International Journal of Engineering & Technology, 7 (1.5) (2018) 164-169

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

VLSI design for efficient RSD-Based ECC processor using Karatsuba algorithm

Pasluri Bindu Swetha [1*], V.J. Kishore Sonti [2], A. Murali [3]

[1]*Assistant Professor, Dept of ECE, G. Pullaiah College of Engineering and Technology, Kurnool, A.P.*
[2]*Associate Professor, Dept of ECE, Sathyabama University, Chennai.*
[3]*Associate Professor, Dept of ECE, Miracle Engineering College, Vizayanagaram, A.P.*

Abstract

In this paper, an exportable application-particular direction set elliptic bend cryptography processor in view of repetitive marked digit portrayal is proposed. The processor utilizes broad pipelining strategies for Karatsuba– Of man strategy to accomplish high throughput augmentation. Moreover, an effective particular viper without correlation and a high throughput measured divider, which brings about a short data path for expanded recurrence, are actualized. The proposed design of this paper investigation the rationale size, region and power utilization utilizing Xilinx 13.2. The expansion for the task is Vedic Sutra – Nikhilam Sutra.

Keywords: *Application Specific Instruction-set Processor (ASIP), Elliptic Curve Cryptography (ECC), Field Programmable Gate Array (FPGA), Karatsuba–Ofman Multiplication, Redundant Signed Digit (RSD).*

1. Introduction

In prime field ECC processors, convey free number juggling is important to stay away from protracted data-paths caused via convey spread. Repetitive plans, for example, convey spare math (CSA) [1], [2], excess marked digits (RSDs) [3], or deposit number frameworks (RNSs) [4], [5], have been used in different outlines. Convey rationale or inserted computerized flag preparing (DSP) hinders inside field programmable entryway exhibits (FPGAs) are additionally used in a few outlines to address the convey spread issue "[6], [7]. It is important to fabricate an effective expansion information way since it is a crucial operation utilized in other particular math operations. Secluded duplication is a fundamental operation in ECC. Two fundamental methodologies might be utilized. The first is known as interleaved measured augmentation utilizing Montgomery's technique [8]. Montgomery duplication is generally utilized as a part of usage where self-assertive bends are wanted [9], [10]. Another approach is known as increase then-decrease and is utilized as a part of elliptic bends worked over limited fields of Merssene primes [11]. Merssene primes are the extraordinary kind of primes which take into account proficient particular diminishment through arrangement of increments and subtractions [12], [13]. So as to streamline the augmentation procedure, some ECC processors utilize the gap and vanquish approach of Karatsuba– Ofman increases [14], where others utilize inserted multipliers and DSP obstructs inside FPGA textures [15]- [17].

This paper proposes another RSD-based prime field ECC processor with rapid working recurrence. In this paper, we show the execution of left-to-right scalar point increase calculation. The general processor engineering is of standard cross bar sort with 256 digit wide information transports. The plan procedure and streamlining strategies are engaged toward effective individual secluded number juggling modules instead of the general engineering. The staying of this paper is composed as takes after. Area II gives foundation data on ECC frameworks. Segment III displays the general design of the proposed processor, the engineering of the particular number juggling unit (AU) is exhibited. In Section IV, augmentation of the venture is examined. At last, Results and conclusion is attracted Section V and Section VI.

2. Related work

Karatsuba–Ofman Multiplication:

The multifaceted nature of the consistent increase utilizing the textbook strategy is $O(n^2)$. Karatsuba and Ofman [18], proposed a strategy to play out an increase with multifaceted nature $O(n^{1.58})$by partitioning the operands of the augmentation into littler and measure up to sections. Having two operands of length n to be duplicated, the Karatsuba– Ofman approach proposes to part the two operands into high-(H)and low-(L) sections.

$a_H=(a_{n-1},\ldots\ldots,a_{[n/2]}),a_L=a_{[n/2]-1},\ldots,a_0)$
$b_H=b_{n-1},\ldots\ldots,b_{[n/2]}),\ b_L=(b_{[n/2]-1},\ldots,b_0)$

Consider β as the base for the operands, where β is 2 if there should arise an occurrence of whole numbers and β is x in the event of polynomials. At that point, the augmentation of the two operands is executed as takes after: considering

$a=a_L+a_H^{[n/2]}$ and $b=b_L+b_H^{[n/2]}$ then

$C=AB=(a_L+a_H^{[n/2]})\ (b_L+b_H^{[n/2]})$

$$=a_Lb_L+(a_Lb_H+a_Hb_L)^{[n/2]})+a_Hb_H^n$$

Hence, four half-sized multiplications are needed, where Karatsuba methodology reformulate to

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

$C=AB= (a_L+a_H^{[n/2]}) (b_L+b_H^{[n/2]})$
$=a_Lb_L +(a_Lb_H+a_Hb_L)^{[n/2]}) +a_Hb_H^n$

In this way, just three half-sized increases are required. The first Karatsuba calculation is performed recursively, where the operands are sectioned into littler parts until the point that a sensible size is come to, and after that consistent duplications of the littler portions are performed recursively.

