PalArch's Journal of Archaeology of Egypt / Egyptology

# WALLACE TREE HIGH PERFORMANCE STRATEGY FOR DATA PRIVACY EMPLOYING ELLIPTIC CURVE CRYPTOLOGY

*Amrita Sajja*[1]*, Kiran Kumar Mandrumaka*[2]*, Swapna Punnam*[3]

[1,2,3] ECE Department, Anurag Group of Institutions Hyderabad, Telangana, India

Corresponding Author: Email: [2]kirankumarece@cvsr.ac.in

**Amrita Sajja, Kiran Kumar Mandrumaka, Swapna Punnam. Wallace Tree High Performance Strategy for Data Privacy Employing Elliptic Curve Cryptology -- Palarch's Journal of Archaeology of Egypt/Egyptology 18(9), 561-575. ISSN 1567-214x**

**Keywords: Ecc, Wallace Tree Multiplier, Enhanced Efficiency, Zynq Board, Xilinx 2015.2.**

## ABSTRACT:

The ECC is the best standard for asymmetric cryptography. The success of ECC is due to its much better protection than many symmetric and asymmetric models. In 1985, Victor Miller and Neal Koblitz proposed entirely different use of elliptic curves in cryptography. Elliptic Cryptography (ECC) is an elliptical image encryption technique related to public curve theory which is used to build easier, smaller and better cryptographic keys. Elliptic curve (ECC) cryptography is indeed a key public cryptography method. The proposed design consists of a single point multiplication algorithm for ECC implementation on FPGA. And instead of Vedic Multiplier, we used Wallace tree multiplier. This paper offers an effective ECC method for cryptography, enhanced efficiency by replacing the Vedic multiplier (16 bits) with Wallace tree multiplier (128 bit). The proposed design not only enhances performance, but processes the information repetitively in smaller area, low power usage and more rapidly. The entire concept proposed is synthesized, simulated and implemented on the ZYNQ FPGA board using Xilinx 2015.2.

## INTRODUCTION

In the presence of intruders, cryptography is the process of study and application of certain mathematical principles that are used for safe communication networks. Encryption and decryption are core of cryptography. All original message information but not in human readable format is included in the encrypted message. RSA, ECC, Hash function, and digital signature etc are traditional cryptographic primitives.

The most efficient data protection during communication is given by cryptography. Symmetric and Asymmetric Cryptography are two main domains of cryptography [6]. The best Asymmetric Cryptography model is ECC (Elliptic Curve Cryptography) [7]. The ECC's protection is much greater than many symmetrical as well as asymmetrical standards because of its privacy. This is shown in Fig.1, where the distinction between ECC and other Asymmetric and Symmetric algorithms is seen. Figure 2 presents the fundamental ECC algorithm. The 160-bit ECC encryption key offers the same protection as a 1024-bit RSA, according to some studies. The ECC cryptography is used to protect the data from various cyber-attacks.

Our work is innovated in developing and applying a minimum area criterion ECC algorithm and higher efficiency energy consumption. When compared to the RSA method, the ECC Algorithm gives faster performance due to smaller key sizes for encryption and decryption. ECC algorithm is designed using Wallace tree multiplier. The disadvantage of delay in this multiplier is compensated by ECC encryption as it requires less key size when compared to RSA method. The suggested implementation involves a single point multiplication with a 128-bit Multiplier Wallace tree having 256 bits of message carrying power at a time.

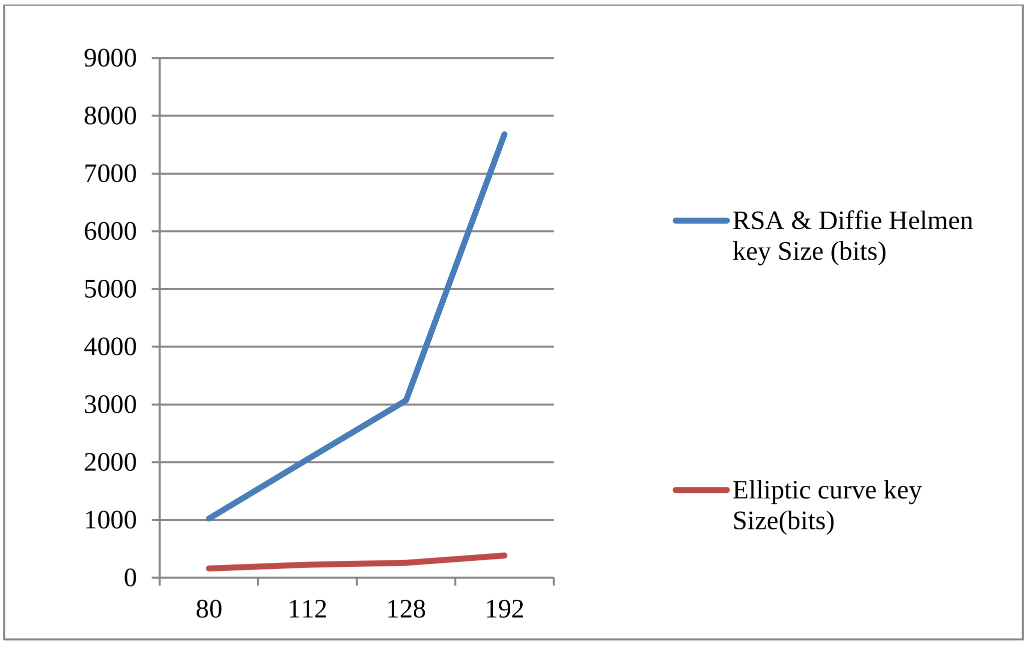


**Figure.1** Key Size Comparison

### *Related Work*

We illustrated some of the approaches used for safe cryptography of elliptic curves in our literature study. In 1985, Neal Koblitz [2] implemented an elliptical curve over a finite field, a public key cryptosystem which employs the more stable multiplicative group. It also notes that its protection level is difficult in the discrete logarithmic problem on the elliptical curve relative to other publicly recognized crypto schemes. In [3], Victor Miller specifies the Diffie-Hellman Key Exchange Protocol, which is safe against targeted hackers. The Elliptic curve groups have similar protection for a smaller key, which can be used in less space-saving embedded devices and minimize power consumption.

