Thesis Overview:

AES development in FPGA

M. Liberatori
Universidad Nacional de La Plata, School of Informatics, April 28th, 2006

The importance of cryptography applied to security in electronic data transactions has acquired an essential relevance during the last years. Each day millions of users generate and interchange large volumes of information in various fields, such as financial and legal files, medical reports, bank services via Internet, telephone conversations, and e-commerce transactions. These and other examples of applications deserve a special treatment from the security point of view, not only in the transport of such information but also in its storage. In this sense, cryptography techniques. use is especially applicable.

Many have been the proposals made to establish implementation standards applicable to the two large branches of cryptography: symmetric key and public key. During many years, one of them -*Data Encryption Standard* (*DES*) . mastered the area of symmetric-key cryptography. Technological advances, as regards data processing speed, placed *DES* in a vulnerable position due to the size of its key. This triggered its replacement as standard.

The *National Institute of Standards and Technology* (*NIST*) created a new standard known as *Advanced Encryption Standard* (*AES*), with the objective of developing the *Federal Information Processing Standard* (*FIPS*) which specifies an encryption algorithm capable of protecting sensitive information to be used by the government of the United States. In October 2000, the *NIST* selected *Rijndael* as the algorithm proposed for the *AES*.

The algorithm has a round shape made up by three uniform and non-reversible transformations which assures broadcast over the total set of fixed rounds and optimal non-linearity properties. This thesis presents an 8-bit FPGA implementation of the 128-bit block and 128 bit-key AES cipher.

The aim of this thesis is focused on Rijndael.s encryption phase, particularly its development in *VHDL* hardware description language and its synthesis for the implementation over *FPGA,* minimizing the necessary hardware resources. Since the objectives of minimizing the area to be used and maximizing the processing speed are opposed, it is necessary to select a suitable architecture for the aim pursued.

It is worth mentioning that the FPGA development platform used is basic, designed for education applications in the fields of digital circuit design, and the synthesis objective device is of low volume, with a really low number of logic cells and embedded memory in comparison to newer platforms. This limitation also presented a challenge, if compared to other known implementations of the algorithm.

The thesis is developed in two main sections. The first is dedicated to highlighting the theoretical aspects relevant to the Rijndael.s cipher and is extended in three Chapters (2, 3, y 4). The second section deals with the topic of implementation in hardware, and the results (Chapter 5 to 8).

In the first section, the reader may find an introduction to Cryptography (Chapter 2), a summary of the basic algebraic principles supporting operations in finite fields (Chapter 3), and a complete description of the cipher specification (Chapter 4). The first two topics are briefly treated due to their extension and complexity. Basically, in the introduction to Cryptography, those Symmetric Key Cryptography aspects which are more closely related to the Rijndael Algorithm are highlighted. Mathematical principles are presented advancing from basic concepts to those more complex, without theorems tests but with enough useful reference for those readers who may be interested in the topic.

The section dedicated to the implementation in hardware begins with an elemental block design strategy (Chapter 5), which presents a complete analysis of the different transformations associated to the cipher and their possibilities of implementation. This chapter explains the used design strategy and methodology, highlighting the different known architecture options and supporting the selection made. Then, the cipher is described (Chapter 6) together with its performance (Chapter 7). Both chapters are complementary, the first presenting a detailed explanation of the final circuit, its various components and interconnections; and the second offers a detailed analysis of the performance taking as example the different results obtained by the simulations. Chapter 8 presents the results obtained, their applicability in terms of a de-encryption circuit implementation, and a comparison to other known implementations. This chapter focuses on the achievement of the searched objective: the design of a cipher AES-128 of minimum area and, thus, of low cost. Finally, the Thesis paper presents in Chapter 9 a global analysis and summary of the results. In addition, the entire developed VHDL code is available as Appendix.

Due to the initial design requirements limited to optimize resource consumption in terms of area, the architecture develops a single round which works iteratively requiring minimum resources as regards the area and offering a modest performance in relation to processing speed. The introduction of internal parallel processing into the architecture improves the speed parameters.

The proposed circuit, programmed in VHDL language, has as synthesis objective the family Flex 10K of Altera FGPA chips; in particular, the Altera Flex EPF10K20TC144-3 device, available in development board. The synthesis was made using the tool Altera MAX+PLUS II Version 7.21 Student Edition.

The analysis of the results and the comparison to other known architectures which use the devices of the Altera Family as synthesis objective allows locating this design as the most compact in terms of resources use. This characteristic opens the possibility of implementing it over inferior devices of this or other families, providing the presented design with effectiveness in terms of cost.

Horacio Villagarcía Wanza
hvw@info.unlp.edu.ar