Architecture for Programmable Generator Polynomial Based Reed-Solomon Encoder and Decoder

Jaydeb Bhaumik, Anindya Sundar Das and Jagannath Samanta

***Abstract*—Reed-Solomon Codes are popularly used for error correction in many applications like storage devices (CD, DVD), wireless communications, high speed modems and satellite communications. In this paper, a modified scheme for programmable generator polynomial based Reed-Solomon encoder and decoder has been proposed. The works reported in this paper corrects errors in derived equations and decoder architecture proposed by Shayan et al. Moreover, modified architectures for programmable generator polynomial based Reed-Solomon encoder and decoder are reported.**

***Index Terms*— Reed-Solomon Code, Finite Field, Encoder and Decoder Architectures**

I. INTRODUCTION

Reed-Solomon (RS) code was discovered by Irving Reed and Gus Solomon in 1960[1]. It is a linear block code and defined over finite field. RS code has a wide range of applications in wireless communications, high speed modems and storage devices (CD, DVD). Several important applications of RS codes have been discussed in [10]. A number of general encoding and decoding schemes of the RS codes may be found in the literature [11] [12]. The complexity of RS encoder and decoder increases with the error correcting capability of the codes. Hence, many researchers have directed their efforts to minimize the complexity of RS decoder. A high-speed architecture for Reed-Solomon decoders is proposed in [9]. VLSI design of a reconfigurable multi-mode Reed-Solomon codec for high speed communication systems with programmable codeword length and error correcting capability has been proposed in [5]. Most of the existing programmable RS codec have programmable codeword length and error correcting capability. Beside the application of RS code for error correction, it has applications in the design of diffusion layer for a substitution permutation networks type block cipher [10], secret sharing scheme, message authentication codes [7][8].

In [2], RS code has been used to design integrated code for both message authentication and error correction. In this scheme programmable generator polynomial based RS-code is employed but no architecture for the proposed scheme is mentioned in [2]. Decoding of Reed-Solomom code generated by any generator polynomial discussed in [3].

A versatile time-domain Reed-Solomon decoder is proposed in [4]. A method was also presented to decode an **RS** code generated by any generator polynomial. But for the proof design equations [3] is referred. But there are mistakes in the derived equation in [3].

In this paper, an improved scheme for programmable generator polynomial based RS encoder and decoder has been proposed. Present work rectifies the errors in the derived equations proposed in [3]. Also architectures for programmable encoder and decoder have been introduced. Programmable generator polynomial based encoder may be employed for error correction and to provide security in communication systems.

Rest of the paper is organized as follows. Section II presents basics of Reed-Solomon encoder and decoder. Principle of programmable generator polynomial based RS encoder and decoder is discussed in Section III. In section IV, architecture for programmable encoder and decoder is proposed. Programmable generator polynomial based shortened RS codec is discussed in Section V and finally the paper is concluded in Section VI.

II. BASICS OF REED-SOLOMON ENCODER AND DECODER

A brief description of RS encoder and decoder are provided in this section.

A. Encoder

The RS encoder takes a block of symbols and appends extra parity check symbols. The number and types of errors that can be corrected depends on the characteristics of the RS code. Parameters RS (n, k) code defined over GF(2^m) are as follows.

m is the number of bits per symbol
k is the un-coded data length in symbols
n is the codeword length in symbols, where $n = 2^m – 1$
n – k is the number of parity check symbols, where $(n−k) = 2t$ t is the error correction capability of the code.

Figure 1 shows the block diagram of a typical systematic Reed-Solomon encoder.

B. Decoder

The decoder processes each block and attempts to correct the errors which may occur during transmission or storage.

Manuscript received on January, 2013.
Jaydeb Bhaumik, Haldia Institute of Technology, Haldia, India.
Anindya Sundar Das, Haldia Institute of Technology, Haldia, India.
Jagannath Samanta, Haldia Institute of Technology, Haldia, India.

