

> (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014

# An Efficient Design of Fully Fault Tolerant Communication by FSD-ECC with Low Power Consumption and More Security

B. Sai Bhargavi<sup>1</sup>, P. Praveen Kumar<sup>2</sup>

PG(VLSI) Student, Department of ECE, QIS College of Engineering and Technology, Prakasam, Andhra Pradesh,

India<sup>1</sup>

Assistant Professor, Department of ECE, QIS College of Engineering and Technology, Prakasam, Andhra Pradesh,

India<sup>2</sup>

ABSTRACT: This paper presents "an advanced fully fault tolerant communication by FSD-ECC with low power consumption and more security" To prevent soft errors from causing data corruption, memories are typically protected with error correction codes. An advanced error correction codes are used when an additional protection is needed. a fully fault-tolerant memory architecture that is capable of tolerating hardware or software errors not only in the memory bits but also in the supporting logic including the ECC encoder and corrector with low power consumption and more security. This project uses a Euclidean Geometry codes, SEA (Scalable Encryprion Algorithm). Hence proved that these codes are part of a new subset of ECCs that have FSD(fault secure detector - error correcting code). This is useful as majority logic decoding can be implemented serially with simple hardware but requires a large decoding time. For memory applications, this increases the memory access time. The method detects whether a word has errors in the first iterations of majority logic decoding, and when there are no errors the decoding ends without completing the rest of the iterations. Since most words in a memory will be error-free, the average decoding time is greatly reduced. In this brief, we study the application of a similar technique to a class of Euclidean geometry low density parity check (EG-LDPC) codes that are one step majority logic decodable. The results obtained show that the method is also effective for EG-LDPC codes. Other than this LDPC codes satisfies a new, restricted definition for ECCs which guarantees that the ECC codeword has an appropriate redundancy structure such that, it can detect multiple errors occurring in both the stored codeword in memory and the surrounding circuitries. which makes the area overhead minimal and keeps the extra power consumption low. Extensive simulation results are given to accurately estimate the probability of error detection for different code sizes

### I. INTRODUCTION

Memory cells have been protected from soft errors for more than a decade, due to the increase in soft error rate in logic circuits, the encoder and decoder circuitry around the memory blocks have become susceptible to soft errors as well and must also be protected. A fault- tolerant nano-scale memory architecture which tolerates transient faults both in the storage unit and in the supporting logic (i.e., encoder, decoder, corrector and detector circuitries) is introduced.

**Transient faults**: When a node in the system loses its effective charge due to ionized particle hit or various sources of noises, it may cause the value of a node to be flipped in the circuit. However, the error does not permanently change the circuit, and it only generates a faulty bit value at the node that can last for one or few cycles. The transient fault rate is the probability that a single node loses its correct value during one clock cycle. Feature-size scaling, faster clock cycles and lower power designs increase the transient fault rate. Feature-size scaling and voltage level reduction shrinks the amount of critical charges holding logical state on each node; this in turn makes each node more susceptible to transient faults, e.g., an ionized particle strike has higher likelihood of being fatal as the critical charge is reduced in a node, which may cause a glitch or bit-flip. Furthermore operating at higher clock frequency increases the probability that a glitch in the signal is latched and propagated as an erroneous value throughout the circuit. However, many



(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

transient faults will not be latched. Some of the latched data may not be relevant to machine operation and there will be no perceivable error in the program operation. Hence, the effective error rate of a large combinational circuit needs to be dreaded Particularly, a class of error-correcting codes (ECCs) that guarantees the existence of a simple fault-tolerant detector design is identified. This class satisfies a new, restricted definition for ECCs which guarantees that the ECC codeword has an appropriate redundancy structure such that it can detect multiple errors occurring in both the stored codeword in memory and the surrounding circuitries. This type of error-correcting codes are called as fault-secure detector capable ECCs (FSD-ECC). The parity-check Matrix of an FSD-ECC has a particular structure that the decoder circuit, generated from the parity-check Matrix, is Fault-Secure. The ECCs identified in this class is close to optimal in rate and distance, suggesting we can achieve this property without sacrificing traditional ECC metrics. The faultsecure detection unit is used to design a fault-tolerant encoder and corrector by monitoring their outputs. If a detector detects an error in either of these units, that unit must repeat the operation to generate the correct output vector. Using this retry technique, potential transient errors in the encoder are corrected and provide a fully fault-tolerant memory system.

