http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-11, Issue-3, March, 2022
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Impact Factor: 3.017

DESIGN AND IMPLEMENTATION OF HYBRID GALOIS FIELD ENCODER & DECODER

Tushar Sambhajirao Pisare[1], Dr. N A Charniya[2]
[1]Student, M.E. Digital Electronics, [2]Associate Professor,
[1,2]Department of Electronics & Electrical Engineering,
[1,2]Babasheb Naik college of Engineering, Pusad (M.H.), INDIA,
[1] tusharparodwad@gmail.com, [2]na_charaniya@rediffmail.com

***Abstract*— In The current world of digital communication secure data communication prime task. In this proposed thesis work implement a GF theory on digital data. In this thesis explore a variety of applications of the theory and applications of arithmetic and computation in the finished fields of cryptography and crypt analysis as well as in the field of digital communication. This thesis discusses a new modified method for provide the security of the information in the noise communication channel. For the improvement of security of the codes using the Galious field (G.F.). Computation over finite fields (also called Galois fields) is an active area of research in number theory and algebra, and finds many applications in cryptography, error control coding and combination design.For the implementation of proposed work use VHDL platform.The proposed shows better security as compare to golay and other encoding and decoding method.The performance analysis carried out by analyzing the utilization of Maximum frequency: 87MHz.The number of step calculating Galois Field algorithm taken by device Spartan is 6 steps. Clock cycle for each step required 33.85 MHz. The proposed method shows good result not only in the security purpose also in the frequency level on FPGA implementation.**

***Keywords*—Golay Code, Decoding Techniques, Additive White Gaussian Noise (AWGN),Field Programmable Gate Array (FPGA), Serial-In Parallel-Out (SIPO), etc**

I. INTRODUCTION

1.1 BACKGROUND

A The problem of error correcting codes has arisen in response to practical problems of reliable communication of digitally encoded information. It began in 1948, when Claude Shannon gave a formal description of a communication system. He also presented a good theory on the concept of information. The paper by Claude Shannon "A mathematical theory of communication" marked the birth of a new subject called "Information Theory", part of which is the theory of coding. C. Shannon laid the theoretical foundation of the subject. He showed that "good codes" exist without exposing them. His proof was probabilistic and existential but not constructive. It remained a great challenge to build and implement effective codes for a very long time. While Claude Shannon developed information theory and coding as a mathematical model for communication in the late 1940s, his colleague from Bell Laboratories Bell Richard Hamming found a need for error correction in his own work on computers. Setting to work on this problem R. Hamming has created a way to code information so that if an error was detected it could also be corrected. Richard Hamming was one of the first to actually build and implement error correction codes. Inspired by the work of Hamming, Claude Shannon developed the theoretical framework for the science of coding theory. The theory of error detection and code correction has become a branch of mathematics and engineering that deals with reliable trans-1 mission and data storage. Encoding, and in particular error control coding, is an extremely important part of applied mathematics.

1.2 Golay Codes

In mathematics and electronic engineering, a Golay binary code is a type of error-correction linear code used in digital communications. The Golay binary code, as well as the ternary Golay code, has a particularly deep and interesting connection to the theory of finite sporadic groups in mathematics.

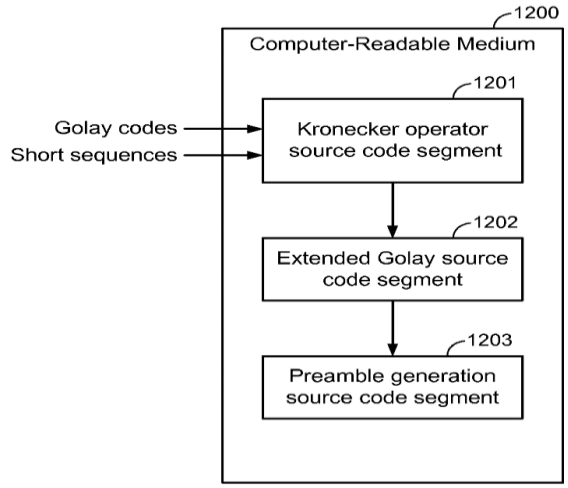

Fig 1 – Golay Code based Encoder and decoder

These codes are named in honor of Marcel JE Golay whose journal 1949 introducing them was called, by ER Berlekamp, the "best published single page" in coding theory. There are two closely related binary codes. The extended Golay binary code, G_{24} (sometimes referred to simply as the "Golay code" in finite group theory) encodes 12 bits of data in a 24-bit word in such a way that all 3-bit errors can be corrected or Any 7 bits Errors can be detected. The other, the good binary Golay code, G_{23}, has code words of length 23 and is obtained from the extended binary Golay code by removing a coordinate position (conversely, the extended binary Golay code is obtained at From the binary Golay code by adding one parity bit). In the standard code notation, the codes have parameters [24, 12, 8] and [23, 12, 7] corresponding to the length of the code words, the code size and the minimum Hamming distance between two Code words respectively advancement.

