New SEC-DED-DAEC Codes for Multiple Bit Upsets Mitigation in Memory

Zhu Ming, Xiao Li Yi
Microelectronics Center
Harbin Institute of Technology
Harbin, China
zhumingbaby@sina.com; xiaoly@hit.edu.cn

Luo Hong Wei
National Key Laboratory of Science and Technology on Reliability Physics and Application Technology of Electrical Component
Guangzhou, China

***Abstract*—Nowadays, multiple bit upsets (MBUs) have been widely investigated in memories. Conventional single error correction and double error detection (SEC-DED) codes are capable of correcting one error and detecting all possible double errors. However, they may not provide adequate protection against MBUs. This paper proposes new single-error-correction, double-error-detection double-adjacent-error-correction (SEC-DED-DAEC) codes to mitigate radiation or noise source induced MBUs in memories. The proposed SEC-DED-DAEC codes are obtained from conventional SEC-DED codes according to the mathematics model established in this paper. They can detect and correct all adjacent double bit errors and assure a lower miscorrection probability for non-adjacent double bit errors compared with other SEC-DED-DAEC codes. Furthermore, the redundancy bits of the proposed scheme are the same as those of conventional SEC-DED codes. This means that the increase of correct-capability do not cause additional hardware overhead for the memory system. Finally, the experiment results reveal that the proposed scheme reduces the miscorrection probability of non-adjacent double bit errors by 12% compared to the best known SEC-DED-DAEC codes. Moreover, compared to the well known BCH codes, the proposed scheme reduces 40% hardware redundancy and keeps an acceptable reliability.**

Keywords-memroy; memroy reliability; SEC-DED-DAEC codes; MBUs

I. INTRODUCTION

As technology size and supply voltage decrease, integrated circuits (IC) are more prone to transient errors than ever before [1]. More and more memories affected by multiple bit upsets (MBUs) are observed in the recent research. The ionizing effect of high-energy particle, neutron and proton can cause MBUs in memories [2]. The high-energy particle can directly affect several adjacent memory cells. Proton and neutron have no electric charge, but they can interact with the silicon nucleus and then produce secondary ionizing particles to induce MBUs. In addition, some noise sources (e.g., electromagnetic interference–EMI, ground bounce and so on) also can provoke similar memory degradation.

Hamming codes and Hsiao codes are well known as single error correction and double error detection (SEC-DED) codes. Because these codes require only a small number of redundancy bits for error correction, their delay, power consumption and area overheads are low. Hamming codes and Hsiao codes are capable of correcting one error and detecting all possible double errors. However, they may not provide adequate protection against MBUs.

A general approach to mitigate MBUs is multibit error correction codes (MECCs). The Bose Chaudhuri Hocquenghem (BCH) codes [3], Reed-Solomon (RS) codes [4], Euclidean Geometry Low Density Parity Check (EG-LDPC) codes [5], Two-dimensional error codes [6,7] and Mix codes [8] can deal with multiple errors in memories. The general drawbacks of these methods are complex encoding and decoding. They will bring more latency and power consumption overheads compared with SEC-DED codes. Moreover, these methods need a large number of redundancy bits, which remarkably increase the area overhead of memory systems.

According to the results of radiation experiment [9,10], the probability of adjacent double bit errors is much higher than other multiple bit errors. Reference [11] and [12] proposed the effective SEC-DED-DAEC codes by selectively constructing the check matrix of SEC-DED code. They employ the same number of check bits as SEC-DED codes commonly used. Therefore, the SEC-DED-DAEC codes proposed by [11] and [12] have low hardware overhead in error correction. However, some non-adjacent double bit error may be treated as adjacent double bit error by mistake, which results in the miscorrection.

