iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Implementation of a High-Speed RSD Based ECC Processor with Vedic Multipliers

Chitra A[1], Sangeethalakshmi K[2], Prabhakar K[3]
[1,2] *Department of Electronics and Communication Engineering, First-Two RMK College of Engineering and Technology,*
[3]*L&T Limited*

Abstract- In this paper, an exportable application-specific instruction-set elliptic curve cryptography processor based on redundant signed digit representation is proposed. The processor employs extensive pipelining techniques for Karatsuba–Ofman method to achieve high throughput multiplication. Furthermore, an efficient modular adder without comparison and a high throughput addition/subtraction, which results in a short data path for maximized frequency, are implemented. We have proposed a novel recursive decomposition algorithm for addition to obtain high-throughput digit-serial implementation. The synthesis results for field programmable gate array (FPGA) and application specific integrated circuit (ASIC) realization of the proposed designs and competing existing designs are compared.
Keywords: Elliptic curve cryptography, Vedic multipliers, Redundant signed digits, Application specific integrated circuit.

I. INTRODUCTION

In this paper, we proposed an 8-bit multiplier using a Vedic Mathematics (Urdhva Tiryakbhyam sutra) for generating the partial products. The partial product addition in Vedic multiplier is realized using carry-skip technique. An 8-bit multiplier is realized using a 4-bit multiplier and modified ripple carry adders. In the design we have reduced the number of logic levels, thus reducing the logic delay. Simulation of the architecture is carried out using Xilinx ISIM and synthesized using Xilinx XST [1]. Architecture to perform high speed multiplication using ancient Vedic math's technique is proposed. To increase the speed of multiplier the half adder and full adder of the Vedic mathematics multiplier is replaced with compressor. In this 4:2 compressors are used for adding more than 3-bits at a time. Upon comparison, the compressor based multiplier introduced in this paper, is almost two times faster than the popular methods of multiplication [2].

In this paper, multiplier based on ancient Vedic mathematics technique has been proposed which employs 4:3 compressor, 5:3 compressor, 6:3 compressor and 7:3 compressors for addition of partial products. Combining the Vedic Sutra- Urdhwa Tiryakbhyam and efficient compressors, a robust area and power efficient multiplier architecture has been achieved. The designs were synthesized and analyzed in Cadence RTL compiler in 180 nm technology. In this higher order compressor for used to design an 8*8 multiplier. It can be used in low area and power critical applications [3].

In this symbol CMOS 4:2 compressor using pass logic is develop. This circuit is design using an X-OR and X-NOR combination gates it eliminates the use of inverters. The total power dissipation has been cut down to a minimum while providing the full output voltage swing at all nodes in the circuit. The total circuit consists of 28 transistors [4].

In this paper a new high speed multiplier is designed is using 4:2 and 7:2 compressors for addition. The compressor based multiplier introduced in this paper. The compressor adder is a logical circuit which is used improves the computational speed of the addition of 4 or more bits at a time. Compressors can efficiently replace the combination of several half adders and full adders, thereby enabling high speed performance of the processor which incorporates the same. This technique in two times faster than the ancient multiplier technique. The multiplier was designed using Xilinx Spartan 3e series of FPGA [5].

II. PROPOSED METHOD

In this paper a new technique is proposed to perform 8*8 multiplications. The multiplier is designed using the combination of half adder, full adder, 4:2compressor, 5:2, and 7:2 compressors. This technique requires low area, high speed and is a very efficient technology. Multipliers are basic elements in several digital signal processing applications, such as filtering, convolution, fast fourier transform, discrete fourier transform, hardware implementation of mathematical functions. Because they are basically accomplished by repetitive application of multiplication and addition, the speed of the multiplication and addition arithmetic's determines the execution speed and performance of the entire calculation. Because the multiplier requires the longest delay among the basic operation blocks in digital system. This ECC processor mainly consists Vedic multiplier. The advantage of using Vedic multiplier Booth is to reduce the number of partial products. The critical path of the multiplier depends on the number of partial

products which reduces the delay when compared to other Multipliers.

