International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Design and implementation of a XOR-Free Lightweight Crypto-Coder System

Jeena Jose[1], David Solomon George[2]

[1] *PG Scholar, Dept. of Electronics and Communication Engineering, Government Engineering College, Idukki, Kerala, India*

[2]*Associate Professor, Dept. of Electronics and Communication Engineering, Government Engineering College, Idukki, Kerala, India*

Abstract - *Handheld mobile devices use wireless 3GPP standards such as GSM, CDMA, etc. for the purpose of communication. Convolutional encoders are used for this purposes to obtain reliability and accuracy. Apart from the above constraints, secure transmission of data is highly desirable. For secure and accurate transmission of data, crypto-coder system is used which combines channel coding with cryptographic coding technique. In this paper, a XOR-free lightweight crypto-coder system for GSM 900 communication standard is proposed with properties of reduced hardware, reduced power consumption and increased speed of operation. Comparison of XOR -free lightweight system with existing one shows a hardware efficiency of 54.33%, delay reduction of 72.36% and power reduction of 24.24%. The system simulation is validated in Xilinx 14.2 ISE and implemented in Xilinx Spartan-3E FPGA.*

Key Words: **GSM, Convolutional encoder, Crypto-coder system, Security, Accuracy, and Xilinx**

1. INTRODUCTION

Wireless communication through hand held devices (such as mobile phones) uses 3GPP standards. Data transmission through wireless channels poses major problem of security, reliability and accuracy.

In digital communication, long distance data transmission is accomplished through channel coding mechanism. Channel coding facilitates efficient data transmission by incorporating the properties of error detection and error correction by adding redundant bits to the transmitted message. For this Forward Error Correction (FEC) codes are used [1]. FEC is classified into block and convolutional codes, of which convolutional codes are generally preferred.

Modern era face the problem of secure data transmission since the increase in number and intensity of cyber threats is high. In spite of this, people are concerned with the privacy of communication not only for confidential data but also for casual daily communication purposes (especially in text messages, online chatting, etc.). Data security is ensured by many cryptographic coding schemes of which AES is widely used due to its ease of realization in both hardware and software.

Popularity of handheld devices especially mobile phones have increased in the past few decades and the trend keeps on increasing with demands in small size, low power consumption and increased speed. Communication modules play an important role in these devices and the above mentioned parameters are crucial for its construction. By incorporating the properties of security, reliability and accuracy into these systems bring in the need for crypto-coding systems. The concept of crypto coding is in traduced by McEliece [2] in 1978.

In this paper, a XOR-free convolutional encoder is combined with Authenticated Lightweight Encryption (ALE) method based on AES to form the XOR-free crypto-coder system for reduced hardware and low power design.

2. CRYPTO-CODER SYSTEM BASED ON CONVOLUTION ENCODER

An Encryption-Encoder based on AES is described in [3]. Crypto-coder system based on convolutional encoder consists of an encryption-encoder at the transmitter side and a decryption-decoder at the receiver. Encryption encoder consists of a convolutional encoder, AES cryptographic module and an authentication module. Viterbi decoder is used for decoding purpose. The system is validated in an AWGN (Additive White Gaussian Noise) channel. Block diagram of crypto-coder system based on convolution encoder is shown in Fig -1.

2.1 Convolutional Encoder

Convolution encoder maps information bit to be encoded sequentially and is convolved depending on some rule. The encoder is realized in Galois Field (GF) in which multiplication and addition is represented in modulo-2 operation i.e. XOR operation. Fig -2 shows a convolutional encoder for GSM 900 communication standard with a

constraint length (K) of 5, code rate (k) of ½ and generator polynomial of $g_0 = 11001$ and $g_1 = 11011$. Number of shift registers (which act as memory elements) used is 4 i.e. (K-1).

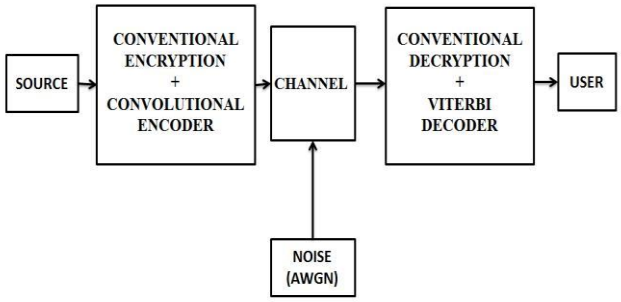

Fig -1: Block diagram of crypto-coder based on convolution encoder

Input sequence enters into the encoder at every clock cycle pushing the previous value through the shift register stages sequentially. The encoded output from the system is obtained depending upon the generator polynomial and the denominator of the code rate gives the number of encoded output.

