Journal of Theoretical and Applied Information Technology
15th May 2017. Vol.95. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FPGA IMPLEMENTATION OF CRYPTOGRAPHIC SYSTEMS FOR SYMMETRIC ENCRYPTION

FAZAL NOORBASHA[1], M. MANASA[2], R. TULASI GOUTHAMI[3], S. SRUTHI[4], D. HARI PRIYA[5], N. PRASHANTH[6], and MD. ZIA UR RAHMAN[7]

[1, 2, 3, 4, 5, 6, 7] Department of ECE, K L University, Vaddeswaram, Guntur, AP – India
E-mail: [1]fazalnoorbasha@kluniversity.in, [2] manasamuliki@kluniversity.in,
[3]tulasi.raavi17@gmail.com, [4]sruthipatnaik3695@gmail.com, [5] haridevanasetty@gmail.com,
[6]prashanthnagisetty1995@gmail.com, [7]mdzr55@gmail.com

ABSTRACT

In this proposed work, implemented a cryptographic system for symmetric encryption and hamming code for error detection and correction. Symmetric key is using same duplicate data i.e. key data for both encryption and decryption. In this encryption and decryption process hamming code which is used to check the one bit error if any. Encrypting a message can be done by supplying a message along with the key while the process of decryption can be done by passing the key along with the resultant output in order to obtain the original message. For this process AES algorithm was adopted. The original 8-bit data is 1's complemented and it will be swapped based on the select lines and swapped data is XOR'ed with the original data finally the encrypted data will be transmitted. Encrypted data is the combination of both swapped data and encrypted data i.e.16-bit data. To get original message data the Swapped data is XOR'ed with the encrypted data which is decrypted data.

Keywords: *Encryption, Decryption, Symmetric Key, Swap Mode, XOR.*

1. INTRODUCTION

From past few years, we are using different techniques to hide and protect the data from others. Cryptography is a technique used for hiding and securing the data. For securing the data we will combine the original data with third party i.e. duplicate data, so that user can only understand about it [1-2]. In cryptography there are many algorithms to secure the data for example, Asymmetric systems are RSA, elliptical curve cryptography, and Symmetric systems are Advanced Encryption Standard (AES) and Data Encryption Standard (DES) etc [3-4]. It is the combination of both encryption and decryption. In encryption original data is combined with the duplicate in order to hide the original data. Decryption is performed to get back the original data [5-8]. Cryptography is used for keeping the data confidentially. Applications of cryptography include ATM cards, Electronic commerce and Computer passwords. The main advantage of cryptography algorithm is to decrease the time delay of execution [9-12]. In military applications we are using cryptography to protect the confidential data from terrorists and al-Qaida's [13-14].

This algorithm is developed using VERILOG HDL code for error detection throughout the process. This developed algorithm is having following modules XOR operation, 1's complement and data swapping. Hamming code module is used to detect and correct one bit error. Key data is important for encryption and decryption of the data. Same key is used for data encryption and decryption which is known as symmetric key cryptography.

2. SYSTEM ARCHITECTURE

In this data encryption process, input data size is 8-bit, by using XOR and swapping methods this 8-bit data is converting into 16-bit. Finally, this 16-bit data will be transmitted. At receiver end 16-bit data will be decrypted in to 8-bit data by using XOR and swapping methods. This total architecture block diagram is shown in figure 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

