RESEARCH ARTICLE OPEN ACCESS

A High-Speed FPGA Implementation of an RSD-Based ECC Processor

[1]K Durga Prasad, [2]M.Suresh kumar

[1]M-Tech, Dept. of ECE, Kakinada Institute of Engineering and technology, korangi.

[2]Asst , Dept. of ECE, Prof in Kakinada Institute of Engineering & Technology, Korangi

Abstract:

In this paper, an exportable application-specific instruction-set elliptic curve cryptography processor based on redundant signed digit representation is proposed. The processor employs extensive pipelining techniques for Karatsuba–Of man method to achieve high throughput multiplication. Furthermore, an efficient modular adder without comparison and a high through put modular divider, which results in a short data path for maximized frequency, are implemented. The processor supports the recommended NIST curve P256 and is based on an extended NIST reduction scheme. The proposed processor performs single point multiplication employing points in affine coordinates in 2.26 ms and runs at a maximum frequency of 160 MHz in Xilinx Virtex 5 (XC5VLX110T) field-programmable gate array.

Keywords — **ASIP, ECC, field-programmable gate array, RSD.**

1. INTRODUCTION

Elliptic curve cryptography (ECC) is an asymmetric cryptographic system that provides an equivalent security to the well-known Rivest, Shamir and Adleman system with much smaller key sizes. The basic operation in ECC is scalar point multiplication, where a point on the curve is multiplied by a scalar. A scalar point multiplication is performed by calculating series of point additions and point doublings. Using their geometricalproperties,points are addedor doubled through series of additions, subtractions, multiplications, and divisions of their respective coordinates. Point coordinates are the elements of finite fields closed under a prime or an irreducible polynomial. Various ECC processors have been proposed in the literature that either target binary fields, prime fields, or dual field operations. In prime field ECC processors, carry free arithmetic is necessary to avoid lengthy datapaths 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 fieldprogrammable gate arrays (FPGAs) are also utilized in some designs to address the carry propagation problem. It is necessary to build an efficient addition datapath since it is a fundamental operation employed in other modular arithmetic operations. 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. 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.

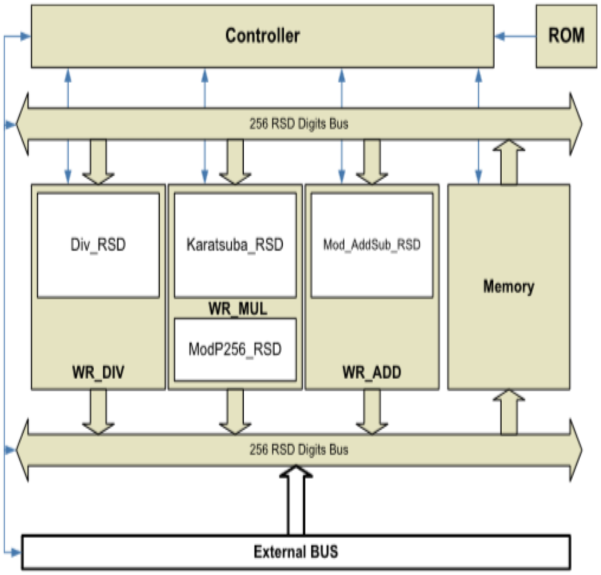


Fig. 1. Overall processor architecture.

External data enter the processor through the external bus to the 256 RSD digits input bus. Data are sent in binary format and a binary to RSD converter stuffs zeros in between the binary bits in order to create the RSD representation. Hence, 256-bits binary represented integers are converted to 512-bits RSD represented integers. To convert RSD digits to binary format, one needs to subtract the negative component from the positive component of the RSD digit.

