Indian Journal of Science and Technology Vol.2 No. 10 (Oct 2009) ISSN: 0974- 6846

VHDL modeling and simulation of data scrambler and descrambler for secure data communication

G.M. Bhat*, M. Mustafa**, Shabir Ahmad** and Javaid Ahmad**
*University Science Instrumentation Center, University of Kashmir, Srinagar, India
**Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India
shabireltr@gmail.com

Abstract VHDL modeling and simulation of a typical data scrambler and descrambler for secure data communication has been presented. The encoder and decoder has been implemented using VHDL approach which allows the reconfigurablity of the proposed system such that the key can be changed as per the security requirements. The power consumption and space requirement is very less compared to conventional discrete I.C. design which is pre-requisite for any system designer. The design has been synthesized on EP1S0F484C5 of Straitx FPGA family. The results of the simulation have been found to be satisfactory and are in conformity with theoretical observations.

Keywords: Scrambler, Descrambler, VHDL, and FPGA.

Introduction

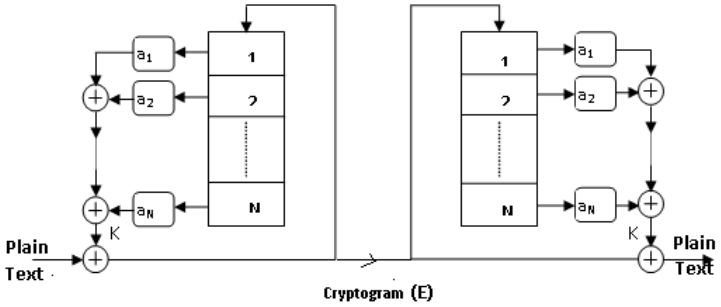
The changing social needs and the development of new technologies bring the evolution of new and sensitive communication capabilities in the form of Internet, electronic banking, electronic mail, pay channel television, cable television, mobile telephone, satellite phone, broad band services, e-journals, tele-medicine and above all several forms of electronic communications employed in defense. However, all forms of unprotected electronic communications are vulnerable to eavesdropping and interference.

A simple method for ensuring security is to encrypt the data. The pseudo-noise (PN) key generation is of paramount importance for any secure communication system. PN sequences based on Linear Feedback Shift Registers (LFSR) and non linear combination based implementations are simplest to give moderate level of security. Chaos based encryption techniques have proved fruitful, but complexity of such systems is high.

Many circuits using LFSR for generation of complex codes have been reported in literature (Schneier, 1996). Feedback with Carry Shift Registers (FCSRs) and schemes using various combinations of LFSRs have been proposed for complex key generation, but seem to be expensive for commercial applications (Waseem, 2001-2002).

An attractive solution for encrypting data with adequate message security at low cost is the use of Scrambler/ Descrambler. In a conventional scrambler the encrypted data is used for generation of key as shown in Fig 1. To enhance the degree of data security in a conventional Scrambler the number of stages of the shift register needs to be increased. This, however, increases error propagation. In the modified scrambler reported in the literature with the modified logic for Pseudo random key generation, selection of the outputs of the shift register for the key generation is controlled by means of a pseudo random sequence generator (Bhat *et al.,* 1996). The same logic has been implemented for key generation in this paper. In this case, an increase in the number of stages of the PN sequence generator results into a significant increase in message security. However, an increase in hardware is necessary for enhancing the security level of a scrambler using conventional integrated circuit implementation. This method of end-user implementation of the Scrambler has several limitations as it leads to increase in space and size of the hardware, more power consumption, power loss at various circuit interconnects, stray capacitance etc.

Fig. 1. Conventional data scrambler/ de-scrambler



The proposed VHDL based implementation of the scheme mitigates most of the limitations cited above. The proposed scheme implements the scrambler and descrambler using Hardware Description Language (VHDL) approach which allows the reconfigurablity (Standaert *et al.,* 2005) of the proposed system such that key can be changed as per the security requirements. An important advantage offered by VHDL implementation is that there is perfect synchronization between transmitter and receiver because VHDL design cares itself for various parameters like, setting time, hold time and propagation delays of various gates that play an important role for synchronization of a trans-receiver.