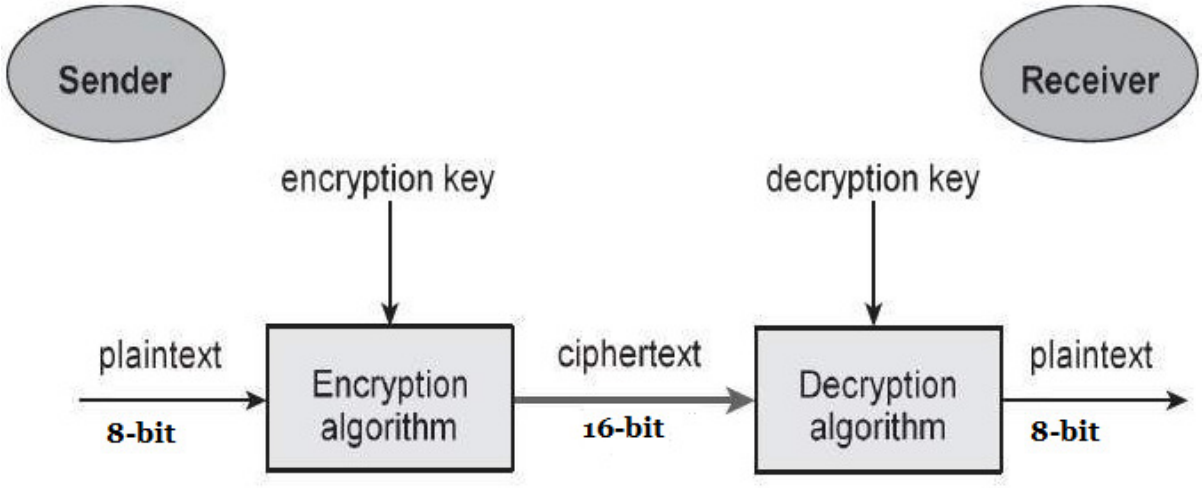

Figure 1: Data Encryption and Decryption process

A. Encryption Process

Security being the most important factor in cloud computing has to be dealt with great precautions. Also, the key generation technique used in this paper is unique in its own way. This has helped in avoiding any chances of repeated or redundant key [15]. The advances in wireless communication technology over the past era have provided better data and voice security. Analog voice scrambling can be inserted into narrowband voice channel as it does not increase the bandwidth [16-17].

Symmetric encryption is also called as conventional or it is also defined as single key encryption. This is only type of encryption which is used before the existence of public key encryption. The symmetric key encryption consists of plain text, encryption algorithm, secret key, cipher text, decryption algorithm. Figure 2 shows the encryption process. In this process we are using 8-bit data as input, by using this input data we are getting two 8-bit data. One 8-bit data is key, i.e. the
Key is 1's complement of 8-bit input data. Another 8-bit data is swapped data of input data. This is first encryption step, in second step XOR operation will be performed between 8-bit key and swapped data. In third step XORed 8-bit data and 8-bit key will be transmitted. Finally 8-bit data will be converted into 16-bit data. For this we are using three step encryption processes. Table 1 is showing the four modes of data swapping.

B. Decryption Process

Decryption process is a reverse of encryption. Decryption is the process of taking the encrypted data and converting back to the original message that can be understandable by the normal computer. Encryption is basically done to protect and secure the information and to retrieve the information back we use decryption. The output of encryption process is given as input to the decryption. Figure 3 shows the decryption process steps. In step one 16-bit data, it will separate into two parts key and swapped data. In step two between these two 8-bit data XOR operation will performed. In third step swapping will be performed to get final 8-bit original data.

The various components of a basic cryptosystem are as follows −

- Plaintext. It is the data to be protected during broadcast.
- Encryption Algorithm. It is a mathematical cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- Ciphertext. It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key.
- Decryption Algorithm, It is a mathematical process, cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm.
- Encryption Key. It is a value that is known to the sender. The sender inputs the encryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

- Decryption Key. It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext [18-19].

