Grenze International Journal of Engineering and Technology, Jan Issue

Elliptical Curve Scalar Multiplication over Pipelined Architecture - GF(2m)

Siva Santosh Kumar Daroga[1] and Dr. D. Kalyani[2]
[1]VNR Vignana Jyothi Institute of Engineering and Technology
Email: dssk18@gmail.com
[2]VNR Vignana Jyothi Institute of Engineering and Technology, IT (CNIS)
Email: kalyani_d@vnrvjiet.in

***Abstract*—An attempt to propose a novel scheme for multiplications through finite field inclusive of Elliptic Curve computations. A serial finite field multiplier i.e.., consider the word length w, for the scalar multiplication is subjected to Implementation, performing a scalar computation in clock cycles with corresponding gate delays within the critical path. The designing and operation characteristics of this mechanism is explained thoroughly.**
Elliptic curve scalar multiplication operations commonly correspond to finite field (FF) executions i.e., addition, multiplication, subtraction, and inversion. By breaking down the addition and doubling operations into FF operations we obtain the parallel and pipelined scalar multiplication resulting in finite field subtraction, squaring, addition, inversion, and multiplication operations, respectively. The proposed scheme refers to one such mechanism of elliptical curve scalar multiplications over finite field.

***Index Terms*— Finite field Operations, ECSM, Scalar Multiplications, Elliptical Curve.**

I. INTRODUCTION

Generally Elliptic curve scalar multiplication is performed by repetition purpose addition and purpose doubling operations over the curve that rely upon finite field (FF) operations i.e., addition/subtraction, multiplication, and inversion. By breaking down the addition and doubling operations into FF operations we obtain the parallel and pipelined scalar multiplication resulting in sequence of FF addition, subtraction, squaring, multiplication, and inversion operations.
Appropriate clustering of the operations un-veil the scope for optimization and this is considered as a significant operation in ECC. The scheme of pipelining is based on key observation. the execution of one operation will not interrupt the other. The processor computes elliptic curve scalar multiplications based on serial bit systolic architecture multiplying single processing element upon division of the binary field. The field elements are represented in standard form. FF operations execution can be done in single clock cycle whereas, for binary fields sphere is proportional resulting in complex squaring which is less than multiplication. Hence, there is a need to deploy a distinct approach for optimization.

II. LITERATURE SURVEY

Numerous demonstrations have been made earlier using K-ary and Signed window method for ECSM over finite

Grenze ID: 01.GIJET.7.1.14

field operations. Commonly optimizations are found with premium memory which cannot be considered as significant. Let us un-veil performance of ECC over binary fields implementing through FPGA operations.
Hardware architecture for implementing ECSM through double fields which predicts Montgomery ladder method involving polynomial origins for finite field (FF) operations. Karatsuba multiplier execution enhances the runtime of multiplication utilizing considerably less hardware units, in context with other operations are running parallelly with FF multiplication operations.
The reformed circuits end in low area requirement contradicting other high-end implementations. National Institute of Standards and Technology (NIST) recommends 163-degree curve, whereas projected style will reach 121 megacycles with ten,417 slices enforced on Xilinx
Implementations of elliptic and hyper-elliptic curve cryptography uses Digit serial multipliers Digit serial multipliers extensively with different architectural enhancements. In LSD - Least significant figure multiplier for binary fields i.e.., GF(2m). double accumulator number and N-accumulator number, that area unit quicker compared to ancient LSD's evaluation of various digit sized multipliers provides optimum selections and shows that presently used digit sizes.

III. PROPOSED METHOD

Employing a two-level pipelined finite field MAC, every occurrence of the primary thread in ECSM takes 6 cycles. The switching (step 5) in 2nd algorithm executed simultaneously selecting input variables among numerical range, which doesn't result in additional clock cycles.
Outcomes of point addition operations are resulting as independent of the price of Ki. Swapping X1 with X2 and Z1 with Z2 providing identical outcomes, i.e., the terms X1Z2 + X2Z1 and X1Z2X2Z1 stay constant. Hence, analyzing point summing (new X1 and new Z1) doesn't correspond to selection based on swapping which isn't the same in the context of point doubling. Evaluating the terms X2 2 & Z2 2, they must align either X2 or X1 □ Z2 or Z1 for constituting FF squarer. Refer the 3-level pipeline in Table 1.
Upon choosing, additional terms, like X4 2 and Z4 2, & X2 2 · Z2 2, selection based on swapping is not considered as we may use the results computed.

