INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 5, Issue - 3, Mar - 2021
Monthly Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 5.743
Received on : 10/01/2021 Accepted on : 20/01/2021 Publication Date: 20/01/2021

A Robust Golay Codes with GF2 field for Encrypted Message Transceiver

Urvashi Verma (M.Tech Scholar VLSI)
Dept. Electronics and Communication Engineering S.R.C.E.M., Banmore, Morena, (M.P.), India
Email - urvashiverma2510@gmail.com

Ashish Duvey (Assistant Professor)
Dept. Electronics and Communication Engineering S.R.C.E.M., Banmore, Morena, (M.P.), India
Email - adsrcem@gmail.com

Abstract: *In this research work proposed 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 analysing the utilization of Maximum frequency: 87 MHz. 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.*

Key Words: *Architecture, decoder, encoder, field programmable gate array (FPGA), Golay code.*

1. INTRODUCTION:

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 cryptanalysis as well as in the field of digital communication. Golay code was presented in [2] to address error correcting phenomena. The binary Golay code (G23) is represented as (23, 12, 7), while the extended binary Golay code (G24) is as (24, 12, 8). The extended Golay code has been used extensively in deep space network of JPL-NASA as well as in the Voyager imaging system [6]. In addition, Golay code plays a vital role in different applications like coded excitation for a laser [7] and ultrasound imaging due to the complete sidelobe nullification property of complementary Golay pair. All these applications need generation of Golay sequence, which is fed as trigger to the laser modules. However, for generating Golay code an automatic pattern generator is used, which is of very high cost. To combat this problem, a hardware module programmed to yield a Golay encoded codeword may be used. Golay decoder is used extensively in communication links for forward error correction. Therefore, a high speed and high throughput hardware for decoder could be useful in communication links for forward error correction. Communication is important in our daily lives. We use phones, satellites, computers and other devices to send messages via a channel to a receiver. Unfortunately, most types of communication are subject to noise, which can cause errors in the messages that are sent. Especially when sending messages is a difficult or expensive task, for example in satellite communication, it is important to find ways of minimizing the occurrence of errors. This is the central idea in coding theory: what message was sent given what we received? To make this problem as simple as possible, we use error correction codes. The main idea is to add redundancy to messages that allows us to identify and correct errors that may occur. This thesis deals with a specific type of error-correcting code, the extended Golay code G24, named after the Swiss mathematician Marcel J.E. Golay (1902-1989). He used mathematics to solve real problems, one of which was the question of how to send messages from satellites through space. Golay Extended Code was used to send Voyager 1 and 2 images of Jupiter and Saturn. With the extended Golay code we are talking about a specific group of Mathieu, M24, as it is strongly related to the code. This group bears the name of the French mathematician Emile Léonard Mathieu (1835-1890). The last part of this thesis describes four geometrical figures with which we can visualize the properties of G24 and M24.

2. BACK GROUND:

There are two closely related binary Golay codes. The **extended binary Golay code**, G_{24} (sometimes just called the "Golay code" in finite group theory) encodes 12 bits of data in a 24-bit word in such a way that any 3-bit errors can be corrected or any 7-bit errors can be detected. The other, the **perfect binary Golay code**, G_{23}, has code words of length 23 and is obtained from the extended binary Golay code by deleting one coordinate position (conversely, the extended binary Golay code is obtained from the perfect binary Golay code by adding a parity bit). In standard code notation the codes have parameters [24, 12, 8] and [23, 12, 7], corresponding to the length of the code words, the dimension of the code, and the minimum Hamming distance between two code words, respectively.

In mathematical terms, the extended binary Golay code G_{24} consists of a 12-dimensional linear subspace W of the space $V=\mathbf{F}_2^{24}$ of 24-bit words such that any two distinct elements of

W differ in at least 8 coordinates. *W* is called a linear code because it is a vector space. In all, *W* comprises 4096 = 2^{12} elements.

- The elements of *W* are called *code words*. They can also be described as subsets of a set of 24 elements, where addition is defined as taking the symmetric difference of the subsets.
- In the extended binary Golay code, all code words have Hamming weights of 0, 8, 12, 16, or 24. Code words of weight 8 are called octade and code words of weight 12 are called dodecads.
- Octads of the code G_{24} are elements of the S(5,8,24) Steiner system. There are 759 = 3*11*23 octads and 759 complements thereof. It follows that there are 2576 = 2^4*7*23 dodecads.
- Two octads intersect (have 1's in common) in 0, 2, or 4 coordinates in the binary vector representation (these are the possible intersection sizes in the subset representation). An octad and a dodecad intersect at 2, 4, or 6 coordinates.
- Up to relabeling coordinates, *W* is unique.

