A Novel Construction of Mixed Parity Code for Secret Data Communication

B. Senthilkumar,
Associate Professor, Department of Electrical and Electronics Engineering,
Veltech (Owned by R.S. Trust) Engineering College,
Avadi, Chennai, Tamilnadu, INDIA – 600062
Email: Senthilkumar_05@yahoo.co.in

Abstract—A novel construction of Mixed Parity Code for secret message communication is presented in this paper. Mixed Parity Code is a tool for secured data transmission with bit error control mechanism. The construction procedure of this code is provided based on the choices of existing error control codes and existing message character sets. Crypto-code words are prepared by the combinations of message bits and parity bits of Mixed Parity Code. Properties of proposed code are described by the functions of randomized parity bits positions and intentional bits inversions of crypto-code words. Comparative analysis for selecting one of the existing codes is done to construct Mixed Parity Code. Statistical analysis of two different Mixed Parity codes are prepared for showing the computational hardness of crypto-code words against Brute Force Attack. These results reveal the relationship between number of ASCII characters 'N' in input block size 'k' and number of combinations of ASCII characters N_c in the output block size 'n' of (n, k, q) MP code. This paper concludes that the security hardness of the proposed code depends on number of iterations required for retrieving the correct message without an original key.

Keyword-Data Communication, Error Correcting code, Block Code, Hamming code, Mixed Parity Code, Crypto-coding, Brute Force Attack

I. INTRODUCTION

The conventional way of transferring the secret message from one end to other end is composed of error correction [1], [2] and encryption [3] techniques. But, the properties and behavior of these two methods are entirely different. Secured message transmission over wireless communication channel is done by forward error correcting codes and cryptography techniques. A good encryption algorithm will penetrate more number of errors on retrieving the original message due to channel error. It leads to the need of most efficient error control algorithm to transfer the secret data over wireless communication channel. In the past few decades, many theoretical links between coding theory and cryptography have been expressed [4]. The present digital scenario of "System on Chip" drives the need for combining the functions of coding and cryptography into a single algorithm without sacrificing required security and error control. This will reduce the considerable amount of delay and power consumptions in digital devices. Coding and Cryptography functions have distinct scopes to achieve their reliability higher. Hence, very few reliable methods have been identified to merge coding and cryptography functions into one function as crypto-coding. The employability of cryptography and error correction functions is at different purpose to each other. A cipher needs the property of avalanche effect on bit inversion of original message with false key and channel coder posses the property of bit error control on original message. The reliability of avalanche effect of chipper and error control of channel coder depends on amount of creation of bit inversion due to wrong usage of keys and amount of correction of bit inversion due to channel noise respectively.

Although, these two functions exhibit differences in their inherent properties, researchers have done much work to combine them to form a single function. This is achieved by looking into few of their common properties such as bit length modulation, non-linearity propagation, uniqueness in the set of output etc. This paper describes one such method of crypto coding.

As per the coding theory, error correction capability can be improved by adding redundancy bits. This leads to the higher computational complexity of forward error control algorithms. In the past few years, diffusion properties of certain error correcting codes have been used to create ciphers [5], [6]. For example, the Mix Column operation of the Advanced Encryption Standard (AES) cipher is generated using Maximum Distance Separable (MDS) codes [5]. Mathematically derived channel codes are bounded by systematic characteristics. So, they do not possess the adequate amount of diffusion required by ciphers. However, researchers are still working on to find an efficient single algorithm for error control and cryptography.

In this paper, we demonstrate a novel crypto-code as a common tool for cryptographically secured block cipher with good error control property. Behavior of this proposed MP code is investigated for achieving good error control capacity along with high security strength. For the above mentioned investigation, we analyze three

major factors as (1) similarity between bit symbols of message input 'k' and bit symbols of codeword output 'n' of (n, k, q) MP Code (2) occurrence of non-linearity in data recovery between input block size 'k' and output block of size 'n' of MP code (3) hamming distance between the set of output blocks 'n_j' (where j ϵ {1,2,3,…., $(1\text{-}2^n)$}) of MP code.

The rest of the paper has been organized as follows. Section II provides preliminary concepts of MP codes; Section III provides the construction and properties of Mixed Parity codes (MP codes); Section IV provides the analysis of MP codes for different block size over the Galois Field GF (q) and Section V provides the conclusion based on the results gathered from the statistical analysis of MP codes for using it as crypto-coding.

II. PRELIMINARY CONCEPTS FOR PROPOSED MIXED PARITY CODES

A. Introduction to Coding Theory

Block Codes: A block code is a set of words that has a well-defined mathematical property or structure, and where each word is a sequence of a fixed number of bits. The words belonging to a block code are called code words. Examples of simple block code with 4-bit code words are BCD codes, Gray Codes. A word with 'n' bits is referred to as n-bit word.

Code word: The idea is to add redundancy to the message or information in order to be able to detect and correct the errors. We use an encoding algorithm to add this redundancy and a decoding algorithm to reconstruct the initial message. A message of length 'k' is transformed into a codeword 'c' of length 'n' with n > k and n= k + r where 'r' is number of redundancy bits in a codeword.

A code, whose code words have 'k' information bits or message bits, 'r' parity bits and n-bit code words where n= k + r, is referred as an (n, k) block code where n and k are the block length and information length of the code respectively. The position of the parity bits 'r' within a code word is quite arbitrary. They can be dispersed within the information bits or kept together and placed on either side of the information bits. A code word, whose information bits are kept together, is said to be systematic code. A code word, whose parity bits are dispersed within the information bits, is referred to as non-systematic code.

Hamming Weight and Hamming Distance: The hamming weight or weight of a word 'v' is defined as the number of nonzero components of 'v' and is denoted by w(v). The Hamming distance or distance between two words 'v_1' and 'v_2', having the same number of bits, is defined as the number of places in which they differ and is denoted by $d(v_1,v_2)$.

For example the words v_1= (011010) and v_2= (101000) have weights of 3 and 2 respectively and are separated by a distance of 3.

The minimum distance d_{min} of a block code is the smallest distance between code words. Hence code words differ by d_{min} or more bits. The minimum distance is found by taking pair of code words, determining the distance between them and then repeating this for all pairs of different code words. The smallest value obtained is the minimum distance of the code.

Application of Hamming Distance: Hamming distance is used to assess the error control ability of a code. The error correction limits 'n' and error detection limits 'l' are bounded by hamming distance or minimum distance d_{min} of a code. Codes with error correction limit 't' and error detection limit 'l' are referred to as t-error correcting codes and l- error detecting codes respectively. Mathematically, $l = d_{min} - 1$ and $t = ½ (d_{min} - 1)$.

Application of block code as error control code: A word with n- bits can be represented by a vector with n-components. For example, 4-bit word can be (1010), (1110), (0010) and so on. A set of words is called code. For an (n, k) block code the input to the encoder is the information word i= $(i_1,i_2,i_3,……,i_k)$ where i_j= 0 or 1 and j is an integer $1 \leq j \leq k$. The encoder determines r = n-k parity check bits $p_1,p_2,……,p_r$ according to the encoding rule of the code and appends them to the information bits or disperse them among the information bits so giving the code word c= $(i_1,i_2,i_3,……,i_k, p_1,p_2,……,p_r)$. The encoding rule of a code is such that the combination of the parity bits and the information bits (i.e. the code word) has the mathematical property required by the code. It is usual to represent code word as c = $(c_1,c_2,…..,c_n)$ *where* $c_j = i_j$ *for* $1 \leq j \leq k$ *and* $c_j = p_{j-k}$ *for* $k < j \leq n$.