Redundant Signed Digits:
The RSD portrayal, first presented by Avizienis [19], is a convey free number juggling where whole numbers are spoken to by the distinction of two different whole numbers. A number X is spoken to by the distinction of its x+ and x− segments, where x+ is the positive segment and x− is the negative part. The idea of the RSD portrayal has the upside of performing expansion and subtraction without the need of the two's supplement portrayal. Then again, an overhead is acquainted due with the excess in the whole number portrayal, since a whole number in RSD portrayal requires twofold word length contrasted and run of the mill two's supplement portrayal. In radix-2 adjusted RSD spoke to numbers, digits of such whole numbers are either 1, 0, or −1.

3. Proposed methodology

The proposed P256 ECC processor comprises of an AU of 256 RSD digit wide, a limited state machine (FSM), memory, and two information transports. The processor can be arranged in the pre-combination stage to help the P192 or P224 NIST prescribed prime bends [20]. Fig. 1 demonstrates the general processor design. Two sub control units are connected to the principle control unit as extra squares. These two sub control units function as FSMs for point expansion and point multiplying, separately. Diverse facilitate frameworks are effortlessly upheld by including relating sub control obstructs that work as indicated by the recipes of the arrange framework.

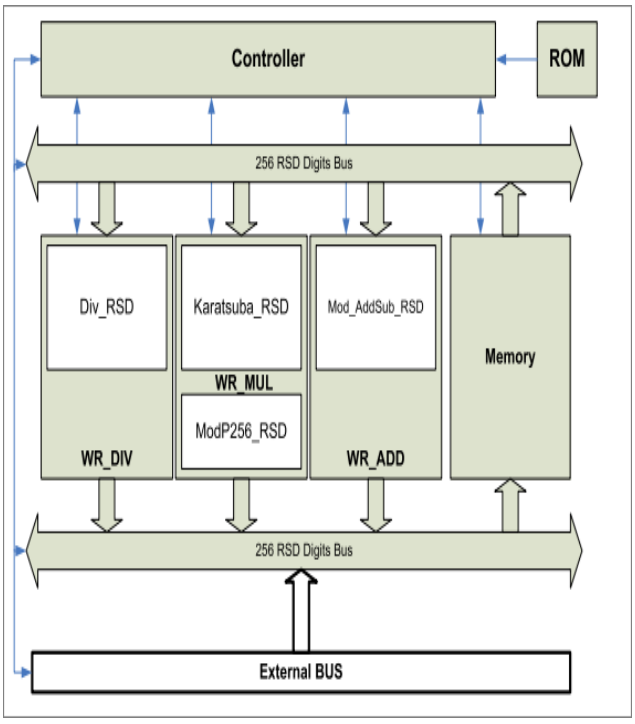

Fig. 1: Overall processor architecture

Arithmetic unit
Particular Addition and Subtraction Addition is utilized as a part of the gathering procedure amid the increase, and also, in the paired GCD secluded divider calculation. In the proposed usage, radix-2 RSD portrayal framework as convey free portrayal is utilized. In RSD with radix-2, digits are spoken to by 0, 1, and −1, where digit 0 is coded with 00, digit 1 is coded with 10, and digit −1 is coded with 01. In Fig. 2, a RSD viper is introduced that is worked from summed up full adders.

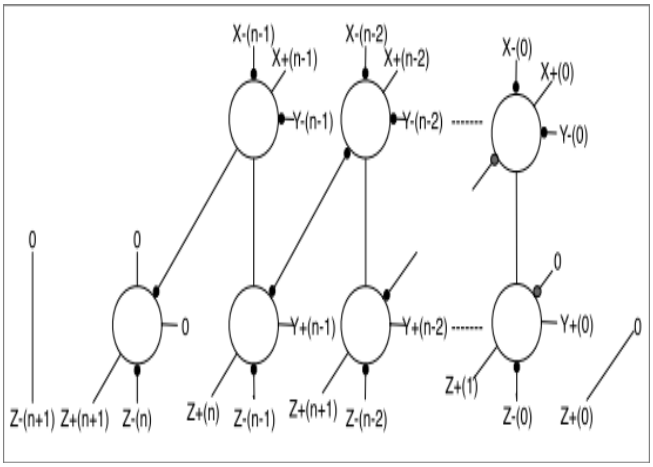

Fig. 2: RSD Adder.

