International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 5, May-2018

DLL BASED MONTGOMERY MODULAR MULTIPLICATION

MD. Shakeeel[1], Dr. M. Venkata Sudhakar [2]
[1] *M. Tech, LBRCE, L.B. Nagar, Mylavaram-521230, Andhra Pradesh, India.*
[2] Professor, LBRCE, L.B. Nagar, Mylavaram-521230, Andhra Pradesh, India.

***Abstract*— Montgomery modular multiplication is rapidly used in cryptographic algorithms and DSP applications. The main objective of this paper is to lessen the delay and area of the multipliers while maintaining less hardware complexity. To speed up, high-speed Montgomery modular multiplication algorithms and hardware architectures employed which increases hardware complexity. This paper describes Design and Implementation of Dual Level Logic(DLL) based Montgomery modular multiplication on FPGA. This proposed, designed architecture provides 42.206ns of delay and occupies 4% of the total memory on FPGA. This architecture has been modeled with Verilog in Xilinx ISE Design Suite 14.7.**

***Keywords*—Dual Logic Level (DLL), Montgomery Modular Multiplication, FPGA, Public key cryptography system.**

I. INTRODUCTION

The data security will play a crucial role in many future computer and communication systems [1]. The fundamental security requirements include confidentiality, authentication, data integrity, and non-repudiation. To provide such security services, most systems use public key cryptography. In public key cryptography algorithms, the essential arithmetic operation is modular multiplication, which is used to calculate modular exponentiation. In public key cryptography algorithms, the essential arithmetic operation is modular multiplication, which is used to calculate modular exponentiation.

The increase in data communication and internet services like electronic commerce, the security occupies a vital role over the internetwork. Public key cryptosystems by Rivest, R.L., et al [2] provides data security to such networks. In these cryptosystems, modular multiplication (MM) plays an essential role in arithmetic functions. To enhance security, MM with large integers is preferred. Montgomery multiplication proposed by Montgomery.P.L.is one of the fast algorithms to carry out the MM more quickly. This algorithm determines the quotient only depending on the least significant digit of operands and replaces the complicated division with a series of shifting modular additions. Montgomery MM is given by=A*B*R-1(Mod N) where N is the k-bit modulus, R-1 is the inverse of R modulo N, $R \times R^{-1} = 1 \pmod{N}$ and $R = 2^k \bmod N$. Hence it can be easily implemented to speed up the encryption and decryption process in VLSI circuits. Long carry propagation is a major problem in performing addition for large operands in binary representation. To solve this problem, several approaches based on carry save addition were proposed to achieve a significant speedup of Montgomery MM. Based on the representation of input and output operands, these approaches can be roughly divided into semi-carry-save (SCS) strategy and full carry-save (FCS) strategy. The single shift operation in Montgomery Modular multiplication algorithm will reduce the time complexity and results in faster encryption and decryption. If the operands are larger value there would be longer carry propagation. So by having a methods like Full Carry Save (FCS) [4] and Semi Carry Save (SCS) [5, 6] provides the advantage of faster carry calculation leading to time complexity reduction of whole algorithm.

II. DLL MONTGOMERY MODULAR MULTIPLICATION

The high-performance dual logic level multiplier gives the less delay. A dual logic level shares its logical operation depends on the preference of the logical operation is executed. It consists of the three layers, and the parts are depending on the bit size. In 2-bit size there are 3 Parts in 3-bit size there are 5 parts and 4-bit size there are 7 parts increase the bit size the parts are double in the architecture. In the architecture, the primary operation depends on the third layer. In the third layer, there are two levels of operations can be done. In that depend on the preference one level of operation is performed and the second one vice versa.

In the internal operation of 2 x 2 dual logic level multiplier, it consists of three layers and three parts shown in Figure The inputs are given to the first layer in the first part a0, b0 inputs given to the first layer AND gate and the result goes down. In the second parta0, b1 and a1, b0 inputs are given to the first layer two AND gates the outputs of the AND gates are given to the inputs of the second layer multiplexer. In this multiplexer two operations are performed XOR, AND.