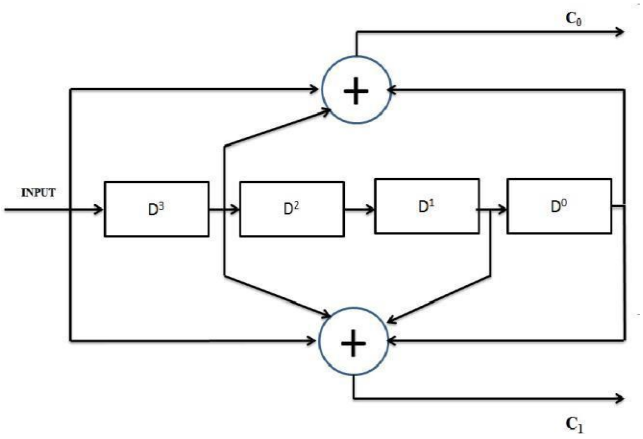

Fig - 2: Convolutional encoder for GSM 900 standard with code rate of 1/2

2.2 AES Module

Advanced Encryption Standard (AES) is the first publically accessible open cipher which is widely used for encryption and decryption purpose due to its ease of implementation in both hardware and software. It is established by U.S. NIST (National Institute of Standards and Technology) in 2001. AES-128 is used for lightweight purpose where 128 represent the input bit as well as key size. It consists of 10 rounds with four stages of transformation namely, Add-Round key, Shift-row, Mix-Column and Substitution Byte transformation. Architecture of AES-128 is shown in Fig -3. Details of each transformation stage are found in [4].

2.3 Viterbi Decoder

Viterbi algorithm [5] is an efficient decoding method for channel coding methods like convolutional encoders, Trellis codes, etc. with maximum likelihood decoding capability. Block diagram of Viterbi decoder [6] is shown in Fig - 4.

Branch Metric Unit (BMU) stores the weight on each branch which is the Euclidian distance between two levels in the Trellis diagram. Path Metric Unit (PMU) stores the sum of branch metric values upto the current level. Add-Compare Select (ACS) unit adds branch metric value with the previous path metric value and finds the minimum path metric upto that stage. Survivor memory management unit traces back through minimum path metrics at each level to find the decoded output.

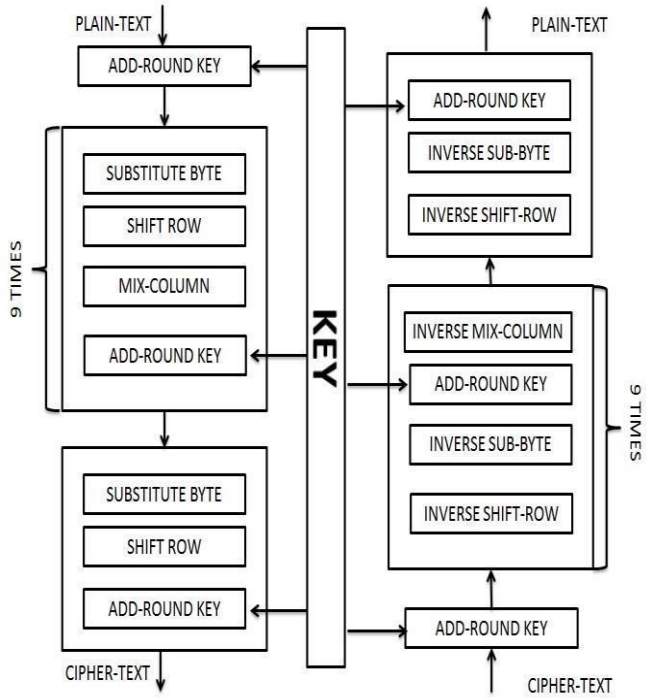

Fig - 3: Architecture of AES-128 [4]

