I J C T A, 9(41), 2016, pp. 13-21 ISSN: 0974-5572

Comparative Analysis of 4-Bit and 8-Bit Galois Encoder in 90 nm Technology

Akhlaquer Rahman*, Ravi Shankar Mishra and Sandeep Dhariwal*****

ABSTRACT

In wireless communication security is the main issue due to the wireless media and as intruders, hackers or attackers are increasing day by day. So, we need a system that must give the guarantee of security. As day by day digitalization is increasing in every application and so that the speed of processors are increasing.

So, to fulfill the demand of security as well as high speed processors for fast computation, in this paper we have developed a new encoding techniques named as "Galois Encoding" technique. Galois Encoding techniques provides the secure communication as well as it does the fast computation within the processors with less delay processing time. Thus, Galois encoding provides security as well as save bandwidth and fast computations.

In this paper 4-bit and 8-bit Galois encoder has been compared on CADENCE 90nm technology, for synthesis we have used Encounter® RTL Compiler v14.10.

Keywords: Galois Algorithm, NIST, irreducible polynomial.

1. INTRODUCTION

Reliability of communication is an important issue in the present day where every device takes place in the digital world, such as message received in our mobile phone might be unreadable if error occurs due to some reason during the transmission or due to scratch in DVDs data may not be able to read. So, reliability is the main concern in the field of digital communication. So we must incorporate the technique which should be error free and should secure that means message should be in some coded form. Also in wireless communication security is the main issue due to the wireless media. As the medium is wireless so we can't detect and correct the transmitted message in the channel. So, one can incorporate the technique which can be done at transmitter only during the transmission of message signal using encoding technique which will actually alter the message into coded form or in some other form rather than the original message using the private key. First of all a code is taken for all the encode words, during transmission of data encoded message is transmitted. Applications such as wireless broadband radio transmissions as well as in computer hard drive data storing systems, errors must be corrected. As such systems has to be worked under extreme conditions, so we need efficient error correcting codes or error free encoding schemes. By need of such means we need fast arithmetic operations within the processors.

As, cryptography is the art of hiding information or converting main information in any other form using coding. In computer passwords, electronic commerce and even in ATM cards, Smart cards, Smartphones we need cryptography. Even in disciplines of mathematics, computer science including engineering we need modern cryptography. In these cryptographic applications encoding in form of multiplication is the most important. Thus, it is desirable to design an encoder which can be used for real time requirement with minimum hardware complexity, less delay to increase the computational speed, consumes less power. For error-correcting coding as well as cryptography even in digital signal processing arithmetic structures are used. Finite field are

* Lovely Professional University, Phagwara, Punjab-144411, *Email: rahman4u1991@gmail.com*

** Associate Professor, Lovely Professional University, Phagwara, Punjab-144411, *Email: ravi.19053@lpu.co.in*

*** Assistant Professor, Lovely Professional University, Phagwara, Punjab-144411, *Email: sandeep.19381@lpu.co.in*

having finitely many elements. So, classification of finite field is done by size. To perform all the operations in the finite field there must be limited number of elements in the finite field. Common Galois operations that are used for checking multiplication results is Ex-OR addition and multiplication. Galois Field multipliers are mainly used for cryptography in VLSI design circuits.

A Galois field multiplication method is used to perform the multiplication by the use of addition and irreducible polynomial along with multiplier and multiplicand. The Galois field multiplication method implements various field multipliers by use of "AND" operation of its items of multiplier factor in a stepwise fashion by rotate the left result values from the performing "ANDing" operation at the earlier step "Ex-ORing" the respective resulted values from the rotation with respect to the corresponding resulted values by performing "ANDing" operation at the present step and operating on the highest polynomial term generated at the earlier step on the basis of generated polynomial. For designing the encoder and decoder section of Galois field such approach is used which provides security by the use of irreducible polynomial which is pre-defined according to the NIST standards.

