Chapter 6

Design of High Speed Re-configurable Co-processor for Next Generation scrambler and de-scrambler system

6.1 Introduction

The new generation of communication systems makes use of more complex standards for communication operation, which results in number of challenging as well as mismatched standards. Some of the standards like DSSS (Direct-Sequence-Spread-Spectrum),FHSS (Frequency-Hopping-Spread-Spectrum) [43], OSHA's Hazard-Communication-Standard (HCS) [44], OFDM (Orthogonal frequency-division-multiplexing), DAB (Digital-Audio-Broadcast) [45], CSMA(Carrier-Sense-Multiple-Access*)* [46], ADSL++ *(*Asymmetric-Digital-Subscriber Line-plus) DVB *(*Digital-video-broadcast*)* are perfect for new generation of communication system that support multi-media signals, multiband programmable operations and many other functions. Each process has been performed in different standards that are having different characteristics according to the principles [47].

6.2 Re-configurable Structures For scrambler and De-scrambler

Scramblers are used in numerous communication system protocols such as SAS/SATA, PCI express, USB. Bluetooth data transmitted data, satellite TV operator and cable. Scrambler is a device used for data encryption is the process of encoding data in such a way that hackers or eavesdroppers cannot be identified it. This encryption process is implemented with the help of VHDL and model sim simulator this regularly done by the use of an encrypted key. If authorized party want to decode the original data using decryption process that regularly requires a secret decryption key.Figure.6.1. Shows encryption process and decryption process using high speed Re-configurable Co-processor for scrambler and de-scrambler system, the binary input data given to scrambler (transmitter) is denoted by ‘C’ the encrypted data is denoted by ‘N’. Figure 6.1. Clearly shows data is encrypted with the help of a key K, generate a last function of ‘A’ transmitted bits ‘N’, which are generated by n-bit serial-in-parallel-out (SIPO) shift register. The output of encryption process produced a Boolean function ‘F’ with A-inputs compute ‘K’. This same function ‘F’ used for generates decryption at de-scrambler (receiver).

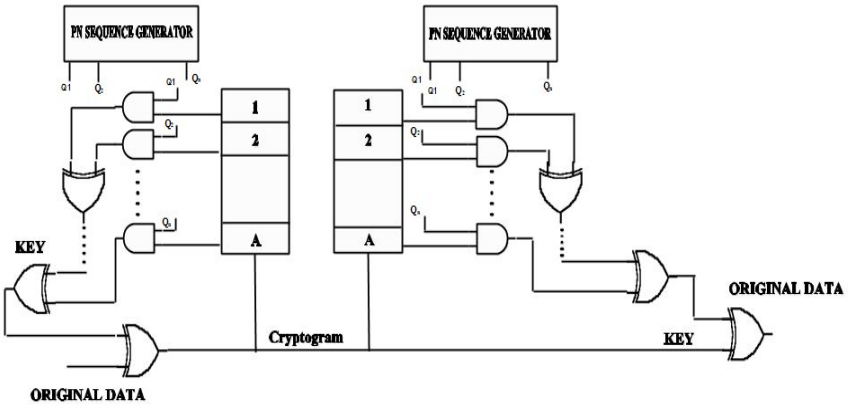

Figure .6.1. The Re-configurable Structures For scrambler and de-scrambler.

At the receiver side it produced a decryption data it same as the original data, it is clearly shows that modulo-2 addition of the key bits 'K' it help to generates original data from the encrypted data at the de-scrambler side.

Figure.6.1.shows the mathematical model of Re-configurable Co-processor for scrambler and de-scrambler system this can implemented by shifting and modulo-2 mechanism it help to produced cryptogram 'N'. Here 'N' can be represented by a mathematical expression as:

$$N=C+ (x_1D^1N+ x_2D^2N+ x_3D^3N+\ldots\ldots\ldots\ldots..+ x_AD^AN) \quad \ldots (1.1)$$

Where D represents the delay operator and x1 represents the i^{th} tap gain, the sequence N delayed by A units is represented by DAN and symbol '+' is represents modulo-2 addition. Equation 1.1 can be rewrite by:

$$N=C+ (x_1D^1+ x_2D^2+ x_3D^3+\ldots\ldots\ldots\ldots..+ x_AD^A)\ N \quad \ldots (1.2)$$

$$N=C+FN \quad \ldots (1.3)$$

With $F= x_1D^1+ x_2D^2+ x_3D^3+\ldots\ldots\ldots\ldots..+ x_AD^A$ … (1.4)

Hence $N=C + K$ … (1.5)

Where the key-bits K=FN

The tap gain value can be '0' or '1' in equation (1.4) .if any tap-gain x_1=1 it represented that the connection is taken from the i^{th} shit register stage and x_1=0 it represented that the no

connection is taken from that stage entire function process depends on the number of 'A' shift register levels and the tap gain values (0' or '1').the complexity of function 'F' increase with an increases in 'A', the cryptogram signal 'C' is hides the information signal from an unauthorized at the receiver side. To design a Re-configurable co-processor for descrambler for decrypting 'N', now we consider a receiver sequence 'N' given by equation (1.2) as:

$N=C+ (x_1D^1+ x_2D^2+ x_3D^3+\ldots\ldots\ldots\ldots..+ x_AD^A) N$

Adding $N=C+ (x_1D^1+ x_2D^2+ x_3D^3+\ldots\ldots\ldots\ldots..+ x_AD^A) N$ to both sides of the above equation we get.