TABLE I: PROPOSED SCHEME EMPLOYING 3 -LEVEL PIPELINE

clk	FF MAC $(A \cdot B + C)$	FF SQR (S^2)
1	$X_2 \cdot Z_1$	Z_2^2 (swap*)
2	$X_1 \cdot Z_2$	X_2^2 (swap*)
3	$Z_2 \leftarrow X_2^2 \cdot Z_2^2$	Z_2^4
4	$X_2 \leftarrow b \cdot Z_2^4 + X_2^4$	X_2^4
5	$X_1 Z_2 \cdot X_2 Z_1$	$Z_1 \leftarrow (X_1 Z_2 + X_2 Z_1)^2$
6	$X_1 \leftarrow x_P \cdot Z_1 + X_1 Z_2 X_2 Z_1$	
7	idle	

* if swap = 1, perform Z_1^2 instead of Z_2^2 and X_1^2 instead of X_2^2.

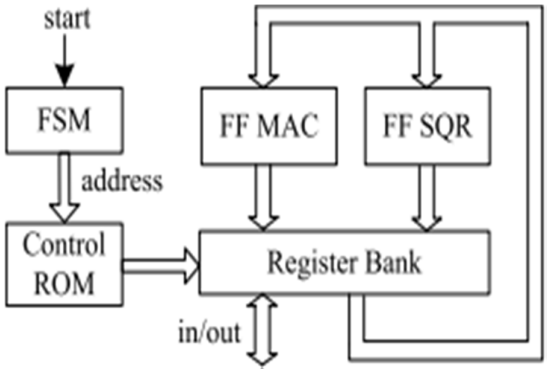


Fig. 1. Depiction of ECSM architecture proposed

Hence, computing recent X1 (point addition nodes) is considered as crucial path, which shall constitute very best call for scheduling. X1 · Z2 i.e.., multiplication is put behind the multiplication X2 · Z1 because the worth of the new X1 is on the market finally. In the same manner, the square X2 2 followed by Z2 2. The extent of recent Z2, Z1, X2, and X1 resulting at 5,6,7 and 8th cycles, respectively. The 7th and 8th cycles correspond to primary and secondary cycles for the following Occurrences.
Therefore, scheme proposed in Table I results in working of FF MAC with no un-necessary cycle during the most ECSM cycles, all the more indicating greater efficiency Similarly, employing a 3- level FF MAC pipeline, each repetition of the loop occurs at seven clock cycles, refer Table II and Fig. 1.
The number of pipeline stages are proportional to, required clock cycles for a scalar multiplication, whereas enhancing frequency features limit, due to introduction of an additional setup, pause duration to the delay of path and stop optimization in combinational logics duration by inserted registers. 2nd,3rd, and 4th-stage pipelined ESCM architecture using on Xilinx Spartan 3E FPGAs are being implemented which achieves far

