Chip Implementation of Text Encryption and Decryption Algorithms

Vishwa Deepak Badoni ,Mr. Arpit jain
M.Tech (CSE), Teerthanker Mahaveer University, Moradabad(UP) ,India
Department of CSE, Teerthanker Mahaveer University,Moradabad(UP),India

Abstract: *Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. A common goal of cryptographic research is to design protocols that provide a confidential and authenticated transmission channel for messages over an insecure network. A cryptographic algorithm is considered to be computationally secured if it cannot be broken with standard resources, either current or future and apart from the algorithm distribution of keys also more important is to make an efficient cryptosystem. TACIT Encryption Algorithm can produce best possible results if key size is the size of the packet expected to pass through the network is small. This paper gives the comparison of the various algorithms with TACIT Encryption Algorithm on the basis of parameters like key length, block size, type and features. The paper is based on the chip designing of the algorithm using VHDL programming language.*

Keywords: *Encryption and Decryption, SoPC (System on Programmable chip),Very High Speed integrated Circuit Hardware Description language (VHDL).*

I. Introduction

In cryptography, encryption [1] is the process of transforming information (referred to as plain text) using an algorithm, called a cipher to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key [1, 2]. The result of the process is encrypted information, in cryptography, referred to as cipher text. The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption. Encryption is also used to protect data in transit, for example data being transferred via networks. The examples of such networks are internet, mobile, wireless microphones, wireless intercom, Bluetooth devices, E- Commerce and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. With the wireless communications coming to homes and offices, the need to have secure data transmission is of utmost importance. Today, it is important that information is sent confidentially over the network without fear of hackers or unauthorized access to it. This makes security implementation in networks a crucial demand. Symmetric Encryption Cores provide data protection via the use of secret key only known to the encryption and decryption ends of the communication path. A hardware system design is proposed to improve its performance. The proposed architecture achieved with three stage pipeline technique an increased encryption throughput as compared to related work. By exploiting modern features in Field Programmable Gate Arrays (FPGA), which allow the modeling of a System-on-Programmable-Chip (SoPC).

II. Mode Of Operation

There are many variance of cipher, where different techniques are used to strengthen the security of the system. The most common methods are ECB (Electronic Code Book), CBC (Chain Block Chaining Mode) and OFB (Output Feedback Mode). There are many other modes like CTR (Counter Mode), CFB (Cipher Feedback Mode). The key size is a very important aspect to secure the data, long key size means the data is more secured. Encryption algorithms are very important for cryptography with an approach of key management because there are different algorithms that offer different degree of security based on key size. There are couples of encryption and decryption algorithms which are already proposed. A comparison of these techniques shows the various cryptographic techniques and their features on the basis of type, key size, and block size. It can be seen that from this comparison table that TACIT encryption technique has a unique independent approach by having a new key distribution system along with mathematical foundation [8]. The main advantage of TACIT logic is that, it can processes 'N' bits blocks and 'N' bits key size. This approach may be good if the block size is less than the key size. The algorithm may be implemented in any languages, which support Unicode system facility like VHDL, Verilog HDL, Java, C#, System C, .Net, etc. One of the main categorization methods for encryption technique commonly used is based on the form of input data they operate on. The two types are Stream and Block Cipher.

• **Block Cipher:** In this method, data is encrypted and decrypted if data is in forms of blocks. In its simplest mode, the plain text is divided into blocks which are then fed to cipher system to produce blocks of cipher text.

• **Stream Cipher:** Stream Cipher functions on a stream of data by operating on it by bits. It consists of two major components: a key stream generator and mixing function. Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique.

III. TACIT Encryption Algorithm

The Encryption [44] of the data at transmitting end includes the following steps. The TACIT encryption logic [21] for data communication between two nodes of NoC is presented with the help of following algorithm. The flow chart of the algorithm is shown in figure 1.