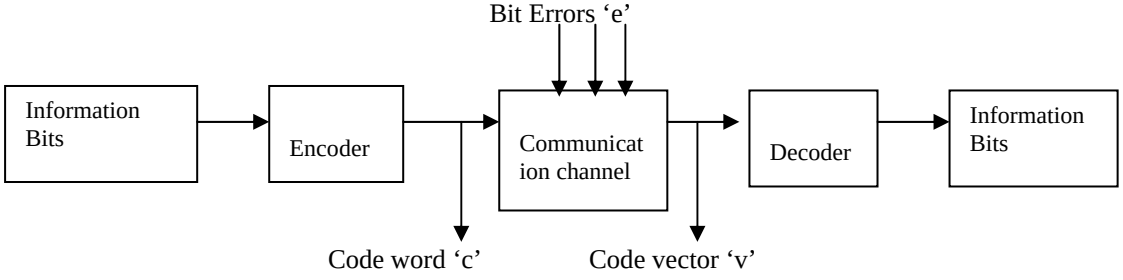

Fig. 1. Generic settings for Error Control Code

When this code word is transmitted over wireless communication channel, there may be the bit inversion on the code word due to channel noise. These errors can be represented by the vectors. An n-bit codeword is liable to a maximum of n errors which can be represented by the error vector or error pattern as $e = (e_1,e_2,\ldots\ldots,e_n)$ where $e_j = 1$ if there is an error in the j^{th} position or $e_j = 0$ if the j^{th} position is error free.

A code word c that incurs an error e results in the word as v = c + e where the components of v are given by the components of c and e added pair wise as

$$\begin{aligned} v &= (c_1,c_2,\ldots..,c_n) + (e_1,e_2,\ldots\ldots,e_n) \\ &= (c_1+e_1,\ c_2+e_2,\ldots\ldots..,c_n+e_n) \\ &= (v_1,v_2,\ldots\ldots,v_n) \end{aligned}$$

where $v_j = c_j + e_j$ for $1 \leq j \leq n$ and where modulo-2 addition is used when adding c_j and e_j together.

The word v represents the code word after it has been subjected to the error e. If all the components of e are zero, then $v_1 = c_1$, $v_2 = c_2,\ldots..,v_n = c_n$ and therefore v = c. The equation v = c +e is central to the decoding process. A decoder has no prior knowledge of c, the only information that it has is the word v that it receives. It is referred to as the received word or decoder input. For an error detecting code the task of the decoder is to establish whether v is a code word. This can be achieved by checking v against a table of code words or by checking whether v has the mathematical property required by the code.

For an error correcting code the decoder has to estimate or guess the code word from v. If the decoder's estimate of the error pattern is ê then, from the equation v = c + e, its estimate of the code word is ĉ = v - ê, and given that modulo-2 addition is used then ĉ = v + ê is the decoder's estimate of c. However, whether a decoder can determine the correct code word from v depends upon the code, the errors incurred and the decoding algorithm.

Galois Fields (GF): Finite fields are referred to as Galois Fields after the mathematician Evariste Galois (1811-1832). It is used to identify the set of components within the field to perform the addition and multiplication operation of a code. The fields are usually expressed as $GF(p^m)$ where p is the number of elements in the base field, which is referred to as the field's characteristics and m is the degree of the polynomial whose root is used to construct the fields. The order of the field is given by $q = p^m$. In the digital communication, where binary digits are only employed, p is always 2 and m = 1, 2, 3, … so on. In normal course, block codes are usually represented with GF fields as (n, k, q) block code. For example, if $q = 2^1$, then the block code is bounded by 0s and 1s only as field components. Otherwise, if $q=2^3$, the field components are 0, 1, α, α^2, α^3, α^4, α^5 and α^6 where α is the root lies within a finite field GF (2^3).

Binary Symmetric Channel (BSC): Figure 2 shows the concept of Binary Symmetric Channel (BSC). It is a channel that transports 1's and 0's from the transmitter (Tx) to the receiver (Rx). It makes an error occasionally, with probability p. A BSC flips a 1 to 0 and vice-versa with equal probability.

Let X and Y be binary random variables that represent the input and output of this BSC respectively. Let the input symbol be equally likely and the output symbols depend upon the input according to the channel transition probabilities as P (Y=0|X=0) = 1-p ; P (Y=0|X=1) = p ; P (Y=1|X=1) = 1-p ; P (Y=1|X=0) = p. These equations implies that the probability of a bit getting flipped (i.e. in error) when transmitted over this BSC is p.

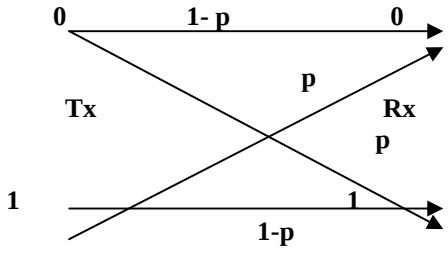

Fig. 2. A Binary Symmetric Channel

B. ASCII character set

The American Standard Code for Information Interchange (ASCII) assigns values between 0 and 255 for upper case letters, numeric digits, punctuation marks and other symbols. ASCII characters can be split into the following sections:

- 0 – 31 for Control codes;

  Examples are 000 – NUL, 002 – SOH, 027 – ESC
- 32 – 127 for Standard, implementation – independent characters;

  Examples are 032 – Space, 049 – 1, 065 – A, 097 – a, 127 - delete

- 128 – 255 for Special symbols, international character sets, non-standard characters;

  Examples are 131 - ƒ, 137 – ‰, 251 - ©

Among the above whole ASCII characters, 32 – 127 are the standard, independent alphanumeric characters being used by the common people for every day.

C. Error Probability after coding

Definition 1: Let C be an (n, k) code over GF (q) and 'a' be any vector of length n. Then the set

$a + C = \{a+x \mid x \in C\}$ is called a coset of C. 'a' and 'b' are said to be in the same coset if $(a-b) \in C$.

Definition 2: The vector having the minimum weight in a coset is called the coset leader. If there are more than one vector with the minimum weight, one of them is chosen at random and is declared the coset leader.

Definition 3: A standard array for an (n, k) code C is a $q^{n-k} \times q^k$ array of all vectors in GF $(q)^n$ in which the first row consists of code C with 0 on the extreme left and the other rows are the cosets $a_i + C$, each arranged in corresponding order, with the coset leader on the left.

Definition 4: The probability of error or word error rate P_{err} for any decoding scheme is the probability that the decoder output is a wrong codeword. It is also called as residual error rate. Suppose there are M code words of length 'n' which are used with equal probability. Let the number of coset leaders with weight 'i' be denoted by α_i. Here BSC channel is assumed with symbol error probability p. A decoding error occurs if the error vector e is not a coset leader. Therefore, the probability of correct decoding will be

$$P_{cor} = \sum_{i=0}^{n} \alpha_i \, p^i (1-p)^{n-i}$$

Hence, the probability of error will be

$$P_{err} = 1 - \sum_{i=0}^{n} \alpha_i \, p^i (1-p)^{n-i}$$

D. Cryptography

The term cryptography (or cryptology derived from Greek kryptós "hidden" and gráfo "write") is the study of message secrecy. The opposite is cryptanalysis which is the study of methods of how to reverse the encrypted message. This chapter aims to give some background on the encryption techniques and application areas considered during the design process of the system.

