Design and Implementation of a Cipher System (LAM)

PANAGIOTIS MARGARONIS[1], DR. EMMANOUIL ANTONIDAKIS[2]
1. Department of Information and Communication System Engineering
University of Aegean
2. Department of Electronics
TEI of Crete
panmarg@yahoo.com

Abstract: - This paper presents the design and implementation of a digital integrated encryption/decryption circuitry called LAM which is based on Peripheral Component Interconnect (PCI) Architecture for a Personal Computer (PC) communication card. The implementation of a hardware PC cryptography card has been designed using a Field Programmable Gate Array (FPGA) chip in combination with the PCI Bus. The main objective of this paper is to provide the reader with a deep insight of the design of a digital cryptographic circuit, which was designed for a FPGA chip with the use of Very (High-Speed Integrated Circuit) Hardware Description Language (VHDL) for a PCI card. A demonstration of the LAM circuitry will be presented. To see the effect of the LAM cryptography in the operation of the card, it was also simulated and analyzed. The Simulations were run under various conditions, which are applicable to most PCI applications.

Keywords: - Hardware, Security, Communication, Computer, Design, Architecture

1 Introduction

Recently, the need for a trustworthy computing system with high requirement which will be at the same time secure seems to be necessary. Moreover, the development speed of the processor possibility creates the requirement for quick motherboards and extension cards on PC. The engineers problem was the development of an interconnection bus between processor and extension cards which would not be necessary to change every time that a new technology would be born, namely an interconnection bus which would offer service for a long time on the motherboard card of PC. Intel's engineers who invented the PCI Bus at the July of 1992 found solution to this problem.

In addition, cryptography nowadays has been chosen for many digital broadcasting applications and networks. LAM is aimed to be a new cryptographic system which can be used for many different electronic communication establishment and commercial conciliation.

Moreover, the implementation of cryptographic algorithms on FPGAs offers a great deal of advantages such as algorithm agility. The same FPGA chip can be reprogrammed to achieve scalable security through different versions of the same algorithm (e.g DES and Triple-DES). The switching of wiring between algorithms on the FPGA chip can be easily achieved. Also the features of the FPGA maximize the opportunity for on-chip parallelism.

In the present work a design of the PCI based LAM system on a FPGA chip has been attempted.

As far as we know the present work is not published or mentioned officially by anyone else.

The basic idea is shown below (Figure 1). PCI/LAM card and the PCI card are two different cards connected each other on the same PCI slot. The application on the PCI card could be a modem/LAN module.

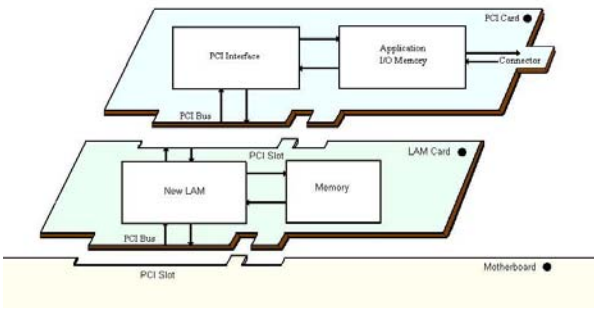

Fig. 1: LAM idea

The LAM card (see Figure 1) comprise a specialty card which from the one side is connected with the PCI bus and on the other side is embedded a PCI slot where any PCI card will be able to be connected. The idea of the LAM card is not to affect at all the operation of the PCI card, just to act as an observer where the data and the control signal of

PCI will pass from the one slot to other via the LAM card. The difference will be on the duration of the PCI data phase and only when the PCI card runs as a master. Then the LAM card will ciphers the data. The LAM card will be as one "black box" for the PC (software and hardware). LAM uses symmetric cryptography in real time communication with a synchronization system which does not send any information as far as key is concerned.

The main contribution of the present paper is the description of a black box crypto-system that is called LAM, which uses symmetric cryptography without the need to send any information about the key from the sender to the receiver and vice-versa.

At the following sections the design of PCI/LAM card, the LAM circuitry and the interconnection of PCI/LAM with the application (modem/LAN module) will be represented.

