IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 8, August 2016

Galois Field Systolic Montgomery Multiplier with Less-Complexity and High Throughput

Pavan Kumar R B[1], **Shashi Kumar R**[2]

M.Tech in LDE, EWIT, Bengaluru, Karnataka[1]

Professor, ECE Dept., EWIT, Bengaluru, Karnataka[2]

Abstract: Cryptographic calculation exploits limited field arithmetic and, specifically, multiplication. Lightweight and quick usage of such arithmetic is fundamental for some delicate applications. This brief proposed a low-complexity systolic Montgomery multiplication over GF (2^m). Our many-sided quality examination demonstrates that the area complexity in quality of the proposed design is decreased contrasted with the past work. This has likewise been affirmed through our application-specific integrated circuit area and time proportional estimations and usage. Consequently, the proposed design seems, by all accounts, to be extremely appropriate for high throughput low-complexity cryptographic applications. This Proposed configuration will be actualized by Verilog HDL and mimicked by Modelsim Tool. The Proposed Montgomery Multiplier is Synthesis by Xilinx and FPGA Spartan 3 XC 3S 200 TQ 144.

Keywords: Galois Field (GF), VLSI, Application Specific Integrated circuits(ASIC) Karatsuba-Of man (KO).

1. INTRODUCTION

Finite field Arithmetic has imperative applications in various fields, for example, Digital Signal Processing and cryptography. Especially, cutting edge cryptographic algorithms depend intensely on finite field arithmetic. A standout amongst the most critical finite field operations is multiplication by which other such operations, including reversal and exponentiation, can be actualized. Additionally, the requirement for quick algorithms to register multiplication is particularly essential on account of asymmetric cryptography, because the key length is longer than symmetric cryptography. There are various methods of the binary extension field, GF (2^m), multipliers relying on different algorithms, for example, Montgomery and Karatsuba-Ofman. Their usage can be structurally arranged, for instance, into bit-serial, bit parallel, digit-serial, linear feedback shift register relying systolic. For vast binary expansion fields, systolic array procedures can bring about high throughput and usual VLSI implementations. Most recent systolic or semi systolic architectures are proposed to use multiplication. Here we proposed a low-complexity systolic Montgomery multiplication based on trinomials that seem to have less space complexity contrasted by past work, but its throughput is very much comparable or significantly higher.

Existing System: In Existing System, digit-serial and digit-parallel systolic structures are displayed for processing multiplication over GF (2^m). Relying on novel decomposition algorithm, we came up with an proficient digit-serial systolic architecture, which includes latency of O ($\sqrt{m/d}$) clock cycles, the current digit-serial systolic multipliers include minimum rate O(m/d) latency for digit-size d. The proposed digit-serial outline can be utilized for AESP-based fields with similar digit-size like trinomial-based fields with a little increment in area. We have likewise proposed digit-parallel systolic design architecture utilizing n-term Karatsuba-like technique.

Existing System Drawbacks:
The number of gate count is high so the area is not efficient.
The latency and critical-path of the designs is very high.

Proposed System: This brief proposed a low-complexity systolic Montgomery multiplication over GF (2m). Our complexity analysis shows that the area complexity of the proposed architecture is reduced compared with the previous work. This has also been confirmed through our application-specific integrated circuit area and time equivalent estimations and implementations. Hence, the proposed architecture appears to be very well suited for high throughput low-complexity cryptographic applications. We have proposed a low-complexity systolic Montgomery multiplication using trinomials that appear to have lower space complexity compared with previous work, whereas its throughput is similar or even higher.
VLSI stands for "Very Large Scale Integrated Circuits". It's a classification of ICs. An IC of common VLSI includes about millions active devices. Typical functions of VLSI include Memories, computers, and signal processors, etc. A semiconductor process technology is a method by which working circuits can be manufactured from designed specifications. There are many such

DOI 10.17148/IJIREEICE.2016.4819

technologies, each of which creates a different environment or style of design. In integrated circuit design, the specification consists of polygons of conducting and semiconducting material that will be layered on top of each other to produce a working chip. When a chip is custom-designed for a specific use, it is called an application-specific integrated circuit (ASIC). Printed-circuit (PC) design also results in precise positions of conducting materials, as they will appear on a circuit board; in addition, PC design aggregates the bulk of the electronic activity into standard IC packages, the position and interconnection of which are essential to the final circuit. Printed circuitry may be easier to debug than integrated circuitry is, but it is slower, less compact, more expensive, and unable to take advantage of specialized silicon layout structures that make VLSI systems so attractive. The design of these electronic circuits can be achieved at many different refinement levels from the most detailed layout to the most abstract architectures. Given the complexity that is demanded at all levels, computers are increasingly used to aid this design at each step. It is no longer reasonable to use manual design techniques, in which each layer is hand etched or composed by laying tape on film. Thus the term computer-aided design or CAD is a most accurate description of this modern way and seems more broad in its scope than the recently popular term computer-aided engineering (CAE).