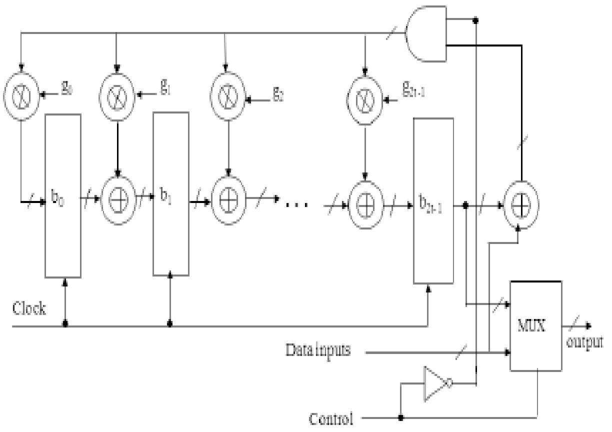

Fig. 1: Reed-Solomon Encoder

RS decoder consists of five sub-blocks namely syndrome generator, key equation solver, error location identification, error magnitude computation and error correction. The key equation solver is the most complex part in the RS decoder. Mainly three different algorithms are used for the key equation solver of RS decoder. The algorithms are Berlekamp-Massey (BM) algorithm, Euclid algorithm and Peterson-Gorenstein-Zierler (PGZ) algorithm. Figure 2 shows the block diagram of RS decoder.

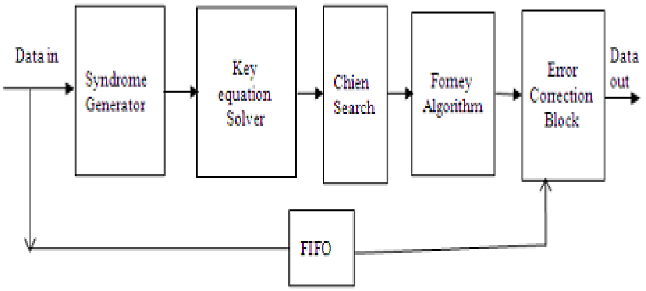

Fig. 2: Reed-Solomon Decoder

III. RELATIONSHIP BETWEEN RS CODES GENERATED BY DIFFERENT POLYNOMIALS

A Reed-Solomon (RS) code with block length n and number of information symbols k defined over GF(2^m), can be generated by any one of the (2^m-1) different generator polynomials is as $\tilde{g}(x)$follows.

$$\tilde{g}(x) = \prod_{i=0}^{n-k-1} (x + \alpha^{(h+i)}) \qquad (1)$$

where m is the size of each element in GF(2^m), α is the primitive element of the Galois field (2^m) and the constant h can be chosen to have values 0, 1, 2,… (n-1) .
For h=1, equation (1) becomes

$$g(x) = \prod_{i=0}^{n-k-1} (x + \alpha^{(1+i)}) \qquad (2)$$

The relation between $\tilde{g}(x)$and g(x) is as follows

$$\tilde{g}(x) = \alpha^{(n-k)(h-1)} g(\alpha^{-(h-1)}x) \qquad (3)$$

RS codes generated by g(x) and $\tilde{g}(x)$ is compared here and relationship between c(x) and $\tilde{c}(x)$ is found. Assume d(x) is the message polynomial, g(x) is the generator polynomial, and p(x) is its parity check polynomial. Then from the construction of systematic RS (n, k) code, we can write

$$x^{(n-k)} d(x) = g(x)q(x) + p(x) \qquad (4)$$

where q(x) is a quotient polynomial. The codeword polynomial for d(x) can be formed as

$$c(x) = d(x) + x^k p(x) \qquad (5)$$

Similarly, if $\tilde{d}(x)$ is the massage polynomial, $\tilde{g}(x)$ is generator polynomial, and $\tilde{p}(x)$ is the parity check polynomial, then

$$x^{(n-k)} \tilde{d}(x) = \tilde{g}(x)\tilde{q}(x) + \tilde{p}(x) \qquad (6)$$

where $\tilde{q}(x)$ is a quotient polynomial. Corresponding code word polynomial is

$$\tilde{c}(x) = \tilde{d}(x) + x^k \tilde{p}(x) \qquad (7)$$

To find the relationship between p(x) and $\tilde{p}(x)$, it is assumed that

$$\tilde{d}(x) = d(\alpha^{-(h-1)}x)$$
$$or \quad d(x) = \tilde{d}(\alpha^{(h-1)}x) \qquad (8)$$