### **1.1. Single Event Upsets (SEU)**

Nowadays, single event upsets (SEUs) altering digital circuits are becoming a bigger concern for memory applications. A single event upset (SEU) is a change of state caused by ions or electro-magnetic radiation striking a sensitive node in a micro-electronic device, such as in a microprocessor, semiconductor memory, or power transistors. The state change is a result of the free charge created by ionization in or close to an important node of a logic element (e.g. memory "bit"). The error in device output or operation caused as a result of the strike is called an SEU or a soft error. The SEU itself is not considered permanently damaging to the transistor's or circuits' functionality unlike the case of single event latchup (SEL), single event gate rupture (SEGR), or single event burnout (SEB). These are all examples of a general class of radiation effects in electronic devices called single event effects. Terrestrial SEU arise due to cosmic particles colliding with atoms in the atmosphere, creating cascades or showers of neutrons and protons, which in turn may interact with electronics. At deep sub-micrometre geometries, this affects semiconductor devices in the atmosphere. If the radiation event is of a very high energy, more than a single bit maybe affected, creating Multi Bit Upset (MBU). For reliable communication, errors must be detected and corrected. Error detection is the way to find out that is a data is correct or incorrect. Reed-Muller is one of the methods of multiple error detection in blocks for digital communications signals. Soft error reliability is to employ Error Detection and Correction (EDAC) techniques or Error Correction Codes (ECC) is employed. Various error detection techniques are used to avoid the soft error. One of the methods is majority logic decoder which used to detect and correct the error in simple way. The drawback of this method is increase the average latency of the decoding process because it depends on the size of the code. Another method is syndrome fault detector which increase the power consumption because it is complex module. Majority Logic Decoder/Detector (MLDD) is used for avoiding those drawbacks of existing methods. For terrestrial radiation environments where there is a low soft error rate (SER), codes like single error correction and double error detection (SEC-DED), are a good solution, due to their low encoding and decoding complexity. However, as a consequence of augmenting integration densities, there is an increase in the number of soft errors, which produces the need for higher error correction capabilities.

### **1.1.1 Error correction edit**

It suppose a *single* bit error has occurred. Mathematically, we can write modulo 2, where  $\mathbf{e}_i$  is the unit vector, that is, a zero vector with a 1 in the  $\mathbf{i}^{th}$ , counting from 1.



Thus the above expression signifies a single bit error in the  $i^{th}$  place. Now, if we multiply this vector by **H**:

 $\mathbf{Hr} = \mathbf{H}(\mathbf{x} + \mathbf{e}_i) = \mathbf{Hx} + \mathbf{He}_i$ Since **x** is the transmitted data, it is without error, and as a result, the product of **H** and **x** is zero. Thus  $\mathbf{Hx} + \mathbf{He}_i = \mathbf{0} + \mathbf{He}_i = \mathbf{He}_i$ 



(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

Now, the product of **H** with the  $i^{th}$  standard basis vector picks out that column of **H**, we know the error occurs in the place where this column of **H** occurs.

For example, suppose we have introduced a bit error on bit #5

$$\mathbf{r} = \mathbf{x} + \mathbf{e}_{5} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

A bit error on bit 5 causes bad parity in the red and green circles The diagram to the right shows the bit error (shown in blue text) and the bad parity created (shown in red text) in the red and green circles. The bit error can be detected by computing the parity of the red, green, and blue circles. If a bad parity is detected then the data bit that overlaps *only* the bad parity circles is the bit with the error. In the above example, the red & green circles have bad parity so the bit corresponding to the intersection of red & green but not blue indicates the errored bit. Now,

$$\mathbf{z} = \mathbf{H}\mathbf{r} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

which corresponds to the fifth column of **H**. Furthermore, the general algorithm used (*see Hamming code # General algorithm*) was intentional in its construction so that the syndrome of 101 corresponds to the binary value of 5, which indicates the fifth bit was corrupted. Thus, an error has been detected in bit 5, and can be corrected (simply flip or negate its value): This corrected received value indeed, now, matches the transmitted value **x** from above.

$$\mathbf{r}_{\text{reconstruction}} = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \end{pmatrix}$$

### 1.1.2 Decoding edit

Once the received vector has been determined to be error-free or corrected if an error occurred (assuming only zero or one bit errors are possible) then the received data needs to be decoded back into the original 4 bits.

