International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

An Optimized FPGA Implementation of RSD Based ECC Processor

M. Rajeswari[1], M. Vijaya Laxmi[2]

1M.Tech, PG Scholar, Department of ECE, Srikalahasteeswara Institute of Technology, Srikalahasthi-India
2Associate Professor, Department of ECE, Srikalahasteeswara Institute of Technology, Srikalahasthi –India

Abstract: ***Elliptic Curve Cryptography (ECC) is a standout amongst the most interested exploration themes in VLSI. System security is turning out to be increasingly significant as the volume of information being traded on the Internet increments. Point addition and doubling are key operations which choose the Performance of ECC. Here the design with the information way which can perform either prime field G(p) operations or binary field G(2m) operations for arbitrary prime numbers has been proposed. Utilizing this design we can accomplish the high throughput of the both fields that is prime and binary fields. A high throughput modular divider (mod 4n) which results in maximum operating frequency and modular multiplier in the processor is optimized based on throughput and modular reduction. The adder is focused for optimization as the addition is needed for accumulation process in multiplication and division. The Xilinx Virtex 5 field programmable gate array has been utilized.***

Keywords: point doubling, Redundant Signed Digit (RSD), point addition

1. Introduction

Public Key encryption algorithms are widely used to ensure the data security of network communications. Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic system which provides higher security than the Rivest, Shamir and Adleman system (RSA) system. The basic operation in ECC is scalar point multiplication which multiples a point on the curve by a scalar.

A scalar point multiplication is performed by calculation of series point additions and point doublings. Points are added or doubled through series of additions, subtractions, multiplications and divisions, point doubling of their respective co-ordinates on using their geometrical properties. Point coordinates are the elements of finite fields closed under a prime or an irreducible polynomial.

Various ECC Processors were proposed in the literature targets binary fields, prime fields or dual field operations.

Modular multiplication is an essential operation in ECC. Some ECC processors use the divide and conquer approach of Karatsuba multipliers for optimization of multiplication process where others use embedded multipliers and DSP blocks within FPGA fabrics.

The Overall processor architecture is of regular cross bar type and has 256 digit wide data buses. The processor is an application-specific instruction-set processor (ASIP) type to provide program ability and configurability.

Our aim is to challenge the basic assumptions about public key cryptography which are based on a traditional software based approach. We propose a custom hardware assisted approach for which we claim that it makes public key cryptography feasible for low-power applications, provided we use the right selection of algorithms.

2. Problem Statement

The problem occurs in ECC processor are redundant signed digits and modulus addition which occurs mainly in binary and number fields

Redundant Signed Digits:

The RSD representation, first introduced by Avizienis is a carry free arithmetic where integers are represented by the difference of two other integers. An integer X is represented by the difference of its x+ and x− components, where x+ is the positive component and x− is the negative component. The nature of the RSD representation has the advantage of performing addition and subtraction without the need of the two's complement representation.

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. RSD-based Modular Addition/Subtraction and Multiplier for ECC processor with fast working recurrence. The RSD representation is a carry free arithmetic in which numbers are spoken to by the distinction of two different numbers. The way of the RSD representation has the upside of performing expansion and subtraction without the need of the two's supplement representation. On the other side, because of redundancy in the representation of integers an overhead is introduced. The novelty of our processor revolves around the following.

- Studies to be carried out on different existing technique and also existing algorithms to achieves the objectives like addition without inversion in mixed co-ordinate, multiplication within shortest period of time, highest operating frequency, transferring capability to other FPGA and ASIC technologies.
- To perform point expansion and point multiplying over binary field using the algorithm that has been developed based on Karatsuba and Vedic multiplication

- Literature survey to be carried out in the area of implementation of ECC processor using VLSI technology. Survey includes studies on different techniques and different algorithm.
- Then the Verilog code will be written for algorithms of key operations of ECC processor and implemented in virtex 5 FPGA board.

3. Elliptic Curves Over Dualfield

Elliptic curve serves as good trapdoor function that is an algorithm which is simple in one direction and hard in another direction.

