STM JOURNALS

Journal of VLSI Design Tools & Technology
ISSN: 2249-474X (Online), ISSN: 2321-6492 (Print)
Volume 7, Issue 3
www.stmjournals.com

High Speed and Low Area Energy Efficient FPGA Implementation using RSD based Elliptic Curve Cryptography

Abhay Arvind Koparde*, K. Sujatha
Department of Electronics and Telecommunication, Shree Ramchandra College of Engineering, Pune, Maharashtra, India

Abstract

In this paper we will study high speed energy efficient FPGA implementation using redundant sign digit elliptic curve cryptography. In existing system to design processor with high area and low speed computation process so that we proposed to low area with high speed computation using Elliptical cryptography processor. Here we use redundant signed digit to reduce the overhead due to computations. For modular arithmetic operation for multiplication, we used Karatsuba-Ofman algorithm; an efficient modular adder without comparison and a high throughput modular divider using GCD, which results in a short data path for maximum frequency, Processor arithmetic operation consist of 256 bits. This proposed processor supports P256 NIST prime field curve standards using Xilinx 14.7 software we analyze logic size, area and power consumption.

Keywords: *Application-specific instruction-set processor (ASIP), elliptic curve cryptography (ECC), field programmable gate array (FPGA), Karatsuba-Ofman multiplication, redundant signed digit (RSD), Greatest common divisor (GCD)*

****Author for Correspondence*** E-mail: aakoparde20@gmail.com

INTRODUCTION

Elliptic Curve Cryptography (ECC) is one of the most interesting research topics in VLSI. Network security in the world becoming more important crucial factor as the volume of data in network being exchanged on the Internet increases. ECC provides high security for networking and communication for data. Field programmable gate array (FPGA) based architecture for ECC co-processor, which has providing performance in terms of both Space Complexity and Time Complexity; is proposed in this paper. Co-processor consists of three levels of arithmetic operations, which consisting of elements operations over point added and doubled operations, scalar multiplication and binary finite field on elliptic curve. In this work on co-processor, point addition operation is performed with mixed co-ordinates to improve the performance of scalar multiplication. VHDL codes were developed for all these operations. The modules are simulated using Modelsim SE software and synthesized using Xilinx ISE software. Experimental results show that ECC co-processor realized in this architecture can speed up an elliptic curve scalar multiplication suitable for low area constraint applications and very high speed applications. This paper proposes a new RSD-based ECC processor with high-speed operating frequency. The processor consists of an application-specific instruction-set processor (ASIP) type which provides programmability and configurability. In this paper, we demonstrate arithmetic computation performance of left-to-right scalar point multiplication algorithm; however, the application specific instruction set which gives feature of the processor allows different algorithms for performing arithmetic performance by the through read-only memory (ROM) programming. Elliptical curve cryptography processor architecture consisting of 256 digit data buses which are used for modular arithmetic operation. This design strategy and most effective techniques are focused toward efficient individual modular arithmetic operation like multiplication, division, addition and subtraction modules rather than the overall architecture.

LITERATURE REVIEW

For RNS implementation of an Fp elliptical curve point multiplier, we have studied conversion of input from binary to RNS in encryption processor and vice versa as RNS to binary in decryption process [1].

We propose an extension of public key cryptosystem to support also private key for a unified architecture for supporting operation in-between Advanced Encryption Standard (AES) and ECC [2].

Implementation of hardware-software co-integration platform using an integrated prime field ECDLP hardware accelerator with high performance modular arithmetic unit [3].

In arithmetic multiplication operation in FPGA, we increase operating clock frequency instantly reducing number of clock cycle in pushing the limits of high speed ECC processor [4].

Better area-delay tradeoffs compared to state-of art implementation in efficient RNS implementation of elliptic curve point multiplication over GF(*p)* [5].

The NTRU cryptography is a lattice-based public key cryptography. This kind of cryptosystem is superior in arithmetic operation than other kind of public key cryptosystem to achieve high speed implementation, stable three moduli set {2n, 2n+1-1, 2n-1} is considered and the encryption cryptosystem and also part of decryption cryptosystem process which implemented by considered RNS bases [5].