Modular Multiplication
Karatsuba's multiplier recursive nature is viewed as a noteworthy downside when executed in equipment [21]. Equipment multifaceted nature increments exponentially with the measure of the operands to be duplicated. To defeat this downside, Karatsuba technique is connected at two levels. A recursive Karatsuba obstruct that works profundity shrewd, and an iterative Karatsuba that works widthwise.

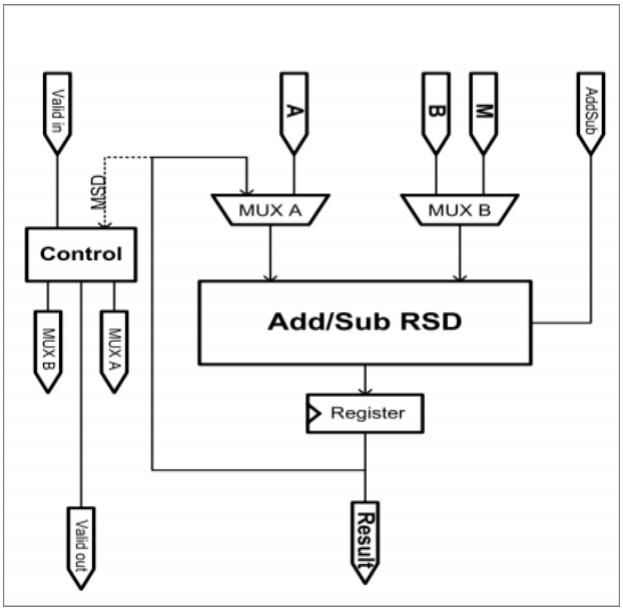

Fig. 3: Modular addition subtraction block diagram

The piece chart of the recursive Karatsuba multiplier is appeared in Fig. 4, where information conditions are plainly taken note. As appeared in Fig. 4, Karatsuba technique requires playing out a subtraction at each level, which is favorable position of the proposed usage since subtraction is performed with no additional cost in RSD portrayal. The piece graph of the recursive Karatsuba module is worked from three half-sized recursive Karatsuba squares and some RSD adders/Subtractors. There is one 1-digit RSD multiplier that is utilized to duplicate the convey digits from the center expansion. As per Fig. 4, the basic data path of the recursive Karatsuba is separated into two ways. The main way experiences the center half-sized recursive Karatsuba piece, and

alternate experiences the cross result of the center expansion with multiplexers and a few adders.

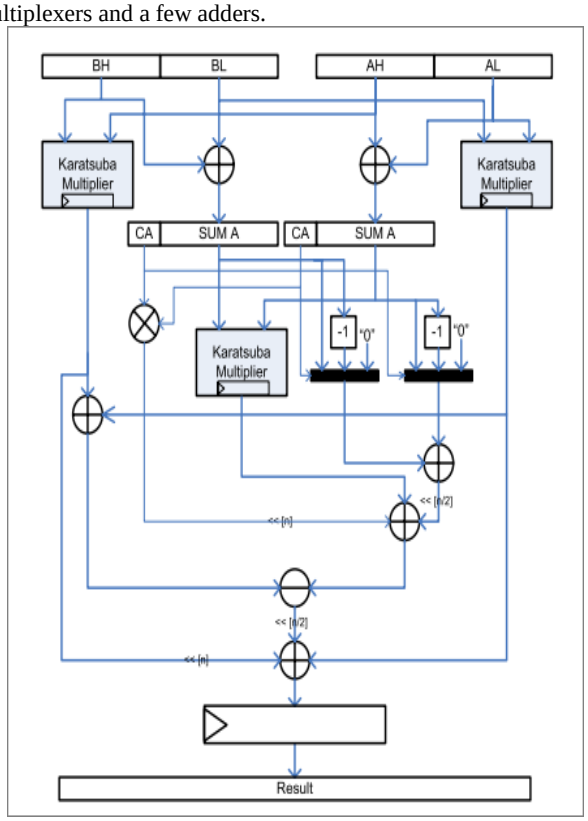

Fig. 4: Karatsuba recursive block

NIST Reduction: Generalized Merssene primes [11] are the uncommon sort prime numbers that permit quick particular lessening. General division is supplanted by couple of increases and subtractions. Such primes are spoken to as p = f (t), where t is an energy of 2. The modulus of the P256 bend is Merssene prime p = 2256−2224+2192+296−1.

