International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

High Speed Fpga Implimantation of Rsd-Based Ecc Processor

K. Satish Goud & M.S. Shyam
M.Tech (VLSI & ES), St. Mary's College of Engineering and Technology, Hyderabad
Assistant Professor, St. Mary's College of Engineering and Technology, Hyderabad

Abstract-*In this paper, an exportable application-particular guideline set elliptic bend cryptography processor in light of repetitive marked digit portrayal is proposed. The processor utilizes broad pipelining systems for Karatsuba–Ofman technique to accomplish high throughput augmentation. Moreover, a productive particular snake without correlation and a high-throughput secluded divider, which brings about a short data path for expanded recurrence, are executed. The processor underpins the suggested NIST bend P256 and depends on a broadened NIST decrease plot. The proposed processor performs single-point increase utilizing focuses in relative arranges in 2.26 ms and keeps running at a greatest recurrence of 160 MHz in Xilinx Virtex 5 (XC5VLX110T) field-programmable entryway cluster.*

I. INTRODUCTION

Cryptography is tied in with creating and separating traditions that envision outcasts or individuals when all is said in done from examining private messages. Diverse points in information security, for instance, data protection, data respectability, check, and non-disavowal are critical to current cryptography. There are two sorts of cryptosystems: symmetric and unbalanced. In symmetric structures the same key that is the riddle key is used to encode and interpret a message. Since the key is shorter long in symmetric frameworks, they are speed in information control contrasted with hilter kilter systems [1]. Open key is used to scramble a message and private key is used to unscramble it by topsy-turvy frameworks. Security to correspondence can be expanded by utilizing topsy-turvy frameworks.

In beginning times diverse strategies like conundrum encryption machine, one-time cushion, pseudo irregular generator, diffiehelman key trade, what's more, steganography were utilized as a part of cryptography.

Cryptography

While performing duplication, expansion is used in the amassing technique [2], and furthermore in one sort of calculation known as twofold measured divider calculation which will be utilized in an unbalanced Cryptographic framework called as Elliptic bend cryptographic framework. With a specific end goal to remain far from long information ways because of convey spread; convey free number juggling is used in prime field ECC processors. A Redundant Signed Digit (RSDs) has been utilized as a part of diverse frameworks. It is vital to manufacture quick viable extension information way since it is a focal operation used in other secluded math operations. Measured duplication is a critical operation in ECC. Cell automata multiplier what's more, Fermat calculation for reversal has been to diagram the number-crunching unit in the limited field GF [3].

This paper proposes another RSD-based Modular Expansion/Subtraction and Multiplier for ECC processor with quick working repeat. The RSD portrayal is convey free math in which numbers are addressed by the qualification of two distinct numbers. The method for the RSD portrayal has the upside of performing extension and subtraction without the need of the two's supplement portrayal. On the opposite side, due to repetition in the portrayal of whole numbers an overhead is presented [4].

The curiosity of our processor advances around the accompanying. Literature review to be completed in the zone of usage of ECC processor utilizing VLSI

innovation. Review incorporates thinks about on various systems and distinctive calculation. Studies to be done on various existing method and furthermore existing calculations to accomplish the goals like expansion without reversal in blended co-ordinate, augmentation inside most limited timeframe, most elevated working recurrence, exchanging ability to other FPGA and ASIC. To perform point extension and point increasing over twofold field utilizing the calculation that has been created in view of karastuba multiplier.

Existing System:

In prime field ECC processors, carry free arithmetic is necessary to avoid lengthy data paths caused by carry propagation. Redundant schemes, such as carry save arithmetic (CSA), redundant signed digits (RSDs), or residue number systems (RNSs), have been utilized in various designs. Carry logic or embedded digital signal processing (DSP) blocks within field programmable gate arrays (FPGAs) are also utilized in some designs to address the carry propagation problem. It is necessary to build an efficient addition data path since it is a fundamental operation employed in other modular arithmetic operations [5]. Modular multiplication is an essential operation in ECC.

