International Journal of Research and Reviews in Applied Sciences And Engineering (IJRRASE) Vol 8. No.1 –2016 Pp.41-44

available at : www.ijcns.com
ISSN: 2231-0061

MIMO WIRELESS BASED CRYPTOSYSTEM USING ELECTRONIC KEY GENERATION UNIT

R.Sowndharya
Department of ECE
Meenakshi College Of Engineering
Chennai-600078, Tamilnadu,
India

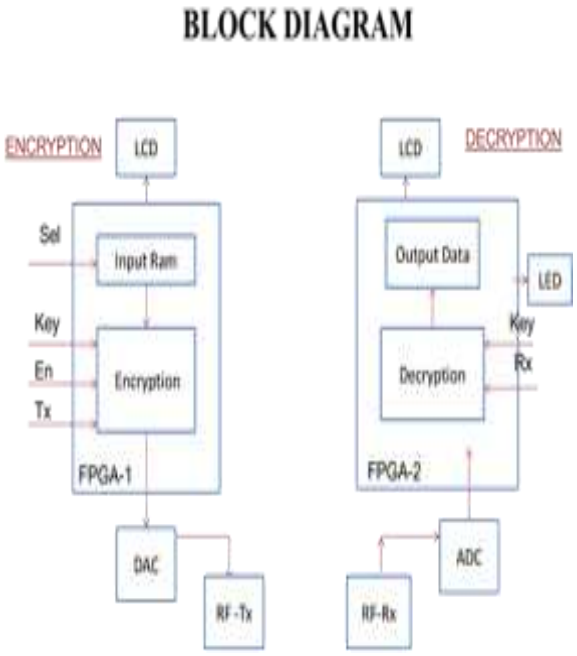
N.Thendral, Assistant Professor
Department of ECE
Meenakshi College of Engineering
Chennai-600078, Tamilnadu,
India

ABSTRACT----Wireless communication systems, multi-input multi-output (MIMO) technology has been field-programmable gate array (FPGA)-based software defined radio (SDR). The implementation of digital FTS in SDR platform is purely a new kind. Software Defined Radio (SDR) platform which replaces a multiple platform-based system with a single platform. In the existing system only one flight can be controlled but in the proposed system more than one flight can be controlled. As computer systems become more pervasive and complex, security is increasingly important. This paper attempts to develop a simple, stronger and safer cryptographic algorithm which would not only be a secure one, but also reduces total time taken for encryption and decryption. In the existing system, there are some security issues. Hence in order to provide security mechanism, we propose an algorithm called Modified Tiny Encryption Algorithm (MTEA). The modified algorithm MTEA is a new secret-key block cipher of 64 bit that uses good features of Tiny Encryption Algorithm (TEA). TEA consumes more time and security level is very low. So, I go for MTEA. In this paper i have use MIMO wireless based cryptosystem.

Keywords: Multi-input multi-output (MIMO), Modified or extended tiny encryption algorithm (MTEA), software defined radio (SDR), Flight termination system (FTS).

I.INTRODUCTION

The Key Generation unit is to provide the key for the Plain text. It is encrypted using Tiny Encryption Algorithm and transmitted either serial or wireless. Decryption unit is to decrypt the encrypted text to plain text by verifying the secure key. I design a short program which will run on most machines and encipher safely. It uses a large number of iterations rather than a complicated program. It is hoped that it can easily be translated into most languages in a compatible way. The first program is given below. It uses little set up time and does a weak non linear iteration enough rounds to make it secure.



II.PROPOSED SYSTEM

For achieving the faster communication most of confidential data transmitted through the network. Cryptographic algorithms are used to improve the security. These algorithms are classified into symmetric and asymmetric. The symmetric cipher is further classified into stream and block ciphers. The exponential growth in the ways and means by which people need to communicate-data communications, voice communications, video communications, broadcast messaging, command and control communications, emergency response communications. Software defined radio (SDR) technology brings the flexibility, cost efficiency and power to drive communications forward, with wide-reaching benefits realized by service providers and product developers through to end users. It consists of three units: Key generation Unit, Encryption unit and decryption unit. Key generation unit is to generate the key and these keys are sending along with cipher text. Modified TEA is used for encryption of the text. Then decryption unit for decrypting the cipher text and convert that to plain text.

A.MODIFIED TINY ENCRYPTION ALGORITHM (MTEA)

Modified Tiny Encryption Algorithm (MTEA) is a block cipher designed to correct weaknesses in TEA. This also uses the same three primitive operations like TEA. Plain text blocks size -64bits.Key size is 128 bits.32 rounds of operation.

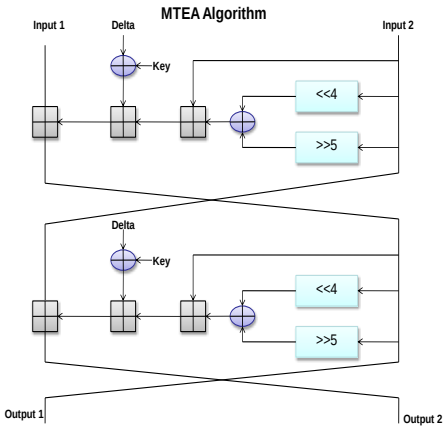


Fig 1.Block Diagram of Proposed System

Initially 64-bit input data is divided into two 32-bit data namely input1 and input2.Then input 2 is rotated left and right by 4 and 5 bits and saved in different registers. These 2 data are XORed and added with original input2.128-bit key is XORed with a constant(delta) and added with the previous data. Finally this data is added to input1 and then input1 and input2 are interchanged.