ECC is a public cryptography which is used for small and secure operation especially for encryption of data for arithmetic operation [6].

For multi-layer system with increased hardware implementation convolution in ECC, a vast range of design and parameter choices affect the overall execution of ECC systems. This kind of survey has various execution towards approaches with the aim of providing a useful for hardware designers for building efficient ECC processors [7].

The design strategy is concentrated totally on modular arithmetic operation modules instead of total ECC processor architecture. ECC processor has a sufficient modular adder to reduce carry propagation problem in computational arithmetic process, a high throughput modular divider which results in maximum operating higher frequency and modular multiplier in the processor is effective based on throughput and modular reduction process in arithmetic [8].

PROPOSED SYSTEM

The architecture of the processor for ECC is of 256 digits which consist of Arithmetic Unit (AU) of 256 RSD digits wide, a finite state machine (FSM), memory and two data buses. It supports the prim curves recommended by as per NIST and can be configured in the pre-synthesis phase. Figure 1 shows the block diagram for the proposed system. Main control unit is attached with two sub-control units. These two sub- control units work as finite state machine for the operation of point addition and point doubling. Different co-ordinates systems are easily supported by adding corresponding sub-control blocks that works according to the formulas used for co-ordinate system. External data are passed through the external bus which enters the processor and is sent to the 256 RSD digits input bus. Binary data are being sent to the processor to get RSD data which is provided by a binary to RSD converter which stuffs zeros in between the binary bits. The ASIP feature of the processor allows different algorithm to be performed through Read Only Memory (ROM) which is being used to store the instruction set.

Different efficient architectures of various blocks like RSD divisor, Karatsuba-Ofman multiplication, Modular RSD addition-subtraction are proposed and it allows replacement of the above individual blocks if different algorithms or modular mathematical techniques are proposed. Binary GCD modular division algorithm is used where affine co-ordinates system is in work. All arithmetic computation is done by modular multiplication, addition and division through proposed system. The processor can be configured in the pre-synthesis phase to

support the P192 or P224 NIST recommended prime curve. This processor consists of modular base arithmetic unit as modular addition/subtraction block, modular multiplication block and modular division block as described each block main part of this processor to avoid lengthy carry free modular arithmetic multiplication as Karatsuba multiplication which is described in detail later. Considering application specific instruction set as ECC we will analysis all arithmetic value as waveform in modelsim as output with respect to input with modular M as carry free addition, multiplication division operation.

Elliptic Curve Cryptography (ECC)

It was introduced by Miller and Koblitz individually as an alternative solution in cryptographic system which is based on the discrete logarithm problem of a finite field. It is a kind of public key cryptosystem like RSA. But in ECC it is different from RSA in its faster developing capacity and providing at alternative way to analyze cryptographic algorithm. The security level which is given by RSA can be provided even by smaller keys of ECC. For given example, 1024 bit security capacity of a RSA could be managed by 163 bit security strength of ECC. It is a public key encoding technique based on elliptic curve cryptosystem that can be used to create smaller, faster and more effective cryptography keys. It generates keys through the equation of properties of the elliptic curve instead of the regular method of generation as the product of very large prime numbers. Most of public key encryption methods are co-related with each other, like Diffie-Hellman and RSA, According to analyst it can yield a level of security with a 164-bit key while other systems require a 1,024-bit key to achieve. Because it helps to establish equivalent security with lower computing power and area with minimum battery resource usage, it is becoming widely used for security in mobile applications. RSA has been developed its own version of ECC. It is based on properties of a particular type of equation created from the mathematical group that is a set of values of any two members of the group to produce a third part of derived from points where the line intersects the axes. To find which number was used by multiplying the point on the curve by a number will produce another point on the curve but it is very difficult, though if you know the result and original point on curve. In Elliptical curve equation we have cryptography capacity instead of regular method. For this cryptographic purpose they are relatively easy to perform and extremely difficult to reverse. In Eq. (1), shown plane curve which consists of the points along with a distinguished point at infinity (∞) in an elliptic curve. Algebraic variety which is underlying is from the structure of the group is inherited from the divisor group.