The binary Golay code, G_{23} is a perfect code. That is, the spheres of radius three around code words form a partition of the vector space. G_{23} is a 12-dimensional subspace of the space $\mathbf{F}_2^{23}$.

Galois Field

The elements of Galois Field $gf(p^n)$ is defined as:

$$gf(p^n) = (0,1,2,\dots,p-1) \cup$$
$$(p, p+1, p+2, \dots, p+p-1) \cup$$
$$(p^2, p^2+1, p^2+2, \dots, p^2+p-1) \cup \dots \cup$$
$$(p^{n-1}, p^{n-1}-1, p^{n-1}-2, \dots, p^{n-1}+p-1)$$

where p $\in$ P and $n \in \mathbb{Z}^+$. The order of the field is given by p^n while p is called the characteristic of the field. On the other hand, gf as can be guessed, represents Galois Field. Note also that the degree of polynomial of each element is at most $n-1$.

Binary System

In the binary number system or base number system 2, we represent each value with 0 and 1. To convert a system of decimal numbers or a system of base numbers-10 to a binary system, we must represent a decimal number In terms of sums of $a_n 2^n$ That is, if x is the so-called decimal number then we want to have:

$$x = \sum_{n \in N} a_n 2^n$$

The coefficients a_n are then written in descending order of n and all leading zeros are then omitted. The final result becomes the binary representation of the decimal x. In the end, the binary system offers another way of representing the elements of a Galois field. The polynomial and binary representation of an element has its own advantages and disadvantages.

Example:

$$19 = \dots + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

So the binary representation of 19 is 10011 while the elements of $gf(2^3)$ in binary are:

$$gf(2^3) = (001, 010, 011, 100, 101, 110, 111)$$

The binary prime field F2, which acts in the same way as a Boolean algebra, serves as a great tool for development and analysis of symmetric ciphers, since many of them can be described using Boolean functions. The binary extension fields F2n are used in both public key cryptography in implementing efficient arithmetic and in symmetric key cryptography in designing cipher components. Algebraic attacks on symmetric ciphers rely heavily on the properties of binary fields for the equation generation and solution. In this thesis, we will use algebraic attacks to analyses a collection of stream ciphers not previously analyzed and comment on their susceptibility to these forms.

3. LITERATURE SURVEY :

Mohammad Saidur R. [2020], *"Reversible Bio-signal Steganography Approach for Authenticating Bio-signals using Extended Binary Golay code"* - In this work, we develop a reversible bio-signal steganography approach using Extended Binary Golay Code based error correction method. Our proposed method embeds secret message as an error within different types of bio-signals such as ECG, PPG, and EEG. Extended Binary Golay code-based error correction technique is used to encode bio-signal samples before embedding secret message. Three bits of the secret message is embedded in randomly selected bio-signal sample as an error. Later, Extended Binary Golay code-based error correction technique is used to correct errors to reconstruct the bio-signal. At the same time, the secret message is retrieved. A pseudo random sequence is used to increase the security of the method as it decreases the cracking probability. Our approach demonstrates the reversibility by means of 0% error rate and PRD in reconstructed bio signal. Additionally, 0% BER in retrieved secret message justifies that approach is reliable. However, the data hiding capacity of our proposed approach depends on the number of samples in cover bio signal. The maximum capacity of our proposed method is three times the number of samples. Hence proposed method has very high data hiding capacity[1].

Maity, Raj Kumar, et.al.[2019], *"An area and power efficient double adjacent error correcting parallel decoder based on (24, 12) extended golay code",* In this paper, a new (24; 12) SEC-DED-DAEC code has been proposed based on the

extended Golay code. Proposed parallel decoder has been designed and implemented in FPGA and ASIC platforms. The performance of proposed parallel decoder has been compared with the parallel decoder of (24; 12) SEC-DAEC extended Golay code. The proposed (24; 12) SECDED-DAEC parallel decoder exhibits better performance in area, delay and power. The parallel decoder of newly proposed code can be employed in protecting SRAMs against MCUs [2].