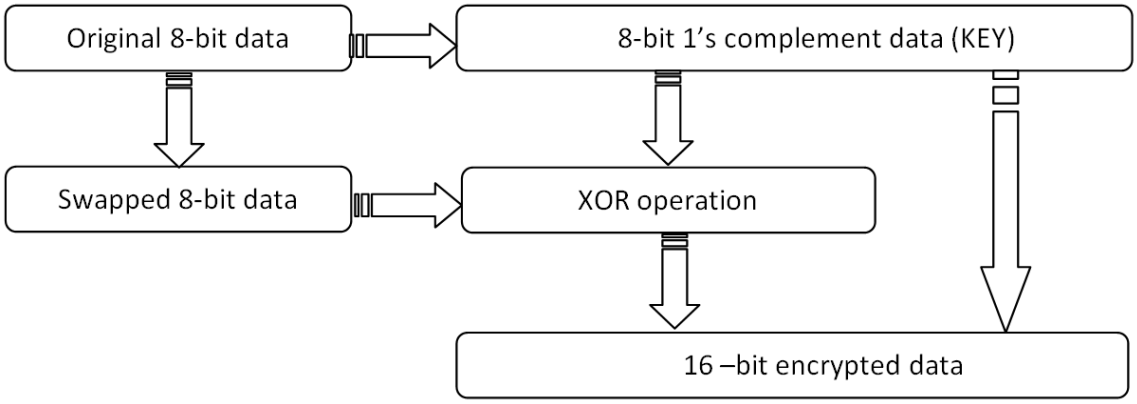

Figure 2: Encryption Process

Swap Mode (S_1S_0)	Swapped 8-bit data ($A_0A_1A_2A_3\ A_4A_5A_6A_7$)
S_0- 00	$A_4A_5A_6A_7\ A_0A_1A_2A_3$
S_1- 01	$A_2A_0A_3A_1\ A_5A_4A_7A_6$
S_2- 10	$A_4A_5A_2A_3\ A_0A_1A_6A_7$
S_3- 11	$A_2A_3A_0A_1\ A_6A_7A_4A_5$

Table 1: Data Swapping

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

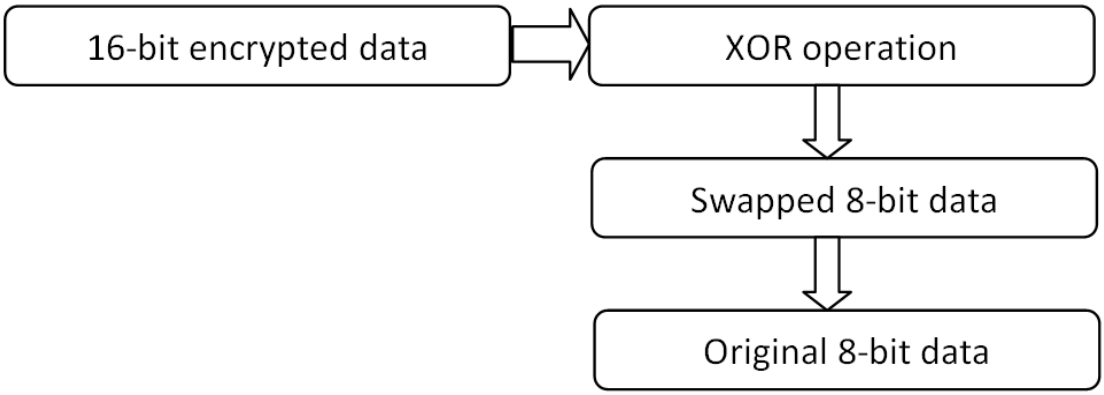

Figure 3: Decryption Process

3. WORKING PRINCIPLE

Advanced encryption standard(AES) for the encryption process in which the encryption is done by using 4 different transformations - initial round, 9 main rounds and the final round. In the initial round we will first do add round key. Then in the 9 main rounds, first we will take the sub-byte from the data. Then we will shift the rows and then we will mix columns. And then we will again do add round key and this continues until the data is encrypted totally. Then in the final round, we again do add round key. But this results in the slow performance of the encryption process. And from this it has been proven to be a weak cipher, therefore should not be trusted to protect the sensitive data and due to key size, it will enhance encryption and decryption for efficient communication. So to overcome these drawbacks we use the below mentioned method for the Encryption and Decryption process.

