IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

High Speed Area Efficient VLSI Architecture of Three Binary Operand Adders

Yedhula Manju, A.Nomeswar, S.Lavanya, Koppedu Narendra, Thummala Pawan Kumar, D.Sakunthala

B.E Final year Student, Department of Electronics and Communication Engineering, Siddharth Institute of Engineering & Technology, Puttur, India

Assistant Professor, Department of Electronics and Communication Engineering, Siddharth Institute of Engineering & Technology, Puttur, India

ABSTRACT: Three-operand binary adder is the basic functional unit to perform the modular arithmetic in various cryptography and pseudorandom bit generator (PRBG) algorithms and also used in many applications. Carry save adder (CS3A) is the widely used technique to perform the three-operand addition. In carry save adder at final stage uses ripple carry adder which will cause large critical path delay. Moreover, a parallel prefix two-operand adder such as Han-Carlson (HCA) can also be used for three-operand addition that significantly reduces the critical path delay with more area complexity. Hence, a new high-speed and area-efficient adder architecture is proposed using pre-compute bitwise addition followed by carry prefix computation logic to perform the three-operand binary addition that consumes substantially less area and less delay. When compare to existing design like three operand carry save adder and two operand based three operand Han-Carlson adder the proposed design consumes less area and less delay. The synthesis and simulation are verified by using Xilinx ISE 14.7 Tool.

I. INTRODUCTION

To achieve optimal system performance while maintaining physical security, it is necessary to implement the cryptography algorithms on hardware Modular arithmetic=such as modular exponentiation, modular multiplication and modular addition is frequently used for the arithmetic operations in various cryptography algorithms. Therefore, the performance of the cryptography algorithm depends on the efficient implementation of the congruential modular arithmetic operation. The most efficient approach to implement the modular multiplication and exponentiation is the Montgomery algorithm [5]–[7] whose critical operation is based binary addition is also a primary arithmetic operation in the linear congruential generator (LCG) based pseudo-random bit generators (PRBG) such as coupled LCG (CLCG) [9], modified dual-CLCG (MDCLCG) and coupled variable input. LCG (CVLCG) . Modified dual-CLCG (MDCLCG) is the most secure and highly random PRBG method among all the LCG-based and other existing PRBG methods. It is polynomial-time .For bit greater than 32-bits. Therefore, the security of the MDCLCG enhances with the increase of operand size. However, the area and critical path delay increases linearly since its hardware architecture consists of four three-operand modulo-2n adders, two comparators, four multiplexer's area in previous papers. Hence, the performance of the MDCLCG can be improved by the efficient implementation of the three-operand adder.

II.LITERATURE SURVEY

I. A. K. Panda and K. C. Ray, "Modified dual-CLCG method and its VLSI architecture for pseudorandom bit generation," *IEEE Trans. CircuitsSyst. I, Reg. Papers*, vol. 66, no. 3, pp. 989–1002, Mar. 2019.

In this paper, pseudorandom bit generator (PRBG) is an essential component for securing data during transmission and storage in various cryptography applications. Among popular existing PRBG methods such as linear feedback shift register (LFSR), linear congruential generator (LCG), coupled LCG (CLCG), and dual-coupled LCG (dual-CLCG), the latter proves to be more secure. This method relies on the inequality comparisons that lead to generating pseudorandom bit at a non-uniform time interval. Hence, a new architecture of the existing dual CLCG method is developed that generates pseudo-random bit at uniform clock rate. However, this architecture experiences several drawbacks such as excessive

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

memory usage and high-initial clock latency, and fails to achieve the maximum length sequence. To implement the design by using carry save adder for the addition of three operand in the design Therefore, a new PRBG method called as "modified dual-CLCG" and its very large-scale integration (VLSI) architecture are proposed in this paper to mitigate the aforesaid problems. The novel contribution of the proposed PRBG method is to generate pseudorandom bit at uniform clock rate with one initial clock delay and minimum hardware complexity. The proposed architecture is implemented using Verilog-HDL and prototyped on the commercially available FPGA device.