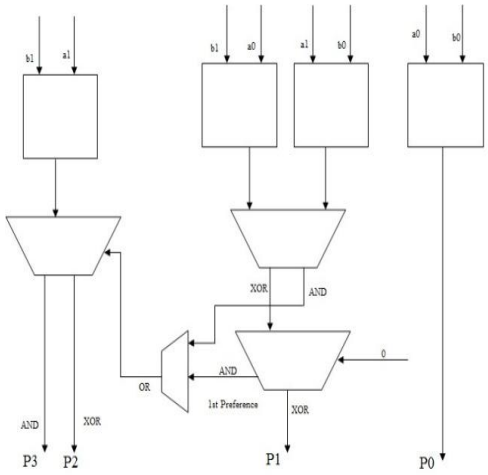

Fig 1. 2 x 2 Architecture of Dual Logic Level Multiplier

The multiplexer has two outputs one output is XOR and the second output is AND the XOR output is given to the one input of the third layer multiplexer, AND output is given to the one input of the third layer OR gate. In this Dual Logic Level Multiplier, architecture operation depends on the third layer. In this third layer, XOR AND operations are performed the XOR operation performed five gates are used to the done operation, but in the AND operation only one gate is used. So in the third layer first preference is going to AND gates next the XOR gate to perform the operations. In the third layer multiplexer XOR output goes down AND output is given to the one input of OR gate and the second input of the OR gate is coming from second layer multiplexer AND output. In the third part first layer inputs a1, b1 is given to the AND gate, and the output is given to the second layer multiplexer and the second input is coming from third layer OR gate output. There are two outputs of the multiplexer are goes down. This is the total internal operation of the 2x2 Dual logic Level Multiplier it has four outputs 2 x m in the 2x2 multipliers 2x2 = 4 outputs where m is either multiplier or multiplicand. In the 4 x4 multipliers having 8 outputs, the following figure shows the architecture of the 4x4 Dual Logic Level.

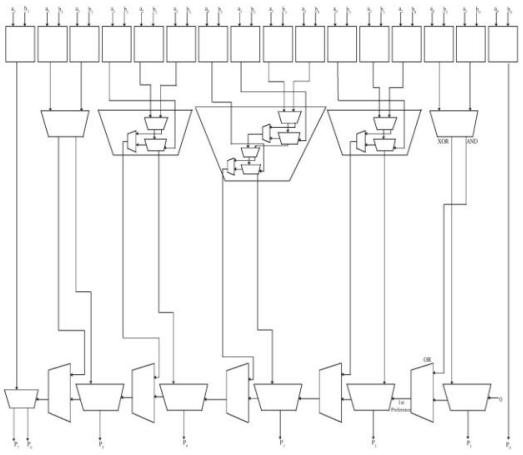

Fig. 2. 4 x 4 Dual Logic Level architecture

In the architecture of 4 x 4 Dual Logic Level Multiplier consists of three layers and seven parts each layer having different blocks perform different logical operations shown in Figure 2. The same operation is performed as 2 x 2 Dual Level Logic Multiplier. In this Multiplier having 2 x m outputs that are eight outputs. As compared to previously existed system technique the area is reduced in this technique. This technique for every bit operation is having three layers and parts are increased but in existed system parts and are layers increased. The main advantage of this Dual Logic Level technique the area is reduced and speed is increased as compared to existed system.

III. RESULTS AND DISCUSSION

The simulation results of the DLL based Montgomery modular multiplication is implemented in ISim simulator in Xilinx. The RTL schematic of 32-Bit DLL is shown in Figure 3. The Technology schematic of the 32-Bit DLL is shown in Figure.4. The Simulation Result of the 32-Bit DLL is shown in Figure.5. Table1. Shows the comparison of parameters between previous method and proposed method.

