International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 11, November 2013)

Design and Implementation of FPGA Based Efficient Data Transmission Using Verilog

Girish Kumar B[1], Prabhu V[2], Siva Prasad T[3], Ruban Thomas[4]
[1]PG Scholar, [2,3,4]Assistant Professor, Vel Tech Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.

***Abstract* - This paper presents, FPGA based efficient & secure data transmission for widely spread communication systems & hand-held devices. Now a day's, secure transmission is necessary to protect data from attackers. Even though, many soft ware's are available to get the original data, but there is no preciseness because it is illegal & they don't know exact no.of rounds performed by master. Here in this paper, the author trying to innovating new methodology for data transmission from one to one. For this we are taking RC5 encryption algorithm which can have capable of N- bit (variable) data transmission with less no.of rounds. This paper presents RC5 encryption algorithm with FPGA (Spartan 3E) & Verilog Hardware Description Language. This security analysis process can be done through the RS232 cable by using hyper Terminal Software.**

***Keywords* – FPGA, Hand-Held Devices, HyperTerminal, RC5 algorithm, RS232, Security & Verilog.**

LITERATURE SURVEY

Up to now a very little research papers are published on network data security using FPGA. In those are illustrates how the security can be provides in network while transmission exists through the FPGA with Hardware Description Languages like VHDL and Verilog. But all are can be tried with only VHDL language for their work.

VHDL is flexible coding language but not for complex works. For example take an intelligent spacecraft designing using neural network in FPGA, here in this work need to design a spacecraft it is complex by using VHDL. This paper illustrates the how a complex works can be implemented using Verilog HDL.

An unlimited data transmission can be establishes with secure data communication. This paper introduces the how Hyper Terminal software is useful network creation.

I. INTRODUCTION

In cryptography, there are two different types of methods to provide the security to a data. They are 1.Symmetric & 2.Asymmetric. Symmetric means same key for sender as well as receiver. Generally, cryptography concepts having three important blocks, they are Encryption, Key generation & Decryption. Data transmission can be starts from sender who can only able to mix the original data with Key which is called as "Cipher Text".

Cipher Text Transmission process can be done through the network medium. Finally, cipher text can be received by receiver who knows the methodology done by the sender. Plain Text can be received without any attacks. Process can be shown in following figure 1.

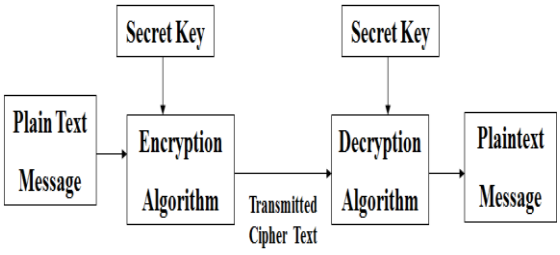

Figure 1: Block Diagram of Symmetric Encryption Process

Here in this process, the cryptoanalysist can provides a systematic procedure which is called as "Cryptography Algorithms".

There are so many no.of cryptography algorithms like DES, Simplified DES, Double DES, Triple DES, IDEA, RC5 and Blowfish. Except RC5 remaining all algorithms having some standards (that means restrictions). Suppose take DES and it's all following generations are used for limited data i.e., all list of parameters are restricted up to its standard. IDEA (International Data Encryption Algorithm) which is having 64-bit input plain text and cipher text as a output using 128-bit Key size. To overcome problems, this paper introducing RC5 encryption algorithm. This contains the Variable no.of data sizes for both plain and cipher texts using (0-2040) – bit key size.

This paper is organized as follows: Section II describes the Security of Hand Held Devices Security, Section III describes various modules of the system, Section IV describes the Proposing Encryption Algorithm, Section V discusses the results and power analysis, Conclusion and references are given in Section VI & VII respectively.

II. EXISTING SECURITY OF HAND - HELD DEVICES

Mainly now a day's every human beings are addicted with highly efficient hand-held devices like mobiles, tablets, Personal digit assistant and so on. Everyone can use their devices frequently.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 11, November 2013)

Even they can send messages from their devices to another friend's devices with trusted connection. In between the transmission & reception, lot of probability is there to attack the unknown persons (hacking). But presently every hand-held devices can provides only F-Secure that means which protects the files within the device only.