Step 1: Text file content is read and position of the character is shuffled by using initial permutation approach using key value.
Step 2: Read the character from the text file corresponding to the text and get the ASCII value of that character.
Step 3: Perform XOR operation with the specific n-bit key value.
Step 4: A secure tacit logic has been introduced (i.e. n^k xor k^k along with some specific operations; where n is the value computed from step 3).
Step 5: Convert the value into binary one.
Step 6: Perform reverse operation on the binary string.

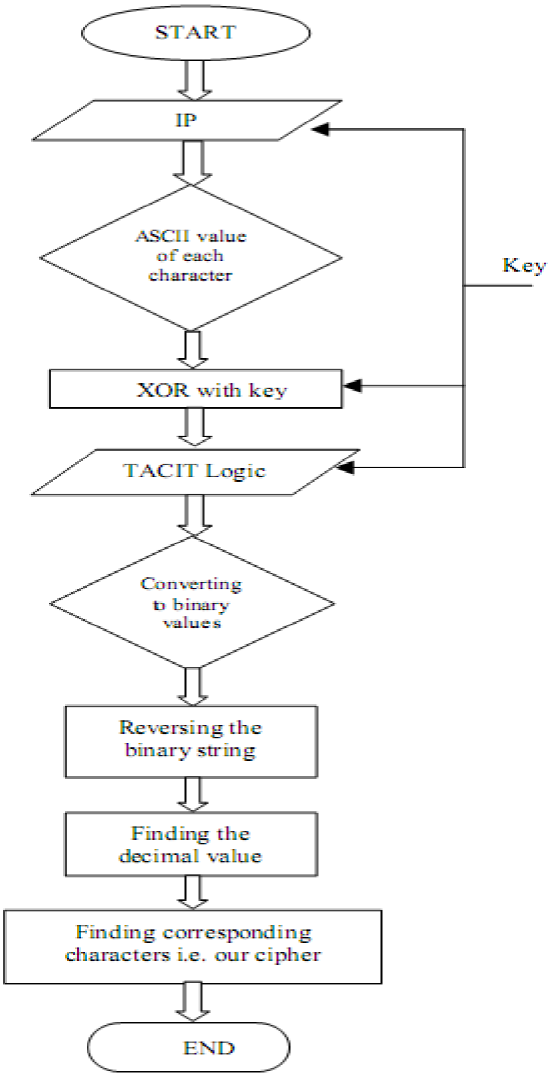

START
IP
ASCII value of each character
Key
XOR with key
TACIT Logic
Converting to binary values
Reversing the binary string
Finding the decimal value
Finding corresponding characters i.e. our cipher
END

Fig.1 Encryption logic

IV. Tacit Decryption Algorithm*:*

The Decryption [44] of the data at receiving end includes the following steps. The TACIT Decryption logic for data communication between two nodes of NoC is presented with the help of following algorithm. The flow chart of the algorithm is shown in figure 2.

Step 1: Read the first character from the cipher text and get the corresponding decimal value of it.
Step 2: The corresponding binary value is evaluated and make the reverse of it.
Step 3: Inverse of the tacit logic is applied.
Step 4: Perform XOR with n-bit key value.
Step 5: The character corresponds to it is determined.
Step 6: Now reshuffling is done using key value.
Step 7: Repeat the steps (1 to 6) till the end.