### 1.2 ECC with Fault Secure Detector

Single-error fault-tolerant decoder and encoder circuits for Reed-Solomon codes have been suggested in. In this work the encoder is protected with parity-prediction and parity checker. The decoder is protected by adding a code checker (detector) block and a hamming distance counter block to count the number of error bits at the output of the decoder. If the code checker detects a non-codeword, then the error in the decoder is detected. If the code checker detects a codeword but the hamming-distance counter indicate a non-zero error, then an error is also detected. Here we propose a multiple-error fault tolerant decoder and encoder that is general enough for any decoder and encoder implementation and for any kind of ECC that satisfies the restricted ECC definition. The restricted ECC definition which guarantees a fault-secure detector capable ECC (FSD-ECC) is as follows: Let C be an ECC with minimum distance d. C is FSD-ECC if it can detect any combination of overall d - 1 or fewer errors in the received codeword and in the detector circuitry.

The following proof depends on the fact that any single error in the detector circuitry can corrupt at most one output (one syndrome bit). This can be easily satisfied for any type of circuitry by implementing the circuit in such a way that



(An ISO 3297: 2007 Certified Organization)

## Vol. 3, Issue 12, December 2014

no logic element is shared among multiple output bits, therefore any single error in the circuit corrupt at most one output (one syndrome bit).

**Proof:** The core of a detector circuitry is a multiplier that implements the vector-matrix multiply of the received vector and the parity-check matrix to generate the syndrome vector. Now if e errors strike the received code-vector the syndrome weight of the error pattern is at least d - e from the assumption. Furthermore, the maximum number of tolerable errors in the whole system is d - 1 and e errors already exist in the encoded vector, therefore the maximum number of errors that can strike in the detector circuitry is d - 1 - e. From the above note, this many errors can corrupt at most d - 1 - e syndrome bit, which in worst case leaves at least one non-zero syndrome bit and therefore detects the errors. Q.E.D The difference between FSD-ECC and normal ECC is the demand on syndrome weight: i.e., a normal ECC demands non-zero syndrome weight while FSD-ECC demands  $\geq d - e$ .

### II. LOW DENSITY PARITY CHECK CODES

In information theory, a **low-density parity-check** (**LDPC**) **code** is a linear error correcting code, a method of transmitting a message over a noisy transmission channel.<sup>[1][2]</sup> An LDPC is constructed using a sparse bipartite graph.<sup>[3]</sup> LDPC codes are capacity-approaching codes, which means that practical constructions exist that allow the noise threshold to be set very close (or even *arbitrarily* close on the BEC) to the theoretical maximum (the Shannon limit) for a symmetric memory less channel. The noise threshold defines an upper bound for the channel noise, up to which the probability of lost information can be made as small as desired. Using iterative belief propagation techniques, LDPC codes can be decoded in time linear to their block length. LDPC codes are finding increasing use in applications requiring reliable and highly efficient information transfer over bandwidth or return channel-constrained links in the presence of corrupting noise. Implementation of LDPC codes has lagged behind that of other codes, notably turbo codes. The fundamental patent for Turbo Codes expired on August 29, 2013.LDPC codes are also known as **Gallager codes**, in honor of Robert G. Gallager, who developed the LDPC concept in his doctoral dissertation at the Massachusetts Institute of Technology in 1960.

In 2003, an LDPC code beat six turbo codes to become the error correcting code in the new DVB-S2 standard for the satellite transmission of digital television.<sup>[9]</sup> The DVB-S2 selection committee made decoder complexity estimates for the Turbo Code proposals using a much less efficient serial decoder architecture rather than a parallel decoder architecture. This forced the Turbo Code proposals to use frame sizes on the order of one half the frame size of the LDPC proposals. In 2008, LDPC beat convolutional turbo codes as the forward error correction (FEC) system for the ITU-T G.hn standard.<sup>[10]</sup>G.hn chose LDPC coded over turbo codes because of their lower decoding complexity (especially when operating at data rates close to 1.0 Gbit/s) and because the proposed turbo codes exhibited a significant error floor at the desired range of operation.<sup>[11]</sup> LDPC is also used for 10GBase-T Ethernet, which sends data at 10 gigabits per second over twisted-pair cables. As of 2009, LDPC codes are also part of the Wi-Fi 802.11 standard as an optional part of 802.11n and 802.11ac, in the High Throughput (HT) PHY specification.Some OFDM systems add an additional outer error correction that fixes the occasional errors (the "error floor") that get past the LDPC correction inner code even at low bit error rates. For example: The Reed-Solomon code with LDPC Coded Modulation (RS-LCM) uses a Reed-Solomon outer code.<sup>[13]</sup> The DVB-S2, the DVB-T2 and the DVB-C2 standards all use aBCH code outer code to mop up residual errors after LDPC decoding.