Two main approaches may be employed. The first is known as interleaved modular multiplication using Montgomery's method. Montgomery multiplication is widely used in implementations where arbitrary curves are desired. Another approach is known as multiply-then-reduce and is used in elliptic curves built over finite fields of Merssene primes. Merssene primes are the special type of primes which allow for efficient modular reduction through series of additions and subtractions [6,7]. In order to optimize the multiplication process, some ECC processors use the divide and conquer approach of Karatsuba–Ofman multiplications, where others use embedded multipliers and DSP blocks within FPGA fabrics.

Disadvantages:

1. Long data paths
2. Less frequency range

II. PROPOSED METHOD

In this System, an elliptical curve cryptography (ECC) processor based on Redundant signed digit (RSD) representation is represented. Here the processor employee's different techniques for Karatsuba-Ofman method in order to achieve high through put multiplication. The processor mainly consists of an AU of 256 RSD, a finite-state machine (FSM), Memory and two Data buses. As a result, an efficient Modular adder without comparison of 2's complement and a high-through put modular divider, it results in a shortest data path for maximized frequencies are represented. The Processor performs Single point multiplication employing points in affine coordinates in 2.26ms and runs at a maximum frequency of 160 MHZ in Xilinx Vertex 5. Here the Processor is implemented in FPGA (i.e.., Field Programmable Gate Array). As Karatsuba-Ofman Multiplier employs divide and conquer method. Here it divides a given operand into MSB and LSB and this continues until the operand is 8-bit length. Karatsuba multiplier is efficient with greater bit lengths and it is not efficient in lesser bit lengths. So, in order to overcome this problem of lesser bit length we go for proposed Design i.e.., Urdhva-Tiryagbhyam multiplier.

Low Power, Area & Delay are disadvantages in the proposed system. So, in order to overcome this problem, we go for Extension System Design to achieve low power Implementation.

Here in the Proposed Design System we go for Urdhva- Tiryagbhyam multiplier to reduce the quantity of phases required for multiplications that can be decreased. Here an Efficient floating-point multiplier is used. Urdhva-Tiryagbhyam multiplier is used to implement a binary multiplier for mantissa multiplication. It is finest algorithm for binary multiplications in terms of area and delay. Thus, Urdhva-Tiryagbhyam algorithm doesn't suit well if the input bit length is more. By designing the whole processor architecture, we can reduce the Power at lower efficient. Hence Low-Power is being achieved.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Block diagram and operation of the processor

The basic block diagram ie., overall processor architecture consists of an AU of 256 RSD digits (Urdhva-Tiryagbhyam Multiplier, Add/Sub and Division), an finite-state machine (FSM), Memory and two buses. The architecture is shown below.

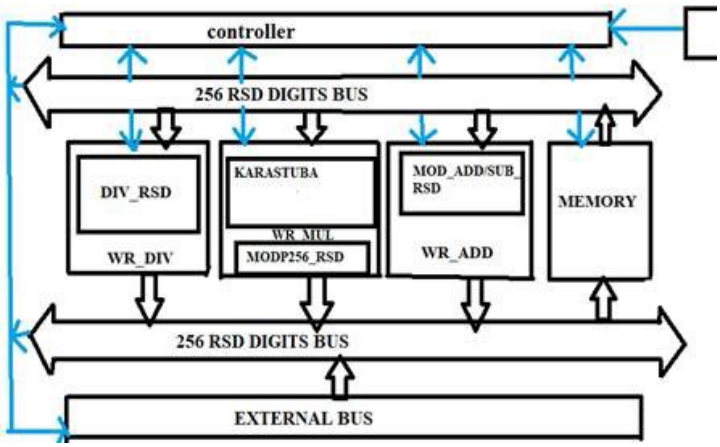


Figure 1: Block Diagram for Proposed Work

OPERATION: The Processor architecture contains mainly AU (Arithmetic Unit), Control Unit and Instruction Set. Here two sub-control units are attached to the main control unit as add-on-blocks. Different coordinate systems are easily supported by adding corresponding sub control blocks that operate according to the formulae of the coordinate system. Here now the external data is sent through the external data bus to 256RSD digits as input bus. Data is sent as binary format and a binary to RSD converter stuffs zeros in between the binary bits in order to create the RSD representation. As a result, 256-bits binary data represented as binary data are converted to 512-bits RSD represented integers.