Nazeri, Morteza et.al. [2018], *"An Efficient Architecture for Golay Code Encoder"*, In this paper, the Golay codes play important role in ECCs. Recently, authors of have proposed efficient architectures for Golay code encoding, but their architectures cannot work for the message with '0' MS bits. In this paper, new encoding architecture was proposed for Golay code. The developed architecture for Golay code encoder was composed of three units: 1) data path, 2) control unit, and 3) converting unit.These units were designed carefully such that the developed architecture can work with '0' and'1' MSB messages. The developed architecture was implemented on FPGA device.The implementation results verified the correctness of developed architecture at the expense of reasonable area and delay time overhead. As a result, the proposed encoder a architect has a huge potential to become an efficient architecture for implementing Golay codes encoder [3].

Allan Jose et.al. [2017], *"FPGA Implementation of Encoder and Decoder for Golay Code"*-In this paper presents a simple and more efficient Golay encoding and decoding scheme. The design was implemented in Spartan 6 FPGA. The encoder is based on the Block RAM method, which outperforms the conventional LFSR method. The decoder is based on the syndrome decomposition algorithm with parallel architecture, which has significantly improved the speed of the system. For both the hardware modules, low latency and high throughput is achieved. The encoder and decoder proposed prove to be a promising choice for high speed operations[4].

Pengwei Zhang et.al. [2017], *"Design of a High-Throughput Low-Latency Extended Golay Decoder"* - A 12 Gb/s highthroughput decoder with low latency is proposed to decode the (24, 12, 8) extended Golay code. The proposed PIMLD decoder provides identical error performances as the IMLD decoder but achieves a much higher throughput. Moreover, it has a latency of merely 5 clock cycles and is therefore very suitable for delay critical communication systems[5].

Pallavi Bhoyar et.al. [2016], *"Design of Encoder and Decoder for Golay code ",* In this design a Golay code based encoder and decoder architecture using CRC processing technique. This technique is to reduce the circuit complexity for data transmission and reception process. The simulation results state that the Golay code encoder architecture provides the CRC generation technique which is based on conventional LFSR. The encoder and decoder modules for Golay code for can be used for various applications in high-speed communication link [6].

4. PROPOSED DESIGN :

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 4.1.

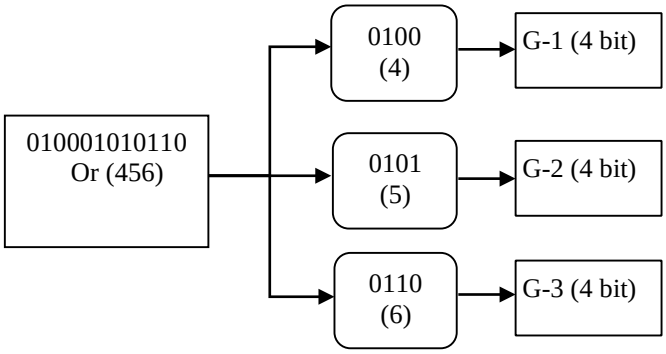


Fig. 4.1 Input Message divide into 4 bit hexadecimal format

The above figure 4.1 shows that how to give the 12 bit binary data into the galious filed. 12 bit data divide into 3 equal part of four-four bit binary data. After the divide input binary data into 3 equal part, further proceeding sending to the G1, G2 and G3 to the galious encoder.

Galious Filed Encoder –

The Galois field (GF) theory deals with numbers that are binary in nature. Galois operations match those of regular mathematics like addition, multiplication and logarithms using the multiplication property of the Galois field an algorithm can be implemented to design an encoder.

Example: if the multiplicand = 1111 (Hexadecimal = 15)
Original data Multiplier = 1111 [Private Key] (Hexadecimal = 15)
Irreducible polynomial [private key] = 10011
STEP1: (0000) XOR (1) AND (1111) = 1111
[Result] [A(3)] [Multiplicand]
MSB High Append Step1 Result With 0
STEP2: (11110) XOR (1) AND (1111) = 11110 XOR 01111 = 10001
Result is 5 Bit subtract polynomial to get 4bit result [10001-10011=00010]
STEP3: (00010) XOR (1) AND (1111) = 00010 XOR 01111=01011
STEP4: 1011+1 AND (1111) =10110 XOR 01111=11001(MSB 1 append 0 to result)
Result is 5 Bit subtract polynomial [11001-10011] =1010
Final outcome is 1010 in form of hexadecimal [15* 15 = 10]

The above statements or steps are used to calculate the Cipher Text or galious encoded data. For cross check our proposed method use the look up tables. With the help of look table cross verified the outcome of the result. In below table also shows the same outcome.