### 2.1 Design structure of Ring counter with clock gated by CG-element

As the extra RS- flip flops still serve as loading of the clock signal and demand more than necessary clock power, the idea is to replace the RS-flip flop by a CG-element which greatly reduce the power consumption. Additionally, replacing D-flip flops by DET flip-flops reduce the clock rate to half and thus also reduce the power consumption on the clock signal.



(An ISO 3297: 2007 Certified Organization)

## Vol. 3, Issue 12, December 2014





Fig.1 Ring counter with clock gated by CG-elements

Fig. 2 Ring counter with clock gated by RS-flip flop

# Block / Initialize1 Initialize2 CLK<sub>1</sub> Modified Ring Counter

### 2.2 Modified Ring Counter

In this paper for improving the power consumption and efficient operation of clock pulse a modified ring counter is used see fig above

### 2.3 Clock Gated D Flip-Flop

An assumption is made that all transitions on Q (output data) should be synchronized with an active clock edge. Data miscommunication errors might be caused due to asynchronous data sampling. The CG (clock gating control) signal is activated when there is a transition in D (input data). Flip-flop is triggered when internal clock pulse is given. The C (internal gated clock) signal maintains its value instead of generating an active edge in the gating mode. C changes after the transition on CLK in the non-gating mode. Asynchronous data transition may occur, if D changes (i.e., it enters the non-gating mode) while C is not equal to CLK and is shown as spikes at the output. synchronous Sampling in the Gated Double Edge-Triggered Flip-Flop with Transmission Gate (G\_DETFF) The flip-flop is built with the Latch-Mux structure using transmission gates as in Fig 1. The two data paths are connected in parallel. The upper data path transmits data on the rising edge and the lower path transmits data on the falling edge. These two data paths alternatively monitor the input and provide the output, which means that the input is always preloaded into the flip-flop.



(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

Instead of generating a pulse for every transition, the clockgating part was designed to toggle C, whenever the data input is changed and also to eliminate power consumption for unnecessary transitions. During the gating periods, C preserves the last used value before being gated. When compared to other clock gating techniques, G\_DETFF uses the clock signal in a more efficient way that is better suited for DETFF



Fig.3 Wang's design G DETFF. (a) DETFF part. (b) Clock-gating part

### III. SYSTEM OVERVIEW

The memory system which can tolerate errors in any part of the system, including the storage unit, encoder and corrector circuit, using the fault-secure detector is shown below. There is a fault secure detector that can detect any combination of errors in the received code-word along with errors in the detector circuit. This fault-secure detector can verify the correctness of the encoder and corrector operation. An overview of the proposed fault secure encoder and decoder is shown in figure 3.1, and is as described below



Fig.4 Block diagram of Fault Secure Encoder and Decoder

Block diagram of Fault Secure Encoder and Decoder. The information bits are fed into the encoder to encode the information vector, and the fault secure detector of the encoder verifies the validity of the encoded vector. If the detector detects any error, the encoding operation must be redone to generate the correct code-word. The code-word is then stored in the memory. Later during operation, the stored codeword will be retrieved from the memory unit. Since the code-word is susceptible to transient faults while it is stored in the memory, the retrieved code-word must be fed into the detector to detect any potential error and possibly to the correct or recover any erroneous bits. In this design



(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

the corrector circuit has parallel structure and is implemented fully pipelined similar to the detector. All the memory words are pipelined through the corrector and then detector, therefore, one corrected memory word is generated every cycle. The detector following the corrector, would raise an error-detection flag only if a transient fault occurs in the corrector or detector circuitry. Due to the relative lower transient fault rate compared to the permanent defects and the relative small corrector and detector circuitry, this happens with low frequency. Therefore, the potential throughput loss of this system is low.