Because of the repetition idea of the RSD portrayal, the duplication procedure may create comes about that are spoken to by more than 512 digits and these outcomes are still in the range −p2 < A < p2. These maybe a couple additional digits are outside the scope of the NIST decrease process. Thus, we determined new equations to incorporate these additional digits in the lessening procedure. The new lessening process has one additional 256-digit term, D5, alongside some alteration of the beforehand existed terms. This term is included restrictively, regardless of whether the additional digit is set or not. Along these lines, two increments are the aggregate overhead required to deal with the additional digits caused utilizing the RSD portrayal. The changed lessening recipe is

B = T + 2S1 + 2S2 + S3 + S4 − D1 − D2 − D3 − D4 − D5 mod p,

Where A16 speaks to the additional digits delivered by RSD Karatsuba multiplier.

$$
\begin{aligned}
T &= (A_7 \| A_6 \| A_5 \| A_4 \| A_3 \| A_2 \| A_1 \| A_0) \\
S_1 &= (A_{15} \| A_{14} \| A_{13} \| A_{12} \| A_{11} \| 0 \| 0 \| 0) \\
S_2 &= (\mathbf{2 * A_{16}} \| A_{15} \| A_{14} \| A_{13} \| A_{12} \| 0 \| 0 \| \mathbf{A_{16}}) \\
S_3 &= (A_{15} \| A_{14} \| 0 \| 0 \| \mathbf{-2 * A_{16}} \| A_{10} \| A_9 \| A_8) \\
S_4 &= (A_8 \| A_{13} \| A_{15} \| A_{14} \| A_{13} \| A_{11} \| A_{10} \| A_9) \\
D_1 &= (A_{10} \| A_8 \| 0 \| 0 \| \mathbf{2 * A_{16}} \| A_{13} \| A_{12} \| A_{11}) \\
D_2 &= (A_{11} \| A_9 \| 0 \| \mathbf{A_{16}} \| A_{15} \| A_{14} \| A_{13} \| A_{12}) \\
D_3 &= (A_{12} \| \mathbf{2 * A_{16}} \| A_{10} \| A_9 \| A_8 \| A_{15} \| A_{14} \| A_{13}) \\
D_4 &= (A_{13} \| 0 \| A_{11} \| A_{10} \| A_9 \| \mathbf{A_{16}} \| A_{15} \| A_{14}) \\
\mathbf{D_5} &= \mathbf{(-A_{16} \| 0 \| 0 \| 0 \| 0 \| 0 \| 0 \| - A_{16})}.
\end{aligned}
$$

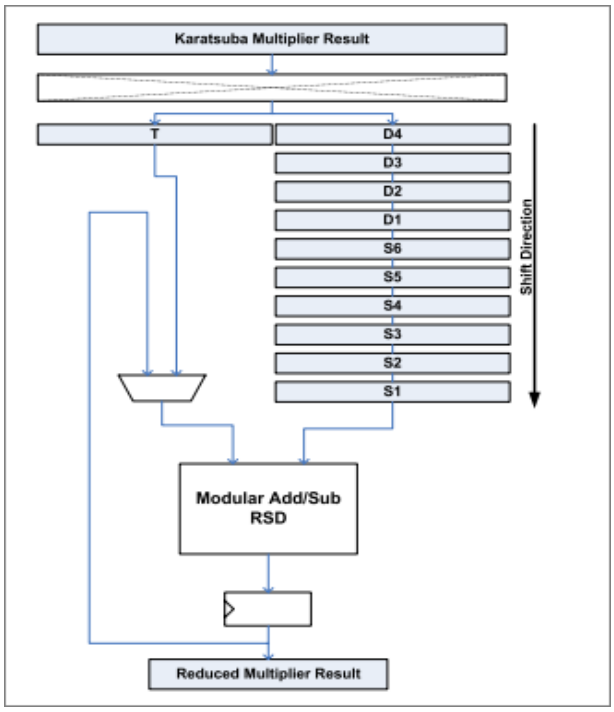

Fig. 5: Mod P256 reduction block.

Keeping in mind the end goal to oblige the additional digit created by the RSD Karatsuba multiplier, NIST lessening is reformulated. The resultant diminishment plot comprises of three additional options. In any case, through reformulation and joining the first terms with the extra terms, the diminishment conspire is improved. In like manner, the secluded multiplier is worked with a Karatsuba multiplier, measured RSD viper, and a few registers to hold the 256-digit terms. Fig. 5 demonstrates the square outline of the Mod P256 RSD multiplier. A controller is utilized to control the stream of the terms to the particular snake and every step of the way, the aftereffect of the measured expansion is amassed and encouraged back to the viper. The cross-bar in Fig. 5 demonstrates the wiring of the 32-digit words to their separate areas inside the expanded NIST decrease registers. High-Radix Modular Division Twofold GCD calculation is a proficient method for performing particular division since it depends on expansion, subtraction, and moving operations. The multifaceted nature of the division operation originates from the way that the running time of the calculation is conflicting and is input" subordinate.