The proposed SEC-DED-DAEC codes are obtained from conventional SEC-DED codes basing on the established mathematics model in this paper. They can detect and correct all adjacent double bit errors and guarantee a lower miscorrection probability for non-adjacent double bit errors compared to other SEC-DED-DAEC codes. Furthermore, the proposed scheme remarkably reduces redundancy bits compared to other MECCs (e.g., BCH codes) without obvious reliability loss. The MECC methodology proposed in this paper constructs the efficient SEC-DED-DAEC codes, which is different from the ones described in [11] and [12]. Firstly, a mathematics model of SEC-DED-DAEC codes is proposed. Secondly, through the mathematics model, the proposed scheme offers a new structure of the check matrix which can improve the correcting capability of ECC by reducing the miscorrection probability of non-adjacent double errors. Then, some restricted conditions and general rules are presented to simplify the search process of the

978-1-4577-0170-2/11/$26.00 ©2011 IEEE

check matrix. Finally, a pseudo-greedy algorithm is used to search the optimal check matrix.

This paper is divided into following sections. In section 2, conventional SEC-DED codes are introduced. In section 3, the proposed SEC-DED-DAEC codes are presented and the constructing process of the check matrix is described. In section 4, encoder and decoder circuits are implemented and the correcting capability is analyzed. Finally, some conclusions are presented in section 5.

II. CONVENTIONAL SEC-DED CODES

SEC-DED codes belong to binary linear block codes. They can correct one error and detect all possible double errors. The proposed SEC-DED-DAEC codes are obtained from conventional SEC-DED codes. Therefore, the same characteristics of encoding and decoding can be found between them. Generally, the systematic generator matrix obtained from equation (1) is used in encoder.

$$G_{\text{systematic}} = \left[P_{k\times(n-k)} \cdot I_{k\times k} \right] \tag{1}$$

where P is a $k\times(n\text{-}k)$ matrix and I is an identity matrix. The check matrix H can be obtained by converting the systematic matrix $G_{\text{systematic}}$ as shown in equation (2).

$$H = \left[P^T \cdot I_{(n-k)} \right] \tag{2}$$

where P^T is the transpose of P matrix. Let $u=(u_0, u_1,\ldots,u_{k-1})$ be the k-bit information vector and $v=(v_0,v_1,\ldots,v_{n-1})$ be the n-bit codeword. The encoder can be implemented by XOR logic from equation (3). The encoded data consists of information bits followed by parity bits.

$$v = u \cdot G_{\text{systematic}} \tag{3}$$

The decoding operation is implemented by the following vector-matrix multiplication:

$$S = (v+e)\cdot H^T = v\cdot H^T + e\cdot H^T = e\cdot H^T \tag{4}$$

where S is an $(n\text{-}k)$-bit vector and is called the syndrome vector. v is the codeword and e is the error pattern. Through equations (1-3), there is $v\cdot H^T = 0$. Therefore, the error pattern e can be decided by the syndrome vector S. If the syndrome vector is zero, there is no error in memory. If the syndrome vector is nonzero, the errors can be checked and then corrected according to the corresponding syndrome bits S_i.

A set of errors e_1, e_2, …, e_i are correctable if all the syndromes $S(e_1)$, $S(e_2)$,…, $S(e_i)$ are distinct. Because the syndromes of some 2-bit errors are undistinguishable, conventional SEC-DED codes can only correct 1-bit error. The syndrome for a single bit error at the bit position i is the same as the i-th column of the check matrix H. Previous SEC-DED-DAEC codes can correct adjacent 2-bit error, but they still have many sharable syndromes between adjacent and non-adjacent 2-bit error. The syndrome for a double bit error can be obtained by the exclusive-or (XOR) operation of two corresponding columns of the check matrix H.

III. PROPOSED SEC-DED-DAEC CODES

Firstly, a mathematics model of SEC-DED-DAEC codes is presented in this section. Basing on this model, new SEC-DED-DAEC codes with high correcting capability are proposed. Then, some structure characteristics of the proposed SEC-DED-DAEC codes are offered. Finally, a pseudo-greedy algorithm is used to search the optimal check matrix.

A. Mathematics Model

Before proposing new SEC-DED-DAEC codes, a mathematics model of SEC-DED-DAEC codes will be introduced firstly. The model can be used as a theoretical basis to construct the check matrix of the proposed SEC-DED-DAEC codes.