1) Basics of Cryptography: Figure 3 shows the tradition within the area of cryptography of using the names Alice, Bob and Eve to represent the different roles played by the communicating devices on a communication channel. By definition Alice sends messages to Bob and Eve is assumed to be eavesdropping on all messages sent on the communication channel.

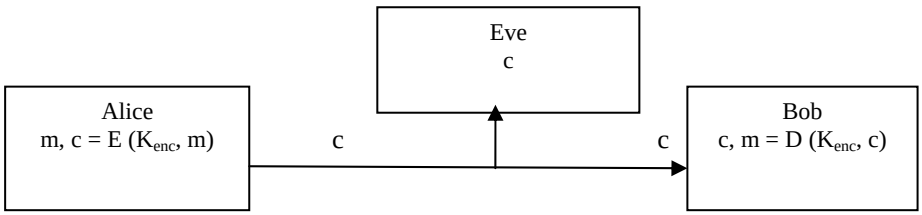

Fig. 3. Generic settings for cryptography

2) Encryption and Decryption Technique: Encryption is used to communicate securely over an insecure communication channel. Consider Alice communicating with Bob. As in the Figure 3, any message from Alice to Bob is also received by Eve. To prevent Eve from understanding the message an encryption function E (K_{enc}, m) is used to transform the so called Plaintext 'm', into the unreadable Cipher text 'c', where K_{enc} represents the encryption key which is to be known only by the authorized communicants and not by Eve. In order for Bob to be able to read the message, a decryption function D (K_{enc}, c) is used to make the reverse transformation from Cipher text into Plaintext.. Both these transformations require a cipher which is an algorithm used for performing encryption and decryption. The key is as mentioned to be kept secret although the algorithm can and should be public.

3) Cryptanalysis: It is the science of science of recovering the plaintext of a message from the cipher text without access to the original key. In cryptanalysis, it is always assumed that the cryptanalyst has full access to the algorithm. An attempted cryptanalysis is known as an attack, of which there are five major types. They are (i)

Brute force attack, (ii) Cipher text –only attack, (iii) Known-plain text attack, (iv) Chosen - plain text attack, (v) Chosen-cipher text attack. *Brute force attack is the technique that requires a large amount of computing power and a large amount of time to run on a computer. It consists of trying all possibilities in a logical manner until the correct one is found. Rests of the cryptanalysis are beyond the scope of this paper.*

E. Construction of Error control codes as crypto-coding

Crypto-coding is the art of combing coding theory and cryptography into a single function. Some of the related terminology used for both coding theory and cryptography are shown below.

TABLE I
Related terminology between coding theory, cryptography and crypto-coding

Sl. No.	Description	Coding Theory	Cryptography	Crypto –Coding using MP codes
1	Input	Information Bits	Message Text	Message Bits
2	Output	Code word	Cipher Text	Crypto-Code Word
3	Input block size	Multiple number of equal length of information bits	Multiple number of equal length of Message text	Multiple number of equal length of Message Bits
4	Output block size	Multiple number of equal length of code words	Multiple number of equal length of Cipher text	Multiple number of equal length of Crypto-Code Words
5	Realization of group of bits for Input and Output character set	Binary Coded Decimal (BCD)	American Standard Code for Information Interchange (ASCII)	American Standard Code for Information Interchange (ASCII)
6	Encryption	Process of converting Information bits to code word by adding redundancy bits	Process of converting Message text to cipher text by S-box, rotation of bits, addition of bits with key	Crypto-encryption that does combined encryption processes of coding theory and cryptography
7	Decryption	Process of converting code word to Information bits by removing redundancy bits	Process of converting cipher text to Message text by S-box, rotation of bits, addition of bits with key	Crypto-decryption that does combined decryption processes of coding theory and cryptography
8	Error message	Bit inversion on code word due to channel noise	Bit inversion on Cipher Text due to wrong key	Bit inversion on Crypto-Code Word
9	Mode of communication	Transmitter and Receiver	Sender and Receiver	Sender and Receiver
10	Communication Channel	Wireless or wired communication	Compact Disc, Internet, Intranet	Compact Disc, Internet, Intranet over Wireless or wired communication
11	Recovery of original input	Error Control Algorithm with code lookup table	Cryptography Algorithm with binary keys	Combined functions of both Error Control Algorithm and Cryptography Algorithm
12	Method of arithmetic operations	Modulo-2 arithmetic operations	Modulo-2 arithmetic operations	Modulo-2 arithmetic operations
13	Method of scrambling the input data	Adding or Dispersing parity bits with information bits	Performing Substitution of bits, rotation of bits, addition of bits with Message text	Adding or Dispersing parity bits with message bits and Performing Substitution of bits, rotation of bits, addition of bits on Crypto-Code Word

The table I illustrates that there are some common processes in both Error control and Cryptographic functions such as input, output, encryption, and decryption. The Error control function adds the extra bits to the length of input as redundant bits. But, the cryptography function may not add or reduce the length of input.

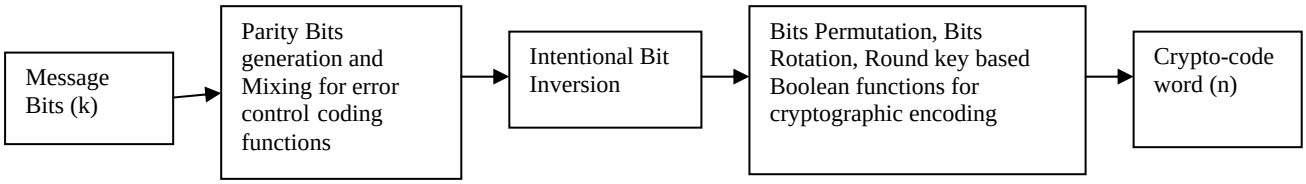

Fig. 4.a. Generic settings for Crypto-Encoding

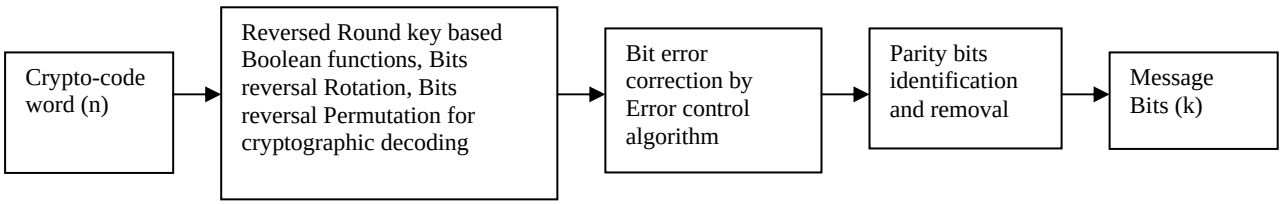

Fig. 4.b.Generic settings for Crypto-Decoding

Figures 4.a and 4.b depict the essential blocks of crypto-coding using Mixed Parity Codes. Crypto-encoding converts the input message block size of 'k' bits into output crypto-code word block size of 'n' bits. Crypto-decoding converts the input crypto-code word block size of 'n' bits into output message block size of 'k' bits.