2. GALOIS ALGORITHM

By taking the Galois field multiplication property an algorithm can be implemented to design an encoder. A Galois multiplication process provides an arithmetical operations such as addition, multiplication by deduction as well as a multiplier by the use of the multiplication process. The Galois multiplication process provides various field multipliers by "ANDing" the corresponding items of multiplier factor in a stepwise fashion by the rotation of left values resulted from the "ANDing" operation at the previous step "XORing" the corresponding values resulted from the rotation with respective corresponding values resulted from "ANDing" operation at the current step along with operating on the highest polynomial term generated at the previous step in accordance with a generated polynomial. So, this excellent multiplication method used in Galois multiplication which provides designing of Galois encoder section, Which gives the security for the transmitted message signal as well as bandwidth usage is reduced .

The Multiplicand that denotes 4-bit or 8-bit of data is considered as the message signal. Galois algorithm is applied over the multiplicand by use the generator key irreducible polynomial. The 4-bit or 8-bit multiplier key respectively according to the design either of 4-bit or 8-bit. Mathematically two 4-bit numbers multiplication results in the 8- bit and two 8-bit multiplication results in16-bit but the Galois algorithm for multiplication will provide the result of 4- bit for two 4-bit numbers multiplications and 8-bit will give 8-bit results. Similarly, n-bit multiplications will give the results of n-bit as the multiplication results. Thus number of bits reduced. The flowchart given below for the Galois algorithm states the encoding schemes with the use of the shift and adds method. All the possible combination of 4-bits as well as 8-bits will cover by operands the result will be 4-bit and 8-bits respectively unlike the standard multiplications. The multiplicand represents the message signal while irreducible polynomial is considered as private key based on "NIST" based standard.

In this paper we are using the "NIST" polynomial $x4 + x + 1$ for 4-bit Galois encoder and $x8 + x4 + x3 + 1$ for 8-bit Galois encoder. Input B_i considered as the message bit, input A_i is consider as multiplier bit. Multiplicand along with the irreducible polynomial is fixed/static. As the operands are all loaded structure is able to multiply and operation of the 4-bit multiplier results as the MSB of the multiplier is under doing "AND" operation with static multiplicand bit and resultant is "XORed" with current result register, which should be start to 0. The result accumulates in "R" result when multiplier bits shifted. If 4th bit of R is a high i.e, 1 then current partial results in overflowing the 4-bit register value. So we have to subtract with the irreducible polynomial. So, each and every time after multiplication two conditions are checked on the multiplication result:

Rule I: Is the MSB of result is = 1? If yes then left shift the result else continue.

Rule II: Is the Result is having carry i.e. overflow? If yes then just subtract the result with "NIST" based Polynomial, else continue without subtracting with Polynomial.

