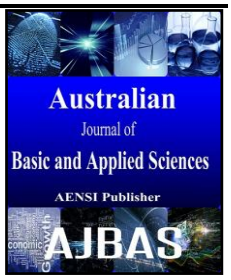
Australian Journal of Basic and Applied Sciences, 9(16) Special 2015, Pages: 457-461

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



FPGA Based design of Elliptic Curve Cryptography OVER Binary Field using Hybrid and Booth Multipliers

[1]M. Ashkar Mohammed and [2]S Suresh Babu

[1]*Research scholar, Noorul Islam Centre for Higher Education, Tamilnadu*
[2]*Principal, Sree Budha College of Engineering, Kerala India*

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:

ABSTRACT

This paper presents a FPGA Based Elliptic Curve Cryptography (ECC) design over binary field, using hybrid and booth multipliers based on the Montgomery scalar multiplication algorithm to perform Point Addition and Point Doubling.ECC provide the secure communication among portable device with small key length. Scalar multiplication is the key operation on the ECC, scalar multiplication on the ECC is Time, Power and Area expensive. The proposed ECC architecture over binary field is designed with three different multipliers namely Array, Hybrid low power encoded multipliers and modified booth multipliers. These multipliers are used in the word-serial finite field arithmetic unit (AU) is proposed with the optimized operation scheduling and bit-parallel modular reduction. The comparison with other ECC designs justifies the effectiveness of the proposed FPGA design in terms of performance and area- time efficiency. The architecture is implemented using Spartan3E family device XC3S1600E using Modelsim5.7 and Xilinx 9.2i.

To Cite This Article: M. Ashkar Mohammed and S Suresh Babu, FPGA Based design of Elliptic Curve Cryptography OVER Binary Field using Hybrid and Booth Multipliers. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 457-461, 2015*

INTRODUCTION

The Elliptic Curve Cryptography (ECC) has been regarded mature to provide robustness for secure data transaction. Compared with RSA, ECC can supply equivalent level of security with a much smaller key length. Therefore, ECC has become an attractive alternative cryptosystem and many designs have been proposed in recent years (N. Koblitz, 1987). ECC was proposed by Koblitz and Miller in 1985 and predominant usage in portable device such as smart cards, mobile phones, personal digital assistant(PDA) and high bandwidth digital content protection(HDCP) etc.ECC contains many standards such as IEEE 1263(IEEE 1363, 2000) and NIST (NIST, 1999) for elliptic curve digital signature algorithm. The various numbers of multipliers used to perform the scalar multiplication over the both binary and prime field. The combined the arithmetic and shifter units with booth multiplier has been proposed (V. S. Miller, 1986;C. Shu *et al*, 2005). In hybrid multiplier operation is performed depends upon the number of 1's and its position in the multiplier data. The comparison of different modular multipliers such as serial multiplier, Booth multiplier suitable for use in an elliptic curve processor, has been proposed optimized of improved Barrett modular multipliers for public key cryptography. The C-testable technique for detecting transition faults with 100% fault coverage in the polynomial basis(PB) bit parallel(BP) multiplier circuits over GF(2m).In a low energy modulo multiplier has been proposed for elliptic curve cryptography processor, especially for authentication in mobile device or key encryption in embedded health care system. In this proposed work an efficient ECC processor over GF (2160) is designed based on the Montgomery scalar multiplication and to perform the addition and doubling operations using array multiplier, modified booth multiplier and hybrid multiplier. Performance analysis of all three multipliers is given in this work. Array multiplier is having same number of shifting and addition operations. For perform four bit multiplication, array multiplier provide four partial products. Modified booth multipliers requires less number of adders than the shifting operations. For perform four bit multiplication, hybrid multiplier provide only one partial products. The comparison shows that our approach achieves a very high performance with significant area-time efficiency.

Proposed New Eliptical Curve Cryptography Processor:

The proposed new ECC processor architecture

Corresponding Author: M. Ashkar Mohammed, Research scholar, Noorul Islam Centre for Higher Education, Tamilnadu India
E-mail: ashkarmohammed@yahoo.co.in

for key generation using different multipliers is shown in fig1. This architecture is mainly used to generating the key for encryption with less power consumption. Point identifier, clock control, montgo multiplication, Point addition, point doubling and multipliers modules are used in this architecture. The point P(x,y) is selected on Elliptic curve over GF(2160) is done on Point identifier module. Montgo multiplication module generates the key for encryption and performs the coordinate conversion. Clock control unit used to issue the clock signal to all the modules. Montgo multiplication module uses the both point addition and point doubling module for mathematical operations in key generation. In multiplier module three types of multipliers are used, namely array, modified booth and hybrid multiplier. Among three multipliers, hybrid low power encoded multiplier is consumed low power while generating the key in ECC architecture.