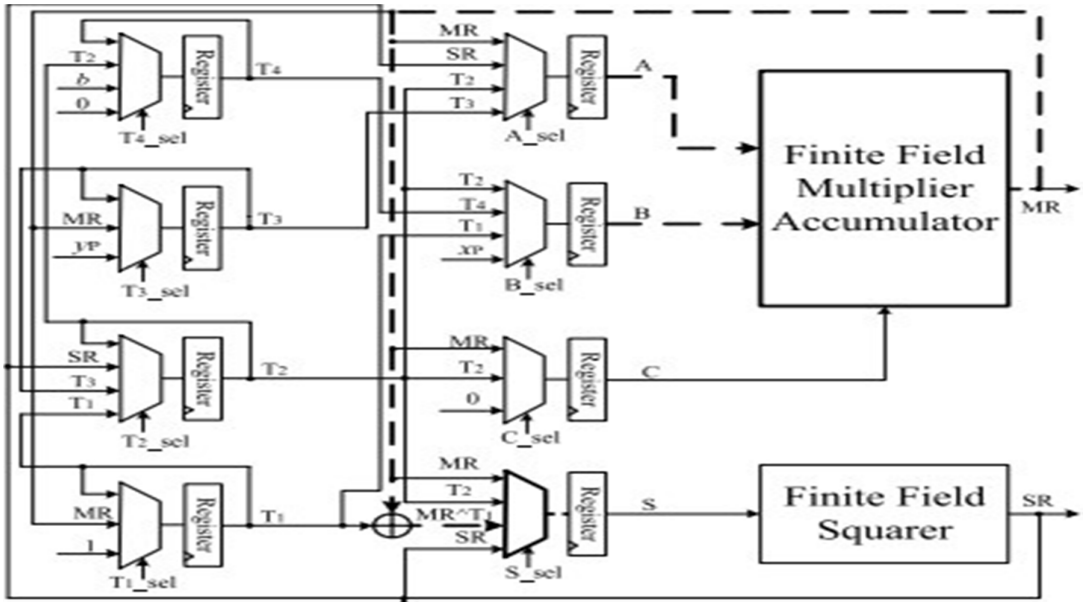


Fig. 2. ECSM implemented in three-level pipelined FF MA

better optimized performance. The stage upon executing all the operations is also to be considered though it is not the critical aspect of ESCM main objective is to transfer the data through primary grouping at the best instead of comprising with generalized number of clock cycles. Upon scheduling the architecture exhibits better execution enhancing Montgomery ladder algorithm, as shown in Fig. 1.

We deploy 6 × 18 control ROM which stores the pulse further multiplexing and replacing selection units Employing a three-stage pipelined FF MAC is given for instance in Fig. 2. Multipliers with threshold τ with LUT delay = logk 2τ. The levels assigning r steps with k ≥ 4 delay for each step of LUT. In GF(2163), the scheme using the 3-level KOM where k = 6 results in an approximate of 10 LUTs, therefore employing 4-level KOM with k □ 2s:1 multiplexing, s elements, generates an output □ 2s:1 where multiplexing is a attribute of 2s s elements. DMUX = logk (2s s) will be the delay for input of 2s elements.

