Text Encryption Technique using low power ZigBee device

Chinmay V. Deshpande, and Prof. Chankya K. Jha.

Abstract: In this paper, an encryption technique is used to convert plaintext into cipher-text. By means of various algorithms such as SFEA, PES-counter, Simplified PES the plaintext is converted into cipher which is a binary code. For conversion of plain text into cipher text different rounds (n = 10, 12, 14 as per key length) are used. This technique is very useful for data protection. Keys are used to protect data.

Keywords – Encryption, SFEA, ES-counter, Simplified ES, ZigBee.

I. INTRODUCTION

ZigBee is a new emerging technology which provides high level communication protocol that forms personal area networks (PANs). ZigBee is recognized as IEEE 802.15.4 standard.

ZigBee device passes data over longer distance through multi-hop routing with the help of intermediate devices forming three topologies star, tree and mesh topology.

Manuscript received July, 2015.

C. V. Deshpande is with Department of Electronics and Tele-communication Engineering, Pune University, Sahyadri Valley College of Engineering & Technology , Rajuri. Maharia Charitable Trust, Rajuri, District: Pune, India.

Prof. Chankya K. Jha, is Vice-Principal and IEEE member with Department of Electronics and Tele-communication Engineering, Pune University, Sahyadri Valley College of Engineering & Technology, Rajuri. Maharia Charitable Trust, Rajuri, District: Pune, India.

In star topology, coordinator must be central node. Both tree and mesh topologies provides communication at the network layer.

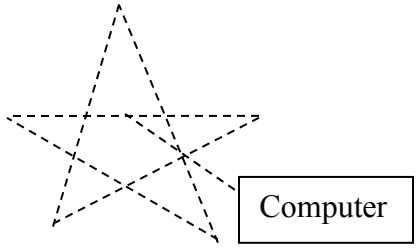

Figure 1: Star Topology.

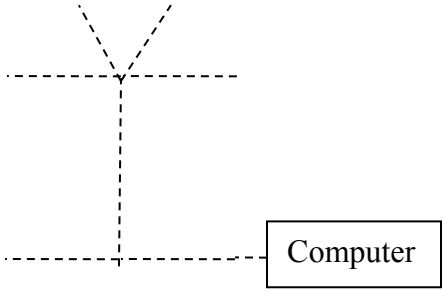

Figure 2: Tree topology.

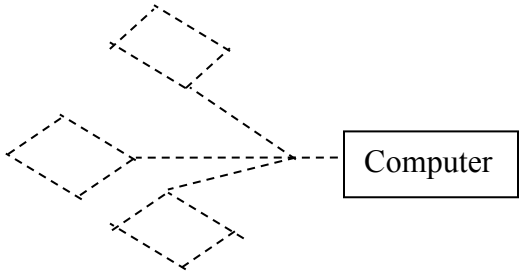

Figure 3: Mesh Topology.

II. LITERATURE SURVEY

In this paper mainly three algorithms are described that are as follows:

- Simplified PES algorithm.
- PES counter mode.
- Sturdy and Fast Encryption Algorithm Scheme (SFEA).

1) Simplified Progress Encryption Standard (PES) algorithm.

In simplified PES algorithm ten rounds are used which contains four transformations: SubByte, Shift rows, Mix column and Key substitution. Using these four transformations plaintext given as an input is converted into binary bits stream. Binary number system can be understood by

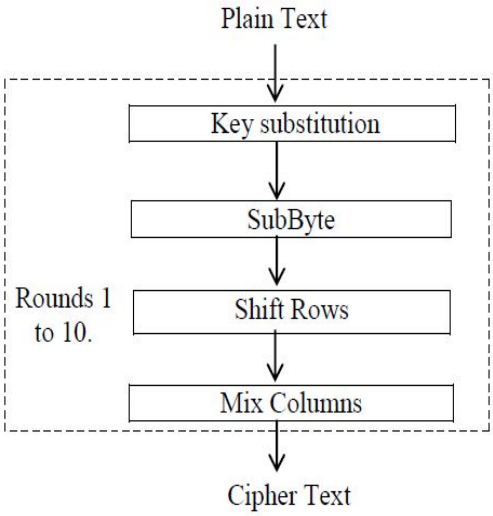

Figure 4: Simplified PES algorithm.

computer as low level language. But it becomes difficult for users to understand meaning of binary bits stream. For total encryption minimum 10 rounds are required. In this project 10 rounds are used to encrypt data given as hexadecimal input.

2) Progress Encryption Standard (PES) counter mode.