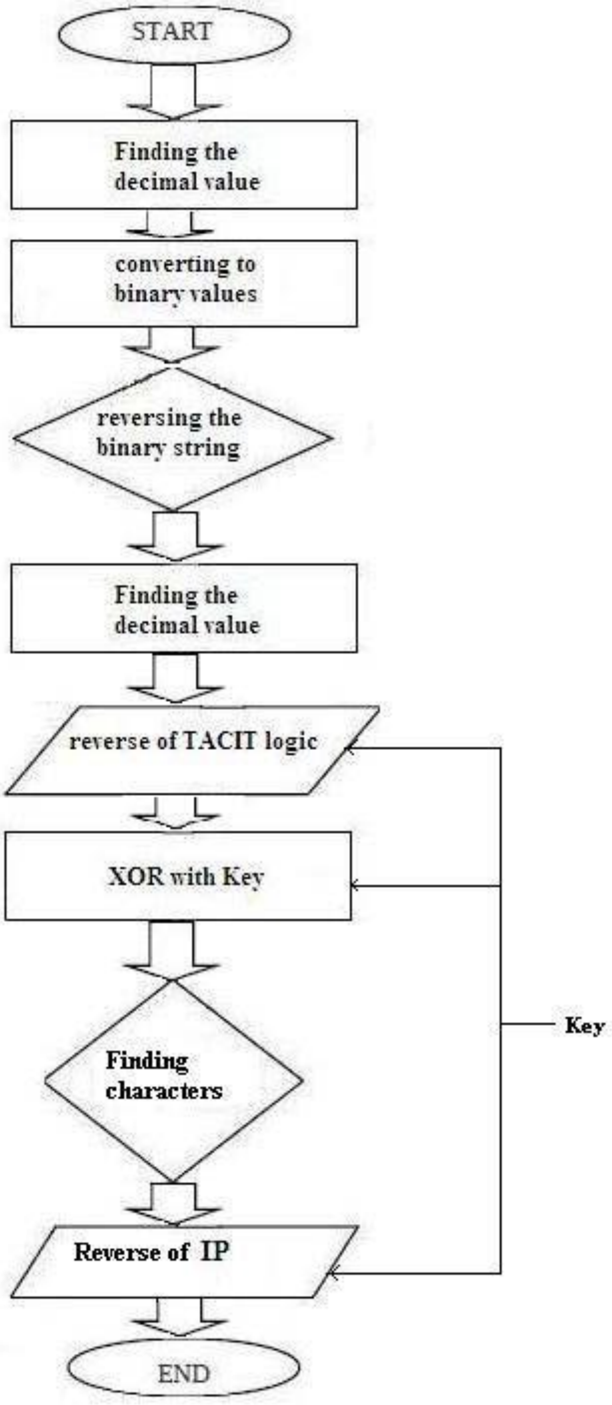

START
Finding the decimal value
converting to binary values
reversing the binary string
Finding the decimal value
reverse of TACIT logic
XOR with Key
Finding characters
Reverse of IP
END
Key

Fig.2 Encryption logic

Xilinx [7] [8] has been a semiconductor industry leader at the forefront of technology, market and business achievement. It is a tool to design the IC and to view their RTL (Register Transfer Logic) schematic .It is a tool to test the code on FPGA environment and we can get the all parameters details required to implement the Chip.

V. Tools Used

The details of the tools are given below.

- **Model SimEE 10.1 b student edition of Mentor Graphics Company**

Mentor Graphics [9] was the first to combine single kernel simulator (SKS) technology with a unified debug environment for Verilog HDL, VHDL, and System C. The simulation and synthesis combination of industry-leading and native SKS performance with the best integrated debug and analysis environment make Modelsim the simulator of choice for both ASIC and FPGA design. The design platform and standards support in the industry make it easy to adopt in the majority of process and tool flows.

VI. Simulation Results

RTL view of the chip is a top view representation depicting its pins details and input/ output logic. The possible inputs and outputs used in the development of the chip are represented with their RTL view. The functional simulation depends on the test inputs in design. c*lk* and *reset* are used for the synchronization. Figure 3 shows the RTL view, internal schematics and model simulation for the encryption logic. In the simulation reset = ‘1’, clk is used for synchronization and then run. The rising edge of clock pulse is applied to check the results on the rising edge of applied clock pulse with 50% duty cycle. Again reset = ‘0’, same clk is used for synchronization. Select the text value and then force.

