# Performance Comparison of New Designs of Chien Search and Syndrome Blocks for Bch and Reed Solomon Codes 

Mohamed Elghayyaty ${ }^{1}$, Omar Mouhib ${ }^{1}$, Azeddine Wahbi ${ }^{2}$, Ahmed Amine Barakate ${ }^{1}$, Anas El Habti El Idrissi ${ }^{1}$, Laamari Hlou ${ }^{1}$ and Abdelkader Hadjoudja ${ }^{1}$<br>${ }^{1}$ Laboratory of Electrical Engineering and Energy System, Faculty of Sciences, University Ibn Tofail, Kenitra, Morocco<br>${ }^{2}$ Laboratory of Industrial Engineering, data processing and logistic, Faculty of sciences Ain Chock, University Hassan II, Casablanca, Morocco


#### Abstract

Error correcting codes constitute one of the core technologies in telecommunications field, especially digital communication applications. The objective of this paper is to compare performance among new designs of chien search block on the one hand and syndrome architectures on the other hand in error correcting codes. All comparison of all designs is made by computing the number of logic, bit error rate values and number of iteration in the case of syndrome architectures Analysis results show that the performances of the new designs based on both second factorization method and Three-Parallel Syndrome architecture are superior to the performances of traditional designs.


Keywords: Error Correcting Codes, Error Locator Polynomial, Chien Search Block, Syndrome Computation Block, Bit Error Rate (BER).

## 1. Introduction

The quality of a digital transmission depends mainly on the quantity of errors introduced into the transmission channel [1] [2]. Error checking by coding is therefore essential. The use of digital signal processing techniques, and in particular the coding of the information to be transmitted, allows the detection and correction of transmission errors [3] [4]. As these techniques make it possible to control the errors induced by the noise of the transmission channel, they are called "channel coding". Among the main techniques used, block coding and convolution coding are predominant. Blocks coding are used in particular in Ethernet networks, in wireless transmission standards such as Bluetooth, and in HDTV (High Definition Television) and DVB-C (Digital Video Broadcasting-Cable) transmission standards. Convolution coding is very common in digital wireless communication systems [5] [6] [7] and other codes like RS (Reed-Solomon), and BCH (Bose, Ray-Chaudhuri) [8].
The Reed Solomon codes are block and not binary codes where the message is divided into blocks to which is added redundant information. The length of the blocks depends on the capacity of this code. For each block on the addition of protection bits or of the additional parity for the old code, a word of $n$ symbols. It is also a systematic code, i.e. the control symbols are added at the end of the information. The coder takes K data symbols and calculates the control information to construct n symbols, which gives $\mathrm{n}-\mathrm{k}$ control symbols. The decoder can correct at most $t$ symbols, or $2 t=$ $\mathrm{n}-\mathrm{k}$. There are more efficient codes for detecting and correcting errors, for example, the RS code $(255,233.33)$ which is used by NASA in space communications and also in a digital terrestrial transmission chain (DVB-T).

The BCH codes (Bose, Ray-Chaudhuri, Hocquenghem), were invented in the 1960, they are cyclic codes and today they are used as a reference for many recent error correction codes. . These are relatively efficient codes, simple to implement and for which there is a set of low complexity algebraic decoding algorithms. The encoder / decoder assembly makes it possible to construct a cyclic code and to correct a number of $t$ errors in a block of $n$ coded symbols transmitted. Understanding the concepts of algebra in the Galois Field (GF) is necessary to better understand these codes. The block length of the BCH code built on GF ( $\left.2^{\mathrm{m}}\right)$ is given by $\mathrm{n}=2^{\mathrm{m}}-1$. Their uses are in particular in communications by satellite DVB-S2, compact discs CD and DVD.
A number of methods have been proposed to enhance the performance of the chien search block and syndrome architecture [9] [10] [11] [12] [13].
The goal of this work is to present a comparison analysis of the new chien search and new syndrome block with others designs in order to enhance these performances [14] [15] [16] [17].
Finally, the obtained results indicate the proposed designs as having high performance. All designs are evaluated in terms of BER, number of iterations and logic gate resources [18].
The rest of the paper is organized as follows: The Proposed robust factorization methods for RS and BCH decoder are presented in section 2. The syndromes architecture is presented in the session 3, Performance Analysis of the designed circuits are presented in section 3, followed by a conclusion.

## 2. Proposed Robust Factorization Methods for RS and BCH Decoder

The proposed algorithm is based on a specific and methodic factorization of the error locator polynomial such as $\{(\mathrm{P}(\mathrm{x})$ $=A x^{n}+B$, where $\left.\left.n=1\right)\right\}$ should be depicted in this polynomial. This method allows us to conceive a new circuit of Chien Search Block i.e. we can minimize both the number of components and the response time compared to the basic Chien search block.