It can also know as anti- virus protection. No one can provide the data protection while the transmission. This paper describes detailed description of the data protection while it is in transmission. Mobile handheld devices containing confidential, personal, sensitive, and generally all information belonging to employ encryption or equally strong measures to protect the corporate data stored on the device, as stated incorporate encryption standards 0.The basic principles are shown below.

A. Security risks are on the rise because of mobile devices

71% say mobile devices have contributed to increased security incidents.

The Android mobile platform is considered to introduce the greatest security risks.

B. Employee behavior impacts security of mobile data

47% report customer data is stored on mobile devices.

Lack of employee awareness about security policies ranked as having the greatest impact on the security of mobile data.

72% say careless employees are a greater security threat than hackers

C. Extensive use of mobile devices on corporate networks

Participants were asked if mobile devices, such as smart phones or tablets, connected to their corporate networks.

The IT professionals who took the survey reported broad use of mobile devices within their organizations with 89% saying that they had mobile devices connecting to corporate networks.

Most participants, 65%, reported that their organizations had devices that were personally owned by employees in addition to company-owned mobile devices accessing corporate networks.

1. Limitations:

- Less data sizes
- More complex to provide security
- Security restricted to the within the mobile.
- More number of rounds required to provide the security.
- Execution time is high because it has more number of Keys.
- High Power Consumption.

III. Proposing Security System

In this paper, we are proposing new security system for Hand – Held devices which provides unlimited data transmission with efficient security. In this system, we are using RC5 Encryption algorithm which is suitable for unlimited data. This system contains three different modules which are listed as following.

- Key Generation
- Encryption
- Decryption

A. Key Generation:

RC5 encryption algorithm is having symmetric key at both ends that means same key is used in both sender & receiver which is shown in figure 1.The key expansion routine expands the user's secret key K to fill the expanded key array S_ so that S resembles an array of t = (2r+1) random binary words determined by K. The key expansion algorithm uses two "magic constants" and consists of three simple algorithmic parts.

Definition of the Magic Constants: The key expansion algorithm uses two word sized binary constants P_w and Q_w. They are defined for arbitrary was follows.

P_w = odd $((e-2)2^w)$ (1)

Q_w = odd $((\varphi-1)2^w)$ (2)

Where

e = 2.78281828159

(Base of natural logarithm)

φ = 1.61803398871

B. Encryption:

We assume that the input block is given in two w-bit registers A and B. We also assume that key-expansion has already been performed, so that the arrays (0, t-1) has been computed. Here is the encryption algorithm in following figure 2.

Here in this diagram illustrates the Fiestal structure which is basic principle of the symmetric data security process. Basic operation of RC5 encryption algorithm is shown in figure 3.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 11, November 2013)

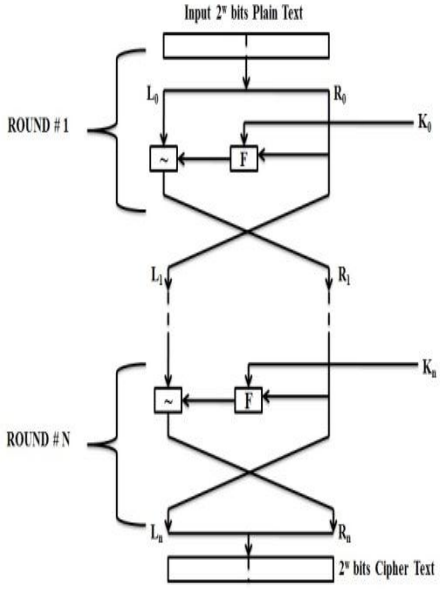

Figure 2: Encryption Process

Where

F --- Round Function
~ --- Substitution
K --- Key

Round Function:

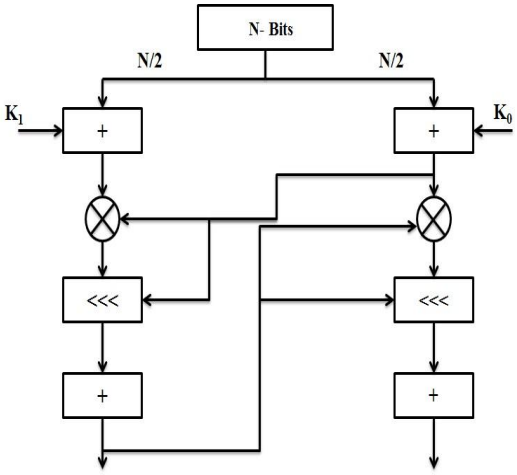

Figure 3: Round Operations

Where

+ --- Modulo Addition
X --- xor operation
<<< --- Left Cyclic Rotation

C. Decryption:

It is exactly reverse procedure of the encryption process. It is shown from the following structure.

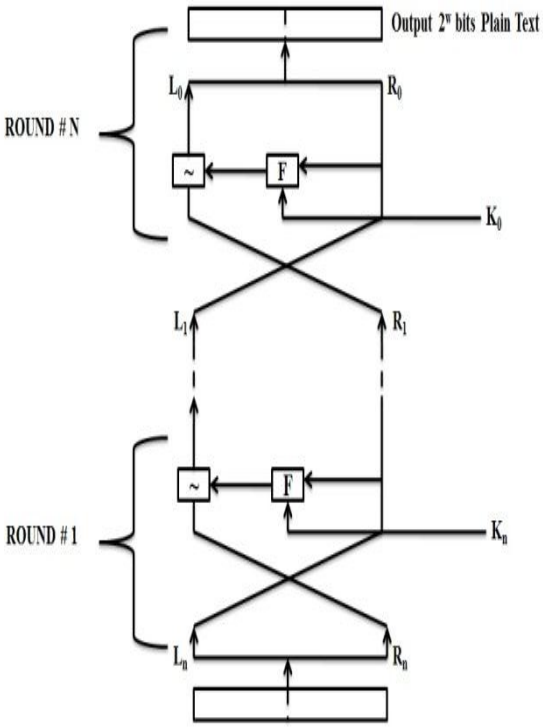

Figure 4: Decryption Process

Where

F --- Round Function
~ --- Substitution
K --- Key

IV. RESULTS

By using round functions especially xor modulo addition and left cyclic rotation takes less memory requirements when compare to other encryption algorithms. Xilinx synthesis tool measures configurable logic block. It does not require special UART because of all handheld devices already have it. This project was done using HyperTerminal software which is used as medium between the FPGA and VGA Display.

VI. IMPLEMENTATION

The paper is implements in hardware like FPGA (Spartan IIE) and with the help of Hyper Terminal communication module for security functions in industrial standards along with the Verilog Coding.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 11, November 2013)

A real time working model of a system based RC5 Encryption Algorithm were created as per design. After the design and selection of appropriate software components and hardware components were developed in order to interface the system with real-time environments.

Before going to implementation process, we are designing the entire System UML Model for the system which gives correctness of the particular system. Initially we are applying the raw data in form of bits to encryption block and then we are generating the various keys and they are applied to the every round of the process and then we are generating the cipher.

At the receiver end, we are going to applying the cipher as the input to the decryption block and finally retrieving the original data at the end. Key Generation is the main factor of the system; here it was generated in Xilinx Platform in the variable bits (0-2040 bits). The main function of the Key is to change the original data into confused manner no one can't understand the format which is known as the Cipher Text. At the receiver section they can decrypt the cipher with help of key only.