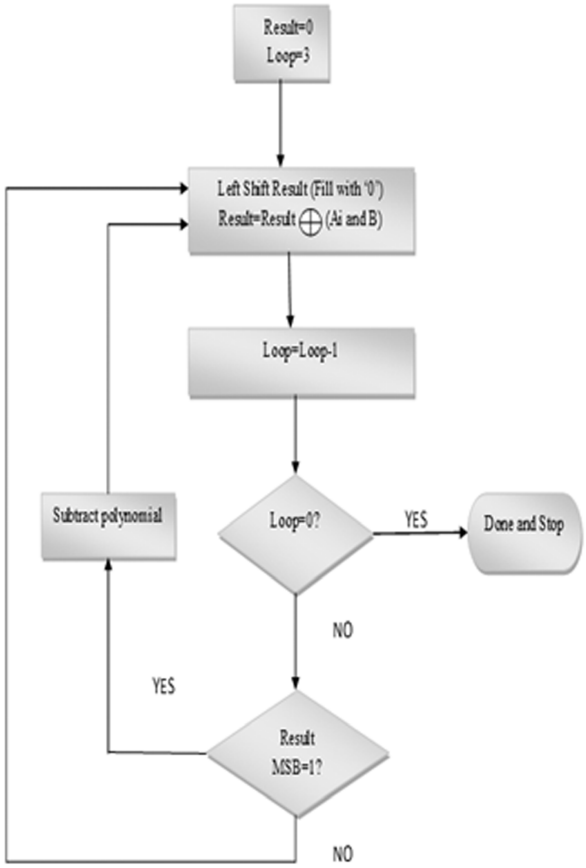

Figure 1: 4-bit Galois Encoder Algorithm

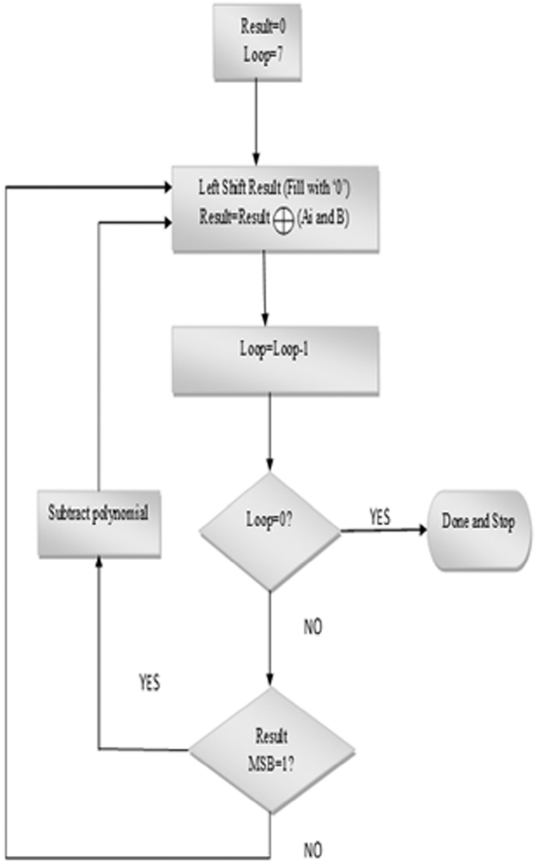

Figure 2: 8-bit Galois Encoder Algorithm

In case of 4-bit encoder loop will runs 3 times while in 8-bit encoder loop will run 7 times for multiplication of two numbers.

3. RESULTS AND ANALYSIS

For verification of logic we have taken the two number of 4 bit each and applying the algorithm to calculate the result and verified with industry standard CADENCE tools.

In the same way 8-bit Galois Encoder is designed using 8-bit Galois multiplier. All the steps followed for the 4-bit encoder will be followed again in case of 8-bit Galois Encoder design. For designing 8-bit Galois Encoder here we have used the "NIST" polynomial $x^8 + x^4 + x^3 + x + 1$.