III. PROPOSED WORK

The proposed processor was executed in Xilinx Virtex 5-XC5VLX110T FPGA and a solitary point multiplication for P256 is accomplished inside 2.26 ms. Itemized implementation consequences of individual pieces are recorded in Table V. Such point by point comes about are helpful in understanding the fundamental piece supporters of the general equipment assets. It can be noticed that the particular multiplier is the biggest piece inside the plan because of the three recursively fabricated Karatsuba squares, which work in parallel. With the broad pipelining techniques that are connected to the Karatsuba hinders, the CPD is abbreviated down to 6.24 ns. Such CPD figure permits the processor to work at 160 MHz, which is the speediest accomplished in the writing in FPGA gadgets without inserted pieces.

Our secluded divider plays out the quickest planning of prime field dividers and aggressive to twofold field GF2233 particular divider. The execution improvement is because of the use of RSD, which prompts short data path and high working recurrence. Effective engineering that depends on actualizing complex operations through straightforward moving single piece checking is another factor that gives our divider such upgrade. The exportability highlight of the processor originates from the way that none of the macros or installed obstructs inside the FPGA texture is used in the proposed processor. Such element gives our processor the flexibility to be actualized in various FPGA gadgets from various vendors and, inevitably, as an application-indicated incorporated circuit (ASIC). Henceforth, our processor is Look-Up Table (LUT)- based which implies that straightforward consistent operations can be mapped effortlessly to both, LUT on FPGA and standard cells on ASIC innovations. We surveyed the exportability highlight while considering the decency in comparing our processor with different processors proposed in the writing. Our processor is actualized in four diverse FPGA gadgets from Xilinx and one gadget from Altera.

We found that Xilinx Virtex E, Virtex 2 Pro, and Virtex 4 gadgets share a similar structure of 4 × 1 LUTs. Then again, Virtex 5 has a LUT setup of 6 × 2 which gives the upside of fusing bigger coherent net-works contrasted and the 4 × 1 design. A burden of 6 × 2 LUTs is that there is a high likelihood of under use of equipment assets since a basic 2 × 1

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

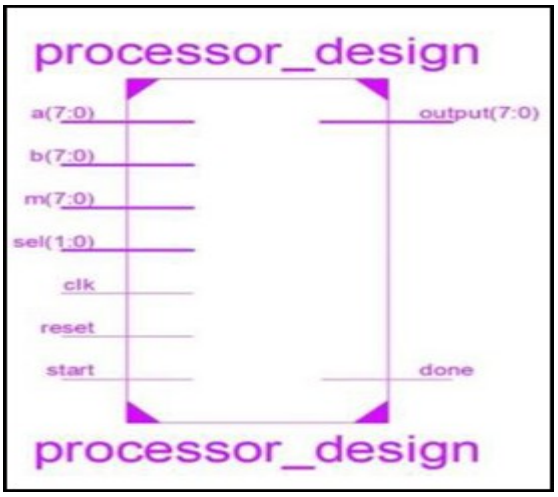
intelligent operation may possess an indistinguishable equipment assets from a completely 6 × 1 coherent system. Altera's versatile LUT (ALUT) in Cyclone and Stratix II gadgets tries to decrease the under usage issue of substantial LUTs. A solitary ALUT incorporates two 3 × 1 and two 4 × 1 LUTs which are utilized to give numerous setup alternatives of up to 7 × 1. Our processor is actualized in five unique gadgets as recorded in Table VIII. The processor involves ∼48 K of LUTs in gadgets with 4 × 1 LUTs, where it expends 34 K in Virtex 5 and 29 K in Cyclone FPGA. The most extreme working recurrence changes because of various variables, for example, the handling innovation of the gadgets, the interconnect models; the structure of the configurable obstructs, the thickness of the gadget, et cetera.