Substituting the values of $\tilde{g}(x)$ and $\tilde{d}(x)$ from (3) and (8) into (6), we get

$$x^{(n-k)} d(\alpha^{-(h-1)}x) = \alpha^{(n-k)(h-1)} g(\alpha^{-(h-1)}x)\tilde{q}(x) + \tilde{p}(x) \qquad (9)$$

Changing the variable x to $\alpha^{(h-1)}x$ and dividing both sides of (9) by $\alpha^{(n-k)(h-1)}$ yields

$$x^{(n-k)}d(x) = g(x)\tilde{q}(\alpha^{(h-1)}x) + \alpha^{-(n-k)(h-1)}\tilde{p}(\alpha^{(h-1)})\, x \qquad (10)$$

Comparing (4) and (10) it is noted that degrees of p(x) and $\tilde{p}(x)$ are respectively lower than q(x) and $\tilde{q}(x)$, we can conclude that

$$p(x) = \alpha^{-(n-k)(h-1)}\tilde{p}(\alpha^{(h-1)}x) \qquad (11)$$

Now c(x) can be evaluated using (5), (8) and (11). Since in a field of order n, the n^{th} power of any element of the field is 1, therefore $\alpha^{-n(h-1)} = 1$ and right-hand side of (11) becomes

$$p(x) = \alpha^{k(h-1)}\tilde{p}(\alpha^{(h-1)}x) \qquad (12)$$

Change of variable x to $\alpha^{(h-1)}x$ in (7) yields

$$\tilde{c}(\alpha^{(h-1)}x) = \tilde{d}(\alpha^{(h-1)}x) + x^k\alpha^{k(h-1)}\tilde{p}(\alpha^{(h-1)}x) \qquad (13)$$

After simplification equation (13) can be written as

$$\tilde{c}\left(\alpha^{(h-1)}x\right) = d(x) + x^k p(x) \qquad (14)$$

Comparing (5) and (14), relationship between c(x) and $\tilde{c}(x)$ is obtained

$$c(x) = \tilde{c}(\alpha^{(h-1)}x)$$
$$\tilde{c}(x) = c\left(\alpha^{-(h-1)}x\right) \qquad (15)$$

IV. ARCHITECTURE FOR PROGRAMMABLE ENCODER AND DECODER

In this section, architecture for programmable generator polynomial based RS encoder and decoder have been discussed.

A. *Architecture for Encoder*

Programmable generator polynomial based Reed-Solomon encoder is shown in Fig. 3. The basic encoder is based on the generator polynomial g(x). Programmable encoder requires extra four multipliers over GF(2^m), and two m bits registers.

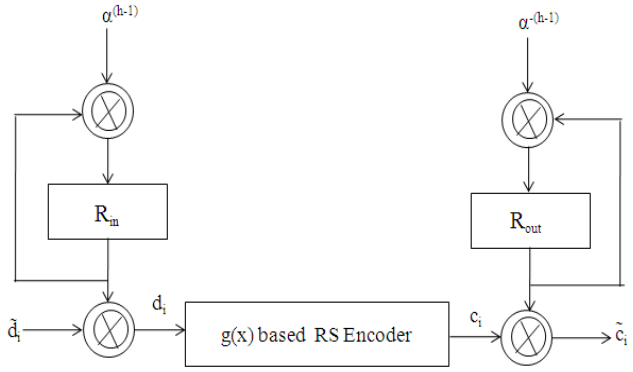

Fig. 3: Programmable Generator Polynomial Based Reed-Solomon Encoder

$$d_j = \tilde{d}_j\, \alpha^{j(h-1)}, \text{where } j = 0, 1, 2, \ldots (k-1) \qquad (16)$$
$$\tilde{c}_i = c_i\, \alpha^{-i(h-1)}, \text{where } i = 0, 1, 2, \ldots (n-1) \qquad (17)$$

In these equations, $d_j, \tilde{d}_j, c_i, \tilde{c}_i$ are coefficients of the corresponding polynomials in (8) and (15).