Description of data scrambler/ descrambler

Scramblers are a class of substitution ciphers and have been found to be suitable for various security requirements such as those used by cable and satellite TV operators and mobile phone service providers. A Scrambler is a coding operation which basically randomizes the data streams. In addition to its use as a stream cipher, a scrambler is commonly used to avoid long strings of 0's and 1's which are responsible for DC wander and synchronization problems in communication circuits. Scramblers are very popular for their use to encrypt video and audio signals for broadcasting and many other applications. The low cost and complexity, high speed of operation and easy to use are the main features of scramblers.

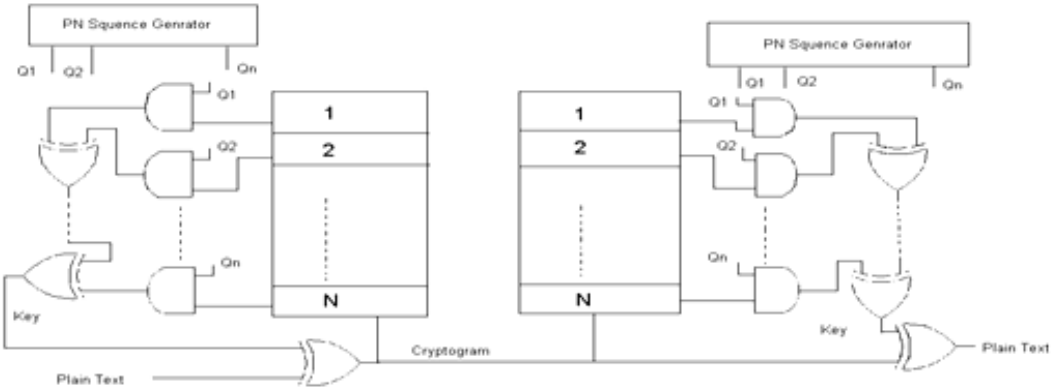
Fig.1 outlines encryption/decryption using conventional scrambling/descrambling technique. The input to the scrambler is the plain text or clear text 'C' whereas the encrypted text called as Cryptogram, is denoted by E. As is clear from the Fig. 1, data is encrypted using a key K, generated as a function of last N

Indian Journal of Science and Technology Vol.2 No. 10 (Oct 2009) ISSN: 0974- 6846

transmitted bits E, which are available through an n-bit Serial-in-Parallel-out (SIPO) shift register. A Boolean function 'f' with N-inputs computes K. The same function 'f' is used at the descrambler to compute the key K. It can be seen from the figure that the key K, generated for decryption at the receiver, is the same as that generated for encryption. It is evident that whereas modulo-2 addition of the key-bits K to the message bits C produces the encrypted text E at the scrambler output. The modulo-2 addition of the same key bits to the corresponding encrypted text bits E reproduces the original clear text message C at the output of the Descrambler.

The mathematical model for implementation of data

Fig. 2. Modified data scrambler/de-scrambler



Scrambler and Descrambler uses a shifting mechanism to introduce the delay in the data so as to obtain the required Cryptogram E. Here E can be represented mathematically as:

$$E = C + (a_1 D^1 E + a_2 D^2 E + a_3 D^3 E + \ldots\ldots + a_N D^N E) \quad \ldots(1.1)$$

Where a_i represents the i[th] tap gain and D represents the delay operator (i.e. $D^N E$ is the sequence E delayed by N units). The symbol '+' in the above equations represents modulo-2 addition. Eqn. 1.1 can be written as:

$$E = C + (a_1 D^1 + a_2 D^2 + a_3 D^3 + \ldots\ldots + a_N D^N) E \quad \ldots(1.2)$$

$$E = C + fE \quad \ldots(1.3)$$

With, $f = a_1 D^1 + a_2 D^2 + a_3 D^3 + \ldots\ldots + a_N D^N$ ...(1.4)

Hence $E = C + K$ ...(1.5)

Where the key $K = fE$

The tap gain values in Eqn. (1.4) can be 0 or 1. Any tap-gains a_i =1 means connection is taken form the i[th] shift register stage, and a_i = 0 means no connection is taken from that stage. Thus the function f depends upon the tap-gain values and the number of shift register stages N. The parameter f, whose complexity increases with an increase in N, hides the information signal C from an unauthorized receiver. The sequence of a's should also be known for proper decryption.