The two processors for each shape a solitary point augmentation inside practically a similar time. Notwithstanding, their work gets a noteworthy preferred standpoint using the inserted multipliers that enable them to perform incomplete 18*18 increase inside one clock cycles. This makes up the aggregate number of clock cycles to 32 clock cycles for a solitary full 256 secluded increase. In the event that the processor utilizes our secluded multiplier, at that point it would play out solitary point duplication in virtex 2 pro rather than 42-K LUTs and 32 implanted multipliers. Our processor keeps running at higher working recurrence and beats the processor .regarding scalar point increase by just about a twofold. Then again, the point increase quickening agent proposed is an extraordinary class without anyone else. This quickening agent utilizes effectively the DSP squares and the their committed interconnects to accomplish a high recurrence of 490 MHz Note that the detailed recurrence is achievable if just DSP squares are utilized with no control rationale, since other FPGA segments can't keep running at such recurrence. Subsequently, the outcomes detailed don't speak to a full useful ECC processor.

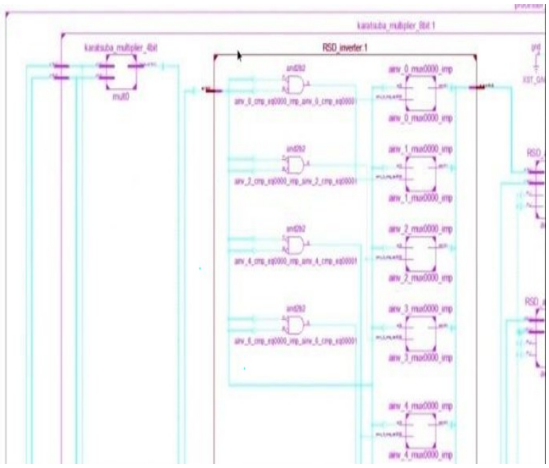
The processor deliberately picks base sizes that can be effectively mapped to the DSP obstructs inside Altera's Startix II gadget. Our processor is executed in Altera's Cyclone V gadget, which has the same ALUT structure as in Stratix II gadget. Despite the fact that the processor is based on substantially littler field sizes and enormously relies upon the DSP obstructs, our processor could accomplish a focused operating recurrence of 99 MHz, also the way that Cyclone gadgets are financially savvy and lower final results instead of Stratix II gadgets. This elite capacity is primarily acquired from the RNS framework. Moreover, RNS-based and could accomplish superior in a moderate gadget, for example, the Virtex E.

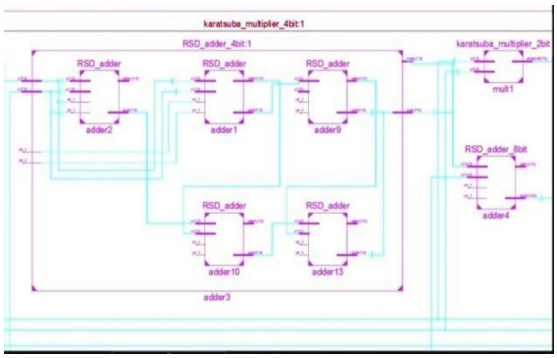
The plan system of our processor is like numerous CMOS-based ECC processors detailed in the writing. Most CMOS-based ECC processors embrace convey free number juggling, for example, CSA and RSD to keep away from long data paths. The processor is a word-based processor of 64-bit measure. It works on discretionary field sizes utilizing Montgomery duplication. With the interconnects overhead

