# A secure data communication in Wi-Fi technology using Encryption And Decryption

**Fareed M.A**
**M.Tech Student,**
**(Digital Electronics and Communication Systems),**
**Department of ECE,**
**ACE Engineering College.**

**Dr. P. Sumithabhashini**
**M.Tech, Ph.D,**
**Professor,**
**Department of ECE,**
**ACE Engineering College.**

## Abstract-

This article proposes a new design scheme and hardware implementation of encryption system based on Wi-Fi technology. This system uses a digital chaotic encryption core based on FPGA. The initial key generated by Logistic digital sequence can be used to output stream cipher, by which the plaintexts are encrypted. Then the scheme realizes a safe and reliable information transmission by Wi-Fi module. This paper embeds the scheme into two modules. The simulation and synthesis results show that the system is available.

## Keywords:

Wi-Fi technology; FPGA; digital chaotic encryption; secure transmission.

## I.INTRODUCTION:

With the developments of mobile communication technology, more and more people are obsessed with the Internet. However, there are many vulnerabilities on the internet, the information transmission process can easily be monitored or theft. Thus, the security and reliability problems of information in transmission need much attention [1]. This paper designs a digital chaotic encryption core based on FPGA, which combined with Wi-Fi technology to achieve data secure transmission as mentioned in [2] and [3]. The data is encrypted at the sender and transferred to the remote receiver. This algorithm has a high security feature and can be easily applied, thus the intercepted cipher text cannot be deciphered.

Meanwhile, legitimate receiver takes the corresponding decryption algorithm to recover the plaintext data, so that a safe and reliable transmission can be achieved [4]. The detail of this article is organized as follows. In Section2, it describes the overall scheme design of Wi-Fi technology based encryption system. Section 3 introduces the scheme design the module of hardware circuit. Then, in Section 4 it shows the hardware implementation and analysis results. Finally, comes to the conclusion in Section 5.

## II.THE OVERALL SCHEME DESIGN OF WI-FI TECHNOLOGY BASED ENCRYPTION SYSTEM:
## A. Logistic Chaotic Encryption Theory:

This system uses the Logistic digital sequence ciphers to generate initial keys. This stream cipher is stream cipher. Initial key sequences such as $Z= \{Z_i\}$ are generated from Logistic digital sequences. System uses $\{Z_i\}$ to encrypt the plaintext sequence $m=\{m_i\}$ bit by bit to obtain the cipher text $c=\{c_i\}$[5].

In practical stream cipher, we can identity a key sequence by using algorithm. The stream cipher conversion formulas are shown in equation (1) and (2).

$$C_i = m_i \oplus z_i \qquad (1)$$
$$m_i = c_i \oplus z_i \qquad (2)$$

The security of sequence password mainly depends on the security of the key sequence. Suppose $\{z_i\}$ is an uniformly distributed random binary sequence, then the password system is for the one-time pad system and the information is undecipherable [6].

However, the sequence cipher is a pseudo random sequence produced by k and a certain algorithm, so it's very significant to generate other better performance stream cipher in the near future [7]. This system uses chaotic encryption algorithm and digital circuit theory. The schematic diagram of the encryption algorithm is shown in Fig.I.

The embedded encryption core part is to realize information data encryption. The encryption algorithm in the core can be changed, and because it is a high performance FPGA technology, so during the upgrade process the encryption core can be substituted without changing the circuit [8]. Encryption reset and upgrade of the system are very convenient.
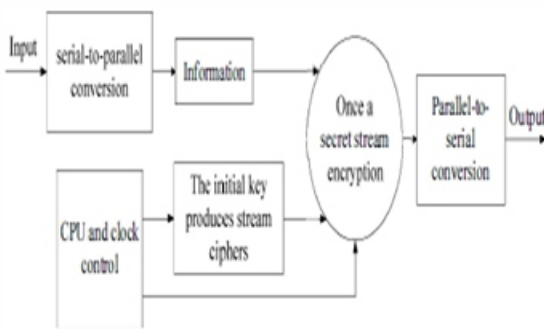


**Fig 1. The schematic diagram of the encryption algorithm**

## B. System Design Principles:

The Wi-Fi encryption system is composed of eight parts: the initial value of transmit side / plaintext input section, the plaintext display part at the sending side, the chaotic encryption core of sending side, Wi-Fi sender module, Wi-Fi receiving side module, decryption key input section at the receiving side, receiving side displaying part and the chaos decryption core of receiving side [9].