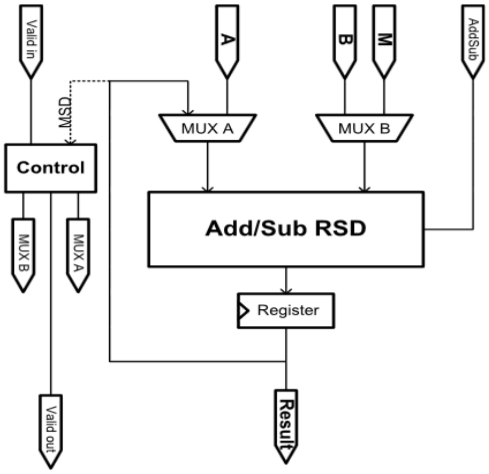
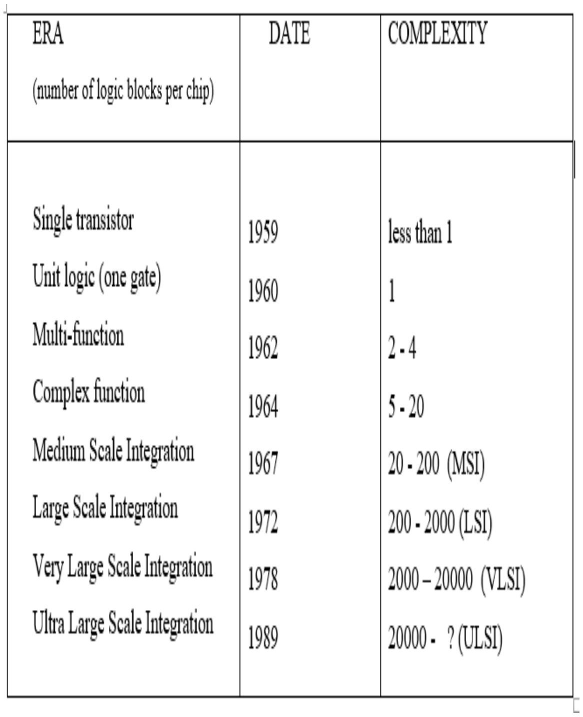


Fig. 2. Modular addition subtraction block diagram.



ERA (number of logic blocks per chip)	DATE	COMPLEXITY
Single transistor	1959	less than 1
Unit logic (one gate)	1960	1
Multi-function	1962	2 - 4
Complex function	1964	5 - 20
Medium Scale Integration	1967	20 - 200 (MSI)
Large Scale Integration	1972	200 - 2000 (LSI)
Very Large Scale Integration	1978	2000 – 20000 (VLSI)
Ultra Large Scale Integration	1989	20000 - ? (ULSI)

In order to overcome the problem of overflow introduced in the adder proposed in, a new adder is proposed based on the work proposed in. The proposed adder consists of two layers, where layer 1 generates the carry and the interim sum, and layer 2 generates the sum, as shown in Fig. 3. Table I shows the addition rules that are performed by layer 1 of the RSD adder, where RSD digits 0, +1, and −1 are represented by Z, P, andN, respectively. It works by assuring that layer 2 does not generate overflow through the use of previous digits in layer 1. The proposed adder is used as the main block in the modular addition component to take advantage of the reduced overflow feature. However, overflow is not an issue in both the multiplier and the divider when an RSD adder is used as an internal block. Hence, the reduced area is taken as an advantage in instantiating adders within the multiplier and the divider. The n-digits modular addition is performed by three levels of RSD addition. Level 1 performs the basic addition of the operands which produces n+1 digits as a result. If the most significant digit (MSD) of level 1 output has a value of 1/−1, then level 2 adds/subtracts the modulo P256 from the level 1 output correspondingly. The result of level 2 RSD addition has n+2 digits; however, only the n+1th digit may have a value of 1/−1. This assertion is backed up by the fact that the operation of level 2 is a reversed operation with the modulo P256, and most importantly, the proposed adder assures that no unnecessary overflow is produced. If the n+1th digit of level 2 result has a value 1 or −1, then level 3 is used to reduce the output to the n-digit range. Algorithm 3 shows the sequence of operations performed by the modular addition block. Notice that one modular addition is performed within one, two, or three clock cycles.