As mentioned earlier, Vedic Mathematics can be divided into 16 different sutras to perform mathematical calculations. Among these the Urdhwa Tiryakbhyam Sutra is one of the most highly preferred algorithms for performing multiplication. The algorithm is competent enough to be employed for the multiplication of integers as well as binary numbers. The term "Urdhwa Tiryakbhyam" originated from 2 Sanskrit words Urdhwa and Tiryakbhyam which mean "vertically" and "crosswise" respectively. The main advantage of utilizing this algorithm in comparison with the existing multiplication techniques, is the fact that it utilizes only logical "AND" operations, half adders and full adders to complete the multiplication operation. Also, the partial products required for multiplication are generated in parallel and apriority to the actual addition thus saving a lot of processing time.

The formulas of urdhwa tiryakbhyam sutra for multiplication of two eight bit numbers is given below,

P0= A0*B0

C1P1 = (A1*B0) + (A0*B1)

C3C2P2 = (A2*B0) + (A1*B1) + (A0*B2) + C1

C5C4P3 = (A3*B0) + (A2*B1) + (A1*B2) + (A0*B3) +C2

C7C6P4 = (A4*B0) + (A3*B1) + (A2*B2) + (A1*B3) + (A0*B4) + C3 + C4

C10C9C8P5 = (A5*B0) + (A4*B1) + (A3*B2) + (A2*B3) + (A1*B4) + (A0*B5) + C5 + C6

C13C12C11P6 = (A6*B0) + (A5*B1) + (A4*B2) + (A3*B3) + (A2*B4) + (A1*B5) + (A0*B6) +C7 + C8

C16C15C14P7 = (A7*B0) + (A6*B1) + (A5*B2) + (A4*B3) + (A3*B4) + (A2*B5) + (A1*B6) +(A0*B7) + C9 + C11

C19C18C17P8 = (A7*B1) + (A6*B2) + (A5*B3) + (A4*B4) + (A3*B5) + (A2*B6) +(A1*B7) + C10 + C12 + C14

C22C21C20P9 = (A7*B2) + (A6*B3) + (A5*B4) +(A4*B5) + (A3*B6) + (A2*B7) +C13+ C15 + C17

C25C24C 23P10 = (A7*B3) + (A6*B4) + (A5*B5) + (A4*B6) + (A3*B7) + C16 +C18 + C20

C27C26P11 = (A7*B4) + (A6*B5) + (A5*B6) +(A4*B7) + C19 + C21 + C23

C29C28P12 = (A7*B5) + (A6*B6) + (A5*B7) + C22 +C24 + C26

C31C30P13 = (A7*B6) + (A7*B6) + C25 +C27 + C28

C32P14 = (A7*B7) + C29 + C30

P15 = C31 + C32

Let us consider two 8 bit numbers A7 -A0 and B7-B0, where 0 to 7 represent bits from the Least Significant Bit (LSB) to the Most Significant Bit (MSB). P0 to P15 represent each bit of the final computed product. It can be seen from equation (1) to (15), that P0 to P15 are calculated by adding partial products, which are calculated previously using the logical AND operation. The individual bits obtained from equations (1) to (15), in turn when concatenated produce the final product of multiplication which is depicted in (16).The carry bits generated during the calculation of the individual bits of the final product are represented from C1 to C32.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