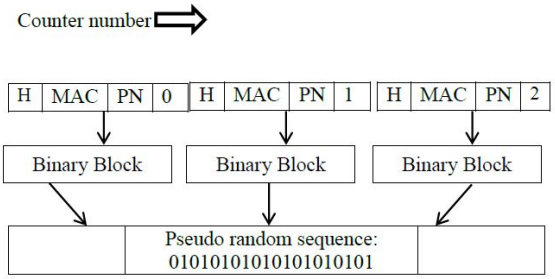

Figure 5: PES counter mode.

The PES counter converts plain text given as hexadecimal input into binary bits of output. For conversion of plaintext into binary bits = XOR operation is used.

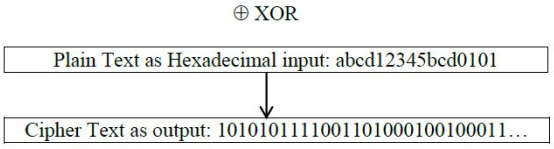

Figure 6: Conversion of plain text into cipher text.

The intermediate variable bits generated during conversion of plaintext into cipher are stored into wire. These variables are having 128 bits of length. The variables in 'wire' are denoted by capital letters A, B and so on.

3) Sturdy and Fast Encryption Algorithm.

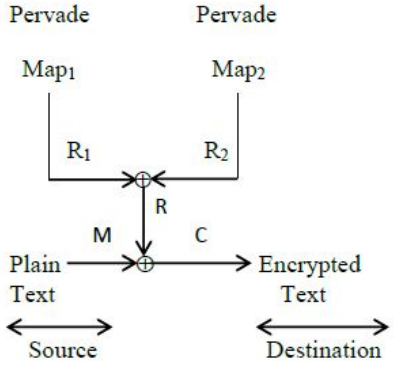

Figure 7: Sturdy Fast Encryption Algorithm.

In Sturdy Fast Encryption Algorithm two pervade maps are utilized. Using XOR gate plain text given as an input is converted into encrypted text. The truth table of XOR operation is shown in Table 1.

Table 1

XOR gate output.

Inputs to XOR		Output of XOR
M	R	C
0	0	0
0	1	1
1	0	1
1	1	0

The equation for output of XOR gate is:

C = M R = .

II. VERILOG

Verilog and Verilog Hardware Description Language (VHDL) are two languages used by hardware designer in an industry. VHDL was made IEEE standard in 1987 and Verilog in 1995. Verilog is alike but not identical to C language. Instructions written in Verilog language are defined in 'module' as an entity. Input variables are defined by keyword 'input' and output variables are defined inside keyword 'output', intermediate outputs are stored in 'wire' also known as intermediate bits.

Verilog HDL was a property of Cadence. Cadence made this language as proprietary and has given this language to public domain.

Verilog-XL gained a strong foothold among the high-end designers for the following reasons:

- Behavioral constructs of Verilog could describe both hardware and test stimulus.
- Verilog-XL simulator was fast, especially at the gate level and could handle designs in excess of 100,000 gates.

III. HARDWARE REQUIREMENT.

INTEGRATED CIRCUITS:

Integrated circuits are fabricated using CMOS technology. Basically, CMOS consists of three types of terminals known as source, gate and drain. Source is doped with n+ or p+ impurity with substrate as base material made up of Si.

The integrated circuits are classified according to the number of transistor present on an IC. Following are types of ICs:

1) Microprocessors.
2) Microcontrollers.
3) ASICs.

V. SOFTWARE REQUIREMENT.

- Verification Tool
  - Modelsim 6.4c
- Synthesis Tool
  - Xilinx ISE 9.1

MODELSIM 6.4 c.

ModelSim SE – High Performance Simulation and Debug.

ModelSim 6.4c SE is UNIX, Linux and Windows-based implementation, simulation and debug environment, combining high performance with the most powerful and intuitive GUI in the industry.

Xilinx ISE 9.1

To construct Xilinx Static Random Access Memory (SRAM) cell two cross-coupled inverters are required. Inverters are fabricated using CMOS technology. An example of Static RAM (SRAM) is shown in figure 8. This cell drives the gate terminal of another transistor on chip to make a connection by turning on or to break a connection by turning off.

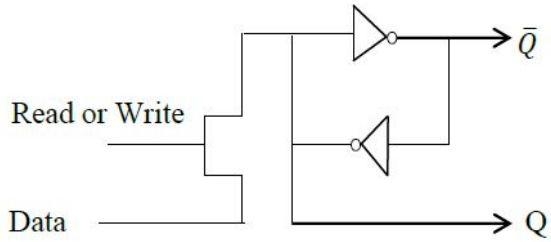

Figure 8: Static RAM cell.

Here output Q makes connection with another CMOS and breaks the connection by turning off the gate terminal of other CMOS.

Xilinx ISE Tools:
Xilinx provides various design tools these are: Constraints editor, core generator, schematic viewer, timing analyzer FPGA editor, FPGA editor, XPower Analyser, iMPACT, SmartXplorer and so on.
Schematic viewer provides RTL schematic and technology schematic of Verilog program.