The main building block to incorporate elliptical curve cryptography was invented by Hackerson. It also provided different scalar multiplication and refined projection coordinate structures and the NIST premium reduction approach for different NIST primes. The [4] mapping mechanism illustrates how a plaintext is mapped to affinity points on the curve by transforming it into ASCII values and by multiplying the ASCII value by one base point on the curve these entities are translated into finite points [5] discusses koblitz decoding where the message is encoded into ASCII values, translated to x and y on the curve by Koblitz method. By taking x=mk+1 where k is a constant step and repeat a step before the curve co-ordinates. Carry save adder [8] is used in wallace tree to reduce the area and delay. The proposed design uses efficient and improved adder-based multiplexer to reduce area and latency. By using this redundant data can be added without waiting for the partial products. It improves the speed of the proposed design, but has a limitation of threshold voltage drop when large input data is taken [9]. Two possible architectures for a Vedic real multiplier are designed based on the URDHVA TIRYAKBHYAM sutra of Indian Vedic mathematics and an expression for path delay of a NN Vedic real multiplier with minimum path delay architecture improves computational efficiency and processing time due to decrease of combinational path delay results in complex design.[11] The new introduced adders utilize less area and power. In addition to that it employs Vedic multiplier and unsigned Baugh-wooley Wallace tree multiplier to enhance the productivity of multiplier with less area and power.[12] Sets of elliptic curves suggested by various criteria for cryptography are selected, and the selected curves are evaluated, focusing on the performance and security properties. The performance of each curve is measured in terms of computing time. The study is performed by examining individual curve for the design of the Elliptic Curve Diffie-Hellman (ECDH) technique and the Authentication Algorithm (ECDSA) (ECDSA).[13] The Montgomery algorithm is a new algorithm for multiplying two points on a curve. The Montgomery technique is a quick and fast way to compute scalar multiplication.[14] Efficient ECC solution for cryptography with improved performance by substituting the traditional multiplier with a Vedic multiplier (16 bit). Not only does the design enhance efficiency, but it also provides output in less space, with much less power usage, and at a rapid rate. The suggested concept includes an ECC implementation on an FPGA with a double point multiplication algorithm. In addition, we employed Vedic Multiplier rather than Conventional (Array) Multiplier.[15] Modular RNS Addition is a useful RNS procedure. Because no carry is communicated across channels, RNS addition has a significantly lower latency than addition in large prime fields. On the Xilinx FPGA platform, an RNS hardware architecture supporting rapid elliptic curve point-addition (ECPA), point-doubling (ECPD), and point-tripling (ECPT) is implemented. In addition, it is difficult to identify carry overflow with RNS.[16]

## *Proposed Method*

In mathematics, the elliptical curve is a flat algebraic curve defined by the non-singular equation for $Y^2=X^3+aX+b$; where x and y are the standard variables defining the function while the constant coefficients defining the curve are as a and b. that is, the curve has no cusps or intersections. An elliptic curve is not an ellipse, and in the usual sense, it may not be a curve. There is a link between elliptic curves and ellipses, but it is indirect. The Proposed ECC algorithm is as shown in Fig.3. The private key of the sender i.e., 64-bits and the points from the elliptic curve which is of 64-bits are multiplied by using Wallace tree multiplier for generating public key Q. Using Wallace tree multiplier reduces the total number of intermediate values that are generated during multiplication, hence increasing speed of the design. Cipher text C1 is generated by multiplying the public key and random key bits. The cipher text C2 is generated by multiplying random key with the message signal. Both Cipher texts C1 and C2 are sent by using transmitter

***Public Key Is Given By***

Public Key $Q = d1 \times P1 \quad (1)$

Where d1 is private key of sender & receiver, and P1 is points on the curve.

**At Encryption** shown in Fig 2. Cipher text is given by

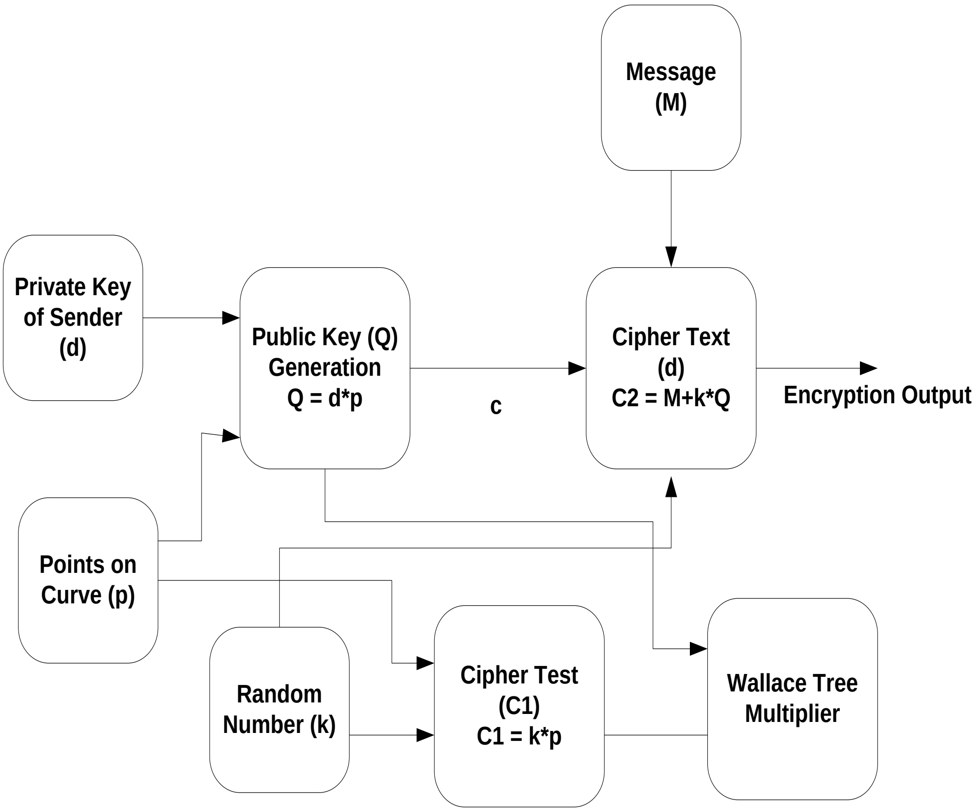


**Figure.2** Encryption Output of ECC Algorithm

$$C1 = k \times P1 \quad (2)$$

$$C2 = M + (k \times Q) \quad (3)$$

So, we have C1 & C2 to send to the receiver at the encryption end.