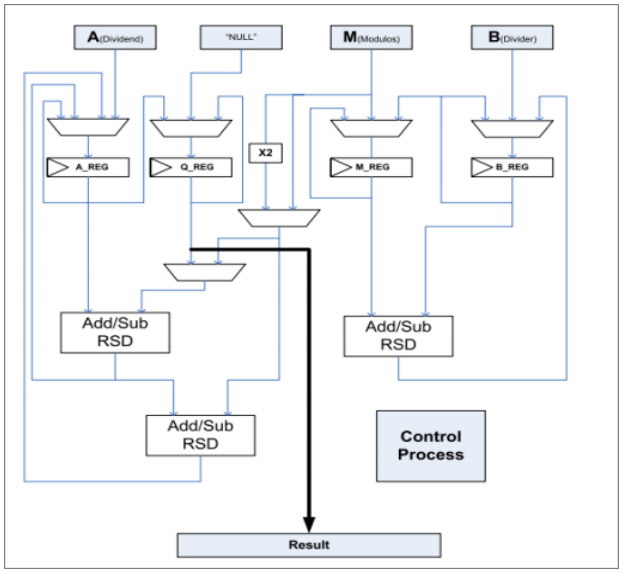

Fig. 6. Modular divider block

4. Vedic Sutra – Nikhilam Sutra

Nikhilam Sutra means "all from 9 and last from 10". Nikhilam Sutra stipulates subtraction of a number from the nearest power of 10 i.e. 10, 100, 1000, etc. Nikhilam Sutra in Vedic Mathematics can be used as shortcuts to multiply numbers, divide numbers in faster approach.

Nikhilam sutra seems to have special advantage when the multiplicand and multiplier are same. If both multiplicand and multiplier are equal then multiplication operation is known as squaring. Squaring is considered as special case of multiplication. First we write the Nikhilam Squaring algorithm which can be used to compute square of a binary integer. Nikhilam Squaring algorithm is in turn called by Nikhilam Multiplication to perform the multiplication. Multiplication and squaring related to each other by the following well known formula:

Nikhilam Multiplication is described in Algorithm [22]. It takes two binary numbers A and B as input and compute their multiplication(C) as output. It performs two calls to Nikhilam Squaring algorithm and using that, outputs the desired result. Nikhilam Multiplication uses only 1 multiplication, 1 division and O(c ∗ n) add/subtract and shift operations for some constant c.

Algorithm : NikhilamMultiplication(A, B)

INPUT: $A = \sum_0^{n-1} a_i x^i, B = \sum_0^{n-1} b_j x^j$

OUTPUT: $C = AB = \sum_0^{2n-1} c_k x^k$

$D_1 \leftarrow$ **NikhilamSquaring** $(A + B)$

$D_2 \leftarrow$ **NikhilamSquaring** $(A - B)$

return $C \leftarrow (D_1 - D_2)/4$

5. Experimental Results

Synthesis and Simulation Results of the Proposed and Extension are observed Xilinx ISE 13.2.

Results of proposed method.

Simulation.

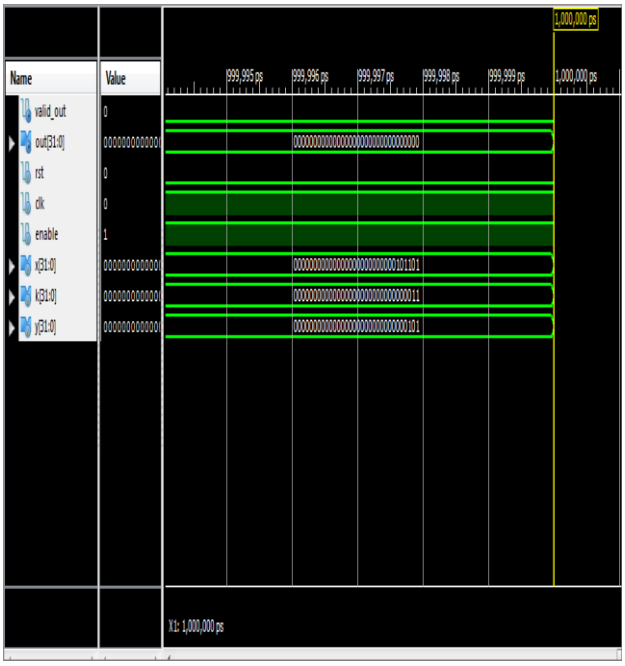

Fig. 7: proposed main module Synthesis result shows the block diagram, delay and area.

