International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

Design of Light Cipher Cryptographic Algorithm Computation Block Using Verilog for IoT Applications

Dr. Yasha Jyothi M Shirur, Nithin Iyer K S, Sujay K S, Uday V N

Professor of Dept. of ECE, B N M Institute of Technology, Bangalore, Karnataka.
Students from Dept. of ECE, B N M Institute of Technology, Bangalore, Karnataka.

Date of Submission: 21-11-2022 Date of Acceptance: 30-11-2022

ABSTRACT: This project provides the algorithm for efficient and easy to implement point multiplication in ECC. The ECC algorithm works on the elliptical curve arithmetic for each and every step of the encryption and decryption process. This makes the algorithm more secure from the attacks compared algorithms.

KEYWORDS:Left to Right point Multiplication, Scalar Multiplication, Elliptic Curve Cryptography.

I. INTRODUCTION

Cryptography or cryptology refers to the study and application of techniques for secure communication in the environment of adversarial behaviour. Data is encrypted and decrypted using two separate keys that are mathematically connected in asymmetric encryption. The public key and private key are the two keys. The user's encryption and decryption are carried out utilising these two keys, as indicated in Figure-1, to exchange the public key.

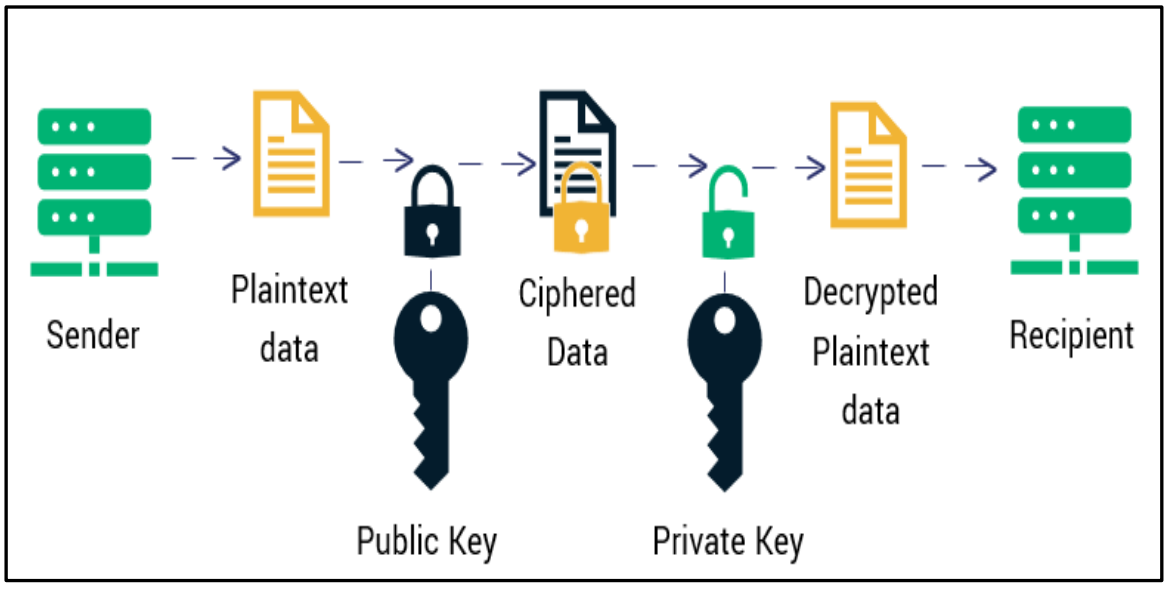

Figure 1. Asymmetric Encryption

I. Elliptic Curve Cryptography

In the middle of the 1980s, Koblitz and Miller developed the encryption technique known as Elliptic Curve Cryptography (ECC). As seen in Figure-1, it is a type of public key encryption. It is based on the theory of elliptic curves, which is used

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

to produce faster, smaller, and more effective cryptographic keys. Instead of multiplying extremely large prime numbers, ECC creates the keys using the elliptic curve equation. Due to the discrete logarithmic problem, it is nearly impossible to decrypt ECC encrypted text and is exceedingly tough to do. The elliptic curve stretches to infinity and is difficult to determine the points as shown in Figure-2. Hence it is confined to a certain point by using a modulus operation, as shown in Figure-3.