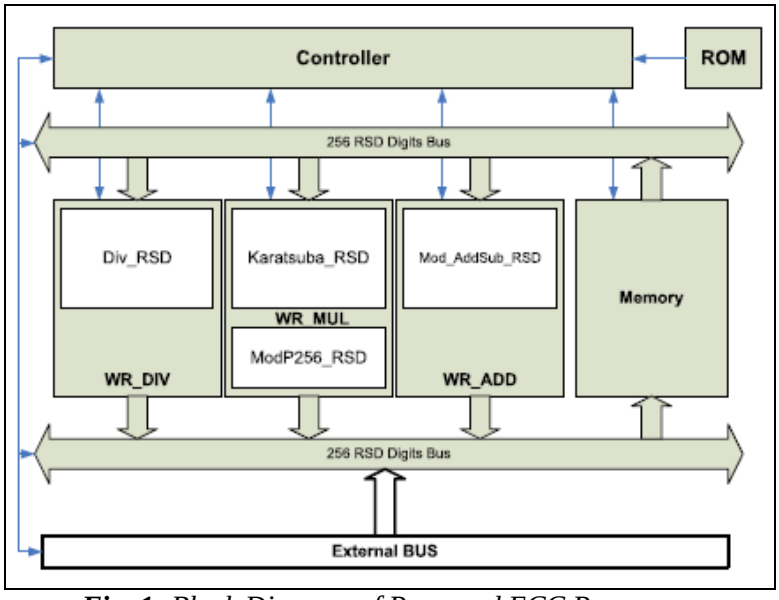

Fig. 1: *Block Diagram of Proposed ECC Processor.*

Elliptic curve for a field k is characterized by the weier strass condition given in Eq. (1), for two and three characteristic of the field the above equation is applicable.

$$E: y^2 = x^3 + ax + b \quad (1)$$

$4a^3 + 27b\text{^}2 \neq 0$ gives the smoothness of the curve and roots are ensured. Points addition and points doubling are performed to obtain the points. For point addition result is calculated by the following formula, assuming

P= (x_1, y_1),

Q= (x_2, y_2)

and R= P+Q= (x_3, y_3):

$$x_3 = \left\{\frac{y_2 - y_1}{x_2 - x_1}\right\}^2 - x_1 - x_2 \quad (2)$$

$$y_3 = \left\{\frac{y_2 - y_1}{x_2 - x_1}\right\}^1 (x_1 - x_3) - y_1 \quad (3)$$

Eqs. (2) and (3) gives the point co-ordinates by performing point addition operation. Similarly point doubling operation can be performed as follows:

$$x_3 = ((3(x_1)\text{^}2 + a)/2y_1)\text{^}2 - 2x_1 \quad (4)$$

$$x_3 = ((3(x_1)\text{^}2 + a)/2y_1)\,(x_1 - x_3) - y_1 \quad (5)$$

Eqs. (4) and (5) gives the point co-ordinates by performing point addition operation.

Redundant Signed Digits

For representation of single binary digit, we preferred redundant signed digits in numerical binary value system that uses more than required binary value which has several representation for conversion. An integer A is represented by the difference of its *a*+ and *a*− components, where *a*+ is the positive component and *a*− is the negative component. For arithmetic addition and subtraction without two's complement facility available in redundant sign digits while single binary generates overheads. On the other hand, an overhead is introduced due to the redundancy in the integer representation; since an integer in RSD representation requires double word length compared with typical two's complement representation. In radix-2 balanced RSD represented integers, digits of such integers are 1, 0, or −1.

Karatsuba-Ofman Multiplication

The regular multiplication complexity is given by $O(n^2)$. The methodology proposed by Karatsuba and Ofman gives the complexity $O(n^{1.58})$ for performing multiplication. In this the operands of the multiplication are divided into smaller and equal segments. Assume two operands of the multiplication of length n to be multiplied. The methodology splits the two operands into low and high segments.

$$a_H = (a_{n-1}, \ldots\ldots, a_{\frac{n}{2}}) \quad (6)$$

$$a_L = (a_{(\frac{n}{2})-1}, \ldots\ldots, a_0) \quad (7)$$

$$b_H = (b_{n-1}, \ldots\ldots, b_{\frac{n}{2}}) \quad (8)$$

$$b_L = (b_{(\frac{n}{2})-1}, \ldots\ldots, b_0) \quad (9)$$

The multiplication of both operands is executed as following equation when consider β as the base for the operands, where β is 2 in case of integers and β is x in case of polynomials.

