International Journal of Research Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

# HIGH-SPEED NOVEL ARCHITECTURE OF CRYPTOGRAPHY USING FINITE FIELD MULTIPLIER

[1]B. SPANDANA, [2]K.RAJKAMAL, M.Tech [Ph.d]
[1]M.tech-Scholar, Dept of ECE, Guntur Engineering College, Guntur, A.P, India.
[2]Associate Professor, Dept of ECE, Guntur Engineering College, Guntur, A.P, India.

**ABSTRACT:** We proposed an efficient pipelined architecture of elliptic curve scalar multiplication (ECSM) over GF($2^m$) in this paper. The architecture utilizes a multiplier accumulator (MAC) of bit-parallel finite field (FF) which depends on the algorithm of Karatsuba–Ofman. The algorithm of Montgomery ladder is improved for better allocating of execution paths. The data path is well designed in the architecture, hence that the critical path includes some extra logic primitive separated from the FF MAC. The optimal number of pipeline stages are founded by scheduling schemes with various pipeline stages are proposed and thoroughly analyzed the ideal placement of pipeline registers .

**Index Terms:** field-programmable gate array (FPGA), pipelining, Elliptic curve cryptography (ECC), Karatsuba–Ofman multiplier (KOM), scalar multiplication.

## I. INTRODUCTION

The number of transistors for every two years on a chip almost doubles which is according to Moore's Law. For more heat on the circuits and more power density, designs which are complicated can be developed on the chip. In security technologies public Key cryptography is popular and most significant one. It can provide certain unique security Services, such as key exchange and digital Signature. As mentioned above public's key Cryptography is used for the purpose of Security, they are two types (1) RSA (2) Elliptic curve.

EC cryptosystem utilizes shorter key when compared with RSA for producing the same level of Security. EC utilized in an EC crypto system is defined over finite field's Design of finite field arithmetic which is low-power and produces results in an EC cryptosystem. It consumes less power and for wireless application it is more suitable.

For implementing in hardware binary Extension field is denoted by GF and it very attractive due to it offers carry free arithmetic. There are different methods for representing field Elements in GF like polynomial basis (PB) normal basis, and dual basis. The most popularly utilized basis is PB due to the reason i.e., it is adopted as one of the basis choices by organizations that set standards for applications of cryptography. We propose a generalized PB or efficient implementation of multipliers over GF. The complexity of a finite field multiplier is affected by irreducible polynomial P(x) choice.

Polynomials are irreducible having non-zero terms which are less in number. Irreducible polynomials can produce multipliers with capacity which is lower. The architectures of PB finite field multiplier can be classified into digit serial and bit – serial, bit parallel

architectures. Bit serial architecture is area efficient, and it is too slow for many applications. Bit –parallel is fast and expensive in term of area. The architecture of digit serial is flexible, it has reasonable cost of implementation and moderate speed. Digit serial PB multipliers with two low-energy have been proposed. Binary tree structure of XOR gates are utilized rather than a linear array of XOR gates far degree reduction, which reduces both delay and power consumption. Various digit serial multipliers were proposed Such as most significant digit, least Significant digit with modifications in architecture. A factoring technique is involved in a digit serial PB multiplier design in GF.

## II. EXISTED SYSTEM

A finite Field is described as set of finite elements where there are operations of addition and multiplication. A binary extension field GF ($2^m$) is generated by a degree m irreducible polynomial,

P(x) = x m +pm-1 x m -1 + ------p2 x2 +p1x+1.
P1 is either O or 1.

Dynamic power consumption in CMOS based design consists of a large number of standard cells and nets. It can be expressed as

p dynamic = p switching + p internal

Pswitching is defined as the total switching power which is considered by souring all nets [a net is defined as a connecting to the inputs of cells as outputs]. Switching power is the power which is dissipated because of the charging and discharging of the output load capacitance of a cell. P internal is the total internal power obtained by summing over all cells. The internal power of each cell is the power consumed within the cell because of the charging and discharging of internal nodes capacitances of a cell and short circuit nearest dynamic power (P dynamic) can be reduced by lowering P switching or p internal. The effective method to reduce power consumption is factoring applicable for both architecture and gate level.

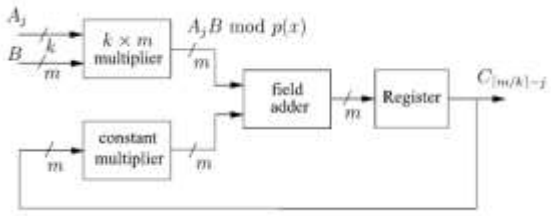


**Fig. 1 Finite Field Multiplier**

Architecture for PB multiplier in GF is exhibit in above fig 1. Three Modules are considered those are field adder, and k x m multiplier. K x m Multiplier contains two Operands B of m-bit is one operand and A j of k-bit is another operand. A j is changes for various clock cycles j. Therefore it has higher switching activity when compared with operand B.

