IOSR Journal of Engineering (IOSRJEN **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 04 (April. 2014), ||V2|| PP 50-53

Double layer Lookup table technique implemented with (FPGA) for security

Zuhir Nemer Alaaraj, Abdelrasoul Jabar Alzubaidi
1 Sudan Academy of Sciences (SAS); Council of Engineering Researches & Industrial Technologies
2 Electronic Dept. - Engineering College –Sudan University for science and Technology

Abstract: - This work proposes a solution to improve the security of data through flexible bitstreem encryption, by using the two lookup table (LUT)s that is embedded in the FPGA.This technique concentrates on building high data security to make it difficult for an adversary to capture the real data.The syntheses proposed can be implemented in two steps:
First step: programming the FPGA to create a two LUT by VHDL language each LUT has a predefined length and contents.
Second step: applying security strategy.
A high security and more reliability can be achieved by using this mechanism when applied on data communication and information transformed between networks.

Keywords: - *LUT, FPGA.VHDL, embedded system, security.*

I. INTRODUCTION

The FPGA architecture consists of three types of configurable elements - a perimeter of input/output blocks (IOBs), a core array of configurable logic blocks (CLBs), and resources for interconnection. The IOBs provide a programmable interface between the internal arrays of logic blocks (CLBs) and the device's external package pins, see figure (1). CLBs perform user-specified logic functions, and the interconnect resources carry signals among the blocks [1].

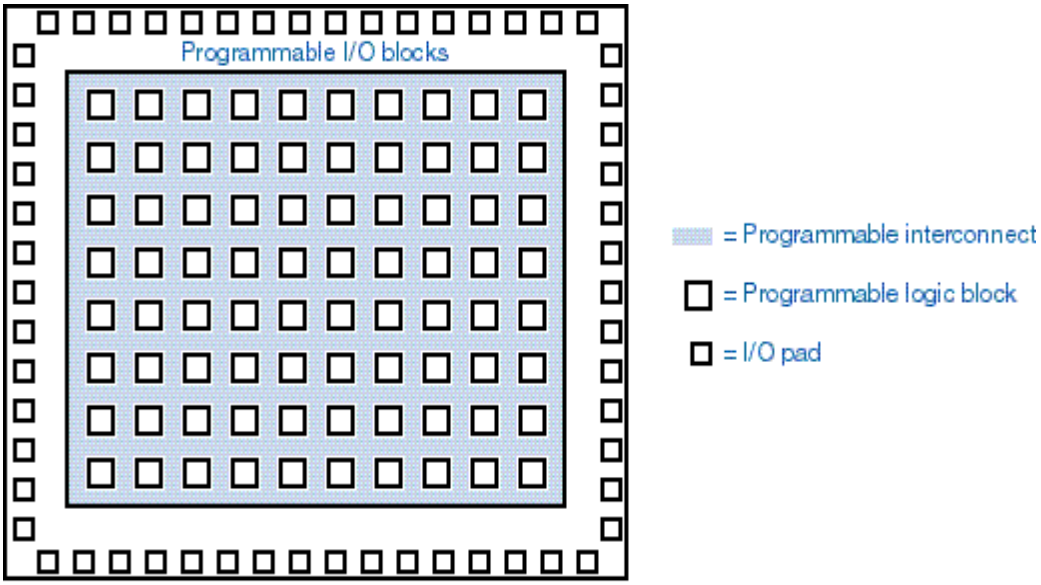


Figure 1 Structure of FPGA

Those FPGAs are attractive for executing the actual cryptographic algorithms and are, thus, of particular importance from a security point of view.
FPGA produced by XILINX will be used.
Today FPGAs represent an efficient design solution for numerous systems. They become necessary to improve data security.

SYNTHESIS .II

All randomly stored values in FPGA are indexed with the addresses at the lookup table.
These random values are stored by the user (program).
The obtained structures from this mechanism are blind, and the adversary who doesn't know the algorithms cannot reverse it to the original feature values.
These types of techniques were developed to prevent an attacker from knowing the real data.
The logic design of a module can be done with a standard hardware description language, such as Verilog or VHDL.

III. DESIGN THEORY

The procedure includes embedding a two LUT to deploy security.
In the beginning we start by defining two variables which we apply on each lookup table:

1. The length of lookup table which is the number of data bytes we would like to embed in it.
2. The content of data inserted by the programmer in the LUT.