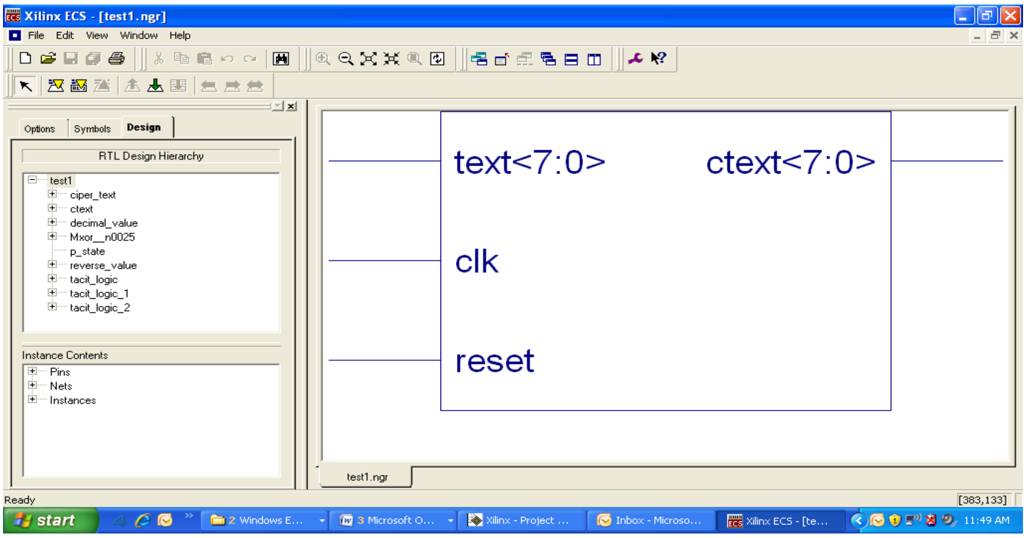
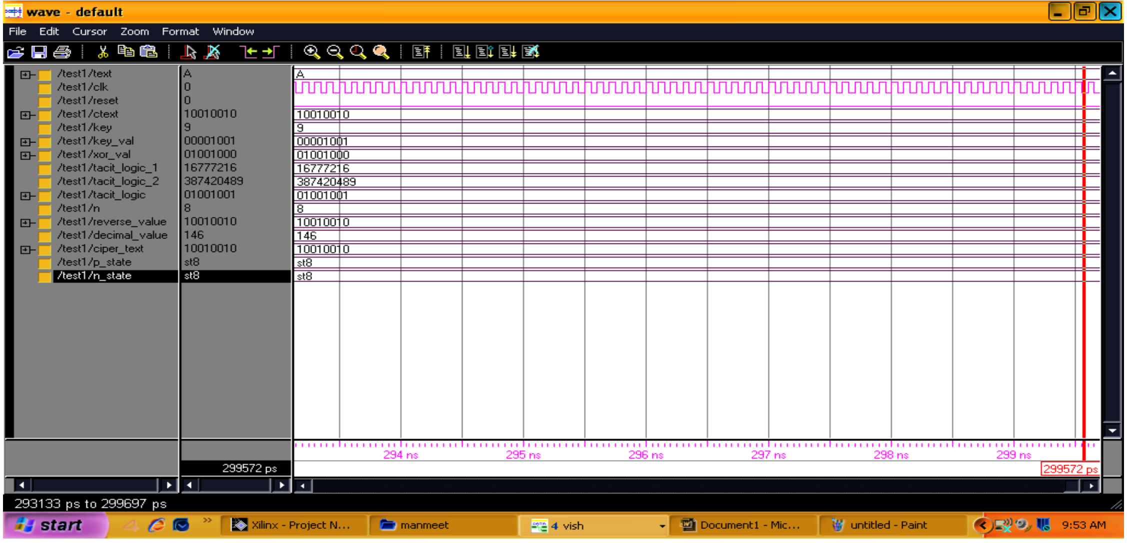


Fig. 3 RTL view of encryption (8 bits data)



```
/test1/text              A
/test1/clk               0
/test1/reset             0
/test1/ctext             10010010
/test1/key               9
/test1/key_val           00001001
/test1/xor_val           01001000
/test1/tacit_logic_1     16777216
/test1/tacit_logic_2     387420489
/test1/tacit_logic       01001001
/test1/n                 8
/test1/reverse_value     10010010
/test1/decimal_value     146
/test1/ciper_text        10010010
/test1/p_state           st8
/test1/n_state           st8
                         299572 ps
293133 ps to 299697 ps
```

Fig. 4 Modelsim output waveform of encryption (8 bits)

Figure 5 to 6 shows the RTL view and model simulation for the Decryption logic. In the simulation reset = ‘1’, clk is used for synchronization and then run. The rising edge of clock pulse is applied to check the results on the rising edge of applied clock pulse with 50% duty cycle. Again reset = ‘0’, same clk is used for synchronization. Select the text value and then key value which may be any random number then force.