The curves are named as elliptic curves as they are illustrated by equations which are in cubic form, which are taken for calculating the circumference.

Elliptic bends are simple capacities which can be drawn as smooth circling lines in (x, y) plane. By and large, cubic condition for elliptic bend can be given by utilizing summed up Weierstrass equation as given in

$$Y^2 + m_1xy + m_3y = m_2x^2 + m_4x + m_6$$

Where $m_1, m_2, m_3, m_4, m_5, m_6 \epsilon$ Fp and p is a prime integer

An elliptic bend with group of points (x,y) over the real numbers forms a abelian group if it satisfy the condition as shown in equation

$$Y^2 = x^3 + m^2x + n$$

Where m and n are real numbers, x and y use the values in the real numbers. The two finite fields over which the elliptic curves are mainly defined are:

- Binary field GF (2^n)
- Prime field GF (p)

For prime field the elliptic curve equation is given by,

$$Y^2 \bmod p = (x^3 + cx + d) \bmod p$$

Elliptic curve equation over Binary field is given by

$$Y^2 + xy = x^3 + ax^2 + b$$

ECC over binary field achieves the high performance without considering the carry and modular reduction. These fields are ideal for the utilization in equipment as far as speed and area.

3.1 Binary Field

The most imperative elliptic curve conditions are (Weierstrass condition in GF (2m)) for binary field. In binary field, addition is XOR operation and multiplication is polynomial based, and the result is reduced by using the irreducible polynomial. Squaring is achieved by shift operation. So multiplication is performed based on the hybrid Karatsuba multiplier. Here primary focus is on ECC over binary field based on the short Weierstrass equation.

$$Y^2 + xy = x^3 + ax^2 + b$$

3.1.1Point Addition over Binary field

In this method, one point is in projective Co-ordinate and another point is an affine Co-ordinate. The output point that results will appear in projective Co-ordinate so that the operation like inversion will be avoided.

$$Y^2 \bmod p = (x^3 + cx + d) \bmod p$$

3.1.2 Point doubling over binary field:

Adding the point over the elliptic curve to itself is known as point doubling. In these equations ‘a’ & ‘b’ are considered as parameters of elliptic curve.

3.2 Prime Field

The most imperative elliptic curve conditions are

$$Y^2 = x^3 + cx + d$$

(Weierstrass condition in GF (p)) for prime field. The fixed number of modular multiplications, squares, additions, shifts, and basic arithmetic operations are required while performing addition and doubling over each elliptic curve. The real number of these operations relies on upon the way the bend is spoken to; as a rule it is multiplications and squaring operations that rule the running time, and the running the reality of the situation will become obvious eventually precisely with the quantity of arithmetic operations required. Here primary focus will be on ECC over prime field based on the short Weierstrass equation.

3.2.1. Point addition over Prime field:

The elliptic curve considered in GF (p), has the general elliptic point (x,y) which is projected to (X1,Y1,Z1), where x=X/Z2, and y=Y/Z3 and the second point considered is affine point that is (x2,y2).

3.2.2 Redundant signed digits:

The RSD representation, first introduced by Avizienis, is a carry free arithmetic where integers are represented by the difference of two other integers. An integer X is represented by the difference of its x+ and x− components, where x+ is the positive component and x− is the negative component.

The nature of the RSD representation has the advantage of performing addition and subtraction without the need of the two’s complement representation. 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 either 1, 0, or −1.

4. The Elliptic Curve Architecture

We developed an elliptic curve architecture using the scaled modulus technique and our specialized inversion algorithm.

Our aim in implementing this hardware was to actually see the outcomes of our techniques.

4.1 Design Methodology

We built our elliptic curve scheme over the prime field GF $((2^{167}+1) =3)$. This particular prime allows us to use a scaled modulus $m = 2^{167} + 1$ with a very small scaling factor $s = 3$. To implement the field operations we use Algorithm.

Our simulation for this particular choice of prime showed that our inversion technique is only by about three times slower than a multiplication operation. Furthermore, the inversion is implemented as a division saving one multiplication.

