Design of High Performance Systolic Parallel and Serial Multipliers

E.Karnakar[1] M.Srujana[2]
[1]M.Tech Student [2]Associate Professor
[1]Department of VLSI Design [2]Department of Electronics and Communication Engineering
[1,2]Pathfinder Engineering College (Pech), Thimmapur, Hanamkonda, Warangal Telangana,India

Abstract— The cryptograpy systems are mostly performed with the finite field multipliers which have high performance and low latency but such multipliers not so redundant over GF(2m) NIST pentonomials. Here we are presenting two types of high performance multipliers such as bit parallel and digit serial systolic multipliers. The proposed design mostly depends on the several parallel arrays in 2D(2-dimensional) that is BP1 with low critical path and the serial systolic multiplier sDS1 also depend on the vertical parallel arrays in the 2-dimensional series. For high performance we are designing the two different multipliers which are BP-II and DS- II. Both these multipliers are designed with several Processing elments(PE's). These proposed multipliers should contain less delay and high performance compare with the existed designs.

Key words: Digit serial, Bit parallel, NIST, GF multipliers

I. Introduction

F INITE FIELD multiplication over could be a basic field operation, that is often utilized in elliptic curve cryptography (ECC) to perform point-additions and point-doubling operations on Associatein Nursing elliptic curve. The irreducible pentanomials have been popularly accustomed generate binary extension fields to be utilized in ECC. Moreover, National Institute of Standards and Technology(NIST)has suggested 3 pentanomials for ECC implementation. many efforts have thus been created on economical realization of multiplication over based on irreducible pentanomials. Systolic styles give area time economical implementation due to modularity and regularity of their structures, wherever each processing part (PE) has identical or similar circuitstyle, and one letter of the alphabet will pass the signals to its neighboring letter of the alphabet at a high speed on a completely pipelined path Systolic realization of field multiplications over based mostly on pentanomials aren't therefore pr. A heartbeat multiplier factor based mostly on general polynomial is conferred. A semi-systolic multiplier factor is projected in and 2 heartbeat multipliers are proposed for error detection in an exceedingly recent report, Meher has conferred Associate in Nursing economical bit parallel heartbeat structure for multiplication over supported irreducible pentanomial. Alow-latency bit parallel heartbeat multiplier factor is introduced.

A completely unique low-latency Montgomery multiplier factor is recently reported. to attain area-time trade-off, digit-serial multipliers supported pentanomials area unit reported. Very recently, low-latency digit-serial heartbeat multipliers area unit projected. however, the planning strategy is appropriate just for nearly equally spaced polynomial (AESP), and can't be applied to fields supported the National Institute of Standards and Technology suggested pentanomials.

Generally, all existing heartbeat multipliers, as well as bit-parallel and digit-serial structures, involve giant latency and suffer from many alternative issues as made public within the following.

– Bitparallel heartbeat structures sometimes have giant register complexity not just for pipelining, however conjointly for providing the staggered input to the PEs to attend for the suitable accumulated partial product
– Critical-paths of digit-serial heartbeat structures sometimes increases with digit-size or field-order, that reduces throughput rate effectively. except that the typical computation time (ACT) of the digit-serial structures will increase with digit-size or field-order.

Keeping these in sight, during this paper, we tend to introduce 2 pairs of low-latency high-throughput bit-parallel and digit-serial heartbeat structures specifically for the National Institute of Standards and Technology suggested pentanomials. A novel decomposition theme is projected to decompose the multiplication into many freelance machine tasks to get a low-latency bit parallel heartbeat array structure with a critical- path , wherever is that the propagation delay of Associate in Nursing XOR circuit.

II. Proposed bit-parallel systolic multiplier-I (BP-I):

The proposed bit-parallel beat multiplier-I (BP-I) supported algorithmic program 1 is shown in Fig. 1. It consists of 1 pre computing (PRC) cell, one pipelined adder tree (PAT), and w beat arrays (each array has PEs). The PRC cell, as shown in Fig. 1(b), consists of a M-I cell and a bit-rewiring cell. It yields w outputs(B0,B1,….Bw-1) to be fed toarrays of the structure.

(ThM-I cell in PRC derives Bew-1 from B). the interior structure of PEs, i.e., PE-1, regular PEs (PE-2 to PE- and also the last PE (PE-d), ar shown in Fig. 1(c)–(e), severally. A regular PE consists of a M-II cell (M-II cell in alphabetic character-1 to PEderives B(v+1)w+u from Bvw+u for v=0,1,…d-1and u= 0,1,000w-1), AN AND cell ANd an XOR cell. throughout every cycle amount, the results of AND cell is additional along in XOR cell with another input from left and also the result's then bolted out to the proper. Meanwhile, the output of M-II cell is bolted out to consecutive alphabetic character to be utilized in consecutive cycle. Thus, critical-path of BP-I is [M-II cell has a length of in line with where, and see the propagation time of PRC cell, M-II cell, AND gate and gate, severally.

BP-I yields its initial output cycles when the operands ar fed to the structure, and the serial output are obtainable in each cycle

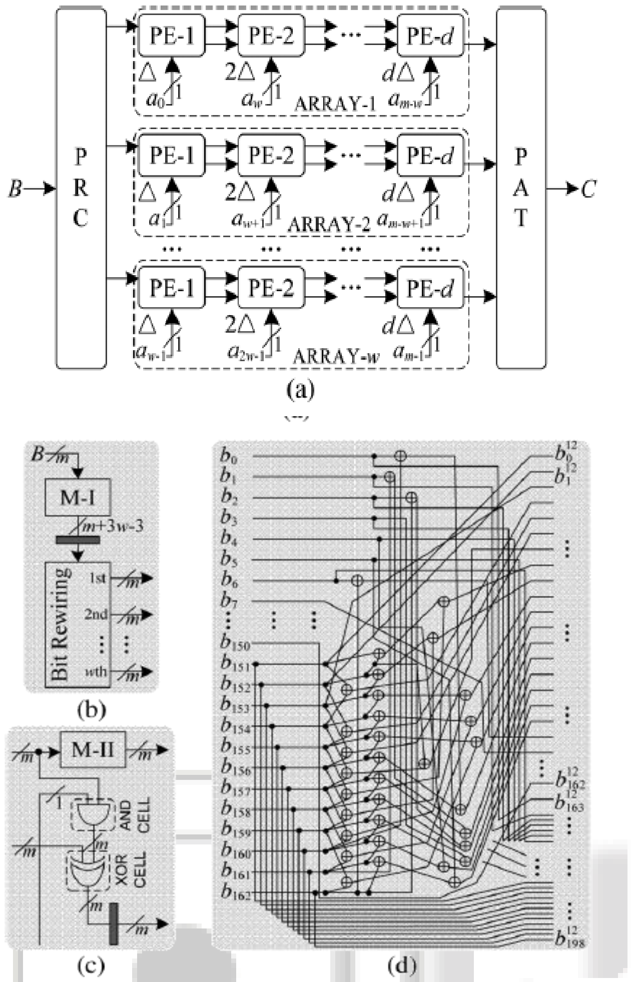


Fig. 1. Proposed bit-parallel systolic multiplier-I (BP-I) over $GF(2^m)$, where △ denotes a unit delay and each black block denotes register cell. (a) Proposed systolic structure. (b) Internal structure of PRC cell. (c) Internal structure of PE-1. (d) Internal structure of M-I cell where $m = 163$.

III. PROPOSED DIGIT-SERIAL SYSTOLIC MULTIPLIER-I (DS-I):

we will project the parallel arrays of BP-I on vertical direction to possess the planned digit-serial beat multiplier-I (DS-I) as shown in Fig. 3. DS-I consists of PEs and one accumulation (AC) cell. the interior structures of PE-0, regular alphabetic character and AC cell ar shown in Fig. 3(b)–(d), severally. As shown in Fig. 3(b), all bits of quantity ar loaded in to AN input register and also the output of that register is fed to PE-1 furthermore because the M-IV cell to perform modular operation by one degree throughout every cycle amount (to get from , for). The output bits of M-IV cell ar then bolted back in to the input register to be used by PE-0 within the next cycle amount. The regular alphabetic character, from PE-1 to PE- , contains a M-II cell, AN AND cell, AN XOR cell and a register cell (same as that in BP-I). The AC cell, as shown in Fig. 3(d), contains parallel bit-level finite field accumulators. During every cycle amount, the freshly received input is then additional with the antecedently accumulated result and also the results of addition is stored within the register cell to be used throughout consecutive cycle. DS-I has the same critical-path as that of BP-I/MBP-I, and it offers the primary output of desired product cycles when the combine of operands are fed to the structure, whereas the serial output ar created at the interval of cycles thenceforth.

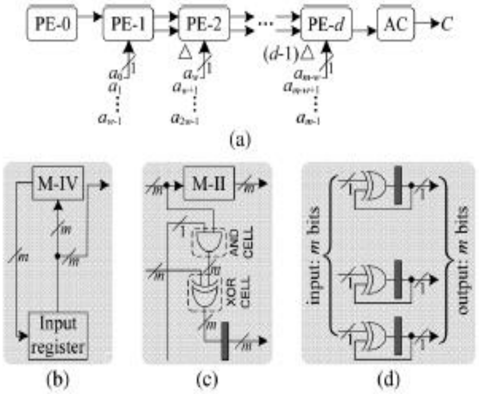
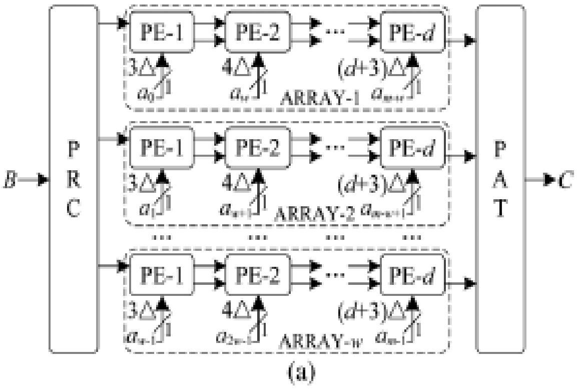


Fig. 3. Proposed digit-serial systolic multiplier-I (DS-I), where Δ denotes unit delay and each black block denotes register cell. (a) Proposed structure. (b) Internal structure of PE[0], where $0 \le u \le w - 1$. (c) Internal structure of a regular PE. (d) Internal structure of AC cell.

IV. PROPOSED BIT-PARALLEL SYSTOLIC MULTIPLIER-II (BP-II)

The proposed BP-II supported algorithmic program a pair of is shown in Fig. 4. The block level structure of BP-II multiplier factor is comparable thereto of BP-I but differs within the internal structures of PRC and alphabetic character. the interior structure of PRC is shown in Fig. 4(b), wherever it yields outputs from arrays. to keep up the critical-path of PRC as , we have conjointly used a two-stage pipelined M-I cell to understand the operation. the interior structure of normal alphabetic character is shown in Fig. 4(c). Fig. 4(d) depicts the detail style of M-V cell in PRC to derive from . M-VI is another novel standard reduction cell. it's similar structure as M-III to understand the operations given in Table IV. The propagation delay of M-V cell and M-VI cell (according to Tables II and IV) is . BP-II so has a critical-path of (M-I cell is two-stage pipelined and so critical-path of PRC is), wherever and see the propagation time of M-V cell and M-VI cell, severally. BP-II yields its initial output cycles when the operands ar fed to the structure.

while the serial output ar obtained in each cycle thenceforth. BP-II, therefore, has higher outturn rate than BP-I at the value of alittle variety of XOR gates and registers. The overhead of hardware quality, however, is minor compared to the rise in outturn rate achieved by this structure.



(a)

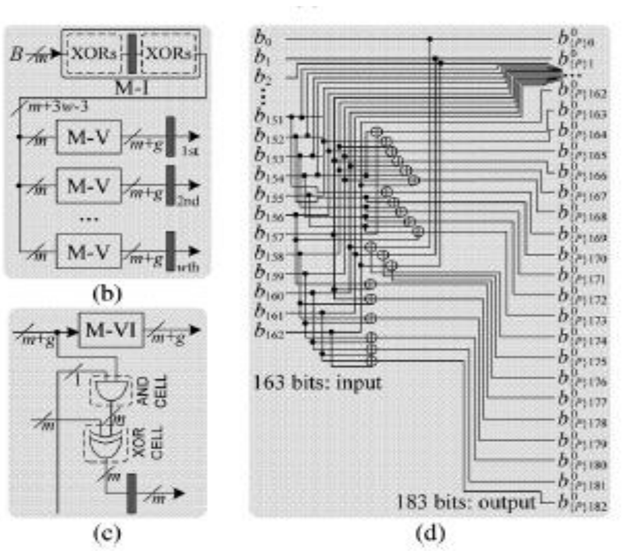


Fig. 4. Proposed BP-II, where $g = (2w - k1 + k3)$. (a) Proposed structure. (b) Internal structure of PRC, where M-I cell is designed into two-stage pipeline to reduce the critical-path to T_X. (c) Internal structure of a regular PE. (d) Detailed structure of M-V cell in PRC (derives B^0_P from B^0, $m = 163$).

V. Proposed Digit-Serial Systolic Multiplier-II (DS-II):

primarily based on planned algorithmic program a pair of, and novel standard reduction approach we have derived the DS II multiplier factor as shown in Fig. 6. It consists of PEs and one accumulation (AC) cell. the interior structures of PE-0, regular alphabetic character and AC cell ar shown in Fig. 6(b)–(d) respectively. As shown in Fig. 6(b), all bits of quantity ar fed to the M-V cell and also the output is then loaded in to bit-registers and then ar bolted out (meanwhile the output bits are fed to PE-1) to the M-VII cell to perform standard operation by one degree throughout every cycle amount.

The output bits of M-VII cell are then bolted back in to the registers to be utilized in by PE-0 in the next cycle amount. The regular alphabetic character, from PE-1 to PE- , contains a M-VI cell, AN AND cell, a XOR cell and a register cell, the same as that in BP-II. The AC cell, as shown in Fig. 6(d), contains parallel bit-level finite field accumulators.

Throughout every cycle amount, the freshly received input is then additional with the antecedently accumulated result and also the results of addition is hold on in the register cell to be used throughout consecutive cycle. DS-II has the same critical-path as that of BP-II. It offers the primary output of desired product when cycles, whereas the serial output ar produced at the interval of cycles thenceforth.

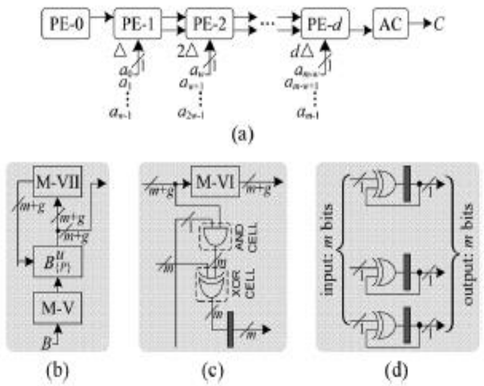
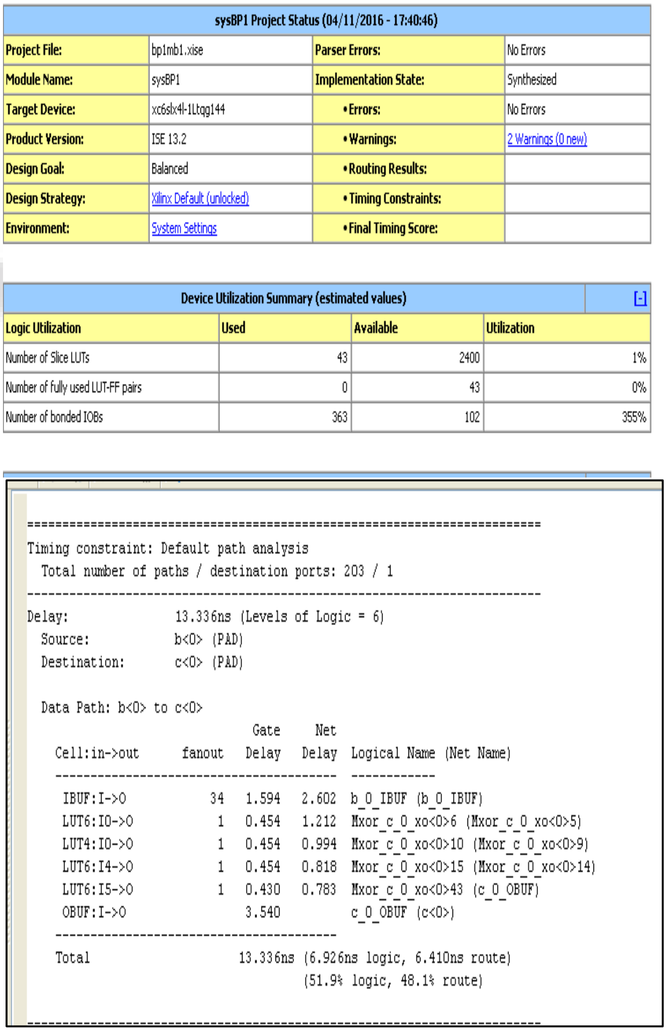


Fig. 6. Proposed digit-serial systolic multiplier-II (DS-II), where Δ denotes unit delay, each black block denotes register cell and $g = (2w - k1 + k3)$. (a) Proposed structure. (b) Internal structure of PE[0], where $0 \le u \le w - 1$. (c) Internal structure of a regular PE. (d) Internal structure of AC cell.

VI. Synthesis and Simulation Results

The proposed designs BP-I ,BP-II,DS-I and DS-II can be synthes and simulated by using the XILINX ISE14.5 software and it is imlemented with the Verilog HDL. The synthesis and simulation results are shown in the below figure.



sysBP1 Project Status (04/11/2016 - 17:40:46)			
Project File:	bp1mb1.xise	**Parser Errors:**	No Errors
Module Name:	sysBP1	**Implementation State:**	Synthesized
Target Device:	xc6slx4l-1Ltqg144	**• Errors:**	No Errors
Product Version:	ISE 13.2	**• Warnings:**	2 Warnings (0 new)
Design Goal:	Balanced	**• Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	**• Timing Constraints:**	
Environment:	System Settings	**• Final Timing Score:**	

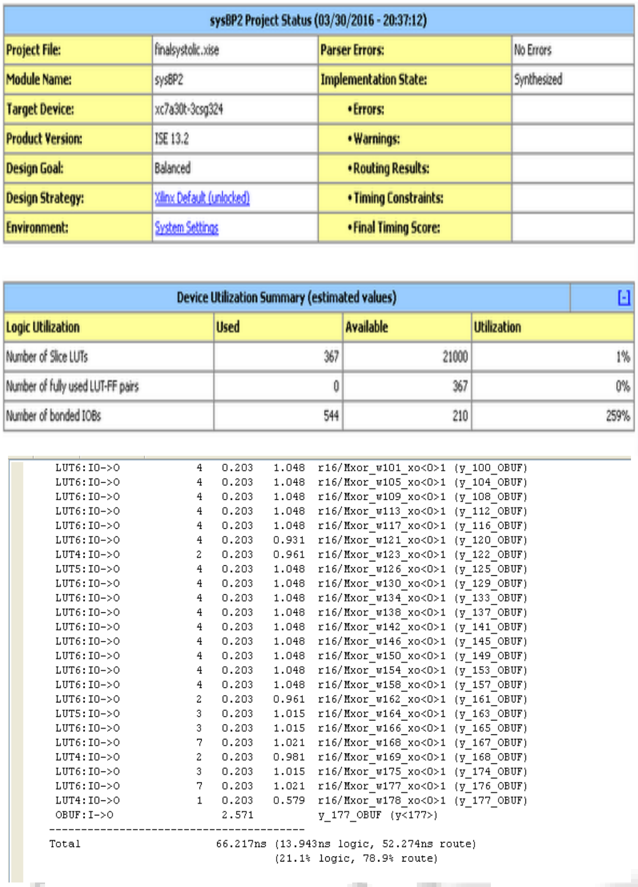
Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice LUTs	43	2400	1%
Number of fully used LUT-FF pairs	0	43	0%
Number of bonded IOBs	363	102	355%

```
=========================================================================
Timing constraint: Default path analysis
  Total number of paths / destination ports: 203 / 1
-------------------------------------------------------------------------
Delay:               13.336ns (Levels of Logic = 6)
  Source:            b<0> (PAD)
  Destination:       c<0> (PAD)

  Data Path: b<0> to c<0>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     IBUF:I->O            34   1.594   2.602  b_0_IBUF (b_0_IBUF)
     LUT6:I0->O            1   0.454   1.212  Mxor_c_0_xo<0>6 (Mxor_c_0_xo<0>5)
     LUT4:I0->O            1   0.454   0.994  Mxor_c_0_xo<0>10 (Mxor_c_0_xo<0>9)
     LUT6:I4->O            1   0.454   0.818  Mxor_c_0_xo<0>15 (Mxor_c_0_xo<0>14)
     LUT6:I5->O            1   0.430   0.783  Mxor_c_0_xo<0>43 (c_0_OBUF)
     OBUF:I->O                 3.540          c_0_OBUF (c<0>)
    ----------------------------------------
    Total                     13.336ns (6.926ns logic, 6.410ns route)
                                       (51.9% logic, 48.1% route)

-------------------------------------------------------------------------
```

Fig. 6.1: Synthesis result of BP1

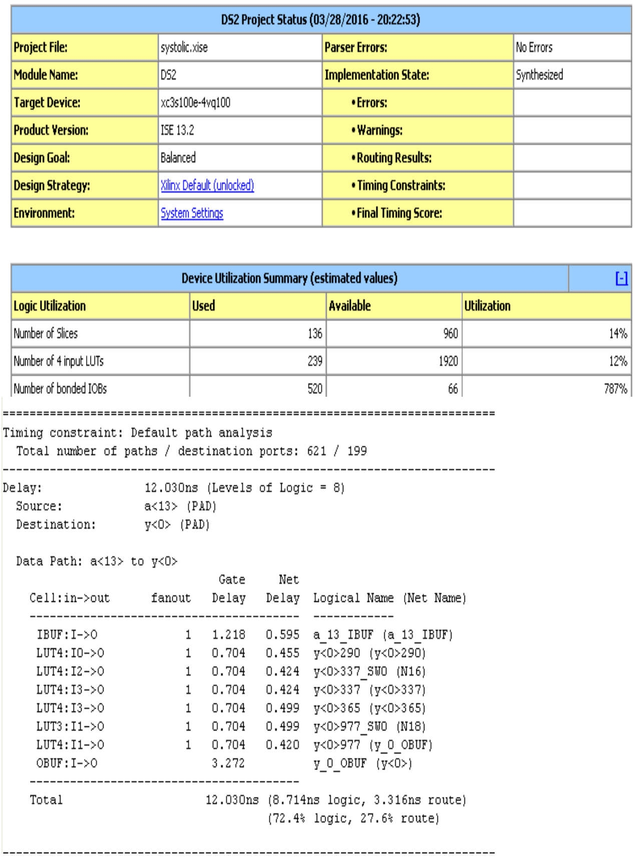


sysBP2 Project Status (03/30/2016 - 20:37:12)			
Project File:	finalsystolic.xise	Parser Errors:	No Errors
Module Name:	sysBP2	Implementation State:	Synthesized
Target Device:	xc7a30t-3csg324	• Errors:	
Product Version:	ISE 13.2	• Warnings:	
Design Goal:	Balanced	• Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	
Environment:	System Settings	• Final Timing Score:	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slice LUTs	367	21000	1%
Number of fully used LUT-FF pairs	0	367	0%
Number of bonded IOBs	544	210	259%

```
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w101_xo<0>1 (y_100_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w105_xo<0>1 (y_104_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w109_xo<0>1 (y_108_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w113_xo<0>1 (y_112_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w117_xo<0>1 (y_116_OBUF)
    LUT6:I0->O           4   0.203   0.931  r16/Mxor_w121_xo<0>1 (y_120_OBUF)
    LUT4:I0->O           2   0.203   0.961  r16/Mxor_w123_xo<0>1 (y_122_OBUF)
    LUT5:I0->O           4   0.203   1.048  r16/Mxor_w126_xo<0>1 (y_125_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w130_xo<0>1 (y_129_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w134_xo<0>1 (y_133_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w138_xo<0>1 (y_137_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w142_xo<0>1 (y_141_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w146_xo<0>1 (y_145_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w150_xo<0>1 (y_149_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w154_xo<0>1 (y_153_OBUF)
    LUT6:I0->O           4   0.203   1.048  r16/Mxor_w158_xo<0>1 (y_157_OBUF)
    LUT6:I0->O           2   0.203   0.961  r16/Mxor_w162_xo<0>1 (y_161_OBUF)
    LUT5:I0->O           3   0.203   1.015  r16/Mxor_w164_xo<0>1 (y_163_OBUF)
    LUT6:I0->O           3   0.203   1.015  r16/Mxor_w166_xo<0>1 (y_165_OBUF)
    LUT6:I0->O           7   0.203   1.021  r16/Mxor_w168_xo<0>1 (y_167_OBUF)
    LUT4:I0->O           2   0.203   0.981  r16/Mxor_w169_xo<0>1 (y_168_OBUF)
    LUT6:I0->O           3   0.203   1.015  r16/Mxor_w175_xo<0>1 (y_174_OBUF)
    LUT6:I0->O           7   0.203   1.021  r16/Mxor_w177_xo<0>1 (y_176_OBUF)
    LUT4:I0->O           1   0.203   0.579  r16/Mxor_w178_xo<0>1 (y_177_OBUF)
    OBUF:I->O                2.571          y_177_OBUF (y<177>)
   ----------------------------------------
   Total                    66.217ns (13.943ns logic, 52.274ns route)
                                     (21.1% logic, 78.9% route)
```

Fig. 6.2: Synthesis result of BP 2



DS2 Project Status (03/28/2016 - 20:22:53)			
Project File:	systolic.xise	Parser Errors:	No Errors
Module Name:	DS2	Implementation State:	Synthesized
Target Device:	xc3s100e-4vq100	• Errors:	
Product Version:	ISE 13.2	• Warnings:	
Design Goal:	Balanced	• Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	
Environment:	System Settings	• Final Timing Score:	

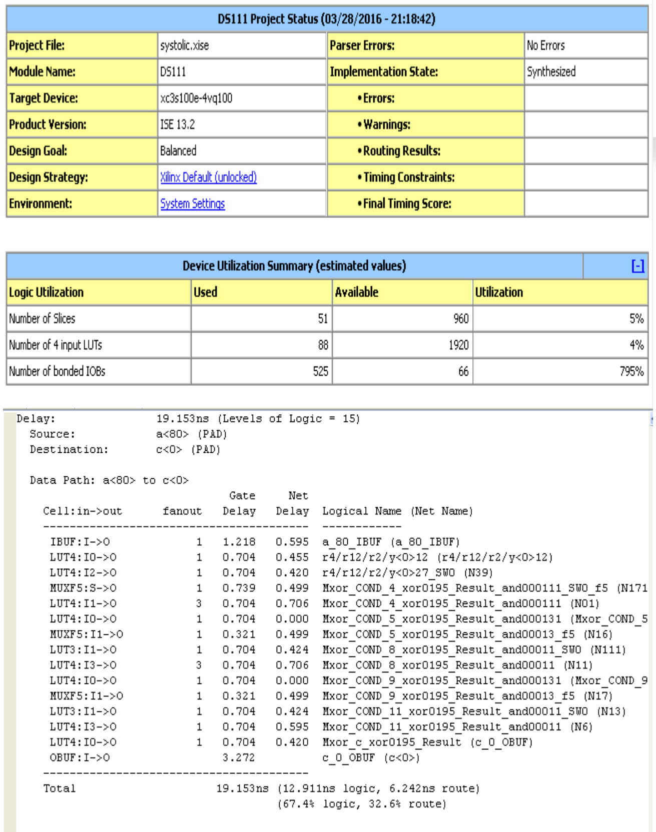
Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	136	960	14%
Number of 4 input LUTs	239	1920	12%
Number of bonded IOBs	520	66	787%

```
=========================================================================
Timing constraint: Default path analysis
  Total number of paths / destination ports: 621 / 199
-------------------------------------------------------------------------
Delay:               12.030ns (Levels of Logic = 8)
  Source:            a<13> (PAD)
  Destination:       y<0> (PAD)

  Data Path: a<13> to y<0>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     IBUF:I->O             1   1.218   0.595  a_13_IBUF (a_13_IBUF)
     LUT4:I0->O            1   0.704   0.455  y<0>290 (y<0>290)
     LUT4:I2->O            1   0.704   0.424  y<0>337_SW0 (N16)
     LUT4:I3->O            1   0.704   0.424  y<0>337 (y<0>337)
     LUT4:I3->O            1   0.704   0.499  y<0>365 (y<0>365)
     LUT3:I1->O            1   0.704   0.499  y<0>977_SW0 (N18)
     LUT4:I1->O            1   0.704   0.420  y<0>977 (y_0_OBUF)
     OBUF:I->O                 3.272          y_0_OBUF (y<0>)
    ----------------------------------------
    Total                    12.030ns (8.714ns logic, 3.316ns route)
                                      (72.4% logic, 27.6% route)

-------------------------------------------------------------------------
```

Fig. 6.4: Synthesis result of DS2



DS111 Project Status (03/28/2016 - 21:18:42)			
Project File:	systolic.xise	Parser Errors:	No Errors
Module Name:	DS111	Implementation State:	Synthesized
Target Device:	xc3s100e-4vq100	• Errors:	
Product Version:	ISE 13.2	• Warnings:	
Design Goal:	Balanced	• Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	
Environment:	System Settings	• Final Timing Score:	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	51	960	5%
Number of 4 input LUTs	88	1920	4%
Number of bonded IOBs	525	66	795%

```
Delay:               19.153ns (Levels of Logic = 15)
  Source:            a<80> (PAD)
  Destination:       c<0> (PAD)

  Data Path: a<80> to c<0>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     IBUF:I->O             1   1.218   0.595  a_80_IBUF (a_80_IBUF)
     LUT4:I0->O            1   0.704   0.455  r4/r12/r2/y<0>12 (r4/r12/r2/y<0>12)
     LUT4:I2->O            1   0.704   0.420  r4/r12/r2/y<0>27_SW0 (N39)
     MUXF5:S->O            1   0.739   0.499  Mxor_COND_4_xor0195_Result_and000111_SW0_f5 (N171
     LUT4:I1->O            3   0.704   0.706  Mxor_COND_4_xor0195_Result_and000111 (N01)
     LUT4:I0->O            1   0.704   0.000  Mxor_COND_5_xor0195_Result_and000131 (Mxor_COND_5
     MUXF5:I1->O           1   0.321   0.499  Mxor_COND_5_xor0195_Result_and00013_f5 (N16)
     LUT3:I1->O            1   0.704   0.424  Mxor_COND_8_xor0195_Result_and00011_SW0 (N111)
     LUT4:I3->O            3   0.704   0.706  Mxor_COND_8_xor0195_Result_and00011 (N11)
     LUT4:I0->O            1   0.704   0.000  Mxor_COND_9_xor0195_Result_and000131 (Mxor_COND_9
     MUXF5:I1->O           1   0.321   0.499  Mxor_COND_9_xor0195_Result_and00013_f5 (N17)
     LUT3:I1->O            1   0.704   0.424  Mxor_COND_11_xor0195_Result_and00011_SW0 (N13)
     LUT4:I3->O            1   0.704   0.595  Mxor_COND_11_xor0195_Result_and00011 (N6)
     LUT4:I0->O            1   0.704   0.420  Mxor_c_xor0195_Result (c_0_OBUF)
     OBUF:I->O                 3.272          c_0_OBUF (c<0>)
    ----------------------------------------
    Total                    19.153ns (12.911ns logic, 6.242ns route)
                                      (67.4% logic, 32.6% route)
```