After the competing the transmitter end process. The next stage of proposed work is communication channel (CC). When the

INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 5, Issue - 3, Mar - 2021
Monthly Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 5.743
Received on : 10/01/2021 Accepted on : 20/01/2021 Publication Date: 20/01/2021

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.

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.

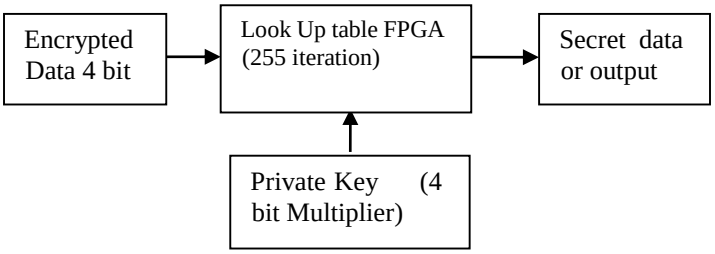


Fig 4.2 Shows the Galious Field Encryption

With the help of this table recreate the data. That is final outcome of the proposed method.

Table 4.2 Look up table for direct multiplication of Galious filed

MULTIPLICATE	Multiplier (Private Key)															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
	3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
	4	0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
	5	0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
	6	0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
	7	0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
	8	0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
	9	0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
	10	0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
	11	0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
	12	0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
	13	0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
	14	0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
	15	0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

Finally got the received input message. That is the overall explanation of proposed method.

5. SIMULATION AND RESULT

In the simulation output calculate the different output of the of proposed method like register transistor logic (RTL) view of the proposed. 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 5.5 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.

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.

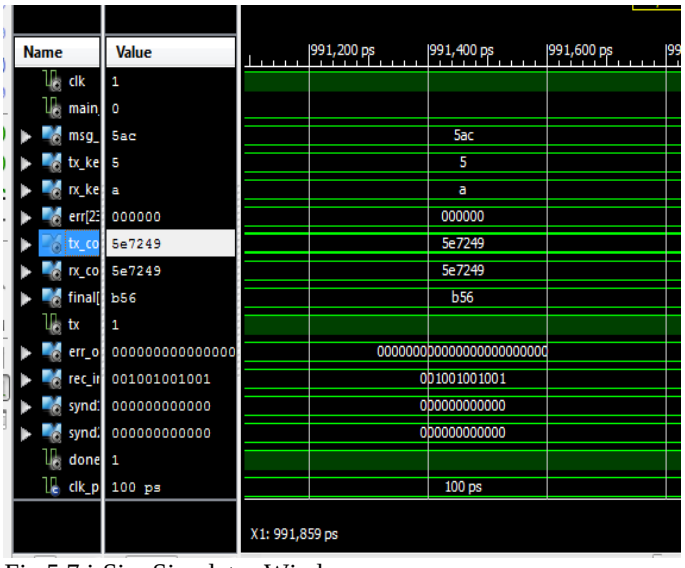
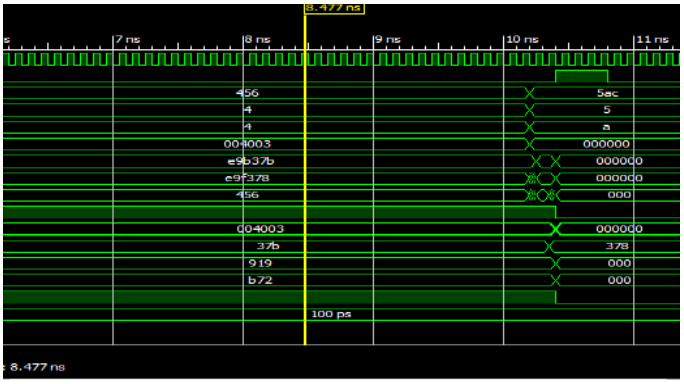


Fig 5.7 i-Sim Simulator Window



In the last of the simulation and result discuss the compression of outcomes with other previous method. In the table 1 shows the compression of slices and frequency of the proposed method and previous method.

