IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 05, Issue 02 (February. 2015), ||V1|| PP 53-56

Data encryption using Field Programmable Logic Controller

Motea Abdul Aziz Mohammed Noman1, Saifeldeen Fatooh2,
Abdelrasoul Jabar Alzubaidi 3
1 PHD candidate motiea@hotmail.com, 2 Dean of Emarat college, 3 Sudan University of science and Technology- Engineering College- Electronics Department Rasoul46@live.com

Abstract: Data Encryption is the process of protecting the privacy and confidentiality of data. To provide this protection, professionals frequently look to commonly accepted technologies and methodologies to safeguard the data while at rest and in transit. One technology capable of providing this type of protection is encryption.
Security rule has long identified encryption as a mechanism to safeguard electronic protected information. More recently, the standards and certification criteria for electronic security of data must be able to encrypt and decrypt the information in order to qualify for stage 1 of the meaningful use incentive program.
Similarly, a rule identified encryption as one technology that can render protected information "unusable, unreadable, or indecipherable to unauthorized individuals." Protected information that is encrypted in accordance with this guidance is not subject to breach notification requirements. The guidance discusses encryption as a mechanism to protect data in transit and at rest.
Field Programmable Gate Array (FPGA) will be used in the design to perform the real time encryption processing.. Verilog Hardware Description Language (VHDL) will be used to program the FPGA. A data logger is used as a media of data storage .The data stream is generated by a personnel computer (PC) using Turbo C++ language. The paper adopts an embedded system design dedicated for a real time data encryption.

Keywords: *encryption, data, information, FPGA, VHDL, data logger, PC, TC++.*

I. INTRODUCTION

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. Encryption can be used to protect data "at rest", such as files on computers and storage devices .In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail.
Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices 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.

II. METHODOLOGY

The system is divided into parts; hardware and software. In the hardware, an FPGA is used as a real time processing tool in the system design.. A data logger is used as a model for the storage of the encrypted data . In the design a personnel computer is considered as the source of data to the FPGA. The design accepts stream of data from any digital electronic source to supply the FPGA with plain data.
A software code is developed in the FPGA to encrypt the incoming stream of data . The code of encryption is written in VHDL language and downloaded in the FPGA in a (.bit) format. A` multi level gates technique is implemented in structuring the digital electronic circuit into the FPGA. SPARTAN-3 software package is used in programming the FPGA.. The PC generates the plain stream of data using Turbo C++ language) TC++).

III. SYSTEM LAYOUT

The aim of the design is to illustrate the usage of the encryption process and its applications .The electronic devices required to construct the encryption system is a personnel computer, FPGA , data logger , plus interconnection links and lab link cable. The block diagram of the hardware implementation of the entire system is shown in Figure (1) below.

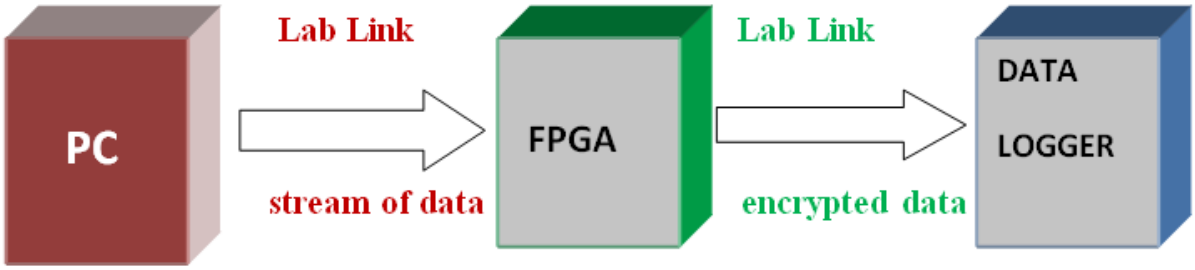

Figure (1) Block diagram of the encyption system

The input system consists of three electron blocks. The mechanism of the system operation is based on equations (1) to (3);

Encrypte-1 = (plain data) XOR (level-1 gates) **…… …… (1)**
Encrypte-2 = (encrypte-1) NAND (level-2 gates) **…… …… (2)**
Encrypte-3 = (encrypte-2) OR (level-3 gates) **…… …… (3)**

The hardware components are :

- Personnel computer (PC) :

A PC furnished with a parallel port is used for programming the FPGA with the VHDL language .The parallel port of the PC is also used to supply the FPGA with plain data in the parallel format byte by byte .

- Field Programmable Gate Array (FPGA) :

An FPGA type (XILINX) is used . Its part number is (XC3S-200). It capacity is 200 kilo gates . It is programmed by VHDL language.

- Data logger:

A **data logger** (also **datalogger** or **data recorder**) is an electronic device that records data over time or in relation to location either with a built in instrument or via external instruments. Increasingly, but not entirely, they are based on a digital processor (or computer). They generally are small, battery powered, portable, and equipped with a microprocessor, internal memory for data storage . Some data loggers interface with a personal computer and utilize software to activate the data logger and view and analyze the collected data, while others have a local interface device (keypad, LCD) and can be used as a stand-alone device.

- Lab links :

Lab links are sort of cables that connects the computer port to external electronic devices .They are used for conveying the stream of data from the PC to the FPGA and from the FPGA to the data logger.