$$N+(x_1D^1+ x_2D^2+ x_3D^3+\ldots\ldots\ldots\ldots..+ x_AD^A) N=C \quad \ldots (1.6)$$

Above equation (1.6) shows that the modulo-2 sums of any n-sequences with itself produced all sequences of 0's.

$$C=N (1+F) \quad \ldots (1.7)$$

With, $F= x_1D^1+ x_2D^2+ x_3D^3+\ldots\ldots\ldots\ldots..+ x_AD^A$

From the equation (1.3) to (1.7) shows that process will continued as long as the function 'F' is same for both scrambler and de-scrambler ,the output of both encrypted and decrypted data will be accurate this can be implemented by Re-configurable co-processor for scrambler and de-scrambler system. This are process it made very difficult to recognize of original signal for unauthorized person at receiver, the value of 'A' should be large, bit error propagation increases due this n errors at the output side.

The proposed Re-configurable Co-processor for scrambler and de-scrambler system used in communication system this is increases the secure data transmission and reception between two authentication persons. This process is implemented by hardware description language [48] [49] .it enhances the communication security, increases the speed of operation, optimizes the power consumption, reduces DC components and synchronization problem and increases pseudorandom number generator (PRNG) [50] [51].

6.3 Implementation Results and Comparisons

VHDL has been used to model the proposed design of high speed Re-configurable Co-processor applicable for scrambler and de-scrambler system structure. The synthesis is then performed using the model-sim. For the proposed structure, the gate count is about 40000 for scrambler and descrambler unit and critical-path is about 0.16 nm. Figure.6.2.shows the internal structure of proposed design of High Speed Re-configurable Co-processor for scrambler and de-scrambler system. Figure 6.3.shows the model-sim simulation waveforms of proposed design of High Speed Re-configurable Co-processor for scrambler and de-scrambler system.

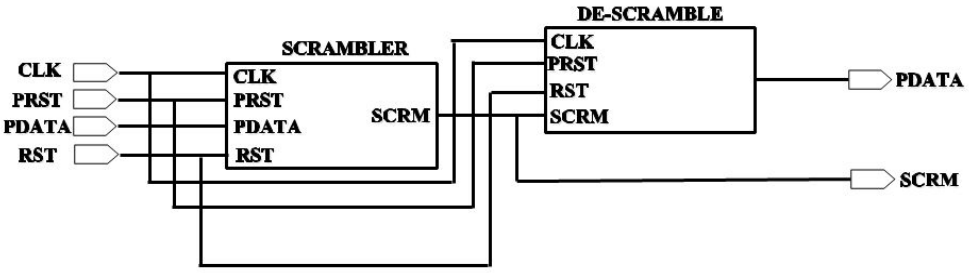

Figure.6.2.The Internal Structure of Proposed scrambler and de-scrambler system.

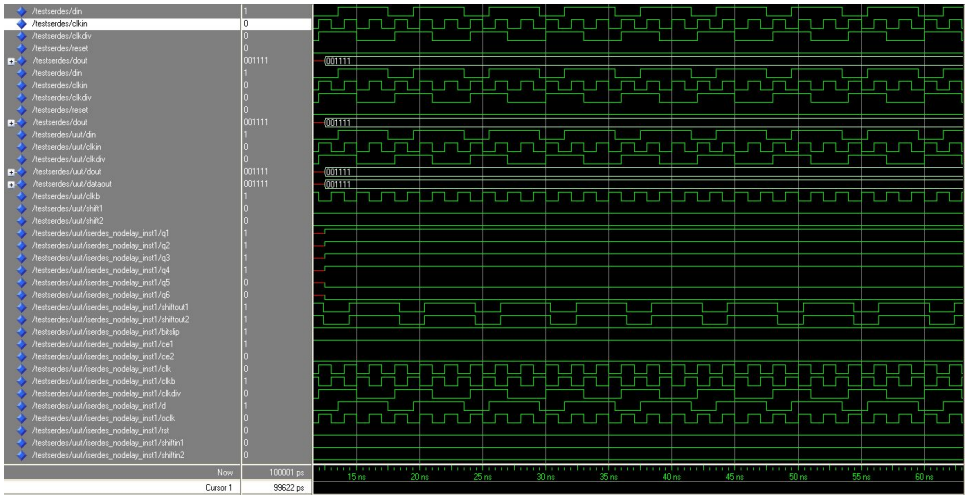

Figure 6.3. The model-sim simulation waveform of proposed scrambler and de-scrambler system.

Evaluation of the proposed Co-processor for various communication algorithms is done with the help of a simulator. The performance comparison between the proposed Co-processor and the conventional DSP (SC-140) [52], i.e., VLIW architecture is shown in Table 6.1.

From the table, we can infer that the proposed co-processor has better performance compared to the conventional DSP (Star-Cores SC-140, TMS320C6x [53], and TMS320C55x) [54] in terms of number of operation per clock cycle [55] [56].

Table 6.1. Performance Comparisons for Various Operations

Operation	TMS320C55x (Operation/Cycle)	Proposed Scrambler and Descrambler (Operation/Cycle)
Scrambler (MIPS) (802.11a,12Mbps)	$39X10^6$	$40X10^6$
Descrambler (MIPS) (802.11a,12Mbps)	$36X10^6$	$40X10^6$
Convolution encoding (cycles)	$77X10^6$	$85X10^6$