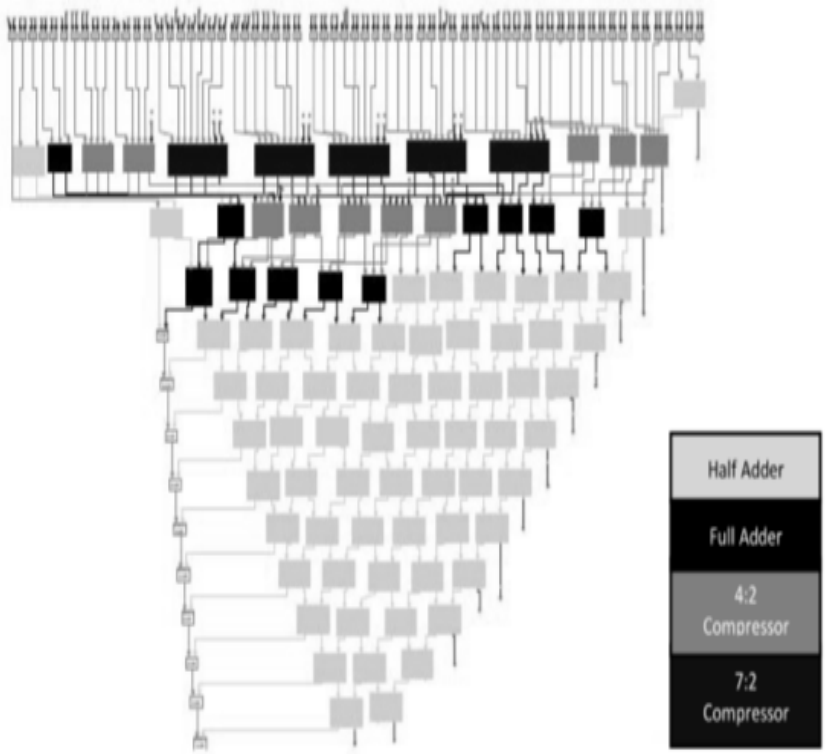


Fig 1-Architecture of Compressor based Urdhwa multiplier

Graphically illustrates the step by step method of multiplying two 8 bit numbers using the Urdhwa Tiryakbyam Sutra. The black circles indicate the bits of the multiplier and multiplicand, and the two-way arrows indicate the bits to be multiplied in order to arrive at the individual bits of the final product. As mentioned earlier, the partial products obtained are added with the help of full adders and half adders. It can be seen, from equation (1) to (16) that in few equations there is a necessity of adding more than 3 bits at a time. This leads to additional hardware and additional stages, since the full adder is capable of adding only 3 bits at a time. In the next section three different types of compressor architectures are explored which assist in adding more that 3 bits at a time, with reduced architecture and increased efficiency in terms of speed.

III. SOFTWARE DESIGN

The electronics industry has achieved a phenomenal growth over the last two decades mainly due to the rapid advances in integration technologies, large-scale systems design – in short, due to the advent of VLSI. Typically, the required computational power of these applications is the driving force for the fast development for this field. One of the most important characteristics of information service is their increasing need for very high processing power and bandwidth. The other important characteristics is that the information services tend to become more and more personalized, which means that the devices must be more intelligent to answer individual demands, and at the same time they must be portable to allow more flexibility and mobility. More complex function is required in various data processing and telecommunications devices; the need to integrate these functions in a small system, packages is also increasing. The level of integration as measured by the number of logic gates in a monolithic chip has been steadily rising for almost three decades, mainly due to the rapid progress in processing technology and interconnects technology.
Therefore, the current trend of integration will also continue in the future. Advances in devices manufacturing technology and especially the steady reduction of minimum feature size support the trend. A minimum size of 0.25 microns was readily achieved. Logic chip such as microprocessor chips and digital signal processing chips contain not only large array of memory (SRAM) Cells, but also many different functional units. As a result, their design complexity is considered much higher than that of memory chips. Sophisticated computer-aided design tools and methodologies are developed and applied in order to manage the rapidly increasing design complexity.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. WORKING

Multipliers play an important role in today's digital signal processing and various other applications. With advances in technology, many researchers have tried and are trying to design multipliers which offer either of the following design targets – high speed, low power consumption, regularity of layout and hence less area or even combination of them in one multiplier thus making them suitable for various high speed, low power and compact VLSI implementation.Common multiplication method is "add and shift" algorithm. In parallel multipliers number of partial products to be added is the main parameter that determines the performance of the multiplier. To reduce the number of partial products to be added, Modified Booth algorithm is one of the most popular algorithms. To achieve speed improvements Wallace Tree algorithm can be used to reduce the number of sequential adding stages. Further by combining both Modified Booth algorithm and Wallace Tree technique we can see advantage of both algorithms in one multiplier. However with increasing parallelism, the amount of shifts between the partial products and intermediate sums to be added will increase which may result in reduced speed, increase in silicon area due to irregularity of structure and also increased power consumption due to increase in interconnect resulting from complex routing. On the other hand "serial-parallel" multipliers compromise speed to achieve better performance for area and power consumption. The selection of a parallel or serial multiplier actually depends on the nature of application. In this lecture we introduce the multiplication algorithms and architecture and compare them in terms of speed, area, power and combination of these metrics. AND gates are used to generate the Partial Products, PP, If the multiplicand is N-bits and the Multiplier is M-bits then there is N* M partial product. The way that the partial products are generated or summed up is the difference between the different architectures of various multipliers. Multiplication of binary numbers can be decomposed into additions. Consider the multiplication of two 8-bit numbers A and B to generate the 16 bit product P.