VI. RESULTS OF EXPERIMENT.

Implementation: For getting result of program implementation process is required first before starting simulation. In implementation process synthesize XST is given by right clicking on synthesize XST and Run, ReRun or Rerun All, the implementation process starts to run.

Simulation: In right hand side to implementation process, simulation process is present above the source window. Using simulation process Behavioral Model can be simulated.

Two types of simulators are used for FPGA design. First is 'logic simulator' for functional, behavioral and timing simulation. Second type of simulator most often used in Field Programmable Gate Array (FPGA) is timing analysis tool.

Encrypted output:

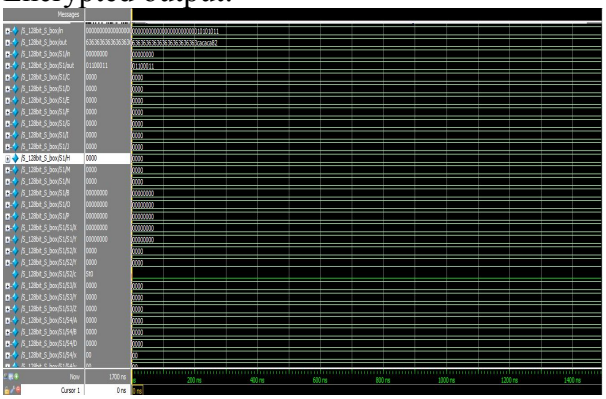

Figure 8: Encrypted output.

Register Transfer Level (RTL) schematic:

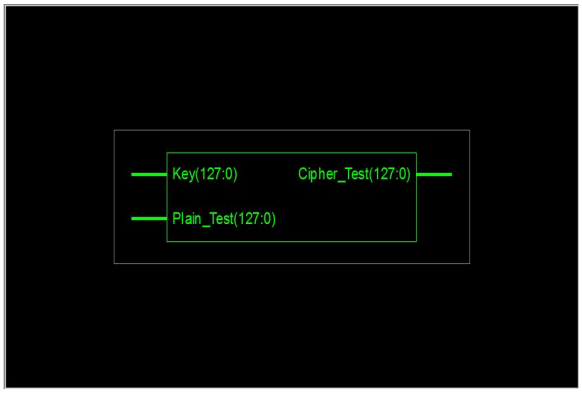

Figure 9: RTL Schematic.

VII. CONCLUSION.

In this paper, text encryption technique is proposed. Text is given as hexadecimal input can be encrypted using different algorithms; programming is done in Verilog language using Xilinx ISE 9.1 software. Keys are used to protect data in documents. This technique is used to prevent recipients from reading or using precious data.

REFERENCES

1] Z. Q. Zhang, X. L. Yang, and Y. M. Zhou, "A wireless solution for greenhouse monitoring and control system based on ZigBee technology," J. Zhejiang Univ. Sci. A, vol. 8, no. 10, pp. 1584-1587, Oct. 2007.

2] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in Proc. ACM Workshop Wireless Security WiSe, 2004, pp. 32-42.

3] Q. He, Q. Qi, Y. Zhao, W. Huang, and Q. Huang, " The application of chaotic encryption in industrial control based on zigBee wireless network," in Proc. 2nd Int. Conf. Symp. Syst. Control Aerospace Astronautics, pp. 1-5, Dec. 2008.

4] W. Puech, J. M. Rodrigues, and J. E. Develay-Morice, "Safe transfer of medical images by conjoined coding: Selective encryption by AES using the stream cipher mode OFB and JPEG compression," Ph.D. dissertation, Centre Hospitalier Univ. Montpellier, Univ. Montpellier II, Nimes, France, 2006.

5] J. Buchmann, Introduction to Cryptography. Berlin, Germany: Springer, 2004.

6] M. Musa, E. Schaefer, and S. Wedig, "A simplified AES algorithm and its linear and differential cryptanalyses," Cryptologia, vol. 27, pp. 148-177, Apr. 2003.

7] S. Babbage, C. De Canniere, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw, "The eStream portfolio," in Proc. ECRYPT pp. 1-10, 2008, IST-2002-507932.

8] H. Wu, "Stream cipher HC-128," in New Stream Cipher Designs. Berlin/Heidelberg: Springer-Verlag, 2008, pp. 39-47.

Chinmay V. Deshpande is pursuing his M. E. in Electronics and Tele-communication Department (VLSI and Embedded Systems) from S. P. Pune University. He graduated in Electronics and Tele-communication Engineering from Sant Gadge Baba Amravati University. His areas of interest are wireless sensor networks, micro-processor and micro-controller and VLSI technology.

