Design of High Speed Reconfigurable Coprocessor for Next Generation scrambler and de-scrambler system

Mallikarjunaswamy S1, Dr.Nataraj K.R2 and Dr.Rekha K.R3
SJB Institute of Technology-Bangalore/VTU-Belgaum.
pruthvi.malli@gmail.com, nataraj.sjbit@gmail.com, rekha.sjbit@gmail.com

Abstract— In this paper we present the high speed Reconfigurable Co-processor for scrambler and de-scrambler system. In a communication system more number of data will be transmitted through a media that transmitted data will be more secure and authenticated. with the help of scrambler device a some unknown data to the original data or by changing some important sequence of the original data in order identification of the original data for unauthorized person is very difficult, in order to identified original data by using appropriately descrambler system. The scrambling and de-scrambling operation is implemented with the help of VHDL and model sim simulator. The critical path about 0.12nm technology and gate count of about 36000 this performance shows that number of operation per clock cycle can be reduced about 52% for scrambler at transmitter side and 51% for de-scrambler at receiver side it show the proposed reconfigurable co-processor it better performance compare existing conventional DSP (Star-CoresSc140, TMS320C6x, TMS320C55x) in terms of number of operation per clock cycle.

Index Terms— Bitshuffleunitstructure, Convolutionalencoding, De-scrambler, FPGA, Model - sim Scrambler, and VHDL.

I. INTRODUCTION

The new generation communication system uses more difficult standards for communication operation, which resulted in number of challenging and mismatched standards. There are some standards are include like DSSS (Direct-Sequence Spread Spectrum) [2], FHSS (Frequency-Hopping Spread Spectrum) [3] OFDM (Orthogonal frequency-division multiplexing), OSHA’s Hazard Communication Standard (HCS) [4], DAB (Digital Audio Broadcast) [4], CSMA(Carrier Sense Multiple Access) [5], ADSL++(Asymmetric Digital Subscriber Line plus) DVB (Digital video broadcast)is a perfect for new generation communication system that supports multi-media signals and multi-band programmable operation and numerous other functions each are perform similar process in different standards that are having different characteristics according to the principles [1].

This paper proposes a Reconfigurable Coprocessor for scrambler and de-scrambler system. this is more accurate, highly reliable, and also has less delay better performance than existing general scrambler and de-scrambler system operations. The Scrambling is a process of adding new components to the original signal or the changing of some important component to the original signal in order to make extraction of the original signal difficult to the unauthorized person [6] as shown in Fig.1. The scrambler further classified as time domain scrambling, frequency domain scrambling variable-band scrambling, additive (synchronous) scramblers and multiplicative (self-synchronizing) scramblers. Fig.1. shows example
of additive scrambling and additive de-scrambling with polynomial $=1+X^5+X^7$. Its characteristics polynomial is $1+X^5+X^7$ because the polynomial function is performed by the output of register 5 and 8 and repeats its sequence after $2^{2N-1}=128$. In this operation performed by the help of linear feedback shift register in additional modulo-2 adder (XOR gate), where polynomial degree is represents by N, $X(i)$ represents the data to be scrambled (at time i), scrambled codeword is represents by $C(i)$, and the “key” produced by the linear feedback shift register is represents by $K(i)$. The original data $(X(i))$ can be shown as follows $C(i) = X(i) + K(i)$. Because $K(i) = K(i-5) \ XOR \ K(i-7), C(i) = X(i) \ XOR \ K(i-7)$ results. At the desscrambling $Y(i) = C(i) \ XOR \ K(i)$ is computed. Assuming that the two function are synchronized, $Y(i) = C(i) \ XOR \ K(i-5) \ XOR \ K(i-7)$ results, hence $Y(i) = X(i) \ XOR \ K(i-5) \ XOR \ K(i-7) \ XOR \ K(i-5) \ XOR \ K(i-7) = X(i)$ [1]. The scrambling and de-scrambling operation is implemented with the help of VHDL and model sim simulator and evaluated performance and comparisons with existing DSP chip (Star-CoresSc140, TMS320C6x, TMS320C55x) in terms of number of operation per clock cycle.

