Reduction of Power in Confined Field Multiplier Using Sorting Technique

DR. DOLA SANJAY S
PhD, M.Tech,
Principal and Professor,
Ramachandra College of engineering,
Eluru, A.P, India.

PETLA KANTHA RATNAM
M.Tech scholar,
Department of ECE ,
Ramachandra College of engineering,
Eluru, A.P, India.

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–Ofman method to achieve high throughput multiplication. Furthermore, an efficient modular adder without comparison and a high throughput 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 implemented by using Xilinx 14.7 version.

I INTRODUCTION

According to Moore's law, the number of transistors on a chip doubles almost every two years. As a result, more functions and more complicated designs can be implemented on one chip, which leads to more power density and more heat on the circuits. Higher power density on the circuit reduces the reliability of the system and the battery life of the battery-based devices. Thus, power and energy consumptions of the circuit gain the same or probably more importance than area, especially for most compact portable devices that work by battery.

Nowadays, lots of information are exchanged through networks, thus providing security services over networks is crucial for protecting information. Among security technologies, public key cryptography is popular and important, since it can provide certain unique security services, such as key exchange and digital signature. There are two public key cryptography techniques, in practice, namely, Rivest–Shamir– Adleman (RSA) and elliptic curve (EC) cryptosystem.

Binary extension field, denoted by GF(2m), is very attractive for hardware implementation, because it offers carry free arithmetic. Multiplication operation has been paid most attention by researchers, because addition is simply bitwise XOR operation between two field elements, and the more complex operations, inversion, can be carried out with a few multiplications. In GF(2m), there are various methods to represent field elements, such as polynomial basis (PB), normal basis, and dual basis. PB is probably the most popularly used basis, because it is adopted as one of the basis choices by organizations that set standards for cryptography applications [1], [2]. Thus, a large number of architectures for efficient implementation of PB finite field multipliers have been proposed. In addition, new representations based on PB called shifted PB (SPB) [3] and generalized PB [4] have been proposed for efficient implementation of multipliers over GF(2m).

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 geometrical properties, points are added or 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 , or dual field operations.

II. BACKGROUND

A. Elliptic Curve Cryptography Elliptic curves over a field K are defined by the reduced Weierstrass equation in (1) when the characteristic of the field is two or three. The set of solutions along with a point at infinity O defines the algebraic structure as a group with point addition as the basic operation

$$E : y^2 = x^3 + ax + b.$$

The smoothness of the curve and distinct roots are guaranteed by 4a3 + 27b2 =! 0. Points on the curve are defined by their affine coordinates (x, y). Point coordinates are of type integers for an elliptic curve defined by (1) and are the elements of an underlying finite field with operations performed modulo a prime number. Such elliptic curves are known as prime field elliptic curves. For prime field elliptic curves defined by (1), the coordinates of the point addition result is calculated as follows, assuming P = (x1, y1), Q = (x2, y2), and R = P + Q =*(x*3*, y*3*)*:

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

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \qquad (3)$$

Whereas the point doubling operation is calculated as follows:

$$x_3 = \left(\frac{3x_1{}^2 + a}{2y_1}\right)^2 - 2x_1 \qquad (4)$$

$$y_3 = \left(\frac{3x_1{}^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \qquad (5)$$

B. 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.

III. PROPOSED SYSTEM

Overall processor architecture

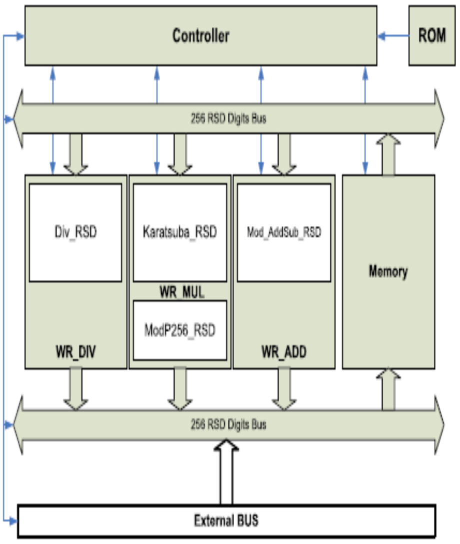


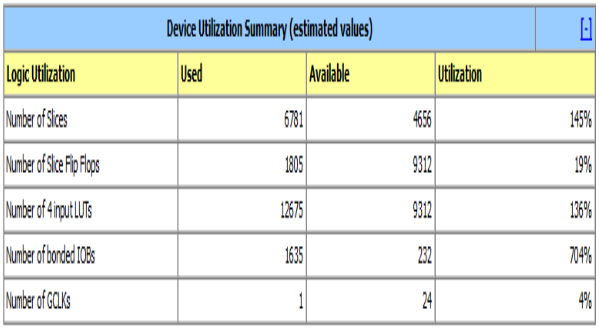
Fig. 1. Overall processor architecture.