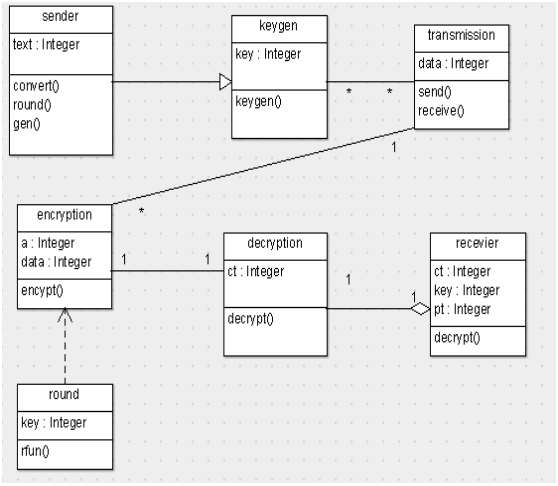

Figure 5: Class Diagram Representation

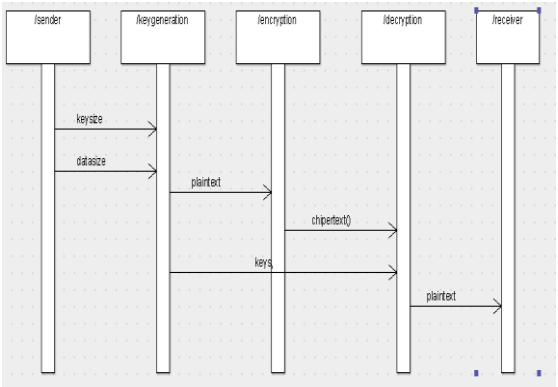

Figure 6: Sequence Diagram Representation

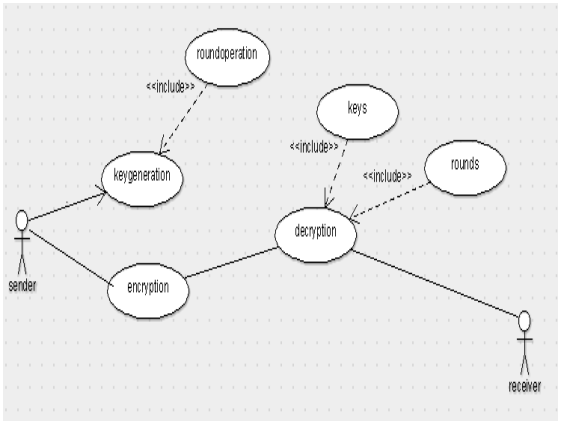

Figure 7: Use Case Diagram Representation

VII. Work Done And Discussion

This paper presents a high speed, low memory, low area and coast effective secure data transmission between two hand held devices .the number of clock cycle required to a single block has been reduced and amount of hardware resources has been optimized.

REFERENCES

[1] V Chaitanya Tummalapalli, MD. Khaja muinnuddin Chisti "Implementation of Low Power RC5 Algorithm in XILINX FPGA" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012, pp.924-928.

[2] R.L. Rivest, "The RC5 encryption algorithm," Proceedings of the 1994 Leuven Workshop on Fast Software Encryption, pp. 86-96, Springer-Verlag, 1995

[3] Olabisi, O. Elkeelany, "Integrated design of RC5 algorithm," InProceedings of The IEEE 39th Southeastern Symposium on System Theory, 2007.

[4] Hua Li, Jianzhou Li, Jing Yang, "An efficient and reconfigurable architecture for RC5", Canadian Conference on Electrical and Computer Engineering, 2005

[5] Schubert and W. Anheier, "Efficient VLSI implementation of modern symmetric block ciphers," proceedings of ICECS'03, pp. 757-760, Pafos, Cyprus, 2003.

[6] S. Nimmagadda, O. Elkeelany, "Performance evaluation of different hardware models of RC5 algorithm," In the Proceeding of The IEEE 39th Southeastern Symposium on System Theory, 2007

[7] N. Sklavos, C. Machas and O. Koufopavlou, "Area optimized architecture and VLSI implementation of RC5 encryption algorithm," Proceedings of 10th IEEE International Conference on Electronics, Circuits and Systems, pp. 172-175, United Arab Emirates, 2003.

[8] Behrouz A. Forouzan," Cryptography and Network Security" THM publications, 2009.

[9] Janick Bergeron," Writing testbenches: Functional verification of HDL models", Kluwer Academic, 2000.

[10] Figure 1-4 are manually drawn and taken from earlier cryptography concepts. Figure 5-6 are UML diagrams for proposing system using AgroUML Software.

AUTHORS

1. Girish Kumar B, PG Scholar in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.
2. Prabhu V, Asst. Prof in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.
3. Ruban Thomas, Asst. Prof in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.
4. Siva Prasad T, Asst. Prof in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.