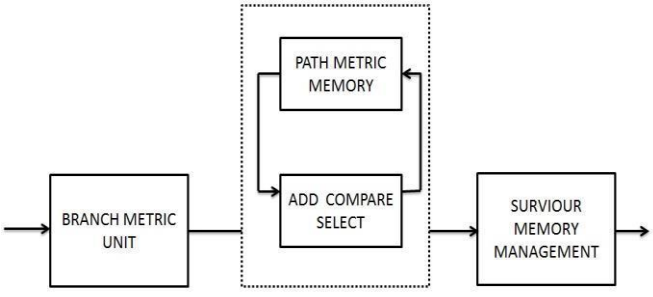

Fig - 4: Block diagram of Viterbi decoder [6]

2.4 Data Integrity Module

Data integrity module is incorporated into the system for authentication purpose i.e. to ensure that the transmitted message does not undergo any alteration before entering the receiver. Hash function along with Toeplitz method is used for integrity verification. During each message bit, the hash function is shifted one bit right and the MSB is replaced by the message bit. After the message has completely arrived, the intermediate digests obtained when the message bit was '1' will be XORed to provide the final digest. Digest is the output obtained after treating the input with hash function. The digest will be transmitted along with the transmitted data.

2.5 Channel

An AWGN channel is used to validate the design where a random noise is added to the transmitted signal which will be removed at the decoder end.

3. XOR-FREE LIGHTWEIGHT CRYPTO-CODER SYSTEM

In this system, conventional convolutional encoder is replaced by a XOR-free encoder and AES is replaced by ALE (Authenticated Lightweight Encryption) design. The block diagram of the proposed system is shown in Fig - 5.

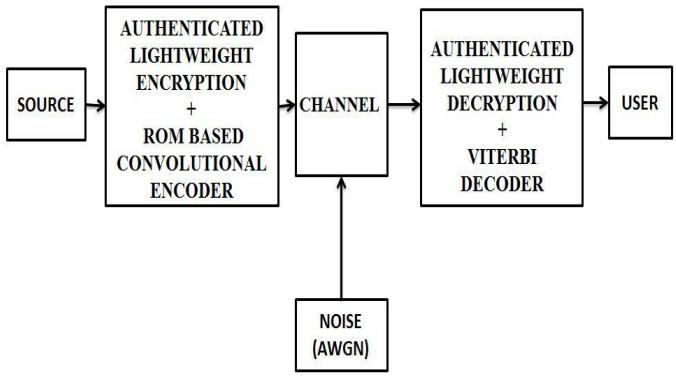

Fig - 5: Block diagram of XOR-free Crypto-coder

3.1 XOR-free Convolutional encoder

In the XOR-free system, the XOR gates are replaced with a multiplexer and ROM. The encoder output is stored in the ROM which can be pre-computed. There will be 2^4 i.e. 16 states for which there will be only four output states i.e. {00, 01, 10, and 11}. Output of the encoder states is determined by the generator polynomials.

Initially, the MSB of encoder states are appended with input '0'. The states with similar output is grouped and then split into Row Tag (RT) and Column Tag (CT) based on the following equations:

$$CT = k^{-1} = 2$$
$$RT = [K - \{CT + 1\}] = 5 - (3 + 1) = 2$$

Algorithm for reduction of the states is obtained from [7]. 32 states of the system is reduced to 8 states. The reduced ROM table is given in Table -1.

Table –1: Reduced ROM Structure

RT/CT	00	01	10	11
0	00	11	01	10
1	11	00	10	01

Fig -6 shows the block diagram of XOR-free convolutional encoder for GSM 900. The 2:1 MUX is used to select the row tag with MSB of shift register as select bit and LSB as column tag.

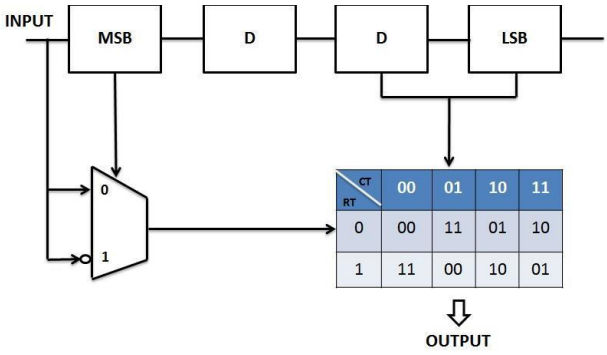

Fig -6: XOR-free Convolutional Encoder

3.2 Authenticated Lightweight Encryption

Lightweight cryptographic methods are becoming popular as it can be used in mobile devices. This method can solve the problems related to hardware complexity and power consumption. The term ALE is coined in [8]. The backbone of the system resembles AES-128. The architecture differs mainly in the S-box construction where the 256 sized S-box is replaced by a combination of gates which is reversible. Moreover, the input data size is also reduced. The S-box construction is based on Littlun-1 concept [9].