Fig 2 Extended binary Golay code and it generator Matrix

1.3 Galious Field

In mathematics, a finite field or a field of Galois (so named in honor of Evariste Galois) is a field that contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction, and division are defined and satisfy some basic rules. The most common examples of finite fields are given by the mod p of the integer number when p is a prime number.

The number of elements of a finite field is called its order. A finite field of order q exists if and only if the order q is a prime power p_k (where p is a prime number and k is a positive integer). All fields of a given order are isomorphic. In a field of order p_k, the addition of p copies of an element always gives zero; That is, the characteristic of the field is p.

In a finite field of order q, the polynomial $X^q - X$ has all q elements of the finite field as roots. The non-zero elements of a finite field form a multiplicative group. This group is cyclic, so all non-zero elements can be expressed as powers of a single element called primitive element of the field (in general, there will be several primitive elements for a given field).

A field has, by definition, a commutative multiplication operation. A more general algebraic structure that satisfies all the other axioms of a field, but whose multiplication need not be commutative, is called a division ring (or sometimes a skeleton). According to the small Wedderburn theorem, every finite division ring must be commutative, and therefore a finite field. This result shows that the limitation of definite can have algebraic consequences. Finite fields are fundamental in a number of fields of mathematics and computer science, including number theory, algebraic geometry, Galois Theory, finite geometry cryptography and coding theory.

Table 1. Shows the Galious filed (GF) look up table

TIMES TABLE FOR 3^2 USING GALOIS EXTENSION FIELD WITH NONZERO ELEMENTS 1									
	00	01	02	10	11	12	20	21	22
00	00	01	02	10	11	12	20	21	22
01	01	12	00	11	22	10	21	02	20
02	02	00	21	12	10	01	22	20	11
10	10	11	12	20	21	22	00	01	02
11	11	22	10	21	02	20	01	12	00
12	12	10	01	22	20	11	02	00	21
20	20	21	22	00	01	02	10	11	12
21	21	02	20	01	12	00	11	22	10
22	22	20	11	02	00	21	12	10	01

II. PROPOSED METHODOLOGY

2.1 INTRODUCTION

There In this chapter describe the complete structure of proposed method. In the proposed method the two major parts are available transmitter end and receiver end. First discuss the transmitter end of proposed phenomena, second the noisy channel and last one is receiver end that based on decoder process.

2.2 THEORY OF OPERATION

2.2.1 Message or Secret Data –

In the transmitter end stating point of the proposed method is input message. In the proposed method independently select the in the binary format in terms of 0 and 1. This binary input message is independent user give any 12 digit binary data at the transmitter end that is same received at the receiver end. If data is mismatch it means method is not proper worked, second condition of data mismatch enter the wrong key in the galious field or third case high noise enter in the data due to highly noise channel. User inter the 12 digit binary data that is divide in to the 3 level binary give the name G1,G2 and G3. The process of divide the binary data is shown in below Figure 4.2.

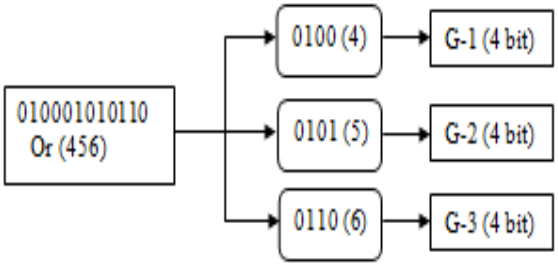

Fig. 3. Input Message divide into 4 bit hexadecimal format

2.3 Communication Chanel –

The competing the transmitter end process. The next stage of proposed work is communication channel (CC). When the message is send to the transmitter end to the receiver send via communication channel, the message corrupted by the impulse noise. Impulse noise is one of the most common type noise in the communication channel. In the impulse noise input data or transmitted data is corrupted by the zeros and ones. It means that the binary data is changed or binary bits are changed by 0 or 1.