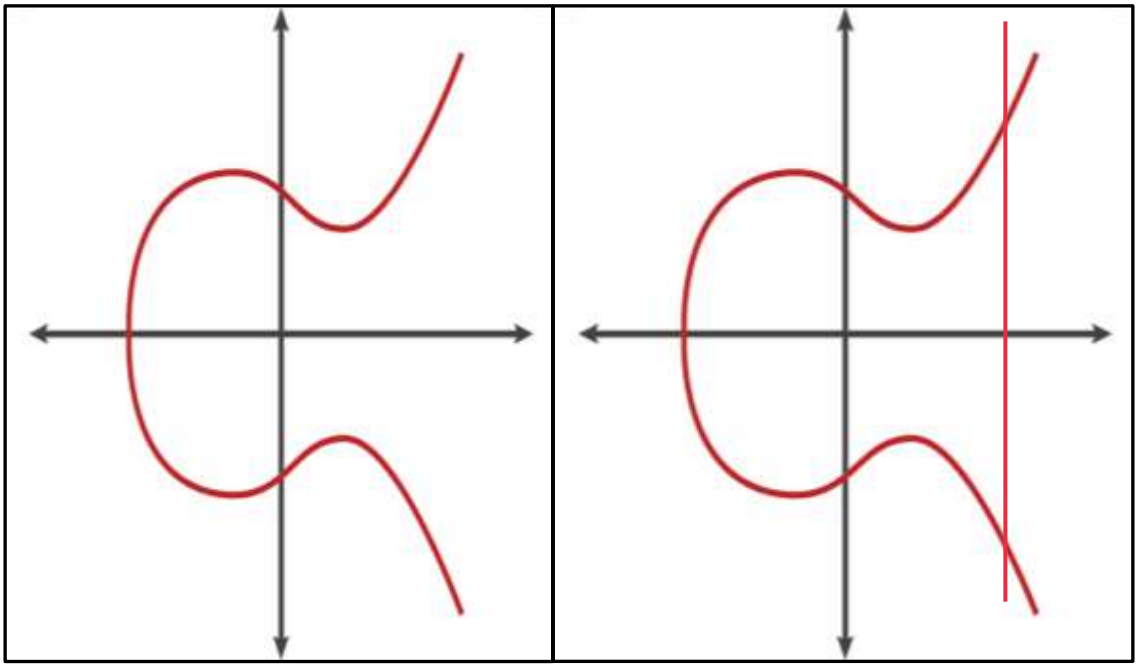

Figure 2. Elliptic CurveFigure 3. Elliptic Curve with Mod operation

II. Ecc Hierarchical Model

Figure 4 illustrates a hierarchical model with four layers that can be used to depict the ECC. Basic mathematic operations are computed at the top layer. Point doublings and additions are computed at layer 2. The major operation, scalar/point multiplication, is computed at layer 3. Elliptic Curve encryption and decryption are implementations of protocols found in layer 4.

This model's implementation starts at Level 1, where the fundamental arithmetic operations are carried out, and mod operations are carried out on this fundamental level itself. These fundamental modules are implemented and tested, and then the point addition and point doubling levels use them. However, only point addition and point doubling are used now to carry out the point multiplication. Lastly, point doubling, point multiplication, and point addition are used at layer 4. Our focus is on point multiplication.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