Here, when we deploy security strategy every byte from the input data stream is altered by XORing it with the written value in the LUT1 and LUT2.
The process continues till the end of each lookup tables content are finished .
The operation is repeated if the data stream is present.
Hence, we obtain a cipher text which is ciphered by two lookup tables content XORed with data, which is known only to the programmer.
The attacker cannot retrieve the original data because he can't know two very important factors in ciphering:

1. The length of each lookup tables and so the number of repeats.
2. The content of each lookup tables which was written by the programmer.

In this methodology the programmer can change the security strategy at his well.

IV. METHODOLOGY

Step1:
Programming of the FPGA:
The process of implementing a design on an FPGA can be broken down into.
The VHDL code is converted into device netlist format. Then the resulting file is converted into a hexadecimal bit-stream file, or bit file. This step is necessary to change the list of required devices and interconnects into hexadecimal bits to download to the FPGA.
The bit file is downloaded to the physical FPGA.
This final step completes the FPGA synthesis procedure by downloading the design onto the physical FPGA see figure (2).

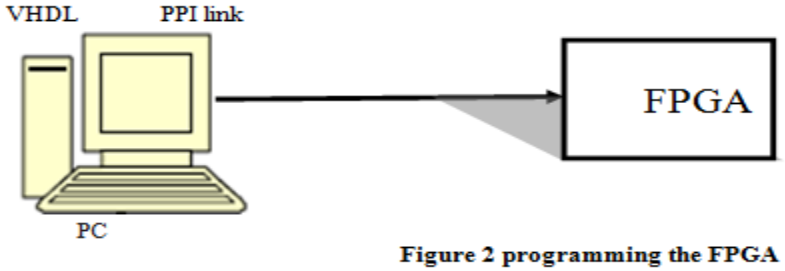


Figure 2 programming the FPGA

Step2:
Application for security on the network

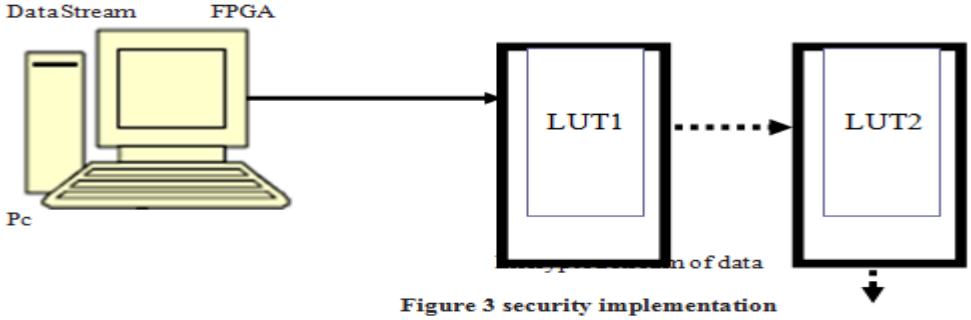
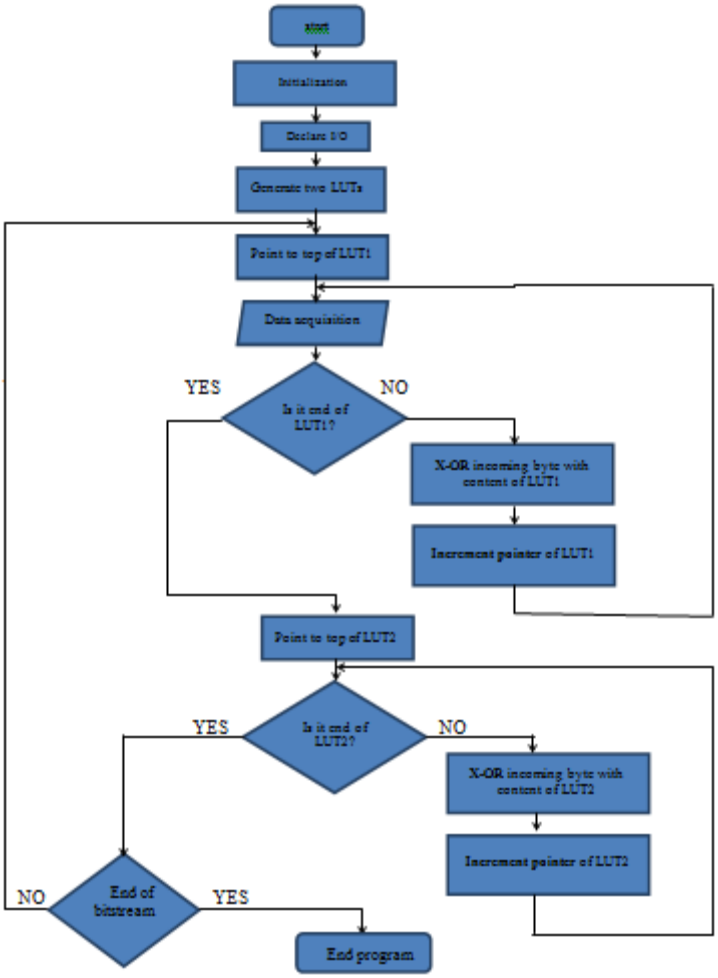