The check matrix H can be written as

$$H = \left[C_1, C_2, \cdots, C_k, I_1, \cdots, I_{(n-k)} \right] \tag{5}$$

where C is the column vector of the check matrix and I is the identity matrix. It is assumed that the column vector sets with 3, 4, 5, 6 and 7-weight are $a^3[C_{n-k}^3]$, $a^4[C_{n-k}^4]$, $a^5[C_{n-k}^5]$, $a^6[C_{n-k}^6]$ and $a^7[C_{n-k}^7]$, respectively. For example, in the 16-bit data check matrix, the number of 3-weight vector is 20 (i.e., $a^3[20]$) and the number of 5-weight vector is 6 (i.e., $a^5[6]$). As a result, the check matrix H can be composed of these vectors. The column vector sets of 16-bit and 32-bit data are shown in table I.

TABLE I. THE COLUMN VECTOR SET FOR 16-BIT AND 32-BIT DATA

Column vector sets	16-bit data		32-bit data	
	Symbol	***Number***	***Symbol***	***Number***
3-weight	$a^3[20]$	20	$a^3[35]$	35
4-weight	$a^4[15]$	15	$a^4[35]$	35
5-weight	$a^5[6]$	6	$a^5[21]$	21
6-weight	$a^6[1]$	1	$a^6[7]$	7
7-weight	—	0	$a^7[1]$	1

If the above vectors satisfy equations (6-8), the check matrix of SEC-DED-DAEC codes can be obtained. It can correct all adjacent double bit errors and minimize the miscorrection probability of non-adjacent double errors.

$$C_i \oplus C_{i-1} \neq C_j \oplus C_{j-1} \quad (1\le i\le k,\ 1\le j\le k,\ i\neq j) \tag{6}$$

$$C_i \oplus C_{i-1} \neq C_i \neq I_1, \cdots, \neq I_{(n-k)} \quad (1\le i\le k) \tag{7}$$

$$\text{Min}\sum\left(C_i \oplus C_{i-1} = C_i \oplus C_j\right) \quad (1\le i\le k,\ 1\le j\le k,\ i\neq j) \tag{8}$$

Proof: It is assumed that C is the column vector of the check matrix and it does not satisfy equations (6-8). Because the syndromes obtained from the check matrix H can correct 1-bit and adjacent 2-bit errors, in order to satisfy equation (4), the column vector C is related with 1-bit error pattern and the XOR result of adjacent two column vector is related with adjacent 2-bit error pattern. Then, equations (9) and (10) can be obtained.

$$s(i) = C_i \quad (1\le i\le k) \tag{9}$$

$$s(i,i+1) = C_i \oplus C_{i+1} \quad (1\le i\le k) \tag{10}$$

Because adjacent 2-bit errors can be corrected by SEC-DED-DAEC codes, their syndromes in adjacent 2-bit error

pattern should be distinct. So there is equation (11).

$$s(i,i+1) \neq s(j,j+1) \neq s(i) \neq s(j) \quad (1 \leq i \leq k,\ 1 \leq j \leq k,\ i \neq j) \quad (11)$$

$s(i) \neq s(j)$ can be achieved since the vectors in $a^3[C_{n-k}^3]$, $a^4[C_{n-k}^4]$, $a^5[C_{n-k}^5]$, $a^6[C_{n-k}^6]$ and $a^7[C_{n-k}^7]$ are different with each other. Through equations (9) and (10), equation (11) can be written as

$$C_i \oplus C_{i-1} \neq C_j \oplus C_{j-1} \neq C_i \neq C_j \quad (1 \leq i \leq k,\ 1 \leq j \leq k,\ i \neq j) \quad (12)$$

In order to guarantee equation (11) be valid, equation (12) will be established. However, equation (12) is contradicted with the initial assumption. Therefore, the column vector *C* must satisfy equations (6-8). Q.E.D.

Consequently, constructing check matrix *H* can be transformed to obtain the optimal solution from $a^3[C_{n-k}^3]$, $a^4[C_{n-k}^4]$, $a^5[C_{n-k}^5]$, $a^6[C_{n-k}^6]$ and $a^7[C_{n-k}^7]$.

B. Codes Structure

A new structure of the check matrix is proposed in this section. Especially, the condition 5 and 6 are quite different from the previous codes, which can further improve the correcting capability of ECC.

1) All columns are non-zero.

2) All columns are distinct.

3) The XOR result of any two columns cannot equal the column vector of the check matrix *H*.