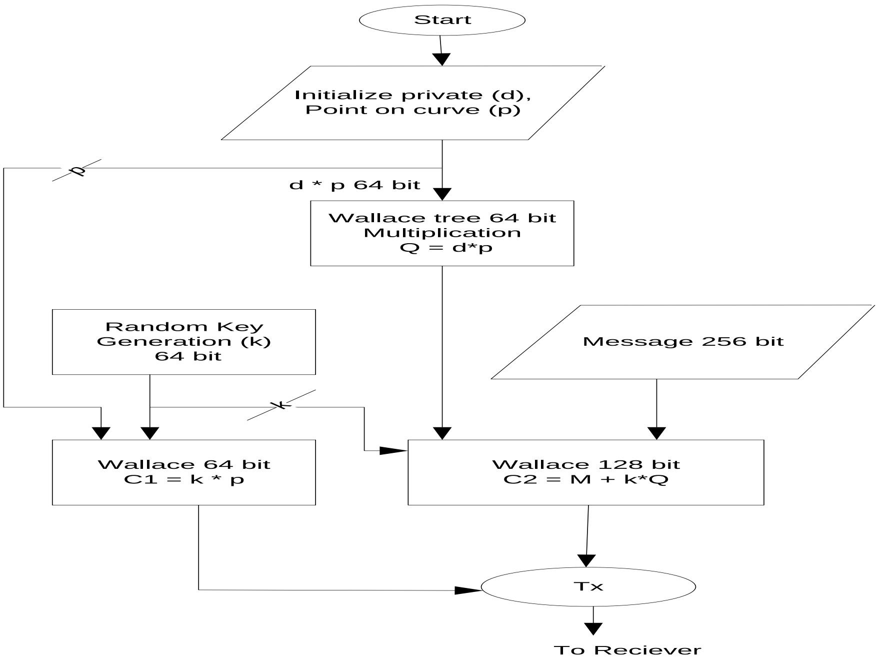

Start
Initialize private (d), Point on curve (p)
p
d * p 64 bit
Wallace tree 64 bit Multiplication Q = d*p
Random Key Generation (k) 64 bit
Message 256 bit
k
Wallace 64 bit C1 = k * p
Wallace 128 bit C2 = M + k*Q
Tx
To Reciever

**Figure.3** Encryption Flow Chart Using ECC Algorithm

Flow chart of encryption is given in Fig.3, where private key and points on elliptical curve are multiplied using Wallace tree multiplication method. The multiplied value is added with message to generate cipher text C2. Cipher text C1 is obtained by multiplying random key and points on elliptical curve. Both cipher texts C1 and C2 are transmitted.

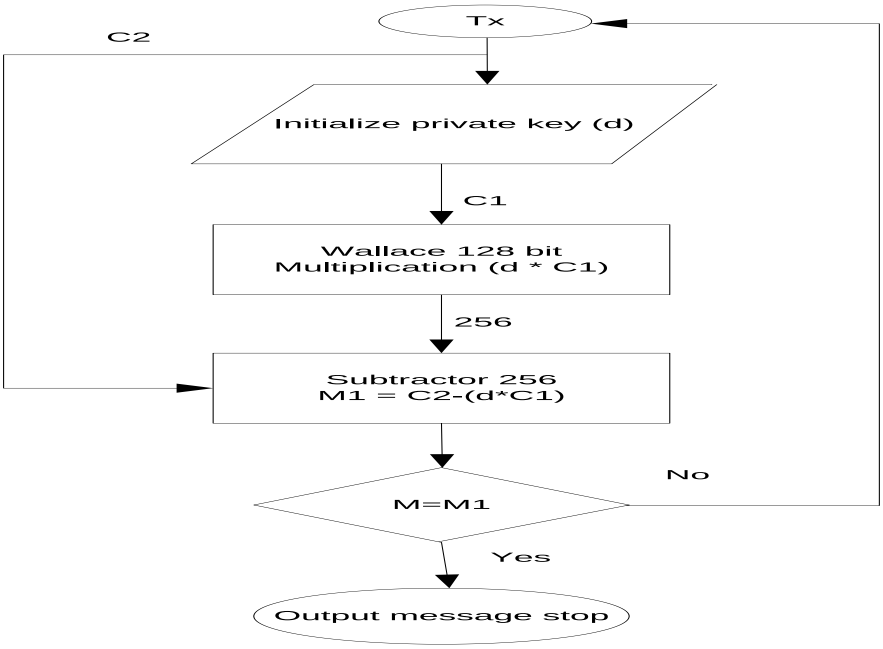

Tx
C2
Initialize private key (d)
C1
Wallace 128 bit Multiplication (d * C1)
256
Subtractor 256 M1 = C2-(d*C1)
No
M=M1
Yes
Output message stop

**Figure.4** Decryption Flow Chart at Receiver

The design flow of decryption at the receiver is shown in Fig.5, where cipher text C1 is multiplied by private key and subtracted from the cipher text C2 to obtain original message signal.

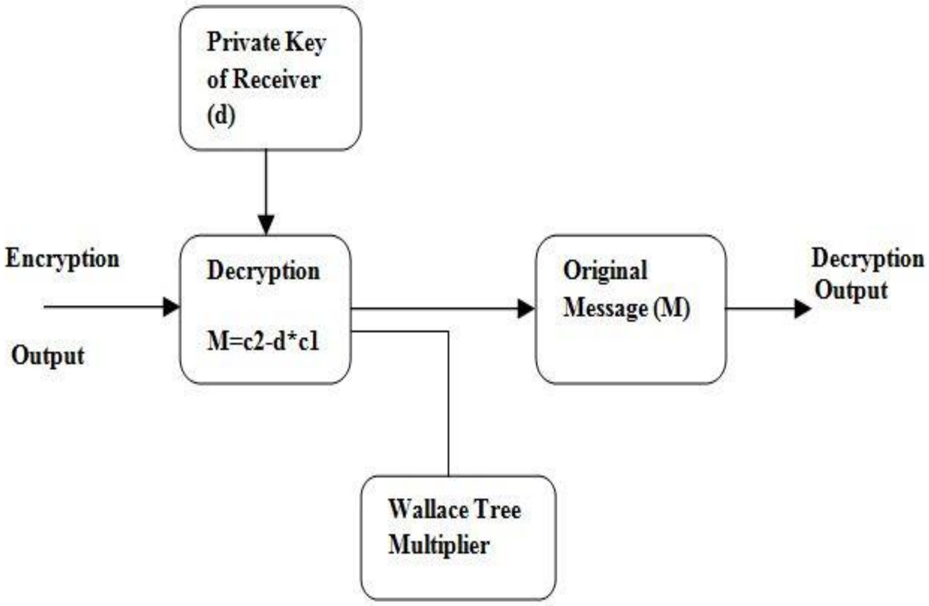


**Figure.5** Decryption Output of ECC Algorithm

**At Decryption** shown in Fig.5. Original message signal is given by
M = C2 – [d1 * C1] ---- (4)

***Wallace Tree Multiplier:***

Multipliers form a major part of DSP applications. Wallace presented an imperative iterative acknowledgment of parallel multiplier. This favorable position turns out to be more articulated for multipliers of greater than 16 bits. In Wallace tree design, every one of the bits of the majority of the incomplete items in every segment is including a lot of simultaneous counters without proliferating any conveys. A different arrangement of counters at that point diminishes this new framework, etc, until a two-push network is created.