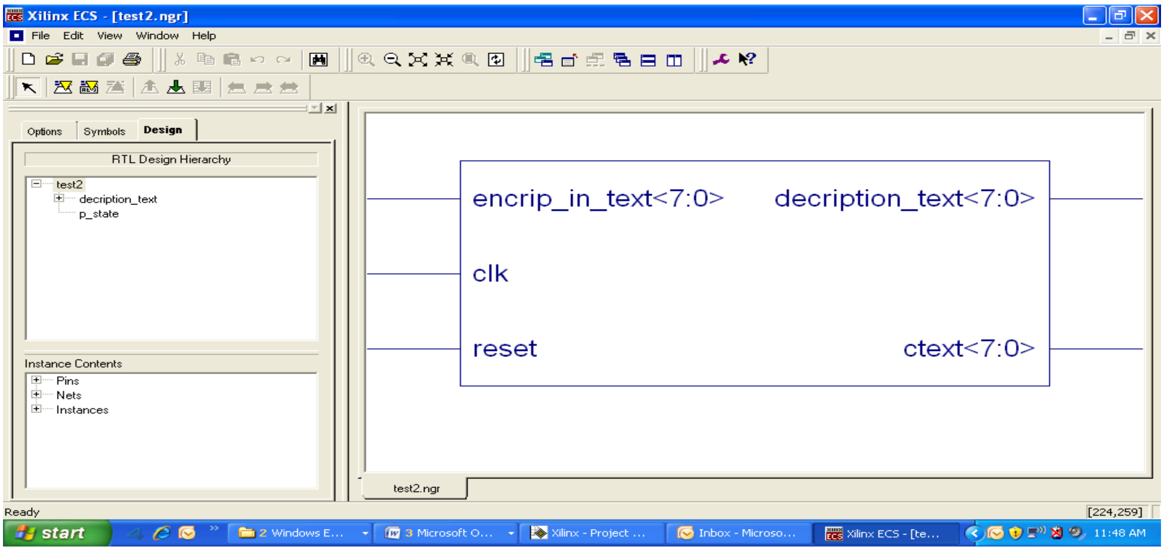
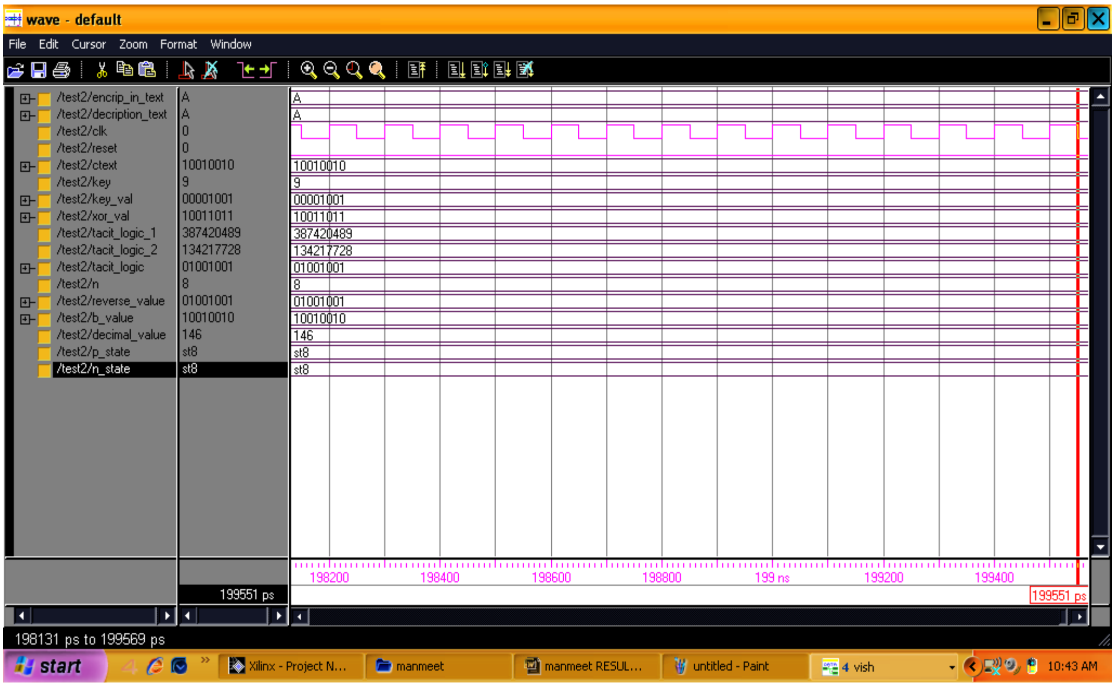


