VRSEC
VELAGAPUDI RAMAKRISHNA SIDDHARTHA ENGINEERING COLLEGE
Estd. 1977
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Implementation Of An Efficient Polynomial Basis Finite Field GF(2^m) Multiplier for IoT Applications

Students Details:

	Name	Roll Number
1.	V. Bhargava Sandeep	188W1A04B0
2.	V. Tejaswini	188W1A04B2
3.	L. Sree Sowjanya	188W1A0489
4.	V. Venkata Abhinav	198W5A0415

Batch No: - B8 **AY 2021-22**

Guide Details:

Name: P. Siva Ramakrishna

Designation: Assistant Professor

Abstract:

- ✓ Advancements in wireless technology led to the evolution of many modern wireless network applications.
- ✓ Internet of Things (IoT) is a state of art communication technology and Edge devices are fundamental in this kind of communication.
- ✓ In IoT edge devices security is one of the concern, asymmetric algorithms like Elliptic curve cryptography (ECC) can be used in this issue which depend on finite field $GF(2^m)$ arithmeticoperations, here *GF* means Galois Field.
- ✓ Multiplication is important operation as it can be utilized in functions like division and inversion. In our work, low complexity Digit Serial finite field $GF(2^m)$ multiplier using primitive polynomials as field irreducible polynomials is done and realized in MATLAB.
- ✓ A Verilog model is developed and simulated for comparing the MATLAB results.

Introduction:

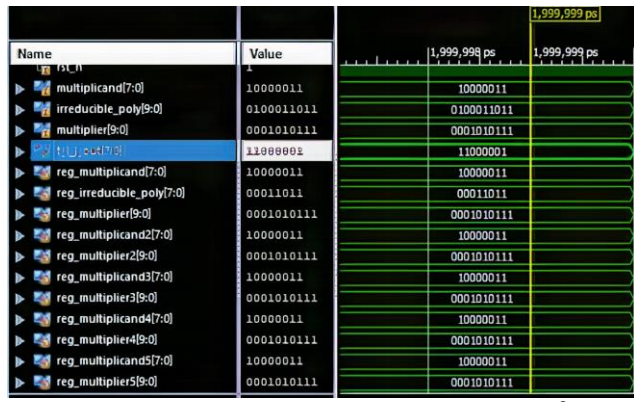
- ✓ Internet of Things (IoT) is a state of art communication technology and several applications are emerged benefiting from this idea and edge-devices play a crucial role in this, these devices have limited memory and less computation resources and sometimes there is a requirement of training large data into them. These are used in IoT applications.
- ✓ Security must be added to these edge devices to avoid network-based attacks. It can be done using Cryptography algorithms we need to see that these security algorithms don't take up much space for proper functioning of other operations.
- ✓ These security and data reliability algorithms rely heavily on finite field GF(2^m) arithmetic computations, in particular, multiplication. So an efficient multiplication algorithm is needed for implementing these security algorithms.
- ✓ There are different architectures to implement GF(2^m) Multiplication like Bit Serial, Digit Serial and Bit parallel. Basic Multiplication formula in Finite Filed Arithmetic can be given as $Z = XY \bmod P(\gamma)$
- ✓ Where X and Y are two Arbitrary Filed elements and $P(\gamma)$ is an irreducible polynomial which is used in modular reduction.

Methodology:-

- ✓ The basic formula for a finite field multiplication process is executed using MATLAB following Digit-Serial algorithm where it require some functions like multiplication and division which in other words can also be stated as convolution and de-convolution.
- ✓ These can be done using pre-defined functions in MATLAB and then with help of XOR logic and shifting of bits we can implement multiplication in Verilog.
- ✓ Functions used in MATLAB and there uses are as follows:
  - ✓ gfconv & gfdeconv- Helps in Multiplication , Modular reduction of polynomials over given Galois field.
  - ✓ primpoly- To find the primitive polynomials over given Galois field.
  - ✓ tic and toc- Set of combined function to assess time needed to execute a specific code.
- ✓ In Verilog we implement XOR and shift operations for performing multiplication and division using modules for functional implementation in behavioral model.

Results:-

- ✓ Using the proposed Methodology we found that in this multiplier the time and space complexity required for performing multiplication operation is reduced. The multiplication result in MATLAB and Verilog are same.



Timing Waveforms of Inputs and Output for a GF(2^8) computation

Conclusion:-

- ✓ The proposed idea of Low Complexity Multiplier using Digit-Serial Algorithm and Primitive polynomials is done using MATLAB and Verilog. We found that using this approach the complexity of implementation is reduced when compared to classical approach.

Outcomes: - (Participation in competitions/ Publication details)

[1] P. Siva Ramakrishna, V. Bhargava Sandeep, V. Tejaswini, L. Sree Sowjanya and V. Venkata Abhinav, "Implementation of Low Complexity Finite Field GF(2^m) Multiplier Using Irreducible Primitive Polynomial" in *2022 IEEE International Conference on Advances in Electrical Computing Communications and Sustainable Technologies (ICAECT 2022)*, Apr 2022.