000000000000000			0000000000000000			
q[5:0]	0011000000000000			0011000000000000			
q[6:0]	000			000			
q[7:0]	0000000000000000			0000000000000000			
q[8:0]	0000000000000000			0000000000000000			
q[9:0]	0000000000000000			0000000000000000			
q[10:0]	0000000000000000			0000000000000000			
q[11:0]	0000000000000000			0000000000000000			
q[12:0]	0000000000000000			0000000000000000			
q[13:0]	0011000000000000			0011000000000000			
q[14:0]	0011000000000000			0011000000000000			

Fig 4.1 Simulation Results of Reversible MAC unit

V. CONCLUSION

Reversible multiplier can be designed with the different logical designs purposed in conventional combinational and sequential logic with the aim to improve the performance of computational units. To improve the performance, the main measures in designing an efficient reversible logic multiplier are: Number of gates, Number of garbage outputs, Number of ancillary inputs. Finally reversible logic gates are occupied less area and delay because it has a many to many input and output relations. so by using of these gates we can design any large circuits with less components and it is the main advantage of reversible logic gates.

Future scope: we may extend this to 16*16 multiplier using 4*4 NS gate. It can be implementing by using other reversible gates for D.S.P applications.

REFERENCES

[1] J R.Landauer, "Irreversibility and Heat Generation in the Computational Process", IBM Journal of Research and Development, 5,pp. 183-191,1961.

[2] C.H. Bennett, "Logical Reversibility of Computation", IBM 1. Research and Development, pp.525-532, November1973.

[3] Bennett, C.H., 1988. "Notes on the history of reversible computation". IBM 1. Res. Develop., 32: 16-23.

[4] E. Fredkin, T Toffoli, "Conservative Logic", International Journal of Theor. Physics, 21(1982), pp.219-253.

[5] [5].Neeraj kumar misra, subodh wairya, vinodkumarsingh, "An inventive design of 4*4 bit reversible NS gate", proceedings of IEEE international conference, 2014.

[6] T.nagapavani, V.rajmohan, p.rajendran"Optimized shift register design using reversible logic", proceedings of IEEE international conference, 2011.

[7] NM Nayeem, MdAHossian, L Jamal and Hafiz Md. HasanBabu, "Efficient design of Shift Registers using Reversible Logic," Proceedings of International Conference on Signal Processing Systems, 2009.

[8] Samir palnitkar, "verilog HDL", second edition, IEEE

1364-2001 compliant.

[9] [9].J. E. Rice, "A New Look at Reversible Memory Elements," Proceedings of IEEE International Symposium on Circuits and Systems, 2006.

[10] [10].H. Thapliyal and M. B. Srinivas, "A Beginning in the Reversible Logic Synthesis of Sequential Circuits," Proceedings of Military and Aerospace Programmable Logic Devices International Conference, 2005.



¹PODETI SIRISHA studied B.Tech at Sri Sarathi Institute Of Engineering &Technology during 2010 – 2014. At present she is pursuing M.Tech at VIKAS GROUP OF INSTITUTIONS. Her area of interest is V.L.S.I Design.



²P. BALA KRISHNA studied B.Tech in Prakasam Engineering College - Kandukur and M.Tech in Dr. Samuel George Institute of Engineering and Technology, Markapur. He has 4 years of teaching experience and present working as Assistant Professor in Vikas Group of Institutions, Nunna, Vijayawada, Andhra Pradesh.



³S.KISHORE BABU studied diploma in Sir C.R.R Polytechnic College, Eluru, B.Tech in S.R.K.R Engineering College, Bhimavaram and M.Tech in J.N.T.U ananthapur. He is Pursuing PH.D in Acharya Nagarjuna University, Guntur