The Wallace tree multiplier is the quick way to multiply two binary integers. It has three stages:

Stage 1: Partial products
Stage 2: Partial addition
Stage 3: Final addition

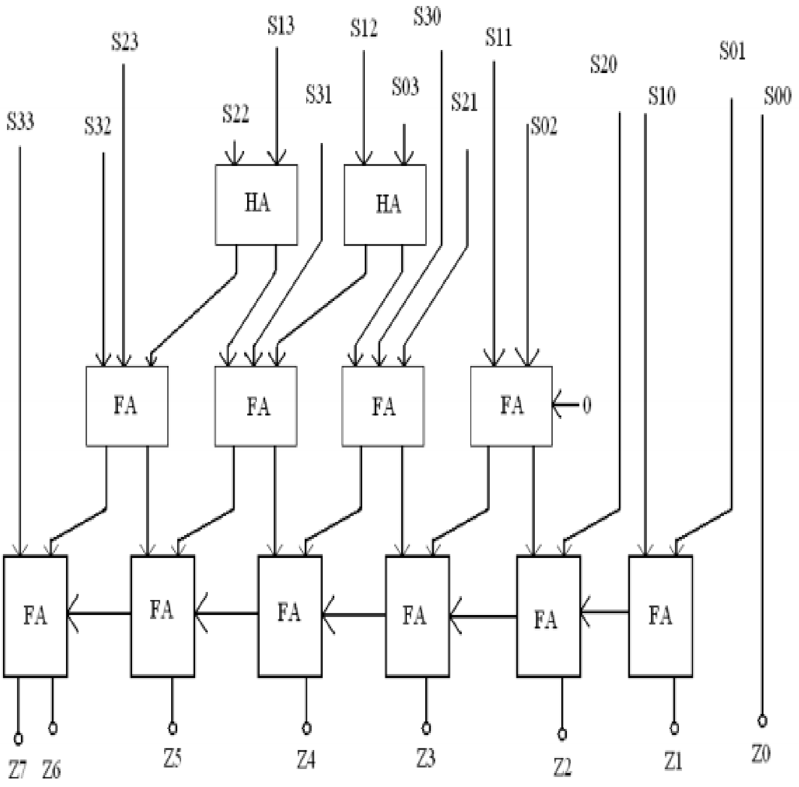


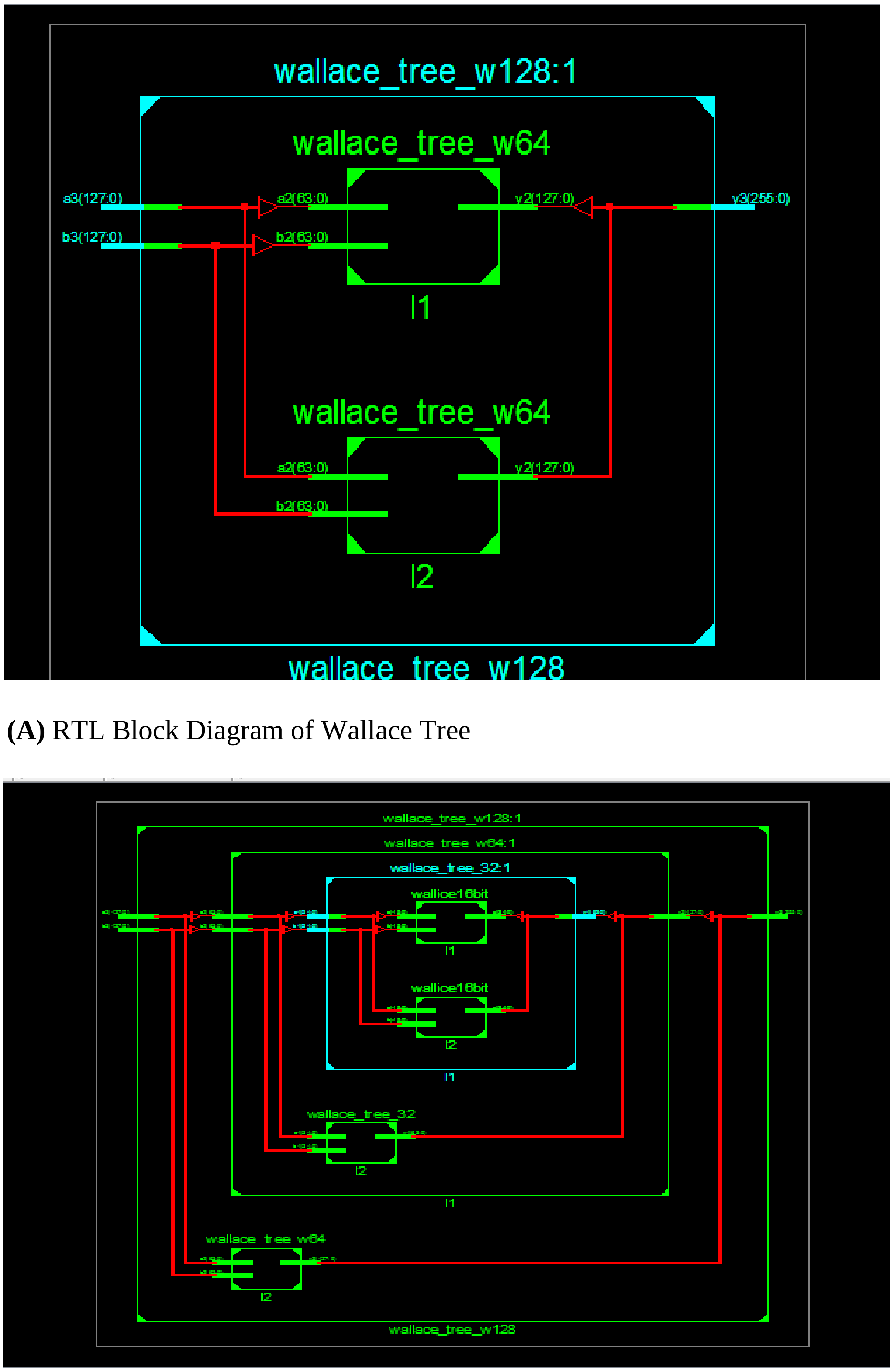
**Figure.6** Proposed Wallace Tree Multiplier

The most widely recognized counter utilized it's a 3:2 counter that's a Full adder. The benefit of Wallace tree is speed on the grounds that the expansion of fractional items is presently O (logN). A square outline of 4-bit Wallace Tree multiplier is appeared beneath.

Wallace tree multiplier uses full adder and half adder stages to reduce stages. This multiplier uses less power and its speed of switching is faster than other multipliers. In the proposed method a Wallace tree for 64bits is created and it is used simultaneously for 128bit multiplication. This technique reduces the number of LUT's and slices needed for the design which reduces the overall area needed for the design.

