# Digital design of a Cryptographic card (LAM) embedded Smart Card Reader

Panagiotis Margaronis[1], Dr. Lambrinoudakis Kostantinos[1], Dr Gritzalis Stefanos[1], Dr. Antonidakis Emmanouil[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 and implementation of a cryptographic card embedded smart card reader. The cryptographic card introduces a digital integrated encryption/decryption circuitry called LAM which is based on Peripheral Component Interconnect (PCI) Architecture for the use on a Personal Computer (PC) communication card. The implementation of the above hardware PC cryptography card has been designed using a Field Programmable Gate Array (FPGA) chip in combination with the digital part of 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 digital integrated encryption/decryption circuitry will be presented.

*Key-words:* Hardware, Security, Communication, Computer, Design, Architecture

## 1 Introduction

Nowadays, the need for a trustworthy computing system with high requirement which will be at the same time secure for many digital broadcasting applications and networks seems to be necessary.

In the present work a design of the PCI based LAM system embedded smart card reader on a FPGA chip has been attempted. LAM is aimed to be a new cryptographic system which can be used for many different electronic communication establishment and commercial conciliation.

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.

To increase the security, LAM card combines also a smart card reader for additional manipulations.

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.

A short mention of the LAM idea follows.

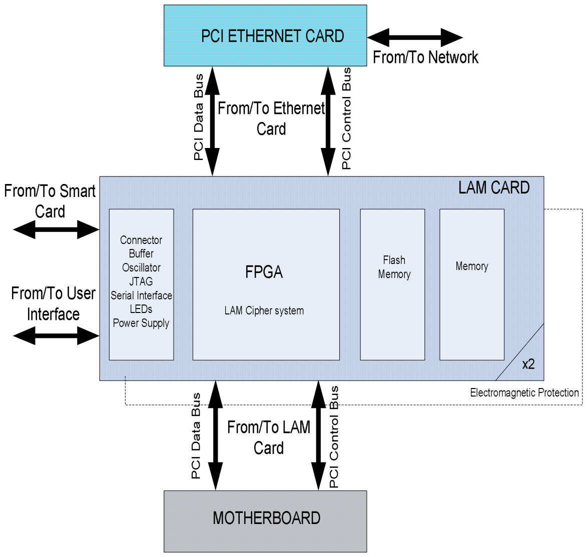

**Fig. 1: LAM idea**

The LAM card (see Figure 1) comprises 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. LAM uses symmetric cryptography in real time communication with a synchronization system which does not send any information as far as key is concerned [11].

The main contribution of the present paper is the description of a black box crypto-card 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 the PCI/ LAM card and the LAM smart card reader 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. The above bit rate was decided only for the testing of the card.

## 2 LAM Cipher System

As it was mentioned above, the LAM card is a crypto system which comprises 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. It is very important LAM does not cipher the headers of protocols

In the following sentences some of the LAM features are mentioned.

The LAM card has to run much more times than the PCI bus clock (at least 10 times more for the One Time Pad cipher method) so as in the same period having greater number of pulses, which means that will be in time for LAM algorithm calculation and will not affect the PCI Card

The LAM card will be as one "black box" for the PC software and hardware. Therefore LAM does not need driver development or PCI Controller implementation.

The LAM is comparing the source and the destination address thus 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.

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 (TCP Sequence number) and an external counter [12].

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. Moreover, LAM card is considered for electromagnetic protection (Multilayer printed circuit board with null voltage plane shield [10]).

Below is illustrated a general view of LAM architecture as well as and the components which are being included.(Figure 2). The basic units of the LAM are:

- Control unit, Comparator, Adder: Create synchronize and logic signals for the realization of the LAM idea.
- Configuration unit, Substitution memory: According to the number of internal (TCP Sequence number) and external counter, the configuration unit creates different address for each LUT memory (Substitution memory) such as to create different key for each byte of data respectively.
- Crypt unit: Up to now the crypt unit uses two different chipper algorithms: DES and One-Time-Pad. DES has been implemented with pipeline architecture.
- LFSR: Keep the keys secret even from the user of the LAM apparatus.
- LAM Smart Card reader: Realizes authorization of the LAM card user and creates different cipher teams