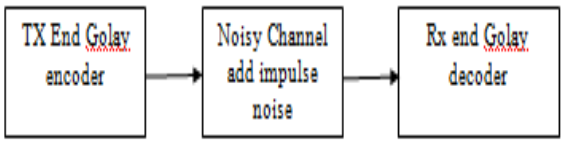

Fig 4 Impulse Noise Add in the Communication Chanel

Galois Decoder –

After the completing the error correction of received code.The received encrypted code is decrypted by the look up table shows in below. With the help of this look up table regenerate the secret message.

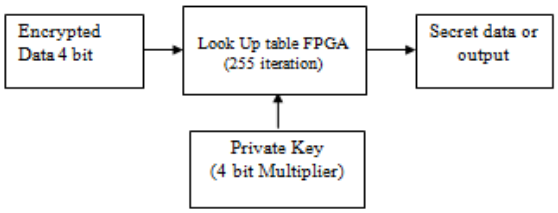

Fig 5 Shows the Galious Field Encryption

III. SIMULATION AND EXPERIMENTAL RESULT

3.1 Introduction

The This chapter describes about simulation and result analysis of proposed method. It conjointly mentioned about technology used. The given algorithm is tested and compared for various input message and different binary data that is corrupted by different impulse noise bit error. Results are describing by graphs and tables and conjointly compare results of projected work with previous work.

Basic configuration of our system is core i3 4GB RAM. The performances are quantitatively measured by the proposed decoder architecture considering resource utilization and speed as defined in given equations. Also compare on the basics of comparison of the proposed decoder architecture considering throughput, latency, and area means total number of gate used in the FPGA structure.

5.2. Result Parameters

The The slice is a sub array of a one-dimensional array, from a single element up to complete array. The prefix used for a slice is the name of the parent array. The index used for a slice must fall in the range of the indexes of the parent array. Moreover, the direction of the slice indexes must be the same as the direction of indexes of parent array (either ascending or descending). The slice is an object which can be used in the same way as its parent array: if the parent array is a signal, then any its slice is also a signal, etc. If the discrete range of a slice is null then the slice is null as well. FPGA are made of basic units called CLBs. In Xilinx FPGAs, a CLB is broken into 4 slices and each slice into 2 LUTs (Look-Up-Table).

Multipliers and DSP Slices

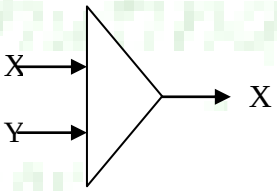

Fig 6 Multiply Function

The seemingly simple task of multiplying two numbers together can get extremely resource intensive and complex to implement in digital circuitry. To provide some frame of reference, Figure 6 shows the schematic drawing of one way to implement a 4-bit by 4-bit multiplier using combination logic.

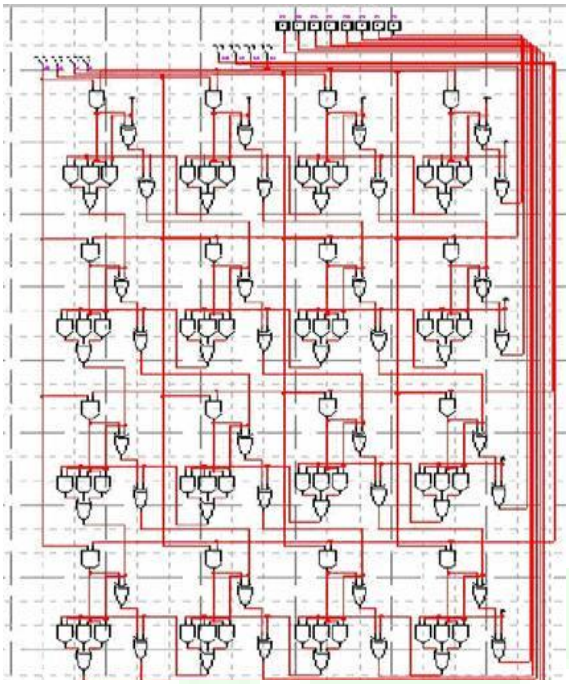

Fig.6 Schematic Drawing of a 4-Bit by 4-Bit Multiplier

Now imagine multiplying two 32-bit numbers together, and you end up with more than 2000 operations for a single multiply. Because of this, FPGA's have prebuilt multiplier circuitry to save on LUT and flip-flop usage in math and signal processing applications.

