International Conference on Computer Applications 2016 [ICCA 2016]

| | | | |
|---|---|---|---|
| **ISBN** | 978-81-929866-5-4 | **VOL** | 05 |
| **Website** | icca.co.in | **eMail** | icca@asdf.res.in |
| **Received** | 14 – March– 2016 | **Accepted** | 02 - April – 2016 |
| **Article ID** | ICCA014 | **eAID** | ICCA.2016.014 |

# MIMO Wireless based Cryptosystem using Electronic Key Generation Unit

**R Sowndharya[1], K Sasi Kumar[2]**

[1]PG Student, [2]Assistant Professor, Department of ECE, Meenakshi College of Engineering, Chennai, Tamilnadu, India

**Abstract:** *Wireless communication systems, multi-input multi-output (MIMO) technology has been recognized as the key ingredient to support higher data rate as well as better transmission quality after using this algorithm of a XTEA or MTEA scheme. Modified TEA is used for encryption of the text. Then decryption unit for decrypting the cipher text and convert that to plain text. Key generation unit is to generate 128bit key and these keys are send along with cipher text. Encryption and decryption system ensures the original data are send and received by the users in secured environment. The Received data are retrieving by the authorized users by providing key generation like private keys this Key Pattern generations provide more security to the messages. Extended tiny encryption algorithm or modified tiny encryption algorithm and tiny encryption algorithm are used to enhance the size, speed and security in the system. These algorithms are better compared to configurable joint detection decoding algorithm (CJDD) and valid symbol finder algorithm.*

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

## I. INTRODUCTION

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 we go for MTEA. In this paper we use MIMO wireless based cryptosystem.

This paper proposes a field-programmable gate array (FPGA)-based software defined radio (SDR). The implementation of digital FTS in SDR platform is purely a new kind. In this paper, we present a Software Defined Radio (SDR) platform which replaces a multiple platform-based system with a single platform. In the existing paper only one flight can be controlled but in the proposed paper 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 we go for MTEA. In this paper we use MIMO wireless based cryptosystem.

This is one of the most modern developments in IC integration. They include more than 10000 transistors per chip. They cannot be operated by normal programming and have specialized programming and coding techniques. Also they paved the way for ASIC designs, VLSI design flows and complex integrated circuits. They helped in revolutionizing the IC technology.

**Cite this article as:** R Sowndharya, K Sasi Kumar. “MIMO Wireless based Cryptosystem using ELECTRONIC Key Generation Unit”. *International Conference on Computer Applications 2016*: 70-73. Print.

Structured VLSI design is a modular methodology originated by Carver Mead and Lynn Conway for saving microchip area by minimizing the interconnect fabrics area. This is obtained by repetitive arrangement of rectangular macro blocks which can be interconnected using wiring by abutment. An example is portioning the layer of an adder into a row of equal bit slices cells. In complex designs this structuring may be achieved by hierarchialnesting. Structured VLSI design has been popular in the early 1980s, but lost its popularity later because of advent of placement and routing tools wasting lot of area by routing, which is tolerated because of the progress of Moore's law, When introducing the hardware description language KARL in the mid-1970s, Reiner Hartenstein coined the term "structured VLSI design".

## II. Architecture Model

### A. Description

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. The Tiny Encryption Algorithm (TEA) and DES.

### B. Tiny Encryption Algorithm (TEA)

We 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. There are no preset tables or long set up times. It assumes 32 bit words.

The Tiny Encryption Algorithm is a Feistel type cipher (Feistel, 1973) that uses operations from mixed (orthogonal) algebraic groups. A dual shift causes all bits of the data and key to be mixed repeatedly. The key schedule algorithm is simple; the 128-bit key K is split into four 32-bit blocks K = ( K[0], K[1], K[2], K[3]). TEA seems to be highly resistant to differential cryptanalysis (Biham et al., 1992) and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text).

Time performance on a workstation is very impressive. There has been no known successful cryptanalysis of TEA. It's believed to be as secure as the IDEA algorithm, designed by Massey and Xuejia Lai. It uses the same mixed algebraic group's technique as IDEA, but it's very much simpler, hence faster.