2. RELATED WORK

The below mentioned papers are about a approach towards Storage devices, Wireless communication
Satellite communication and broadband modems in VLSI in this proposed system, a good and better approach has been done by using less number of gates then previous works in this field.

a. Low-latency digit-serial and digit parallel systolic multipliers for large binary extension fields

For cryptographic algorithms, for example, elliptic curve digital signature algorithm (ECDSA) and pairing algorithm, the crypto-processors are needed to execute vast number of additions and multiplications over limited fields of substantial requests. To have an equal exchange off between space complexity and time complexity, a novel digit-serial and digit-parallel systolic structures are displayed for processing multiplication over GF(2^m). Relying on novel decomposition algorithm, we came up with a more productive digit-serial systolic design (architecture), which includes latency of O($\sqrt{\frac{m}{d}}$) clock cycles, where as the current digit-serial systolic multipliers include in any event O(m/d) latency for digit-size d. The proposed digit-serial outline can be utilized for AESP-based fields with the same digit-size as the instance of trinomial-based fields with a little increment in area. We have additionally proposed digit-parallel systolic architecture utilizing n-term Karatsuba-like technique, here the latency can be diminished from O($\sqrt{\frac{m}{d}}$) to O($\sqrt{\frac{m}{nd}}$). This component would be a noteworthy point of interest for using multiplication for the fields of expansive requests. From union results, it is demonstrated that the proposed architectures have altogether less time complexity, less area delay item, and higher bit throughput than the current digit-serial multipliers.

b. An improved unified scalable radix-2 Montgomery multiplier

This paper portrays an enhanced variant of the Tenca-Koc brought together versatile radix-2 Montgomery multiplier with half latency for little and moderate precision operands and half the queue memory necessity. Like the Tenca-Koc multiplier, this outline is reconfigurable to acknowledge any input exactness in either GF(p) or GF(2^m) up to the measure of the on-chip memory. A FPGA execution can execute 1024-bit modular exponentiation in 16 ms utilizing 5598 4-information lookup tables, making it the quickest brought together adaptable plan until now.

c. Area/performance trade-off analysis of an FPGA digit-serial GF(2^m) Montgomery multiplier based on LFSR

Montgomery Multiplication is a typical and vital algorithm for enhancing the effectiveness of public key cryptographic algorithms, as RSA and Elliptic Curve Cryptography (ECC). A characteristic decision for executing this tedious multiplication characterized on finite fields, predominantly over GF(2^m), is the utilization of Field Programmable Gate Arrays (FPGAs) for being reconfigurable, adaptable and physically secure gadgets. FPGAs permit the execution of this sort of algorithms in a wide scope of uses with various area–performance necessities. Here, we investigate elective designs for developing GF(2^m) digit-serial Montgomery multipliers on FPGAs in view of Linear Feedback Shift Registers (LFSRs) and study their area–performance exchange offs. Distinctive Montgomery multipliers were actualized utilizing a few digits and finite fields to look at their execution measurements, for example, region, memory, latency, clocking frequency and throughput to indicate reasonable setups for ECC usage utilizing NIST prescribed parameters. The outcomes accomplished demonstrate a remarkable change against FPGA Montgomery multiplier beforehand reported, accomplishing the most elevated throughput and the best productivity.

d. Low latency systolic montgomery multiplier for finite field GF(2^m) based on pentanomials

The paper shows a broad and cautious investigation of finite field multiplication over GF (2^m) utilizing polynomial premise and in addition exceptional polynomial like and (AOP). This multiplication is done by

DOI 10.17148/IJIREEICE.2016.4819

utilizing montgomery multiplication plan and use of it is likewise given. This paper concentrates on various arithmetical operation on elliptic curve cryptography over GF (2^m). The parameter execution is additionally talked about in term of number of component, latency, and space and time multifaceted nature.

3. PROPOSED ALGORITHM

This brief proposed a low-many-sided quality systolic Montgomery multiplication over GF (2^m). Our multifaceted nature investigation demonstrates that the area intricacy of the proposed architecture is decreased contrasted and the past work. This has additionally been affirmed through our application-specific integrated circuit area and time proportional estimations and executions. Consequently, the proposed architecture has all the earmarks of being exceptionally appropriate for high throughput low-unpredictability cryptographic applications. We have proposed a low-many-sided quality systolic Montgomery increase utilizing trinomials that seem to have lower space multifaceted nature contrasted and past work, while its throughput is comparative or significantly higher.