In the present work we assume that the architecture runs at 33 MHz with data bus 32 bits, that means 133 MB/sec maximum transfer rate while for 66 MHz is 266 MB/sec. Instead of 66 MHz with data bus 64 bits has 533MB/sec maximum transfer rate. Notice that the extension from 32 bits and 33 MHz to 64 bits and 66 MHz will be future work of the present implementation.

2 LAM Architecture

As it was mentioned above, the LAM card is a crypto system which comprise a specially constructed card between the PCI bus and the PCI card.

If the PCI Card works as an Ethernet card the LAM card check each time the data that come or leave the PCI bus and finds the headers of a TCP/ IP packet comparing each time the data with the IP source address, the IP destination address and the TCP port (which are known for the LAM). LAM works on the Internet layer of TCP/IP standard (see Figure 2 below). It is very important LAM does not cipher the headers of protocols

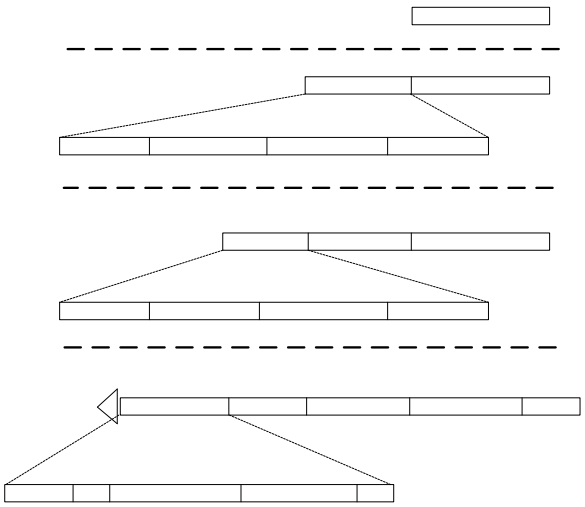

Fig. 2: TCP/IP Standard

Below are mentioned some of the LAM operation characteristics

- The LAM card has to run faster than the PCI bus clock as to have in the same period greater number of palms, which means that will be in time for LAM algorithm calculation and will not affect the PCI Card (see Figure 3 below).

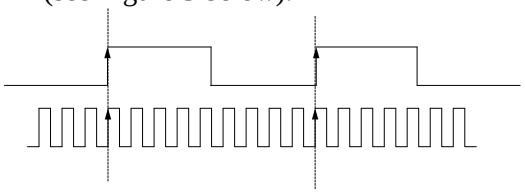

Fig. 3: LAM clock

- The LAM is comparing the source and the destination address therefore could create different cryptographic teams according to the users.
- Due to the fact that LAM checks the headers of the protocols could have been chosen different cipher operation modes according the TCP application port. (e.g FTP= 21 TELNET= 23 SMTP= 25 ECHO= 7 X.400= 103).
- LAM uses symmetric cryptography in real time communication, so has to run with a very strict synchronization. Moreover LAM does not send any information concerning the key.

2.1 Synchronization

For the synchronization LAM uses a combination of the existing TCP/IP Headers and an external counter. The first counter (internal) is included in TCP/IP Headers which have been created as well by the TCP/IP protocol to inform the receiver about the

number of the packet (actually the number of the bytes that has been already sent) for the reassembly of the information). This number is called Sequence number and use 16 bit of the TCP header. The external counter is created by LAM at every final packet of the information. TCP/IP protocol asserts a flag in the header of the final packet of information to inform receiver that this packet is the final. This flag is called F and is 1 bit of the TCP header.

So LAM increases its counter every time that "see" the final packet. The combination of the internal and external counter creates different numbers for every TCP/IP packet which both LAM transmitter and receiver use for the synchronization of their components (e.g. key generator).

Each byte has a different Look Up Table (LUT) memory which provides the key. It is like the cipher book method. There are about 1460 LUT memories (the number of payload bytes that are included in a packet) and each memory has the size of 8x256 bytes. Every byte is ciphered by the crypto unit using the output of the LUT memory for key. According to the number of internal and external counter, the configuration unit creates different address for each LUT memory such as to create different key for each byte of data respectively. Figure 4 illustrates the above sentence.