Fig. 6.3: Synthesis result of DS1

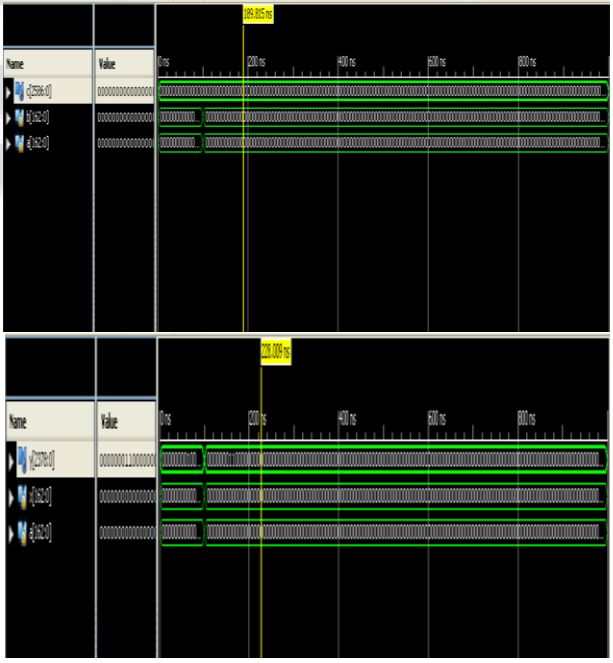
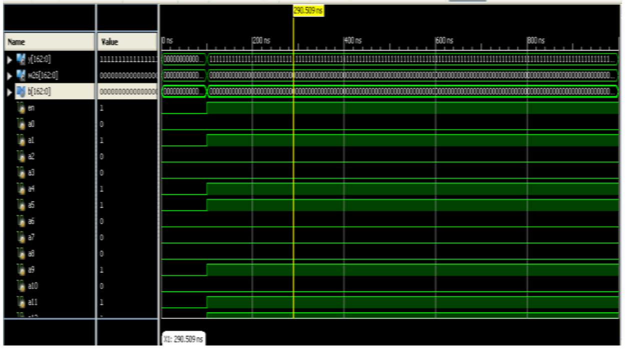
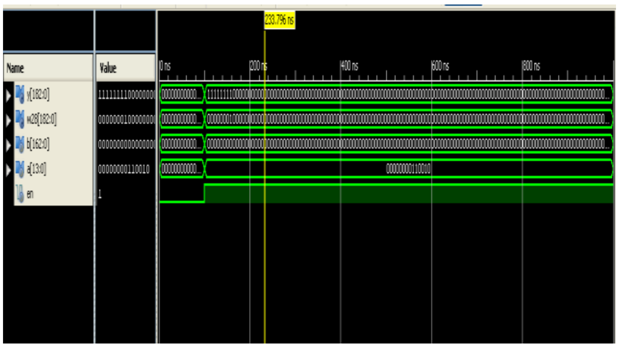


Fig. 6.5: Simulation results of BP I & BP II





VII. CONCLUSION

We have proposed an efficient strategy for data sharing by multiple systolic arrays to reduce the register complexity, and hence the overall area-complexity. Besides, we have proposed a novel modular reduction approach to reduce the delay for modular reduction operation, and based on that we have derived another pair of bit-parallel and digit-serial tructures where the critical-path is reduced to (TA+TX) to achieve high-throughput computation. The synthesis results show that the proposed multipliers have significantly shorter latency, lower area-time complexity and higher throughput than the existing competing designs. To the best of our knowledge, this is the first report on low latency systolic multipliers for finite field Where latency is independent of field order. The proposed designs are flexible to provide trade-off between latency, area-time complexity and throughput rate, which could be leveraged to match with the requirement and constraints of applications and deployment environment. The proposed project can be extended further by increasing the no. of Processing Elements(PE's).

REFERENCES

[1] I. Blake, G. Seroussi, and N. P. Smart, Elliptic Curves in Cryptography, ser. London Mathematical Society Lecture Note Series. Cambridge, U.K.: Cambridge Univ. Press, 1999.

[2] N. R. Murthy and M. N. S. Swamy, "Cryptographic applications of brahmaqupta-bha skara equation," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 7, pp. 1565–1571, 2006.

[3] J. Xie, P. K. Meher, and J. He, "Low-complexity multiplier for based on all-one polynomials," IEEE Trans. Very Large Scale Integr. (VLSI) Syst, vol. 21, no. 1, pp. 168–173, Jan. 2013.

[4] L. Song and K. K. Parhi, "Low-energy digit-serial/parallel finite field multipliers," J. VLSI Digit. Process., vol. 19, pp. 149–166, 1998.

[5] P. K. Meher, "On efficient implementation of accumulation in finite field over and its applications," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 17, no. 4, pp. 541–550, 2009.

[6] C.-Y. Lee, J.-S. Horng, I.-C. Jou, and E.-H. Lu, "Low-complexity bit-parallel systolic montgomery multipliers for special classes of ," IEEE Trans. Comput., vol. 54, no. 9, pp. 1061–1070, 2005.

[7] P. K. Meher, "Systolic and super-systolic multipliers for finite field based on irreducible trinomials," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 55, no. 4, pp. 1031–1040, May 2008.

[8] NIST. Boulder, CO [Online]. Available: http://www.csrc.nist.gov/ publications