III. PROPOSED METHOD

Two kits are used for transmission of data and audio signal using LI-FI technology. One kit for transferring data signal ansection presents a new adder technique and its VLSI architecture to perform the three-operand addition in modular arithmetic. The proposed adder technique is a parallel prefix adder. However, it has four-stage structures instead three-stage structures in prefix adder to compute the addition of three binary input operands such as bit-addition logic, base logic, PG (propagate and generate) logic and sum logic. The logical expression of all these four stages are defined as follows,

Stage-1: Bit Addition Logic:

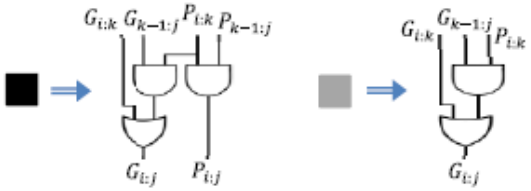
In this a series of full adders are used to generate the sum and carry in which these sum and carry values are sent to base logic

Stage-2: Base Logic:

The base logic uses the propagate and generate values and sends to the next stage

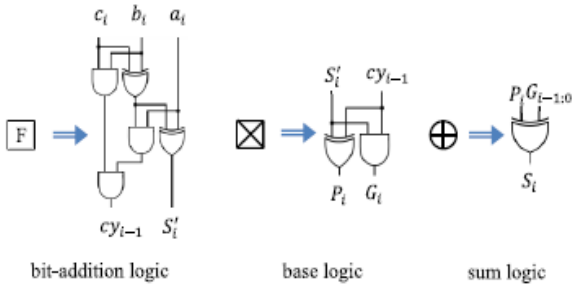
Stage-3: **PG (Generate and Propagate) Logic:**

This stage consists of gray cells and black cells to generate the carry that is sent to next stage**.**



Stage-4: **Sum Logic:**

The final sum is calculated here by performing the EXOR operation between the Carry and Propagate values

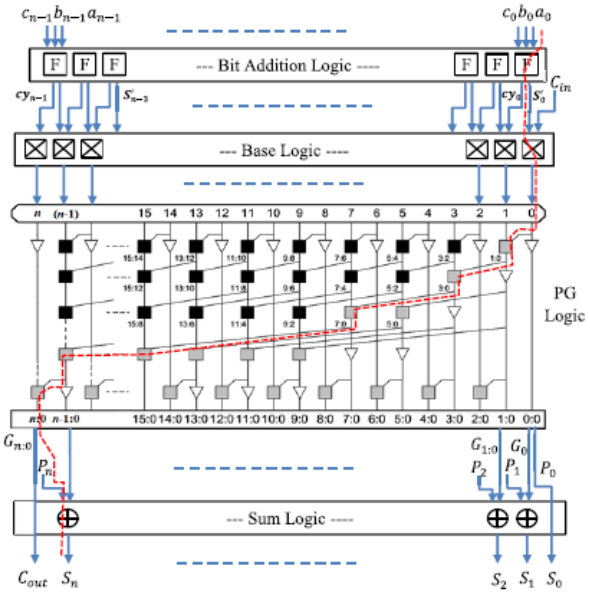


| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

The proposed VLSI architecture of the three-operand binary adder and its internal structure is shown in above figure. The new adder technique performs the addition of three *n*-bit binary inputs in four different stages. In the first stage (bit-addition logic), the bitwise addition of three *n*-bit binary input operands is performed with the array of full adders, and each full adder computes "sum and "carry signals as highlighted in Fig. 3(a). The logical expressions for computing sum and carry signals are defined in Stage-1, and the logicaldiagram of the bit-addition logic is shown in figure.