4) The XOR result of any adjacent two columns cannot equal each other.

5) The weight of the column vector should be as high as possible.

6) The sharable syndromes between adjacent and non-adjacent 2-bit error should be minimized.

Condition 1 ensures that all single bit errors cause a nonzero syndrome so that single bit errors can be detected. Condition 2 guarantees that the syndromes of all single bit errors are distinguishable to correct all single bit errors. Condition 3 restricts that the syndromes of all double bit errors are different from those of the single bit errors. Therefore, all double bit errors can be detected. In order to correct all adjacent double bit errors, condition 4 is associated with condition 2 to ensure that the syndrome of any adjacent double bit error is different from others.

Different from the previous research in [11] and [12], more attention is paid to condition 5 and 6 in this paper. The proposed SEC-DED-DAEC codes can correct all adjacent double bit errors. However, some syndromes of adjacent and non-adjacent double bit errors are the same. Therefore, non-adjacent double bit errors may be treated as adjacent double bit error, resulting in the miscorrection. According to reference [12], the check matrix containing at least one vector of even weight can reduce the miscorrection probability of triple bit error. In fact, the vector of even weight added in the check matrix leads to the increase of column vector weight. By investigating the relationship between the check matrix and syndrome vectors, it can be found that properly increasing the weight of the column vector can improve the diversity of the syndrome vectors. Wider syndrome vector range has positive influence in reducing the miscorrection probability. Therefore, in the proposed SEC-DED-DAEC codes, not only the vector of even weight but also the vector of odd weight can be selected to increase the weight of the column vector. When conditions (1-4) are satisfied, condition 5 and 6 can ensure that the miscorrection probability for non-adjacent double bit errors is minimized.

C. Constructing Rule

In the proposed SEC-DED-DAEC codes, the correcting capability will be affected by the different orders and weights of the column vector. For an ($m \times n$) check matrix, there are $2^{m \times n}$ possible column vector combinations. For example, a 16-bit data with (22×6) check matrix has $2^{132} = 5.4 \times 10^{39}$ possible searches. Therefore, for the ordinary data width (e.g., 16-bit and 32-bit) in memory, there are too many possible searches to obtain the optimal check matrix. An exhaustive search approach is incompetent to construct codes. Through the mathematics model offered by the above section, the search process can be simplified by determining and removing certain columns early.

When constructing the16-bit check matrix, through the mathematics model of SEC-DED-DAEC codes, it is found that 6-weight column vectors cannot coexist with 5-weight column vectors due to their XOR results equaling the identity matrix. 2-weight and 4-weight column vectors cannot be chosen, since 3-weight syndromes generated through the XOR computations between 1-weight column vector and both of them may cause the optional scope of column vectors to decrease.

For the search process of the 32-bit check matrix, similarly, 7-weight column vectors cannot coexist with 6-weight column vectors since their XOR results are equal to the identity matrix. For the same reason, 6-weight and 5-weight column vectors cannot coexist either. If the check matrix includes 7-weight column vector, then the 5-weight column vector cannot contain two successive zero. Otherwise, their XOR results will share the same syndrome with the adjacent two bits.

By establishing the 16-bit and 32-bit data check matrix, some general rules for constructing the check matrix of SEC-DED-DAEC codes can be deduced. Selecting the vector of odd weight can furthest increase the weight of whole check matrix. The 3-weight syndrome obtained from any two column vectors through XOR computation should be avoided, because it will have negative effect on the optional scope of column vectors. Diversifying the XOR results of two column vectors (i.e., the weight of XOR results distributes in a wide range) can minimize the impact of the same syndrome shared by the different errors.

D. Search Algorithm

A pseudo-greedy algorithm can be used to search the above check matrix *H* as shown in Fig.1. Aiming at minimum sharing syndromes, new columns are added one-by-one. Then, the order of the column vector is changed until the check matrix with the optimal correcting capability is obtained. Basing on the above constructing rules, only the

odd-weight vector sets $a^3[C_{n-k}^3]$, $a^5[C_{n-k}^5]$ and $a^7[C_{n-k}^7]$ are selected to construct the check matrix of the proposed SEC-DED-DAEC codes.