The proposed P256 ECC processor consists of an AU of 256 RSD digits wide, an finite-state machine (FSM), memory, and two data buses. The processor can be configured in the pre synthesis phase to support the P192 or P224 NIST recommended prime curves [36]. Fig. 1 shows the overall processor architecture. Two sub control units are attached to the main control unit as add-on blocks.

These two sub control units work as FSMs for point addition and point doubling, respectively. Different coordinate systems are easily supported by adding corresponding subcontrol blocks that operate according to the formulas of the coordinate system. 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.

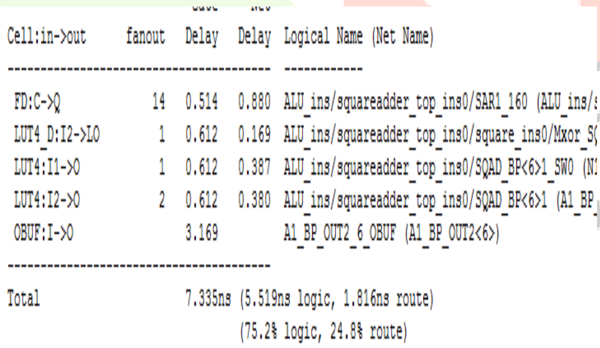
IV RESULTS

Area report:



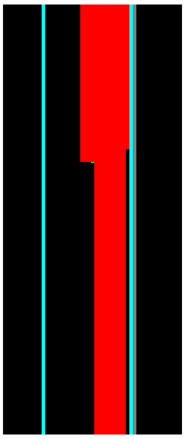
Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	6781	4656	145%
Number of Slice Flip Flops	1805	9312	19%
Number of 4 input LUTs	12675	9312	136%
Number of bonded IOBs	1635	232	704%
Number of GCLKs	1	24	4%

Timing report:

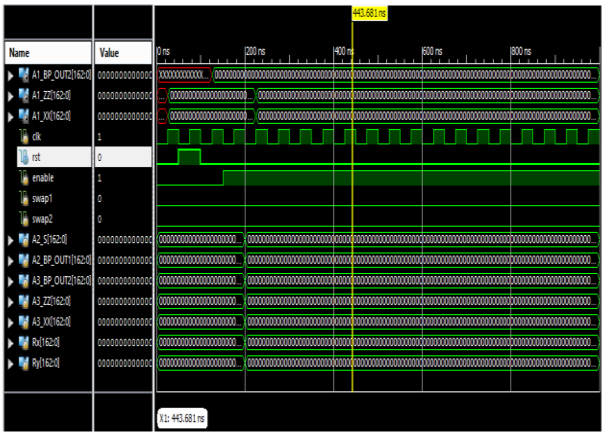


```
                           Gate     Net
Cell:in->out      fanout   Delay    Delay  Logical Name (Net Name)
----------------------------------------   ------------
 FD:C->Q              14   0.514    0.880  ALU_ins/squareadder_top_ins0/SAR1_160 (ALU_ins/s
 LUT4_D:I2->LO         1   0.612    0.169  ALU_ins/squareadder_top_ins0/square_ins0/Mxor_S(
 LUT4:I1->O            1   0.612    0.387  ALU_ins/squareadder_top_ins0/SQAD_BP<6>1_SW0 (N1
 LUT4:I2->O            2   0.612    0.380  ALU_ins/squareadder_top_ins0/SQAD_BP<6>1 (A1_BP_
 OBUF:I->O                 3.169           A1_BP_OUT2_6_OBUF (A1_BP_OUT2<6>)
----------------------------------------
Total                      7.335ns (5.519ns logic, 1.816ns route)
                                   (75.2% logic, 24.8% route)
```

Rtl schematic:



Simulation results:



Name	Value
A1_BP_OUT2[162:0]	0000000000000
A1_ZZ[162:0]	0000000000000
A1_XX[162:0]	0000000000000
clk	1
rst	0
enable	1
swap1	0
swap2	0
A2_S[162:0]	0000000000000
A2_BP_OUT1[162:0]	0000000000000
A3_BP_OUT2[162:0]	0000000000000
A3_ZZ[162:0]	0000000000000
A3_XX[162:0]	0000000000000
Rx[162:0]	0000000000000
Ry[162:0]	0000000000000

V 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 data paths 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.

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.