Point Addition:

In point addition module is one of the most important arithmetic operations in montgo multiplication algorithm for key generation (C. Shu *et al*, 2005). Input and Output for point addition module is (X1,Z1),(X2,Z2),x and (X3,Z3) respectively. Multiplier plays an important role in point addition module. In this module hybrid multiplier is used to perform the multiplication operation for reducing the power consumption.

Point Doubling:

In montgo multiplication algorithm, another frequently used arithmetic operation is point doubling(Satoh *et al*, 2003.). Fig 3 implies the way of execution in point doubling. Input and Output for point doubling module is (X1,Z1),b and (X2,Z2) respectively. In point doubling module also multiplier plays a frequent role in arithmetic operations. In this module hybrid multiplier is used to perform the multiplication operation for reducing the power consumption.

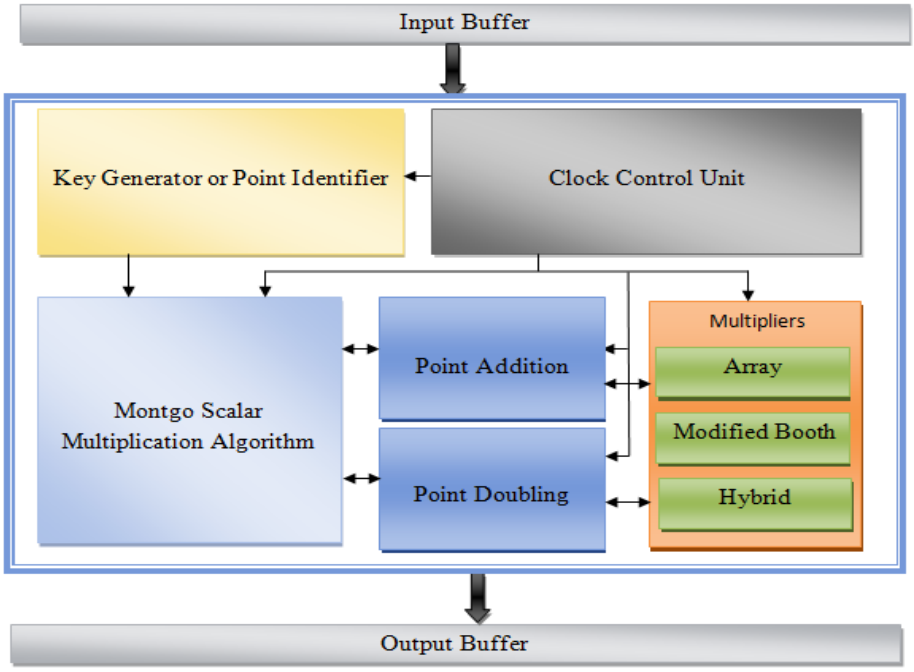


Fig. 1: Proposed ECC Architecture with various multipliers.

Multipliers:

In the proposed architecture array, modified booth and hybrid multipliers are used.

Modified Booth Multiplier:

In digital design one of the commonly used multiplier is Modified booth multiplier (N. Gura *et al*, 2002). It multiplies two binary numbers in two's complement representation. Modified booth multiplication algorithm can handle the signed bit numbers. The two important operations of Modified booth multiplication are shifting and addition. In Modified booth multiplication more shifting operation is used Compare to addition. Shifting operation requires less power and faster operation compare to adder. Modified booth's algorithm involves repeatedly adding one of two predetermined values A and S to a product P, then performing a rightward arithmetic shift on P. Table 1 describe the functionality of Modified Booth Multiplier.

Hybrid Multiplier:

Multiplication plays very important role in digital design and other applications. The important

requirements of digital design are implementation of multiplier should be effective one. The hybrid multiplier encoded low power multiplier is designed using Spurious Switching Suppression Technique (SSST). Number of bits in the input data plays vital role in the proposed hybrid low power encoded multiplier. The dynamic power and switching activity of multiplication is mainly depending upon the input pattern in the given input. Hybrid low power encoded multiplier works based on the number of 1's and its position in the input data. The switching activity of hybrid low power encoded multiplier has been reduced to 46% compared to modified booth multiplier. Due to the reduction of switching activity, power of the hybrid low power multiplier is reduced comfortably compare to modified booth multiplier. The results of the comparison are obtained using Xilinx synthesis tool. The details flow of hybrid low power encoded multiplier is shown in the Fig. 6.