IV. WORKING PRINCIPLE

The three-operand binary addition is one of the critical arithmetic operation in the congruential modular arithmetic architectures various existing methods and LCG-based PRBG methods such as CLCG [9], MDCLCG [10] and CVLCG [11]. It can be implemented either by using two stages of two-operand adders or one stage of three-operand adder. Carry-save adder (CSA) is the commonly used technique to perform the three-operand binary addition [9]–[14]. It computes the addition of three operands in two stages. The first stage is the array of full adders. Each full adder computes "carry" bit and "sum" bit concurrently from three binary input . The second stage is the ripple-carry adder that computes the final *n*-bit size "sum" and one-bit size "carry-out" signals at the output of three-operand addition. The "carry-out" signal is propagated through the *n* number of full adders in the ripple-carry stage. Therefore, the delay increases linearly with the increase of bit length. The architecture of the three-operand carry-save adder is shown below figure. Where critical path delay is highlighted with a dashed line. It shows that the critical path delay depends on the carry propagation delay of ripple carry stage

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

V. RESULTS

Proposed three Operand Adder

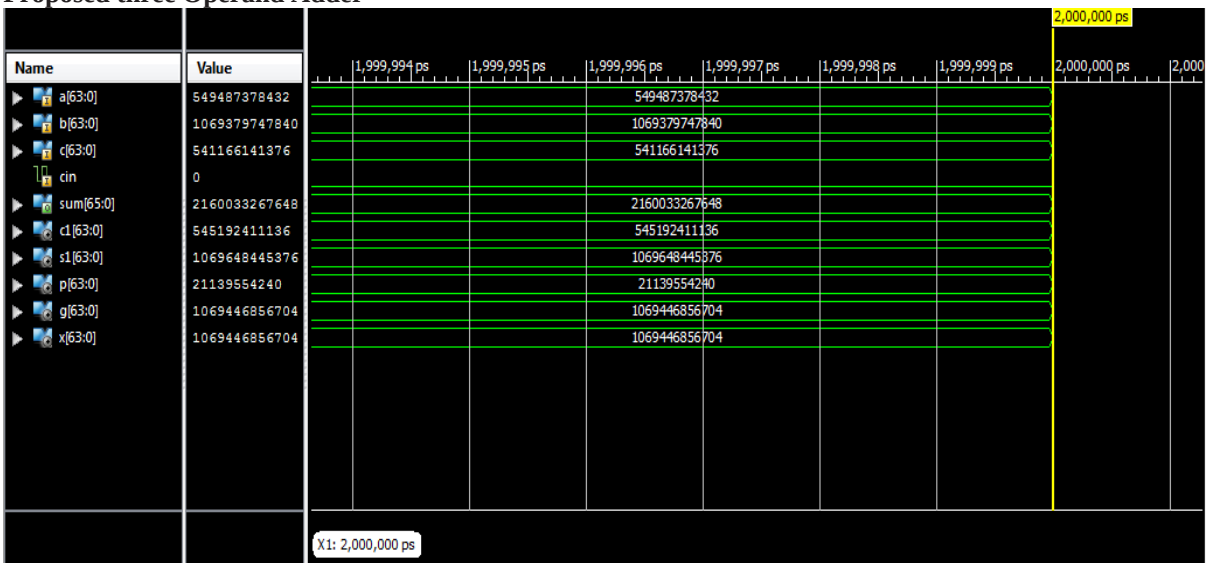


Fig 2. Simulation results of proposed three operand adder

Block Diagram:

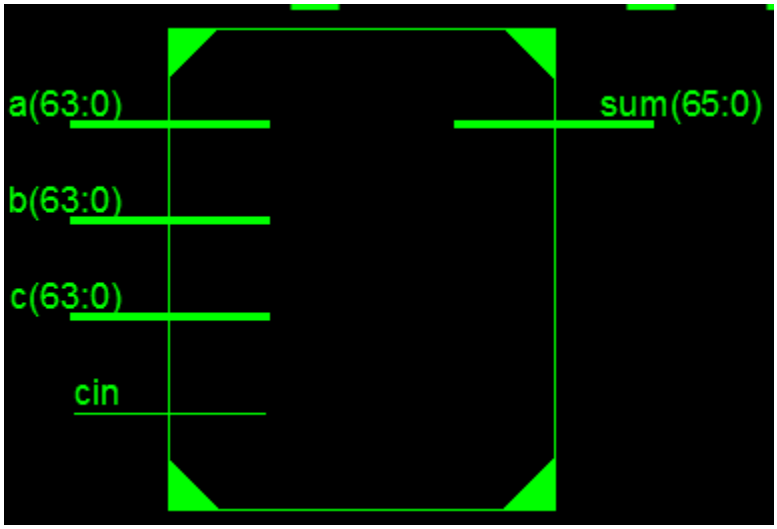


Fig.3 Technology Schematic of Proposed Adder

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

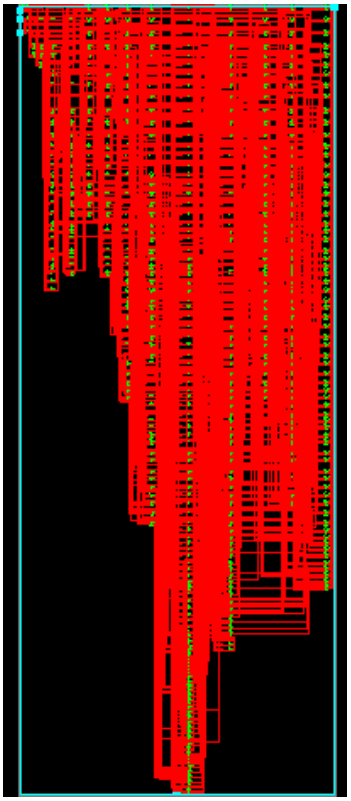


Fig. 4 Technology Schematic of Proposed Adder

AREA REPORT

```
Slice Logic Utilization:
 Number of Slice LUTs:                  368  out of  204000     0%
    Number used as Logic:               368  out of  204000     0%

Slice Logic Distribution:
 Number of LUT Flip Flop pairs used:    368
   Number with an unused Flip Flop:     368  out of    368   100%
   Number with an unused LUT:             0  out of    368     0%
   Number of fully used LUT-FF pairs:     0  out of    368     0%
   Number of unique control sets:         0

IO Utilization:
 Number of IOs:                         259
 Number of bonded IOBs:                 259  out of    600    43%
```

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

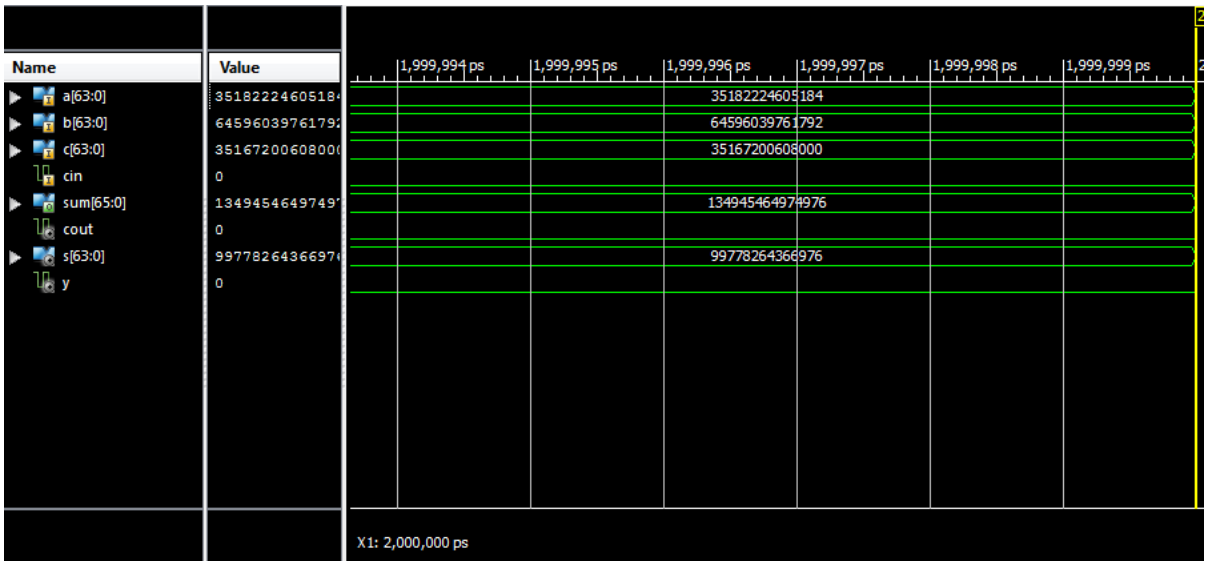
|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