F. Introduction to Mixed Parity Code

Definition 5: For any vector 'u' in GF $(q)^n$ and any integer $r \geq 0$, the sphere of radius r and centre u, denoted by S (u,r), is the set $\{v \in GF(q)^n \mid d(u,v) \leq r\}$.

Theorem 1: A sphere of radius r ($0 \leq r \leq n$) contains exactly $\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{r}(q-1)^r$ vectors.

Theorem 2: A q-ary (n, k) code with M code words and minimum distance (2t +1) satisfies,

$$M \left\{ \binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{t}(q-1)^t \right\} \leq q^n$$

Definition 6: For binary codes, the Hamming bound will be

$$M \left\{ \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t} \right\} \leq 2^n$$

Definition 7: A perfect code is one which achieves the Hamming bound as,

$$M \left\{ \binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{t}(q-1)^t \right\} = q^n$$

1). Binary Hamming Codes: The binary hamming codes have the property that (n, k) = ($2^m - 1$, $2^m - 1 - m$) where 'm' is any positive integer. For example, for m=3, (7,4) code is the hamming code. The parity check matrix of an (n, k) code has n-k rows and n columns. For the binary (n, k) hamming code, the $n = 2^m - 1$ columns consist of all possible binary vectors with n-k = m elements, expect the all zero vector. The minimum hamming distance d_{min} of a (7, 4) hamming code is equal to 3, which implies that it is a single – error correcting code. Hamming codes are called as perfect codes.

2) Modified Binary Hamming Codes: By adding overall parity bit, an (n, k) hamming code can be modified to yield an (n+1, k) code with $d_{min} = 4$. Also, an (n, k) hamming code can be shortened to an (n- l, k – l) code by removing l columns of its parity check matrix H.

Definition 8: The formal definition of hamming code is given as below.

Let $n = (q^k – 1) / (q -1)$, Then the (n, k) hamming code over GF (q) is a code for which the parity check matrix has columns that are pair wise linearity independent over GF (q).

3) Limitations on code word block length 'n': According to shannon's theorem, if C (p) represents the capacity of a BSC with probability of bit error equal to 'p', then for arbitrarily low probability of symbol error, code rate R must be less than C (p). Even though the channel capacity provides an upper bound on the achievable code rate as R = k/n, evaluating a code exclusively against channel capacity may be misleading. The block length of the code, which translates directly into delay, is also an important parameter.

It has been observed that, if block length of the code is increased, the bounds on code rate are closer to channel capacity. However, longer block lengths imply longer delays in decoding. This is because decoding of a code word cannot begin until the receiving of entire code word. The maximum delay allowable is limited by practical constraints. For example, codeword with very large block lengths cannot be used in mobile radio communications where the packets of data are restricted to fewer bits.

4) Mixed Parity Codes: The (n, k) Mixed parity codes (MP Codes) are the resemblance of (n, k) binary hamming codes where the parity bits are dispersed among the information bits unlike the traditional method of appending the parity bits to the left most or right most sides of information bits. The purpose of deliberately dispersing the parity bit among the information bits is to scramble the originality of the information bits for crypto-encoding function without diluting the error control capability of the MP codes. It is the responsibility of the decoder to identify the position of parity bits to control over the error correction on received word vector 'v' after performing crypto-decoding.

This MP codes use the common character set, such as ASCII character set, for performing crypto-coding. This MP code will be a tool to design the crypto-coding system. In this paper, ASCII character set is considered for analysis. Because any character in ASCII character set can be segregated as BCD format as required for error correction technique. For example, the symbol 'A' is represented as 65 and 01000001 in decimal and binary formats respectively. Suppose, 01000001 are grouped in terms of 4 bit BCD code, there will be two 4 bit BCD codes as 0100 and 0001. Also, we may have more different set of two 4 bit BCD combinations out of this ASCII code such as 0000 : 1000, 1000 : 0010 and so on. This process can be called as BCD Coded ASCII (BCA).

In common, if any character in ASCII set is represented by $A = a_7a_6a_5a_4a_3a_2a_1a_0$, then the possible set of 4 bit BCD combinations are $a_7a_6a_5a_4 : a_3a_2a_1a_0$, $a_4a_5a_6a_7 : a_3a_2a_1a_0$, $a_7a_6a_5a_4 : a_0a_1a_2a_3$ and so on.

If (7, 4) hamming code is used to add the parity bits with each 4 bit BCA, a 4 bit BCA can be stretched to 7 bit longer by appending or dispersing 3 parity bits for error correction. An even or add parity is added for this whole 7 bits at the LSB and then there will be a new 8 bit code. This way, a two 8 bit code words can be generated for each ASCII character.

For example, if an ASCII code 01000001 is converted BCA as 0100: 0001, then applying (7, 4) hamming code technique, 0100 is converted as 0100111 and 0001 is converted as 0001011. Further, even parity is chosen to be placed at the MSB of resultant codes, then 0100111 becomes $A_1 = 00100111$ and 0001011 becomes $A_2 = 10001011$.

If A_1 and A_2 are interpreted as ASCII Coded BCD (ACB), 39 is the decimal value of ASCII character set for A_1 and its equivalent message is ''' (single quote). Similarly for A_2, after removing even parity bit at MSB, 11 is the decimal value of ASCII character set and its equivalent message is 'VT' (Vertical Tab \v).

For the same ASCII character 'A', if some other combination of two four bit BCD is interpreted, we will have two different ACB codes. Similarly, if parity bits are dispersed among the information bits, again there will be new sets of ACB codes. Further, some bits are intentionally inverted with the limits bounded by type of code chosen for adding parity bits. For example, (7, 4) hamming code can allow one bit inversion among a 7 bit code word that can be identified and corrected during crypto-decryption. These operations can be selectively performed by crypto-encoder based on the selective keys to ensure the security of transmission of information from one end to another.

III. CONSTRUCTION AND PROPERTIES OF MIXED PARITY CODES

Definition 9: If an intruder assumes the different combinations of meaningful message block as a correct message without having original key, that is known as message misinterpretation. For example, if the original message is "CODING DONE", the intruder gets the message as "THEORY BORN" by brute force attack and will end with that message due to message misinterpretation.

Definition 10: If there is an interconnection between one ASCII characters to another in the crypto-decoding process, the correct message cannot be retrieved without identifying the correct ASCII characters one by one. Hence, if an intruder finds the wrong ASCII character at one point of time, whole output block will be altered to have different combinations. This is known as message dissemination. For example, if the intruder gets the wrong character at the 3rd ASCII character in "CODING DONE" during brute force attack as "COP", he will not get the rests of correct combinations as "ING DONE" due to message dissemination effect.

Definition 11: Bit error penetration is the similar effect of dissemination effect where the realization of error is done between groups of bits of same length instead of ASCII character.

A. Criterions of Mixed Parity Code (MP code)

The main purpose of our work is to construct a code that possesses combined error correction and cryptographic properties. This code should not compromise the required error control and security strength. Hence three measures are developed to satisfy these requirements. They are (1) Criterion for security, (2) Criterion for error control and (3) Criterion for crypto-coding. A good crypto-coding must satisfy all these three measures.