PROPOSED SYSTEM BLOCK DIAGRAM:

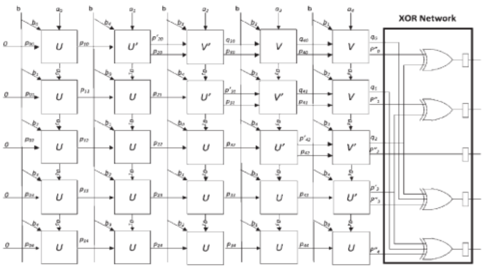
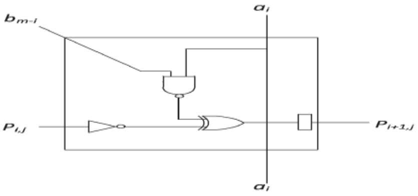


Fig 1: Systolic architecture for Montgomery multiplication in GF (25)

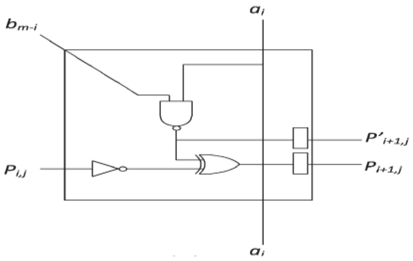
MODULES SEPERATION:

- U cell
- U' cell
- V cell
- V' cell
- XOR Networks
- Systolic architecture for Montgomery multiplication in GF(25)
- Alternative systolic architecture for Montgomery multiplication in GF(25)

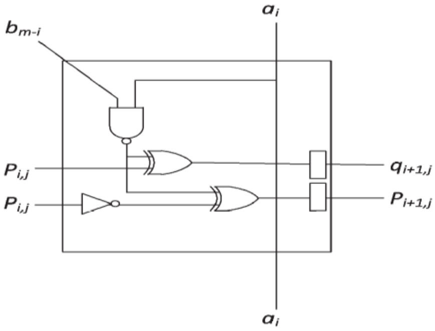
U cell:



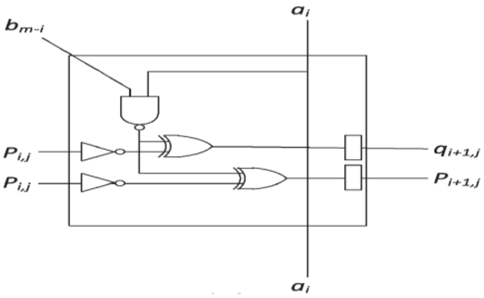
V cell:



U' cell:



V' cell:



XOR NETWORKS:
Systolic architecture for Montgomery multiplication in GF(25):
Four sorts of cells are required. It merits specifying that to diminish the critical path delay (CPD) for every cell, we abuse the method, which reverses both inputs of 2-input XOR gates. Plainly the consequences of XOR operations.

PROPOSED SYSTEM TECHNIQUE:

- Systolic Montgomery multiplication using trinomials

Four sorts of cells are required, as appeared in Fig. 1. It merits saying that to lessen the critical path delay (CPD) for every cell, we extract the method, which modifies both inputs of 2-input XOR gates . Unmistakably, the consequences of XOR operations in both cases are indistinguishable. For better delineations, we assume F(x) = $x^5 + x^3 + 1$. Fig. 2 demonstrates the systolic usage of the multiplier. As appeared in the figure, sort U is being utilized for lower triangular cells, including diagonally, sort U' is utilized as a part of the diagonally right over the U cells, sort V' is utilized as a part of the askew right over the U' cells, and sort V is being utilized for whatever remains of upper triangular cells.

PROPOSED SYSTEM ADVANTAGES:

- Lower Time complexity,
- Lower area-delay product
- Higher bit-throughput than the existing digit-serial multipliers.