Delay Report:

```
Data Path: b<0> to sum<65>
                                   Gate     Net
  Cell:in->out      fanout         Delay    Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   IBUF:I->O             3         0.000    0.507  b_0_IBUF (b_0_IBUF)
   LUT3:I0->O            2         0.043    0.608  g1/carry1 (c1<0>)
   LUT5:I0->O            4         0.043    0.630  pg1/gc1/G1 (x<1>)
   LUT6:I0->O            2         0.043    0.618  pg1/gc33/G1 (x<2>)
   LUT6:I0->O            4         0.043    0.512  pg1/gc2/G1 (x<3>)
   LUT6:I3->O            3         0.043    0.534  pg1/gc4/G1 (x<7>)
   LUT6:I2->O            1         0.043    0.522  pg1/gc8/G1 (pg1/gc8/G)
   LUT4:I0->O            3         0.043    0.417  pg1/gc8/G2 (x<15>)
   LUT6:I4->O            1         0.043    0.405  pg1/gc16/G1_SW0 (N4)
   LUT6:I4->O            5         0.043    0.428  pg1/gc16/G1 (x<23>)
   LUT6:I4->O            1         0.043    0.405  pg1/gc28/G111 (pg1/gc28/G11)
   LUT5:I3->O            5         0.043    0.518  pg1/gc28/G112 (x<31>)
   LUT6:I3->O            2         0.043    0.527  pg1/gc32/G4 (pg1/gc32/G3)
   LUT6:I2->O            1         0.043    0.339  h1/carry1 (sum_65_OBUF)
   OBUF:I->O                       0.000           sum_65_OBUF (sum<65>)
  ----------------------------------------
  Total                            7.531ns (0.559ns logic, 6.972ns route)
                                           (7.4% logic, 92.6% route)
```

Existing method
HC3A Adder:
Simulation results of existing HC3A adder



| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

Area report:

```
Device utilization summary:
---------------------------

Selected Device : 7vx330tffg1157-2


Slice Logic Utilization:
 Number of Slice LUTs:                  444  out of  204000     0%
    Number used as Logic:               444  out of  204000     0%

Slice Logic Distribution:
 Number of LUT Flip Flop pairs used:    444
   Number with an unused Flip Flop:     444  out of    444   100%
   Number with an unused LUT:             0  out of    444     0%
   Number of fully used LUT-FF pairs:     0  out of    444     0%
   Number of unique control sets:         0

IO Utilization:
 Number of IOs:                         259
 Number of bonded IOBs:                 259  out of    600    43%
```