1) Criterion for security: The proposed code will be mainly used for providing bit error penetration and message misinterpretation effects on huge section of the output block for an intruder without having correct key. Block number '**Ь**' is introduced to measure the message dissemination and bit error penetration rates. The block number of a crypto-encoding function Ø, with the input vector x and the output vector Ø(x) is defined as

$$Ь = \text{length of } Ø(x_i) \,/\, \text{length of } x_i \,, \quad (1)$$

where $i \in \{1,2,3,\ldots,(1-2k)\}$ and 'k' is the total number of bits per input message bits

2) Criterion for error control: The error control rate of the proposed code is determined by the pair wise hamming distance between the set of crypto-code words. If the Hamming distance is high value, it guarantees the large amount of error control rates for both error detection and error correction. The MP code must satisfy the following condition for reliable error correction capability.

If Ø(xi) is the crypto-code word generated by MP code of length n= **Ь**.k, (2)

$\min H_d \{f(x_i), f(x_j)\} = \min H_d \{f(Ø(x_i)), f(Ø(x_j))\}$, where $i \neq j$, $i, j \in \{1,2,3,\ldots, (1-2k)\}$ and H_d is the Hamming distance

In equation 2, $f(x_i)$ is the function that selects the number of bits equal to one character bits of ASCII code among the input xi and $f(Ø(x_i))$ is the function that selects the number of bits equal to one character bits of ASCII code among the output $Ø(x_i)$. In general, number of bits equal to one character bits of ASCII code is 7.

3) Criterion for crypto-coding: It is described through increasing the maximum number of probabilities for retrieving message bits without correct key and high value of hamming distance for crypto-code words with good error control capability. It can be accomplished by (i) wrapping the crypto-code word length by dispersing parity bits among message bits, (ii) intentional bit inversion over crypto-code words based on hamming distance, (iii) increasing the security reliability of crypto-coding by doing the bitwise Boolean XOR operation, bit rotation and bit permutation functions over the crypto-code words.

B. Mixed Parity Codes

Let us consider an [n, k,q] block code on the binary Galois field GF(q) of order 2, where n = r + k and n is number of bits in output crypto-code word, k is number of input message bits and r is number of parity bits Then the MP Codes are defined as follows.

Definition 12: An [**Ь**.k, k, q] code C where block number **Ь** = [(r/k) +1)] is said to be a Mixed Parity code with the encoding operation Ø , if it satisfies the following two conditions for all i and j with $i \neq j$, $i, j \in \{1,2,3,\ldots, (1-2^k)\}$;

1) From equation 1, **Ь** = $n/k \geq 2$ (3)

2) From equation 2, $\min H_d (f(m_i), f(m_j)) = \min H_d (f(C_i), f(C_j))$ where 'm' is the input message and 'C' is the Crypto-code word generated by the function $f(Ø(m))$

Equation 3 shows that block number '**Ь'** of Ø is lower bound by 2 for the existence of MP codes. Because minimum output length of a crypto-code word is to be double the length of input message bits for efficient crypto-coding of MP codes. For the construction of mixed parity code, this output block length (n) is achieved by mixing the parity bits with the input block length (k) such that the minimum bound of **Ь** is 2.

Block number **Ь** must be high value for good security of the PM Code. Also, it should be a real number to avoid concatenation of extra redundancy bits at crypto-codeword output for message interpretation.

C. Properties of MP Codes

In this section, we illustrate that the MP Codes posses the maximum possible message dissemination and error correction capability as desired in the design requirement.

1) Strength of code word dissemination: As per the definition of MP Codes, it has the block number **Ь** equal to n/k. Also, the crypto-coding operation Ø from 'k' bits into 'n' bits is done by the following consecutive operations: (1) performing error control functions such as parity bits generation of MP codes, (2) outputting the crypto-code word of length 'n' by random parity bits mixing with input message bits and (3) performing key based cryptographic functions such as bits permutations, bits rotations and Modulo-2 arithmetic functions over crypto-code words. Randomness in all these functions is the vital part of disseminating operation of proposed code. The strength of this disseminating power is proportional to the block number **Ь.** For example, if the input message bits length k is 63, there are 9 ASCII characters bits in k as each character having 7 binary bits. Then the output block length n is 126 where the block number is 2. If these bits are separated by 7 binary bits each, then there are 18 ASCII characters in the output block length 'n'.

2) Strength of error correction: The optimal error correction capability of MP Codes depends on the selection of existing channel code for construction of MP Codes.

Theorem 3: An [n,k,q] MP Code 'C' with encoding operation Ø is a Maximum Disseminating Code with number of correctable error 't' is directly proportional to **Ь(**Ø).

Proof: Generally, if $H_d(C_i, C_j) = h$, where 'h' is the hamming distance and $i \neq j$, $i, j \in \{1,2,3,\ldots, (1-2^n)\}$;

Then, error correction limit of (7, 4) Hamming code is $t = [(h-1)/2]=1$ since $h=3$. (4)

Equation 4 shows that 1 bit error correction is possible for every 7 bit codeword.

If the (56,28) MP code 'C' with **Ь(**Ø)= 2 is constructed using (7, 4) Hamming code as a base code, each codeword has 56 bits out of which 8 ASCII characters can be realized for every 7 bits. Therefore, 8 error corrections can be achieved among the 56 bits at the rate of 1 error correction for every 7 bits.

Then, error correction capacity of MP codes derived from (7, 4) hamming code is given as,

$[(n/7).t]$ where $n = (\mathbf{Ь}(Ø).k)$ (5)

This will lead to the probability of altering all the bits but limited to one bit per 7 symbols which is bound by chosen hamming code for construction of MP Codes. However, if error correcting capability 't' of chosen codes is further increased, then the probability of inverting the bits per set of symbols can be greatly increased.

3) Strength of crypto-coding: The potential in good crypto-coding based on MP Code depends on proper selection of existing channel code. Since the priority of our design is cryptography through error penetration and correction capabilities by mixed parity bits, the chosen code must posses the good message misinterpretation phenomenon on the crypto-code words of MP code. For example, if the input block is collection of ASCII values, hamming code will exhibit all the required properties of crypto-coding. Further, the strength of crypto-coding through MP Code can be increased by key based randomization in parity bit addition and bit inversion on the output bits of MP code. Also, if any crypto-coding operation on output block produces the meaningful message that will lead to the data misinterpretation to the intruder. This is an added advantage to the strength of crypto-coding. The strength of good MP codes depends on the process of resemblances of original message bits from the codeword of MP codes.

4) Existence of (n, k, q) MP code for the finite Galois Field of order q: The basic requirement for existence of MP Code is $n = [\mathbf{Ь}.k]$ where **Ь** is block number, 'n' is length of codeword and 'k' is length of message over Galois field of order 'q' [GF (q)]. The following considerations are valid for GF (q) for all MP code.

Definition 13: $q^x \geq q+1$ is valid for any $q > 1$ and $x \geq 1$, Then, there exist an (n, k, q^x) MP code with the condition $n > k > x$ for finite Galois field.

Definition 14: All the 2^k messages can always be assigned a codeword of length (**Ь**.k) such that all the codeword are in the domain of all the possible input messages of 2^k. This is one of the major requirements of crypto-coding for the purpose of message misinterpretation towards the cryptanalysis by the intruder.

If $(8, 4, 2^1)$ MP code is used where $2^k=2^4=16$ and $\mathbf{Ь} = 8 / 4 = 2$, all the 16 crypto-code words will assume 16 ASCII characters where each crypto-code word is one among the 128 combinations between 0-127 decimal values of ASCII character set.