### 2.1 Design using the First factorization method

If we take the case of $\operatorname{RS}(15,11, \mathrm{t})$ the error locator polynomial is:
$\Lambda(x)=14 X^{2}+14 X+1$
It's a polynomial of degree 2 as type:
$\Lambda(\mathrm{x})=\mathrm{A}_{2} \mathrm{X}^{2}+\mathrm{A}_{1} \mathrm{X}+\mathrm{A}_{0}=(\mathrm{AX}+\mathrm{B})(\mathrm{AX}+\mathrm{C})$

The equation (2) can be written as form:
$\Lambda(\mathrm{x})=(\alpha \mathrm{X}+\beta)(\alpha \mathrm{X}+\gamma)=\alpha^{2} \mathrm{X}^{2}+\alpha \mathrm{X} \gamma+\alpha \mathrm{X} \beta+\beta \gamma$ $=\alpha^{2} X^{2+} \alpha(\gamma+\beta) X+\beta \gamma$
Or $\mathrm{A}_{2}=\alpha^{2}, \mathrm{~A}_{1}=\alpha(\gamma+\beta)$ and $\mathrm{A}_{0=} \beta \gamma$
For equation (2) the basic circuit corresponding is represented in Figure 1.


Figure 1. Basic schema of Chien Search.
For the equation (3) the modified circuit by using the factorization method is represented in Figure 2.


Figure 2. Modified circuit of Chien Search


Figure 3. Modified circuit of Chien Search

For the case of a polynomial of degree 3 we have:

$$
\begin{align*}
\Lambda(X) & =(\alpha X+\beta)(\alpha X+\gamma)(\alpha X+\lambda) \\
& =\left(\alpha^{2} X^{2}+\alpha(\gamma+\beta) X+\beta \cdot \gamma\right)(\alpha X+\lambda) \tag{4}
\end{align*}
$$

Generally for:

$$
\begin{equation*}
\Lambda(\mathrm{X})=(\alpha \mathrm{X}+\beta)(\alpha \mathrm{X}+\gamma) \ldots(\alpha \mathrm{X}+v) \tag{5}
\end{equation*}
$$

The corresponding logic circuit is represented in Figure 3.

### 2.2 Design using the second factorization method

- Case for odd polynomial

If we take the polynomial of degree 3 we have:
$\Lambda(\mathrm{X})=\mathrm{AX}^{3}+\mathrm{BX}^{2}+\mathrm{CX}+\mathrm{D}=\mathrm{X}^{2}(\mathrm{Ax}+\mathrm{B})+(\mathrm{Cx}+\mathrm{D})$
If we take the polynomial of degree5 we have:

$$
\begin{align*}
\Lambda(X) & =\mathrm{AX}^{5}+\mathrm{BX}^{4}+\mathrm{CX}^{3}+D X^{2}+E X+F  \tag{6}\\
& =\mathrm{X}^{4}(\mathrm{Ax}+\mathrm{B})+\mathrm{X}^{2}(\mathrm{CX}+\mathrm{D})+(\mathrm{EX}+\mathrm{F}) \tag{7}
\end{align*}
$$

If we take the polynomial of degree7 we have:
$\Lambda(X)=\mathrm{AX}^{7}+\mathrm{BX}^{6}+\mathrm{CX}^{5}+\mathrm{D} \mathrm{X}^{4}+\mathrm{EX}^{3}+\mathrm{F} \mathrm{X}^{2}+\mathrm{GX}+\mathrm{H}$
$=X^{6}(A x+B)+X^{4}(C x+D)$
$+\mathrm{X}^{2}(\mathrm{EX}+\mathrm{F})+(\mathrm{GX}+\mathrm{H})$
If we take the polynomial of degree 9 we have:
$\Lambda(\mathrm{X})=\mathrm{AX}^{9}+\mathrm{BX}^{8}+\mathrm{CX}^{7}+\mathrm{D} \mathrm{X}^{6}+\mathrm{EX}^{5}+\mathrm{F} \mathrm{X}^{4}+\mathrm{GX}^{3}+\mathrm{H} \mathrm{X}^{2}+\mathrm{IX}+\mathrm{J}$

$$
=\mathrm{X}^{8}(\mathrm{AX}+\mathrm{B})+\mathrm{X}^{6}(\mathrm{CX}+\mathrm{D})+\mathrm{X}^{4}(\mathrm{EX}+\mathrm{F})
$$

$$
\begin{equation*}
+\mathrm{X}^{2}(\mathrm{GX}+\mathrm{H})+(\mathrm{IX}+\mathrm{J}) \tag{9}
\end{equation*}
$$

If we take the polynomial of degree $n$ we have:

$$
\begin{equation*}
\Lambda(X)=A_{n} X^{n}+A_{n-1} X^{n-1}+\ldots+A_{1} X^{1}+A_{0} \tag{10}
\end{equation*}
$$

## - Case for even polynomial

If we take the polynomial of degree 4we have:

$$
\begin{aligned}
\Lambda(\mathrm{X}) & =\mathrm{AX}^{4}+\mathrm{BX}^{3}+\mathrm{CX}^{2}+\mathrm{DX}+\mathrm{E} \\
& =\mathrm{X}^{3}(\mathrm{AX}+\mathrm{B})+\mathrm{X}(\mathrm{CX}+\mathrm{D})+\mathrm{E}
\end{aligned}
$$

If we take the polynomial of degree 6 we have:
$\Lambda(X)=\mathrm{AX}^{6}+\mathrm{BX}^{5}+\mathrm{CX}^{4}+\mathrm{DX}^{3}+\mathrm{EX}^{2}+\mathrm{FX}+\mathrm{G}=\mathrm{X}^{5}(\mathrm{AX}+\mathrm{B})+\mathrm{X}^{3}$

$$
\begin{equation*}
(\mathrm{CX}+\mathrm{D})+\mathrm{X}(\mathrm{EX}+\mathrm{F})+\mathrm{G} \tag{12}
\end{equation*}
$$