## RESULTS AND DISCUSSION

The implemented Wallace tree approach multiplier with RTL Schematic, simulation and hardware implementation are shown in the following figures. ECC design with Wallace tree multiplier implementation consumes 0.121 W power and area coverage number of slices LUTs is 8.14%. Figure 7(a) shows the RTL block diagram of Wallace tree and 7(b) shows the RTL Schematic of proposed 128*128 Wallace tree multiplier which is having the input a and b with 128 bits each and output y of 256 bits. Figure 8(a) shows the RTL block diagram of ECC algorithm encryption and 8(b) shows the RTL Schematic of proposed ECC algorithm encryption.



**(A)** RTL Block Diagram of Wallace Tree

**(B)** RTL Schematic of Wallace Tree

**Figure.7** (A) & (B) RTL Schematic of Proposed 128x128 Wallace Tree Multiplier

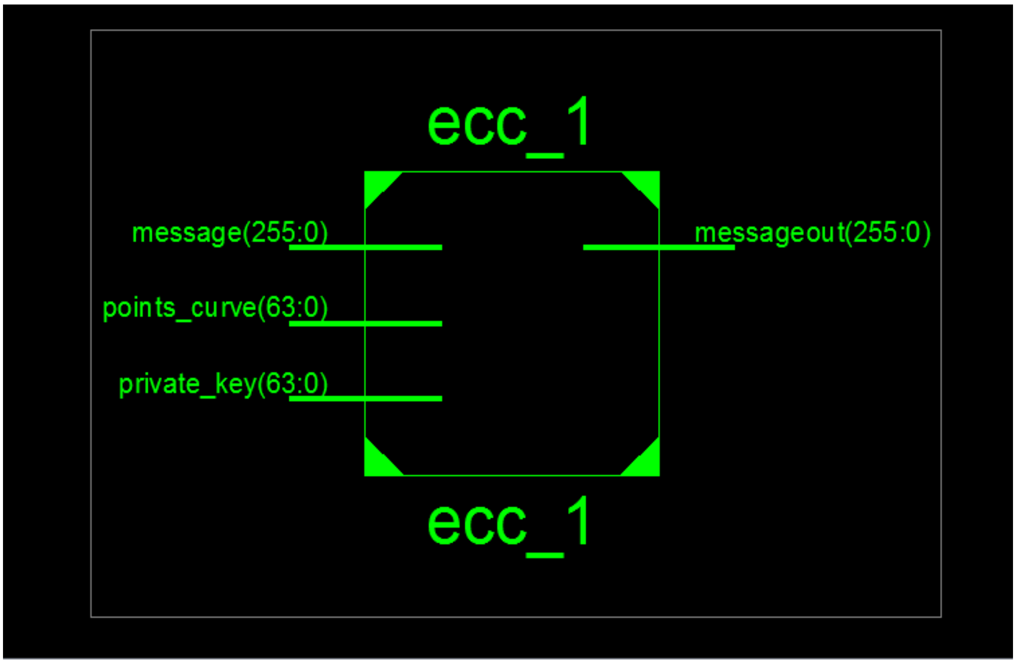


**Figure.8** (A) RTL Block Diagram of ECC Algorithm Encryption

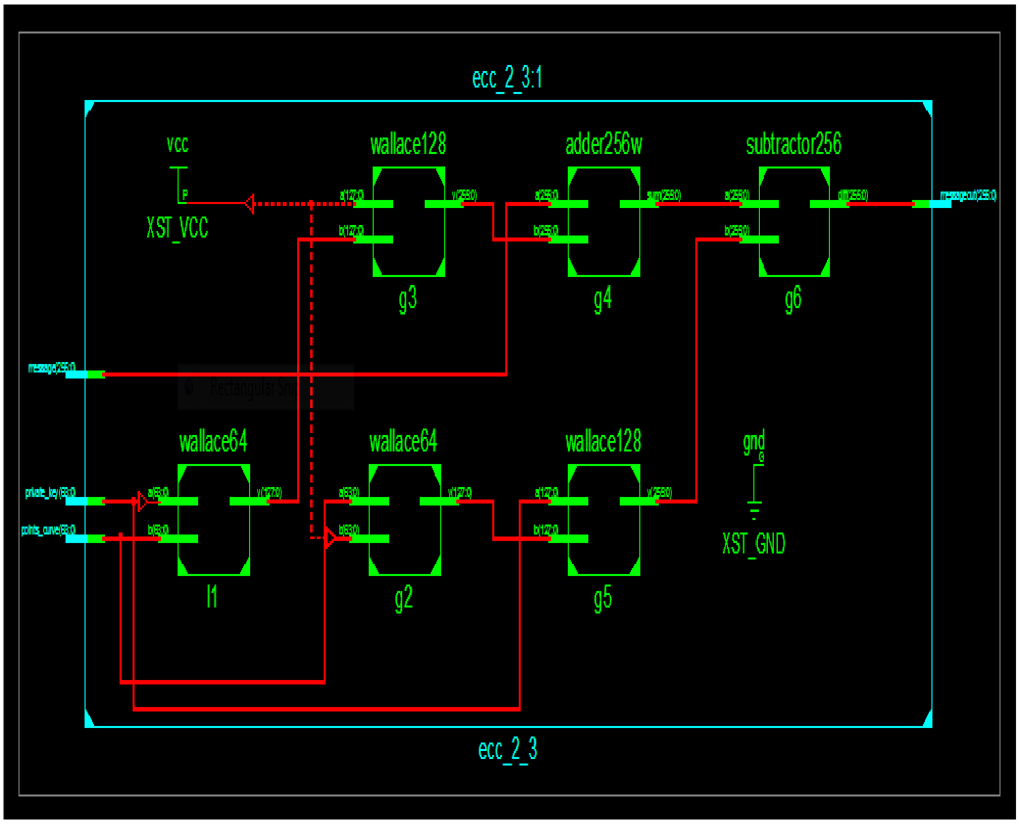
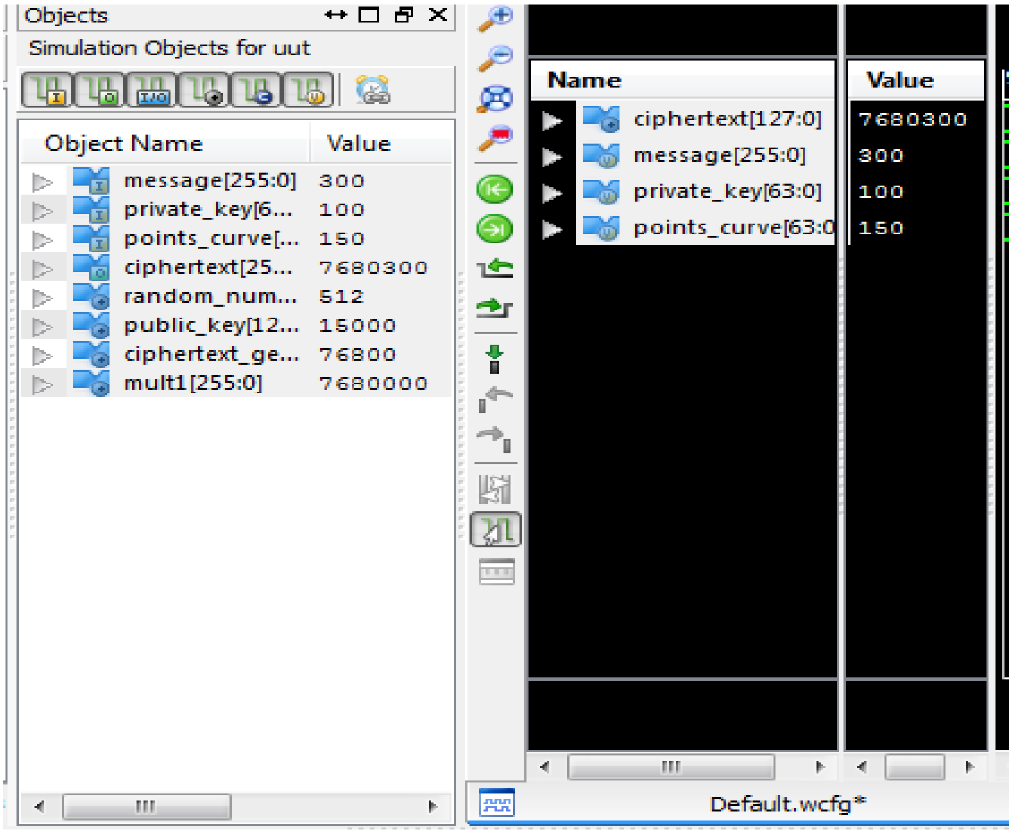