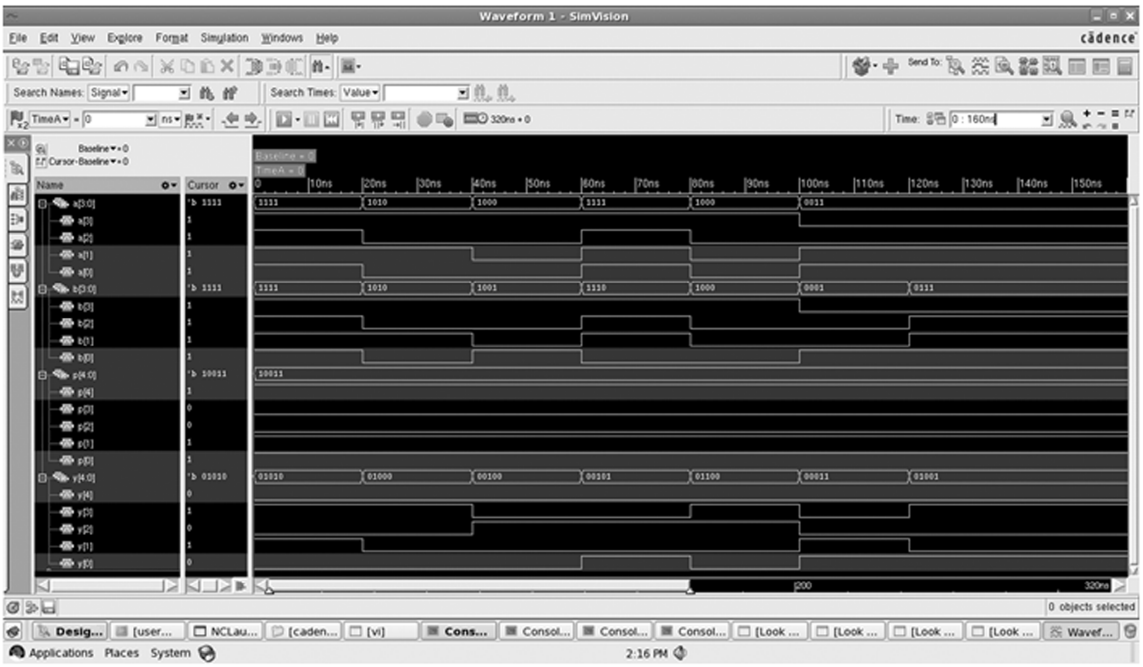

Figure 3: 4-bit Galois Encoder result using 4-bit Galois multiplication

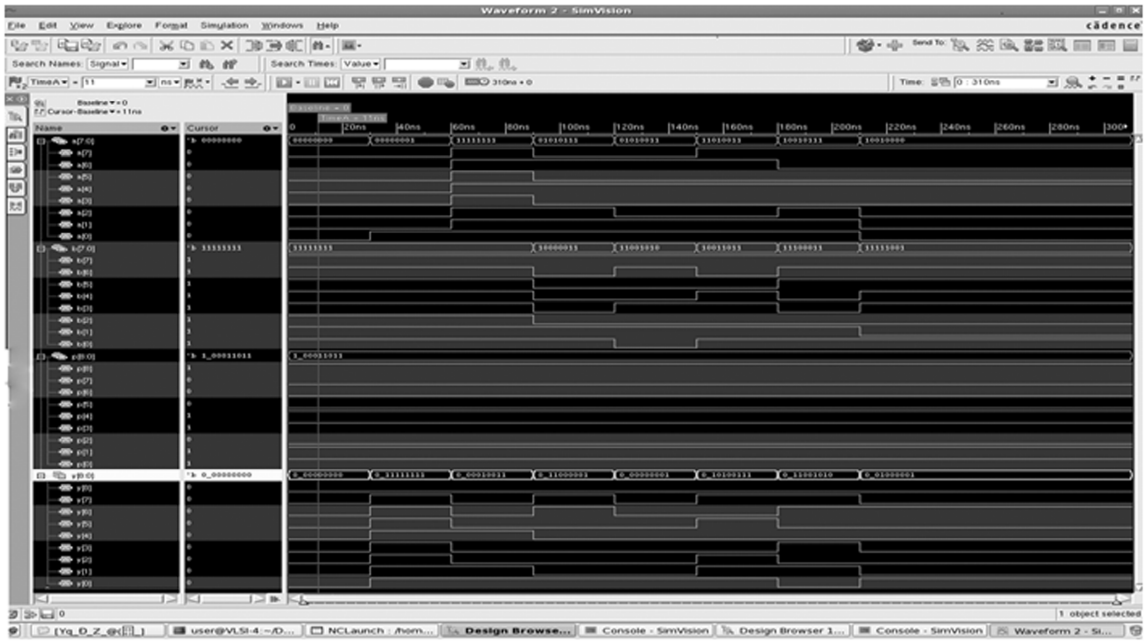

Figure 4: 8-bit Galois Encoder result using 8-bit Galois multiplication

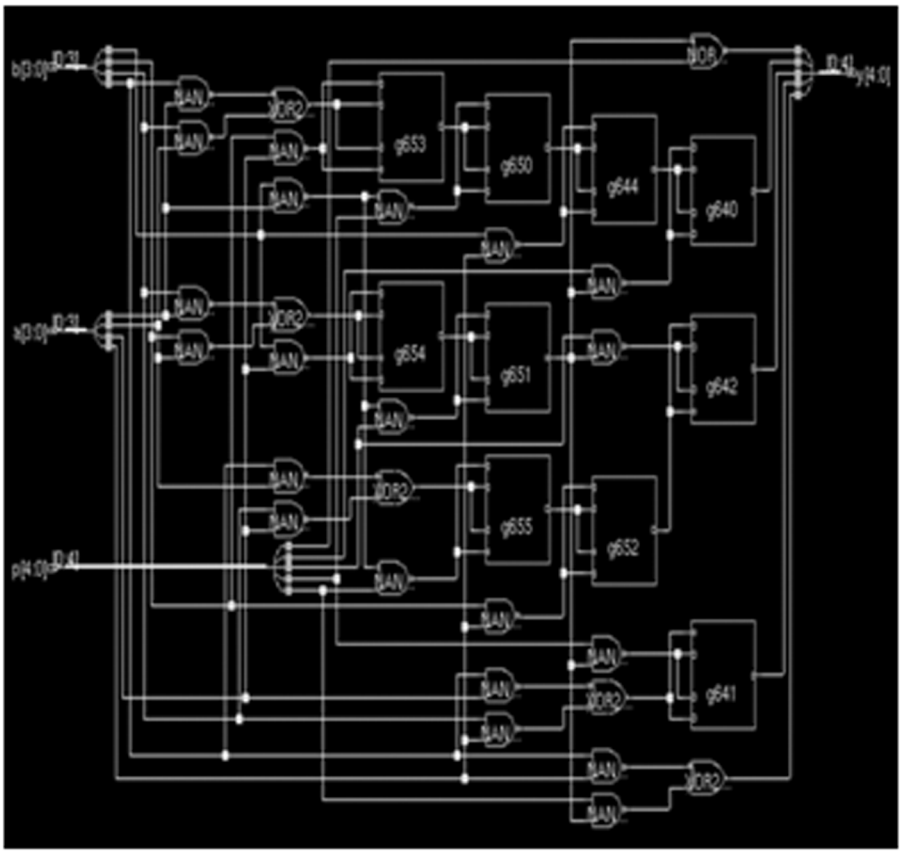

