Digital Design of a Key Synchronization System on a FPGA for a network use

Panagiotis Margaronis[1], Dr. Lambrinoudakis Kostantinos[1], Dr Gritzalis Stefanos [1], Dr. Antonidakis Emmanouil[2], Rigakis Iraklis[2]

[1] University of Aegean, Department of Information and Communication System Engineering

[2] TEI of Crete, Department of Electronics

GREECE

Abstract

This paper presents the design of a programmable digital integrated circuitry for the use on a Personal Computer (PC) communication card for the synchronization of a key generator between two different destinations. The implementation is based on Peripheral Component Interconnectional (PCI) Architecture.

A Hardware PC cryptography card (which is called LAM) has been designed using a Field Programmable Gate Array (FPGA) chip in combination with the digital part (physical layer) of the PCI Bus. LAM card includes a key synchronization system.

The main objective of this paper is to provide the reader with a deep insight of the theory and design of a digital cryptographic circuitry, 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 synchronization circuitry will be presented.

Keywords

Security, Communication, Synchronization, Design, Architecture, Computer

1 Introduction

Recently, the need for a trustworthy computing system with high requirements 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 PCI Bus at the July of 1992 found to be convenient for these requirements.

In addition, cryptography nowadays has been chosen for many digital broadcasting applications and networks. The development of a synchronization unit between sender and receiver on a cipher system which uses symmetric algorithm such as there is not the need of sending any information concerning the key could provide more secure. LAM is aimed to be a new cryptographic system which can be used for many different electronic communication establishments and commercial conciliation by using a key synchronization system.

Moreover, the implementation of the key synchronization system on FPGAs offers a great deal of advantages such as system agility. The same FPGA chip can be reprogrammed to achieve scalable security through different versions of the same key generator. 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 circuitry on a FPGA chip which uses key synchronization has been attempted.

The basic idea is shown below (Fig. 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.

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.

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

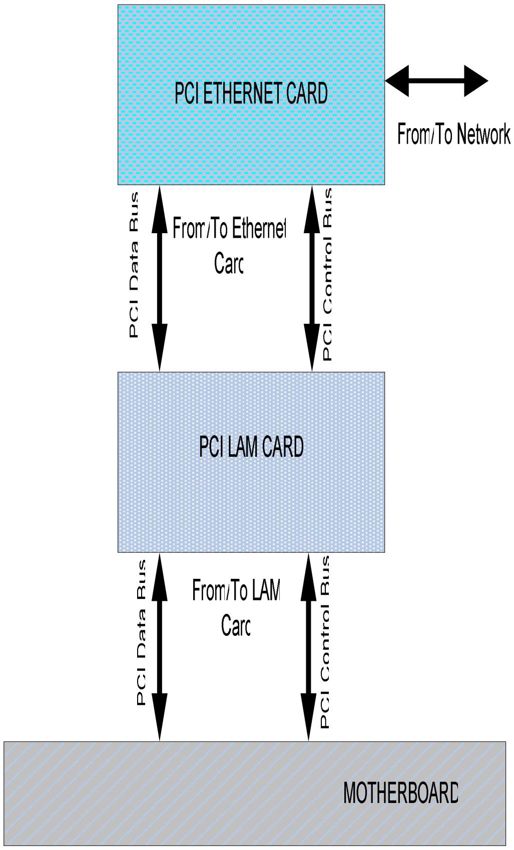

Fig. 1: LAM idea

At the following sections the LAM synchronization method will be represented. Moreover a short overview mention of the LAM architecture will be illustrated.

2 LAM Architecture

The LAM card (see Fig. 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 cipher the data. The LAM card will be as one “black box” for the PC software and hardware.

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 Fig. 2 below). It is very important LAM does not cipher the headers of protocols.