5.3 Simulation output of proposed hybrid Structure of Galious Field and golay

In the simulation output calculate the different output of the of proposed method like register transistor logic (RTL) view of the proposed, technological view of the design, Number of Slices, Number of Slice Flip Flop, Number of 4 input LUTs: Number of bonded IOBs, IOB Flip Flops and Number of GCLKs. All these are calculated in this proposed method and compare with base paper.

Project File:	try1.xise	**Parser Errors:**	No Errors
Module Name:	gg1	**Implementation State:**	Synthesized
Target Device:	xc7v585t-2ffg1157	**• Errors:**	No Errors
Product Version:	ISE 14.1	**• Warnings:**	31 Warnings (0 new)
Design Goal:	Balanced	**• Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	**• Timing Constraints:**	
Environment:	System Settings	**• Final Timing Score:**	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	192	728400	0%
Number of Slice LUTs	568	364200	0%
Number of fully used LUT-FF pairs	154	606	25%
Number of bonded IOBs	168	600	28%
Number of BUFG/BUFGCTRLs	1	32	3%

Fig 7 shows the design summary view of Proposed Design

In this design summery, shows that the proper output of the proposed method. The design summery shows proposed method run successfully with no errors. For run or synthesis proposed method first synthesize the XST. After synthesize of XST shows the RTL view that is shown in below. After analysis of RTL view also shows the technology schematics and other view. If proposed method is without error shows that no error. Sometimes also contains some warnings but warnings are avoidable. In the present of error simulation will not run.

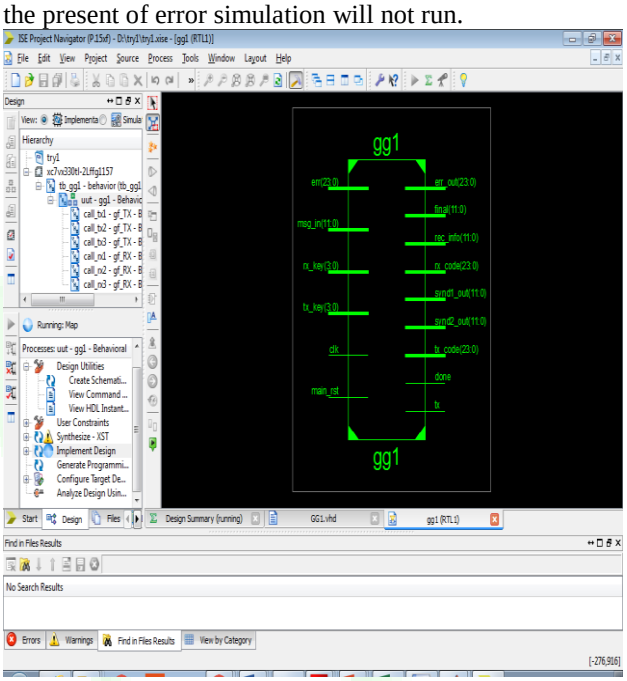

Fig 8 Shows the RTL view of Proposed Design

After the HDL synthesis phase of the synthesis process, you can display a schematic representation of your synthesized source file. This schematic shows a representation of the optimized design in terms of generic symbols, such as adders, multipliers, counters, AND gates, and OR gates, that are independent of the targeted Xilinx® device. Viewing this schematic may help you discover design issues early in the design process.

5.4 Simulation of I-Sim –

In the I-Sim simulator shows the simulation output of the proposed method. In the simulation window the input the predefined in the work bench. Input message, transmitter end key, receiver end key, encoder data, decoded data. The input signal is shown in the below figure.