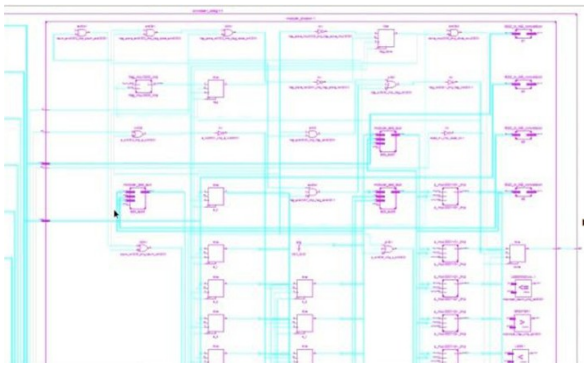
IV. SIMULATION RESULTS

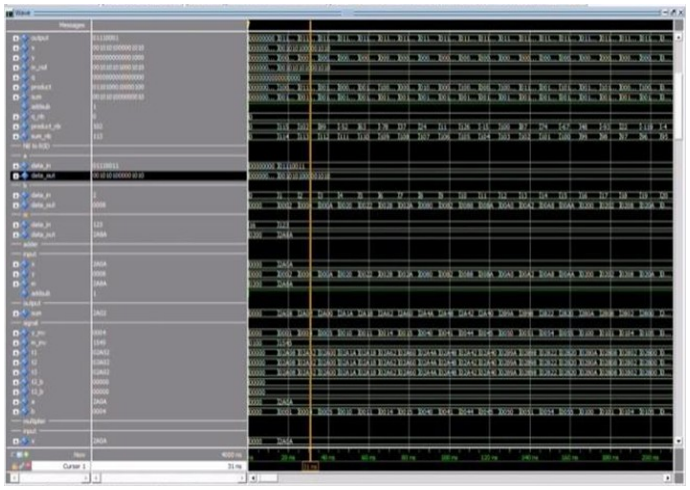


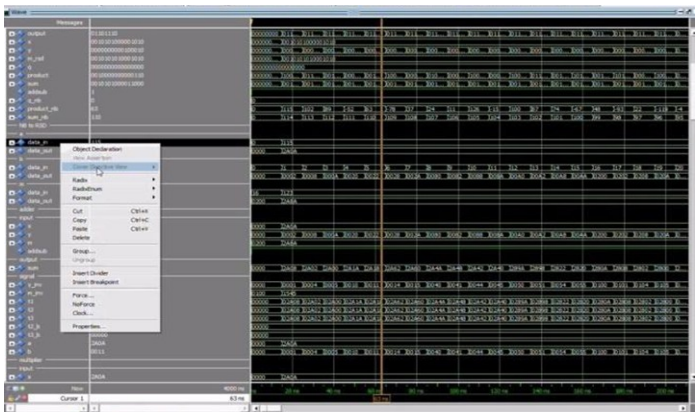
International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018











Advantages of ECC Processor

1. Short data paths
2. Increased maximum frequency
3. Used in Encryption data

APPLICATION OF ECC PROCESSOR

Elliptical Curve Cryptography is a technique which is used to approach a public and private key techniques based on elliptical curves over a finite field. This theory that can create faster, smaller and more efficient Cryptography keys. Cryptography is mainly used for security purpose.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

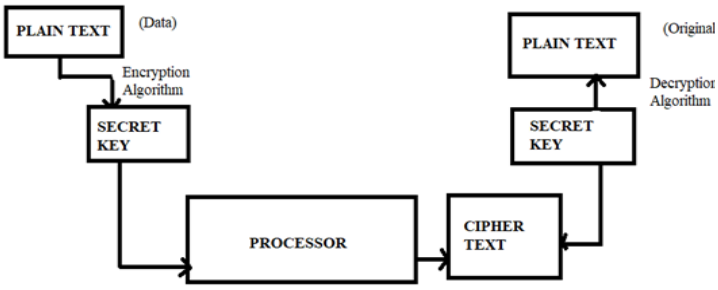


Figure 2: Encryption and Decryption Block Diagram

Operation of block diagram: From above Figure, a Plain text is taken as input and this plain text is being encrypted by encryption algorithm. Here after the text is been encrypted it is hided in secret key and this secret key is processed in the processor and the resultant encryption output i.e.., hidden data/ image/video is given to cipher text. From cipher text the encrypted data is given to secret key and there it processes by the decryption algorithm and thus final output is formed i.e., Original Plain text.