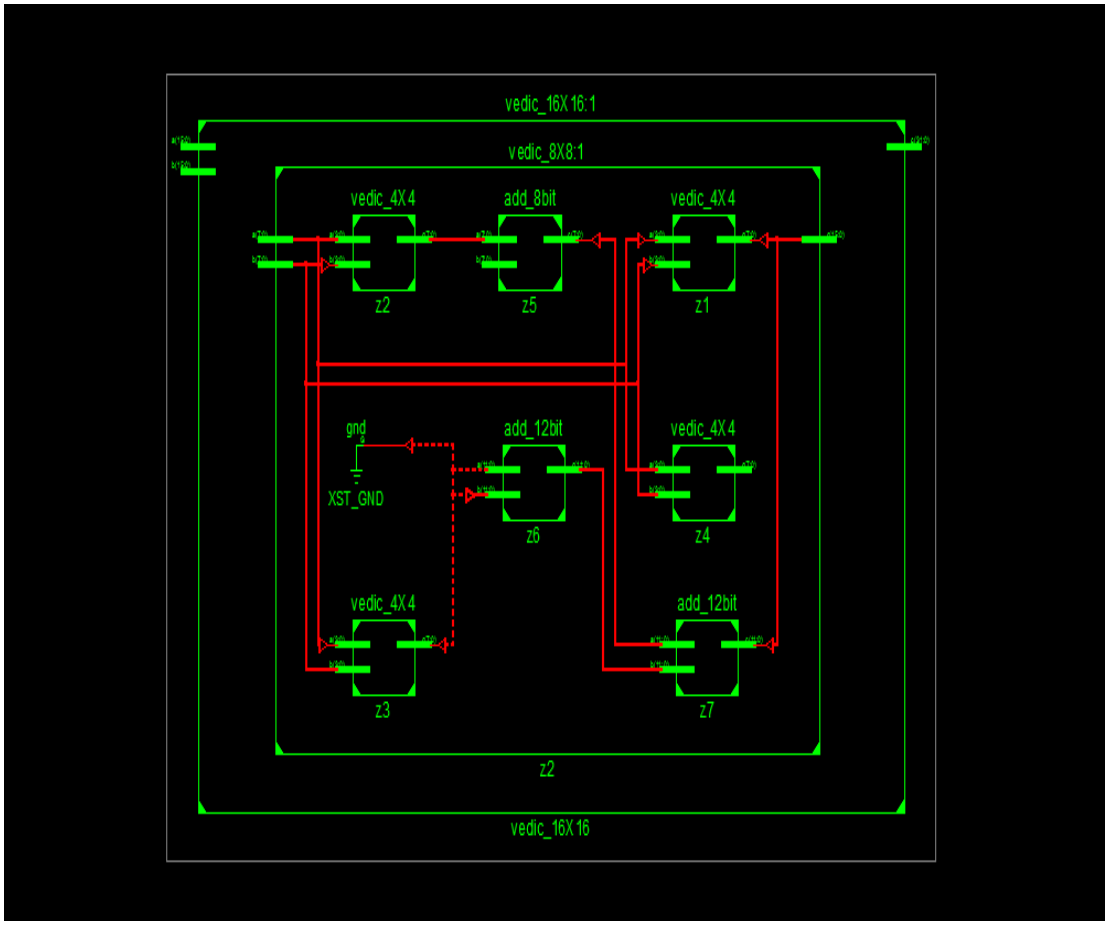


Fig 2. RTL Schematic of Vedic multiplier

V. SIMULATION RESULT

The multiplier based on Urdhwa method of multiplication requires several full adders and half adders to add the necessary partial

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

products. This in turn leads to a large propagation delay due to the reasons explained in the previous section. As part of our novel approach, we combined the compressor architectures explained earlier and utilized the same in the Urdhwa based architecture which was formerly shown below. The architecture for the multiplier given below.