According to the conventional shift and add multiplication, the number of partial products (PP) are equal to the number of bits in the multiplier. The number of partial products can be reduced by half using Booth recoding. In the proposed encoding technique, the partial products can still be reduced which in turn reduces the switching activity and power consumption. The operation can be defined according to the number of 1's and its position in the multiplier. If the number of 1's in the multiplier is less than or equal to 3, the control goes to proposed multiplication technique, otherwise the control split the multiplier in to two parts. Again the number of 1's in the part of the multiplier is verified. If the number of 1's is more than three, the control goes to Booth multiplication. Otherwise the control goes to proposed multiplication technique. If the number of 1's in the multiplier is one and depends upon its position/. The control goes to execute the operation in category A or B. If the number of 1's in the multiplier is two and depends upon its position, the control goes to execute the operation in category C or D. Otherwise the number of 1's in the multiplier is three and depends upon its position, the control goes to execute the operation in category E or F. The operation of hybrid encoding rule is shown in Table 2.According to category E, the proposed encoding rule needs one partial product P1 with two additions. The remaining partial products P2 to P8 are zero, so the addition operation in this area can be neglected, which reduces the switching activity and power consumption. This spurious switching activity can be reduced by freezing the adders which perform this unwanted addition.

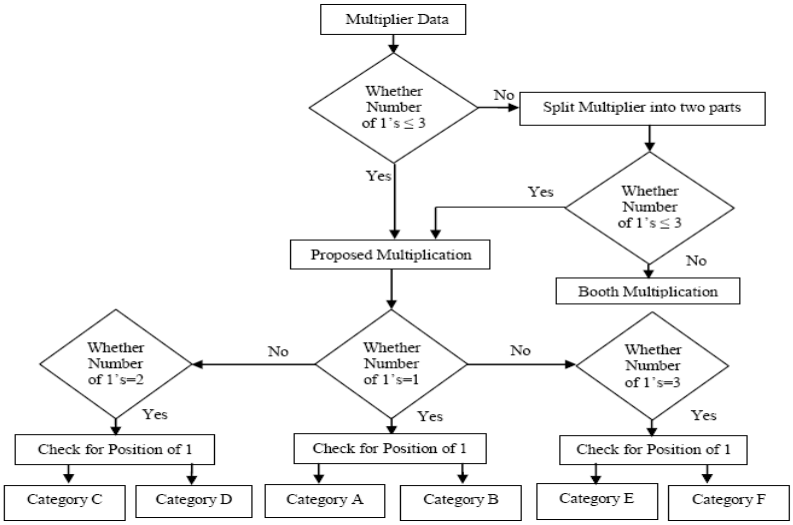


Fig. 2: Flow of Hybrid Multiplier

Table 1: Functionality of Hybrid multiplier.

Numberof1's inthe Multiplier	Positionof the1	Category	Operation
1	1^{st}bit	A	Add0 to multiplicand(M)
1	i^{th}bit	B	ShiftMleft byi-1andadd0
2	1^{st}andi^{th}bit	C	ShiftMleft byi-1andaddM
2	$1^{st}$and i+j^{th}bit	D	ShiftMleft by j,add Mandshifttheresultleft byi-1
3	i^{th}=1^{st},j^{th}andk^{th}bit	E	ShiftMbyk-j, addMandshift theresultleft byj-1,addM.
3	i^{th},$j^{th}$and k^{th} bit	F	ShiftM byk-j,addMandshift theresultleftby j-1,addMand shifttheresult by i.

Power consumption for this ECC processor including the encryption operation is 511mW and 575mW for modified booth and array multiplier respectively.

RESULTS AND DISCUSSIONS

In proposed architecture with various multipliers, less power consumption and less are autilization is achieved by using hybrid low power encoded multiplier to perform point addition and doubling. The ECC processor performs the160 bit binary field, scalar multiplication, coordinates Conversion and encryption operations, with same level of frequency 100MHz, at power consumption of 373mW and are autilizations8743LUT'sinhybrid multiplier, at power consumption of 511mWand areautilizations16260LUT'sin modified booth multiplier and at power consumption of575mW andareautilizations19176LUT's in array multiplier. A160bitbinaryfieldoperationover GF(2^m) written in VHDL language, synthesized in Xilinx 9.2i,spartan3Efamily XC3S1600E device and stimulated in modelsim 5.7.Dynamicpoweris defined as amount of power consumed by switching activities of FF, where as static power is power consumed by leakage current.

Fig.3 shows ECC architecture power summary of modified booth and array multiplier. With Frequency 100MHz, the power

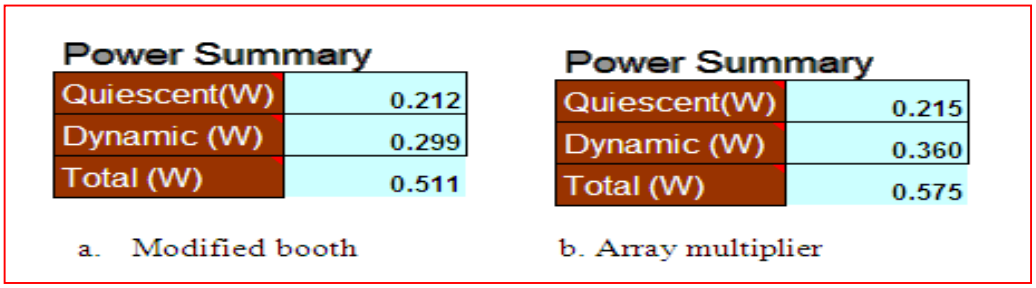


Fig. 3: Power summary of ECC architecture using Modified booth and Array multiplier.