Parameter definition
A: the XOR result of any two columns which is the same as other vector.
B: the XOR result of any adjacent two columns which is equal to each other.
C: the sharable syndromes between adjacent and non-adjacent 2-bit error.
D: the maximal amount of 3-weight vector obtained from XOR operation of any two columns.
validVecSet: the valid column vector set.
currentCol: selected check matrix.

Search procedure
1. Constructing (n-k) identity matrix with the 1-weight vectors.
2. while (currentCol < n) {
   validVecSet = 0;
   while (3≤weight ≤ n-k) {
3. Select (n-k)-weight column vectors
   validVecSet = (n-k)-weight columns;
   currentCol++;
4. Select (weigh-1) columns vectors
   validVecSet [weight-1 columns]= {};
   Check for A and B
   if (! A && ! B)
   select Min C (validVecSet)
   currentCol++;
   weight--;
   if (weight>3 && D=1)
   validVecSet =0;
   weight--;
   else (A or B=1)
   backtracking;
   validVecSet =0;
   weight--;
   continue; }}
5. Count the number of C in currentCol
6. Change the order of columns vectors
   currentCol_temp= {};
   If (C_temp≤C)
   check matrix *H* =currentCol_temp;

Figure 1. Pseudo-greedy search algorithm.

The detailed search process can be described as the following: Firstly, basing on the data width in memory, the length and width of the check matrix *H* are decided. Secondly, constructing the check matrix starts with the identity matrix by selecting the vectors of weight "1". Then, the column vectors with high weight have priority to construct the check matrix according to the conditions (1-4). If the selected column vectors cannot reach the length of the check matrix *H*, the weight of column vector will be reduced and the lower weight will be assigned until the desired check matrix length is obtained. Finally, according to the condition (6), the order of the column vector is changed to minimize the miscorrection probability of non-adjacent double bit errors.

A search result of the check matrix is shown in Fig.2. One 5-weight vector is contained in the 16-bit data check matrix. One 7-weight vector and fourteen 5-weight vectors are contained in the 32-bit data check matrix.

$$\begin{bmatrix}
1&1&1&1&0&1&1&0&1&1&0&1&1&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&1&0&0&1&0&0&0&0&1&0&1&0&1&0&0&0&0\\
0&1&0&0&1&1&1&1&0&1&0&1&0&0&1&1&0&0&1&0&0&0\\
1&1&1&1&1&0&0&1&0&0&1&1&0&1&0&1&0&0&0&1&0&0\\
0&1&1&0&0&0&0&1&0&1&1&0&1&0&1&0&0&0&0&0&1&0\\
1&1&0&0&1&0&1&0&1&0&1&0&1&1&1&0&0&0&0&0&0&1
\end{bmatrix}$$

Figure 2. The check matrix of the proposed (22,16) code.

IV. Experimental Results

Our proposed scheme has been implemented in Verilog for typical memory word sizes of 16-bit. The design has been simulated with ModelSim and tested for functionality by given various inputs. Synopsys Design Compiler has been used for synthesizing the encoder and decoder circuits targeted to the SMIC 0.18um standard cell library. Then, the logic gate and the correcting capability of the proposed scheme are compared with those of the latest SEC-DED-DAEC codes offered by [11] and [12]. Finally, the mean time to failure (MTTF) of the memory protected by different MECC schemes is estimated.

A. Circuit Implement

After obtaining the check matrix, the encoder and decoder can be implemented according to equations (3) and (4). The basic encoder and decoder circuits are shown in Fig. 3 and Fig. 4. The encoder circuit is implemented by six XOR arrays. The number of input ports in XOR gate is equal to the row vector weight minus one.

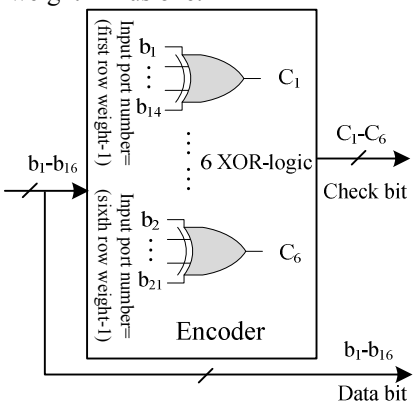

Figure 3. The 16-bit encoder circuit for the proposed scheme.