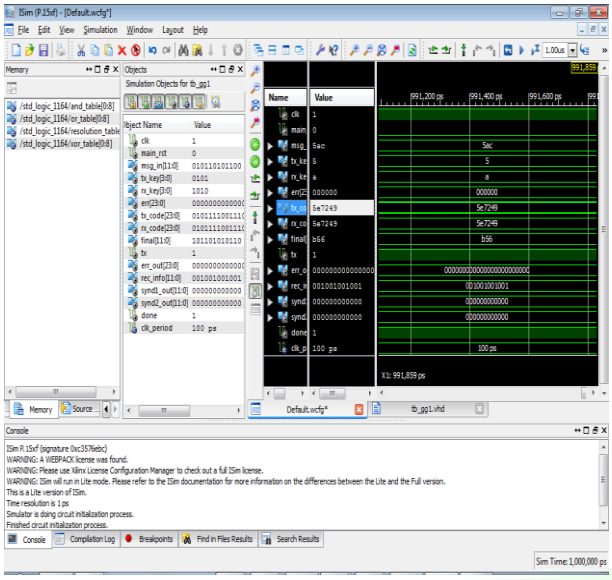

Fig 9 i-Sim Simulator Window

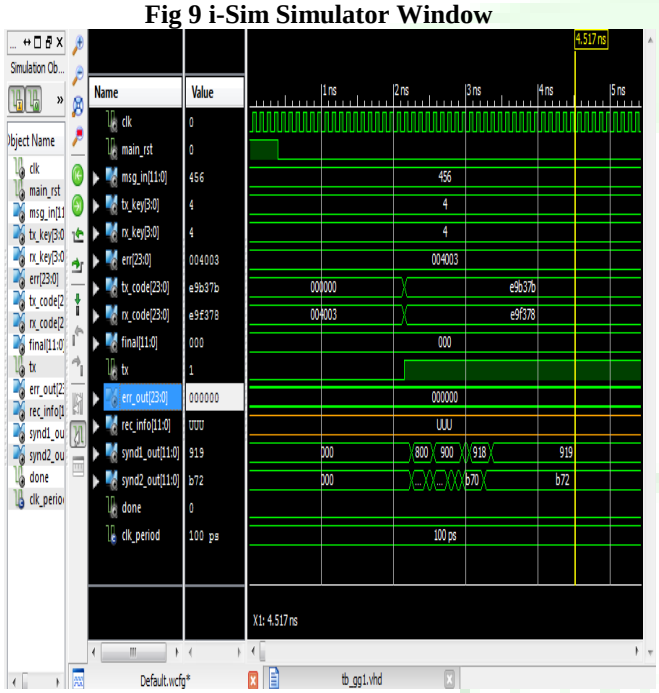

Fig 10 Receiver End Key, Encoder Data, Decoded Data

V. CONCLUSION

In this discuss on A Bird Eyeview On Design And Implementation of Hybrid Galois Field Encoder & Decoder. The important outcomes of this paper are shown in the section of comparative analysis.

In this paper observe that the A Bird Eyeview on Design And Implementation of Hybrid Galois Field Encoder & Decoder. Also most of the Hybrid Galois Field Encoder & Decoder.

In future design a better A Bird Eyeview on Design And Implementation of Hybrid Galois Field Encoder & Decoder. That can improve all these problems in this communication area. In future try to A Bird Eyeview on Design And Implementation of Hybrid Galois Field Encoder & Decoder.

References

[1] SatyabrataSarangi and Swapna Banerjee, "Efficient Hardware Implementation of Encoder and Decoder for Golay Code" IEEE transactions on very large scale integration (VLSI) systems, vol. 23, no. 9, September 2015.

[2] AmirhosseinAlimohammad and SaeedFouladiFard, "FPGA-Based Bit Error Rate Performance Measurement of Wireless Systems", IEEE transactions on very large scale integration (VLSI) systems, vol. 22, issue 7, pp.1583-1592, Jul. 2014.

[3] P. Adde and R. Le Bidan, "A low-complexity soft-decision decoding architecture for the binary extended Golay code," in Proc. 19th IEEE International. Conference Electronics, Circuits, System. (ICECS), Dec. 2012, pp. 705–708.

[4] Patrick Adde, Daniel Gomez Toro, and Christophe Jego,"Design of an Efficient Maximum Likelihood Soft Decoder for Systematic Short Block Codes", IEEE Transaction Signal Process., vol. 60, no. 7, pp. 3914–3919, Jul. 2012.

[5] T.-C. Lin, H. –C. Chang, H. –P. Lee, and T.-K. Truong "On the decoding of the (24, 12, 8) Golay Code", International Science., vol. 180, no. 23, pp. 4729–4736 Dec. 2010.

[6] Yen-Wen Huang and Ying Li, "802.16 Uplink Sounding via QPSK Golay Sequences" vol. 13, no.3PP.152-161, July, 2010.

[7] S.-Y. Su and P.-C. Li, "Photoacoustic signal generation with Golay coded excitation," in Proc. IEEE Ultrason. Symp. (IUS), Oct. 2010, pp. 2151–2154.

[8] Hehn, Thorsten, et al. "Multiple-bases belief-propagation decoding of high-density cyclic codes."*IEEE transactions on communications* 58.1 (2010): 1-8.

[9] Adde, Patrick, et al. "Design and implementation of a soft-decision decoder for cortex codes."*2010 17th IEEE International Conference on Electronics, Circuits and Systems*. IEEE, 2010.