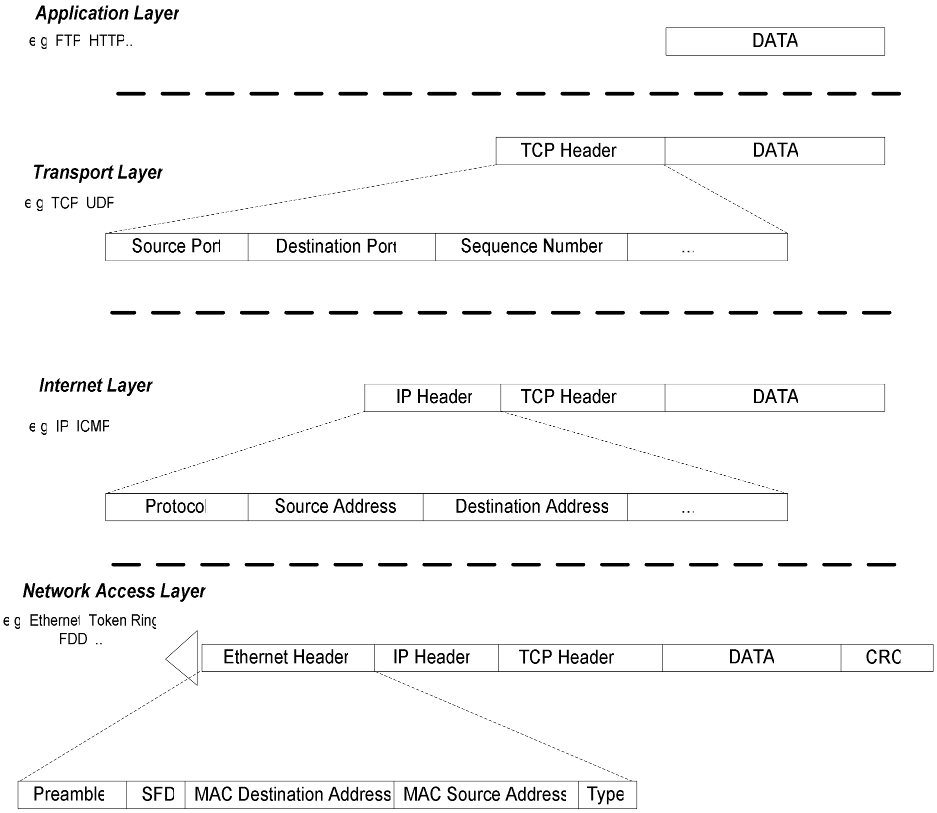

Fig. 2: TCP/IP Standard

LAM does not need driver development or PCI Controller implementation.

3 LAM Synchronization method

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.

For the synchronization LAM uses a combination of the existing TCP/IP Headers and an external counter. Figure 3 illustrates this idea. 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).

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.

Figure 4 illustrates the LAM synchronization unit. 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.