![Fig.1. Scrambling and De-scrambling](image)

**II. RECONFIGURABLE 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. Fig.2. Shows encryption process and decryption process using high speed Reconfigurable 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’. Fig.2. 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 generate decryption at de-scrambler (receiver),

![Fig.2. The Reconfigurable Structures For scrambler and de-scrambler](image)
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.
Fig.2. shows the mathematical model of Reconfigurable 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:
\[ N = C + \left( x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A \right) \]
Where D represents the delay operator and x1 represents the ith 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:
\[ N = C + (x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A) \]
N = C + (x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A) N \]
\[ \text{Hence} \quad N = C + K \]
Where the key-bits K=FN
The tap gain value can be ‘0’ or ‘1’ in equation (1.4) if any tap-gain x1=1 it represented that the
connection is taken from the ith shit register stage and x1=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 reconfigurable co-
processor for descrambler for decrypting ‘N’, now we consider a receiver sequence ‘N’ given by equation
(1.2) as:
\[ N = C + \left( x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A \right) \]
Adding \[ N = C + \left( x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A \right) \] N to both sides of the above equation we get.
\[ N + (x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A) N = C \]
Above equation (1.6) shows that the modulo-2 sums of any n-sequences with itself produced all
sequences of 0’s.
\[ C = N (1+F) \]
With, \[ F = x_1D^1 + x_2D^2 + x_3D^3 + \ldots + x_AD^A \]
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 reconfigurable 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.
Fig.3. shows the proposed shift-XOR operation [11] First step it receives X+Y as input data bits and
Mask1, and generates the Y shifted data that are shifted by 1 through Y bits. Next step, it performs parallel
XOR operations of the input data and the Y shifted data selected by Mask1(Y-bits). Consider M-th bit of
Mask1 (Y-bits), set to “1”, the M-bit shifted data is XORed with the input data. Hence, the Y output data are
generated and transferred to the switching unit. The switching network stores all or some of the Y output data
on the registers according to Mask1 (Y-bits). Mask1 (Y-bits) is the selection signal that enables the registers
to store the only valid outputs among the Y output data is transferred to the switching network [12] [1].
The proposed reconfigurable 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 [13] [14].it enhances the communication security,
increase the speed of operation, optimize the power consumption, reduces DC components and
synchronization problem and increases pseudorandom number generator (PRNG) [15] [16].

III. IMPLEMENTATION RESULTS AND COMPARISONS
The proposed design of high speed reconfigurable coprocessor for scrambler and de-scrambler system
structure has been modeled by VHDL and synthesis has been performed using the model-sim. The proposed
Structures gate count of about 36000 for scrambler and descrambler unit and critical path about 0.12nm
technology. Fig.4.shows The Internal Structure of Proposed Design of High Speed Reconfigurable
Coprocessor for scrambler and de-scrambler system. Fig. 5 shows the model-sim simulation waveform of Proposed Design of High Speed Reconfigurable Coprocessor for scrambler and de-scrambler system.

Fig. 3. Shift-XOR Array Architecture

The proposed coprocessor has been evaluated for various communication algorithms using the simulator. Table I and Fig. 6 shows the performance comparisons between the proposed coprocessor and the conventional DSP (SC140) [7] that is VLIW architecture. It shows the proposed coprocessor as better performance than the Conventional DSP (Star-Cores Sc140, TMS320C6x [8], and TMS320C55x) [9] in terms of number of operations per clock cycle [10] [17].

Fig. 4. The Internal Structure of Proposed scrambler and de-scrambler system
Fig.5. shows The model-sim simulation waveform of proposed scrambler and de-scrambler system

### TABLE I. PERFORMANCE COMPARISONS FOR VARIOUS OPERATIONS

<table>
<thead>
<tr>
<th>Operation</th>
<th>TMS320C55x (Operation/Cycle)</th>
<th>Proposed Scrambler and Descrambler (Operation/Cycle)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrambler (MIPS)</td>
<td>39X10⁹</td>
<td>40X10⁹</td>
</tr>
<tr>
<td>(802.11a,12Mbps)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descrambler (MIPS)</td>
<td>96X10⁹</td>
<td>40X10⁹</td>
</tr>
<tr>
<td>(802.11a,12Mbps)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convolution encoding</td>
<td>77X10⁸</td>
<td>85X10⁹</td>
</tr>
<tr>
<td>(cycles)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IV. CONCLUSIONS

In this work, we have proved the design and the implementation of high speed reconfigurable coprocessor for scrambler and de-scrambler system. The reconfigurable coprocessor that can support various communication standards and algorithms. An efficient operation of distribution communication system networks can be achieved by using reconfiguration techniques. The communication system network reconfiguration is carried out by changing the code rate and an instructions status of the sectionalizing switches. In a communication system more number of data will be transmitted through a media that transmitted data will be more secure and authenticated. With the help of scrambler device a some unknown data to the original data or by changing some important sequence of the original data in order identification of the original data for unauthorized person is very difficult, in order to identified original data by using appropriately descrambler system. The scrambling and de-scrambling operation is implemented with the help of VHDL and model sim simulator. The critical path about 0.12nm technology and gate count of about 36000 this performance shows that number of operation per clock cycle can be reduced about 52% for scrambler at transmitter side and 51% for de-scrambler at receiver side it show the proposed reconfigurable co-processor it better performance compare existing conventional DSP (Star-Cores Sc140, TMS320C6x, TMS320C55x) in terms of number of operation per clock cycle.

### REFERENCES