Delay Report:

```
Data Path: a<1> to sum<65>
                           Gate     Net
  Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   IBUF:I->O             3   0.000   0.534  a_1_IBUF (a_1_IBUF)
   LUT4:I0->O            4   0.043   0.422  g1/gc1/G1 (g1/c<1>)
   LUT5:I3->O            7   0.043   0.529  g1/gc2/G1 (g1/c<3>)
   LUT5:I2->O            7   0.043   0.529  g1/gc4/G11 (g1/gc4/G1)
   LUT5:I2->O            5   0.043   0.518  g1/gc4/G1 (g1/c<7>)
   LUT6:I3->O            4   0.043   0.367  g1/gc8/G1 (g1/gc8/G)
   LUT5:I4->O            3   0.043   0.417  g1/gc8/G2 (g1/c<15>)
   LUT6:I4->O            2   0.043   0.410  g1/gc16/G11 (g1/gc16/G11)
   LUT4:I2->O            5   0.043   0.518  g1/gc16/G12 (g1/gc16/G1)
   LUT6:I3->O            4   0.043   0.367  g1/gc28/G111 (g1/gc28/G111)
   LUT5:I4->O            5   0.043   0.626  g1/gc28/G112 (g1/gc28/G11)
   LUT6:I1->O            4   0.043   0.422  g1/gc28/G (g1/c<55>)
   LUT5:I3->O            4   0.043   0.630  g1/Mxor_sum<63:1>_56_xo<0>1 (s<57>)
   LUT6:I0->O            3   0.043   0.625  g2/bc28/P1 (g2/p1<27>)
   LUT6:I0->O            1   0.043   0.613  g2/gc32/G6_SW0 (N96)
   LUT6:I0->O            1   0.043   0.405  g2/gc32/G6 (g2/gc32/G5)
   LUT5:I3->O            2   0.043   0.618  g2/gc32/G7 (cout)
   LUT6:I0->O            1   0.043   0.339  g3/carry1 (sum_65_OBUF)
   OBUF:I->O                 0.000          sum_65_OBUF (sum<65>)
  ----------------------------------------
  Total                      9.622ns (0.731ns logic, 8.891ns route)
                                     (7.6% logic, 92.4% route)
```

VI. CONCLUSION

In this paper, a high-speed area-efficient adder technique and its VLSI architecture is proposed to perform the three operand binary addition in various cryptography algorithms. The proposed three-operand adder technique is a parallel prefix adder that uses four-stage structures to compute the addition of three input operands. The novelty of this proposed architecture is the reduction of delay and area in the prefix computation stages in PG logic and bit-addition logic that leads to an overall

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007138 |

reduction in critical path delay. It also decrease the area complexity when compare to other parallel prefix three operand adders. Form the above comparison, the proposed three operand binary adder consists of less area and less delay when compare to existing in CS3A and HC3A three operand adder. The synthesis and simulation are verified by using Xilinx ISE tool.

REFERENCES

[1] M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal, and Y. M. Jang, "FPGA implementation of high-speed area-efficient processor for elliptic curve point multiplication over prime field," IEEE Access, vol. 7, pp. 178811–178826, 2019.
[2] Z. Liu, J. GroBschadl, Z. Hu, K. Jarvinen, H. Wang, and I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things," IEEE Trans. Comput., vol. 66, no. 5, pp. 773–785, May 2017.
[3] Z. Liu, D. Liu, and X. Zou, "An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor," IEEE Trans. Ind. Electron., vol. 64, no. 3, pp. 2353–2362, Mar. 2017.
[4] B. Parhami, Computer Arithmetic: Algorithms and Hardware Design. New York, NY, USA: Oxford Univ. Press, 2000.
[5] P. L. Montgomery, "Modular multiplication without trial division," Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.
[6] S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu, "Low-cost high-performance VLSI architecture for montgomery modular multiplication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 24, no. 2, pp. 434–443, Feb. 2016.
[7] S.-R. Kuang, J.-P. Wang, K.-C. Chang, and H.-W. Hsu, "Energy-efficient high-throughput montgomery modular multipliers for RSA cryptosystems," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 11, pp. 1999–2009, Nov. 2013.
[8] S. S. Erdem, T. Yanik, and A. Celebi, "A general digit-serial architecture for montgomery modular multiplication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 5, pp. 1658–1668, May 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details