That the compressor based Urdhwa multiplier requires only 12 parallel stages as opposed to 15 which was in the case of the conventional Urdhwa Tiryakbhyam multiplier. This is a major improvement with respect to high-speed multiplier design. Also, it can be seen that, many of the stages have now been reduced to logical XOR operation, with an initiative to reduce area. An analysis on the area occupied by the new design and also the improvement in speed in comparison with other popular methods of multiplication has been presented in this section

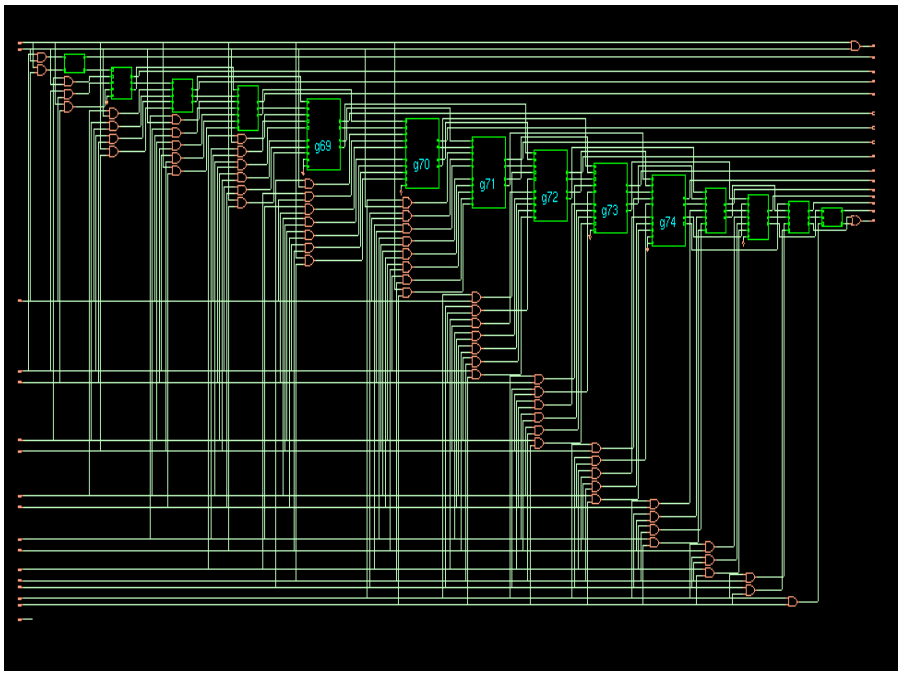


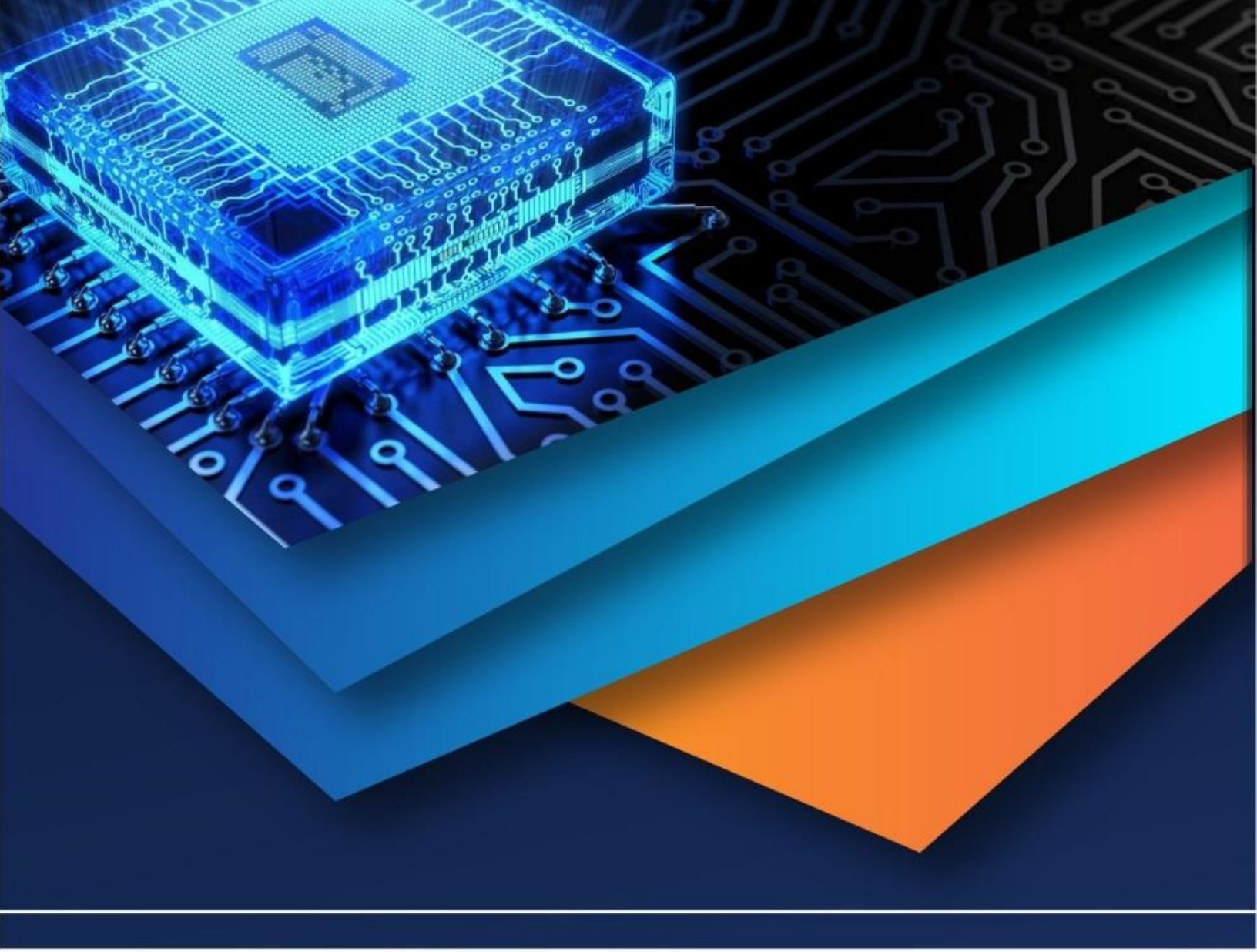
Fig 3. Output schematic of multiplier

VI. CONCLUSION

This multiplier provides high-speed performance for the elliptical curve cryptography for encryption of binary bits. The delay time of this Vedic multiplier is very much less when compared to the existing model. The pipelining in the Vedic multipliers are faster and highly robust when compared to the normal multipliers. This reduces the time consumption for the encryption and decryption process in ECC process. Equally, new demands arising from unconventional applications have stimulated new solutions, combining proven technologies in novel and innovative ways.

REFERENCES

[1] Cristophe bhode 'Introduction to reconfigurable ECC PROCESSOR' architectures algorithms and applications springer.
[2] Diffie W and HellmanM. E. (1976) 'New directions in ECC cryptography,' IEEETrans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654.