If we take the polynomial of degree 8 we have:
$\Lambda(\mathrm{X})=\mathrm{AX}^{8}+\mathrm{BX}^{7}+\mathrm{CX}^{6}+\mathrm{DX}^{5}+\mathrm{EX}^{4}+\mathrm{FX}^{3}+\mathrm{GX}^{2}+\mathrm{HX}+\mathrm{I}$
$=\mathrm{X}^{7}(\mathrm{AX}+\mathrm{B})+\mathrm{X}^{5}(\mathrm{CX}+\mathrm{D})$
$+X^{3}(E X+F)+X(G X+H)+I$
If we take the polynomial of degree 10 we have:
$\Lambda(\mathrm{X})=$

$$
\begin{align*}
& \mathrm{AX}^{10}+\mathrm{BX}^{9}+\mathrm{CX}^{8}+\mathrm{DX}^{7}+\mathrm{EX}^{6}+\mathrm{FX}^{5}+\mathrm{GX}^{4}+\mathrm{HX}^{3}+\mathrm{IX}^{2}+\mathrm{JX}+\mathrm{K} \\
= & \mathrm{X}^{9}(\mathrm{AX}+\mathrm{B})+\mathrm{X}^{7}(\mathrm{CX}+\mathrm{D})+\mathrm{X}^{5}(\mathrm{EX}+\mathrm{F})+\mathrm{X}^{3}(\mathrm{GX}+\mathrm{H}) \\
+ & \mathrm{X}(\mathrm{IX}+\mathrm{J})+\mathrm{K} \tag{14}
\end{align*}
$$

If we take the polynomial of degree n we have:

$$
\begin{equation*}
\Lambda(\mathrm{X})=\mathrm{A}_{\mathrm{n}} \mathrm{X}^{\mathrm{n}}+\mathrm{A}_{\mathrm{n}-1} \mathrm{X}^{\mathrm{n}-1}+\ldots+\mathrm{A}_{1} \mathrm{X}^{1}+\mathrm{A}_{0} \tag{15}
\end{equation*}
$$



Figure 4. Modified circuit 2 of Chien Search Block polynomial as degree 5


Figure 5. Modified circuit 2 of Chien Search Block polynomial as degree 6

## 3. Syndromes Architecture

The calculation of the syndrome is defined as the remainder of the division between the received polynomial $R(x)$ and the generator polynomial $g(x)$. The rest indicated the presence of errors. As the division operation is always a complex operation in relation to sums and additions, we are led to look for another method for calculating the syndrome.
The calculation of the syndrome can also be carried out by an iterative process as illustrated in Figure 6. Before being able to calculate the polynomial of the syndrome, we must wait until we have received all the elements of the polynomial $\mathrm{R}(\mathrm{x})$.


Figure 6. syndrome calculator cell
Given the binary codeword polynomial:
$\mathrm{C}(x)=\mathrm{C}_{0}+\mathrm{C}_{1} x+\cdots+\mathrm{C}_{n-1} x^{n-1}$
The received polynomial $\mathrm{R}(x)=\mathrm{R}_{0}+\mathrm{R}_{1} x+\cdots+\mathrm{R}_{n-1} x^{n-1}$ is the sum of $\mathrm{C}(x)$ and $\mathrm{E}(x)$
$R(\mathrm{x})=C(x)+E(x)$
Where:

$$
\begin{equation*}
\mathrm{E}(x)=\mathrm{E}_{0}+\mathrm{E}_{1} x+\cdots+\mathrm{E}_{n-1} x^{n-1} \tag{18}
\end{equation*}
$$

We obtain:

$$
\begin{equation*}
\mathrm{S}_{\mathrm{i}}=\mathrm{R}\left(\alpha^{\mathrm{i}}\right)=\mathrm{C}\left(\alpha^{\mathrm{i}}\right)+\mathrm{E}\left(\alpha^{\mathrm{i}}\right)=\mathrm{E}\left(\alpha^{\mathrm{i}}\right) \tag{19}
\end{equation*}
$$

Or:

$$
\begin{equation*}
M(x) \cdot X^{n-k}=g(x) \cdot q(x)+X(x) \tag{20}
\end{equation*}
$$

$\mathrm{M}(\mathrm{x}) \cdot \mathrm{X}^{\mathrm{n}-\mathrm{k}}+\mathrm{X}(\mathrm{x})=\mathrm{g}(\mathrm{x}) \cdot \mathrm{q}(\mathrm{x})=\mathrm{C}(\mathrm{x})=\mathrm{g}\left(\alpha^{i}\right) \cdot \mathrm{q}\left(\alpha^{i}\right)=0$

Then:

$$
\begin{align*}
\mathrm{S}_{\mathrm{i}}=\mathrm{R}\left(\alpha^{\mathrm{i}}\right) & =\mathrm{E}\left(\alpha^{\mathrm{i}}\right)=\mathrm{Y}_{1} \alpha^{\mathrm{iel}}+\mathrm{Y}_{2} \alpha^{\mathrm{ie} 2}+\ldots+\mathrm{Y} v \alpha^{\mathrm{i} e v} \\
& =\mathrm{Y}_{1} \mathrm{X}^{\mathrm{i}}{ }_{1}+\mathrm{Y}_{2} \mathrm{X}^{\mathrm{i}}{ }_{2}+\ldots+\mathrm{Y} v \mathrm{X}^{\mathrm{i}} v \tag{21}
\end{align*}
$$