The project's overall design concept is based on FPGA chip as the core controller, the general PS2 keyboard as an information input device, 12864 as a display device and Wi-Fi module as the wireless transceiver equipment. Through this way, the system can achieve a safe and reliable transmission of information [10]. Apart from this, we also extend the wireless communication transmission between the FPGA-Wi-Fi module and the Laptop.

Under the control of the main controller, this project can use simplex structures. The sender and receiver side are two parts of this system. With this overall project design, we realized the system in the laboratory.

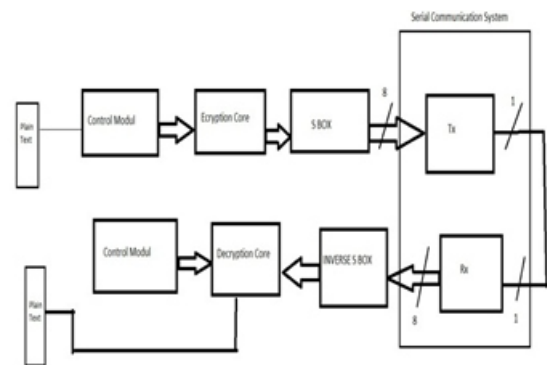**The principle diagram of this scheme is shown in Fig.2.**



**Fig 2. The principle diagram of this overall scheme design of encryption algorithm.**

## III.THE SCHEME DESIGN OF HARDWARE CIRCUIT MODULE:

The Wi-Fi based encryption system consists of two modules: Wi-Fi circuit and FPGA circuit. The system uses the chaotic encryption core to encrypt the information, and achieve the real-time information. The transmission completely depended on the hardware implementation, and it is enhancing the reliability and security of the encryption.

To achieve long-range wireless information transmission, we select Wi-Fi module. The sender includes: clock module, potter rate generator, reset module, PS2 controller module, LCD liquid crystal display module, the main control CPU module, generating chaotic key module, encryption module, buffer module and the asynchronous serial transmission module.

The composition of receiver is the same as above. In Fig.3, it shows the software working flow chart of development board for this system realization.
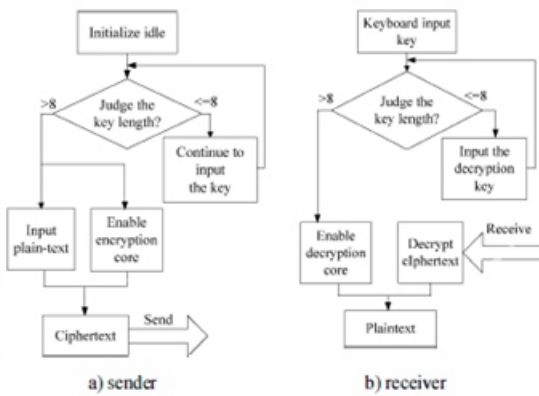
Fig 3. The flow chart by VHDL language in development board

This system uses the design scheme given above and FPGA with high performance. The system downloads encryption / decryption algorithm IP core into FPGA, which easily improved the performance of encryption algorithm in IP core without changing any circuits and just by downloading different IP cores.

This system not only can realize different algorithms, but also saves time and energy. The technology in this system has been tested for the performances of real-time encryption, decryption and safe authentication etc. Thus, encryption reset and upgrade of the system are very convenient.

The hardware module of chaotic sequence generator is shown in FigA. And Fig.5 demonstrates the photo of hardware circuit board.