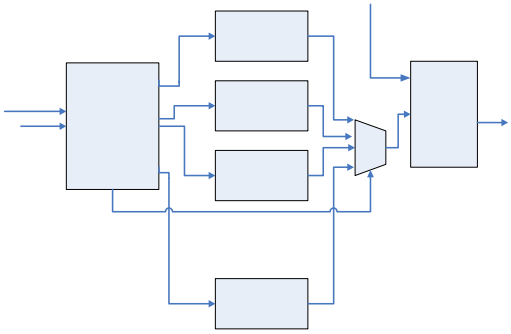

Fig. 4: Configuration- Synch LAM

If a packet requires retransmission the same header is needed to be created as before. The difference maybe is on the start Sequence number of TCP. Thus, LAM recognizes the header and acts like before in order not to change the cipher data. If the connection between sender and receiver fall then LAM holds the value of the external counter at the same value in order that when will be reconnected both devices would have the same counter value. Notice that LAM creates different counter value for each byte of a packet that is sent in order to be on time with the TCP/IP sequence number.

LAM circuitry includes external user interface for various uses like manual synchronization reset (initialization external counter) and all the necessary circuits for the FPGA reprogramming. LAM card includes the same circuit two times for more flexibility. Figure 5 represents the previous clause.

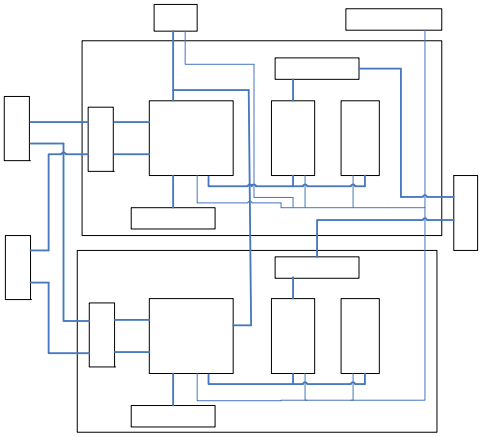

Fig. 5: LAM card Architecture

LAM does not need driver development or PCI Controller implementation

Below is illustrated a general view of LAM architecture as well as and the components which are being included (see Figure 6). The basic stages of the LAM are: Control unit, Comparator, Adder, Configuration unit, Substitution memory and final the Crypt unit.

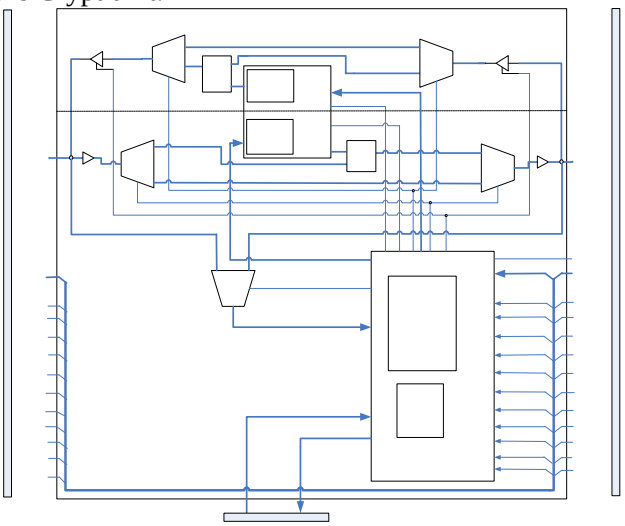

Fig. 6: LAM architecture

Up to now the crypt unit uses two different chipper algorithms: DES and One-Time-Pad.

The steps that have been followed for the development of the LAM are illustrated in figure 7.

3 Implementation

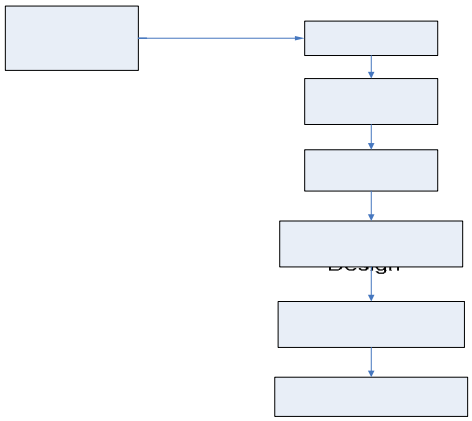

Fig. 7: LAM development dataflow

The software which has been used is:

- UltraEdit editor for the VHDL
- Xilinx ISE 9.1i for the implementation
- LeoNardo for the synthesis
- ModelSim for the simulation

Figure 8 (LAM design summary) represents the process view of the LAM implementation while figure 9 (LAM top placement), 10, 11 illustrates the LAM view inside the FPGA chip

The chip which was used for the realization of the LAM is xcv600e-8bg560 from Xilinx.