In this method, first we will take the input data. Then we will do 1's complement of the input data and we will swap the data that is complemented based on select lines. Then we will do XOR operation for the input data and the swapped data. This gives the *Encrypted data*. Then the encrypted data is divided into Swapped data and Key data. Now the swapped data and the Key data are XOR'ed which gives the *Decrypted data*. The decrypted data is the original input data that we gave.

The encrypted data is replaced with the 16-bit data. Hamming code is applied for S-box and it is used to detect the errors. But the disadvantage of using Hamming code is that it is used for detection of only one error. Because of this drawback we have check the data every time for the detection of error in each bit. But by using the Hamming code we can increase the performance of the encrypted data. In the Hamming code, we have to find the number of check bits which will help us to find the error in the encrypted data. Then we have to identify the error and get rid of the error by using the check bits which will give the information whether the encrypted data is having any error or not.

This clearly explained by using an example where original 8-bit data is taken as A_0A_1 A_2 A_3 A_4A_5 A_6A_7.This is represented as 'D'. Now 1's complement of 8-bit data $A'_0A'_1$ A'_2 A'_3 $A'_4A'_5$ $A'_6A'_7$ which is represented as complemented data. Based on the select lines S_1S_0 the complemented data is swapped and we get a swapped data SD. The swapped data is XOR'ed with the original data; we get a XOR'ed data i.e. X. XORed is combined with the key data and we get an encrypted data i.e. E.

The encrypted data i.e. E is separated into key data (K) and swapped data(X). Key data and swapped data is XOR'ed to get and decrypted data i.e. D original data.

Table 2 and table are showing that the steps involved in the encryption and decryption.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Data Encryption Steps

Original 8-bit data		10 01 11 00	$D = A_0A_1\ A_2A_3\ A_4A_5\ A_6A_7$
8-bit Key (1's complement of 8-bit data)		01 10 00 11	$K = A'_0A'_1\ A'_2A'_3\ A'_4A'_5\ A'_6A'_7$
8-bit swapping data (Swap Mode-S_1S_0)	00	11 00 10 01	$SD_1 = A_4A_5\ A_6A_7\ A_0A_1\ A_2A_3$
	01	01 10 11 00	$SD_2 = A_2A_0\ A_3A_1\ A_5A_4\ A_7A_6$
	10	11 01 10 00	$SD_3 = A_4A_5\ A_2A_3\ A_0A_1\ A_6A_7$
	11	01 10 00 11	$SD_4 = A_2A_3\ A_0A_1\ A_6A_7\ A_4A_5$
8-bit XORed data	00	10 10 10 10	$X_1 = (D \wedge (SD_1))$
	01	00 00 11 11	$X_2 = (D \wedge (SD_2))$
	10	10 11 10 11	$X_3 = (D \wedge (SD_3))$
	11	00 00 00 00	$X_4 = (D \wedge (SD_4))$
16-bit encrypted data (Swap Mode-S_1S_0)	10 10 10 10	01 10 00 11	$E_1 = \{X_1, K\}$
	00 00 11 11	01 10 00 11	$E_2 = \{X_2, K\}$
	10 11 10 11	01 10 00 11	$E_3 = \{X_3, K\}$
	00 00 00 00	01 10 00 11	$E_4 = \{X_4, K\}$