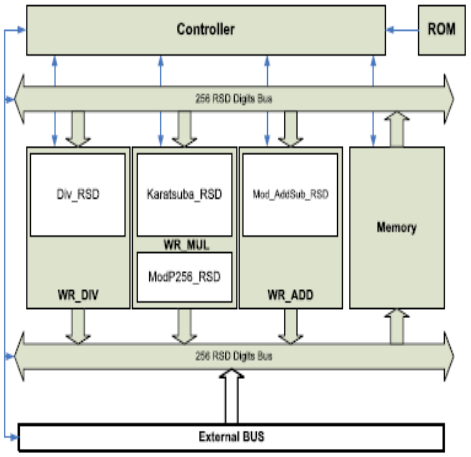

Figure: ECC processor architecture

Operation. Thus the actual ratio is closer to two. Since inversion is relatively fast, we prefer to use affine coordinates.

Besides faster implementation, affine coordinates provides a significant amount of reduction in power and circuit area since projective coordinates requires a large amount of extra storage. For an elliptic curve of form

$$Y^2 = x^3 + ax + b$$

defined over GF $(2^{167} + 1)=3)$ we use the standard point addition operation defined in.

For power efficiency we optimize our design to include minimal hardware. An effective strategy in reducing the power consumption is to spread the computation to a longer time interval via serialization which we employ extensively.

On the other hand, a reasonable time performance is also desired. Since the elliptic curve is defined over a large integer field GF (p) (168-bits) carry propagations are critical in the performance of the overall architecture. To this end, we built the entire arithmetic architecture using the carry-save methodology. This design choice regulates all carry propagations and delivers a very short critical path delay, and thus a very high limit for the

Operating frequency. The redundant representation doubles all registers in the arithmetic unit, i.e. we need two separate registers to hold both the carry part and the sum part of a number.

Furthermore, the inherent difficulty in comparing numbers represented in carry-save notation is another challenge. In addition, shifts and rotate operations become more cumbersome. Nevertheless, as evident from our design it is possible to overcome these difficulties.

In developing the arithmetic architecture we primarily focused on finding the minimal circuit to implement Algorithm X efficiently. Since the architecture is built around the idea of maximizing hardware sharing among various operations, the multiplication, squaring and addition operations are all achieved by the same arithmetic core. The control is hierarchically organized to implement the basic arithmetic operations, point addition, point doubling, and the scalar point multiplication operation in layers of simple state machines. The simplicity of Algorithm X and scaled arithmetic allows us to accomplish all operations using only a few small state machines.

5. Results

Below results show the simulation output for power report, synthesis report, and delay report.

Comparison Results

	Existing design	Proposed design
Slices	3140	2923
Maximum frequency (Mhz) (operating frequency for only one cycle)	169	100
Delay (ns)	66.10	36.10
Power(w)	1.795	1.257