### **3.1 Design Structure:**

In this section the design structure of the encoder, corrector, and detector units of the proposed fault secure encoder and decoder is provided. Encoder: An n-bit code-word c, which encodes k-bit information vector i is generated by multiplying the k-bit information vector with  $k \times n$  bit generator matrix G, i.e.,  $c = i \cdot G$ . Figure 3.2 shows the generator matrix of (15, 7) EG-LDPC code. all the rows of the matrix are cyclic shifts of the first row. This cyclic code generation does not generate a systematic code and the information bits must be decoded from the encoded vector, which is not desirable for our fault-tolerant approach due to the further complication and delay that it adds to the operation. The generator matrix of any cyclic code can be converted into systematic form (G = [I : X])

### **3.2 DET (Double edge triggered flip-flops):**

Double-edge-triggered (DET) flip-flops are utilized to reduce the operating frequency by half The logic construction of a double-edge-triggered (DET) flip-flop, which can receive input signal at two levels the clock, is analyzed and a new circuit design of CMOS DET In this paper, we propose to use double-edge-triggered (DET) flip-flops instead of traditional DFFs in the ring counter to halve the operating clock frequency. Double edge-triggered flipflops are becoming a popular technique for lowpower designs since they effectively enable a halving of the clock frequency. The paper by Hossain etal showed that while a single-edge triggered flipflop can be implemented by two transparent latches in series, a double edge-triggered flipflop can be implemented by two transparent latches in parallel.

### 3.3 C ELEMENT:

The Muller C-element, or Muller C-gate, is a commonly used asynchronous logic component originally designed by David E. Muller. It applies logical operations on the inputs and has hysteresis. The output of the C-element reflects the inputs when the states of all inputs match. The output then remains in this state until the inputs all transition to the other state. This model can be extended to the Asymmetric C-element where some inputs only effect the operation in one of the transitions (positive or negative). The figure shows the gate-level and transistor-level implementations and symbol of the C-element.



Fig 5: C- Element Table Corrector

Fig.6 Serial one-step majority logic corrector structure

One-step majority-logic correction is a fast and relatively compact error-correcting technique. There is a limited class of ECCs that are one-step-majority correctable which include type-I two-dimensional EG-LDPC. In this section, we present a brief review of this correcting technique. Then we show the one step majority-logic corrector for EG-LDPC codes.

### **3.4 Power Reports**

The power reports of the existing and proposed systems are as shown below. The table 1 shows the power report of the existing system and the table 9.2 shows the power report of the proposed system. The power consumed by the existing



(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

system is 914mw and the power consumed by the proposed system is 229mw and the difference between the both existing and proposed power consumptions is of 39% difference. The tables are below here

Power summary:	I(mA)	P(mW)
Total estimated power consumption:		914
Vccint 1.20V:	287	345
Vccaux 2.50V:	53	132
Vcco25 2.50V:	175	438
Clocks:	11	14
Inputs:	0	0
Logic:	7	9
Vcco25	175	438
Signals:	192	230

### Table 1: Power Report of Proposed system

#### **3.5 Fault Secure Detector:**

The core of the detector operation is to generate the syndrome vector, which is basically implementing the following vector-matrix multiplication on the received encoded vector c and parity-check matrix H. C T H = S The C-element stores its previous state with two cross-coupled inverters, similar to an SRAM cell. One of the inverters is weaker than the rest of the circuit, so it can be overpowered by the pull-up and pull-down networks.

# **3.6 Serial one-step majority logic corrector structure Simulation Results Synthesis Reports:**





(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

# 3.7 RTL Schematic:



#### 3.8 wave form of the corrector



38% power reduction is observed in proposed technique with more security

### IV. CONCLUSION

In this report, a fully fault-tolerant memory system that is capable of tolerating errors not only in the memory but also in the supporting logic is designed. The LDPC codes are proved as part of a new subset of FSD-ECCs. Using these FSDs a fault-tolerant encoder and corrector is designed. Here for low power we have used the C elements and provided security for the fault tolerant system by using the Scalable Encryption Algorithm to encrypt and Decrypt the data.