Where $X_{1}=\alpha^{\mathrm{el}}, X_{2}=\alpha^{\mathrm{e} 2}$.
$\mathrm{X} v=\alpha^{\mathrm{e} v}$
By the equation (21) we can define the different equations which link the polynomial Syndrome errors:
$\mathrm{S}_{\mathrm{i}}=\mathrm{Y}_{1} \mathrm{X}^{\mathrm{i}}{ }_{1}+\mathrm{Y}_{2} \mathrm{X}^{\mathrm{i}}{ }_{2}+\ldots+\mathrm{Y} v \mathrm{X}^{\mathrm{i}} v$
$\mathrm{S}_{0}=\mathrm{Y}_{1} \mathrm{X}^{0}{ }_{1}+\mathrm{Y}_{2} \mathrm{X}^{0}{ }_{2}+\ldots+\mathrm{Y} v \mathrm{X}^{0} v$
$\mathrm{S}_{1}=\mathrm{Y}_{1} \mathrm{X}^{1}{ }_{1}+\mathrm{Y}_{2} \mathrm{X}^{1}{ }_{2}+\ldots+\mathrm{Y} v \mathrm{X}^{1} v$
$\mathrm{S}_{2}=\mathrm{Y}_{1} \mathrm{X}^{2}{ }_{1}+\mathrm{Y}_{2} \mathrm{X}^{2}{ }_{2}+\ldots+\mathrm{Y} v \mathrm{X}^{2} v$
The General equations of syndromes are:
$\left[\begin{array}{c}s_{0} \\ s_{1} \\ \cdot \\ \cdot \\ \cdot \\ s_{2 t-1}\end{array}\right]=\left[\begin{array}{cccccc}X_{1}^{0} & X_{2}^{0} & \cdot & \cdot & \cdot & X_{V}^{0} \\ X_{1}^{1} & X_{2}^{1} & \cdot & \cdot & \cdot & X_{V}^{1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ X_{1}^{2 t-1} & X_{1}^{0} & \cdot & \cdot & \cdot & X_{V}^{2 t-1}\end{array}\right]\left[\begin{array}{c}Y_{1} \\ Y_{2} \\ \cdot \\ \cdot \\ \cdot \\ Y_{V}\end{array}\right]$
If the received code $r(x)$ is not affected by errors then all the coefficients of the Syndrome will be zero ( $\mathrm{r}(\mathrm{x})=\mathrm{c}(\mathrm{x})$ ).

### 3.1 Methods for Calculing the syndromes

The syndrome computation block calculates all the syndromes
Si $(1 \leq i \leq 16)$ by putting the roots of generator polynomial $g(x)$ into the received codeword polynomial $\mathrm{R}(\mathrm{x})$.
For example the code $\mathrm{RS}(15,11)$ : $2 \mathrm{t}=4$ syndrome ( $\mathrm{S} 0, \mathrm{~S} 1$, S2,S3)

$$
\begin{equation*}
S(x)=S_{3} x^{3}+S_{2} x^{2}+S_{1} x^{1}+S_{0} x^{0} \tag{23}
\end{equation*}
$$

## Direct Method:

The equation for calculing the syndrome with the direct method [19] is:
$\mathrm{S}_{\mathrm{i}}=\mathrm{R}\left(\alpha^{\mathrm{i}}\right)=\mathrm{R}_{\mathrm{n}-1}\left(\alpha^{\mathrm{i}}\right)^{\mathrm{n}-1}+\mathrm{R}_{\mathrm{n}-2}\left(\alpha^{\mathrm{i}}\right)^{\mathrm{n}-2}+\ldots+\mathrm{R}_{1}\left(\alpha^{1}\right)+\mathrm{R}_{0}$
For calculing $S_{1}$ we replace x by $\alpha_{1}$ in the following equation:
$S_{0}=\left(\alpha^{0}\right)^{14}+2\left(\alpha^{0}\right)^{13}+3\left(\alpha^{0}\right)^{12}+4\left(\alpha^{0}\right)^{11}+5\left(\alpha^{0}\right)^{10}+11\left(\alpha^{0}\right)^{9}+$
$7\left(\alpha^{0}\right)^{8}+8\left(\alpha^{0}\right)^{7}+9\left(\alpha^{0}\right)^{6}+10\left(\alpha^{0}\right)^{5}+11\left(\alpha^{0}\right)^{4}+3\left(\alpha^{0}\right)^{3}+\left(\alpha^{0}\right)^{2}+$
$12\left(\alpha^{0}\right)+12$
$S_{0}=15$
$S_{1}=\left(\alpha^{1}\right)^{14}+2\left(\alpha^{1}\right)^{13}+3\left(\alpha^{1}\right)^{12}+4\left(\alpha^{1}\right)^{11}+5\left(\alpha^{1}\right)^{10}+11\left(\alpha^{1}\right)^{9}+$
$7\left(\alpha^{1}\right)^{8}+8\left(\alpha^{1}\right)^{7}+9\left(\alpha^{1}\right)^{6}+10\left(\alpha^{1}\right)^{5}+11\left(\alpha^{1}\right)^{4}+3\left(\alpha^{1}\right)^{3}+\left(\alpha^{1}\right)^{2}+$
$12\left(\alpha^{1}\right)+12$
$S_{1}=3$