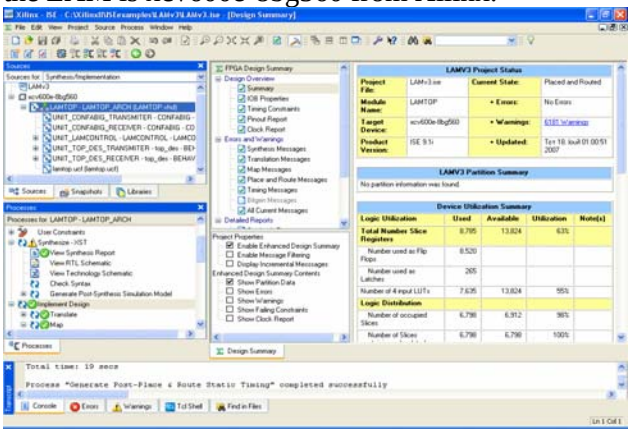

Fig. 8:LAM Process View from Xilinx ISE 9.1i

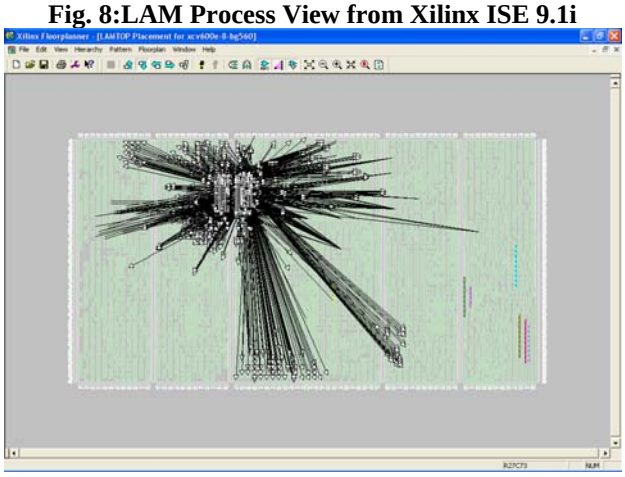

Fig. 9: LAM view from Xilinx Floorplanner

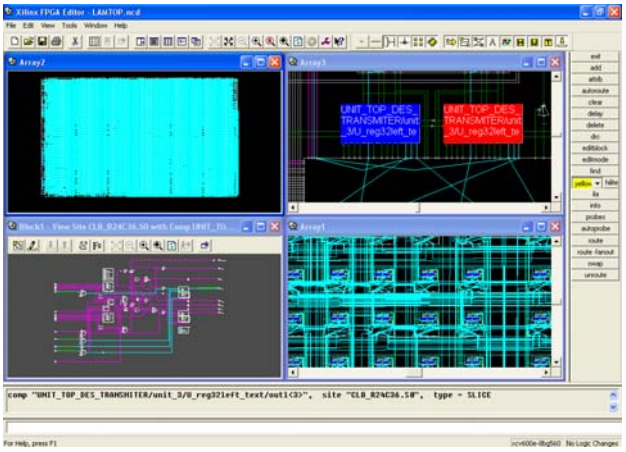

Fig. 10: LAM view from Xilinx FPGA Editor

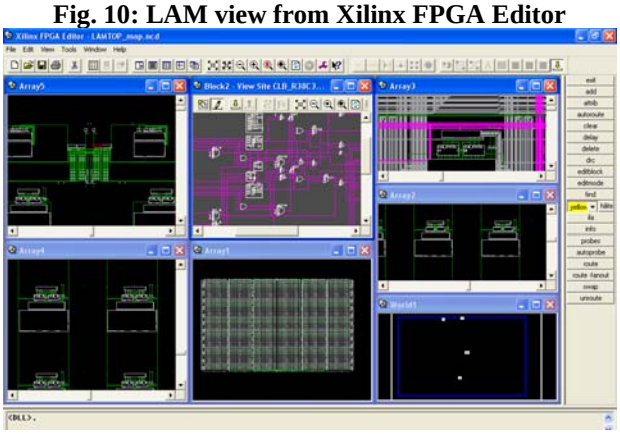

Fig. 11: LAM view From Xilinx FPGA Editor

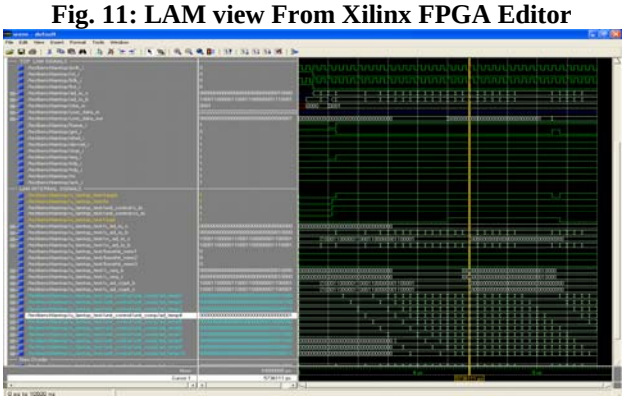

Fig. 12: LAM Simulation

Figure 12 illustrates a simulation of the LAM top signals which was realized for the verification of the LAM operation.

Up to now the implementation has been run in Register Transfer Level (RTL). Notice that the present implementation is for testing purpose only.

4 Conclusion

This paper introduced an overview of hardware cryptography based on PCI Bus and the noteworthy points of the digital PCI card and LAM system design. The design can be used for the implementation on digital communication systems such as on PCI Ethernet card. A real time secure

communication between two PCs which use telnet protocol through the LAM card could be realized.

The extension-redesign of the present implementation such as to support all of the versions of the PCI bus like PCI-X and PCI-Express constitute future scope for the authors. According to the above presentation the redesign of other protocols which use likewise rules does not indicate many changes.

References:

[1] Tom Shanley, Don Anderson, *"PCI SYSTEM ARCHITECTURE"* Fourth Edition, Addison Wesley, 1999.