Simulation Outputs

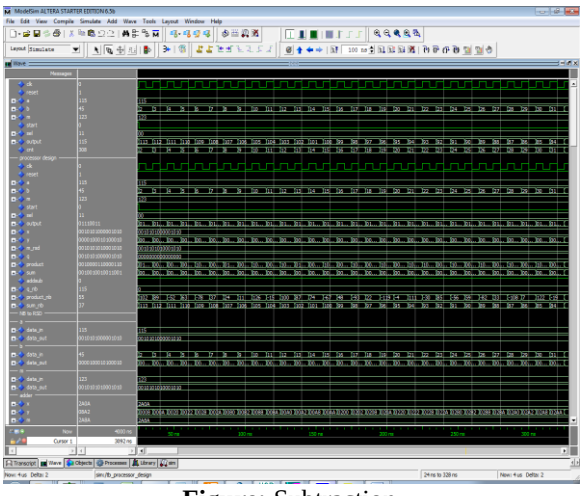

Figure: Subtraction

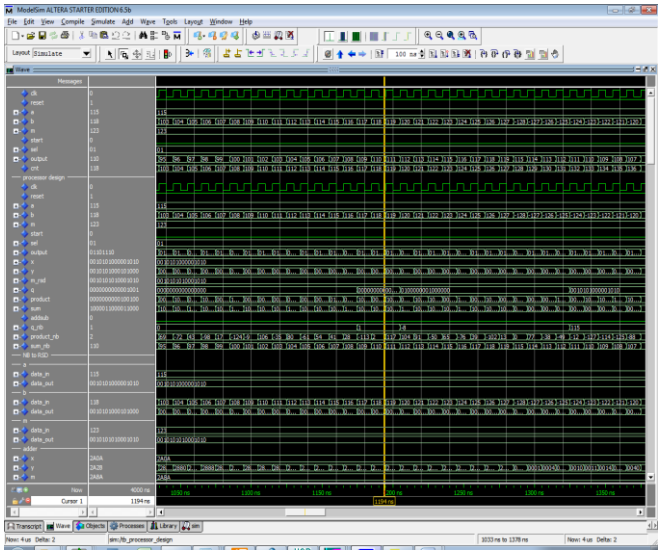

Figure: Addition

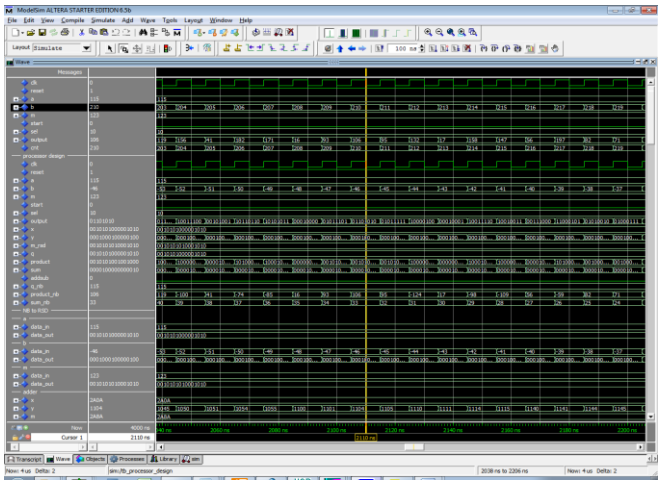

Figure: Multiplication

Power Report:

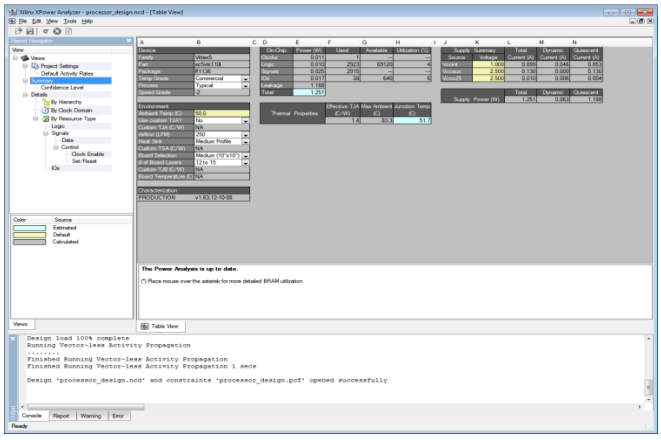

Figure: Power Report

Delay Report:

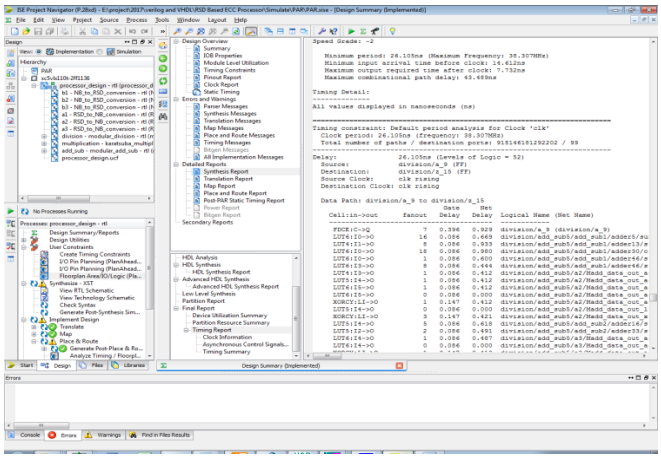

Figure: Delay Report

Synthesis Report:

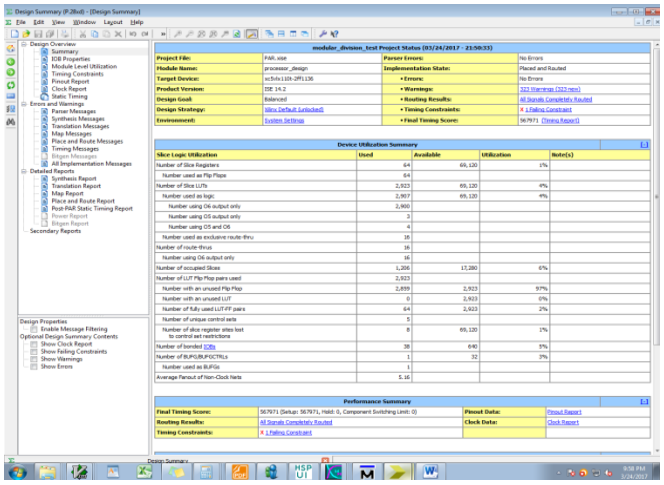

Figure: Synthesis Report

6. Conclusion

In this thesis we demonstrated that scaled arithmetic, which is based on the idea of transforming a class of primes into special forms that enable efficient arithmetic, can be profitably used in elliptic curve cryptography.

Implementation results show that the use of scaled moduli in elliptic curve cryptography offers a superior performance in terms of area, power, and speed. We proposed a novel inversion algorithm for scaled moduli that result in an efficient hardware implementation. It has been observed that the inversion algorithm eliminates the need for projective coordinates that require prohibitively a large amount of extra storage. The successful use of redundant representation (i.e. carry-save notation) in all arithmetic operations including the inversion with the introduction of an innovative comparator design leads to a significant reduction in critical path delay resulting in a very high operating clock frequency.

The fact that the same data path (i.e. arithmetic core) is used for all the field operations leads to a very small chip area. Comparison with another implementation demonstrated that our implementation features desirable properties for resource-constrained computing environments.

References

[1] G. B. Agnew, R. C. Mullin, and S. A. Vanstone. An Implementation of Elliptic Curve Cryptosystems over F2155 .IEEE Journal on Selected Areas in Communications, 11(5):804{813, June 1993.
[2] Avizienis. Signed-digit number representations for fast parallel arithmetic. IRE Trans. Electron. Computers, EC(10):389{400, September 1961.
[3] E. Berlekamp. Algebraic Coding Theory. McGraw-Hill, New York, NY, 1968.
[4] D. Boneh and M. Franklin. Identity-based Encryption from the Weil Pairing. In Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213{229. Springer-Verlag, 2001.
[5] G. Bertoni, J. Guajardo, S. Kumar, G. Orlando, C. Paar, and T. Wollinger. Efficient GF(pm) Arithmetic Architectures for Crypto-C.E. graphic Applications. In Topics in Cryptology - CT RSA 2003, volume 2612 of Lecture Notes in Computer Science, pages 158{175. Springer-Verlag, 2003.
[6] R. E. Crandall. Method and Apparatus for Public Key Exchange in a Cryptographic System. U.S. Patent Number 5,159,632, October 1992.
[7] W. Diffe and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22:644{654, November 1976.
[8] B. S. Kaliski Jr. The Montgomery Inverse and its Applications. IEiEE Transactions on Computers, 44(8):1064{1065, 1995.
[9] N. Koblitz. Elliptic Curve Cryptosystems. Mathematics of Computation, 48(177):203{209, January 1987

Author Profile

M. Rajeswari Completed B.Tech in Srikalahasteeswara Institute of Technology, Srikalahasti. Pursuing M.Tech in Srikalahasteeswara Institute of Technology, Srikalahasti.

M. Vijaya Laxmi, Associate Professor, Electronics and Communication Engineering, Srikalahastheeswara institute of technology, Srikalahasti.