## Horner Method:

The equation for calculing the syndrome with the Horner Method [20] is:

$$
\begin{equation*}
\mathrm{S}_{\mathrm{i}}=\left(\ldots \ldots \ldots\left(\mathrm{R}_{\mathrm{n}-1} \alpha^{\mathrm{i}}+\mathrm{R}_{\mathrm{n}-2}\right) \alpha^{\mathrm{i}}+\ldots+\mathrm{R}_{1}\right) \alpha^{1}+\mathrm{R}_{0} \tag{25}
\end{equation*}
$$

$S_{2}=\left(\left(\left(()\left(\left(()\left(\left(() \alpha^{2}+2\right) \cdot \alpha^{2}+3\right) \alpha^{2}+4\right) \cdot \alpha^{2}+5\right) \alpha^{2}+11\right) \cdot \alpha^{2}+\right.\right.$
7). $\left.\left.\left.\left.\alpha^{2}+8\right) \alpha^{2}+9\right) \alpha^{2}+10\right) \cdot \alpha^{2}+11\right)$
$S_{2}=4$
$S_{3}=\left(\left(()\left(\left(()\left(\left(()\left(1 \alpha^{3}+2\right) \cdot \alpha^{3}+3\right) \alpha^{3}+4\right) \cdot \alpha^{3}+5\right) \alpha^{3}+11\right) \cdot \alpha^{3}+\right.\right.$ 7) $\left.\left.\left.\left.\cdot \alpha^{3}+8\right) \alpha^{3}+9\right) \alpha^{3}+10\right) \cdot \alpha^{3}+11\right)$
$\mathrm{S}_{3}=12$
$S(x)=S_{3} x^{3}+S_{2} x^{2}+S_{1} x^{1}+S_{0} x^{0}$
$S(x)=12 x^{3}+4 x^{2}+3 x^{1}+15 x^{0}$
The following figure shows the principle of calculation of the four syndromes at the same time:


Figure 7. Logic circuit of the RS syndrome block (15, 11)

### 3.2 Serial Architecture

The serial syndrome computation block is implemented by following equation 4.

$$
\begin{equation*}
\mathrm{S}_{\mathrm{i}}=\mathrm{R}\left(\alpha^{\mathrm{i}}\right)=\mathrm{r}_{254}\left(\alpha^{\mathrm{i}}\right)^{254}+\mathrm{r}_{253}\left(\alpha^{\mathrm{i}}\right)^{253}+\ldots \ldots . . \mathrm{r}_{1}\left(\alpha^{\mathrm{i}}\right)+\mathrm{r}_{0} \tag{26}
\end{equation*}
$$



Figure 8. Serial Syndrome Block Diagram
The received vector enters serially to the circuit to compute the syndrome coefficients in parallel in n or (255) clock cycles, as shown in Figure 8.
For the case of RS (255, 239,) where: $\mathrm{N}=255, \mathrm{~K}=239$ we have $\mathrm{N}-\mathrm{K}=\mathrm{t}=16=>16$ Syndromes: $\mathrm{S} 1, \mathrm{~S} 2, \ldots, \mathrm{~S} 16$.
S1 can be calculated by the direct method and the even syndromes can be calculated using the following relationship $\mathrm{S}_{2 \mathrm{i}}=\mathrm{Si} 2$.

### 3.3 Three-Parallel Syndrome

Three -parallel syndrome computation block [ref] can be expressed by the equation presented in equation. 4. Which equivalent to equation. 4.1 but in another form.

$$
\begin{align*}
& \mathrm{R}(\mathrm{x})=\mathrm{r}_{2544} \mathrm{X}^{254}+\mathrm{r}_{253} \mathrm{x}^{253}+\ldots \ldots \mathrm{r}_{1} \mathrm{X}+\mathrm{r}_{0}  \tag{27}\\
& \mathrm{G}(\mathrm{x})=\left(\mathrm{x}-\alpha^{0}\right)\left(\mathrm{x}-\alpha^{1}\right) \ldots \ldots \ldots\left(\mathrm{x}-\alpha^{14}\right)\left(\mathrm{x}-\alpha^{15}\right) \tag{28}
\end{align*}
$$

$\mathrm{Si}=\mathrm{R}\left(\alpha^{\mathrm{i}}\right)=\mathrm{r}_{254}\left(\alpha^{\mathrm{i}}\right)^{254}+\mathrm{r}_{253}\left(\alpha^{\mathrm{i}}\right)^{253}+\ldots \ldots . \mathrm{r}_{1}\left(\alpha^{\mathrm{i}}\right)+\mathrm{r}_{0}$


Figure 9. Three parallel syndrome computation block
The Three parallel syndrome computation block calculated by this equation:

$$
\begin{align*}
& \mathrm{S}_{\mathrm{i}}=\mathrm{R}\left(\alpha_{\mathrm{i}}\right)= \\
& \left(\left(\ldots\left(\mathrm{r}_{254}\left(\alpha^{\mathrm{i}}\right)^{2}+\mathrm{r}_{253}\left(\alpha^{\mathrm{i}}\right)^{1}+\mathrm{r}_{252}\right)\left(\alpha^{\mathrm{i}}\right)^{3}+\mathrm{r}_{251}\left(\alpha^{\mathrm{i}}\right)^{2}+\mathrm{r}_{250}\left(\alpha^{\mathrm{i}}\right)^{1}+\mathrm{r}_{249}\right)\right. \\
& \left.\left.\left(\alpha^{\mathrm{i}}\right)^{3}+\ldots .\right)\left(\alpha^{\mathrm{i}}\right)^{3}+\mathrm{r}_{2}\left(\alpha^{\mathrm{i}}\right)^{2}+\mathrm{r}_{1}\left(\alpha^{\mathrm{i}}\right)^{1}+\mathrm{r}_{0}\right) \tag{30}
\end{align*}
$$