[3] .Eslami Y, Sheikholeslami A, GulakP. G.,Masui S, and Mukaida K(2006).'An area-efficient universal ECC cryptography processor for smart cards,'IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 14, no. 1, pp.43–56.
[4] Goodman J and A. P. Chandrakasan, (2001) 'An energy-efficient reconfigurablepublic-key ECC cryptography processor,' in the proceedings of IEEE J. Solid-State Circuits,vol. 36, no. 11, pp. 1808–1820.
[5] HoWon Kim, Member, IEEE, and Sunggu Lee,(2004).'Design and Implementation of a Private and Public Key ECC Crypto Processor and Its Application to a Security System' in the proceedings of IEEE Transactions on Consumer Electronics, Vol. 50, No. 1.
[6] Jun-Hong Chen, Ming-Der Shieh, Member, IEEE, and Wen-Ching Lin(2010).'A High-Performance Unified-Field Reconfigurable ECC Cryptographic Processor' in the proceedings of IEEE transactions on very large scale integration (vlsi) systems, vol. 18, no. 8.
[7] Jan Zutter, Max Thalmaier, Karsten-Olaf Laux Wipotec (2009).'Acceleration of RSA Cryptographic Operations using FPGA Technology',
[8] C. E. Leiserson and J. B. Saxe,(1991). 'Retiming synchronous circuitry,' in the proceedings of Algorirhmica, vol. 6, pp. 5-35.
[9] Neil Smyth, Máire McLoone and John V McCanny (2005).'Reconfigurable Processor for Public-Key Cryptography' in the proceedings of IEEE.
[10] Nibouche', M. Nibouche', and A.Bouridane(2004) 'High speed FPGA implementation of RSA encryption algorithm', in the proceedings of IEEE.
[11] Omar Nihouche, Mokhtar Nibouche, Ahmed Bouridane, and Ammar Belatreche, (2004). 'Fast Architectures For FPGA-Based Implementation of RSA EncryptionAlgorithm', in the proceedings of IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY