Dr.Ravi Shankar Mishra, Prof Puran Gour, Mohd Abdullah/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
www.ijera.com
Vol. 1, Issue 3, pp.820-823

Design & Implementation of 8 Bit Galois Encoder for on FPGA Secure Data Transmission

Dr.Ravi Shankar Mishra
Head Of Department
NRI IST BHOPAL

Prof Puran Gour
Assistant Professor
NRI IST BHOPAL

Mohd Abdullah
M.Tech Scholar
NRI IST BHOPAL

ABSTRACT:-

Galois Field Theory deals with numbers that are binary in nature, have the properties of a mathematical "field," and are finite in scope. Galois operations comprises of Addition, multiplication and logarithms[1]. Galois Field multipliers have been used for coding theory and for cryptography [9]. Both areas are complex, with similar needs, and both deal with fixed symbolic alphabets that neatly fit the extended Galois Field model. The use of FPGA Spartan XC3S400-4PQG208C in this area is new, but their utilization is intriguing for their security capabilities as well as for their performance and power characteristics. In addition, the nonvolatility of FPGA is useful for polynomial and key storage within devices, and Spartan XC3S400-4PQG208C, particularly, provide multiple security features

In this paper we present GF (2^m) Galois field encoder its verification on FPGA Spartan XC3S400-4PQG208C using the National Institute Standard & Technology(NIST) chosen irreducible polynomial. A complete verification of multiplication is simulated on ModelSim 10.0 a & implemented on FPGA Spartan 3 will be presented to assure its validity .

Keywords: Galois field, Irreducible polynomial, Galois Encoder, FPGA

1.INTRODUCTION:-

A Galois field multiplication method enables for a arithmetical operations including addition a deduction a multiplication and a multiplier utilizing the multiplication method . The Galois field multiplication method easily realizes various field multipliers by ANDing

respective items of multiplier factor in a stepwise manner rotating left values resulted from the AND operation at the previous step Exclusively ORing the respective values resulted from the rotation with respective corresponding values resulted from AND operation at the current step and operating on the highest polynomial term generated at the previous step in accordance with a generated polynomial. This approach of galois field can be used for designing the encoder and decoder section for the security purposes using the irreducible polynomial based on the NIST standard. .

2.Galois field algorithm

The message signal is taken in form of the multiplicand that denotes 8 bit of data. Galois algorithm is implemented on the multiplicand using the generator key irreducible polynomial and a 8 bit multiplier key. Mathematically 8 bit multiplication results in the 16 bit of the result but the Galois technique multiplication will result 8 bit resultant for 8 bit multiplication. As for the case of n bit multiplication it will result in n bit result.

The flowchart of Galois field algorithm describes the encoding technique using the shift and adds method . Operands will cover all combination of four binary bits and unlike standard multiplication the result will be four bit. In order to design four bit of Galois encoder the pre-requisite information is taken as message signal. The message signal is represented as the multiplicand the private key is taken as the irreducible polynomial based on NIST recommended specifications for cryptographic applications. The message bit is taken as input B , multiplier bit is taken input Ai .The irreducible polynomial and multiplicand remain static.The structure is able to multiply when the operands are all loaded .
Operation of the 8-bit multiplier brings as the MSB of the multiplier is under ANDing process with static multiplicand bit and resultant is EX-OR with current result register, which must initialize to 0. As multiplier bits shift, the result

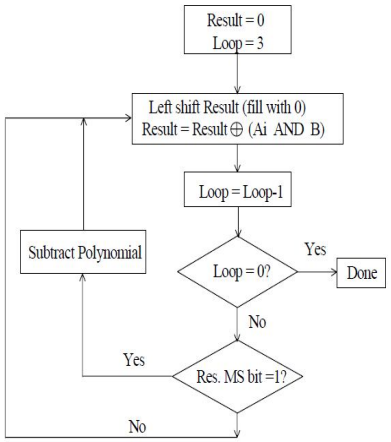

Fig.1. **Algorithm for GF (2^m) Multiplication (Shift and Add Technique)**

accumulates in "R" result. If R (3) is a 1, that means the current partial result is overflowing the 8-bit register and we must subtract a copy of the irreducible polynomial. Note that "subtraction" is also the EX-OR operation. This accomplishes the overall "modulo an irreducible polynomial" correction process.

3. Galois Encoder

The Galois encoder is used to encrypt the message using GF (2^m) algorithm. On receiving the original Message signal the Galois algorithm implemented on the FPGA encodes the message using the private key the irreducible polynomial and multiplier. The 8 bit multiplication results 8 bit encrypted data. The vhdl code is simulated on the model sim 10.0a edition and implemented on FPGA XC3S400-4PQG208C yields 65536 cryptographic results for GF (2^m)multiplier where m =8 of all possible combination inputs.

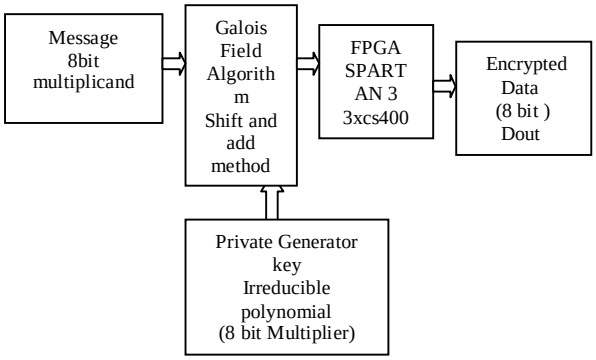

Fig. 2. **Block diagram for Galois Encoder**

The Galois encoder block diagram describes the flow design of the encryption process that generates the encrypted data using galois field algorithm.

6. Results

1) Synthesis result

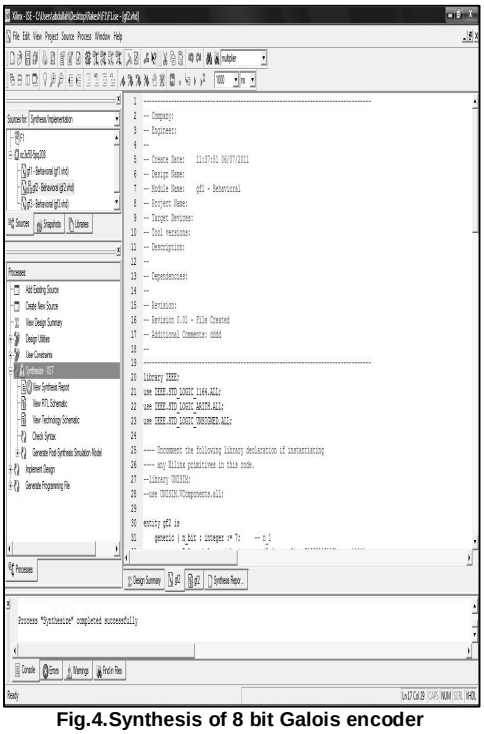

Fig.4.Synthesis of 8 bit Galois encoder

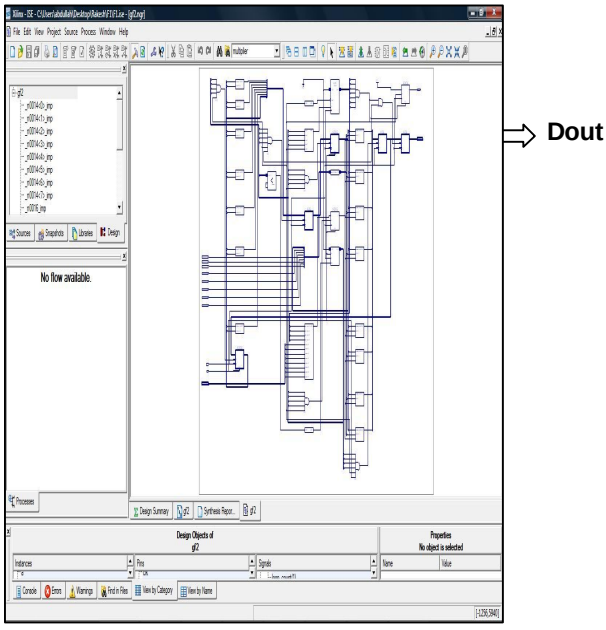

Fig 5. RTL view of 8 bit Galois encoder

2) **Device utilization Summary**

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	42	768	5%
Number of Slice Flip Flops	37	1536	2%
Number of 4 input LUTs	66	1536	4%
Number of bonded IOBs	23	124	18%
Number of GCLKs	1	8	12%

Table 1: Device utilization Summary

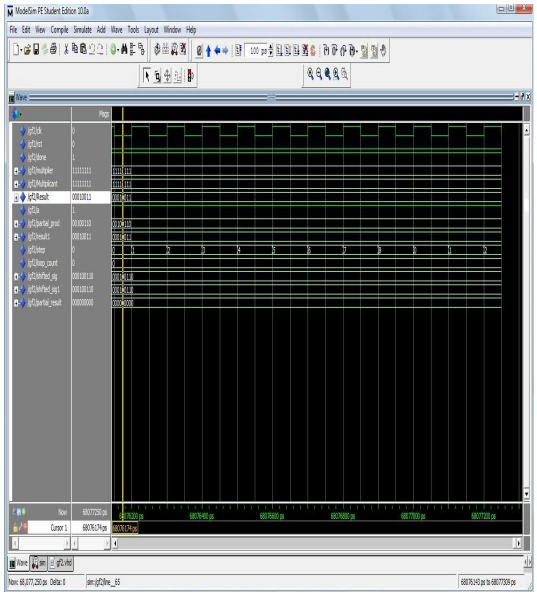

Fig.7.Simulation 8 bit Galois Encoder

3) Model sim 10.a simulated results

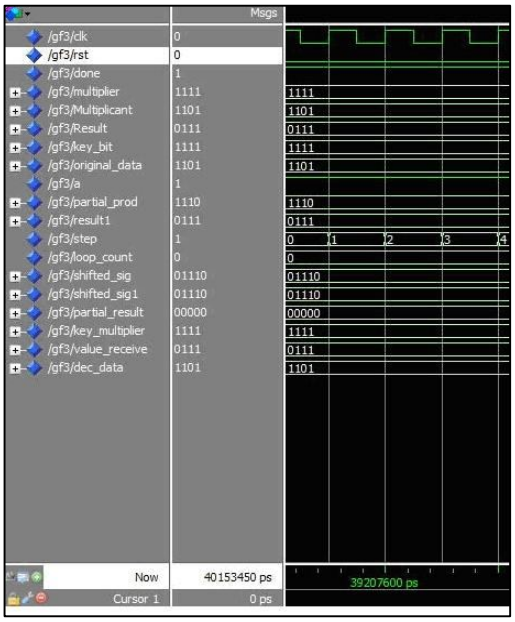

Fig.6.Intial state simulation

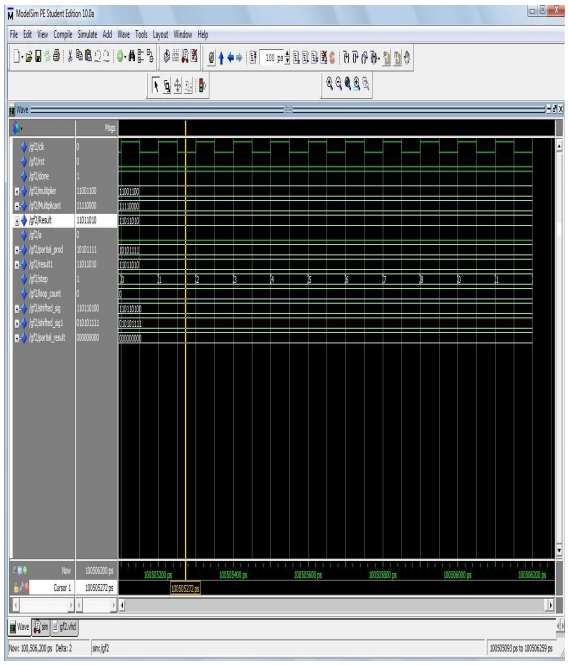

Fig.8. simulation of 8 bit Galois Encoder

The data encryption using the Galois field algorithm is shown in tabular format. When reset is taken as 1 the loop count is loaded with 4.Now again changing the reset pin from 1 to 0 & clk on 1 the results are fetched for encoding of the message signal. The encoded data result describes the conversion of data into encoded information.

Table 2:Analysis of different control Signals

7. Conclusion

We have presented the FPGA implementation of a *GF* (2^m) 8 bit Encoder which is based on recommended irreducible polynomial by NIST for applications in cryptosystems. The structure of the used multiplication algorithm, has allowed us to use effectively the resources in the FPGA Spartan3 , as it has already demonstrated in the previous results .The paper simples the circuit and performs high speed operation by decreasing the number of logic gates & increases security during communication dialogue This circuit would be in future designs, such as an 64 bit encoder . We have used a FPGA Spartan XC3S400-4PQG208C for physical implementation, and for synthesis and simulation process we have used the computational packet ISE8.1i provided by Xilinx.

S.NO	SIGNALS	INITIAL	RESULT1	RESULT2
1	CLK	0	1	1
2	RESET	1	0	0
3	MULTIPLICAND	00000000	11111111	11001100
4	MULTIPLER	00000000	11111111	11110000
5	ENCODED DATA	00000000	00010011	11011010
6	LOOP COUNT	4	0	0

8. References

[1]. FPGA Implementation of an Efficient Multiplier over Finite Fields GF(2m) Proceedings of the 2005 International Conference on Reconfigurable Computing and FPGAs (ReConFig 2005)
0-7695-2456-7/05 © 2005 IEEE

[2]. P. Kitsos, G. Theodoridis y O. Koufopavlou. “An efficient reconfigurable multiplier for Galois field GF(2m)”. *Microelectronics Journal*. Vol. 34, Pags. 975-980, 2003.

[3] A. Daly y W. Marnane. “Efficient Architectures for implementing Montgomery Modular Multiplication and RSA Modular Exponentiation on Reconfigurable Logic”. *FPGA´02*. Monterey, Ca. USA, 2002.

[4] G. Bertoni, J. Guajardo, S. Kumar, G. Orlando, C. Paar y T. Wollinger. “Efficient GF(pm)Arithmetic Architectures for Cryptographic Applications”. In Marc Joyce (Ed.): The Cryptographers´ Track at the RSA Conference CT-RSA 2003, volume LNCS 2616, pp. 158-175,San Francisco, CA, USA, April 2003.

[5] G.C. Ahlquist, B. Nelson y M. Rice. “Optimal Finite Field Multipliers for FPGA´s”. In P. Lysaght, J. Irvine, R. Hartenstein (Eds.): Field Programmable Logic and Applications. 9th International Workshop,FPL´99, volume LNCS 1673, pp. 51-60, Glasgow, UK, August/September 1999.

[6] S. Lin y D.J. Castello. *“Error Control Coding, Fundamentals and Applications”*, Prentice Hall, New Jersey, 1983.

[7] F.J. Mac Williams, N.J.A. Sloane, “*The theory of error correcting codes*”, North-Holand, 1977.

[8] L. Song y K.K. Parhi, “ Efficient Finite Field Serial/Parallel Multiplication”, *Proc. of International Conf. On Application Specific Systems, Architectures andProcessors*, pp. 72-82, Chicago,USA, 1996.

[9] Recommended Elliptic Curves for Federal GovernmentUse. *://csrc.nist.gov/CryptoToolkit/dss/ecdsa/NIST R eCur.pdf*

[10] J.López and R. Dahab. “Fast Multiplication on Elliptic Curves over GF(2m) without Precomputation”. In C.K. Koc and C. Paar (Eds.): Cryptography Hardware and Embedded Systems, CHES 1999, LNCS, Springer-Verlag, pp. 316-327, 1999.

[11] E. Savas, A.F. Tenca and C.K. Koc. “A Scalable and Unified Multiplier Architecture for Finite Fields GF(p) and GF(2m)”. In C.K. Koc and C. Paar (Eds.):Cryptography Hardware and Embedded Systems,CHES 2000, LNCS, Springer-Verlag, pp. 277-292,2000.

[12] F. Rodríguez-Henríquez. *New Algorithms andArchitectures for Arithmetic in GF(2m) Suitable forElliptic Curve Cryptography*. PhD Thesis, Oregon State University, 2000 Proceedings.

[13] http://www.xilinx.com/products/xaw/