Also its public domain, whereas IDEA is patented by Ascom-Tech AG in Switzerland. IBM's Don Coppersmith and Massey independently showed that mixing operations from orthogonal algebraic groups performs the diffusion and confusion functions that a traditional block cipher would implement with P- and S-boxes. As a simple plug-in encryption routine, it's great. The code is lightweight and portable enough to be used just about anywhere. It even makes a great random number generator for Monte Carlo simulations and the like.

## III. Results and Discussion

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.

To increase the speed and security of communication system. To reduce hardware complexity. To adapt with many real time constraints by using Modified Tiny encryption algorithm. This section explains the related concept to be identified and the existing techniques and method how can use in the project explanation specified. Over all introductions about the previous system to be discussed follows. 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.

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.

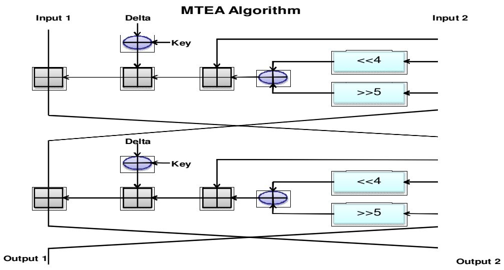
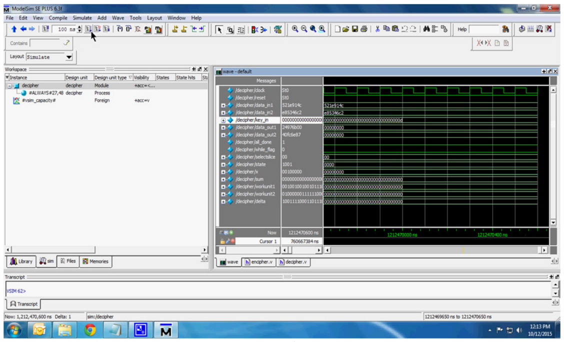


Fig 1 Block Diagram of Proposed System

- Thousands of software defined radios have been successfully deployed in defense applications
- Cellular infrastructure systems are increasingly using programmable processing devices to create "common platform" or "multiband multiprotocol" base stations supporting multiple cellular infrastructure standards.

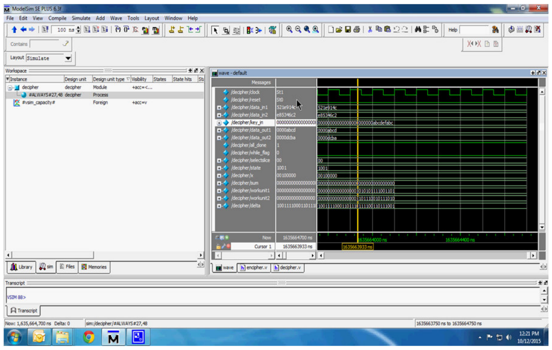
Snapshot is nothing but every moment of the application while running. It gives the clear elaborated of application. It will be useful for the new user to understand for the future steps.

Encipher



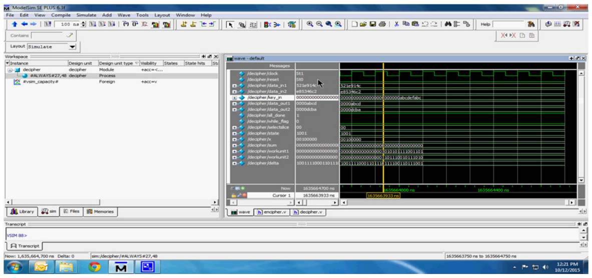
| Messages | |
|---|---|
| /decipher/clock | St0 |
| /decipher/reset | St0 |
| /decipher/data_in1 | 521e914c |
| /decipher/data_in2 | e85346c2 |
| /decipher/key_in | 0000000000000000 |
| /decipher/data_out1 | 24976b00 |
| /decipher/data_out2 | 40fc6e87 |
| /decipher/all_done | 1 |
| /decipher/while_flag | 0 |
| /decipher/selectslice | 00 |
| /decipher/state | 1001 |
| /decipher/x | 00100000 |
| /decipher/sum | 0000000000000000 |
| /decipher/workunit1 | 0010010010010111 |
| /decipher/workunit2 | 0100000011111100 |
| /decipher/delta | 1001111000110111 |
| Now | 1212470600 ns |
| Cursor 1 | 760667384 ns |