**Figure.8** (B) RTL Schematic of Proposed ECC Algorithm Design



Objects

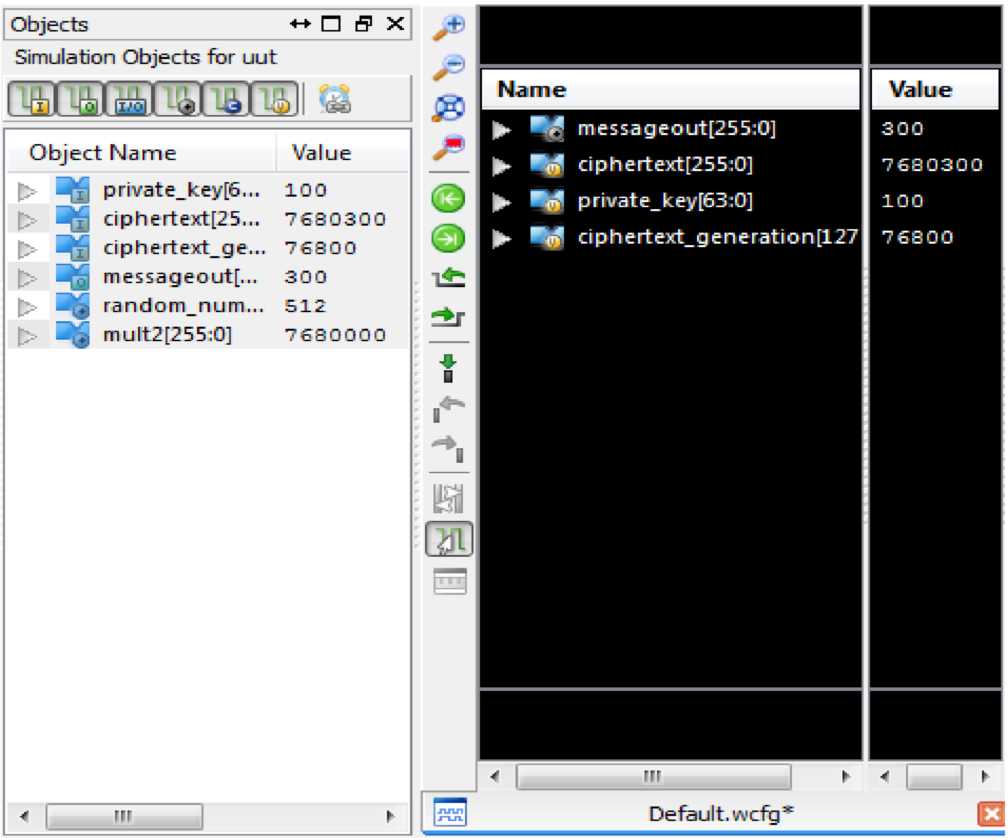
Simulation Objects for uut

| Object Name | Value |
|---|---|
| message[255:0] | 300 |
| private_key[6... | 100 |
| points_curve[... | 150 |
| ciphertext[25... | 7680300 |
| random_num... | 512 |
| public_key[12... | 15000 |
| ciphertext_ge... | 76800 |
| mult1[255:0] | 7680000 |

| Name | Value |
|---|---|
| ciphertext[127:0] | 7680300 |
| message[255:0] | 300 |
| private_key[63:0] | 100 |
| points_curve[63:0 | 150 |

Default.wcfg*

**Figure.9** Simulation Results for Proposed ECC Encryption Design



Objects

Simulation Objects for uut

| Object Name | Value |
|---|---|
| private_key[6... | 100 |
| ciphertext[25... | 7680300 |
| ciphertext_ge... | 76800 |
| messageout[... | 300 |
| random_num... | 512 |
| mult2[255:0] | 7680000 |

| Name | Value |
|---|---|
| messageout[255:0] | 300 |
| ciphertext[255:0] | 7680300 |
| private_key[63:0] | 100 |
| ciphertext_generation[127 | 76800 |