In the first clock, the mot received is (r254, r253, r252) in parallel, the second mot $r_{252}$ is going to adder, $r_{523}$ is multiplied by $\alpha^{\mathrm{i}}$ and added to $\mathrm{r}_{252}$, the final $\mathrm{r}_{254}$ is multiplied by $\left(\alpha^{\mathrm{i}}\right)^{2}$ and added to $\left(\mathrm{r}_{253} *\left(\alpha^{\mathrm{i}}\right)^{1}+\mathrm{r}_{251}\right)$. So the output of latch(1) is : $\mathrm{r}_{254}\left(\alpha^{\mathrm{i}}\right)^{2} \mathrm{r}_{253} *\left(\alpha^{\mathrm{i}}\right)^{1}+\mathrm{r}_{251}$. the second clock the output of latch(1) is multiplied by $\left(\alpha^{\mathrm{i}}\right)^{3}$ and then added with $\mathrm{r}_{251}\left(\alpha^{\mathrm{i}}\right)^{2}+\mathrm{r}_{250}\left(\alpha^{\mathrm{i}}\right)^{1}+\mathrm{r}_{249}$

## 4. Performance Analysis of the Designed Circuits

## 4.1 performance and Comparison of designs based factorization methods

The proposed circuits are compared in terms of BER performance and Number of iterations, and number of minimized logic gates.
Tables 1, 2 and 3, also Figure 10, 11, 12, 13, 14 and 15 show the evaluation of the performance based on the number of the used logic gates and the obtained values of bit error rate BER for all designs by using the modified circuit for different error locator polynomials, especially in the case of second factorization method both odd error locator and even error locator.

Table 1. Computational minimization rate logic gates and BER values of the design based first factorization method

| Error locator polynomial | Minimization rate $\left(\frac{\mathrm{Nm}}{\mathrm{Nb}} \mathrm{X100}\right) \%$ | BER $\left(\frac{100-\mathrm{Mr}}{100}{\mathrm{X} 10 \mathrm{x}^{-4}}^{4}\right)$ |
| :---: | :---: | :---: |
| $\Lambda(\mathrm{X})=\mathrm{AX}^{2}+\mathrm{BX}+\mathrm{C}$ | 45, 45 | 0,000054 |
| $\begin{aligned} & \Lambda(\mathrm{X})=\mathrm{AX}^{3}+\mathrm{BX}^{2}+ \\ & \mathrm{CX}+\mathrm{D} \end{aligned}$ | 46,66 | 0,000053 |
| $\begin{aligned} & \Lambda(X)=\mathrm{AX}^{4}+\mathrm{BX}^{3}+ \\ & \mathrm{CX}^{2}+\mathrm{DX}+\mathrm{E} \end{aligned}$ | 47,36 | 0,000052 |
|  |  |  |
| $\begin{aligned} & \Lambda(\mathrm{X})=\mathrm{A}_{\mathrm{n}} \mathrm{X}^{\mathrm{n}}+ \\ & \ldots \ldots .+\mathrm{A}_{1} \mathrm{X}+\mathrm{A}_{0} \end{aligned}$ | $\left(\frac{2 n+1}{3+4 n} .100\right) \%$ | $\left(\frac{100-\mathrm{Mr}}{100} \mathrm{X} 10 \mathrm{x}^{-4}\right)$ |

Where: $\mathrm{i}=1,2, \ldots, 2 \mathrm{t}$

Table 2. Computational minimization rate logic gates and BER values of the design based second factorization method with odd error locator polynomial

| Error locator polynomial | Minimization rate $\left(\frac{\mathrm{Nm}}{\mathrm{Nb}} \times 100\right) \%$ | $\begin{aligned} & \text { BER } \\ & \left(\frac{100-\mathrm{Mr}}{100} \mathrm{XiOx}^{-4}\right) \end{aligned}$ |
| :---: | :---: | :---: |
| $\begin{aligned} & \Lambda(\mathrm{X})=\mathrm{AX}^{3}+\mathrm{BX}^{2}+ \\ & \mathrm{CX}+\mathrm{D} \end{aligned}$ | 33,33 | 0.000066 |
| $\begin{aligned} & \Lambda(X)= \\ & A X^{5}+B X^{4}+\mathrm{CX}^{3}+\mathrm{DX}^{2}+ \\ & \mathrm{EX}+\mathrm{F} \end{aligned}$ | 34,78 | 0.000065 |
| $\begin{aligned} & \Lambda(\mathrm{X})=\mathrm{AX}^{7}+\mathrm{BX}^{6}+\mathrm{CX}^{5} \\ & +\mathrm{DX}^{4}+\mathrm{EX}^{3}+\mathrm{FX}^{2}+\mathrm{GX}+ \\ & \mathrm{H} \end{aligned}$ | 35,48 | 0.000064 |
| . | . |  |
| $\begin{aligned} & \Lambda(\mathrm{X})=\mathrm{A}_{\mathrm{n}} \mathrm{X}^{\mathrm{n}}+ \\ & \ldots \ldots .+\mathrm{A}_{1} \mathrm{X}+\mathrm{A}_{0} \end{aligned}$ | $\left(\frac{2 n-(n-1) / 2}{3+4 n} \times 100\right)$ | $\left(\frac{100-\mathrm{Mr}}{100} \mathrm{XiOx}^{-4}\right)$ |