Table 3: Data Decryption Steps

16-bit encrypted data (Swap Mode-S_1S_0)	10 10 10 10	01 10 00 11	$E_1 = \{X_1, K\}$
	00 00 11 11	01 10 00 11	$E_2 = \{X_2, K\}$
	10 11 10 11	01 10 00 11	$E_3 = \{X_3, K\}$
	00 00 00 00	01 10 00 11	$E_4 = \{X_4, K\}$
8-bit XORed data	S_0	11 00 10 01	$X_1 = \{X_1 \wedge K\}$
	S_1	01 10 11 00	$X_2 = \{X_2 \wedge K\}$
	S_2	11 01 10 00	$X_3 = \{X_3 \wedge K\}$
	S_3	01 10 00 11	$X_4 = \{X_4 \wedge K\}$
8-bit swapping data (Swap Mode-S_1S_0)	S_0	11 00 10 01	$SD_1 = A_4A_5\ A_6A_7\ A_0A_1\ A_2A_3$
	S_1	01 10 11 00	$SD_2 = A_2A_0\ A_3A_1\ A_5A_4\ A_7A_6$
	S_2	11 01 10 00	$SD_3 = A_4A_5\ A_2A_3\ A_0A_1\ A_6A_7$
	S_3	01 10 00 11	$SD_4 = A_2A_3\ A_0A_1\ A_6A_7\ A_4A_5$
Original 8-bit data	10 01 11 00		$D = A_0A_1\ A_2A_3\ A_4A_5\ A_6A_7$

4. FPGA IMPLEMENTATION AND SIMULATION RESULTS

A field-programmable gate array (FPGA) is a semiconductor device that can be programmed after manufacture to perform a specific application design, typically specified as a digital logic system. Taxonomy of FPGAs commonly starts with the program storage technology. Figure 4 and figure 5 are showing the RTL schematic view of encryption and decryption systems.

Table 4: Fpga Synthesis Report

Synthesis Element	Encryption	Decryption
Number of Slice LUTs	16	8
Number of LUT Flip Flop pairs	16	8
Number of bounded IOB	26	24
Total memory usage	449032 kilobytes	351416 kilobytes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