To design a matched Descrambler for decrypting E, we start with the received sequence E (which is available at the receiver) given by Eqn. (1.2) as

$$E = C + (a_1 D^1 + a_2 D^2 + a_3 D^3 + \ldots\ldots + a_N D^N) E$$

Adding $(a_1 D^1 + a_2 D^2 + a_3 D^3 + \ldots\ldots + a_N D^N) E$ to both sides of the above equation we get,

$$E + (a_1 D^1 + a_2 D^2 + a_3 D^3 + \ldots\ldots + a_N D^N) E = C \quad \ldots(1.6)$$

The above result is obtained by the fact that the modulo-2 sum of any sequence with itself gives a sequence of all 0's. Eqn. (1.6) can further be written as:

$$C = E(1 + f) \quad \ldots(1.7)$$

With, $f = a_1 D^1 + a_2 D^2 + a_3 D^3 + \ldots\ldots + a_N D^N$

It follows from Eqn. (1.3) and (1.7) that so long as f is same for the Scrambler and Descrambler, the message can be encrypted and decrypted faithfully by the system. To make the decryption difficult for an unauthorized receiver, the value of N should be large, which however increases bit error propagation resulting into n errors at the output, for a single erroneous bit.

Description of proposed reconfigurable scrambler/ descrambler using VHDL

The proposed technique for secure message communication uses Hardware Description Language (VHDL) and exploits the reconfigurablity feature of description languages to enhance the system security, optimize the power consumption and speed of operation. The spreading sequences as used in modified Scrambler /Descrambler obtained using VHDL approach have been fed to different AND gates to generate the tap gains. These tap gains are given to logic function generator (as shown in Fig.2) which manipulates the data and produces the complex key. The key is modulo-2-added with plain text which results into a Cryptogram. The Cryptogram is applied to the shifting logic so as to increase complexity of the key and hence security of data. At the receiving end same key has been generated and used for the successful decryption of

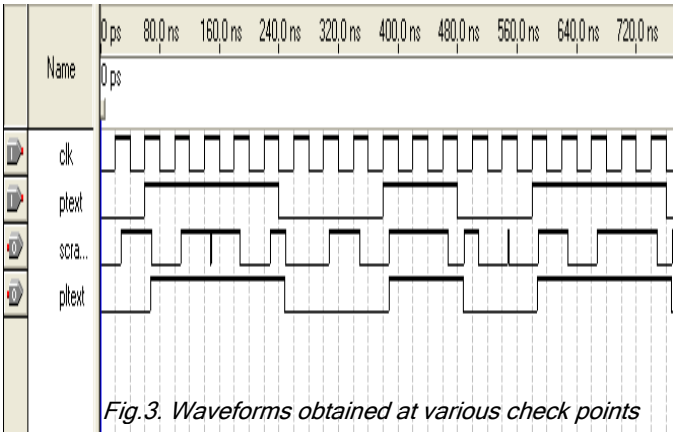


Fig.3. Waveforms obtained at various check points

Indian Journal of Science and Technology Vol.2 No. 10 (Oct 2009) ISSN: 0974- 6846

received data.

Simulation results and verification

The proposed scheme has been synthesized and simulated using Quarts Altera Software. The waveforms obtained at various check nodes have been investigated and found in conformity with the theoretical observations. Various waveforms obtained have been presented in Fig.2. As shown in Fig.3. *Clk* and *Ptext* are input signals and represent clock (that drives the system) and the Plain text to be scrambled. *Scram* and *Pltext* are output signals that denote scrambled signal and received text respectively. It is evident from the Fig. 3 that input data and received data is in complete agreement while as input data does not resemble the scrambled data at all, The RTL viewers of the synthesized design are given in Figs. 4-6.