Table 1: shows the Comparison of Slices and frequency

Ref.	Year	Device	Slices (% of utilization)	Software	Frequency	Advantage
[4]	IEEE 2018	Spartan 6 XC6slx253	1.24	MATLAB R2014b	318.77 MHz	High frequency (single Operation)
Proposed	2020	Spartan 6 XC6slx253	0.263514	Xilinx 2014a	203.116 MHz	Error Correction + Data Encryption +Data Decryption

Table 2: shows the Comparison of Throughput and FPGA Board

Reference	Throughput	Board
[10]	1 output/144 clock cycle	Virtex -E
[15]	Not available	Virtex -E
[16]	Not available	Virtex -E
[23]	1 output/24 clock cycle	Virtex -E
Base Paper IEEE 2018 [4]	1 output/2 clock cycle	Spartan 6 XC6slx253
Proposed	1 output/2 clock cycle	Virtex -E

Table 3: Device Utilization Summary (estimated values)

Logic Utilization	Used	Available	Utilization
Number of Slice Registers	192 (encoder - 94 and decoder - 90)	728400	0.26%
Number of Slice LUTs	568	364200	0.50%
Number of fully used LUT-FF pairs	154	606	25%
Number of bonded IOBs	168	600	28%
Number of BUFG / BUFGCTRLs	1	32	3%

In the above there are three tables shown table 1, 2 and 3. With the help of this table all the result parameters are easily describe. Table 5.2 and 5.3 shows the Comparison of proposed method with different previous method and also with base paper. The result of the proposed method is good in different parameters but higher in terms of frequency. For completing proposed method calculating the time or frequency, proposed method contains higher frequency as compare to other method. The reason behind them is dual operation in the base paper only golay codes works but in proposed method perform the two tasks golay and galious both. Therefore, frequency of the proposed method is 100MHz.

6. CONCLUSION:

This is the proposed scheme is a hybrid structure of golay code and galious filed. Special emphasis is laid on its auto morphism group, the group that acts on all code-words and leaves the code unaltered.

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: 203.116 MHz. 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.

REFERENCES:

1. Satyabrata Rahman, Mohammad Saidur, Ibrahim Khalil, and Xun Yi. "Reversible Biosignal Steganography Approach for Authenticating Biosignals using Extended Binary Golay code." IEEE Journal of Biomedical and Health Informatics (2020).
2. Maity, Raj Kumar, Jagannath Samanta, and Jaydeb Bhaumik. "An area and power efficient double adjacent error correcting parallel decoder based on (24, 12) extended golay code." In 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1-6. IEEE, 2019.
3. Nazeri, Morteza, Abdalhossein Rezai, and Huzain Azis. "An Efficient Architecture for Golay Code Encoder." In 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), pp. 114-117. IEEE, 2018.

4. Jose, Allan, and S. Sujithamol. "FPGA implementation of encoder and decoder for Golay code." In 2017 International Conference on Trends in Electronics and Informatics (ICEI), pp. 892-896. IEEE, 2017.

5. Zhang, Pengwei, Francis CM Lau, and Chiu-W. Sham. "Design of a high-throughput low-latency extended golay decoder." In 2017 23rd Asia-Pacific Conference on Communications (APCC), pp. 1-4. IEEE, 2017.

6. Bhoyar, Pallavi. "Design of encoder and decoder for Golay code." In 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 1491-1495. IEEE, 2016.

7. Satyabrata Sarangi 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.

8. Amirhossein Alimohammad and Saeed Fouladi Fard, "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.

9. 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.

10. 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.

11. 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.

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

13. 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.

14. 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.

15. 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

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

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

18. 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.

19. Weixun Cao "Decoder with Optimized Permutation Decoding" Signals, Systems and Computers (ASILOMAR), IEEE Conference, May 1996.

20. 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.

21. 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.

22. 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.

23. A. D. Abbaszadeh and C. K. Rushforth, Baosheng "VLSI Implementation of a maximum-likelihood decoder for the Golay (24, 12) Code," IEEE J. Sel. Areas Commun., vol. 6 no. 3, pp. 558-565, Apr. 1988.

24. Curtis, R. T. "A new combinatorial approach to M24". Mathematical Proceedings of the Cambridge Philosophical Society. 79: 25 42. 1979.

25. Golay, Marcel J. E. (1949). "Notes on Digital Coding". Proc. IRE. 37: 65

26. W. Cao, "High-speed parallel VLSI-architecture for the (24, 12) Golay decoder with optimized permutation decoding," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), Connecting World, vol. 4. May 1996, pp. 61–64.