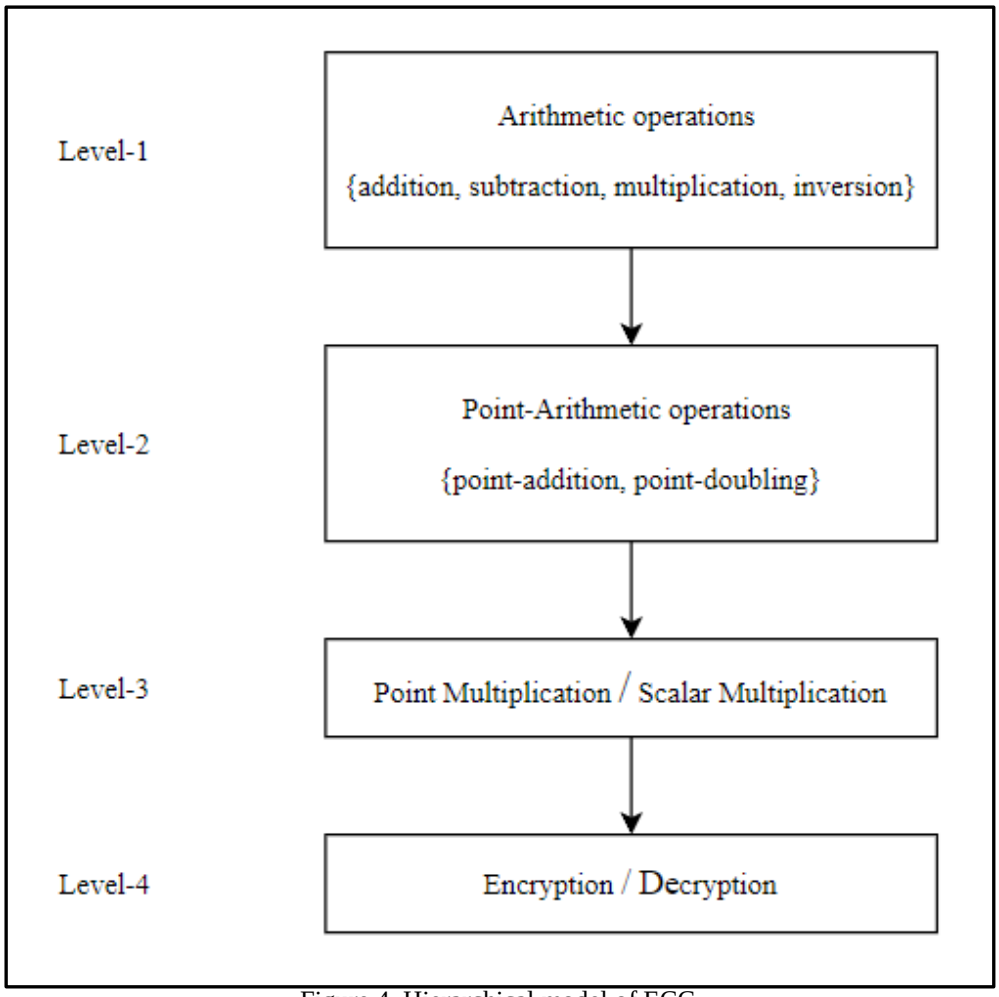

Figure 4. Hierarchical model of ECC

Scalar / Point Multiplication

The point multiplication layer is the third layer of the hierarchical model. This module uses ECC mathematic techniques to multiply a scalar quantitywith a point. The module receives a point coordinate and a scalar as inputs, and it outputs the result as a point coordinate. Points are multiplied by constantly doubling and accumulating them. The layer-2 functions of the hierarchical model of ECC, as illustrated in Figure 4, are point addition and point doubling, which are both used in the left to right algorithm.

Algorithm for Left to Right Point Multiplication:

STEP 1: START
STEP 2: Identify the first MSB bit which is 1, ignore the bit and go to Step 2.
STEP 3: If the next MSB is 1 then perform both point_double and point_add
STEP 4: If the next MSB is 0 then perform only point_double
STEP 5: Ignore the current bit and shift to the next MSB
STEP 6: Repeat Step 2 until the LSB is reached
STEP 7: STOP

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

Flowchart for Point Multiplication:

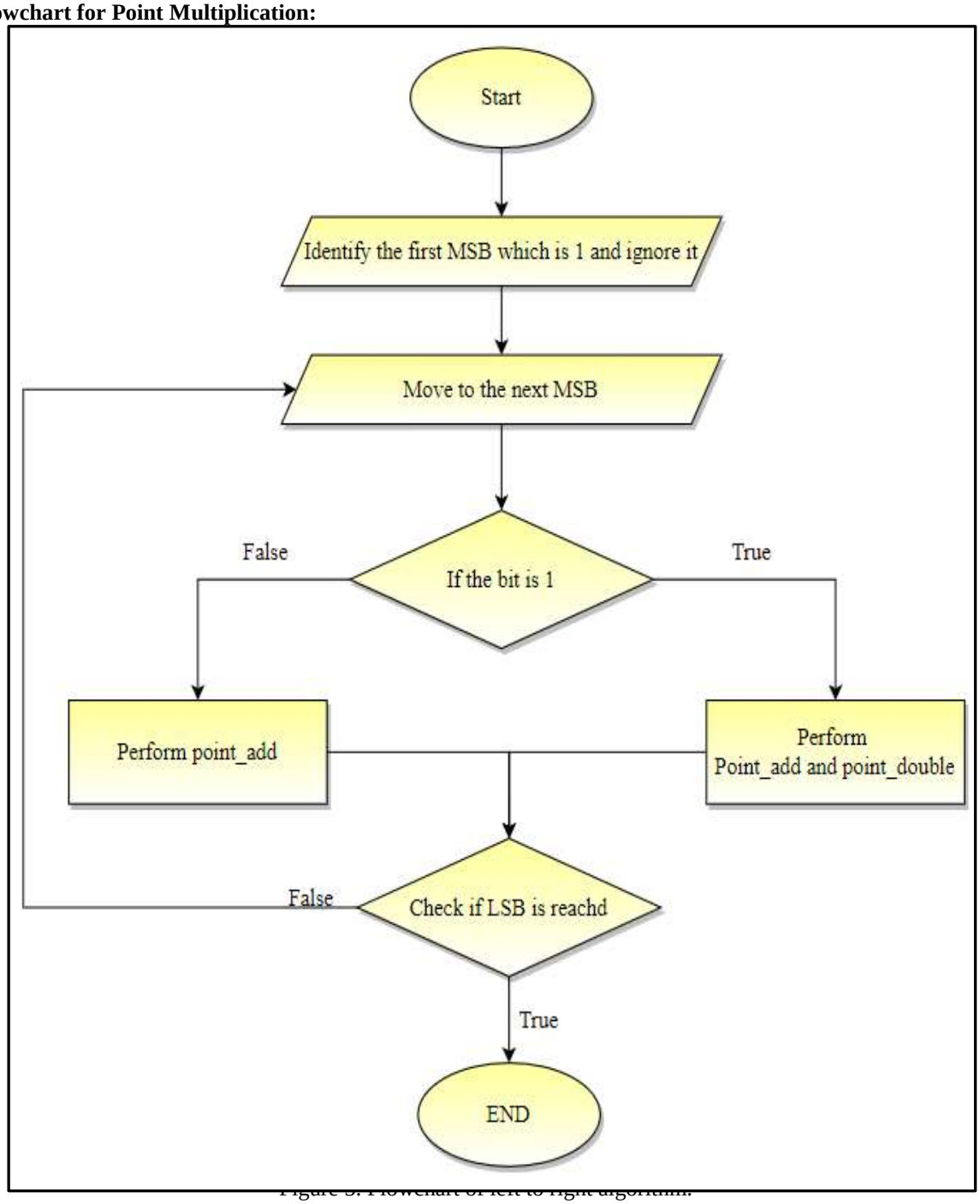

Figure 5. Flowchart of left to right algorithm.

The visual representation for carrying out the previously mentioned left to right algorithm is shown in figure 5. It is crucial to note that the scalar must be converted into its binary form for this algorithm to function, and that this binary number will be used to repeatedly point-add and point-double the input point to obtain the output.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