2. SIMULATIONIMPLEMENTATION

GENERAL

The proposed processor was implemented in Xilinx Virtex 5-XC5VLX110T FPGA and a single point multiplication for P256 is achieved within 2.26 ms. Detailed implementation results of individual blocks are listed in Table V. Such detailed results are useful in understanding the main block contributors to the overall hardware resources. It can be noted that the modular multiplier is the largest block within the design due to the three recursively built Karatsuba blocks, which operate in parallel. With the extensive pipelining techniques that are applied to the Karatsuba blocks, the CPD is shortened down to 6.24 ns. Such CPD figure allows the processor to operate at 160 MHz, which is the fastest achieved in the literature in FPGA devices without embedded blocks. Detailed timing performance of operations performed by the processor that is operating at 160 MHz on Virtex 5 device are listed in Table VI. Table VII lists a comparison of our modular divider implementation results against other FPGA-based designs. Our modular divider performs the fastest timing of prime field dividers and competitive to binary field GF2233 modular divider. The performance enhancement is due to the usage of RSD, which leads to short datapath and high operating frequency. Efficient architecture that is based on implementing complex operations through simple shifting single bit checking is another factor that gives our divider such enhancement. Finally, the modular divider operates on higher radix which results in improved throughput. The exportability feature of the processor comes from the fact that none of the macros or embedded blocks within the FPGA fabric is utilized in the proposed processor. Such feature gives our processor the freedom to be implemented in different FPGA devices from different vendors and, eventually, as an application-specified integrated circuit (ASIC).

VERILOG

Verilog is a HARDWARE DESCRIPTION LANGUAGE (HDL). A hardware description Language is a language used to describe a digital system, for example, a network switch, a microprocessor or a memory or a simple flip−flop. This just means that, by using a HDL one can describe any hardware (digital) at any level. One can describe a simple Flip flop as that in above figure as well as one can describe a complicated designs having 1 million gates. Verilog is one of the HDL languages available in the industry for designing the Hardware. Verilog allows us to design a Digital design at Behaviour Level, Register Transfer Level (RTL), Gate level and at switch level. Verilog allows hardware designers to express their designs with behavioural constructs, deterring the details of implementation to a later stage of design in the final design.

Verilog differ from software programming languages and Hardware description languages because they include ways of describing the propagation of time and signal dependencies (sensitivity).

3. SIMULATION RESULTS

4.