Fig.4. RTL viewer of the implemented logic

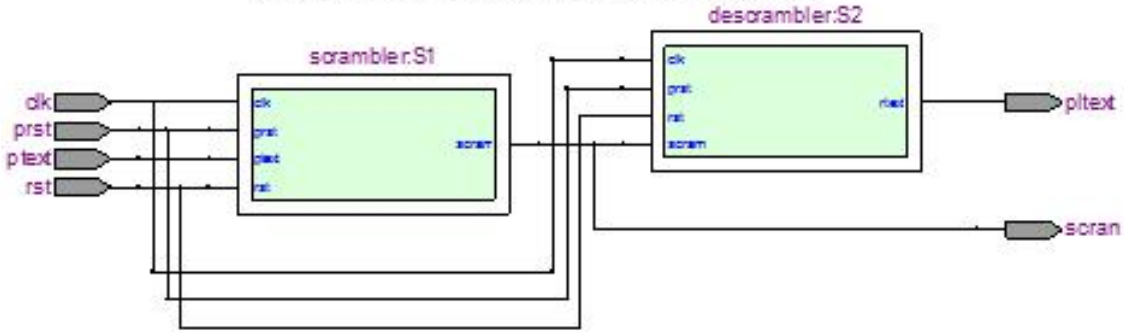


Fig.5. RTL viewer of the implemented scrambler

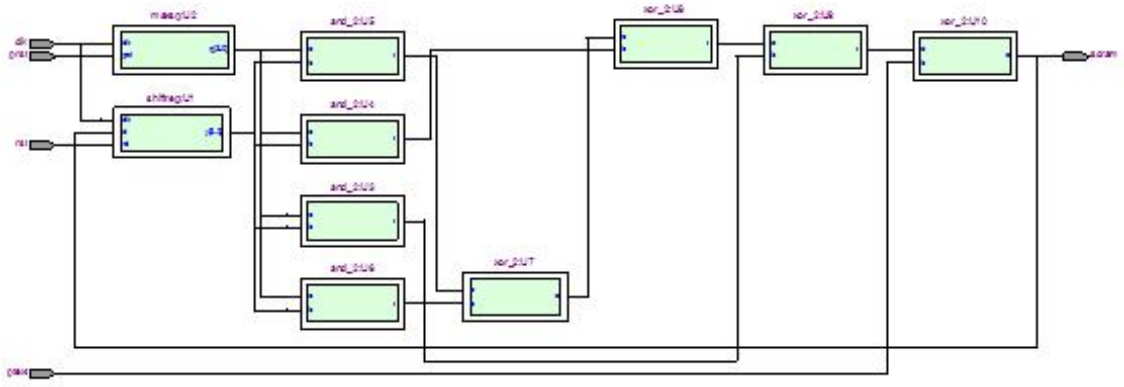
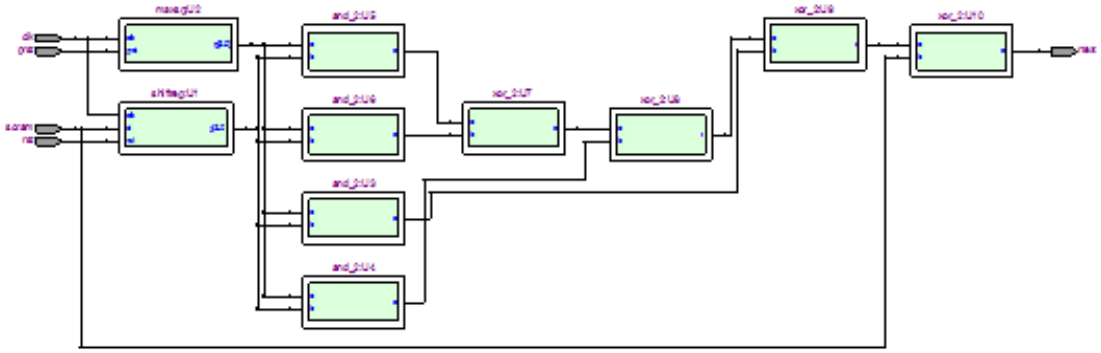


Fig.6. RTL viewer of the implemented descrambler



Conclusion

An efficient scheme for data scrambling and descrambling for secure data transmission using VHDL has been proposed. The proposed scheme has been synthesized and simulated for target device EP1S10F484C5 of Straitix FPGA family. It has been found that the proposed scheme is capable of providing a range of applications in Spread Spectrum Modulation, Code Division Multiple Access and Global Positioning Systems. The proposed scheme can be synthesized and implemented on any of the existing CPLD and FPGA systems as per the degree of optimization required. The simulation and verification carried out at transmitting and receiving ends of the system has proved the efficacy of the proposed scheme. The results have been presented in the form of various waveforms.

References

1. Bhat, G. M and Ahmad W. "Reliable and Secure Data Transmission". Electronics Engineering, Vol. 68, No. 832, pp. 32-34, April 1996, London, U. K.
2. Schneier B (1996) Applied Cryptography. John Wiley & sons, Inc., Singapore.
3. Standaert, F. Piret, G. Rouvroy, G and Quisquater J.J, "FPGA Implementations of the ICEBERG Block Cipher", in the proceedings of ITCC 2005, vol 1, pp 556-561,Las Vegas, Nevada, April 2005.
4. Wasim Ahmad (2001- 2002) Development of low-cost secure communication techniques. AICTE (R&D) Project. Deptt. of Electronics Engg., AMU, Aligarh.