III. Ecc Design Methodology

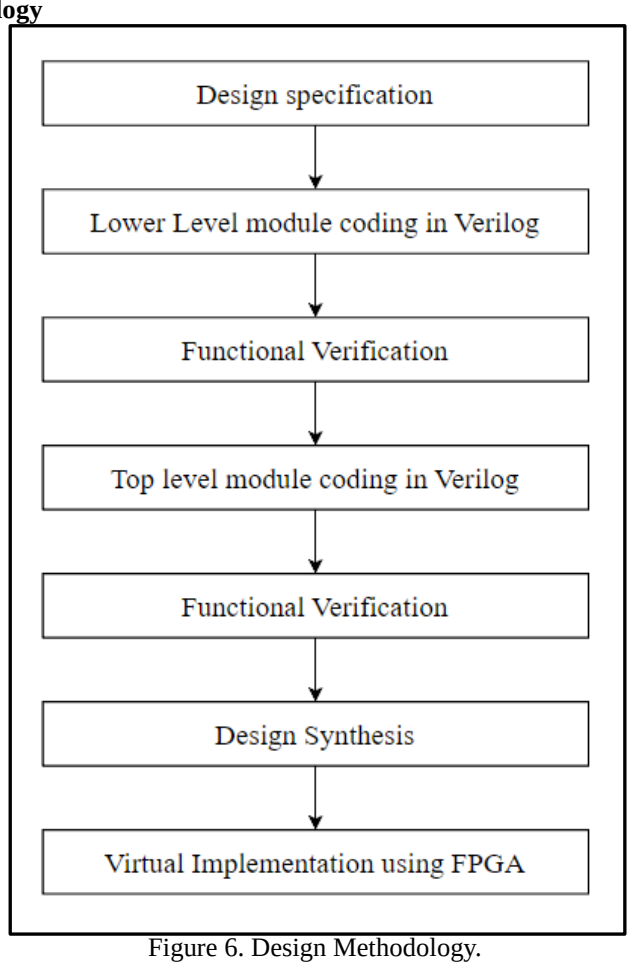

Figure 6. Design Methodology.

The design objectives are first noted, followed by the coding of the Point-Arithmetic operations while focusing on a single module at a time, and the testing and validation of each module's functionality. As shown in the flowchart in Figure-6, the top layer module is next built by appropriately integrating the lower-level modules and recalled whenever needed. This integrated module is then tested and approved.

The Xilinx Vivado HLx application is used to do a virtual implementation once the design code has been synthesised with the cadence tool.

IV. Test Cases

As was previously discussed, point multiplication (ECC Arithmetic point multiplication) requires two inputs: a point coordinate and a scalar, both of which must be multiplied to produce another point as an output.

Consider a test case where the scalar is K = 20 and the point to be multiplied with is q = (20 , 20). And after the multiplication, the result is Q = (20, 12), as depicted in Figure 8.

Normal decimal multiplication is repetitive addition of the number with itself it can be considered the same with elliptic curve arithmetic but here the point is added with itself using point addition for a number of times. Hence by substituting normal point addition with left-to-right multiplication, the number of computations can be reduced. Previously, the computations used 20-point additions; however, this has been simplified to a 1-point addition and a 4-point doubling. As show in Figure 7 and summarised in Table 1.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