RTL Schematic.

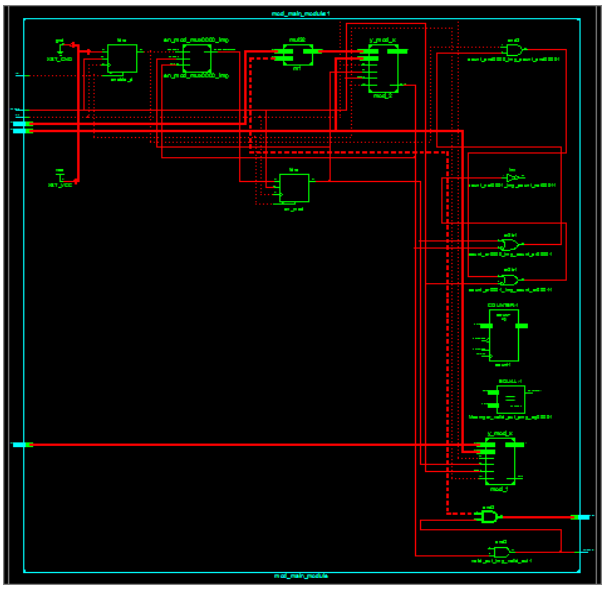

Fig. 8: Proposed main module Technology Schematic.

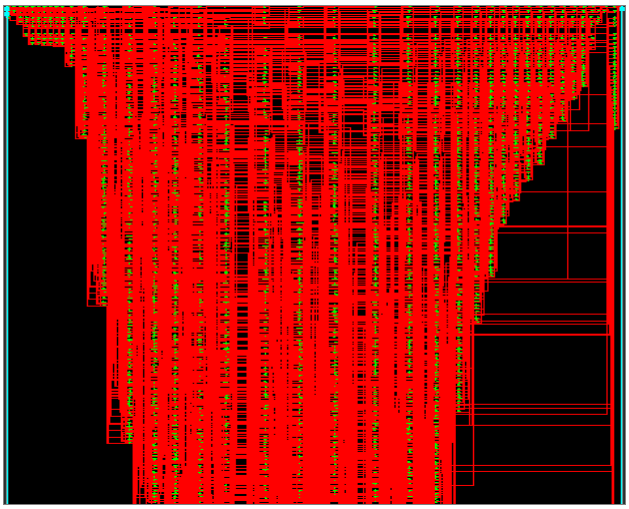

Fig. 9: Proposed main module

Extension.

Simulation.

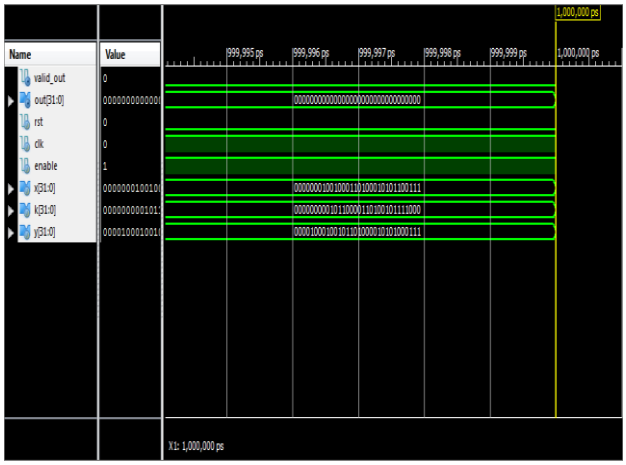

Fig. 10: Nikhilam Sutra x mod y RTL Schematic.

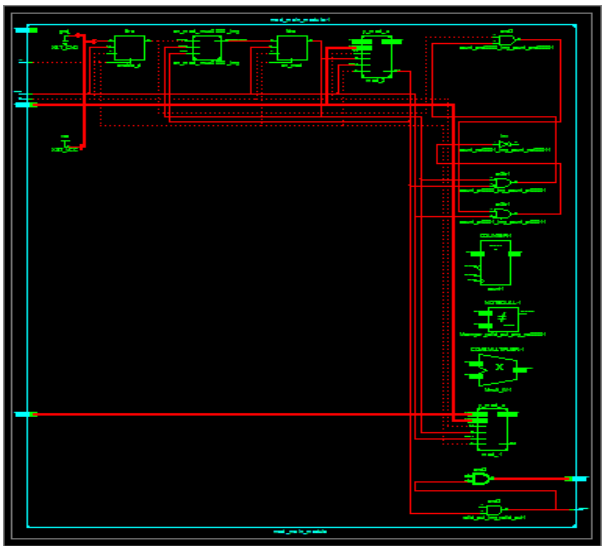

Fig. 11: RTL Schematic of Nikhilam Sutra x mod y Technology Schematic.