Figure 3 security implementation

The algorithm

The design proposes a creation of ten bytes lookup table.
The contents of the ten bytes can have any value.
The flow chart for the design is shown in figure (4).



6. Results:

Assume a data stream being input to the FPGA (column 1 in figure 5), and the ten characters of the lookup table (column 2 in figure 5).
Xoring column 1 with column 2 gives us encrypted data output shown in column 3 of figures (5).

Column1 (xor) column2 = column3
ST (XOR) LUT1 = EN1 …….. Equation (1)

Column 1	Column 2	Column 3
Data stream (ST)	LUT1	ST(XOR)LUT1=EN
(41)H	(45)H	(04)H
(43)H	(4C)H	(0F)H
(45)H	(45)H	(00)H
(47)H	(43)H	(04)H
(49)H	(54)H	(1D)H
(4B)H	(52)H	(19)H
(4D)H	(4F)H	(02)H
(4F)H	(4E)H	(01)H
(51)H	(49)H	(18)H
(53)H	(43)H	(10)H

Figure 5 example based on LUT1

In layer two the lookup table2 have the ten characters(column4 in figure 6) this content Xoring with the ciphered data that obtained from layer one (ST (XOR) LUT1) column 3 that gives us encrypted data output shown in column 5 in figure (6).

Figure (5) and figure (6) shows the complete picture of the assumption.

The data stream and the contents of the (LUT1) and (LUT2) are given in (ASCII) code.

Column3 (xor) column 4 = column 5

EN (XOR) LUT2=EN2 ……..Equation (2)

Column 3	Column 4	Column 5
EN	LUT2	EN(XOR)LUT2=EN2
(04)H	(3C)H	(38)H
(0F)H	(45)H	(4A)H
(00)H	(34)H	(34)H
(04)H	(2D)H	(29)H
(1D)H	(5B)H	(46)H
(19)H	(4F)H	(56)H
(02)H	(47)H	(45)H
(01)H	(39)H	(38)H
(18)H	(50)H	(48)H
(10)H	(4A)H	(5A)H

Figure 6 example based on LUT2

The cipher text that obtained from double layer lookup table has four blind variables the length of each lookup table and its contents.

V. SUMMARY AND CONCLUSION

Excessive security related to using a single layer lookup table. And more reliability and high performance can be achieved by using this mechanism, when applied on data communication and information transferred between networks.

This paper is demonstrating new security structures concepts embedded in self reconfigurable VLSI technology environment. The resulting secret ciphers exhibit new security application horizons due to the particular possibility of constructing autonomous practical secret unknown functions. Keeping functions secret was assumed as a non-realistic assumption in cryptographic systems [2].

REFERENCES

[1] A. S. Daniel Ziener and T. J□urgen. Identifying FPGA IP-Cores based on lookup table content analysis. In Field Programmable Logic and Applications, August 2006. http://www12.informatik.uni-erlangen.de/publications/pub2006/zienerfpl06.pdf

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi.The EM side-channel(s).In Cryptographic Hardware and Embedded Systems Workshop, volume 2523 of LNCS, August 2002.http://www.springerlink.com/content/mvtxbq9qa287g7c6/\