Table 3. Computational minimization rate logic gates and BER values of the design based second factorization method with even error locator polynomial
$\left.\begin{array}{|l|l|l|}\hline \text { Error locator polynomial } & \left.\begin{array}{l}\text { Minimization } \\ \text { rate } \\ \left(\frac{\mathrm{Nm}}{\mathrm{Nb}} \mathrm{X100}\right)\end{array}\right) & \begin{array}{l}\text { BER } \\ \left(\frac{100-\mathrm{Mr}}{100} \mathrm{X10x}\right.\end{array} \\ \hline \begin{array}{c}\Lambda(\mathrm{X})=\mathrm{AX}^{4}+\mathrm{BX}^{3}+\mathrm{CX}^{2}+ \\ \mathrm{DX}+\mathrm{E}\end{array} & 31,57\end{array}\right)$

These tables provide the necessary information about the performance of each design in terms of Number of minimized logic gates and the bit error rate (BER).
During testing from all designs, we can see that there is a significant decrease of number of minimized logic gates after enhancement is applied (for both proposed designs). Minimization rate for the second factorization method is over $34 \%$ or $35 \%$, and for the first factorization method varies from $45 \%$ to $47,36 \%$. Therefore, although for both presented figures $10,11,12,13,14$ and 15 , also table 1,2 and 3 comparisons, we can say that both proposed designs, especially, the one based first factorization are adequate solutions for BCH and RS decoders and give slightly better results.


Figure 10. Evolution of the minimization rate depending on the degree of the error locator polynomial for the modified circuit based first factorization method


Figure 11. Evolution of the minimization rate depending on the degree of the odd error locator polynomial for the modified circuit based second factorization method


Figure 12. Evolution of the minimization rate depending on the degree of the even error locator polynomial for the modified circuit based second factorization method


Figure 13. Evolution of the bit error rate BER depending on the minimization rate for the modified circuit based first factorization method


Figure 14. Evolution of the bit error rate BER depending on the minimization rate for the modified circuit based second factorization method with odd error locator polynomial


Figure 15. Evolution of the bit error rate BER depending on the minimization rate for the modified circuit based second factorization method with even error locator polynomial

## 4.2 performance and Comparison of the serial and parallel

## Circuits for the syndrome Computation architectures

Let's discuss now the performances of different types of Syndrome Computation Architectures by using number of iteration criteria. In this context, Table 5 shows the effect of the number of iteration to the performance of the proposed designs.
In this table 4 shows the number of the gained iterations by using the basic and the modified circuit for different RS and BCH codes.
Table 4. Computational minimization rate of logic gates and number of iterations of the serial and parallel Circuits for the
syndrome Computation block

| Code <br> $\mathrm{N}^{\circ}$ | Codes RS <br> or <br> BCH | Number <br> of <br> iterations <br> serial <br> Circuit | Number <br> of <br> iterations <br> parallel <br> circuit | Number <br> of <br> gained <br> iterations | Minimization <br> rate |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | $(63,55)$ | 64 | 22 | 42 | 65.62 |
| 2 | $(63,47)$ | 64 | 22 | 42 | 65.62 |
| 3 | $(63,39)$ | 64 | 22 | 42 | 65.62 |
| 4 | $(63,31)$ | 64 | 22 | 42 | 65.62 |
| 5 | $(63,23)$ | 64 | 22 | 42 | 65.62 |
| 6 | $(63,15)$ | 64 | 22 | 42 | 65.62 |
| 7 | $(255,239)$ | 256 | 86 | 170 | 66.40 |
| 8 | $(255,225)$ | 256 | 86 | 170 | 66.40 |
| 9 | $(255,205)$ | 256 | 86 | 170 | 66.40 |
| 10 | $(255,191)$ | 256 | 86 | 170 | 66.40 |
| 11 | $(255,183)$ | 256 | 86 | 170 | 66.40 |
| 12 | $(255,175)$ | 256 | 86 | 170 | 66.40 |
| 13 | $(255,165)$ | 256 | 86 | 170 | 66.40 |
| 14 | $(255,135)$ | 256 | 86 | 170 | 66.40 |
| 15 | $(3240$, | 3241 | 1081 | 2160 | 66.64 |
| n | Code (n, k) | $\mathrm{n}+1$ | $(\mathrm{n} / 3)+1$ | $\mathrm{~A}-\mathrm{B}$ | $\left(\frac{\mathrm{A}-\mathrm{B}}{\mathrm{n}+1} \mathrm{X100}\right)$ |

As can be seen, we use the following parameter Block Length ( n ) and the number of information symbols in a code word (k). Thus, from this analysis, we can see that first design based the first factored method gives the better performance than the other design in term number of gained iterations. Because, it needs $((n / 3)+1)$ iteration instead $(\mathrm{n}+1)$ for the second design, however this method gives Minimization rate between 66.40 and 65.62.
This increase in performance, as well as the increase in reliability makes it perfect for BCH and RS decoders. Here the number of iterations are taken are minimize and its summary of the performance is presented in Table 5.
Figure 16 shows the minimization rate performance of the modified Circuit for the syndrome Computation architectures. Performance analysis is carried out by varying the Block Length ( n ) and number of information symbols in a code word (k) and calculating the corresponding number of iteration and minimization rate percentage. The results obtained are compared to that obtained from the serial circuit.