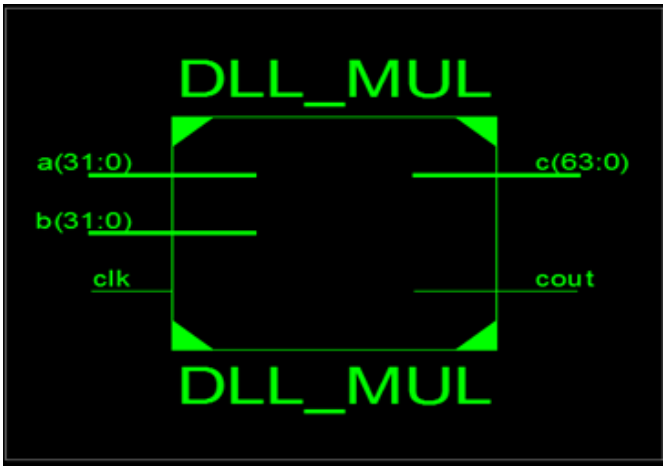

Fig. 3. RTL schematic 32-Bit Dual Logic Level architecture

Technology schematic opens an NGC file that can be viewed as an architecture-specific schematic. This schematic is generated after the optimization and technology targeting phase of the synthesis process. It shows a representation of the design in terms of logic elements optimized to the target Xilinx device. Viewing this schematic allows you to see a technology-level representation of HDL optimized for a specific Xilinx architecture, which might help you discover design issues early in the design process. Technology schematic for the DLL architecture design is shown in the Figure4.