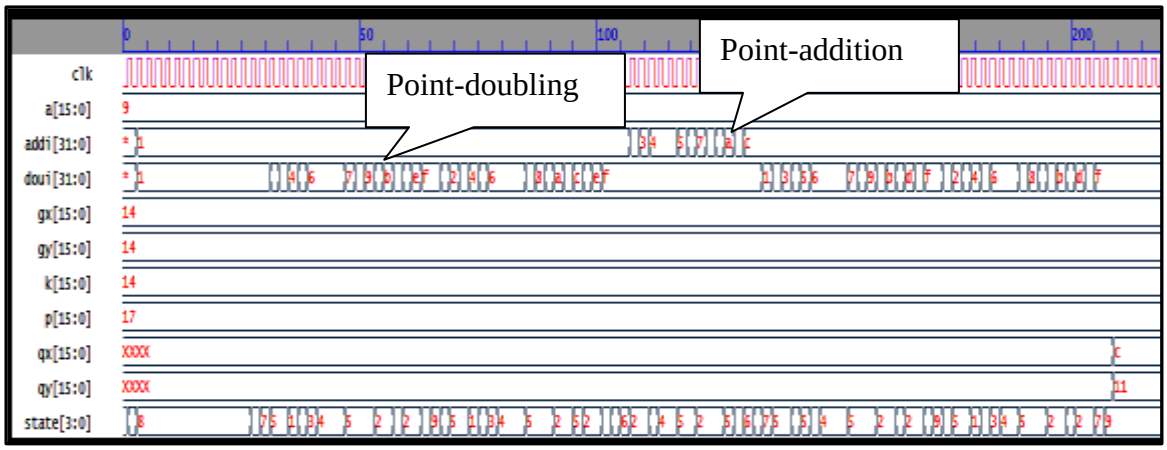

Figure 7. Test case for Point multiplication

```
K =    20, a = 9 , p = 23
gx =    20(0014)  gy =    20(0014)
Qx =    20(xxxx)  Qy =     x(xxxx)     x
K =    20, a = 9 , p = 23
gx =    20(0014)  gy =    20(0014)
Qx =    20(000c)  Qy =    12(0011)    17
```

Figure 8. Output of point multiplication

II. CONCLUSION

Table 1 Comparison between Standard and Implemented scheme

Scheme	**Computations**
Standard method	20 (point additions)
Implemented method	5 (4 point doubling and 1 point addition)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 971-977 www.ijaem.net ISSN: 2395-5252

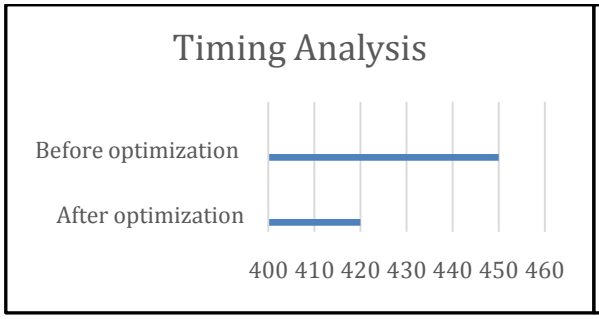

Figure 9. Timing report

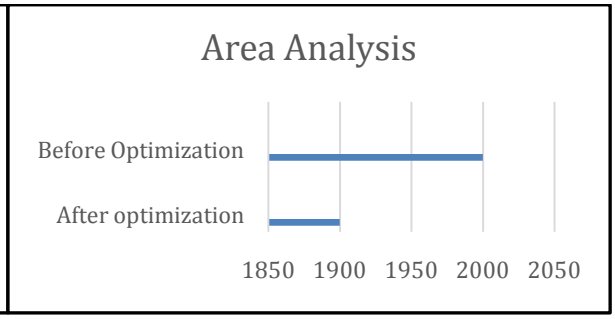

Figure 10. Area report

The two mentioned reports demonstrate how the module can be improvised after being optimised with constraints. Efficiency is greatly improved when speed and area are prioritised, but there is a trade-off with power. The power consumption of this optimization has increased. Thus, this design can only be used wherever speed and area are given top priority.

From Table 1 also shows that the number of computations has been significantly reduced for a 4-bit number and that this algorithm significantly reduces the number of computations when more bits are implemented.

REFERENCES

[1] Martin Ekera, "Computing information on domain parameters from public keys selected uniformly at random"
[2] Malik Imran, Imran Shafi, Atif Raza Jafri, Muhammad Rashid, "Hardware Design and Implementation of ECC based Crypto Processor for Low area applications on FPGA"
[3] Tanja Lange, "A note on L´opez-Dahab coordinates"
[4] Thammaneni Snehitha Reddy, Y. David Solomon Raju, "Implementation of Data Security with Wallace Tree Approach Using Elliptical Curve Cryptography on FPGA"
[5] Sharad Kumar Verma, Dr. D.B. Ojha, "A Discussion on Elliptic Curve Cryptography and Its Applications"
[6] Xianmin Wei, Peng Zhang, "Research on Improved ECC Algorithm in Network and Information Security"
[7] Nelson Josias G. Saho, Eugène C. Ezin "Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm"
[8] Anoop MS, "Elliptic Curve Cryptography an Implementation Guide"
[9] Rajesh Mohan, "Project: Elliptic Curve Cryptography"
[10] Samir Palnitkar, "Verilog HDL: A Guide to Digital Design and Synthesis", Pearson Education,Second Edition