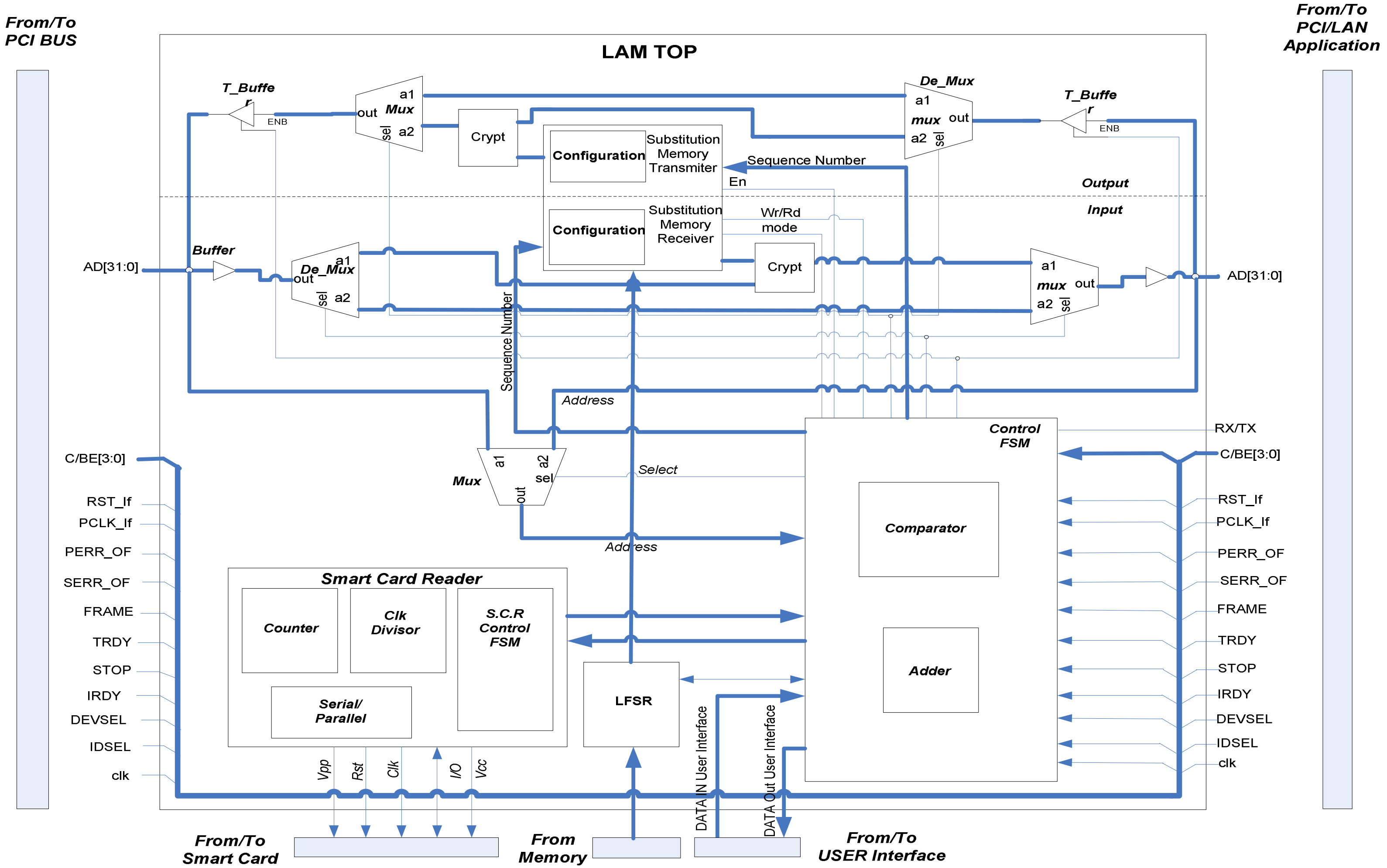

Fig. 2: LAM architecture

Up to now the implementation has been run in Register Transfer level (RTL) level

## 3 LAM Smart Card Reader

The LAM smart card reader uses specific elaborations that are described on the ISO 7816 standard (for T=0). The Finite State Machine (FSM) of the reader is illustrated bellow (Figure 3). The idea of the reader is to run only a constant number of manipulations in order to realize authorization of the LAM card user and to create different cipher teams. In addition keeps the keys secret even from the user of the LAM apparatus. As mentioned before according to the destination address of TCP/IP it can be created different cipher teams. Therefore each team has to use its own card in order to communicate. Different keys will be included to the smart card for each team respectively. Different teams can communicate to each other if first exchange their cards.