4. RESULTS AND DISCUSSION

The system is designed using Xilinx ISE 14.2 Design Suite and implemented in Spartan-3E FPGA Basys2 board. Simulation result, RTL, schematic, device utilization summary

and power consumed by the system is discussed in this section.

Fig -7 show the simulation window of a conventional crypto-coder system. It gives the output value for the corresponding inputs. Clock (clk) and reset (rst) are provided along with input (in) to obtain the decoded output (decode_out). Simulation result for both conventional and XOR-free crypto-coder system remains the same.

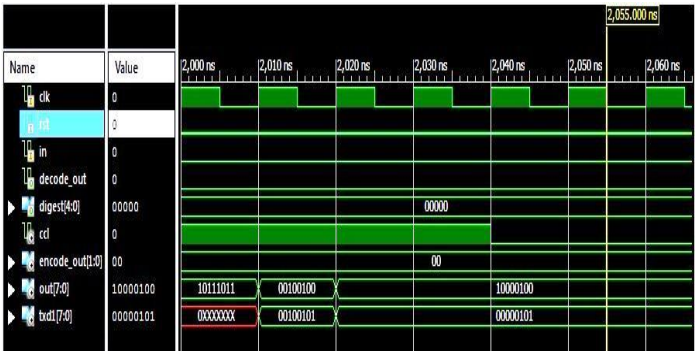

Fig -7: Functional simulation the system

Fig -8 gives the top level RTL of the system. This figure is similar to both systems where the only change comes at the cryptographic module and encoder module.

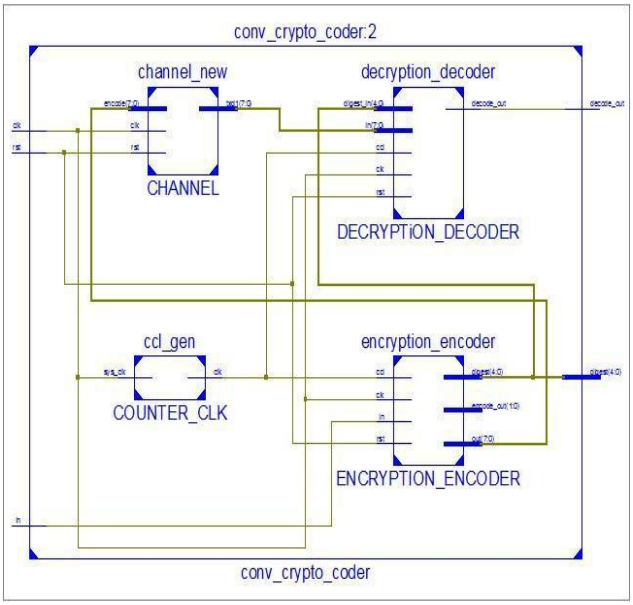

Fig –8: RTL of conventional crypto-coder system

Table - 2 shows the device utilization summary along with delay and power. A major reduction is obtained in the total number of 4-inout LUTs i.e. from 860 to 325. Similarly delay of the systems also reduces from 76 ns to 21 ns. Power reduction obtained is in mill watts range.

Table -2: Performance analysis of crypto-coder systems

Summary of crypto-coder system	Conventional system	XOR-free System
Total no. of slice registers	216	203
No. of occupied slices	576	291
Total no. of 4 input LUTs	860	325
Delay (ns)	76	21
Power (mW)	92	69.7

Chart -1 gives the graphical representation of device utilization summary. It gives the number of slice registers used, number of 4-input LUTs and the number of occupied slices.