The decoder consists of the syndrome generating circuit, error pattern estimating circuit and error correcting circuit. The syndrome generating circuit is implemented by six XOR gates to produce 6-bit syndrome S_i. The error pattern estimating circuit distinguishes 1-bit, 2-bit or no error

according to the syndrome S_i. If there are errors in memory, the error correcting circuit inverts corresponding error information and exports corrected data basing on the output result of the error pattern estimating circuit.

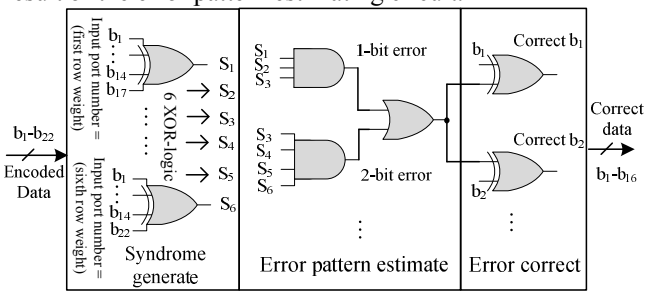

Figure 4. The16-bit decoder circuit for the proposed scheme.

B. *Correcting Capability Analysis*

An XOR gate with n inputs can be implemented by (n-1) XOR gates with 2 inputs. Table II shows the number of 2-input XOR gates in the encoder/decoder and the sharable syndromes between adjacent and non-adjacent 2-bit error. The increase of column vector weight leads to the increase of XOR gates. It can be seen from table II that the small increase of the encoder and decoder hardware overheads trade off higher protection level, which is useful for the high reliability memory. The miscorrection probability of non-adjacent double bit errors can be obtained from equation (13). The proposed codes for 16 and 32 information bits reduce the miscorrection probability of non-adjacent double bit errors by 1.7% and 12.0% compared to the best previously known codes, respectively.

$$\text{Miscorrection Probability} = \frac{\text{Sharable Syndromes}}{C_n^2 - (n-1)} \qquad (13)$$

TABLE II. PROPOSED SEC-DED-DAEC CODES IN COMPARISON WITH OTHER CODES

(n,k)	Codes	2-input XOR gates	Sharable syndromes
(22,16)	Dutta [11]	48	118
	Richter [12]	48	118
	Proposed SEC-DED-DAEC	50	116
(39,32)	Dutta [11]	96	379
	Richter [12]	115	274
	Proposed SEC-DED-DAEC	128	241

C. *Reliability and Redundancy Analysis*

MTTF is usually used as a metric parameter to assess the memory reliability. By using MTTF, it can be found whether the proposed scheme meets reliability requirement under given radiation conditions. In the previous research [13], the influential factor of memory reliability, such as the overlap of multiple bit errors, is considered in analyzing MTTF. It produces a more precise analysis in the calculation of MTTF for memory systems under MBUs. The reliability model of memories can be given by equation (14) and the detailed analysis process can be found in reference [13].

$$MTTF\,|_{mbu}^{\lambda} \cong \frac{1}{\lambda} \cdot \sqrt{\frac{\pi \cdot M}{2 \cdot \sum_{i+j>L} \left[p_i \cdot p_j \cdot \left(1 - \frac{L}{N}\right) \right]}} \qquad (14)$$

where M is the number of words and λ represents the event arrival rate. N is the number of bits (N includes data bits and redundancy bits) and L is the correct-capability. P_i and P_j are the probability of i errors and j errors. $\sum_{i+j>L} p_i \cdot p_j$ is the probability combination whose total number of errors is more than L.

BCH codes have been well known as one of MECCs. They can correct any 2-bit error in memory. The reliability of Hamming codes, BCH codes and the proposed scheme has been analyzed under certain radiation conditions. Assume that the event arrival rate is 10^{-4} per word. The errors that arrive to memories are assigned to a Poisson distribution, which is representative of real radiation environments [14]. The MTTF versus different M under MBUs=2 is depicted in Fig. 5.