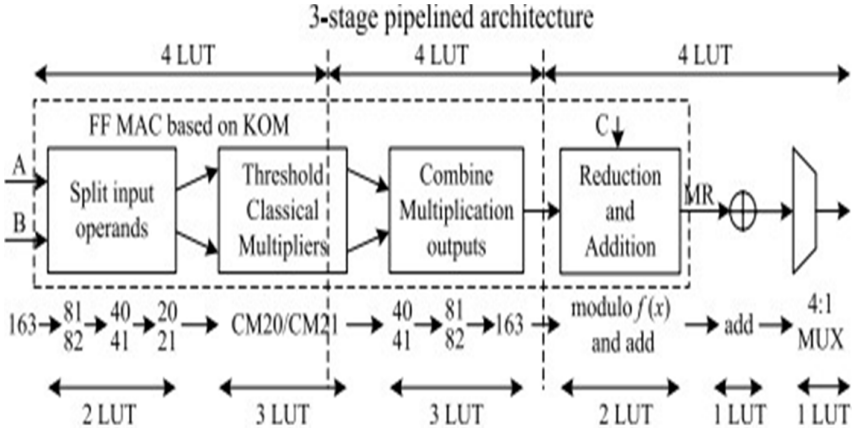


Fig. 3. Computations in the pipelined scheme

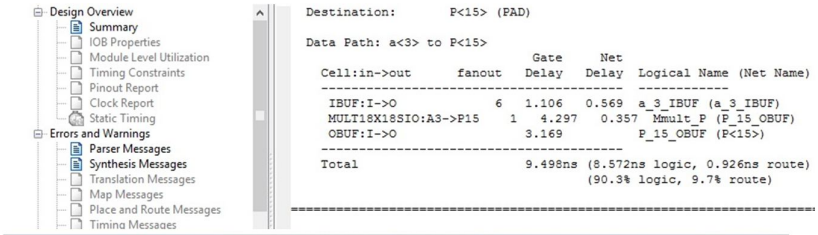
Therefore 4:1 multiplexing results in 1 LUT for k = 6 and two LUTs for k = 4 of delay. Registers are subjected to combinational logic to attain the pipeline. To reduce the delay, we need to split the primary execution. Consider k □8, with 16 LUTs over the primary path over GF (2163) of ECSM. In a two-leveled pipeline, splitting the ratio 8:8, depicting registers subjected to a combination = KOM40/KOM41. In a 3-leveled scheme, the ratio is effectively split over 4:4:4. Where CM20/CM21 includes the registers with initial cycle upon

subjecting to combination of KOM163 in the consecutive cycle, and 3:3:3:3 comes out to be the preferred split ratio in a 4-leveled scheme depicted under Fig 3.

The optimization of frequency in a 3-levelled scheme cannot be expected in context with elevated levels of executions. We can quote that a 3-levelled scheme has basic optimization. Therefore, in ECSM analysis of the delay in FPGAs (considering 4 staged architecture or more) or on other binary fields is performed in series of pipelined scheme.

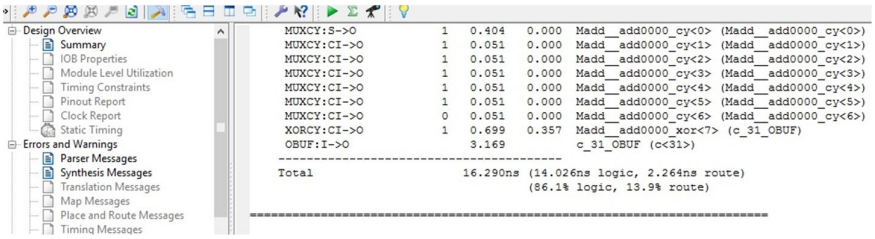
IV. RESULTS

Existing Methodology



Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	26	4656	0%
Number of 4 input LUTs	46	9312	0%
Number of bonded IOBs	33	232	14%
Number of MULT18X18SIOs	1	20	5%

Proposed Architecture Results



Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	21	4656	0%
Number of 4 input LUTs	39	9312	0%
Number of bonded IOBs	64	232	27%
Number of MULT18X18SIOs	4	20	20%

V. Conclusion

Scalar multiplication performance is optimized to in 25(m − 1) clock cycles. Considerably this results to be 2.75 times optimized when compared to traditional implementation using a pseudo pipe-lined serial w multiplier (word length - w) supporting the existing Montgomery scalar multiplication algorithm. The multiplier executes loading/unloading of information adding to the field multiplication in ⌈m/w⌉ clock cycles. TAND log2 wTXOR is the gate delay within the path of multiplier.

References

[1] F. Rodríguez-Henriquez, 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 Nordic Conf. 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 Scale Integr. (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 cryptographic processor," 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 Large Scale Integr. (VLSI) Syst., vol. 13, no. 9, pp. 1048–1059, Sep. 2005.

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

[8] B. Ansari and M. A. Hasan, "High-performance architecture of elliptic curve scalar multiplication," IEEE Trans. Comput., vol. 57, no. 11, pp. 1443–1453, Nov. 2008.

[9] C. Rebeiro, S. S. Roy, and D. Mukhopadhyay, "Pushing the limits of high-speed GF (2m) elliptic curve scalar multiplication on FPGAs," in Proc. 14th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES), 2012, pp. 494–511.

[10] D Siva Santosh Kumar, Dasari Kalyani, " Secure Encryption scheme with key exchange for Two server Architecture ". IJERCSE, Volume 4, Issue 11, November 2017.

[11] Kalyani D., Sridevi R. "Private Communication Based on Hierarchical Identity-Based Cryptography". Emerging Technologies in Data Mining and Information Security. vol 755. Springer, Singapore.

[12] D. Kalyani, R. Sridevi, "Survey on Identity-based and Hierarchical Identity-based Encryption Schemes". International Journal of Computer Applications, Volume 134 – No.14, January 2016.