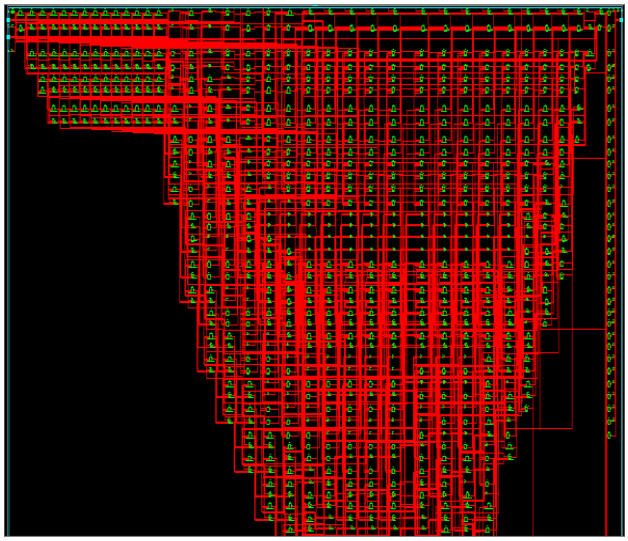

Fig. 12: Technology Schematic of Nikhilam Sutra x mod y

Comparison of the Proposed Kasturba multiplier and Extension Nikhilam Sutra results vary in area and delay which shows that there is a decrease in them and the performance is better in Nikhilam sutra.

	AREA	DELAY(ns)	
	SLICES		LUTS
PROPOSED	930	1741	177
EXTENSION	223	439	165

6. Conclusion

In this paper, a NIST 256 prime field ECC processor execution in FPGA has been displayed. A RSD as a convey free portrayal is used which brought about short data paths and expanded most extreme recurrence. We presented upgraded pipelining strategies inside Karatsuba multiplier to accomplish high throughput execution by a completely LUT-based FPGA usage... Besides, an effective measured expansion/subtraction is presented in light of checking the LSD of the operands as it were. A control unit with add-on like design is proposed as a reconfigurability highlight to help distinctive point augmentation calculations and organize frameworks. The fundamental focal points of our processor incorporate the exportability to other FPGA and ASIC advancements and expandability to help diverse organize frameworks and point duplication calculations.

References

[1] S.-C. Chung, J.-W. Lee, H.-C. Chang, and C.-Y. Lee, "A highperformance elliptic curve cryptographic processor over GF(p) with SPA resistance," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2012, pp. 1456–1459.

[2] J.-Y. Lai and C.-T. Huang, "Elixir: High-throughput cost-effective dualfield processors and the design framework for elliptic curve cryptography," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 16, no. 11, pp. 1567–1580, Nov. 2008.

[3] D. Karakoyunlu, F. K. Gurkaynak, B. Sunar, and Y. Leblebici, "Efficient and side-channel-aware implementations of elliptic curve cryptosystems over prime fields," IET Inf. Secur., vol. 4, no. 1, pp. 30–43, Mar. 2010.

[4] D. M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas, and T. Stouraitis, "An RNS implementation of an Fp elliptic curve point multiplier," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 56, no. 6, pp. 1202–1213, Jun. 2009.

[5] D. Schinianakis and T. Stouraitis, "Multifunction residue architectures for cryptography," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 61, no. 4, pp. 1156–1169, Apr. 2014.

[6] J. Vliegen et al., "A compact FPGA-based architecture for elliptic curve cryptography over prime fields," in Proc. 21st IEEE Int. Conf. Appl.-Specific Syst. Archit. Process. (ASAP), Jul. 2010, pp. 313–316.

[7] T. Güneysu and C. Paar, "Ultra high performance ECC over NIST primes on commercial FPGAs," in Proc. 10th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES), 2008, pp. 62–78.

[8] P. L. Montgomery, "Modular multiplication without trial division," Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.

[9] K. Sakiyama, N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, "Reconfigurable modular arithmetic logic unit for high-performance public-key cryptosystems," in Proc. 2nd Int. Workshop Reconfigurable Comput., Archit. Appl., vol. 3985. 2006, pp. 347–357.