In the encoder $\tilde{d}_0$ is the first and $\tilde{d}_{k-1}$ is the last information symbol. The encoder first transmits k number of information symbols and after that n-k parity symbols. To generate $\alpha^{i(h-1)}$ the m bit register R_{in} is initialized to α^0 =1, when the first symbol $\tilde{d}_0$ is fed. By feeding the next symbol $\tilde{d}_1$ the register R_{in} is clocked and the new value in the register $\alpha^{(h-1)}$ is multiplied by $\tilde{d}_1$ to form d_1. This procedure goes on for remaining information symbols. The circuitry for generating the output of the encoder is similar to the input circuitry. In this circuitry the register R_{out} is clocked when outputting a symbol from the encoder.

Consider an RS (7, 5) Code over GF(2^3) with primitive polynomial $m(x) = x^3 + x + 1$. Assume the five message symbols are (1, 1, 1, 1, α^2).

The corresponding message polynomial is as follows.

$$\tilde{d}(x) = x^4 + x^3 + x^2 + x + \alpha^2 \qquad (18)$$

So

$$x^2\tilde{d}(x) = x^6 + x^5 + x^4 + x^3 + x^2\alpha^2 \quad (19)$$

Consider the generator polynomial

$$\tilde{g}\,(x) = x^2 + (\alpha^2 + \alpha^3)\,x + \alpha^5 \qquad (20)$$

The corresponding parity check polynomial is

$$\tilde{p}(x) = (\alpha^{15} + \alpha^{14} + \alpha^{13} + \alpha^7)x + (\alpha^{17} + \alpha^{16} + \alpha15{+}\alpha12{+}\alpha10{+}\alpha9{+}\alpha8 \qquad (21)$$

Simplifying equation (21) by employing the primitive polynomial m(x), we get

$$\tilde{p}(x) = \alpha^5 x + \alpha^5 \qquad (22)$$

Therefore, the codeword polynomial $\tilde{c}(x)$ is

$$\tilde{c}(x) = x^5\tilde{p}(x) + \tilde{d}(x) = \alpha^5x^6 + \alpha^5x^5 + x^4 + x^3 + x^2 + x + \alpha^2 \qquad (23)$$

Since$d_j = \tilde{d}_j\, \alpha^j$, therefore we can write

$$d(x) = \alpha^4x^4 + \alpha^3x^3 + \alpha^2x^2 + \alpha x + \alpha^2 \quad (24)$$

Therefore

$$x^2d(x) = \alpha^4x^6 + \alpha^3x^5 + \alpha^2x^4 + \alpha^1x^3 + \alpha^2x^2 \quad (25)$$

Since generator polynomial

$$g(x) = x^2 + (\alpha^1 + \alpha^2)x + \alpha^3 \qquad (26)$$

Therefore corresponding parity check polynomial is as follows.

$$p(x) = (\alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^6)x \; + (\alpha^{15} + \alpha^{14} + \alpha13{+}\alpha10{+}\alpha8{+}\alpha7{+}\alpha6 \qquad (27)$$

Equation (27) can be simplified by employing primitive polynomial m(x).

$$p(x) = \alpha^4 x + \alpha^3 \qquad (28)$$

Therefore, the codeword polynomial c(x) is

$$c(x) = x^5p(x) + d(x)$$
$$= \alpha^4x^6 + \alpha^3x^5 + \alpha^4x^4 + \alpha^3x^3 + \alpha^2x^2 + \alpha x + \alpha^2 \qquad (29)$$

From equations (23) and (29), it can be shown that

$$\tilde{c}(\alpha x) = c(x)$$

B. *Architecture for Decoder*

Modified RS decoder architecture with programmable generator polynomial is shown in Fig. 4. The basic decoder is based on the generator polynomial g(x). Programmable decoder requires extra four multipliers over GF(2^m), and two registers besides the decoder based on generator polynomial g(x). Assume the error vector e_i is as follows