Default.wcfg*

**Figure.10** Simulation Results for Proposed ECC Decryption Design

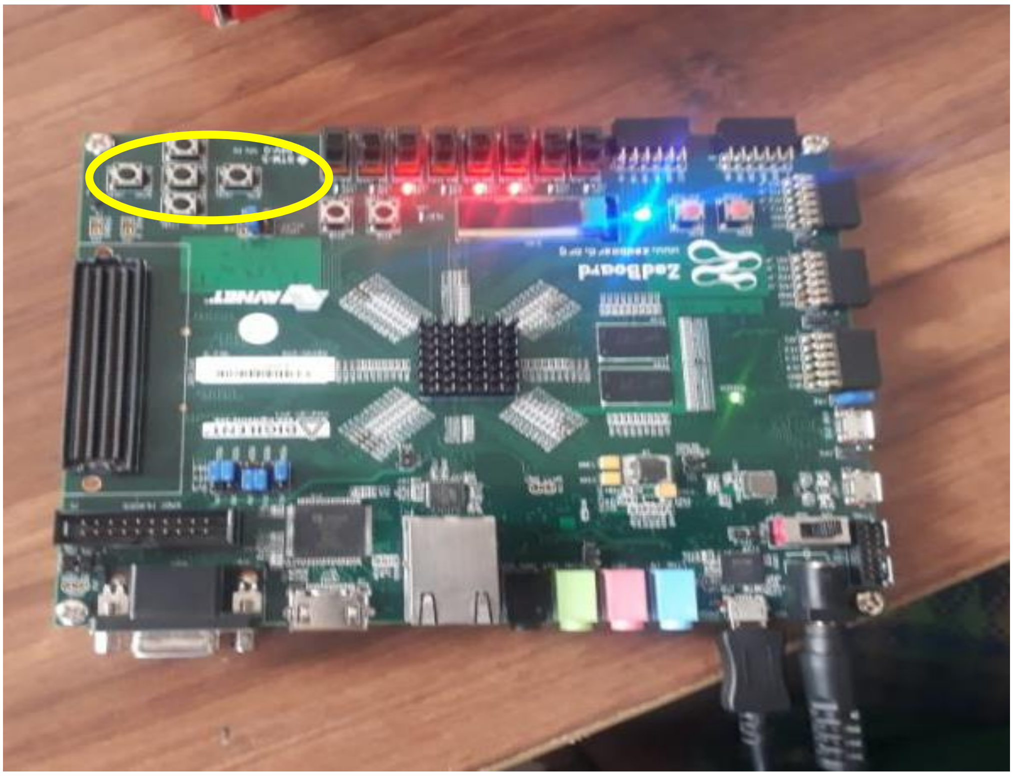


**Figure.11** On-Board Output

**Inputs:**

Message (M) = $(300)_{10}$(256 bit)
Private Key (d) = $(100)_{10}$ (64 bit)
Points on curve (p) = $(150)_{10}$ (64 bit)
Random number (k) = $(512)_{10}$ (64 bit)
Public key generation
(Q)=d*p
=100*150=15000 (64-bit multiplier used)
Cipher text
(c1) =k*p=512*150=76800
Cipher text
(c2) =M + (k*Q)
=300+(512*15000) =7680300(Encryption output)

**Output**:

Message output
(M)=c2-(d*c1)
=7680300-(100*76800) (128-bit multiplier used)
Output =300(Decryption output 256 bit)
= $(100101100)_2$

**Table 2.** Area Comparison Between Vedic &Wallace Tree Multipliers

| Multipliers | Number of slices | Number of 4-input LUT's | No. of bounded IOB's |
|---|---|---|---|
| ECC Design with Vedic Multiplier | 4656 | 9312 | 16 |
| ECC Design with Wallace Tree Multiplier | 1760 | 4331 | 128 |

Table 2 gives the comparison between Wallace tree multiplier and Vedic multiplier approach. Proposed approach consumes a smaller number of Look up tables, and slices when compared to Vedic approach. Even number of inputs is increased in proposed method, it still consumes less area. For implementation IPs are used. While showing the results on the Zed board only last 8-bits are displayed i.e. $(00101100)_{2}$ as shown in Fig.11.

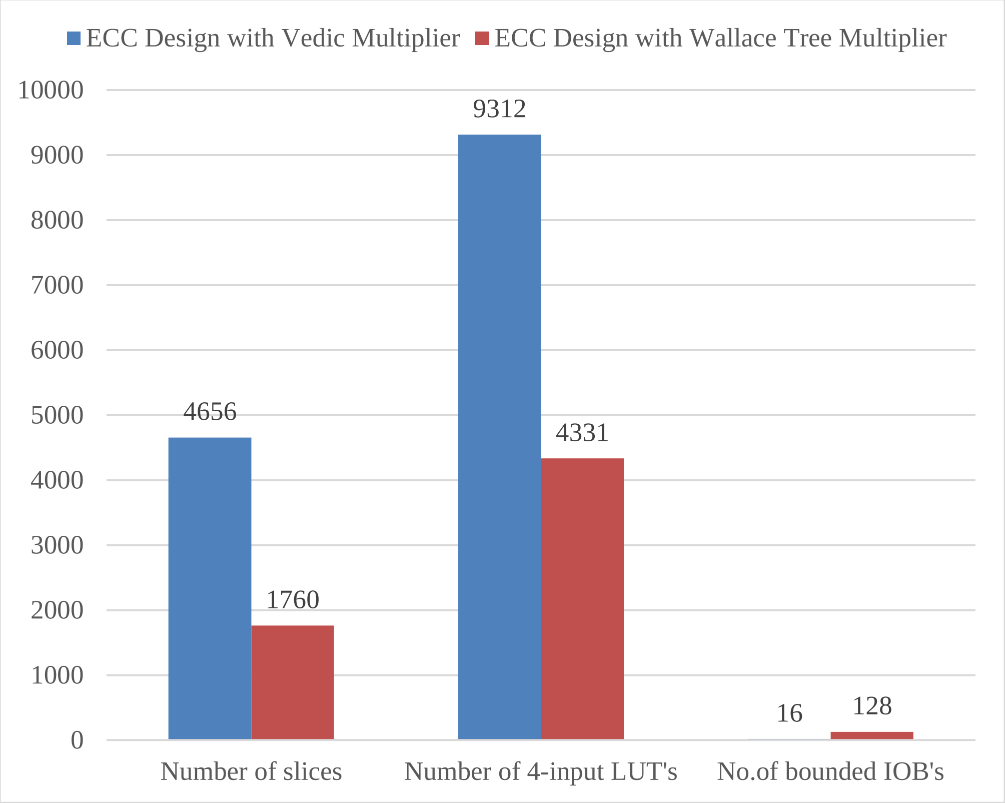


**Figure.12** Comparison of LUT’s, IOB’s

Table: 3. shows that Wallace tree approach consumes less delay, when compared to Vedic due to reduction of partial products that are required. Fig.13 shows the wast difference in delay between both approaches and the proposed method is much faster. The power required for the proposed design is very approximately 4 times less, which makes the approach more suitable for continuous usage.