Figure 5: RTL view of 4-bit Galois Encoder

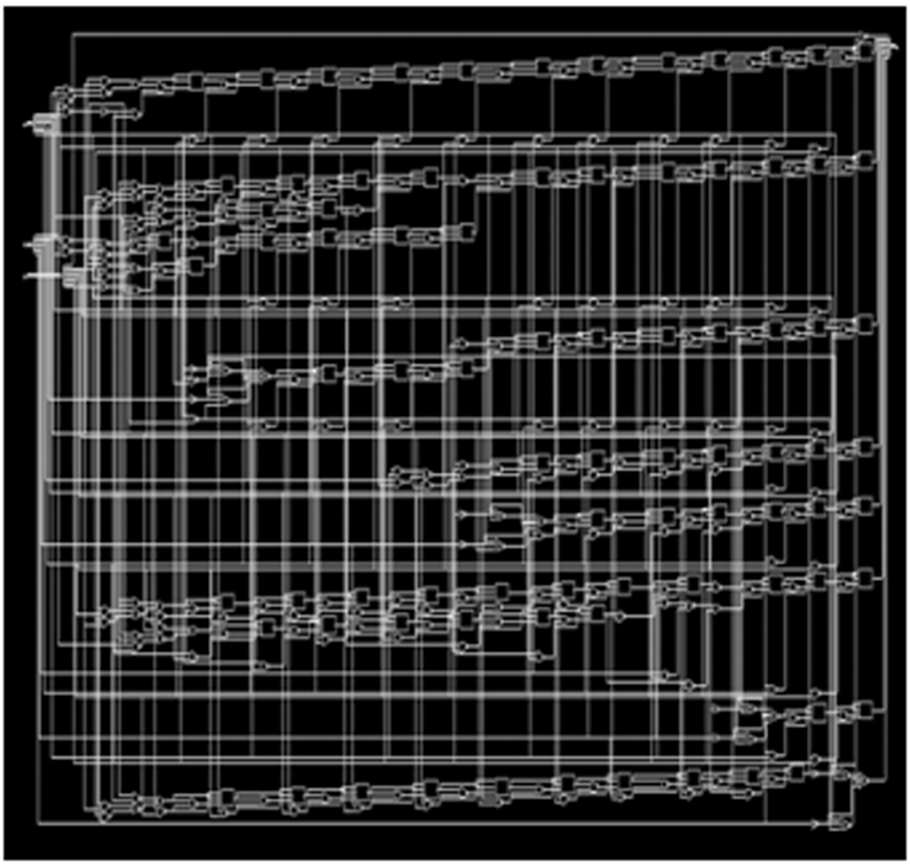

Figure 6: RTL view of 8-bit Galois Encoder

For verification of logic we have taken the two number of 8-bit each and applying the algorithm to calculate the result and verified with industry standard CADENCE tools.