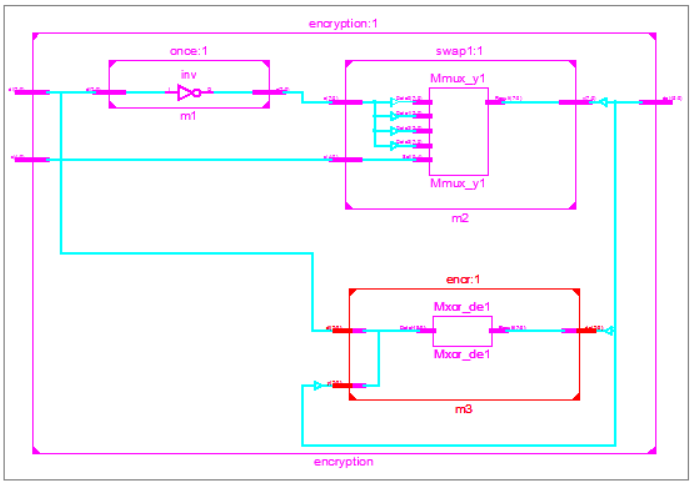

Figure 4: RTL Schematic View Of Encryption System

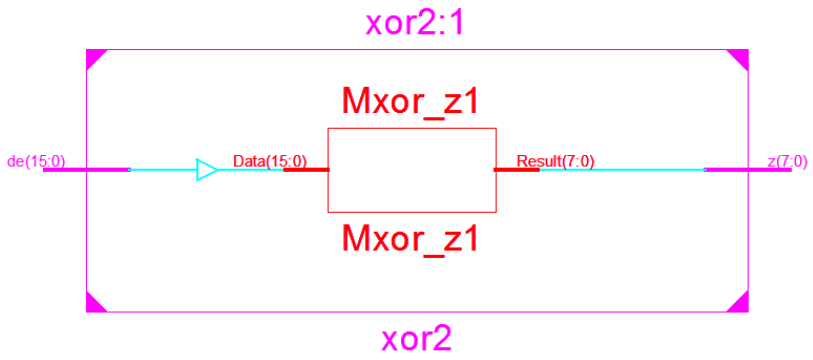

Figure 5: RTL Schematic View Of Decryption System

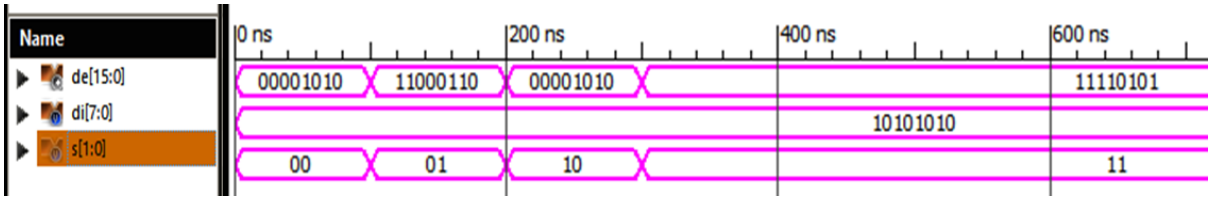

Figure 6: Simulation Results Of Data Encryption Process

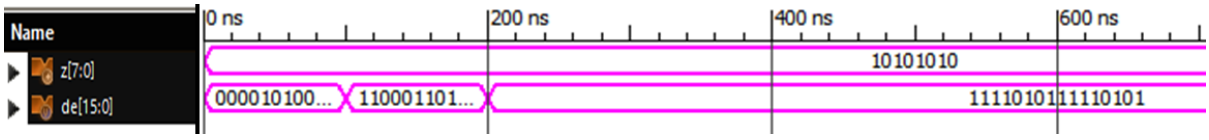

Figure 7: Simulation Results Of Data Decryption Process

Table 4 show the FPGA synthesis report. *Encryption timing analysis:* Maximum combinational path delay: 1.611ns. Total REAL time to Xst completion: 28.00 secs. Total CPU time to Xst completion: 28.16 secs. *Decryption timing analysis:* Maximum combinational path

delay: 0.757ns. Total REAL time to Xst completion: 22.00 secs. Total CPU time to Xst completion: 21.76 secs.

Figure 6 and figure 7 shows the simulation results of data encryption and decryption process. Where 's' is swap mode data it is a two bit vector, by setting these two data bits we can get four different type of modes. 'di' is input data it is 8-bit. 'de' is 16-bit encrypted hamming code data. 'z' is 8-bit decrypted data.

In this process hamming code module is used advantage is it can detect and correct one bit data error. But drawback is it cannot correct more than one error bits.

5. CONCLUSIONS

From our work we have concluded that FPGA implementation of cryptographic systems for symmetric systems can be implemented using Xilinx. Our algorithm is quite easier to design having less complexity and deals with swapping numbers. Time taken for encrypting and decrypting the message is less and the process is very efficient because simple methods are employed. Use of symmetric key insures verification and privacy. Algorithm absolutely satisfies the necessities of a high-quality encryption algorithm for providing secure communication. This proposed algorithm converts the 8-bit original data into 16-bit encrypted – hamming coded data and 16-bit encrypted – hamming coded data into 8-bit original data. This same method can be used for more number of input data bits.

REFERENCES

[1] T. Narendra Babu, Fazal Noorbasha, M. Harita, N. Tejashree and K. Vamsi Krishna, "FPGA Implementation of High Speed Error Detection and Correction of Orthogonal Codes using Segmentation Method", Indian Journal of Science and Technology, Vol 9(30), August 2016, PP. 1-7.

[2] P. M. Durai Raj Vincent, Syed Amber Iqbal, Karan Bhagat and Kamal Kant Kushwaha, "Cryptography: a Mathematical Approach", Indian Journal of Science and Technology, Vol 6(12), December 2013, PP 5607–5611.

[3] Narendra Babu T., Fazal Noorbasha, Sai Krishna Ch., Sai Charan K. and R. S. V. S. Sai Kalyan, "FPGA implementation of cryptographic system using BODMAS sequence of operations", ARPN Journal of Engineering and Applied Sciences, Vol. 11, No. 19, October 2016, PP. 11475- 11479.