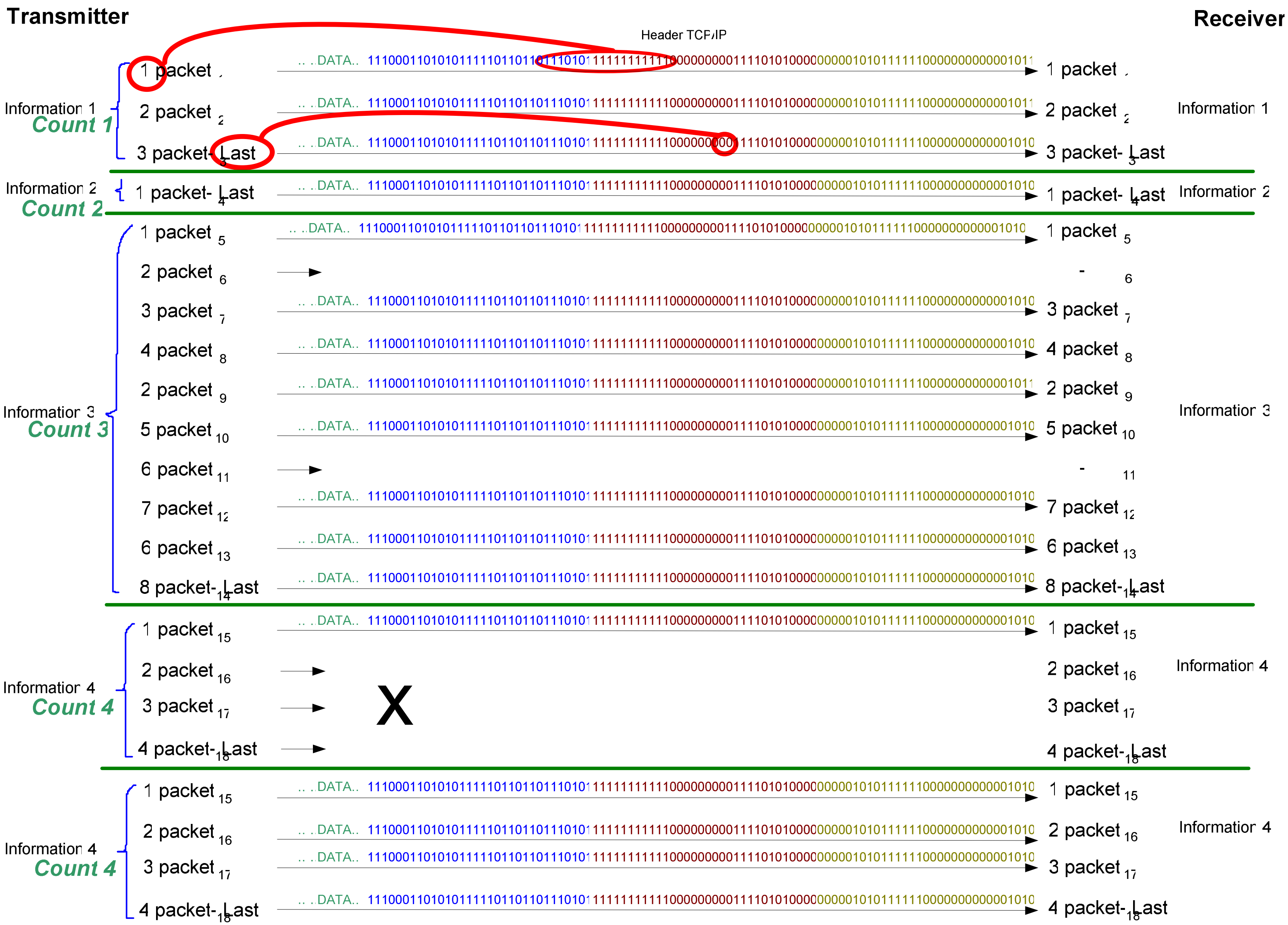

Fig. 3: LAM Synchronization

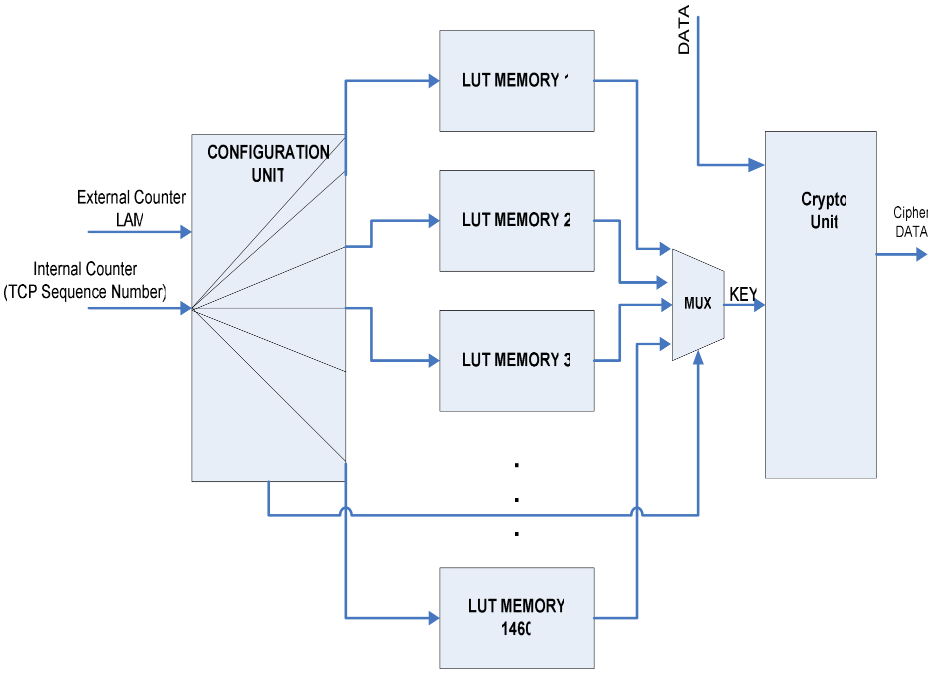

Fig. 4: LAM Synchronization unit

This method requires frequently upload of the memories. The cipher life time of the memories depends of the use of sending crypto messages but could be increased by parallel structure. The same FPGA chip can be reprogrammed to achieve scalable security through different versions of the same LUT key memories. The crypto-unit could host every symmetric cryptographic algorithm.

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 circuitry two times for more flexibility.

4 Conclusion

The above work introduces a new method for the synchronization of two different destinations which use the same key generator unit. Also an overview of hardware cryptography based on PCI Bus and the noteworthy points of the digital PCI card and LAM system design were illustrated.

The design can be used for the implementation on digital communication systems such as on a PCI Ethernet card.

The substitution of the LUT memories by pseudorandom key generators for each byte of data constitutes future work for the authors.

5 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.