Fig. 5 RTL view of encryption (8 bits data)



```
/test2/encrip_in_text    A
/test2/decription_text   A
/test2/clk               0
/test2/reset             0
/test2/ctext             10010010
/test2/key               9
/test2/key_val           00001001
/test2/xor_val           10011011
/test2/tacit_logic_1     387420489
/test2/tacit_logic_2     134217728
/test2/tacit_logic       01001001
/test2/n                 8
/test2/reverse_value     01001001
/test2/b_value           10010010
/test2/decimal_value     146
/test2/p_state           st8
/test2/n_state           st8
                         199551 ps
198131 ps to 199569 ps
```

Fig. 6 Modelsim output waveform of decryption (8 bits)

VII. Conclusion

The hardware chip implementation of TACIT logic for encryption and decryption is done in Xilinx 14.1 and functional simulated in Modelsim 10.1 b. The TACIT logic has proven best result in comparison to the other techniques available for encryption and decryption. The design is developed for the ‘N’ bits key value and ‘N’ bits block size. The functional simulation is done for the different text size and key values. The code is synthesized for ‘N’ bits data size on Sparten-3E FPGA.

Rferences

[1]. Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, “Implementation of AES Encryption and Decryption” International Conference on “Control, Automation, Communication and Energy Conservation -2009, (page 1-5)

[2]. Beerel P, Roncken “Low power and energy efficient asynchronous design”. Journal of Low Power Electron Vol.3, No. 3, pp (234–253), Dec. 2007.

[3]. C. J. Glass and L. M. Ni, “The turn model for adaptive routing,” Journal of the ACM, vol. 41, no. 5, pp. 874–902, 1994.

[4]. D. Park, C. Nicopoulos, J. Kim, N. Vijaykrishnan, and C. R. Das, “Exploring fault-tolerant network-on-chip architectures,” in Proceedings of the 2006 International Conference on Dependable Systems and Networks, (DSN ’06), pp. 93–104, Philadelphia, Pa, USA, June 2006.

[5]. Hiroaki Morino Thai Thach Bao Nguyen Hoaison Hitoshi Aida Tadao Saito “A Scalable Multistage Packet Switch for Terabit IP Router Based on Deflection Routing and Shortest Path Routing” © 2002 IEEE, pp (2179-2185)

[6]. M. Daneshtalab, A. A. Kusha, A. Sobhani, Z. Navabi, M. D. Mottaghi, and O. Fatemi, “Ant colony based routing architecture for minimizing hot spots in NOCs,” in Proceedings of the Annual Symposium on Integrated Circuits and System Design, pp. 56–61, September 2006.

[7]. Prosanta Gope, Ashwani Sharma Ajit Singh Nikhil Pahwa “An Efficient Cryptographic Approach for Secure Policy Based Routing (TACIT Encryption Technique)”, Conference Proceedings, IEEE Xplorer, (2011), pp (359-363)

[8]. R. Venkateswaran Dr. V. Sundaram “Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography,” International Journal of Computer Applications (0975 – 8887) Volume 3 – No.7, June 2010, (page 1 and 7)