[4] Tulasimani Lakshmanan, Madheswaran Muthusamy, "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[5] Upputuri Neelima, Fazal Noorbasha, "Data Encryption and Decryption using Reed-Muller Techniques", International Journal of Engineering and Technology (IJET), Vol 8, No 1, Feb-Mar 2016, PP 83-91.

[6] Xiao-Bie Liu, Soo Ngee Koh, Chee-Cheon Chui and Xin-Wen Wu, "A study on reconstruction of linear scrambler using dual words of channel encoder", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 3, March 2013, PP. 542-552.

[7] Narendra Babu T, Fazal Noorbasha, Leenendra Chowdary Gunnam, "Implementation of High Security Cryptographic System with Improved Error Correction and Detection Rate using FPGA ", International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 2, April 2016, pp. 602-610.

[8] Câncio Monteiro,Yasuhiro Takahashi,Toshikazu Sekine, "Low-power secure S-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design", IET Circuits, Devices & Systems, Vol.9, Iss.5, 2015, PP.362–369.

[9] Fazal Noorbasha, K. Sundar Teja, Bhavana Endreddy, Nikitha Adidela and Ch. Naga Pavan Kumar, "Implementation of Cryptography Algorithm with Adders and Subtractor", Indian Journal of Science and Technology, Vol 10(4), January 2017, PP. 1-9.

[10] Junzuo Lai, Deng R H, Chaowen Guan, JianWeng, Attribute-Based Encryption With Verifiable Outsourced Decryption, in IEEE Transactions on Information Forensics and Security, vol. 8(8), pages 1343-1354,2013.

[11] Fatemi Moghaddam F,KarimiO, Alrashdan M T, A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments, in IEEE 2nd International

Conference on Cloud Networking (CloudNet),pages 185-189, 2013.

[12] Lan Zhou, Varadharajan V, Hitchens M, Integrating Trust with Cryptographic Role-Based Access Control for Secure Cloud Data Storage Trust, in 12th IEEE International Conference on Security and Privacy in Computing and Communications (TrustCom), pages 560-569, 2013.

[13] Qin Liu, Tan CC, Jie Wu, Guojun Wang, Reliable Re Encryption in Unreliable Clouds, in IEEE International Conference on Global Telecommunications (GLOBECOM),pages 1-5, 2011.

[14] Miwen, Rongxinglu, Kuanz hang, Jing Shenglei, Xiaohuiliang and Xueminshen, PaRQ: A Privacy Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid, in IEEE International Journal of Computer Networks, pages 178-191, 2013.

[15] Gholase M, Takare LP, Deshmukh AY., "Enhancement of error detection and correction capability using orthogonal code convolution", International Journal of Computational Engineering Research, April-2013; 3(4), PP: 66-71.

[16] Narendra Babu T, Fazal Noorbasha, Gunnam LC., "Implementation of high security cryptographic system with improved error correction and detection rate using FPGA", International Journal of Electrical and Computer Engineering, April-2016; 6(2), PP.602-610.

[17] Trio Adiono, Vincentius Timothy, Nur Ahmadi, Aditya Candra, Khafit Mufadli, "CORDIC and Taylor based FPGA music synthesizer ", IEEE TENCON 2015, 1-4 Nov. 2015, DOI: 10.1109/ TENCON.2015.7372964.

[18] Vishwanath S Mahalle, Aniket K Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm ", International Conference on Power, Automation and Communication (INPAC), 6-8 Oct. 2014, DOI: 10.1109/INPAC.2014.6981152.

[19] Gaurav R. Bagwe , Dhanashree S. Apsingekar , Sayali Gandhare , Smita Pawar, "Voice encryption and decryption in telecommunication ", International Conference on Communication and Signal Processing (ICCSP), 6-8 April 2016, DOI: 10.1109/ICCSP.2016.7754475.