3.1. Power Analysis

For power analysis we have taken supply voltages 1.1V for 90 nm technology.

```
====================================================================
  Generated by:           Encounter(R) RTL Compiler RC14.10 - v14.10-p008_1
  Generated on:           Apr 05 2016  06:46:11 pm
  Module:                 galoisfinal11
  Technology library:     fast
  Operating conditions:   fast (balanced_tree)
  Wireload mode:          enclosed
  Area mode:              timing library
====================================================================

                    Leakage   Dynamic    Total
   Instance   Cells Power(nW) Power(nW) Power(nW)
--------------------------------------------------
galoisfinal11    44  1923.586 13104.199 15027.785
```

Figure 7: 4-bit Galois encoder power synthesis report.

```
====================================================================
  Generated by:           Encounter(R) RTL Compiler RC14.10 - v14.10-p008_1
  Generated on:           Apr 05 2016  06:21:03 pm
  Module:                 galoism
  Technology library:     fast
  Operating conditions:   fast (balanced_tree)
  Wireload mode:          enclosed
  Area mode:              timing library
====================================================================

                 Leakage    Dynamic     Total
Instance Cells Power(nW)  Power(nW)  Power(nW)
-------------------------------------------------
galoism    321  9070.748 121720.116 130790.864
```

Figure 8: 8-bit Galois encoder power synthesis report

3.2. Delay Analysis

```
====================================================================
  Generated by:           Encounter(R) RTL Compiler RC14.10 - v14.10-p008_1
  Generated on:           Apr 05 2016  06:46:11 pm
  Module:                 galoisfinal11
  Technology library:     fast
  Operating conditions:   fast (balanced_tree)
  Wireload mode:          enclosed
  Area mode:              timing library
====================================================================

 Pin        Type      Fanout  Load  Slew  Delay  Arrival
                      (fF)    (ps)  (ps)   (ps)
--------------------------------------------------------
a[2]       in port        3   5.1     0     +0        0 F
g672/A                                    +0        0
g672/Y     NAND2XL        1   1.9    14    +13       13 R
g666/A                                    +0       13
g666/Y     XNOR2X1        1   3.7    18    +59       72 F
g662/B                                    +0       72
g662/Y     XNOR2X1        2   3.5    18    +54      126 R
g658/A                                    +0      126
g658/Y     NAND2XL        1   1.8    22    +15      142 F
g655/B0                                   +0      142
g655/Y     OAI21XL        5   8.6    89    +44      185 R
g648/A                                    +0      185
g648/Y     NAND2XL        1   3.8    39    +27      212 F
g644/B                                    +0      212
g644/Y     XOR2XL         1   0.0     8    +40      252 R
y[0]       out port                     +0      252 R
--------------------------------------------------------
Timing slack :  UNCONSTRAINED
Start-point  : a[2]
End-point    : y[0]
```

Figure 9: 4-bit Galois encoder Delay synthesis report.

```
====================================================================
  Generated by:           Encounter(R) RTL Compiler RC14.10 - v14.1
  Generated on:           Apr 05 2016  06:31:03 pm
  Module:                 galoism
  Technology library:     fast
  Operating conditions:   fast (balanced_tree)
  Wireload mode:          enclosed
  Area mode:              timing library
====================================================================

 Pin        Type      Fanout  Load  Slew  Delay  Arrival
                      (fF)    (ps)  (ps)   (ps)
--------------------------------------------------------
a[6]       in port        8  13.6     0     +0        0 F
g6026/A                                   +0        0
g6026/Y    NAND2XL        1   1.9    14    +13       13 R
g5982/A                                   +0       13
g5982/Y    XNOR2X1        2   3.5    18    +58       71 F
g5966/A1                                  +0       71
g5966/Y    OAI21XL        8  13.6   132   +101      172 R
g5933/A                                   +0      172
g5953/Y    NAND2XL        2   3.5    46    +25      196 F
g5931/A0                                  +0      196
g5931/Y    OAI21XL        8  13.6   132   +108      304 R
g5926/A                                   +0      304
g5926/Y    NAND2XL        2   3.5    46    +25      329 F
g5897/A0                                  +0      329
g5897/Y    OAI21XL        8  13.6   132   +108      437 R
g5885/A                                   +0      437
g5885/Y    NAND2XL        2   3.5    46    +25      462 F
g5838/A0                                  +0      462
g5858/Y    OAI21XL        8  13.6   132   +108      570 R
g5847/A                                   +0      570
g5847/Y    NAND2XL        2   3.5    46    +25      595 F
g5834/A0                                  +0      595
g5824/Y    OAI21XL        8  13.6   132   +108      707 R
g5806/A                                   +0      707
g5806/Y    NAND2XL        2   3.5    46    +25      732 F
g5786/A0                                  +0      732
g5786/Y    OAI21XL        8  13.6   132   +108      841 R
g5765/A                                   +0      841
g5765/Y    INVXL          3   5.2    50    +23      863 F
g5760/A1                                  +0      863
g5760/Y    AOI21XL        1   1.6    27    +33      897 R
g5749/A0                                  +0      897
g5749/Y    OAI22XL        1   0.0    19    +17      914 F
y[0]       out port                     +0      914 F
--------------------------------------------------------
Timing slack :  UNCONSTRAINED
Start-point  : a[6]
End-point    : y[0]
```