$$e_i = \tilde{e}_i\alpha^{i(h-1)} \qquad (30)$$

Let ri be the received codeword vector. It has two component ci and ei, where

$$r_i = c_i + e_i \qquad (31)$$

A new vector $\tilde{r}$i has the same number of errors as ri, where

$$r_i = \tilde{r}_i\alpha^{i(h-1)}$$

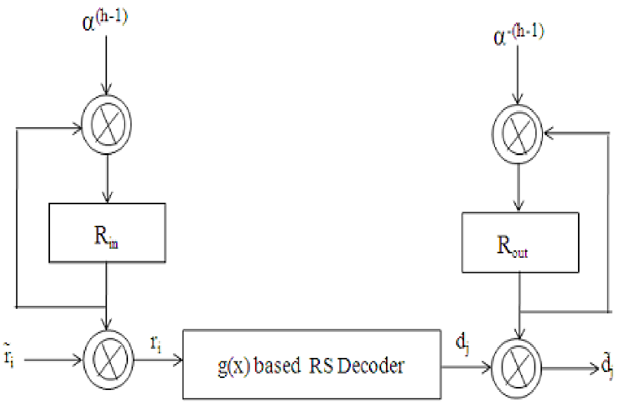

Fig. 4: Programmable Generator Polynomial Based Reed-Solomon Decoder

In the decoder, symbol $\tilde{r}_0$ is received first and the symbol $\tilde{r}_{n-1}$ last. In decoder to generate $\alpha^{i(h-1)}$ the m bit register R_{in} is initialized to α^0 =1 when the first symbol $\tilde{r}_0$ is received. By receiving the next symbol $\tilde{r}_1$ the register R_{in} is clocked and the new value in the register $\alpha^{(h-1)}$ is multiplied by $\tilde{r}_1$ to form r_1. This procedure goes on for remaining received symbols. . The circuitry for generating the output of the decoder is similar to the input circuitry. In this circuitry the register R_{out} is clocked when outputting a symbol from the decoder.

V. PROGRAMMABLE SHORTENED RS CODEC

An (*n*, *k*) linear code can be shortened to an (*n-i*, *k-i*) code by setting the first *i* information bits to zero. Generator matrix for shortened RS code can be constructed by omitting *i* rows and *i* columns from the generator matrix **G** of (n, k) code. Similarly, the parity-check matrix for shortened RS code can be constructed by omitting *i* columns from the generator matrix **H** of (n, k) code. For a shortened RS code equation (11) is satisfied but equation (15) is not applicable.

Consider an RS (6, 4) Code over GF(2^3) with primitive polynomial $m(x) = x^3 + x + 1$. Assume the five message symbols are (1, 1, 1, 1).

The corresponding message polynomial is as follows.

$$\tilde{d}(x) = x^3 + x^2 + x + 1 \qquad (32)$$

So

$$x^2\tilde{d}(x) = x^5 + x^4 + x^3 + x^2 \qquad (33)$$

Consider the generator polynomial

$$\tilde{g}\,(x) = x^2 + (\alpha^2 + \alpha^3)\,x + \alpha^5 \qquad (34)$$

The corresponding parity check polynomial is

$$\tilde{p}(x) = (\alpha^{12} + \alpha^{11} + \alpha^{10} + \alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2)x + (\alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^{10} + \alpha^9 + \alpha^8 + \alpha^7 + \alpha^5) \qquad (35)$$

Simplifying equation (35) by employing the primitive polynomial m(x), we get

$$\tilde{p}(x) = \alpha^6 x \qquad (36)$$

Employing equation (8), d(x) can be written as

$$d(x) = \alpha^3x^3 + \alpha^2x^2 + \alpha x + 1 \qquad (37)$$

Therefore

$$x^2d(x) = \alpha^3x^5 + \alpha^2x^4 + \alpha^1x^3 + x^2 \qquad (38)$$

Since generator polynomial

$$g(x) = x^2 + (\alpha^1 + \alpha^2)x + \alpha^3 \qquad (39)$$

Therefore corresponding parity check polynomial is as follows.

$$p(x) = (\alpha^{11} + \alpha^{10} + \alpha^9 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha x + \alpha 12 + \alpha 11 + \alpha 10 + \alpha 8 + \alpha 7 + \alpha 6 + \alpha 5 + \alpha 3 \qquad (40)$$

Equation (40) can be simplified by employing primitive polynomial m(x).

$$p(x) = \alpha^5 x \qquad (41)$$

From equations (36) and (41), it is observed that

$$p(x) = \alpha^{-2}\,\tilde{p}(\alpha x) \qquad (42)$$

For a shortened programmable generator polynomial based RS encoder $\tilde{p}(x)$ is computed from $p(x)$ employing equation (11). And then $\tilde{p}(x)$ is appended with $\tilde{d}(x)$ to compute $\tilde{c}(x)$. In a decoder p(x) is computed from $\tilde{p}(x)$ and d(x) from $\tilde{d}(x)$ and they are fed at the input of g(x) based RS decoder to detect and correct errors. These modifications are required in architectures because equation (12) is not valid for shortened RS code.