REAL TIME EXAMPLE:

GF Multiplier used in RS codes. This RS codes are used in

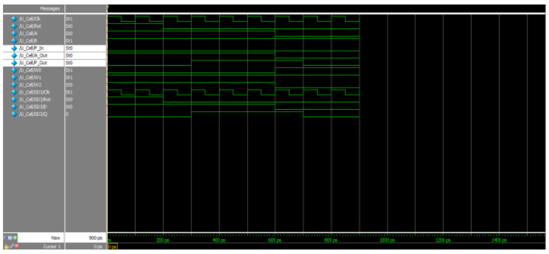
- Storage devices
- Wireless communication
- Satellite communication & broadband modems
- Encryption Decryption Circuit

4. SIMULATION RESULTS

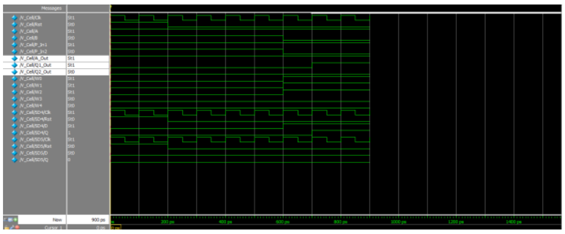
To perform the simulation, open the Wave window and specify that the simulation should run for 800 ns, as indicated. Then, click on the Run-All icon. The result of the simulation will be displayed as presented. Observe that the output f is equal to 1 whenever two or three inputs have the value 1, which verifies the correctness of our design.

The purpose of this tutorial is to provide a quick introduction to Modelsim, explaining only the rudimentary aspects of functional simulation that can be performed using the Modelsim Graphical User Interface. More details about the Modelsim GUI and its use in simulation can be found in the Generating Stimulus with Waveform Editor chapter of Modelsim SE User's Manual, which is available as part of an installed Modelsim-SE simulator. A more extensive discussion of simulation using the Modelsim simulator is provided in the tutorial Using Modelsim to Simulate Logic Circuits for Altera Devices, which is available on Altera's University Program Web site.

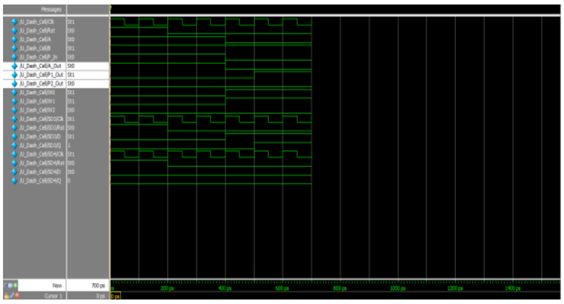
U CELL:



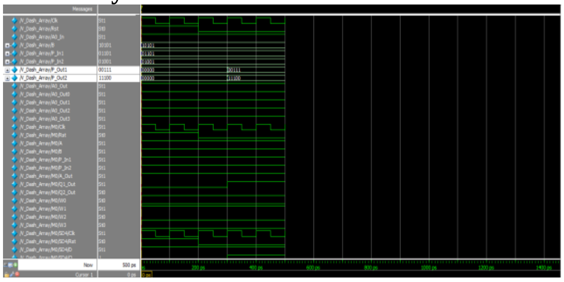
V CELL:



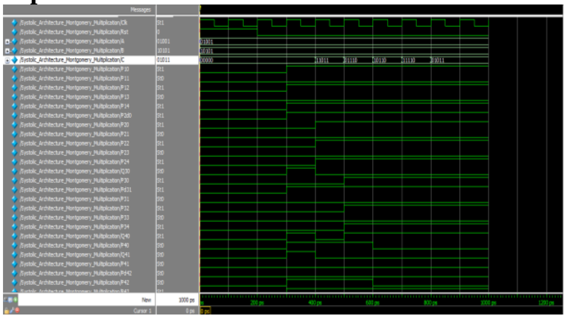
U Dash Cell:



V Dash Array:

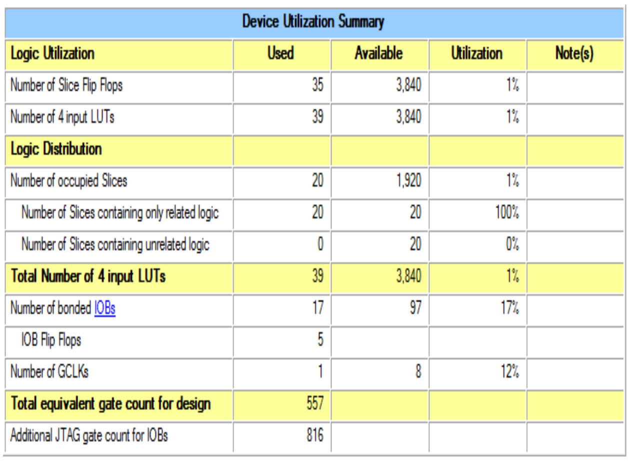


New Systolic Architecture for Montgomery Multiplication:



5. SYNTHESIS RESULTS

Synthesis is main to show the valued results of simulation process. this helps to show the exact Results after Fabrication.



Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	35	3,840	1%	
Number of 4 input LUTs	39	3,840	1%	
Logic Distribution				
Number of occupied Slices	20	1,920	1%	
Number of Slices containing only related logic	20	20	100%	
Number of Slices containing unrelated logic	0	20	0%	
Total Number of 4 input LUTs	39	3,840	1%	
Number of bonded IOBs	17	97	17%	
IOB Flip Flops	5			
Number of GCLKs	1	8	12%	
Total equivalent gate count for design	557			
Additional JTAG gate count for IOBs	816			

Fig 2: Synthesis Results of Proposed System.

DOI 10.17148/IJIREEICE.2016.4819

6. CONCLUSION

We have proposed systolic architectures for binary field Montgomery multiplications. The complexities of our work and related previous work have been presented through ASIC implementation. Our experiments have shown that the area and latency of our work are 12.83% and 4.74% lower than previous work. Based on the various requirements such as performance and area consumption, one can use the proposed multiplier for certain applications.

REFERENCES

[1] C. K. Koc and T. Acar, “Montgomery multiplication in GF(2k),” Designs, Codes Cryptography, vol. 14, no. 1, pp. 57–69, 1998.

[2] J.-S. Pan, C.-Y. Lee, and P. Meher, “Low-latency digit-serial and digitparallel systolic multipliers for large binary extension fields,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 60, no. 12, pp. 3195–3204, Dec. 2013.

[3] D. Harris, R. Krishnamurthy, M. Anders, S. Mathew, and S. Hsu, “An improved unified scalable radix-2 Montgomery multiplier,” in Proc. 17th ARITH, 2005, pp. 172–178.

[4] M. Morales-Sandoval, C. Feregrino-Uribe, P. Kitsos, and R. Cumplido, “Area/performance trade-off analysis of an FPGA digit-serial GF(2m) Montgomery multiplier based on LFSR,” Comput. Elect. Eng., vol. 39, no. 2, pp. 542–549, Feb. 2013.

[5] J. Xie, J. J. He, and P. K. Meher, “Low latency systolic Montgomery multiplier for finite field GF(2m) based on pentanomials,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 2, pp. 385–389, Feb. 2013.

[6] C. Y. Lee, J. S. Horng, and I. C. Jou, “Low-complexity bit-parallel systolic Montgomery multipliers for special classes of GF(2m),” IEEE Trans. Comput., vol. 54, no. 9, pp. 1061–1070, Sep. 2005.

[7] C. Y. Lee, C. C. Chen, and E. H. Lu, “Compact bit-parallel systolic Montgomery multiplication over GF(2m) generated by trinomials,” in Proc. IEEE TENCON, Hong Kong, Nov. 2006, pp. 1–4.

[8] C. Y. Lee, C. W. Chiou, J. M. Lin, and C. C. Chang, “Scalable and systolic Montgomery multiplier over GF(2m) generated by trinomials,” IET Circuits, Devices Syst., vol. 1, no. 6, pp. 477–484, Dec. 2007.

[9] A. F. Tenca and C. K. Koc, “A scalable architecture for modular multiplication based on Montgomery’s algorithm,” IEEE Trans. Comput., vol. 52,no. 9, pp. 1215–1221, Sep. 2003.

[10] S. Talapatra, H. Rahaman, and J. Mathew, “Low-complexity digit serial systolic Montgomery multipliers for special class of GF(2m),” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 18, no. 5, pp. 847–852, May 2010.

[11] C. Y. Lee, “Low-complexity bit-parallel systolic multiplier over GF(2m) using irreducible tinomials,” in IEE Proc. Comput. Digit. Technol., vol. 150, no. 1, pp. 39–42, Jan. 2003.

[12] C. Y. Lee, “Low-complexity parallel systolic montgomery multipliers over GF(2m) using Toeplitz matrix vector representation,” IEICE Trans. Fundam. Electron., Commun. Comput. Sci., vol. E91-A, no. 6, pp. 1470–1477, Jun. 2008.

[13] P. K. Meher, “Systolic and super-systolic multipliers for finite field GF(2m) based on irreducible trinomials,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 55, no. 4, pp. 1031–1040, 2008.

[14] NanGate Standard Cell Library. [Online]. Available: http://www.si2.org/

[15] P. Gallagher and C. Furlani, Federal information processing standards publication digital signature standard (DSS), Nat. Inst. Standards Technol., Gaithersburg, MD, USA, FIPS PUB 186-3, 2009

DOI 10.17148/IJIREEICE.2016.4819