[10] Byrne, E. Popovici, and W. P. Marnane, "Versatile processor for GF(pm) arithmetic for use in cryptographic applications," IET Comput. Digit. Tech., vol. 2, no. 4, pp. 253–264, Jul. 2008.

[11] J. Solinas, "Generalized Mersanne number," Univ. Waterloo, Waterloo, ON, Canada, Tech. Rep. CORR 99-39, 1999.

[12] S. Mane, L. Judge, and P. Schaumont, "An integrated prime-field ECDLP hardware accelerator with high-performance modular arithmetic units," in Proc. Int. Conf. Reconfigurable Comput. FPGAs, Nov./Dec. 2011, pp. 198–203.

[13] B. Ansari and M. A. Hasan, "High-performance architecture of elliptic curve scalar multiplication," IEEE Trans. Comput., vol. 57, no. 11, pp. 1443–1453, Nov. 2008.

[14] N. Smyth, M. McLoone, and J. V. McCanny, "An adaptable and scalable asymmetric cryptographic processor," in Proc. Int. Conf. Appl.-Specific Syst., Archit. Processors (ASAP), Sep. 2006, pp. 341–346.

[15] C. J. McIvor, M. McLoone, and J. V. McCanny, "Hardware elliptic curve cryptographic processor over GF(p)," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 9, pp. 1946–1957, Sep. 2006.

[16] K. Ananyi, H. Alrimeih, and D. Rakhmatov, "Flexible hardware processor for elliptic curve cryptography over NIST prime fields," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 17, no. 8, pp. 1099–1112, Aug. 2009.

[17] M. Hamilton and W. P. Marnane, "FPGA implementation of an elliptic curve processor using the GLV method," in Proc. Int. Conf. Reconfigurable Comput. FPGAs (ReConFig), Dec. 2009, pp. 249–254.

[18] Karatsuba and Y. Ofman, "Multiplication of multidigit numbers on automata," Soviet Phys. Doklady, vol. 7, p. 595, Jan. 1963.

[19] Avizienis, "Signed-digit numbe representations for fast parallel arithmetic," IRE Trans. Electron. Comput., vol. EC-10, no. 3, pp. 389–400, Sep. 1961.

[20] NIST. (2000). Recommended Elliptic Curves for Federal Government Use. [Online]. Available: http://csrc.nist.gov/encryption.

[21] S. Yazaki and K. Abe, "VLSI design of Karatsuba integer multipliers and its evaluation," Electron. Commun. Jpn., vol. 92, no. 4, pp. 9–20, 2009.

[22] "An Efficient Multiplication Algorithm Using Nikhilam Method" Shri Prakash Dwivedi.

[23] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.
[24] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.
[25] N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.
[26] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.
[27] Mahesh Mudavath, K Hari Kishore "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs” Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.
[28] P Bala Gopal, K Hari Kishore, B.Praveen Kittu “An FPGA Implementation of On Chip UART Testing with BIST Techniques”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015
[29] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.
[30] N Bala Gopal, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.
[31] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.
[32] N.Prathima, K.Hari Kishore, “Design of a Low Power and High Performance Digital Multiplier Using a Novel 8T Adder”, International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 3, Issue.1, Jan-Feb., 2013.
[33] Harikishore Kakarla, Madhavi Latha M and Habibulla Khan, “Transition Optimization in Fault Free Memory Application Using Bus-Align Mode”, European Journal of Scientific Research, Vol.112, No.2, pp.237-245, ISSN: 1450-216x135/1450-202x, October 2013.
[34] T.Padmapriya, Ms. N. Dhivya, Ms U. Udhayamathi, “Minimizing Communication Cost In Wireless Sensor Networks To Avoid Packet Retransmission”, International Innovative Research Journal of Engineering and Technology, Vol. 2, Special Issue, pp. 38-42.
[35] S.V.Manikanthan and K.Baskaran “Low Cost VLSI Design Implementation of Sorting Network for ACSFD in Wireless Sensor Network”, CiiT International Journal of Programmable Device Circuits and Systems,Print: ISSN 0974 – 973X & Online: ISSN 0974 – 9624, Issue : November 2011, PDCS112011008.
[36] M. Rajesh, Manikanthan, “GET-UP-AND-GO EFFICIENT MEMETIC ALGORITHM BASED AMALGAM ROUTING PROTOCOL”, International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-116, No. 21, Oct 2017.
[37] Rajesh, M., and J. M. Gnanasekar. "An optimized congestion control and error management system for OCCEM." International Journal of Advanced Research in IT and Engineering 4.4 (2015): 1-10.