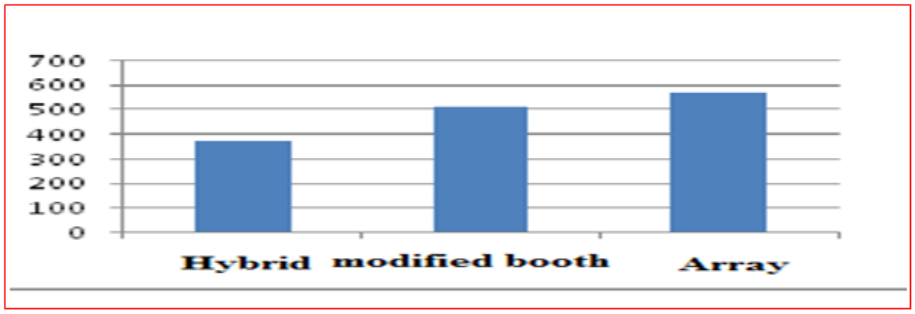


Fig. 4: Power consumption of various multipliers (Y-axis-milliwatts)

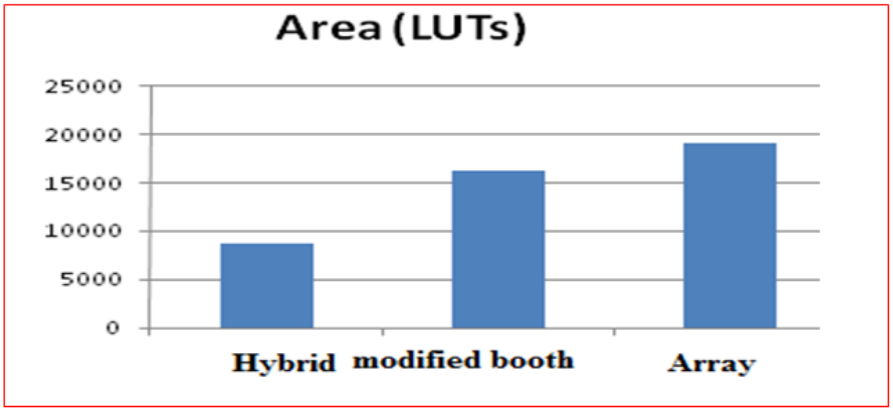


Fig. 5: Area Utilization of various multipliers (Y-axis-Number of look uptables)

Fig.4 and Fig.5 shows the power consumption and area utilization of various architecture with different multipliers. In order to obtain high security ,the encryption operation received new key from Montgomery module for each plain text values, which will avoid the Brute– Force attack.

Conclusion:

This paper has presented a FPGA based high-performance ECC architecture with the operation scheduling for the Montgomery scalar multiplication algorithm and bit-parallel modular reduction. The comparison indicates that our approach outperforms other ECC designs significantly both in terms of performance and cost-effectiveness. The proposed Elliptic Curve Cryptography processor with 160 bit point multiplication and coordinates Conversion can be done in 575mW, 511mW and 373mW with frequency 100 MHz and 19176,16260 and 8743 LUTs in array multiplier, modified booth multiplier and hybrid multiplier respectively. The architecture is implemented using spartan3E family device XC3S1600E using Modelsim 5.7 and Xilinx 9.2i.

REFERENCES

Gura, N., S.C. Shantz, H. Eberle, S. Gupta, V. Gupta, D. Finchelstein, E. Goupy and D. Stebila, 2002. "An End-to-End Systems Approach to Elliptic Curve Cryptography," CHES 2002,Lecture Notes in Computer Science, 2523: 349-365.

http://csrc.nist.gov/encryption

IEEE, 1363. Standard Specifications forPublickey Cryptography, 2000.

Koblitz, N., 1987. "Elliptic Curve Cryptosystems," Mathematics of Computation, 48: 203–209.

Miller, V.S., 1986. "Use of elliptic curves in cryptography," in CRYPT0, 85: 417-426.

NIST, 1999. Recommended elliptic curves for federal government use.

Satoh and K. Takano, 2003. "A Scalable Dual-Field Elliptic Curve Cryptographic Processor," IEEE Trans. Computers, 52(4): 449-460.

Shu, C., K. Gaj and T. El-Ghazawi, 2005. "Low Latency Elliptic Curve Cryptography Accelerators for NIST Curves over Binary Fields," FPT, pp: 309-310.