Solitary scalar point duplication is performed by our processor in shorter time than the processor. Be that as it may, the processor has the benefit of working on various field sorts and sizes rather than our processor, which works on committed NIST prime fields. Despite the fact that the processor worked over RSD number-crunching, our processor could accomplish higher throughput due to the broad pipelining strategies and the proficiency of the executed consistent operations. Correlation as far as equipment assets amongst FPGA-and CMOS-based plans is unfeasible since the correct entryway likeness diverse LUT arrangement is hard to ascertain or assess. In our plan, for example, a 6 × 1 LUT in Virtex 5 may speaks to an intelligent system of 48 entryways in one a player in the outline, and 12 doors in another piece of the outline.

The accomplished short basic way is expected to the enhanced pipelining methodologies utilized as a part of Karatsuba multiplier and the effective design of the divider. The utilization of RSD representation is basic in decreasing CPD of the processor.

Nonetheless, on the off chance that we represented the implanted multipliers and DSP obstructs that are used by most FPGA plans notwithstanding the convey rationale inside the FPGA, the equipment overhead because of RSD can be legitimized. Likewise, the expansion of such implanted pieces to the quantity of LUTs devoured by various plans makes our processor involves aggressive equipment assets figures, if not beating them. It is vital to take note of that there is no reasonable metric to change over DSPs and implanted multipliers to identical LUT so as to show reasonable correlation.

The power utilization is evaluated for the proposed processor utilizing XPower Analyzer apparatus in the Xilinx ISE 10.1 suit. The power utilization of the proposed processor running on Virtex 5 and working at recurrence 160 MHz is assessed at 1.755 W with dynamic power at 0.693 W. These power utilization estimations are computed for default working parameters of the gadget, for example, temperature at 25 °C, Vccint at 1 V, and VCCAUX and VCCO at 2.5 V.

V. 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 greatest recurrence. We presented upgraded pipelining procedures inside Karatsuba multiplier to accomplish high throughput execution by a completely LUT-based FPGA usage. A productive double GCD particular divider with three adders and moving operations is presented also. Besides, an effective secluded expansion/subtraction is presented in view of checking the LSD of the operands as it were. A control unit with add-on like design is proposed as a re-configurability highlight to help diverse point augmentation calculations and facilitate frameworks.

The usage consequences of the proposed processor demonstrated the most brief data path with a greatest recurrence of 160 MHz, which is the speediest

revealed in the writing for ECC processors with completely LUT-based plan. A solitary point augmentation is accomplished by the processor inside 2.26 ms, which is practically identical with ECC processors that depend on implanted multipliers and DSP obstructs inside the FPGA. The primary preferences of our processor incorporate the exportability to other FPGA and ASIC innovations and expandability to help distinctive organize frameworks and point increase calculations.

Future scope

To evaluate the practicality of the proposed project we can even achieve it in images and speeches. As in proposed project we have done encryption and decryption by taking input as data message. In future, we can even take image and speech messages as input for encrypting and decrypting. Here in proposed paper we have done in 180 nm and 90nm technology. There is a huge scope in doing this paper in 45nm technology also. Here by using different arithmetic unit techniques (addition, subtraction multiplication and division) we can modify Processor. We can also use this Urdhva-Tiryagbhyam Multiplier in for two variable multipliers using KCM and Vedic mathematics. And in application purpose we can use it in images and speeches. In this paper, we survey the various implementation approaches with the aim of providing a useful reference for hardware designers for building efficient ECC processors.

REFERENCES

[1] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987.

[2] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.

[3] C. Rebeiro, S. S. Roy, and D. Mukhopadhyay, "Pushing the limits of high-speed GF (2^m) elliptic curve scalar multiplication on FPGAs," in Proc. Cryptograph. Hardw. Embedded Syst. (CHES), vol. 7428. Jan. 2012, pp. 494–511.

[4] Y. Wang and R. Li, "A unified architecture for supporting operations of AES and ECC," in Proc. 4th Int. Symp. Parallel Archit., Algorithms Programm. (PAAP), Dec. 2011, pp. 185–189.

[5] 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.

[6] M. Esmaeildoust, D. Schinianakis, H. Javashi, T. Stouraitis, and K. Navi, "Efficient RNS implementation of elliptic curve point multiplication over GF(p)," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 8, pp. 1545–1549, Aug. 2012.

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