Proof: we show that $[\mathbf{Ь}.(1- (r/n))] = 1$ where the factor $(1- (r/n))$ is the probability of existence of original message symbols among the total length of the output symbol 'n'. The probability factor (1- r/n) multiplied with block number **Ь** always yields the result 1 such that the function Ø produces a multiple number of message blocks in the output of MP Code. Again this will lead to the required data misinterpretation towards the cryptanalysis by the intruder.

By substituting $k = n – r$ in equation (3) which gives,

n = [**Ь** (n-r)] where 'r' is number of redundancy bits among 'n'. (6)

If equation (6) is rearranged , we will get {**Ь**. [1-(r/n)]} =1 (7)

Theorem 4: For a given [n,k,q] MP Code over GF(2) where n is one output block size and k is one input block size, if X is the total number of output block sizes of MP Code generated by the crypto-encoding function Ø where (n /**Ь**) = k, then X_j / k always produces 'm**'** number of input block size in the finite set of x ϵ { x_1 , x_2 , x_3,….,x_p} where p= $(1-2^k)$and j ϵ {1,2,3,…., $(1-2^n)$}. Also, 'm' is always divisible by the block number **Ь.**

Therefore, $f(Ø(x_i)= X_j= \{x_{i1} \| x_{i2} \| x_{i3} \| \ldots. x_{i\,m}\}$ (8)

where m= X_j / k and i ϵ $\{1,2,3,\ldots., (1-2^k)\}$.

For example, if two output blocks of length (X_j) 112 is generated by the (56, 28, 2^1) MP code,

then, m=112 /28=4 and m/ **Ь** =2.

D. Construction of MP codes

The major consideration for construction of MP Code mainly depends on it usage for crypto-coding. Since the MP Code will undergo traditional cryptographic processes such as bit permutation, bit rotation, bit wise Boolean XOR operation, it will show the security strength against well-known attacks such as plain text attack, cipher text attack, brute force attack. Also, the error correction capability of the MP code must play the dual role. If redundancy bits are not flipped purposefully at the sender side, the whole error correction capacity of MP code will be retained for receiver side to correct the errors occurred during the transmission of crypto-code words over noisy channel. But, if part of the redundancy bits is flipped purposefully so as to increase the message dissemination capacity at the sender side using key based functions, then the receiver side will have the reverse key functions to retrieve the original redundancy bits. Then the error correction technique is applied to restore the original message.

1) Choice of existing codes: Since the common message input format to computers is based on ASCII values whose binary symbol length is 7 for each character, the (7, 4) hamming code is chosen here to construct the MP Code.

TABLE III
Comparison of various codes for their error correction features

Type of code (1)	**Block size (n ,k)** (2)	**Galois field GF(q)** (3)	**Number of output bits in a codeword (n)** (4)	**Number of message bits (k)** (5)	**Number of Parity bits (n-k)** (6)	**Number of error correction bits of block size in column (2)** (7)	**Error correction efficiency w.r.t 'n' {[(7) / (4)] x 100]} %** (8)
Hamming code (Single error correction)	(7,4)	$GF(2^1)$	7	4	3	1	14.28571
BCH Code (Single error correction)	(15,11)	$GF(2^4)$	60	44	16	4	6.66667
BCH Code (Double error correction)	(15,7)	$GF(2^4)$	60	28	32	8	13.33333
Reed-Solomon Code (Single error correction)	(7,5)	$GF(2^3)$	21	15	6	3	14.28571
Reed-Solomon Code (Double error correction)	(15,11)	$GF(2^3)$	45	33	12	6	13.33333

The MP Codes can be constructed by using any one of the existing channel codes. However, the choice of selection depends on number of symbols in the input block, number of symbols in the output block, possession of cyclic and nonlinearity properties after adding redundancy bits, maximum number of bit penetration with minimum number of bit inversion. As for as MP code is concerned, the importance is given to plaintext dissemination and misinterpretation with parity bits mixing by key based function rather than simply the length of the output with parity bits during the outcome of encryption process.

Also, Table II shows that the selection of (7, 4) is the better choice among some of the other existing codes as for as specified selection of input symbol block length is concerned. Also, it reveals that if the behavior of the communication channel is known, choice of hamming code is better than any other commonly used codes in terms of required number of reduced redundancy bits for crypto-coding with specified length.

2) Method of making (56, 28) MP code from Hamming Code: The block size is so chosen that the output length of the block must be able to produce the meaningful ASCII characters by subdividing total length in terms of 7 symbols per characters. This is the required plaintext misinterpretation property at out crypto-coding technique. So, the total number of input bits must be divisible by both 4 and 7 as well as total number of output bits must be divisible by 7. Therefore, number of input binary symbols per encoding function Ø can be 28, 56, and 84… so on. The increase in input block size leads to the increase in probability of combinations of characters using output block size. If we choose, 4 ASCII characters for the encoding function Ø, then the input block size will be 28. Then, (7, 4) hamming code is used for generation of parity bits, there are 21 parity bits for each 4 bits of input bits. Now, the resultant bits are multiples of 7. That is, in our case, resultant bits are 49. Again another 7 redundancy bits can be generated such that one odd or even parity bit for every 7 symbols. This last 7 set of parity bits employs the vital role in bit inversion and rotation process in crypto-coding. Because, if we are able to retrieve the first generated 49 bits without any error at the decryption side, even though the whole 7 bits are inverted at encryption side, we will retrieve it using respective parity check algorithm. So, if this scrambled parity symbols block of 7 bits is effectively used for bit error penetration throughout the encryption process at crypto-coding, which will strengthen the overall security of the proposed MP code. Here we have generated 8 ASCII characters with code word size of 56 bits as the outcome of function Ø from the input of 4 ASCII characters with message size of 28 bits. So, the bit magnify number for the described example is 2. If the bit magnify number is further increased, the number of outcome of ASCII character also gets increased. This function will show the strength to the crypto-coding when the generated parity bits and ASCII characters are placed randomly among themselves to have message dissemination.

3) Error correction mechanism of MP codes: As illustrated in the Table I, Hamming code possesses the maximum efficiency with specified number of bits. However, it has the limitations on bulk error correction in single code word. But, randomly placed parity bits along with the message bits may show bulk error correction probability up to some extent over the controllable noisy channel or known communication channel. In our example, with the aid of Table II, we can conclude that there is the possibility of correcting maximum of 7 bits but limited to one bit per 7 binary symbols of first 49 parity mixed message bits. Remaining 7 parity bits show the strength to the bulk error correction as that can be corrected with the knowledge of correctly recovered first 49 bits.

Since the good crypto-coding requires the nonsystematic successive outputs, concatenation of parity bits to the message bits in MP codes need not be a systematic operation. So, these parity bits can be randomly placed in anywhere among the total length of output bits. But, only the knowledge of placement of parity bits is to be preserved such a way that it can be identified at the decoding process for retrieving original message from codeword or cipher text

E. Security of crypto-coding using MP codes

The code word output of the MP codes is separable into distinct words in terms of specified input symbol size. It provides the greater plaintext permutation. Further, if error correction capability of the MP code is decisively used to perform the selective bit inversion process, it will provide higher degree of non-linearity in the output of crypto-coding.