[2] Peter J.Ashenden, *"The VHDL CookBook"*, first edition, Dept. Computer Science University of Adelaide South Australia, 1990.

[3] A. Menezes, P. van Oorschot, and S. Vanstone *"Handbook of Applied Cryptography"*, CRC Press, 1996.

[4] D. KAHN, *"The Codebreakers"*, Macmillan Publishing Company, New York, 1967.

[5] D. Stinson.*"Cryptography: Theory and Practice"*, 2nd Edition, Chapman and Hall/CRC, 2002.

[6] Kevin Burns *"TCP/IP Analysis and Troubleshooting Toolkit"*, Wiley Publishing 2003.

[7] Gilberd Held *"Ethernet Networks- Design. Implementation. Organization and Management"*, Fourth Edition, Wiley Publishing 2003.

[8] Andrew G. Blank *"TCP/IP Foundation"* SYBEX Inc 2004.

[9] Panagiotis Margaronis, Lambrinoudakis Kostantinos, Gritzalis Stefanos, AntonidakisEmmanouil, Rigakis Iraklis *"Digital Design of a Key Synchronization System on a FPGA for a network use"*, 6th WSEAS International Conference May, 2007

[10] Panagiotis Margaronis, Lambrinoudakis Kostantinos, Gritzalis Stefanos, AntonidakisEmmanouil *"Digital design of a Cryptographic card (LAM) embedded Smart Card Reader"*, 11th WSEAS International Conference July, 2007

[11] Panagiotis Margaronis, Dr. Lambrinoudakis Kostantinos, Dr Gritzalis Stefanos, Dr.Antonidakis Emmanouil, Chrysocheris Ilias *"Design and Implementation of a Cipher System (LAM) on a FPGA based on PCI architecture"*, 6th WSEAS International Conference May, 2007.