[10] M.-H. Jing, Y.-C. Su, J. –H. Chen, Z.-H. Chen, and Y. Chang, "High-Speed Low-Complexity Golay Decoder Based on Syndrome weight Determination" in Proc. 7th Int. Conf. Int., Communication , Signal Process, Dec. 2009, pp. 1-4.

[11] Wong, Yin Sweet, et al. "Implementation of convolutional encoder and Viterbi decoder using VHDL."*2009 IEEE Student Conference on Research and Development (SCOReD)*. IEEE, 2009.

[12] Hehn, Thorsten, et al. "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes."*IEEE Transactions on Information Theory* 54.12 (2008): 5308-5331.

[13] Chunjian, Deng, et al. "MCU Interface Based Golay Coder & Decoder in SoC Realization."*2008 Second International Symposium on Intelligent Information Technology Application*. Vol. 2. IEEE, 2008.

[14] X. –H. Peng, and P. G. Farrell, "On Construction of the (24, 12, 8) Golay Codes", IEEE Trans. Inf. Theory, vol. 52, no. 8, pp. 3669–3675, Aug. 2006

[15] Chr, Ching-Lung, Szu-Lin Su, and Shao-Wei Wu. "Decoding the (23, 12, 7) Golay code using a low-complexity scheme."*IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 89.8 (2006): 2235-2238

[16] Murugan, Arul D., et al. "A unified framework for tree search decoding: Rediscovering the sequential decoder."*IEEE Transactions on Information Theory* 52.3 (2006): 933-953.

[17] G. Campobello, G. Patane, and M. Russo, "Parallel CRC Realization" IEEE Trans. Comput., vol. 52, no. 10, pp. 1312-1319, Oct. 2003.

[18] Engin, Nur, and Kees van Berkel. "Viterbi decoding on a coprocessor architecture with vector parallelism."*2003 IEEE Workshop on Signal Processing Systems (IEEE Cat. No. 03TH8682)*. IEEE, 2003.

[19] Chang, Yaotsu, et al. "Algebraic decoding of (71, 36, 11),(79, 40, 15), and (97, 49, 15) quadratic residue codes."*IEEE transactions on communications* 51.9 (2003): 1463-1473.

[20] Kwak, Jaeyoung, and Kwyro Lee. "Design of dividable interleaver for parallel decoding in turbo codes."*Electronics Letters* 38.22 (2002): 1362-1364.

[21] Uchida, Yoshihiro, et al. "VLSI architecture of digital matched filter and prime interleaver for W-CDMA."*2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353)*. Vol. 3. IEEE, 2002.

[22] M. Spachmann, "Automatic generation of parallel CRC circuits", IEEE Des. Test. Comput., vol. 18, no. 3, pp. 108-114, May/Jun. 2001.

[23] Winstead, Chris, et al. "Analog MAP decoder for (8, 4) Hamming code in subthreshold CMOS."*Proceedings 2001 Conference on Advanced Research in VLSI. ARVLSI 2001*. IEEE, 2001.

[24] Fekri, Faramarz, et al. "Decoding of half-rate wavelet codes; Golay code and more."*2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221)*. Vol. 4. IEEE, 2001.

[25] Solomon, G. "Golay encoding/decoding via BCH-Hamming."*Computers & Mathematics with Applications* 39.11 (2000): 103-108.

[26] R. Nair, G. Ryan and F. Farzaneh"A Symbol Based Algorithm for Hardware Implementation of Cyclic Redundancy Check (CRC)," in Proc. VHDL Int. Users' Forum, Oct. 1997, pp. 82-87.

[27] Cao, Weixun. "High-speed parallel VLSI-architecture for the (24, 12) Golay decoder with optimized permutation decoding."*1996 IEEE International Symposium on Circuits and Systems. Circuits and Systems Connecting the World. ISCAS 96*. Vol. 4. IEEE, 1996.

[28] A.Vardy and Y. Be'eg, "More Efficient Soft Decoding Of The Golay Codes," IEEE Trans. Inf. Theory, vol. 37, no. 3, pp. 667-672, May 1991.

[29] S. –W. Wei and C. –H. Wei, "On High-speed Decoding of the (23,12,7) Golay Code," IEEE Trans. Inf. Theory, vol. 36, no. 3, pp. 692-695, May 1990.

[30] J. Snyders and Be' ery, "Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes," IEEE Trans. Inf. Theory, vol. 35, no. 5, pp. 963-975, Sep. 1989.