Decipher



| Messages | |
|---|---|
| /decipher/clock | St1 |
| /decipher/reset | St0 |
| /decipher/data_in1 | 521e914c |
| /decipher/data_in2 | e85346c2 |
| /decipher/key_in | 0000000000000000 |
| /decipher/data_out1 | 0000abcd |
| /decipher/data_out2 | 0000dcba |
| /decipher/all_done | 1 |
| /decipher/while_flag | 0 |
| /decipher/selectslice | 00 |
| /decipher/state | 1001 |
| /decipher/x | 00100000 |
| /decipher/sum | 0000000000000000 |
| /decipher/workunit1 | 0000000000000000 |
| /decipher/workunit2 | 0000000000000000 |
| /decipher/delta | 1001111000110111 |
| Now | 1635664700 ns |
| Cursor 1 | 1635663933 ns |

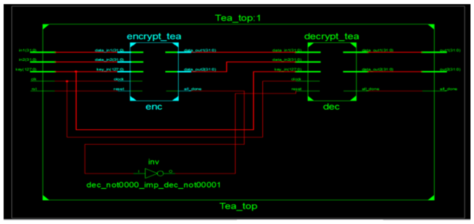
Original Data



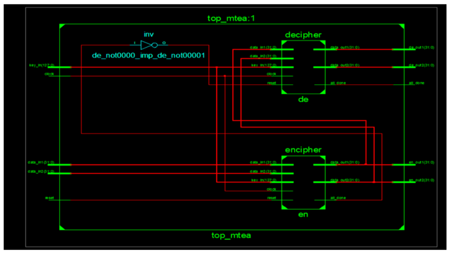
| Messages | |
|---|---|
| /decipher/clock | St1 |
| /decipher/reset | St0 |
| /decipher/data_in1 | 521e914c |
| /decipher/data_in2 | e85346c2 |
| /decipher/key_in | 0000000000000000 |
| /decipher/data_out1 | 0000abcd |
| /decipher/data_out2 | 0000dcba |
| /decipher/all_done | 1 |
| /decipher/while_flag | 0 |
| /decipher/selectslice | 00 |
| /decipher/state | 1001 |
| /decipher/x | 00100000 |
| /decipher/sum | 0000000000000000 |
| /decipher/workunit1 | 0000000000000000 |
| /decipher/workunit2 | 0000000000000000 |
| /decipher/delta | 1001111000110111 |
| Now | 1635664700 ns |
| Cursor 1 | 1635663933 ns |

**Cite this article as:** R Sowndharya, K Sasi Kumar. "MIMO Wireless based Cryptosystem using ELECTRONIC Key Generation Unit". *International Conference on Computer Applications 2016*: 70-73. Print.

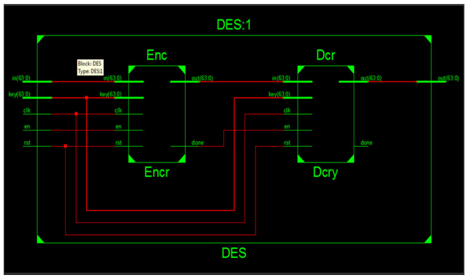
Schematic Digram for Tiny Encryption Algorithm



Schematic Diagram for MTEA



Schematic Diagram for DES



## 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. A Survey of Lightweight-Cryptography Implementations Swarnendu Jana, Jaydeb Bhaumik, Manas Kumar Maiti International Journal of Soft Computing and Engineering (IJSCE).
2. 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.
3. Chai-tea, Cryptographic Hardware Implementations of xTEA Jens-Peter Kaps
4. 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.
5. 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).
6. Extended TEA Algorithms Tom St Denis April 20th 1999
7. Impossible Di_erential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT Jiazhe Chen, Meiqin Wang and Bart Preneel
8. New Lightweight DES Variants Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm.
9. Performance Analysis of Contemporary Light-Weight Block Ciphers on 8-bitmicrocontrollers. S¨oren Rinne, Thomas Eisenbarth, and Christof Paar.
10. Software Defined Radio: The Software Communications Architecture By John Bard, Vincent J. Kovarik.

**Cite this article as:** R Sowndharya, K Sasi Kumar. “MIMO Wireless based Cryptosystem using ELECTRONIC Key Generation Unit”. *International Conference on Computer Applications 2016*: 70-73. Print.