ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Multiplier for Finite Field Class Using Dynamic Algorithm

Mohammad Neha Samreen
MTech Student
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

B.Sowmya
Assistant Professor
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

ABSTRACT: ***Finite field multipliers are widely used in elliptic curve cryptography as a basic building block. Normal basis is the most suitable for representation of binary field elements since squaring operation can be done by simple cyclic shift of its binary digits. In this paper, efficient word level multipliers using normal basis and reordered normal basis in Galois field is proposed, where Reordered Normal Basis (RNB) is referred to as certain permutation of optimal normal basis type- II. These architectures provide a better area and power efficiency when compared to the existing Word Level finite field multiplier using Normal Basis (WLNB) and Reordered Normal Basis (WLRNB). WLNB and WLRNB are coded in VHDL and simulated in Modelsim10.0b. Area and Power reports are obtained using Xilinx ISE.***

Index Terms: ***Neighbor position verification, mobile ad hoc networks, vehicular networks***

INTRODUCTION:

Fast multiplication in a finite field GF(2m) is a basis step in communications engineering applications, such as error-correcting codes or cryptograph algorithms. A new parallel algorithm on the polynomial basis bit-parallel multiplier is presented. This new parallel algorithm saves about 25% execution time while comparing with the conventional algorithms. The hardware version for the proposed parallel algorithm is also invented. The new hardware structure requires only the space complexity of O(m) while existing multipliers need the space complexity of O(m2). The time complexity of the proposed multiplier takes only about half of the time complexity of the existing Lee's multiplier Hardware implementation of finite field multipliers can be classified into three categories. First category are bit level multipliers. A bit level multiplier takes m clock cycles to finish one multiplication in a field of size m. The multipliers in this class are considered to be low power consuming and taking small area of silicon. Their main disadvantage is their low multiplication speed for large field sizes. The second category is full parallel multipliers. A full parallel multiplier takes one clock cycle to finish the multiplication for any field size. These multipliers are impractical since they require large silicon area. The third category is word level finite field multiplier which takes d clock cycles, $1 \leq d \leq m$, to finish one multiplication operation of size m. The value of d can be selected by designer to set the tradeoff between area and speed

Existing System

Digit-serial systolic multiplication architecture for all-one polynomials (AOP) over GF (2^m) for efficient implementation of Montgomery Multiplication (MM) Algorithm, suitable for cryptosystem. Analysis shows that the latency and circuit complexity of the existing architecture are significantly greater than those of proposed designs for same classes of polynomials.

EXISTING SYSTEM ALGORITHM:

Low-Complexity Bit-Parallel Systolic Montgomery Multipliers for Special Classes of GF (2^m)

EXISTING SYSTEM DRAWBACKS:

1.The number of gate count is high so the area is not efficient.
2. The latency and critical-path of the designs is very high

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proposed System:

In Proposed system, we have presented a novel register- sharing technique to reduce the register requirement in the systolic structure. The proposed algorithm not only facilitates sharing of registers by the neighboring PEs to reduce the register complexity but also helps reducing the latency. Cut-set retiming allows introducing certain number of delays on all the edges in one direction of any cut-set of a signal flow-graph (SFG) by removing equal number of delays on all the edges in the reverse direction of the same cut-set.

PROPOSED SYSTEM BLOCK DIAGRAM:

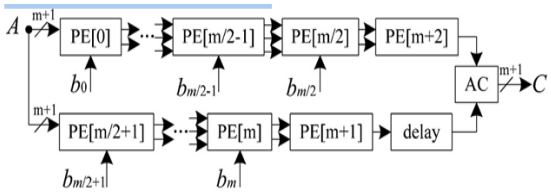

Fig. 1 Proposed Low Latency Systolic Structure

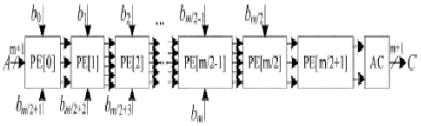

Fig. 2 Proposed Register Sharing Systolic Structure

PROPOSED SYSTEM TECHNIQUE:

- Cut set retiming
- Register Sharing

PROPOSED SYSTEM ADVANTAGES:

1.Less area-time-power complexity compared with the existing designs.

2.We have presented a novel register-sharing technique to reduce the register requirement in the systolic structure

3. The proposed structure not only facilitates sharing of registers by the neighboring PEs to reduce the register complexity but also helps reducing the latency

Practical evaluation

To confirm the results in practice we implemented 64, 128, and 256 bit versions of hCKM and hRAIK for a 0.25µm CMOS technology and measured the area and the timing. The results are shown in Table 5. We also estimated the power consumption for one multiplication based on the Synopsys Primepower tool[12]. The practical measurements approve the theoretical assumptions very well. OurSequential Polynomial Multiplier Even with the hRAIK method combinatorial multiplier with long bit sizes are still quite slow and not as small as it is desirable for mobile devicess or even wireless sensor nodes. Common approaches use smaller combinatorial multiplication units and serialize the multiplication. Actually the original iterative Karatsuba multiplier (IKM) approach was presented as solution for this purpose. It uses smaller combinatorial multiplication blocks, and applies them repeatedly following the Karatsuba method in order to perform a larger polynomial multiplication. The IKM design for a 233 bit multiplication unit presented in [1] is the starting point for the investigation concerning improved IKM design. It consists of three main parts:The selection logic selects and combines the factors of the partial multiplication (left column of Tab. 2), the partial multiplier performs the partial multiplication within one clock cycle, and the accumulation logic computes the final product by accumulating the partial products. The number of clock cycles depends on the size of the segmentation

Systolic Design

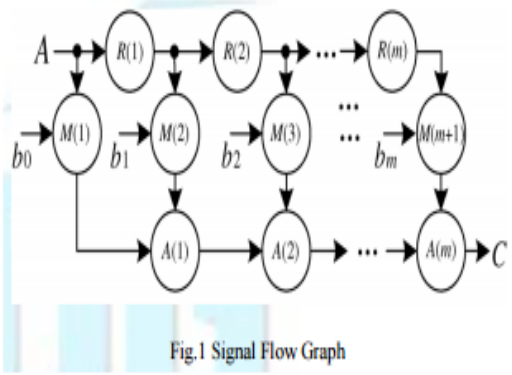

Fig.1 Signal Flow Graph

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

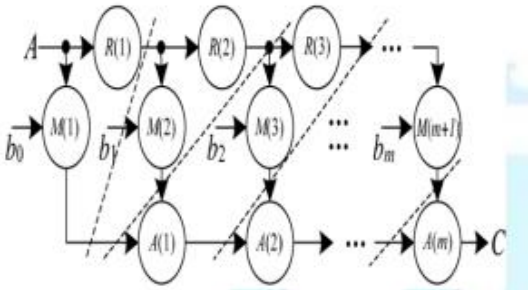

Fig.2 Cut set Retimed Signal Flow Graph

Proposed Systolic Structure

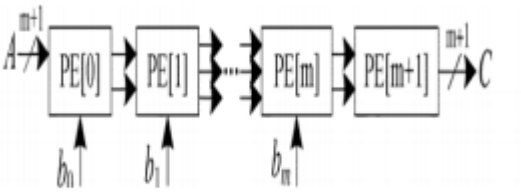

Fig.3 Proposed Systolic Array

TECHNOLOGIES

Currently there are four technologies in use. They are: static RAM cells, anti-fuse, EPROM transistors, and EEPROM transistors. Depending upon the applications, one FPGA technology may have features desirable for that application.

1. Static RAM Technology

In the Static RAM EPGA programmable connections are made using pass-transmission, transmission gates, or multiplexers that are controlled by SRAM cells. This technology allows fast in-circuit reconfiguration. The major disadvantage is the size of the chip required by the RAM technology and that the chip configuration needs to be loaded to the chip from some external source (usually external non-volatile memory chip). The FPGA can either actively read its configuration data out of external serial or byte-parallel PROM (master mode), or the configuration data can be written into the FPGA (slave and peripheral mode). The FPGA can be programmed an unlimited number of times.

2.Anti-Fuse Technology

An anti-fuse resides in a high-impedance state; and can be programmed in to low impedance or "fused" state. This technology can be used to make program once devices that are less expensive than the RAM technology.

3. EPROM Technology

This method is the same as used in the EPROM memories. The programming is stored without external storage of configuration. EPROM based programmable chip cannot be re-programmed in circuit and need to be cleared with UV erasing.

4. EEPROM Technology

This method is the same as used in the EEPROM memories. The programming is stored without external storage of configuration. EEPROM based programmable chips can be electrically erased but generally cannot be re-programmed in-circuit FUSE-One-time programmable.

DESIGN PROCESS ALGORITHM

Step 1: Understand the problem.

Step 2: Draw the block diagram (data path)

Step 3: Design the state machine (control)

Step 4: Code in VHDL or Verilog

Step 5: Simulate it (ensure the functional correctness)

Step 6: Synthesis it (get the EDIF file)

Step 7: Implement it (get the bit file)

Step 8: Write the software driver

Step 9: Download to FPGA and get results

CONCLUSION

Modified systolic design for the multiplication over GF(2m) based on irreducible AOP using register sharing technique is proposed. Using cut-set retiming we have been able to reduce the critical path to one XOR gate delay and using register sharing technique,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

we achieved a low-latency bit-parallel systolic multiplier. Compared with the existing systolic structures for bit-parallel realization of multiplication over GF(2m), the proposed design is found to involve less area, shorter critical-path and lower latency.

REFERENCES:

[1] 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[3] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning:Attacks and Countermeasures," Proc. IEEE Military Comm. Conf.(MILCOM), Nov. 2008.

[4] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

[5] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13, pp. 27-59, 2007.

[6] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes," Proc. IEEE INFOCOM, Apr. 2008.

[7] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P.Hubaux, "Secure Neighborhood Discovery:AFundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.

[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.