Constant multiplier module perceives that multiplication among the constant $x^k$ field adder and field element modules which implements the addition of finite field by utilizing in m two –input XOR gates which are established as a one layer network.

Among these three k x m multiplier is the most complex module. We proposed cryptography in communications for security applications by utilizing this multiplier.

## III. PROPOSED SYSTEM

The post processing stage of ECSM also requires careful consideration. While this stage is not the crucial part of ECSM, its optimization goal is to share the data path with the main loop as much as possible, rather than to reduce the required number of clock cycles. After ECSM proper scheduling, the higher performance architecture is proposed which depends on the algorithm of Montgomery ladder scalar multiplication. The proposed ECSM architecture contains register bank, one bit-parallel finite field (FF) multiplier accumulator (MAC), a 6 × 18 control ROM, single FF squarer, and a finite-state machine. By utilizing the Karatsuba–Ofman algorithm, we are implementing the FF MAC and are pipelined. The pipelined FF MAC of n-stage considers 'n' clock cycles for finishing the single multiplication.

The squarer of FF is not pipelined, and requires one clock cycle for finishing one square. The inputs for FF MAC are *A*, *B*, and *C* and the input to FF squarer is *S*, are all registered. Another four registersT1, T2, T3, and T4 are used in the data path for data caching. Each register has a MUX before it. The MUXs control signals are given at each clock cycle to switch among various operations in ECSM. The inputs are given to MUXs of registers which are carefully considered with the guideline that every MUX consists of atleast four branches. In this way, the input delay for registers is only the delay of a 4:1 MUX. The control signals are different at every clock cycle for each iteration of the main loop and the post processing stage.

A heavy state machine is required to provide all the control signals in sequence. Here, we utilize a 6 × 18 control ROM to load the control signals for swapping selection (2 bits) and the MUXs (16 bits). A small state machine is utilized for conditional branching and jumping, and is producing the 6-bit address to the control ROM. For the FPGA implementation, the control ROM can be realized by utilizing Block RAMs in Xilinx devices or embedded memory blocks in Altera devices. Hence, in FPGA, it does not consume logic resources.

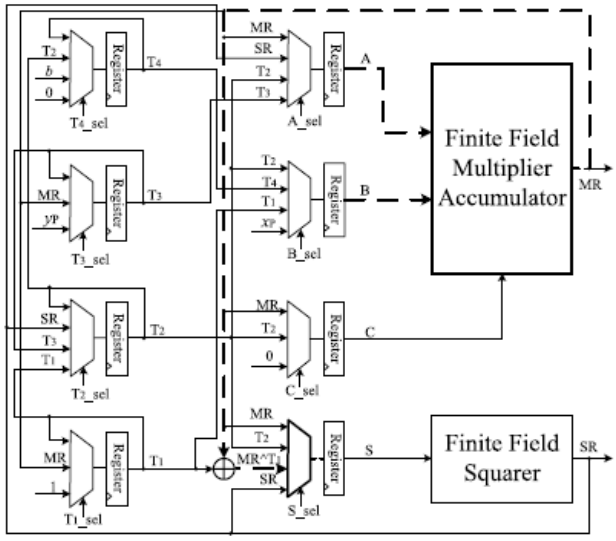


**Fig 2. Data Path Of ECSM Using a Three-Stage Pipelined FF MAC.**

The data path of ECSM is utilizing a three-stage pipelined FF MAC which is provided

as an example in Fig. 2. The terms such as X1, X2, Z1, and Z2 are the results which are intermediate of the FF Squarer or FF MAC so they are not presented. The bold dashed line in above Fig. 2 shows the pipelined architecture of three-stage critical path and contains an addition (XOR), a 4:1 MUX and pipelined FF MAC. Data paths with other pipeline stages are similar to Fig. 2 except for different data connections. Control signals stored in the control ROM are also different. But, the delay of critical path is unchanged.