Figure 10: 8-bit Galois encoder Delay synthesis report.

3.3. Performance Evaluation

So, from the above table and graphs it is clear that 4-bit Galois encoder has less leakage power than that of 8-bit Galois power.Number of cells used, Dynamic power as well as Total power is also less for the 4-bit Galois encoder than that of 8-bit Galois encoder.

Table 1
Power and Delay Analysis of 4-bit and 8-bit Galois Encoder.

Parameters	*4-Bit Galois Encoder*	*8-Bit Galois Encoder*
Cells Used	44	321
Leakage Power(nW)	1923.586	9070.784
Dynamic Power(nW)	13104.199	121720.116
Total Power(nW)	15027.785	130790.864
Total Delay(ps)	252	914

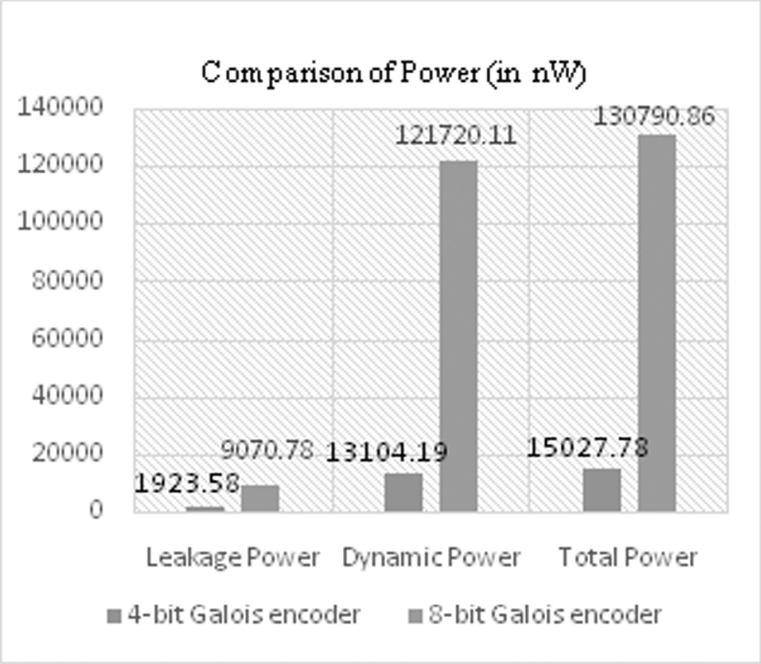

Figure 11: Graph for Comparison of Power (in nW)