III.SOFTWARE DEFINED RADIO

A number of definitions can be found to describe Software Defined Radio, also known as Software Radio or SDR. The SDR Forum, working in collaboration with the Institute of Electrical and Electronic Engineers P1900.1 group, has worked to establish a definition of SDR that provides consistency and a clear overview of the technology and its associated benefits. Over-the-air or other remote reprogramming, allowing "bug fixes" to occur while a radio is in service, thus reducing the

time and costs associated with operation and maintenance.

A. Software Defined Radio - Rate of Adoption

The SDR Forum commissioned a number of research reports in 2006 to evaluate the adoption of SDR technologies in various markets. The results of these studies demonstrated that, in certain markets, SDR is moving beyond the innovators and early adopters as defined by Geoffrey Moore in "Crossing the Chasm" into the early majority phase.

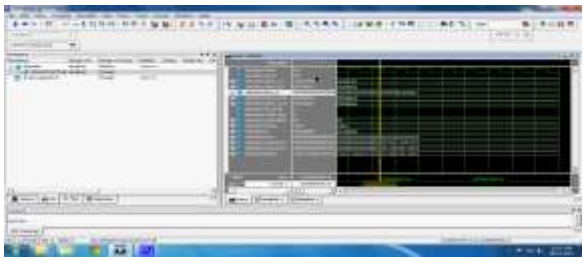
Fig 3.SDR Adoption

Figure 2. Software Defined Radio – Value Chain

IV. RESULTS AND DISCUSSION

Fig (a) Encipher

Fig(b)Decipher



Fig(c) Original Data

In the fig (a), encryption is done. Input 1, input 2 and key is given and the resulting enc1 and enc2 are noted. In the fig (b) and fig (c), decryption is done. The noted enc1 and enc2 is given to input 1 and input 2 respectively. We have to note that in fig (b), different key is given that is the key used in fig (a) is not given. So the output will be 0.When the key used in the fig (a) is given then the input data from the fig (a) is displayed as output for fig (c).

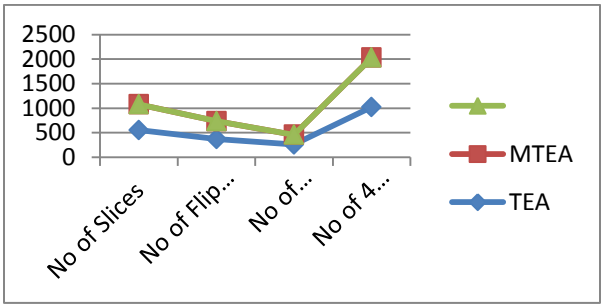


Fig 1. Comparison of the MTEA and TEA results

V.CONCLUSION

This project have implemented MTEA algorithm suitable for short distance communication. MTEA architecture is well suited for devices in which low cost and low power consumption are desired. The proposed folded architecture achieves good performance and occupies less area than TEA. I have compared size, complexity and

security level of TEA and MTEA crypto system. This paper improved the size and security level. Complexity level of MTEA is reduced. Which was compared using graph. The encryption speed, functionality, and cost make this solution perfectly applicable for resource constrained applications passive RFID and wireless sensor networks.

REFERENCES

[1]. Study on Cryptanalysis of the Tiny Encryption Algorithm …Rajashekarappa, K M Sunjiv Soyjaudah, Sumithra Devi K A (Feb 2013)

[2]. Implementation of a modified lightweight cryptographic TEA algorithm in RFID system..M.B.Abdelhalim et.al(2011)

[3]. To Improve Data Security by Using Secure Data Transmission…Manisha Yadav (Dec 2013)

[4]. Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack).. Ali Ahmad Milad, et al (2012)

[5]. Image Steganography Using Discrete CosineTransform (DCT) and Blowfish Algorithm presented by Monika Gunjal , Jasmine Jha (March 2014)

[6]. Compact Hardware Implementations of ChaCha, BLAKE, Threefish, and Skein on FPGA…. Nuray At et,al (Feb 2014)

[7]. A Modified XTEA…Niladree De, JaydebBhaumik (May 2012)

[8]. A Survey of Lightweight-Cryptography Implementations *Swarnendu Jana, Jaydeb Bhaumik, Manas Kumar Maiti International Journal of Soft Computing and Engineering (IJSCE).*

[9]. Algorithm and Architecture of Configurable Joint Detection and Decoding for MIMO Wireless Communications With Convolutional Codes *Chung-An Shen, Member, IEEE, Chia-Po Yu, and Chien-Hao Huang.*

[1O]. Chai-tea, Cryptographic Hardware Implementations of xTEA *Jens-Peter Kaps* Compact Hardware Implementations of chacha, BLAKE, Threefish, and Skein on FPGA *Nuray At, Jean-Luc Beuchat, Eiji Okamoto, Ismail San, and Teppei Yamazaki IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 61, NO. 2, FEBRUARY 2014.*

[11]. Efficient Tiny Hardware Cipher under Verilog *Issam Damaj Samer Hamade, and Hassan Diab Proceedings of the 2008 High Performance Computing & Simulation Conference ©ECMS Waleed W. Smari (Ed.) ISBN: 978-0-9553018-7-2 / ISBN: 978-0-9553018-6-5 (CD).*

[12]. Extended TEA Algorithms *Tom St Denis April 20th 1999* .

[13]. Impossible Di_erential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT *Jiazhe Chen, Meiqin Wang and Bart Preneel.*

[14]. New Lightweight DES Variants *Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm..*

[15]. Performance Analysis of Contemporary Light-Weight Block Ciphers on 8-bitmicrocontrollers. *S¨oren Rinne, Thomas Eisenbarth, and Christof Paar.*