## IV.HARDWARE IMPLEMENTATION AND PART OF THE TEST ANALYSIS:

Chaos system is a complex nonlinear dynamic system, which has good pseudo random property, orbital unpredictability, and extremely sensitive characteristic for initial value as mentioned in [11] and [12]. These characteristics make chaotic secure communication become an important research subject in the secure communication field. The initial key of sequence generator adopt Logistic chaotic algorithm and allow it to participate in the operation [13]. The matlab simulation diagram of original Logistic sequence and the digital Logistic chaotic sequence is shown in Fig.6.

The whole project is based on the Logistic equation, and its purpose is to design a new digital chaotic generator. It's very powerful, and it can get the initial values, perform the mathematical operations etc. The Logistic chaotic module simulation result is shown in Fig.4.

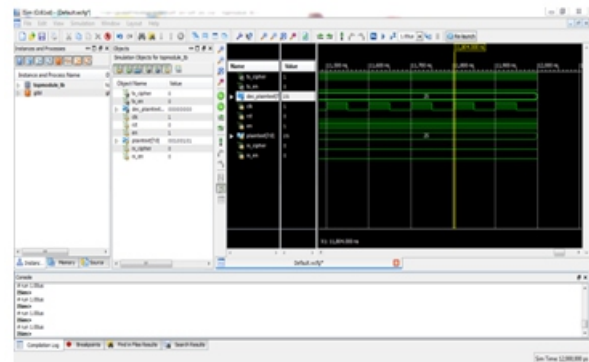## V.RESULTS
## Simulation Results:



Fig 4: Simulation Result of Communication System:
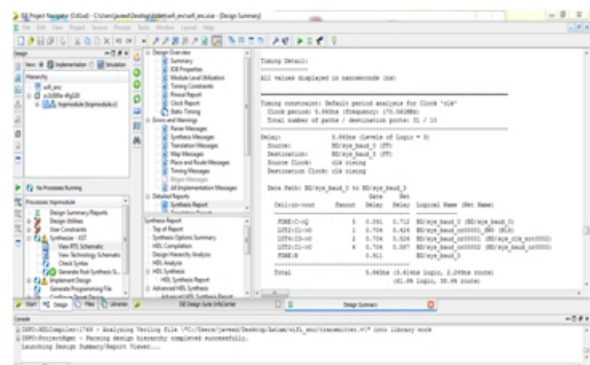## Timing Report:



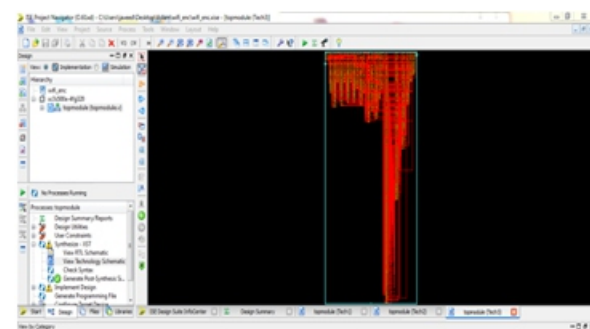Fig 5: Timing Report of Communication System
## RTL Schematic:



Fig 6: RTL Schematic of Communication System
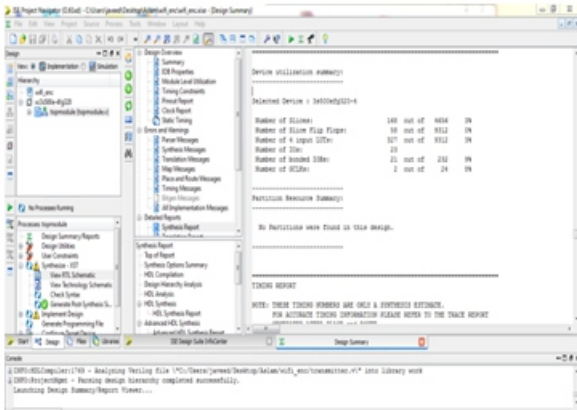
## Device Utilization Report:



**Fig 7: Device Utilization Report of Communication System.**

## VI.CONCLUSION AND PROSPECT:

This article designs a security encryption system based on Wi-Fi technology and has shown its software implementation results. This system uses a digital chaotic encryption core based on FPGA, in which Logistic digital sequence generates the initial key and uses its output stream cipher to encrypt the plaintext, then it uses Wi-Fi module to realize a safe and reliable transmission of information. These two development modules can realize the goal of our scheme design successfully.

This article, it illustrates the overall design framework, the schematic diagram, Simulation and synthesis results of the chaotic encryption algorithm, of this Wi-Fi encryption system. Meanwhile, we make some optimization design on speed and interface to cater the tastes of the public. Therefore, there are excellent application prospects of this design scheme.

## REFERENCES:

[I] Ping An Wang. Infonnation security knowledge and behavior:An adapted model of technology acceptance[J].Education Technology and Computer(I CETC),20 1 0(2): 364-367.

[2] Ravichandiran C, Yaithiyanathan Y. An Incisive SWOT Analysis of WiFi, Wireless Mesh,WiMAX and Mobile WiMAX Technology[J]. Education Technology and Computer,2009:239-243.

[3] Qi E H,Meylemans M,Hattig M.Augmenting wireless LAN technology for Wi-Fi PAN[J].Signals,Systems and Computers,2009:321-324.

[4] Jing Pan, Na Qi, Bingbing Xue, Qun Ding. "Design and hardware implementation of FPGA & chaotic encryption-based wireless transmission system". International Journal of Innovative Computing, Information and Control (IJICIC), pp692-695 2011.

[5] Xiao-Jun Tong,Ming-gen Cui,Wei Jiang.The Production Algorithm of Pseudo-Random Number Generator Based on Compound Non-Linear Chaos System[J]. Intelligent Information Hiding and Multimedia Signal Processing,2006:685-688.

[6] Qun Ding, Yong Zhu, Fangyi Zang, Xiyuan Peng, "Discrete Chaotic Circuit and The Property Analysis of Output Sequence", International Symposium on Communications and Infonnation Technologies (IEEE ISCIT Beijing ), 2005. 147.

[7] Dabal P,Pelka R.FPGA implementation of chaotic pseudo-random bit generators[J].Mixed Design of Integrated Circuits and Systems (MIXDES),2012:260-264.

[8] Qun Ding, Jing Pang, Jingqing Fang, Xiyuan Peng,. "Designing of Chaotic System Output Sequence Circuit Based on FPGA and its Possible Applications in Network encryption card". International Journal of Innovative Computing, Information and Control (IJICIC), Yol.3, No.2, pp449-456 2007.

[9] Zhan Lei,Zhao Jing.A hardware encryption and decryption system design[J].Computer Engineering and Technology(ICCET), 2012:75-77.

[10] Qun Ding, Jing Pan, Lu Wang, Guanrong Chen. "The Cipher Code Parameter Selection and Impact on Output Cycles", 2009 International Workshop Chaos-Fractals Theories and Applications(IWCFT A2009), ppI43-147 2009.

[11]Xiaoli Geng,Qun Ding. "Similar-short periodicity analysis and application in image compression encryption of digital chaos". 2012 Fifth International Workshop on Chaos-fractals Theories and Applications(IWCFTA2012), ppI68-171 2012.

[12] Yu Fei,Zhao Jie,Wu Yating.A dynamic password chip design based on Logistic chaotic algorithm[J]. Communication Software and Networks (ICCSN),2011 :255-259.

[13] DING Qun, PENG Xi-yuan, YANG Zi-heng, "The Cipher Chip of Combining Stream Based on the Neural Network Algorithm", Acta Electronica Sinica, Vo1.34, No.3, pp409-412 2006.