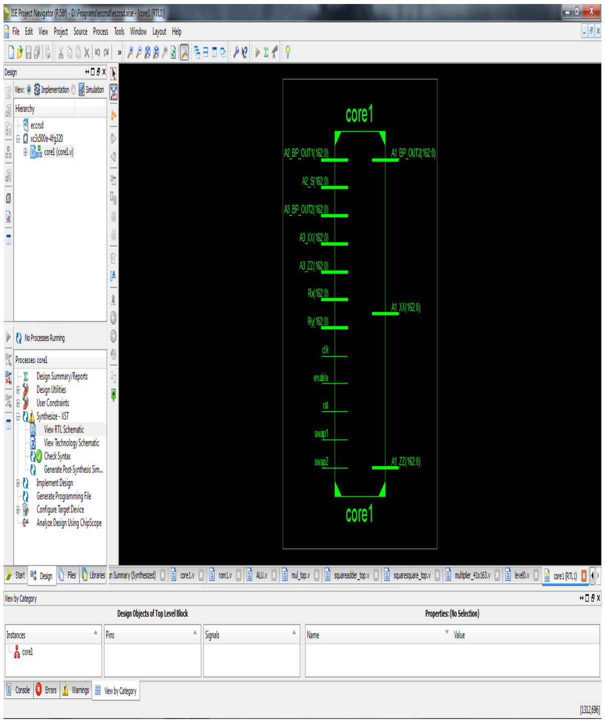


Fig:-3 Schematic output

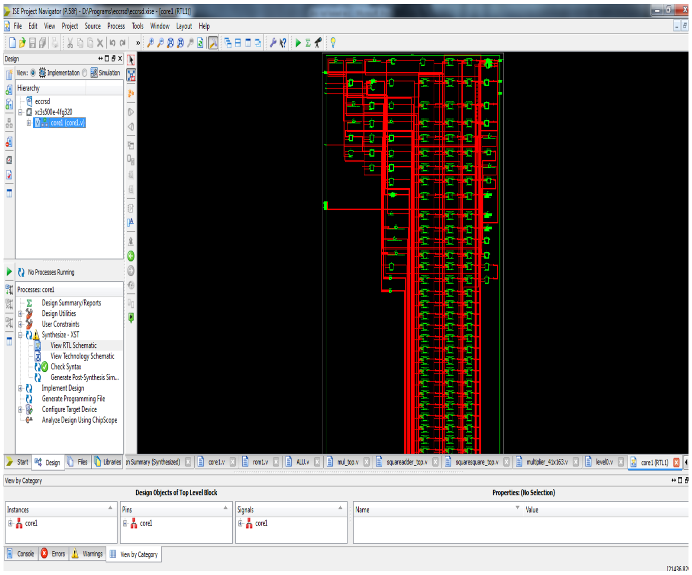
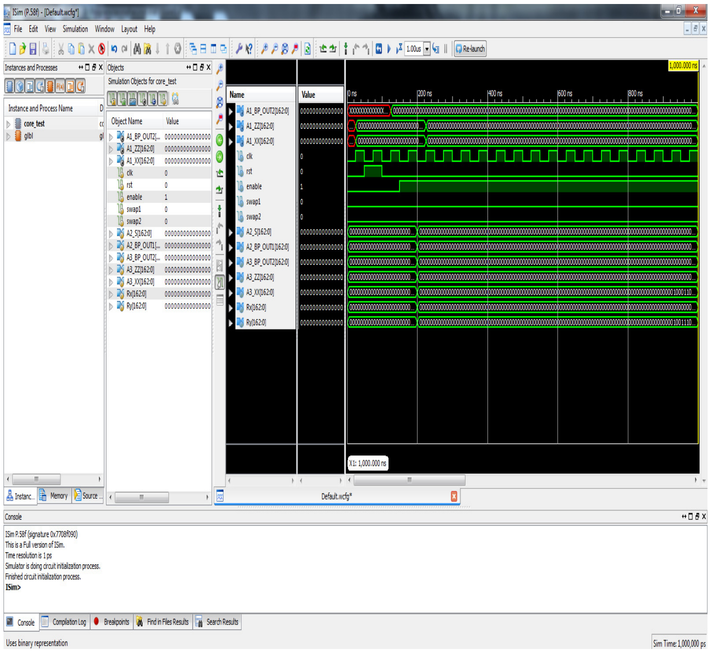


Fig:-4 Schematic internal



```
ISim P.58f (signature 0x7708f090)
This is a Full version of ISim.
Time resolution is 1 ps
Simulator is doing circuit initialization process.
Finished circuit initialization process.
ISim>
```

Fig:-5 Simulation output

5. CONCLUSION

In this paper, a NIST 256 prime field ECC processor implementation in FPGA has been presented. An RSD as a carry free representation is utilized which resulted in short datapaths and increased maximum frequency. We introduced enhanced pipelining techniques within Karatsuba multiplier 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 coordinate systems. The implementation results of the proposed processor showed the shortest datapath with a maximum frequency of 160 MHz, which is the fastest reported in the literature for ECC processors with fully LUT-based design. A single point multiplication is achieved by the processor within 2.26 ms, which is comparable with ECC processors that are based on embedded multipliers and DSP blocks within the FPGA. The main advantages of our processor include the exportability to other FPGA and ASIC technologies and expandability to support different coordinate systems and point multiplication algorithms.

6. 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(2m) 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 Fp elliptic curve point multiplier,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 56, no. 6, pp. 1202–1213, Jun. 2009.

[8] J.-W. Lee, S.-C. Chung, H.-C. Chang, and C.-Y. Lee, “Efficient poweranalysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 1, pp. 49–61, Feb. 2013.

[9] J.-Y. Lai and C.-T. Huang, “Energy-adaptive dual-field processor for high-performance elliptic curve cryptographic applications,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 8, pp. 1512–1517, Aug. 2011.

[10] 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.

Authors Profile

I Durga Prasad was born in samanthakurru, Andhara Pradesh on August 19, 1993 .I graduated from the Bonam Venkata Chalamayya Institute of technology & science (jntuk).Presently Iam studying M tech in Kakinada Institute of Engineering and technology , korangi

M.Suresh kumar

Mr M.SURESH KUMAR was born GIDDALUR, AP, on DECEMBER 20 1986. He graduated from the Kakinada institute of engineering and technology, JNTU Hyderabad, Post-graduated from the Kakinada institute of engineering and technology, JNTU Kakinada, Presently He is working as an Asst Prof in Kakinada Institute of Engineering & Technology, Korangi. So far he is having 3 Years of Teaching Experience in various reputed engineering colleges. His special fields of interest included VLSI-embedded system, analog and digital communications.