VI. CONCLUSION

In this paper, architectures for programmable generator polynomial based RS encoder and decoder have been proposed. It rectifies the errors in Shayan et al. scheme and introduces modified architectures for programmable RS encoder and decoder. Programmable generator polynomial based RS encoder and decoder can be used in communication systems for both error correction and message authentication.

REFERENCES

[1] I. Reed and G. Solomon, "Polynomial codes over certain finite fields,"*Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, Jun 1960, pp. 300-304.

[2] J. Bhaumik and D. Roy Chowdhury, "An Integrated ECC-MAC Basedon RS Code," *Transactions on Computational Science*, vol. IV, LNCS5430, Apr. 2009, pp. 117-135.

[3] Y. R. Shayan and T. Le-Ngoc, "Decoding Reed- Solomon codes generated by any generator polynomial," Electronics Letters, vol. 25, no. 18, Aug. 1989, pp. 1223-1224.

[4] Y. R. Shayan, T. Le-Ngoc and V. K. Bhargava, "A versatile time-domain Reed-Solomon decoder," IEEE Journal on Selected Areas in Communications archive, Vol. 8 no. 8, Sept. 2006, pp. 1535-1542.

[5] H. Y. Hsu and A. Y. Wu, "VLSI Design of a Reconfigurable Multimode Reed-Solomon Codec for High Speed Communication Systems," in *IEEE Asia-Pacific Conference on ASIC*, 2002, pp. 359-362

[6] S. B. Wicker and V. K. Bhargava, *Reed Solomon Codes and Their Applications*. IEEE Press, 1994.

[7] H. Krawczyk, "LFSR-based hashing and authentication," in *Proc. Advances in Cryptology-CRYPTO*, 1994, vol. LNCS 0839, pp. 129-139.

[8] C. C. Y. Lam, G. Gong and S. Vanstone, "Message authentication codes with error correcting capabilities," in *4th Int. Conf. on Information and Communications Security*, 2002, vol. LNCS 2513, pp. 354-366

[9] D. V. Sarawate and N. R. Shanbhag, "High-speed architectures for Reed- Solomon decoders," *IEEE Trans. on VLSI Systems*, vol. 9, no. 5, Oct. 2001, pp. 641-655.

[10] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers and E. De Win, "The cipher SHARK," in *Fast Software Encryption*, 1996, vol. LNCS 1039, pp. 99-111.

[11] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.

[12] R. E. Blahut, *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.

Dr. Jaydeb Bhaumik is currently working as an Associate Professor in the Department of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, India. He obtained his PhD degree from G. S. Sanyal School of Telecommunications, Indian Institute of Technology Kharagpur, India in 2010. He received his B. Tech. and M. Tech. degrees in Radio Physics and Electronics from University of Calcutta in 1999 and 2001 respectively. His research interests include Cryptography, Cellular Automata, Error Correcting Codes, and Digital VLSI Design. He is a member of IEEE and Cryptology Research Society of India..

Mr. Anindya Sundar Das is currently working as a JRF at Haldia Institute of Technology. He did his M. Tech in Electronics and Communication Engineering (specialization in Micro Electronics and VLSI Design) under West Bengal University of Technology in the year 2012. He obtained his B. Tech degree from Uttar Pradesh Technical University in the year of 2006 in Electronics and Instrumentation Engineering. His area of research area includes Error control coding, Optical communication and VLSI design.

Mr. Jagannath Samanta has received his Bachelors Degree B.Tech in Electronics and Communication Engineering under West Bengal University of Technology, Kolkata, West Bengal, in the year 2005, and achieved his Master's Degree M.Tech in Embedded System under West Bengal University of Technology, Kolkata, West Bengal, in year 2008. He has awarded Gold Medal in Master's Degree. His research interest in Digital VLSI Design, Error Correction Code, Network-on-chip (NOC) Design etc. Presently Mr. Samanta is serving as Assistant Professor in the Department of Electronics and communication Engineering, Haldia Institute of Technology, Haldia, West Bengal, India. He has more than 8 international publications.