Figure 16. Evolution of the minimization rate depending on the code ( $\mathrm{n}, \mathrm{k}$ )

## 5. Conclusions

In this work, different designs were analyzed and compared .therefore, several test scenarios concerning the proposed designs have been carried out, in order to validate its effectiveness. Evaluation performances showed that it is effective when the new designs are applied.
The major advantage of the proposed design using second factorization method is its minimized number of logic gates and ease of implementation. That is can decrease the BER to optimal values.
For the second contribution, the new design based ThreeParallel Syndrome architecture shows a high performance in term number of gained iterations. It can be seen that when considering the minimized number of iterations, the ThreeParallel Syndrome architecture is the obvious choice for the real time RS and BCH decoders.
Further work could be done in optimizing designs for RS and BCH codes and developing techniques specifically designed and LPDC codes.

## References

[1] Orhan Gazi, "Forward Error Correction via Channel Coding Engineering", Springer, Cham, 2020
[2] P. Salija and B. Yamuna, "Optimum energy efficient error control techniques in wireless systems: a survey", journal of Communications Technology and Electronics, vol. 60, pp. 1257-1263, 2015.
[3] Todd K. Moon, 'Error Correction Coding: Mathematical Methods and Algorithms", 1st Edition, Electronic ISBN: 9780471739210, 2005.
[4] Robert H. Morelos, "Zaragoza, The Art of Error Correcting Coding", John Wiley \& Sons, Electronic, ISBN:9780470847824, 2002.
[5] к. Deergha Rao, "Channel Coding Techniques for Wireless Communication"s, Electronic ISBN: 978-81-322-2292-7, Springer India, 2015.
[6] Trung Q. Duong and Nguyen-Son Vo, "Wireless Communications and Networks for 5G and Beyond", Mobile Networks and Applications, vol. 24, pp. 443-446, 2019.
[7] Krishnamoorthy Narasu Raghavan et al., "Performance Analysis of Convolution Code with Variable Constraint Length in Shallow Underwater Acoustic Communication", International Journal of Computer Network and Information Security (IJCNIS), Vol.11, No.2, PP. 13-20, 2019.
[8] Rajashri Khanai et al., "Performance Analysis of Underwater Acoustic Communication using IDMA-OFDM-MIMO with Reed Solomon and Turbo Code", International Journal of Computer Network and Information Security (IJCNIS), Vol.10, No.12, PP.41-46, 2018.
[9] Elghayyaty Mohamed et al., "Minimized Logic Gates Number Of Components In The Chien Search Block For ReedSolomon (RS)", American Journal of Engineering Research (AJER), Vol.7, No.2, pp. 110-116, 2018.
[10] MelikeYigit, PinarSarisarayBoluk, V. CagriGungor, "A new efficient error control algorithm for wireless sensor networks in smart grid", Computer Standards \& Interfaces, Vol. 63, pp. 27-42, 2019.
[11] Vrajkishandugar et al., "A Survey On Hamming Codes For Error Detection", 2nd International Conference On Intelligent Computing, Instrumentation And Control Technologies (ICICICT), pp. 633-638, 2019.
[12] Jagannathsamanta et al., "FPGA Based Area Efficient RS(23, 17) Codec", Microsystem Technologies, Vol. 23, pp. 639-650, 2017.
[13] Vicente Torres et al., "Soft-Decision Low-Complexity Chase Decoders For The Rs $(255,239)$ Code", Electronics, Vol. 9, No. 8, 2019.
[14] Elghayyaty Mohamed et al., "Performance Study of BCH Error Correcting Codes Using the Bit Error Rate Term BER", Int. Journal of Engineering Research and Application, Vol. 7, No. 2, pp.52-54, 2017.
[15] V. Pushpa et al., "BER Analysis Of BPSK for Block Codes and Convolution Codes Over AWGN Channel", International Journal Of Pure And Applied Mathematics, Vol. 114, No. 11, pp. 221-230, 2017.
[16] Alyaa Al-Barrak et al., "Enhancing BER Performance Limit of BCH and RS Codes Using Multipath Diversity", Computers, Vol. 6, No. 21, pp. 1-13, 2017.
[17] Bashar Tahir et al., "BER Comparison Between Convolutional, Turbo, LDPC, and Polar Codes", IEEE 24th International Conference On Telecommunications (Ict), pp. 1-7, 2017.
[18] Yuval Genga et al. , "Improving the Decoding Performance of the PTA Algorithm for RS Codes Through the Extension of the Parity Check Matrix", IEEE Africon, pp. 171-174, 2017.
[19] Richard W. Middlestead, "Digital Communications with Emphasis On Data Modems: Theory, Analysis, Design, Simulation, Testing, And Applications", Wiley Telecom, Electronic ISBN: 9781119011866, JOHN Wiley \& Sons, INC., 2017.
[20] Horner, W. G. "A New Method of Solving Numerical Equations of al. Orders by Continuous Approximation." Philos. Trans. Roy. Soc. London 109, pp. 308-335, 1819.