IV. SOFTWARE PROGRAM AND ALGORITHM

To achieve the objective of the real time encryption and data logging , we need to go through five steps as follows:

1. Step one is developing a VHDL program in the computer by using Spartan-3 software .
2. Step two includes VHDL synthesis in the design, which converts the design in the behavioral description file into gates. The synthesis tools figure out what gates to be used based on the VHDL program file.
3. Step three includes downloading of the (.bit file) into the FPGA as shown in figure (2).
4. Step four includes interconnecting the FPGA to the data logger by a lab link , as shown in figure (1).
5. Step five in includes testing and debugging the operation of the whole system .

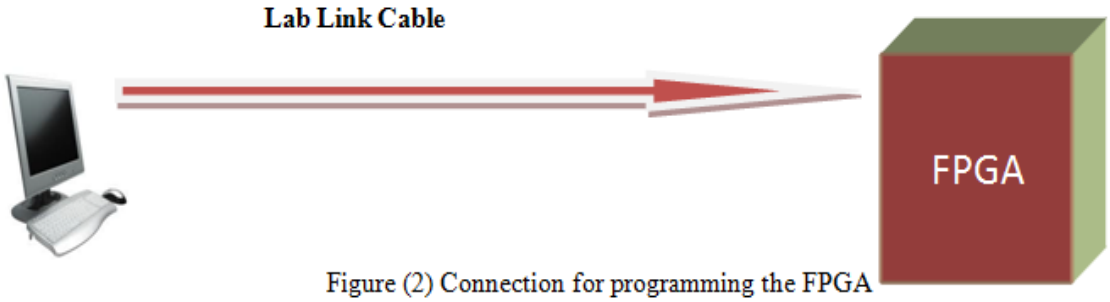

Figure (2) Connection for programming the FPGA

The algorithm performs a real time encryption of data and storage in the data logger. The algorithm contains four subroutines . Calling the subroutine one after the other makes the program modular .The first subroutine processes the data encryption related to level-1 gates array in the FPGA. The second subroutine processes the data encryption related to level-2 gates array in the FPGA. The third subroutine processes the data encryption related to level-3 gates array in the FPGA. The fourth subroutine processes the data conveyance from the FPGA to the data logger .The execution of the four subroutines means performing a complex encryption procedure on a single byte of the data stream .The processing is repeated till the end of the data stream coming from the PC. The FPGA algorithm is :

Start
Initialization :
… Program FPGA connector (A1) as input.
… Program FPGA connector (A2) as output.
... Clear the FPGA output connector (A2).

Poll for data input:
.. If a byte is received , then call level-1 encryption subroutine..
.. Call level-2 encryption subroutine..
.. Call level-3 encryption subroutine..
.. Call output to data logger subroutine..
Go to Poll the sensors.

Level-1 encryption subroutine :
… Pass the byte though eight XOR gates array.
… Pass byte to level-2.
Return.

Level-2 encryption subroutine :
… Pass the byte though eight NAND gates array.
… Pass byte to level-3.
Return.

Level-3 encryption subroutine :
… Pass the byte though eight OR gates array.
… Pass byte to FPGA output connector (A2).
Return.

Output to data logger subroutine:
… Pass the encrypted byte to the data logger .
.. Give byte finish acknowledge.
Return.

The PC supplies the FPGA with plain data byte by byte through the parallel port . Turbo C++ programming language is used .The PC algorithm: is :

Start
Initialization:
... Clear the parallel port output.

Generate byte:
… Generate a byte at the parallel port output.
… If bytes generation is finished , then go to end.
… Go to generate byte.
End

V. RESULTS

The system performs two types of tasks. The first task is programming the FPGA with VHDL language . The second task is the plain data generation ,encryption and storage in the data logger..Table (1) below shows the results when operating the system .The table indicates the result obtained for a randomly selected byte..

Table (1) The results when operating the system

BYTE	LEVEL-1 (XOR)	LEVEL-2 (AND)	LEVEL-3 (OR)	BYTE IN DATA LOGGER
0	1	0	0	0
1	0	0	1	1
0	1	1	1	1
0	1	1	1	1
0	1	1	1	1
0	1	1	1	1
0	1	1	1	1
1	0	0	0	0

NOTE: ASCII code of input byte represents (A) , while the byte in the data logger becomes (~).

VI. CONCLUSION

The circuit that enabled the data encryption in the FPGA adapted three levels strategy of gate arrays. The number of levels can be changed as well as the algorithm of performing the encryption. . The electronic FPGA represents an embedded system . Any change in the strategy and the algorithm results in a total change in the stored data in the data logger.. A model of the system is constructed and its operation is satisfactory.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practice, 5th Edition, Prentice Hall, 2011.
[2] Volnei A. Pedroni, Circuit Design with VHDL, MIT press, Massachusts, 2004.
[3] ISE Simulator (ISim), UG682(v1.0), 2009.
[4] Deming.C, Jason.C, and Peichan. P, " FPGA Design Automation: A Survey", now Publishers In, (2006).
[5] Stephen .B and Zvonko.V,"Fundamental of Digital logic with VHDL Design",McGrow Hil,(2005)