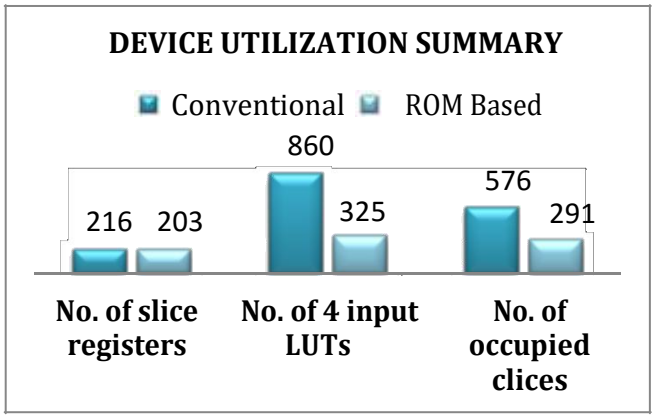

Chart -1: Device utilization summary

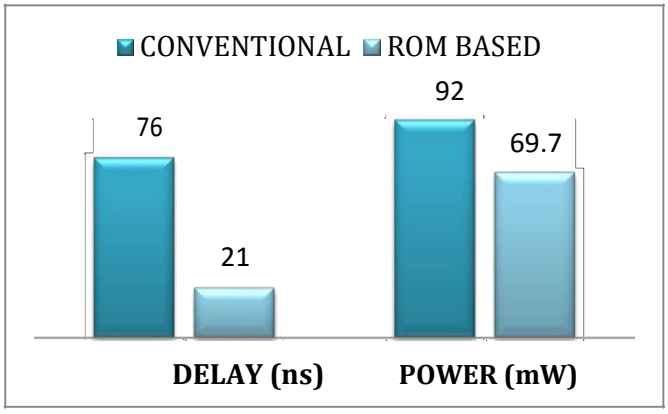

Chart -2: Delay and power variations

Chart -2 shows the variation in delay and power obtained. Delay changes from 71 ns to 21 ns and power from 92 mW to 69.7 mw. The whole design gives a hardware efficiency of 54.33%, power efficiency of 24.24% and delay reduction efficiency of 72.36%.

5. CONCLUSIONS

This paper introduces a XOR-free lightweight crypto-coder system which contains a XOR-free convolutional encoder instead of conventional encoder and ALE based cryptographic module instead of AES-128 for GSM 900 communication standard. The design mainly focuses on small handheld devices with design goals of hardware and power reduction along with increase in speed. The system is designed in Xilinx ISE 14.2 design suite and implemented in Spartan-3E FPGA. A hardware efficiency of 54.33%, power reduction of 24.24% and delay reduction of 72.36% is obtained.

REFERENCES

[1] J. Viterbi, "Convolutional codes and their performance in communication systems", IEEE Trans. Commun. Technol., vol. 19, no. 5, pp. 751–772, Oct. 1971.

[2] R. J. McEliece, Robert, "A public-key cryptosystem based on algebraic coding theory" DSN progress report, vol. 42, no. 44, pp. 114-116, 1978.

[3] Oluwayomi Adamol, Shengli Fu, and Murali Varanasi, "Hardware-Efficient Encryption Encoder and Decoder Unit", Military Communications Conference, MILCOM 2008, IEEE.

[4] William Stallings, "CryptoChart -y and network security principles and practice", Pearson publications, fifth edition, 2011, pg. 148 to 172.

[5] G. Davis Forney Jr., "The Viterbi algorithm", Proc. IEEE, vol. 61, pp. 268-278, March 1973.

[6] T. Kalavathi Devi and Sakthivel Palaniappan, "An Asynchronous Low Power and High Performance VLSI Architecture for Viterbi Decoder Implemented with Quasi Delay Insensitive Templates", Hindawi Publishing Corporation Scientific World Journal, Volume 2015, Article ID 621012, November, 2015.

[7] G. Purohit, K. S. Raju, V. K. Chaubey, "A New XOR-Free Approach for Implementation of convolutional Encoder", IEEE embedded systems letters, vol. 8, no. 1, March 2016.

[8] Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V., Tischhauser, E., "ALE: AES-Based Lightweight Authenticated Encryption", 20th International Workshop on Fast Software Encryption – FSE, 2013.

[9] Pierre, Karpman and Benjamin Grégoire, "The LITTLUN S-box and FLY block cipher", 2016.