The procedure of parity bits mixing with message bits makes the MP code as one of most efficient tool for crypto-coding. For example, single codeword with 7 bits of (7, 4) hamming code will have 3 parity bits and 4 message bits. If these 3 parity bits are placed in between the message bits with different combinations, the total number of combinations is 210. This number of combinations can be further increased by increasing input length size. Therefore, if key round is used to make these parity mixing combinations to preserve the reverse process at the decryption, this property of MP codes provides greater data misinterpretation for the cryptanalysis.

As described in the section III.C, the in-built error correction technique of MP codes can be trickily used to strength the crypto-coding algorithm. Although, if the length of the output block size is large enough, some of the mixed parity bits can be deliberately inverted to penetrate further data manipulation and rest of the mixed parity bits can be left out for overcoming the noisy communication channel. However, number of bits utilized

for these two purposes depends on choice of the base code for the construction of MP code, input message block size and output codeword block size of selected MP code.

If the parity mixing, bit inversion, bit rotation and output block segregation in terms of input block size are efficiently performed with the help of key rounds as required by cryptography, the traditional method of substitution boxes for bit permutation can be removed. The alternative for the substitution boxes is one of the major criteria for the present cryptography algorithm, as this technique requires larger look up table for high through put and occupies large amount of memory size hardware implementation of traditional algorithms.

Since the process of mixed parity bits provides the large number of combinations with minimum amount of bits, it shows the security strength against Known Plaintext Attack. Also, inclusion of bit inversion at encryption process and error correction at the decryption process with specified block size increases the probability of getting erroneous messages during Known cipher Attack. These two security properties collectively showing the strength to another well-known attack called Brute Force Attack which is mainly based on searching with all possible keys. Because, a single key can provide more number of combinations of message text for different crypto-coding functions of MP codes such as parity mixing, bit inversion, bit rotation and output block segregation for the specified set of block. This will lead to the computationally infeasible process with Brute Force Attack to retrieve the original message block with the stipulated time period as required by the present cryptography algorithm.

F. Factors influenced by MP codes for good crypto-coding

The following factors are to be mainly considered for the design of cryptographically secured block cipher with high rate of error resilience using crypto-coding.

(1) Choice of existing code based on maximum error correcting capability with fixed length of input and output block size, (2) Choice of input symbol based on character set of plaintext to be relevant to the output block size of chosen code (3) Proper positioning/mixing of the parity bits in the plaintext with key based preservation for achieving high error control reliability over noisy channel and (4) Round key based Boolean functions with bit rotations for penetrating non linearity in cipher text

IV. ANALYSIS OF MP CODES FOR DIFFERENT BLOCK SIZES

The strength of crypto-coding using proposed MP code depends on the probability of getting different messages of fixed length by (1) formulating the relationship between set of input messages and set of output messages, (2) mixing the maximum possible parity bits with message bits and (3) inverting some of the output bits limited to the error correction capabilities of chosen base code for making MP Code.

In our work, we have chosen ASCII code for inputting message to crypto-coding system. This code has 128 characters set with each of 7 bit length. If the number of input binary symbols to each encoding functions Ø is chosen as 28, the block size of MP code is (56, 28).

Further, (7, 4) Hamming code is chosen as the base code for construction of (56, 28) MP code. So, there are 4 input characters and 8 output characters which are segregated in terms of input character length. As listed in the Table 1, if one bit is inverted for each 7 bit of single character size so as to retrieve the originality later using appropriate error control algorithm of chosen code, there are 8 different bits can be inverted among the total output of 56 bits in our chosen MP code.

If 128 ASCII characters set is considered for making input message, then the probability of the cryptanalysis function for retrieving at least one of the original characters among the 8 different characters of output becomes 1/128 (0.0078125<<1). Also, the probability of the cryptanalysis function for retrieving all the 8 original characters is equal to $1/128^8$ (1.38777×10^{-17}) which shows the computational hardness to restore the combination of original characters even with the small block size of 56 bits.

The Table III illustrates the Statistical analysis of two different MP codes for cryptanalysis. These MP codes are constructed using different base codes of different block size as illustrated in Table 1.These two codes are so chosen since they only provide the basic requirement for choice of base code to construct the MP codes. That is, chosen block size of the input message relevant to base code must be divisible by the length (total number of bits) of the single character in the input message set to have a block number '**Ь**' as real number.

As our desired message set is ASCII code of 7 bit characters, the input message block sizes (56,28) from (7,4) hamming code with 7 input characters and (70,35) from (7,5) Reed-Solomon Code with 15 input characters are chosen for comparative analysis. Both of these MP codes have the block number '**Ь**' equal to 2.

Figure 5 depicts the realistic analysis of computational hardness of two different MP codes against cryptanalysis by Brute Force Attack. It clearly shows that the minimum amount of characters in the message set with small input block size will have less computational complexity.

TABLE IIIII
Statistical analysis of two different MP codes for crypto-coding

Base Code with block size	(n,k) MP Code with 'b' = 2		No. of ASCII characters in 'n'	No. of ASCII characters in 'k'	Probability (p) of retrieving original message size of 'k' with fixed no. of characters 'N' for input message set. $p= (1/N)^k$	
	No. of input bits (k)	No. of output bits (n)			N=26 (Alphabets)	N=36 (Alphanumeric)
(7,4) Hamming code (Single error correction)	28	56	4	8	4.78865E-12	3.5447E-13
	56	112	8	16	2.29312E-23	1.2565E-25
	84	168	12	24	1.09809E-34	4.4539E-38
	112	224	16	32	5.25839E-46	1.5788E-50
	140	**280**	**20**	**40**	**2.51806E-57**	**5.5963E-63**
	168	336	24	48	1.20581E-68	1.9837E-75
	196	392	28	56	5.77421E-80	7.0317E-88
	224	448	32	64	2.76507E-91	2.493E-100
	252	504	36	72	1.3241E-102	8.835E-113
	280	**560**	**40**	**80**	**6.3406E-114**	**3.132E-125**
(7,5) Reed-Solomon Code (Single error correction)	35	70	5	10	7.0838E-15	2.7351E-16
	70	140	10	20	5.01803E-29	7.4808E-32
	105	210	15	30	3.55467E-43	2.0461E-47
	140	**280**	**20**	**40**	**2.51806E-57**	**5.5963E-63**
	175	350	25	50	1.78374E-71	1.5306E-78
	210	420	30	60	1.26357E-85	4.1865E-94
	245	490	35	70	8.9509E-100	1.145E-109
	280	**560**	**40**	**80**	**6.3406E-114**	**3.132E-125**
	315	630	45	90	4.4916E-128	8.566E-141
	350	700	50	100	3.1817E-142	2.343E-156