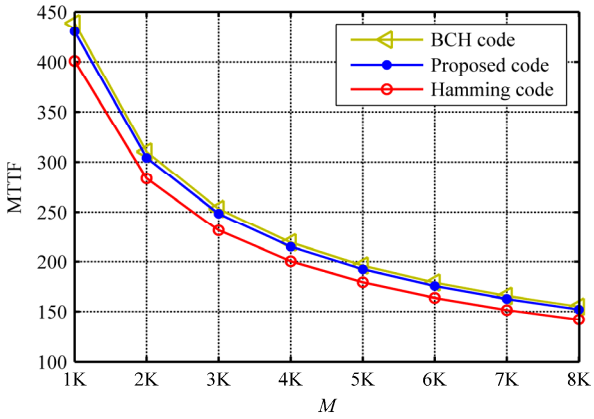

Figure 5. MTTF versus word M for a 16-bit memory with MBUs=2.

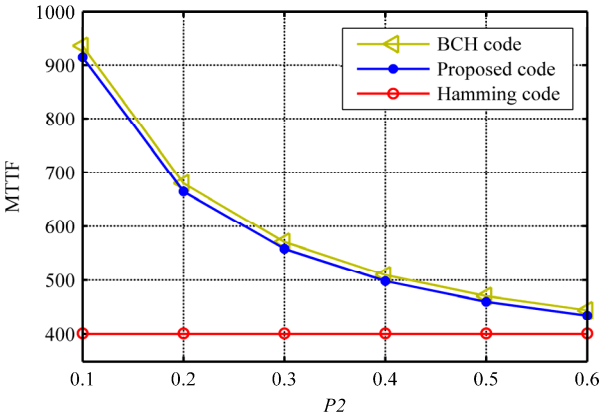

Figure 6. MTTF versus 2-bit error probability for a 16-bit memory with MBUs=2, M=1K.

It can be seen that the MTTF of the proposed scheme is close to BCH codes and higher than Hamming codes. The MTTF versus 2-bit error probability under MBUs=2 and *M*=1K is depicted in Fig. 6. When 2-bit error is not frequent in memory system (e.g., *P*2=0.1), the MTTF of the proposed scheme is 2.2% decreased compared to BCH codes, but it is 128.2% higher than Hamming codes.

Because memory cells take up more than 90% area of the whole memory system, the number of redundancy bits will directly determine the area overhead of the memory system. Table III shows the redundancy bits of BCH codes and the proposed scheme. It can be seen that the redundancy bits of the proposed SEC-DED-DAEC codes for 16-bit and 32-bit data decreases by 40% and 41%, respectively, compared to that of BCH codes.

TABLE III. THE REDUNDANCY BITS OF SEC-DED-DAEC CODES AND BCH CODES

Data width	**Redundancy bit (n-k)**	
	Proposed SEC-DED-DAEC codes	***BCH codes***
16 bit	6	10
32 bit	7	12

BCH codes can correct any 2-bit errors, while the proposed SEC-DED-DAEC codes can correct any adjacent 2-bit errors. However, when the energy of radiation is not very high and adjacent 2-bit errors are dominant, the proposed SEC-DED-DAEC codes reduce 40% hardware redundancy at the cost of very low reliability loss. The hardware redundancy of the proposed scheme is the same as that of Hamming codes, but the MTTF of the proposed scheme is 128.2% higher than that of Hamming codes.

In addition, comparing with BCH codes, the proposed scheme can easily combine with bit interleaving to provide greater flexibility for memory reliability due to its redundancy overhead is close to conventional SEC-DED codes. In this situation, every two adjacent bits are assigned to different logical words, which can reduce interleaving distance.

V. CONCLUSION

This paper proposes the SEC-DED-DAEC codes with a new structure to assure the reliability of memory in presence of MBUs. The redundancy bits of the proposed scheme are the same as those of the well known Hamming codes, while it can detect and correct all adjacent double bit errors. Through heuristic search, the proposed codes have a lower miscorrection probability for non-adjacent double bit errors compared to other SEC-DED-DAEC codes. The mathematics model for constructing SEC-DED-DAEC codes with high correcting capability is also proposed. Although the number of XOR gates increases, the proposed scheme has a lower miscorrection probability, which is very helpful to design a high reliability memory system. Furthermore, when the probability of multiple bit error is not very high, the proposed scheme reduces 40% hardware redundancy compared to BCH codes while the MTTF does not obviously decrease. Therefore, the proposed scheme can be well applied to the memory system in presence of MBUs under low radiation energy. It can guarantee the reliability of memory with low redundancy overhead.

