INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 5 DEC 2016

A NOVEL MODULAR REDUCTION APPROACH TO REDUCE THE DELAY FOR HIGH-THROUGHPUT COMPUTATION, AND LOW LATENCY

B.Dinesh [(1)] Dr.D.Satyanarayana.Ph.D [(2)]

PG Scholar, Rajeev Gandhi Memorial CollegEngg.&Tech.,(Autonomous)[(1)]

Professor,Rajeev Gandhi Memorial CollegEngg.&Tech.,(Autonomous)[(2)]

Abstract: Recently, finite field multipliers having high throughput rate and low-latency have gained great attention in emerging cryptographic systems, but such multipliers over GF(2^M) for National Institute Standard Technology (NIST) pentanomials are not so abundant. In this paper, we present two pairs of low-latency and high-throughput bit-parallel and digit-serial systolic multipliers based on NIST pentanomials. We propose a novel decomposition technique to realize the multiplication by several parallel arrays in a 2-dimensional (2-D) systolic structure (BP-I) with a critical-path of , where is the propagation delay of an XOR gate. The parallel arrays in 2-D systolic structure are then projected along vertical direction to obtain a digit-serial structure (DS-I) with the same critical-path. For high-throughput applications, we present another pair of bit-parallel (BP-II) and digit-serial (DS-II) structures based on a novel modular reduction technique, where the critical-path is reduced to TA+TX,TA being the propagation delay of an AND gate. A strategy for data sharing between a pair of processing elements (PEs) of adjacent systolic arrays has been proposed to reduce area-complexity of BP-I and BP-II further

INTRODUCTION

Finite Field multiplication over operation, which is frequently used in elliptic curve cryptog-raphy is a basic field (ECC) to perform point-additions and point-doubling operations on an elliptic curve. The irreducible Pentanomials have been popularly used to generate binary extension fields to be used in ECC. Moreover, National Institute of Standards and Technology (NIST)has recommended three pentanomials for ECC implementation. Several efforts have therefore been made on efficient realization of multiplication over GF(2^M) based on irreducible Pentanomials.

Systolic designs provide area-time efficient implementation due to modularity and regularity of their structures, where each processing element (PE) has the same or similar circuit design, and one PE can pass the signals to its neighboring PE at a high speed on a fully pipelined path.

The traditional LSD-first multiplication given by (2) can be described by Algorithm 1. Fig. 1 shows a digit-serial multiplier over GF(2m) based on Algorithm 1. It consists of one multiplier core, two registers for two reduction

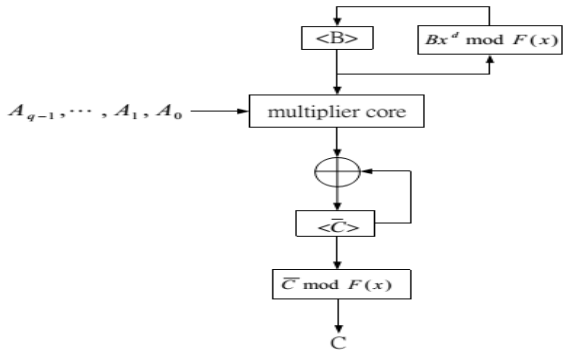
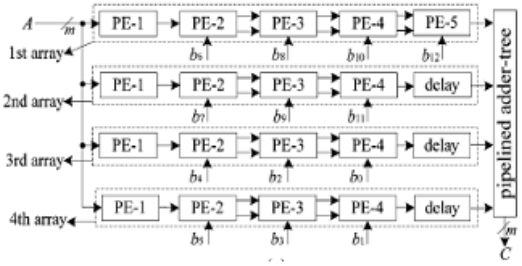


Figure. Traditional LSD-first digit-serial multiplier

Montgomery multiplication is a method for computing ab mod m for positive integers a, b, and m. It reduces execution time on a computer when there are a large number of multiplications to be done with the same modulus m, and with a small number of multipliers.

Volume 5, Issue 5 DEC 2016

Montgomery multiplication is a method for computing ab mod m for positive integers a, b, and m. 1 It reduces execution time on a computer when there are a large number of multiplications to be done with the same modulus m, and with a small number of multipliers.



EXISTING SYSTEM

Generally, all existing systolic multipliers, including bit-parallel and digit-serial structures, involve large latency and suffer from several other issues as outlined in the following.

• Bit-parallel (BP-1) systolic structures usually have large registercomplexity not only for pipelining, but also for providing the staggered input to the PEs to wait for the appropriate accumulated partial products.

• Critical-paths of digit-serial (DS-1) systolic structures usually increases with digit-size or fielddigit-size or field-order, which reduces throughput rate effectively

• Apart from that the average computation time (ACT) of the digit-serial structures increases with digit-size or field-order

Bit-Parallel Systolic Multiplier-I (BP-I)

The proposed bit-parallel systolic multiplier-I (BP-I) based on Algorithm 1 is shown in Fig. 1. It consists of one pre-computing (PRC) cell, one pipelined adder tree (PAT), and W systolic arrays (each array has PEs). The PRC cell,1,U=0,1,W-1 and the last PE (PE-), are shown in Fig. 1(c)–(e), respectively

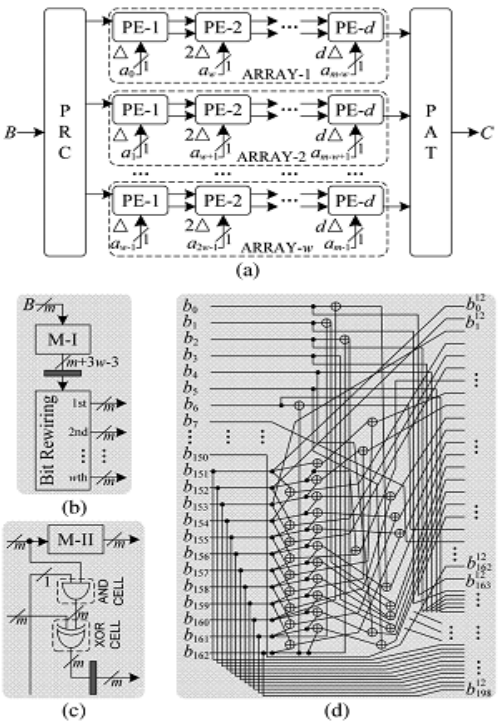


Fig. 1. Proposed bit-parallel systolic multiplier-I (BP-I) overGF(2^M) , where DELTA denotes a unit delay and each black block denotes register(a) Proposed systolic structure. (b) Internal structure of PRC cell. (c) Internal structure of PE-1. (d) Internal structure of M-I cell where M=16]

Digit - Serial Systolic Multiplier -I (DS -I)

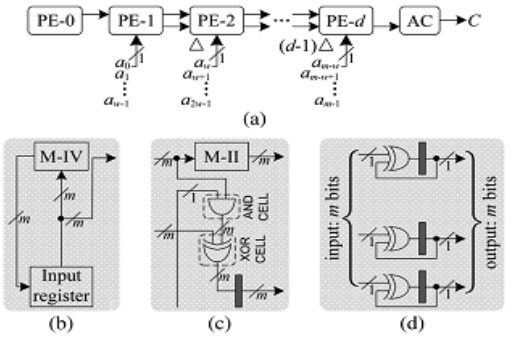


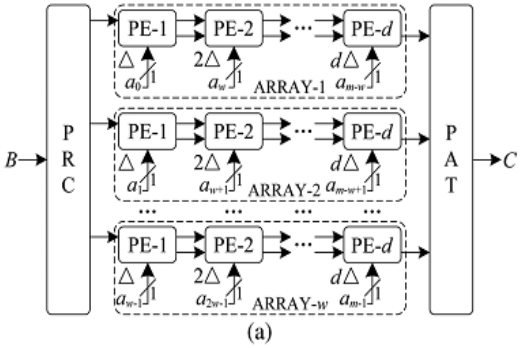
Fig. 2. Proposed digit-serial systolic multiplier-I (DS-I), where denotes unit delay and each black block denotes register cell. (a) Proposed structure. (b) Internal structure of PE[0],. (c) Internal structure of a regular PE. (d) Internal structure of AC cell.

We can project the parallel arrays of BP-I along vertical direction to have the proposed digit-serial systolic multiplier-I (DS-I) as shown in Fig. 2. DS-I consists of PEs and one accumulation (AC) cell. The internal structures of PE-0, regular PE and AC cell are shown in Fig. 2(b)–(d), respectively. As shown in Fig. 2(b), all bits of operand are loaded in to an input register and the output of that register is fed to PE-1 as well as the M-IV cell to perform modular operation by one degree during each cycle period

Proposed bit-parallel and digit-serial multiplication

Proposed Bit - Parallel Systolic Multiplier - II (BP -II)

The proposed BP-II based on Algorithm 2 is shown in Fig.3. The a critical-path of $\max\{T_M \ \ r, T_M \ \ r, T_A + T_X\} = (T_A + T_X)$ (M-I cell is two-stage pipelined and thus critical path of PRC is T_X), where and refer to the propagation time of M-V cell and M-VI cell, respectively. BP-II yields its first output (d+1 $\log_2 w$)cycles after the operands are fed to the structure, while the successive output are obtained in every cycle thereafter. BP-II, therefore, has higher throughput rate than BP-I at the cost of a small number of XOR gates and registers. The overhead of hardware complexity, however, is minor compared to the increase in throughput rate achieved by this structure



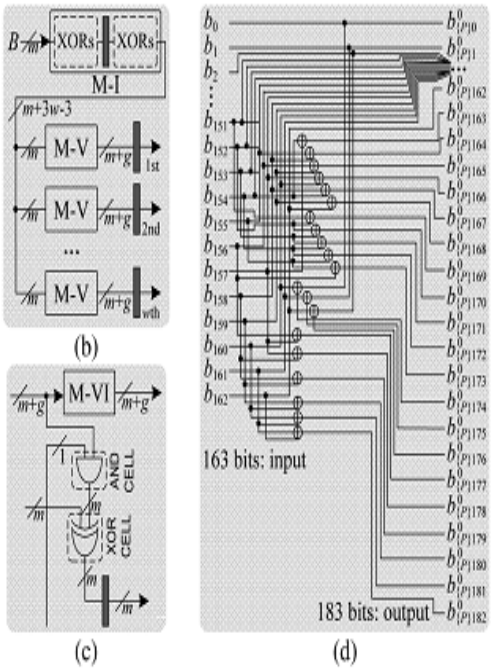


Fig.3. Proposed BP-II, where.(a) Proposed structure. (b) Internal structure of PRC, where M-I cell is designed into two-stage pipeline to reduce the critical-path to . (c) Internal structure of a regular PE. (d) Detailed structure of M-V cell in PRC

Proposed Modified Bit- Parallel Systolic Multiplier – II

Where we can have the modified BP-II (MBP-II) multiplier as shown in Fig. 4. The internal structures of PRC cell and regular PE of various arrays are shown in Fig. 4(b)–(d), respectively. The critical-path and latency of MBP-II are exactly the same as BP-II. M-VI cell in regular PE of Array-1 derives $B_{NE}^{(V+1)W+U}$ from $B_{NE}^{(VW+U)}$. Since there is no M VI cell in PEs of Array-2 to Array- , the area-complexity of MBP-II is smaller than that of BP-II

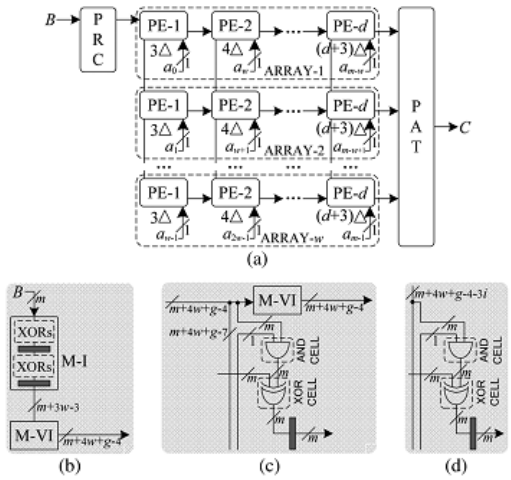


Fig.4. Proposed modified bit-parallel systolic multiplier-II (MBP-II) over GF(2^M), where denotes a unit delay, black block denotes register cell and g=(2w-k1+k3). (a) Proposed systolic structure. (b) Internal structure of PRC cell. (c) Internal structure of regular PE of Array-1. (d) Internal structure of regular PE of Array-2 to Array-w ,

Proposed Digit-Serial Systolic Multiplier-II (DS-II)

Novel modular reduction approach we have derived the DS-II multiplier as shown in Fig. 5. It consists of PEs and one accumulation (AC) cell. Theinternal structures of PE-0, regular PE and AC cell are shown in Fig. 4(b)–(d), respectively. As shown in Fig. 4(b), all bits of operand are fedto the M-V cell and the output is then loaded in to bit-registers and then are latched out (meanwhile the output bits are fed to PE-1) to the M-VII cell to perform modular operation by one degree during each cycle period (to obtain from , for).

The output bits of M-VII cell are then latched back in to the registers to be used in by PE-0 in the next cycle period. The regular PE, 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. 4(d), contains parallel bit-level finite field accumulators. During each cycle period, the newly received input is then added with the previously accumulated result and the result of addition is stored in the register cell to be used during the next cycle. DS-II has the same critical-path as that of BP-II. It gives the first output of desired product after cycles, while the successive output are produced at the interval of cycles thereafter.

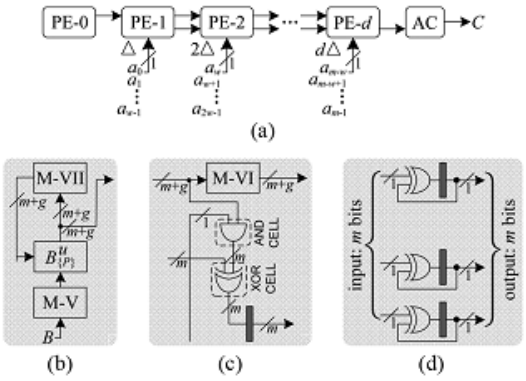
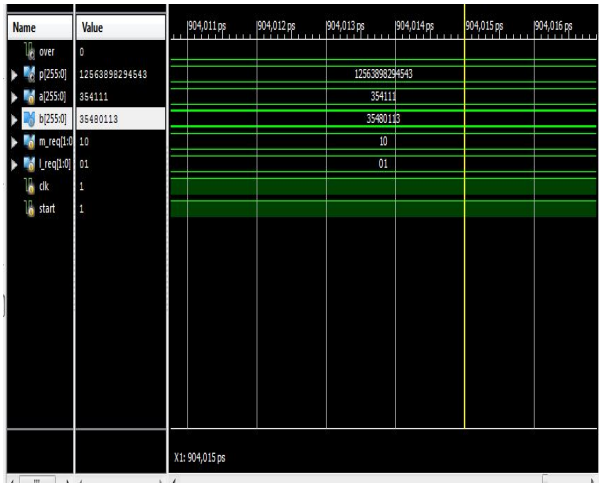


Fig. 5. Proposed digit-serial systolic multiplier-II (DS-II), where denotes unit delay, each black block denotes register cell and.(a) Proposed structure. (b) Internal structure of PE[0], where . (c) Internal structure of a regular PE. (d) Internal structure of AC cell.

RESULTS

SIMULATION RESULTS



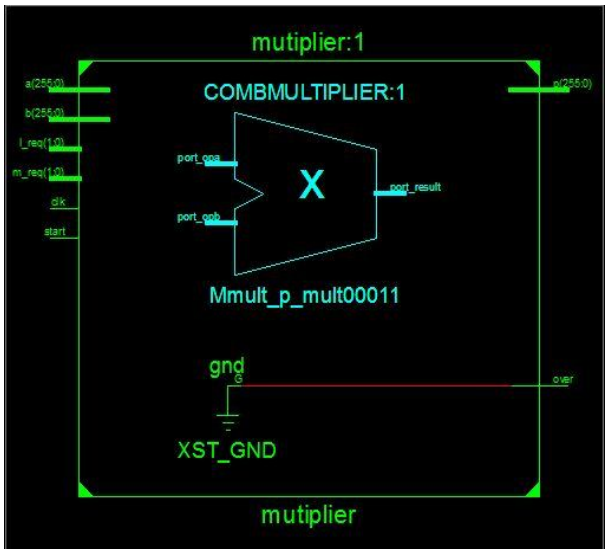
Design summary

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	16384	4656	351%
Number of 4 input LUTs	32641	9312	350%
Number of bonded IOBs	769	232	331%

Timingreport:

```
LUT2:I1->O            1   0.612   0.000  Mmult_p_mult0001_Madd223_lut<249>
MUXCY:S->O            1   0.404   0.000  Mmult_p_mult0001_Madd223_cy<249>
XORCY:CI->O           1   0.699   0.426  Mmult_p_mult0001_Madd223_xor<250>
LUT2:I1->O            1   0.612   0.000  Mmult_p_mult0001_Madd239_lut<250>
MUXCY:S->O            1   0.404   0.000  Mmult_p_mult0001_Madd239_cy<250>
XORCY:CI->O           1   0.699   0.426  Mmult_p_mult0001_Madd239_xor<251>
LUT2:I1->O            1   0.612   0.000  Mmult_p_mult0001_Madd247_lut<251>
MUXCY:S->O            1   0.404   0.000  Mmult_p_mult0001_Madd247_cy<251>
XORCY:CI->O           1   0.699   0.426  Mmult_p_mult0001_Madd247_xor<252>
LUT2:I1->O            1   0.612   0.000  Mmult_p_mult0001_Madd251_lut<252>
MUXCY:S->O            1   0.404   0.000  Mmult_p_mult0001_Madd251_cy<252>
XORCY:CI->O           1   0.699   0.426  Mmult_p_mult0001_Madd251_xor<253>
LUT2:I1->O            1   0.612   0.000  Mmult_p_mult0001_Madd253_lut<253>
MUXCY:S->O            1   0.404   0.000  Mmult_p_mult0001_Madd253_cy<253>
XORCY:CI->O           1   0.699   0.426  Mmult_p_mult0001_Madd253_xor<254>
LUT2:I1->O            1   0.612   0.000  Mmult_p_mult0001_Madd254_lut<254>
MUXCY:S->O            0   0.404   0.000  Mmult_p_mult0001_Madd254_cy<254>
XORCY:CI->O           1   0.699   0.357  Mmult_p_mult0001_Madd254_xor<255>
OBUF:I->O                 3.169          p_255_OBUF (p<255>)
----------------------------------------
Total                    35.435ns (30.963ns logic, 4.472ns route)
                                  (87.4% logic, 12.6% route)
```

RTL Schematic



CONCLUSION

Low-latency high-throughput systolic structures for multipliers over GF(2^M)based on NIST recommended pentanomials are pre ented. We have proposed an algorithm to decompose the multiplication to be processed independently by multiple systolic arrays in parallel in order to lower the latency.Based on proposed decomposition scheme we have suggested a pair of bit-parallel and digit-serial systolic multipliers. 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 structures where the critical-path is reduced to to TA+TXachieve high-throughput computation.

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-bhaskara 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.