#### REFERENCES

[1] C. W. Slayman, "Cache and memory error detection, correction, and reduction techniques for terrestrial servers and workstations," *IEEE Trans. Device Mater. Reliabil.*, vol. 5, no. 3, pp. 397–404, Sep. 2005.

[2] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," *IEEE Trans. Device Mater. Reliabil.*, vol. 5, no. 3, pp. 301–316, Sep. 2005.

[3] J. von Neumann, "Probabilistic logics and synthesis of reliable organisms from unreliable components," Automata Studies, pp. 43–98, 1956.

[4] M. A. Bajura *et al.*, "Models and algorithmic limits for an ECC-based approach to hardening sub-100-nm SRAMs," *IEEE Trans. Nucl. Sci.*, vol. 54, no. 4, pp. 935–945, Aug. 2007.



(An ISO 3297: 2007 Certified Organization)

### Vol. 3, Issue 12, December 2014

[5] R. Naseer and J. Draper, "DEC ECC design to improve memory reliability in sub-100 nm technologies," in *Proc. IEEE ICECS*, 2008, pp. 586–589.

[6] S. Lin and D. J. Costello, Error Control Coding, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 2004.

[7] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," IRE Trans. Inf. Theory, vol. IT-4, pp. 38–49, 1954.

[8] J. L. Massey, Threshold Decoding. Cambridge, MA: MIT Press, 1963.

[9] S. Ghosh and P. D. Lincoln, "Low-density parity check codes for error correction in nanoscale memory," SRI Comput. Sci. Lab. Tech. Rep. CSL-0703, 2007.

[10] B. Vasic and S. K. Chilappagari, "An information theoretical framework for analysis and design of nanoscale fault-tolerant memories based on low-density parity-check codes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 11, pp. 2438–2446, Nov. 2007.

[11] H. Naeimi and A. DeHon, "Fault secure encoder and decoder for NanoMemory applications," *IEEE Trans. Very Large Scale Integr. (VLSI)* Syst., vol. 17, no. 4, pp. 473–486, Apr. 2009.

[12] Y. Kato and T. Morita, "Error correction circuit using difference-set cyclic code," in Proc. ASP-DAC, 2003, pp. 585-586.

[13] T. Kuroda, M. Takada, T. Isobe, and O. Yamada, "Transmission scheme of high-capacity FM multiplex broadcasting system," *IEEE Trans. Broadcasting*, vol. 42, no. 3, pp. 245–250, Sep. 1996.

[14] O. Yamada, "Development of an error-correction method for data packet multiplexed with TV signals," *IEEE Trans. Commun.*, vol. COM-35, no. 1, pp. 21–31, Jan. 1987.

[15] P. Ankolekar, S. Rosner, R. Isaac, and J. Bredow, "Multi-bit error correction methods for latency-contrained flash memory systems," *IEEE Trans. Device Mater. Reliabil.*, vol. 10, no. 1, pp. 33–39, Mar. 2010.

[16] E. J.Weldon, Jr., "Difference-set cyclic codes," Bell Syst. Tech. J., vol. 45, pp. 1045–1055, 1966.

[17] C. Tjhai, M. Tomlinson, M. Ambroze, and M. Ahmed, "Cyclotomic idempotent-based binary cyclic codes," *Electron. Lett.*, vol. 41, no. 6, Mar. 2005.

[18] T. Shibuya and K. Sakaniwa, "Construction of cyclic codes suitable for iterative decoding via generating idempotents," *IEICE Trans. Fundamentals*, vol. E86-A, no. 4, pp. 928–939, 2003.

[19] F. J. MacWilliams, "A table of primitive binary idempotents of odd length," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 1, pp. 118–123, Jan. 1979.

[20] IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, VOL. 20, NO. 1, JANUARY 2012 "Efficient Majority Logic Fault Detection With Difference-Set Codes For Memory Applications" Shih-Fu Liu, Pedro Reviriego, *Member, IEEE*, and Juan Antonio Maestro, *Member, IEEE* 

[21] International Journal of VLSI design & Communication Systems (VLSICS) Vol.3, No.2, April 2012 "FAULT SECURE ENCODER AND DECODER WITH CLOCK GATING" N.Kapileswar1 and P.Vijaya Santhi2 Dept.of ECE,NRI Engineering College, Pothavarapadu, INDIA <u>1.nvkapil@gmail.com</u>, 2santhipalepu@gmail.com