$$a = a_L + a_H \beta^{\frac{n}{2}}$$

and

$$b = b_L + b_H \beta^{\frac{n}{2}}$$

Four half-sized duplications are required, where Karatsuba procedure reformulate

$$C = AB = \left(a_L + a_H \beta^{\frac{n}{2}}\right)\left(b_L + b_H \beta^{\frac{n}{2}}\right) \quad (10)$$

$$= a_L b_L + (a_L b_H + a_H b_L)\beta^{\frac{n}{2}} + a_H b_H (\beta\text{^}n). \quad (11)$$

Therefore, only three half-sized multiplication are needed. Karatsuba algorithm is performed repetitive operation, where the operands are split into smaller parts until a required size is reached and the regular multiplication with smaller segments is performed.

Binary GCD Modular Division

A modular division algorithm is proposed based on the extended Euclidean algorithm. This algorithm is considered as the basis for several hardware implementations of modular division. This algorithm computes the modular division Z ≡x/y (mod M) based on the plus–minus version of the original binary GCD algorithm. The algorithm represents the four registers consist of a,b,u and v which is initialized with y,m,x and o according with four registers. From that, it regularly reduces the values of y and m in order to calculate the Greatest Common Division (y,m) which is equal to 1 in well-formed elliptic curves where the modulo is prime. The registers u and v are used to calculate the quotient and the

operations performed on these registers are similar to the operations performed on the a and b registers [9]. The operations on the registers a and b are performed by repetitively reducing the contents of both register by simple shift or add/subtract-shift operations based on the conditions whether the intermediate contents are even or not [10]. In the case where both registers contents are odd, the content of both registers are added if (a+b) is divisible by 4 or subtracted, (a−b), otherwise. ρ and δ are two variables which is used to control the iterations of the algorithm based on the bounds of the registers contents, where δ=α−β, 2α and 2β are the upper bounds of A and B, respectively, and ρ=min(α, β).

RESULTS

The result is described in Tables 1 and 2 with pictorial representations in Figures (1–3).

Table 1: *Type of Designs with respect to Slices, Mhz and ns.*

Metrics	Existing Design	Proposed Design
Slices	3140	2349
Maximum frequency (MHz)	169	169
Delay (ns)	1860	20.03

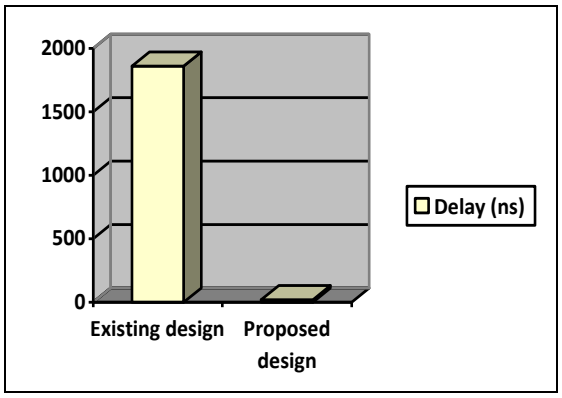

Fig. 2: *Graphical Representation of Design with respect to Range (0–2000).*

Table 2: *Type of Metrices with respect to Multiplier.*

Analyzed Metrics	Modular Add/Sub	Modular Multiplier
Slices	80	795
LUT's	50	634
Flip-Flop	50	342
Maximum Frequency (MHz)	160	120