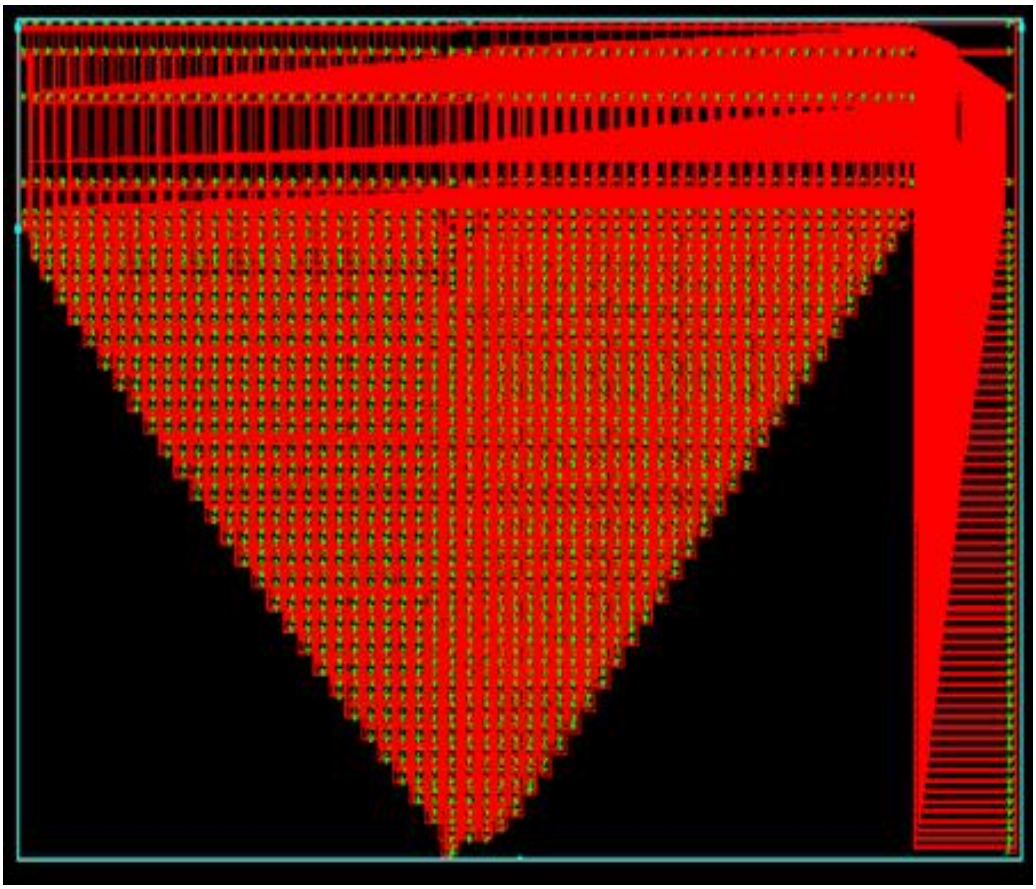

Fig.4.(a). Technology Schematic of 32- Bit Dual Logic Level architecture

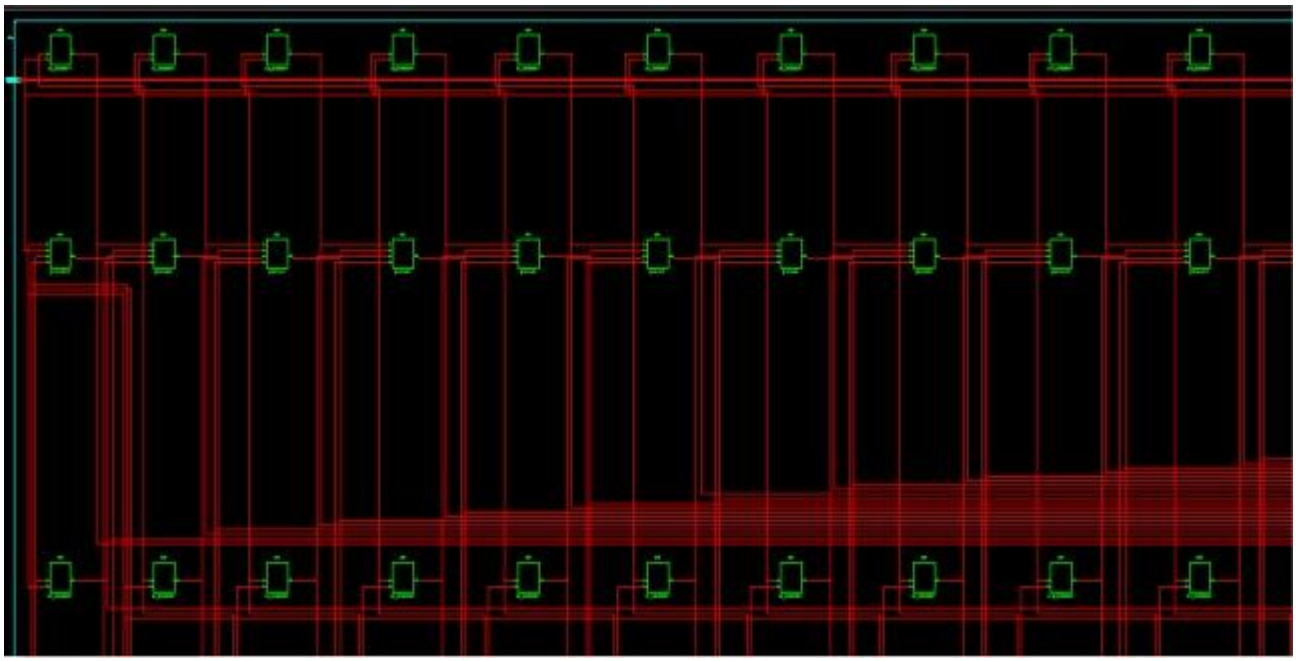

Fig. 4.(b).Expandable View of Technology Schematic of 32-Bit(DLL)