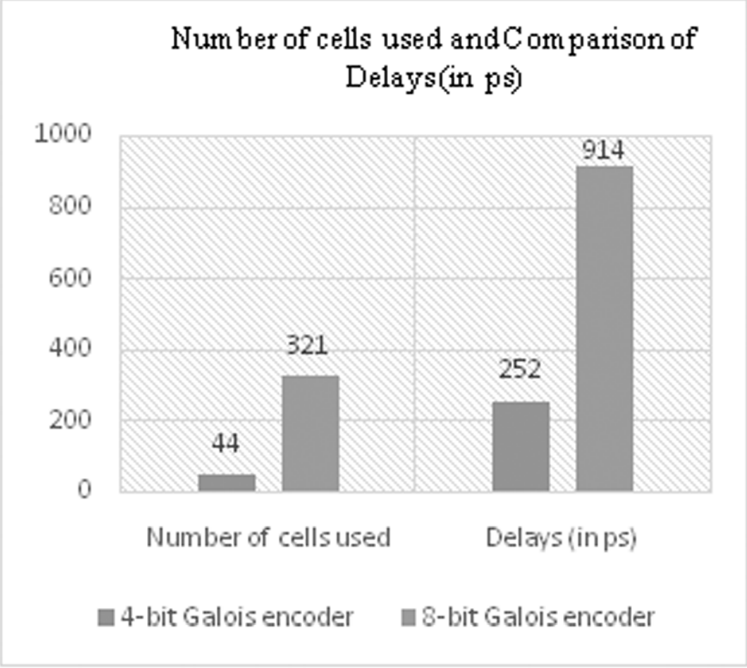

Figure 12: Graph for Cells used and Delays (in ps)

4. CONCLUSION

After designing and analysis of 4-bit and 8 bit Galois encoder logic for 90nm technology,we are getting the optimized results for4-bit Galois encoder in terms of Cells i.e. 44 cells for 4-bit while 321 cell for 8-bit. Total Power 15027.785 nW for 4-bit while 130790.864 nW for 8-bit, and Delay is 252 ps while 914 ps for 8-bit Galois encoder. Considering the delay analysis we found that 4-bit Galois encoder is having less delay as compared to 8-bit Galois encoder. So, 4-bit Galois encoder is more than 3 times faster than the 8-bit Galois encoder.

REFERENCES

[1] Sajid Parvez Ansari, Prof. Namrata Sahyam, "A methodology to hide information using image steganography with Galois Field" *International journal of Engineering Research Online (IJOER)*, Volume 3, Issue.6, Nov.-Dec.-2015.

[2] Ajitha S.S., Retheesh D., "Efficient implementation of bit parallel finite field multipliers" *International journal of Research in Engineering and Technology (IJERT),* Volume: 03, Issue: 03, March-2014.

[3] Dr. Ravi Shankar Mishra, Prof. Puran Gour, and Mohd. Abdullah, "Design and Implementation of 4-bit Galois encoder and decoder on FPGA" *International journal of Engineering Science and Technology (IJEST),* ISSN: 0975-5462, Volume: 03, 7th July-2011.

[4] Naofumi Homma, Kazuya Saito, and Takafumi Aoki, "Formal design of multiple-valued arithmetic algorithms over Galois Fields and its application to cryptographic processor" *IEEE 42nd International Symposium on multiple-valued logic (ISMVL),* 2012.

[5] Dr. Rita Jain, Priya Jain, and Tarun Verma, "Comparison and implementation of cryptography algorithm by using VHDL" International journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN 2250-2459, Volume: 02, Issue: 11, November-2012.

[6] Ankita.N. Sakhare, M.L.Keote, "Application of Galois Field inVLSI using Multi-Valued logic" *International journal of Engineering Science and Innovative Technology (IJESIT),* Volume: 02, Issue: 01, January-2013.

[7] Thomas Conway, Member,IEEE, "Galois Field Arithmetic Over $GF(p^M)$ For High-Speed/Low-Power Error-Control Applications" *IEEE transactions on circuit and systems-I: regular papers,* Volume: 51, and NO.4, APRIL 2004.

[8] Avinash Mahule and Shrikant Bhoyar, "Implementation of Galois Field Multiplier using one Hot Encoding Technique" *Advance in Electronic and Electric Engineering*, ISSN 2231-1297,Volume 4, Number 5 (2014), pp. 437-440, © Research India Publications.

[9] M. Uma Maheswari, S.Baskar, G.M.Keerthi, "High speed finite field multiplier $GF(2^M)$ for cryptographic applications" *International journals of advanced Research in Electronics and Communication Engineering (IJARECE),* Volume: 03, Issue: 11, November 2014.