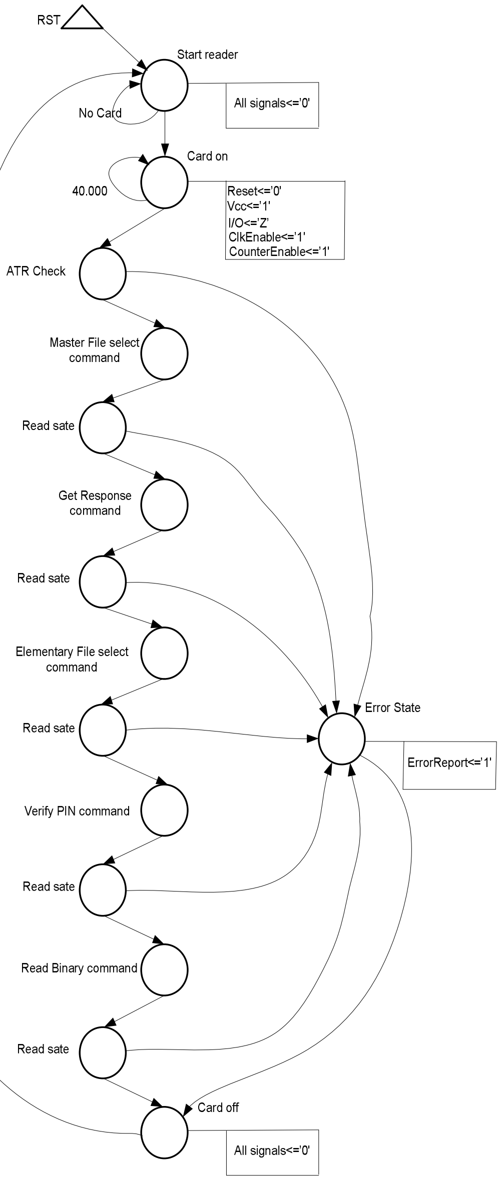

**Fig.3: LAM Smart Card Reader FSM**

According to the Figure 3, the LAM smart card reader communicates with the card and authorizes the user. For the authorization reads a key which is included in a specific file in the card and inform the control unit of LAM. If any information during the communication with the card is wrong then all the processes of LAM are remained in a null state. Notice that the control unit of LAM is aware of all the addresses and values that are included in the smart card. The LAM reader conveys the values which are included in specific addresses of the card to the control unit of LAM. The control unit compares these values and set the configuration unit in a specific operation mode downloading from an external memory the values for the substitution memory.

The substitution memory contains the keys that participate in the transaction. Therefore external memory contains the same keys. To ensure that the keys are unknown from the user (user can read the eternal memory but LAM Chip is lock) LAM uses a programmable Linear Feedback Shift Register (LFSR) which transform the values of the eternal memory according to the operation mode.

All the above manipulations are used only during the initialization of the LAM.

In addition external integrated circuits (buffer) for the suitable voltage and power levels which fed the smart card, the tolerance of the timing for the serial transmission (clock division) and final the errors possibility from line noise (start bit remain to'0' for a whole clock period) have been considered.

## 4 Conclusion

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

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] Wolfgang Rankl, Wolfgang Effing “Smart Card Handbook” third edition , Wiley Publishing 2003.

[10] Roger J. Sutton “Secure Comunication” John Willey & Sons, Ltd, 2002

[11] “Design and Implementation of a Cipher System (LAM) on a FPGA based on PCI architecture”, Panagiotis Margaronis, Lambrinoudakis Kostantinos, Gritzalis Stefanos, Antonidakis Emmanouil, Chrysocheris Ilias, ISBN: 978-960-8457-74-4, ISSN:1790-5117.

[12] “Digital Design of a Key Synchronization System on a FPGA for a network use”, Panagiotis Margaronis, Lambrinoudakis Kostantinos, Gritzalis Stefanos, Antonidakis Emmanouil, Rigakis Iraklis, ISBN: 978-960-8457-74-4, ISSN:1790-5117.