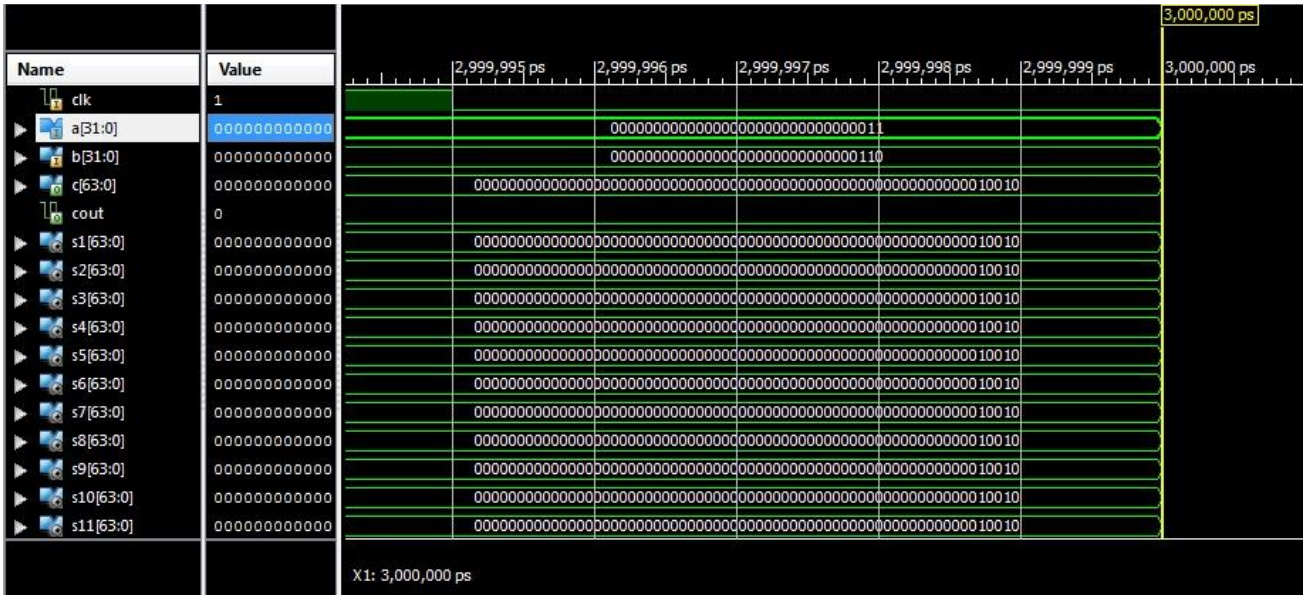

Fig. 5. Simulation Result of 32- Bit Dual Logic Level architecture.

From Figure.5 it is observed that DLL based multiplication is getting exact results for given set of inputs.

```
Delay:              42.206ns (Levels of Logic = 65)
  Source:           b<2> (PAD)
  Destination:      c<63> (PAD)
```

Fig.6(a). Delay for the proposed design

```
Total memory usage is 215752 kilobytes

Number of errors   :     0 (   0 filtered)
Number of warnings :     1 (   0 filtered)
Number of infos    :     0 (   0 filtered)
```

Fig.6(b). Total Memory usage for the proposed design

Fig.6(c).Total area utilization for the proposed design

TABLE I
Parameters and Delay

Methods/Parameters	Area(LUT)	Delay(ns)	Memory Usage(kb)
Previous Method [3]	6%	46.216	1096576
Proposed Method	4%	42.206	215752

IV. CONCLUSIONS

Montgomery modular multiplication is widely used in cryptographic techniques. This Proposed DLL based Montgomery modular multiplication is modeled on FPGA to perform modular multiplication. In this design, the area occupied is 4% on FPGA and the delay is 42.206ns. Furthermore, improvements in the reduction of area and delay are possible if design is implemented on ASIC.

REFERENCES

[1] Vinodhini. NSuganya.CPipelined VLSI Architecture for RSA Based on Montgomery Modular Multiplication Global Research and Development Journal for Engineering | *International Conference on Innovations in Engineering and Technology (ICIET) - 2016 | July 2016e-ISSN: 2455-5703.*

[2] Rivest, R.L., Shamir, A. and Adleman, L. (1978).A method for obtaining digital signatures and public-key cryptosystems *Commun. ACM*, Vol. 21, no. 2,pp. 120–126.

[3] Meenakshi, S., and M. Jagadeeswari. "Efficient VLSI Architecture for Montgomery Modular Multiplier." *African Journal of Basic & Applied Sciences* 9.5 (2017): 272-278.

[4] C. Mc vor, M. Mc Loone and J. V. Mc Canny, "Modified Montgomery modular multiplication and RSA exponentiation techniques," *IEEE Proc. Comput. Digit. Techn. vol. 151, no. 6*, pp. 402–408, Nov. 2004.

[5] Y. Kim, W. Kang, and J. R. Choi, "Asynchronous implementation of 1024-bitmodular processor for RSA cryptosystem," in Proc. *2nd IEEE Asia-Pacific Conf. ASIC*, pp. 187–190, Aug. 2000.

[6] Y. Y. Zhang, Z. Li, L. Yang, and. W. Zhang, "An efficient CSA architecture for Montgomery modular multiplication," *Microprocessors Microsyst*., vol. 31, no. 7, pp. 456–459, Nov. 2007.