ACKNOWLEDGMENT

This work was supported by the Opening Project of National Key Laboratory of Science and Technology on Reliability Physics and Application Technology of Electrical Component (No.ZHD200903).

REFERENCES

[1] R.C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," IEEE Trans. Dev. Mater. Reliab., vol. 5, no. 3, pp. 305–316, Sep. 2005.

[2] G. C. Cardarilli, A. Leandri, P. Marinucci, M. Ottavi, S. Pontarelli, M. Re, A. Salsano, "Design of a fault tolerant solid state mass memory," IEEE Trans. Rel., vol. 52, no. 4, pp. 476–491, Dec. 2003.

[3] R. Naseer, J. Draper, "Parallel double error correcting code design to mitigate multi-bit upsets in SRAMs," in Proc. 34th Euro. Solid-State Circuits Conf., Edinburgh, U.K., 2008, pp. 222–225.

[4] G. Neuberger, D. L. Kastensmidt, and R. Reis, "An automatic technique for optimizing Reed-Solomon codes to improve fault tolerance in memories," IEEE Des. Test Comput., vol. 22, no. 1, pp. 50–58, Jan. 2005.

[5] H. Naeimi, A. DeHon, "Fault secure encoder and decoder for NanoMemory applications," IEEE Trans. VLSI Syst., vol. 17, no. 4, pp. 473–486, Apr. 2009.

[6] C. Argyrides, H.R. Zarandi, D.K. Pradhan, "Matrix codes multiple bit upsets tolerant method for SRAM memories," 22nd IEEE Int. Symp. Defect and Fault-Tolerance in VLSI Syst., 2007. DFT 07, pp. 340–348, Sept. 2007.

[7] C. Argyrides, D.K. Pradhan, T. Kocak, "Matrix codes for reliable and cost efficient memory chips," IEEE Trans. VLSI Syst., vol. 19, no. 3, pp. 420–428, Mar. 2011.

[8] M. Zhu, L. Y. Xiao, L. L. Song, Y. J. Zhang, H. W. Luo, "New Mix codes for multiple bit upsets mitigation in fault-secure memories," Microelectronics Journal, vol. 42, no. 3, pp. 553-561, Mar. 2011.

[9] Y. Yahagi, H. Yamaguchi, E. Ibe, H. Kameyama, M. Sato, T. Akioka, S. Yamamoto, "A novel feature of neutron-induced multi-cell upsets in 130 and 180 nm SRAMs," IEEE Trans. Nucl. Sci., vol. 54, no. 4, pp. 1030–1036, Aug. 2007.

[10] D. Radaelli, H. Puchner, S. Wong, S. Daniel, "Investigation of multi-bit upsets in a 150 nm technology SRAM device," IEEE Trans. Nucl. Sci., vol. 52, no. 6, pp. 2433–2437, Dec. 2005.

[11] A. Dutta, N. A. Touba, "Multiple bit upset tolerant memory using a selective cycle avoidance based SEC-DED-DAEC code," 25th IEEE Int. Symp.VLSI Test, Berkeley, C.A., 2007, pp. 129–135.

[12] M. Richter, K. Oberlaenderz, M. Goessel, "New linear SEC-DED codes with reduced triple error miscorrection probability," 14th IEEE Int. Symp. On-Line Testing, Rhodes, Greece, 2008, pp. 129–135.

[13] M. Zhu, L. Y. Xiao, C. Liu, J. W. Zhang, "Reliability of memories protected by multibit error correction codes against MBUs," IEEE Trans. Nucl. Sci., vol. 58, no. 1, pp. 289–295, Feb. 2011.

[14] P. Reviriego, J.A. Maestro, "Study of the effects of multibit error correction codes on the reliability of memories in the presence of MBUs," IEEE Trans. Dev. Mater. Reliab., vol. 9, no. 1, pp. 31–39, Mar. 2009.