## IV. RESULTS

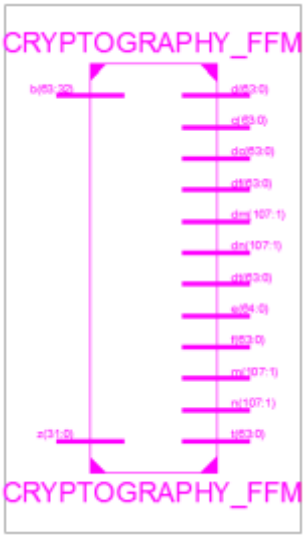


**Fig 3. RTL Schematic**

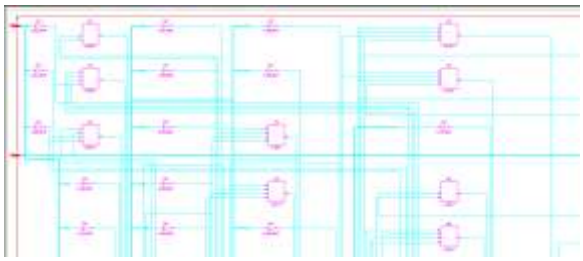

**Fig 4. Technology Schematic**

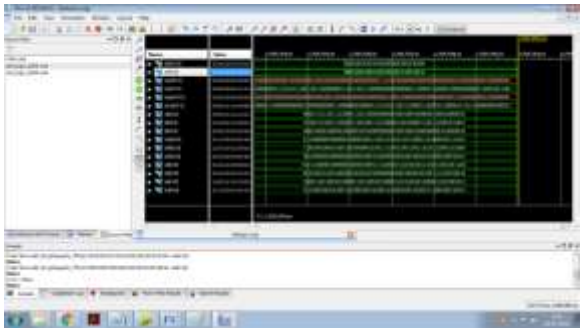

**Fig 5. Output Waveform**

## V.CONCLUSION

This paper focuses on speeding up ECSM over GF(2*m*) on FPGA with the premise of high area utilization efficiency. The proposed architecture mainly contains a non-pipelined FF squarer and a pipelined bit-parallel FF MAC. The reduction of area is done by utilizing the Karatsuba–Ofman algorithm. Compact scheduling schemes are presented for reducing the required number of clock cycles for ECSM. The data path in the architecture is carefully designed to achieve a short critical path. Pipeline techniques are applied to improve the working frequency. Thorough analyzes, supported with detailed experimental results, are produced to find the architecture with the optimal number of pipeline stages. Compared with other existing designs, the proposed architecture outperforms their results in terms of both speed and area.

## VI. REFERENCES

[1] F. Rodríguez-Henríquez, N. A. Saqib, A. D. Pérez, and Ç. K. Koç, *Cryptographic Algorithms on Reconfigurable Hardware*. New York, NY, USA: Springer-Verlag, 2006.

[2] E. Wenger and M. Hutter, "Exploring the design space of prime field vs. binary field

ECC-hardware implementations," in *Proc. 16th NordicConf. Secure IT Syst. Inf. Security Technol. Appl. (NordSec)*, Tallinn, Estonia, Oct. 2011, pp. 256–271.

[3] P. H. W. Leong and I. K. H. Leung, "A microcoded elliptic curve processor using FPGA technology," *IEEE Trans. Very Large ScaleIntegr. (VLSI) Syst.*, vol. 10, no. 5, pp. 550–559, Oct. 2002.

[4] N. Gura *et al.*, "An end-to-end systems approach to elliptic curve cryptography," in *Proc. 4th Int. Workshop CHES*, London, U.K., 2003, pp. 349–365.

[5] A. Satoh and K. Takano, "A scalable dual-field elliptic curve cryptographicprocessor," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 449–460, Apr. 2003.

[6] R. C. C. Cheung, N. J. Telle, W. Luk, and P. Y. K. Cheung, "Customizable elliptic curve cryptosystems," *IEEE Trans. Very LargeScale Integr. (VLSI) Syst.*, vol. 13, no. 9, pp. 1048–1059, Sep. 2005.

[7] K. Sakiyama, L. Batina, B. Preneel, and I. Verbauwhede, "Superscalar coprocessor for high-speed curve-based cryptography," in *Proc. 8th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, 2006, pp. 415–429.

[8] D. Schinianakis, A. Kakarountas, T. Stouraitis, and A. Skavantzos, "Elliptic curve point multiplication in GF(2*n*) using polynomial residue arithmetic," in *Proc. 16th IEEE Int. Conf. Electron., Circuits,Syst. (ICECS)*, Dec. 2009, pp. 980–983.

[1]B.SPANDANA Completed B.tech at GEC in 2016 and At present pursuing M.Tech at Guntur engineering college. Her area of interest is VLSI.

[2]K. RAJKAMAL working as Associate professor at Guntur engineering college. He completed his B.Tech at LITAM College and M.Tech at KL University. He is pursuing Ph.D at KL University.