**Table:3.** Delay and Power Comparison.

| Design | Delay(ns) | Power(W) |
|---|---|---|
| ECC Design with Vedic Multiplier with 16-bits | 8.23ns | 0.518W |
| ECC Design with Wallace Tree Multiplier with 128-bits | 0.7ns | 0.121W |

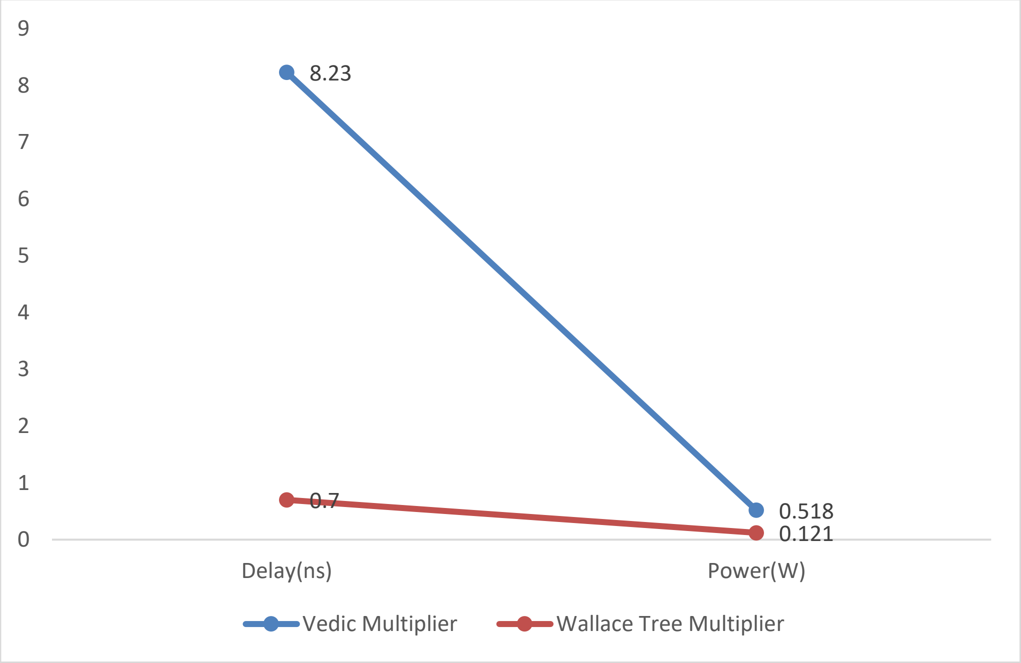


**Figure.13** Comparison Between Vedic and Wallace Tree

## CONCLUSION

The Wallace tree multiplier is implemented in this study utilizing a single point ECC approach. By utilizing this, space and electricity is lessened considerably. Encryption is critical anywhere there is communication. When compared to the RSA method, the ECC Algorithm gives faster performance due to smaller key sizes for encryption and decryption. The Wallace tree multiplier delay is compensated for by utilizing ECC rather than RSA. The ECC method is used to implement cryptography for 128 input bits. The Wallace tree multiplier is used to build the ECC algorithm. It was created in Xilinx Vivado with Verilog code and then simulated, synthesized, and implemented on a Z-board.

"The authors declare no conflict of interest."

## REFERENCES

Rooban.S, Saifuddin.S, Leelamadhuri.S, "Design of fir filter using wallace tree multiplier with kogge-stone adder" International Journal of Innovative Technology and Exploring Engineering,2019.

Nawari, Mustafa, et al. "Fpga based implementation of elliptic curve cryptography." Computer Networks and Information Security (WSCNIS),2015 World Symposium on. IEEE, 2015.

Bobade, Sunil Devidas, and Vijay R. Mankar. "VLSI architecture for an area efficient Elliptic Curve Cryptographic processor for embedded systems." Industrial Instrumentation and Control (ICIC), 2015 International Conference on. IEEE, 2015.

T. Wollinger, J. Guajardo, and C. Paar, "Security on FPGA: state of the art implementations and attacks, "ACM Transactions in Embedded Computing Systems, vol.3, pp.53-59, 2004.

Amir Moradi, Alessandro, Barenghi, Christof paar and Timo Kasper, “On the Vulnerability of FPGA Bit stream Encryption against Power Analysis Attacks” Proceedings of the 18th ACM conference on Computer and communications, pp: 111-124, October2011.

A. Kaleel Rahuman, Dr. G. Athisha, "Reconfigurable Architecture for Elliptic Curve Cryptography," Proceedings of the International Conference on Communication and Computational Intelligence, pp.461-466, December-2010.

Reza Azarderakhsh and Koray Karabina,"A new double point multiplication algorithm and its application to binary elliptic curves with endomorphism", IEEE Transactions on Computers, No.99, May 2013.

Kiran Kumar Mandrumaka, M. Mounika, Fazal Noorbasha, “Design and Testing of 16-bit Carry Save Adder using Reconfigurable LFSR”, IJATCSE, Volume 9, No.5, September - October 2020.

High-Performance Wallace Tree Multiplier K.K. Senthil Kumar*, S. Yuvaraj **, R. Seshasayanan*International Journal of Computer Techniques -– Volume 7, Issue 01, February, 2020

2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON) Indian Institute of Technology (Banaras Hindu University) Varanasi, India, Dec 9-11, 2016. FPGA Implementation of Complex Multiplier Using Minimum Delay Vedic Real Multiplier Architecture. K. Deergha Rao, Ch. Gangadhar, Praveen K Korrai.

Modified wallace tree multiplier using efficient square root carry select adder. Damarla Paradhasaradhi; M. Prashanthi; N Vivek. 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE) Date of Conference: 6-8 March 2014.Date Added to IEEE Xplore: 16 October 2014. Electronic ISBN:978-1-4799-4982-3. DVD ISBN:978-1-4799-4983-0. INSPEC Accession Number: 14665845. DOI: 10.1109/ICGCCEE.2014.6922214. Publisher: IEEE. Conference Location: Coimbatore, India

Low power ASIC implementation of signed and unsigned wallace-tree with vedic multiplier using compressors. Published in: 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon). Date of Conference: 17-19 Aug. 2017.Date Added to IEEE Xplore: 14 May 2018.INSPEC Accession Number: 17754757. DOI: 10.1109/SmartTechCon.2017.8358471. Publisher: IEEE Conference Location: Bengaluru, India

Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications. 2017

IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS). Date of Conference: 13-15 Nov. 2017. Date Added to IEEE Xplore: 04 January 2018. INSPEC Accession Number: 17484810. DOI: 10.1109/COMCAS.2017.8244805. Conference Location: Tel-Aviv, Israel.

ICICES2014 - S.A. Engineering College, Chennai, Tamil Nadu, India. ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE. Secured Elliptic Curve Cryptosystems for Scan Based VLSI Architecture. Mr.K.P. Sridhar1, Mr. M. Raguram1, Mr. B. Prakash1, Mr. S. Koushighan.

High Performance Vedic Approach for Data security using Elliptic Curve Cryptography on FPGA. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018) IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4. Prashant Ahuja, Prof. Hiren Soni.

Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module. IEEE Transactions on Computers (Volume: 69, Issue: 11, Nov. 1 2020) Page(s): 1707 – 1718.Date of Publication: 05 August 2020. INSPEC Accession Number: 20022882. DOI: 10.1109/TC.2020.3013266