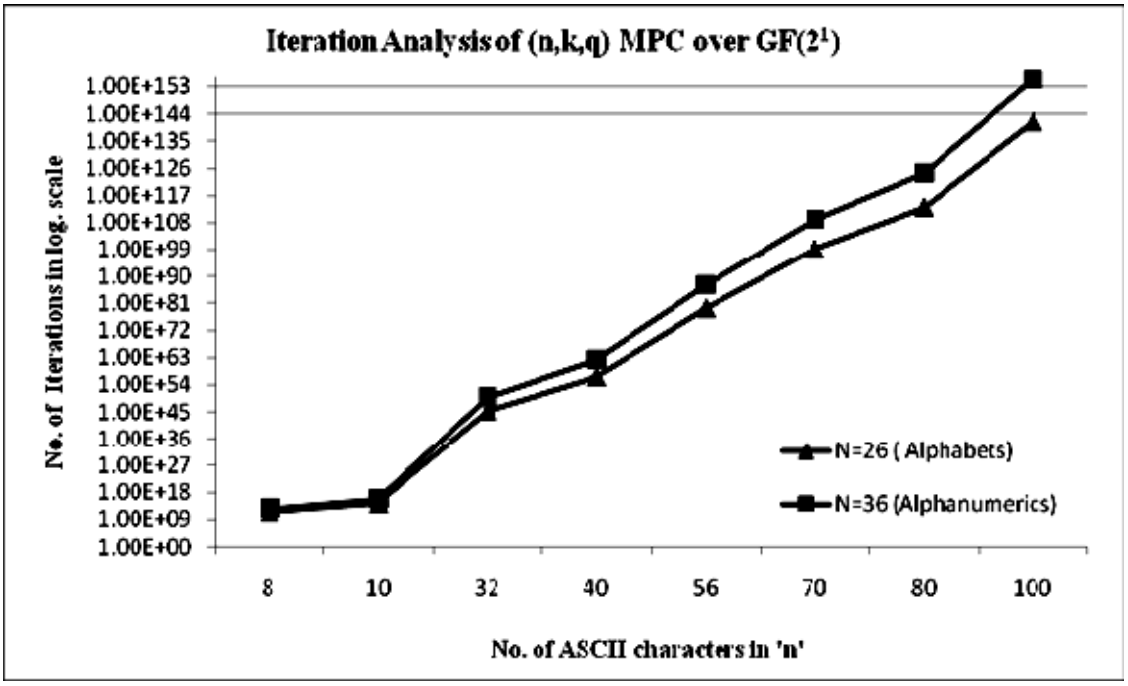

Fig. 5. Analysis of iteration based computational hardness of MP codes for crypto-coding

However, even with the less amount of increase in characters of message set provides high level of computational hardness in retrieving the original message by searching all possible combinations of characters of specified length 'k'. Also, there can be some tradeoff between choices of total number of characters 'N' in input message set and total number of characters Nc of entire plaintext for crypto-coding to maintain the computational hardness against cryptanalysis. Hence, the input message set must be chosen such a way that 'N' is to be high for lower amount of Nc and vice versa.

V. Conclusion

A newly developed Mixed Parity Code (MPC) with its properties and applications were described for crypto-coding technique. The bit magnify number was introduced to deal with the adoptability of the proposed MP Code to be used as a tool for efficient implementation of crypto-coding algorithm. Plaintext dissemination measured by block number '**Ь'** for data misinterpretation and error resilience measured by minimum distance between code words were described. It has been shown that the choice of existing code to construct the MP code depends on its error correcting capacity in terms of minimal block size. Properties and consideration for the MP code were described by the three different criteria. Further, the mechanism of using MP code for constructing efficient block cipher was expressed. The possibility of dual role, namely intentional bit error penetration at encryption and unknown bit error correction at decryption, of MP Code was explained to increase the security strength against some of the well-known attacks. Two different statistical analyses of MP codes, based on the probability and Iteration techniques, were provided for showing strength of MP code in crypto-coding against some cryptanalysis. Finally, a relationship between total number of characters 'N' in input message set and total number of characters N_c of whole plaintext for crypto-coding using MP codes was accomplished for maintaining the computational hardness against brute force attack cryptanalysis.

Acknowledgment

The Author thanks the Management and staff members of department of Electrical and Electronics Engineering, St.Peter's University, Chennai, India, for their support and providing necessary arrangement for doing my research work and for successfully crafting this paper.

References

[1] MacWilliams, F. J. and N. J. A. Sloane, "The theory of error correcting codes I and II", Amsterdam: North-Holland Publishing Co. North-Holland Mathematical Library, Vol. 16, 1977.
[2] Wicker, S. BError, "Control systems for digital communication and storage", Upper Saddle River, NJ, USA: Prentice-Hall, Inc.,1995.
[3] Stinson, D, "Cryptography: Theory and Practice", Second Edition.CRC/C&H, 2002.
[4] Van Tilborg, H, "Coding theory at work in cryptology and vice versa", in: Handbook of Coding Theory (ed. V.S. Pless and W.C. Huffman), North-Holland, pp.1195-1227, 1998.
[5] Chetan Nanjunda Mathur, Karthik Narayan, and K. P. Subbalakshmi, "On the Design of Error-Correcting Ciphers", Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2006, Article ID 42871.
[6] Rajashri Khanai, Dr. G. H. Kulkarni, "Performance Analysis of Conventional Crypto-coding", International Journal of Latest Trends in Computing, Volume 2, Issue 1, March 2011
[7] McEliece, R.,"A Publick Key Cryptosystem Based on Algebraic Codes", DNS Progress Reports 42-44, NASA Jet Propulsion Labaratory,1978.
[8] Berlekamp, E., R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding Problems", IEEE Transactions on Information Theory,1978.
[9] Jordan,J.P, "A variant of a public key cryptosystem based on Goppa Codes", SIGACT News 15(1), 61–66, 1983.
[10] Park, C. S, "Improving code rate of McEliece's public-key cryptosystem", Electronics Letters 25(21),1466–1467,1989.
[11] Lin, M. C. and H. L. Fu, "Information rate of McEliece's publickey cryptosystem", Electronics Letters, 26(1), 16–18. ,1990.
[12] Sendrier, N, "Efficient generation of binary words of given weight", In: Fifth IMA Conference on Cryptography and Coding, 1995.
[13] Berson, T. A, "Failure of the McEliece public-key cryptosystem under message-resend and related-message attack", In: Advances in Cryptology-CRYPTO '97, Lecture notes in computer science. 1997.
[14] Sun, H.-M., "Private-key cryptosystem based on burst-error correcting codes", Electronics Letters 33, 2035–2036,1997.
[15] Stern, J., "A new identification scheme based on syndrome decoding", Advances in Cryptology,CRPTO'93, 0773,1993.
[16] Safavi-Naini, R. S. and J. R. Seberry, "Error-correcting codes for authentication and subliminal Channels", IEEE Transactions on Information Theory 37, 13–17,1991.
[17] Xinmei,W, "Digital signature scheme based on error-correcting codes", Electronics Letters 26, 898–899,1990.
[18] Hwang, T. and T. Rao, "Secret Error-Correcting Codes (SECC)", In: Advances in Cryptography, Crypto 1988.
[19] Preparata, F, "A class of optimum nonlinear double-error correcting codes", Inform. Control 13, 378-400.,1968.
[20] Zeng, K., C.-H. Yang, and T. R. N. Rao, "Cryptanalysis of the Hwang-Rao secret error correcting code Schemes", In: Third International Conference in Information and Communications Security, ICICS 2001, Vol. 2229.,2001.

AUTHOR PROFILE

B. SENTHILKUMAR received his B.E. degree (1997) in Electrical and Electronics Engg., from University of Madras and M.Tech. degree (2002) in VLSI DESIGN, from Sastra University, India. Now, he is working as Associate Professor, in the department of Electrical and Electronics Engineering at VELTECH (Owned by R.S. Trust) Engineering College, Avadi, Chennai. Presently, he is pursuing doctoral degree programme in St. Peter's University, Chennai in Cryptography.