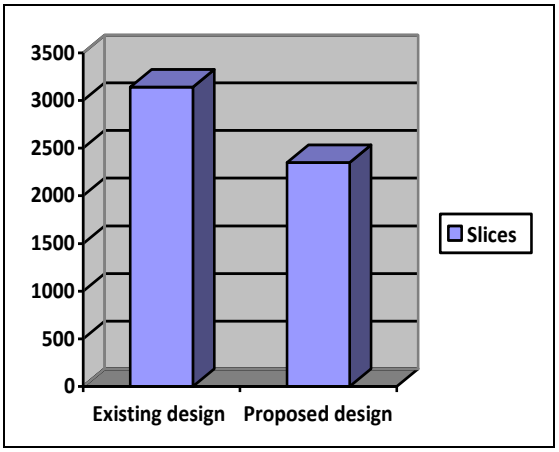

Fig. 3: *Graphical Representation of Design with respect to Range (0–3500).*

CONCLUSION

In this paper, ECC processor arithmetic operation implementation in FPGA has been presented. A Redudand Sign Digit as a carry free arithmetic representation is executed which results in short data paths and increased maximum frequency. We introduced enhanced Karatsuba multiplier pipelining techniques within to achieve high throughput performance by a fully LUT-based FPGA implementation. An efficient binary GCD modular divider with three adders and shifting operations is introduced as well. Furthermore, an efficient modular addition/subtraction is introduced based on checking the LSD of the operands only. A control unit with add-on like architecture is proposed as a reconfigurability feature to support different point multiplication algorithms and co-ordinate systems. The implementation results of the proposed processor showed the shortest data path with a maximum frequency of 160 MHz, which is fastest reported in the literature for ECC processors with fully LUT-based design. The implementation results of the proposed system improves the performance of the processor in speed and reduces the area as LUT's required is less, hence low power consumption processor is proposed.

REFERENCES

1. Schinianakis DM, Fournaris AP, Michail HE, *et al.* An RNS implementation of an *Fp* elliptic curve point multiplier, *IEEE Trans Circuits Syst. I, Reg. Papers*, Jun. 2009; 56(6): 1202–1213p.

2. Wang Y, Li R. A unified architecture for supporting operations of AES and ECC, in *Proc. 4th Int. Symp. Parallel Archit., Algorithms Programm. (PAAP)*, Dec. 2011, 185–189p.
3. Mane S, Judge L, Schaumont P. An integrated prime-field ECDLP hardware accelerator with high-performance modular arithmetic units, in *Proc. Int. Conf. Reconfigurable Comput. FPGAs*, Nov./Dec. 2011, 198–203p.
4. Rebeiro C, Roy SS, Mukhopadhyay D. Pushing the limits of high-speed GF(2*m*) elliptic curve scalar multiplication on FPGAs, in *Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, Jan. 2012; 7428: 494–511p.
5. Esmaeildoust M, Schinianakis D, Javashi H, *et al.* Efficient RNS implementation of elliptic curve point multiplication over GF(*p*), *IEEE Trans Very Large Scale Integr. (VLSI) Syst.* Aug. 2012; 21(8): 1545–1549p.
6. Hamad Marzouqi, Mahmoud Al-Qutayri, Khaled Salah, *et al.* A High-Speed FPGA Implementation of an RSD-Based ECC Processor, *IEEE Trans Very Large Scale Integr. (VLSI) Syst.* Aug. 2015; 21(8: 1545–1549p.
7. Esmaeildoust M, Schinianakis D, Javashi H, *et al.* Efficient RNS implementation of elliptic curve point multiplication over GF (p), *IEEE Trans Very Large Scale Integr. (VLSI) Syst.* Aug. 2012; 21(8): 1545–1549p.
8. Mane S, Judge L, Schaumont P. An integrated prime-field ECDLP hardware accelerator with high-performance modular arithmetic units, in *Proc. Int. Conf. Reconfigurable Comput. FPGAs*, Nov./Dec. 2011, 198–203p.
9. Anupama T, Manjunath MB. Fpga implementation of elliptic curve crypto processor over gf(2163): A Review, *Intl J Sci Eng Technol Res (IJSETR)*. May 2014; 3(5): 1238–1240p.
10. Uma Maheswari, Vivitha V, Siva Priya T. Optimized Arithmetic Modules of a RSD-Based ECC Processor, *IJEET*. 8(01): Jan-June 2016.

Cite this Article
Abhay Arvind Koparde, K. Sujatha. High Speed and Low Area Energy Efficient FPGA Implementation using RSD based Elliptic Curve Cryptography. *Journal of VLSI Design Tools & Technology*. 2017; 7(3): 45–50p.