International Journal of Research Studies in Science, Engineering and Technology [IJRSSET]
Volume 1, Issue 1, April 2014, PP 84-86

Review Paper on Field Programmable Gate Array in VHDL to Enhance Security

Anshul Anand
Asst Prof,
SBMEC, Rohtak

Shilpa
M.Tech Student ,
SBMEC, Rohtak

Abstract: *In this paper we presents an updated implementation of the Advanced Encryption Standard (AES) with some proposed technique, an optimized structure of the Cipher is presented and optimization of the algorithm's encrypt/ decrypt layer are discussed.*

Keyword: *Cryptography, AES, C-based design methodology*

1. INTRODUCTION

Cryptography (or cryptology; derived from Greek κρύπτω krýpto "hidden" and the verb "to write" or "to speak") is the practice and study of hiding information. In modern times, cryptography is considered a branch of both mathematics and computer science.

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography.

2. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES), a as cipher text. The cipher text message contains all the information Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a block cipher that can encrypt and decrypt digital information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits; this it implements the 128 bit standard on a Field-Programmable Gate Array (FPGA) using the VHDL, a hardware description language. In June 2003, the National Security Agency (NSA) announced that AES-128 may be used for classified information at the SECRET level and AES-192/256 for TOP SECRET level documents. Is an algorithm for performing encryption (and the reverse, decryption) which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt or decrypt. In the past, cryptography helped ensure secrecy in important communications, such as those of government covert operations, military leaders, and diplomats. Cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications (Wikipedia). Refer to Appendix A for definitions of key terms used throughout this document.

3. PROBLEM DEFINITION

With the evolution of digital designs, system designers are constantly looking for more efficient means and methods to develop source code and expedite time-to-market. Products, that takes too long to get to market, may fail in the field at great cost to both budget and company reputation. Even exploring whether a design is feasible can cost many months of effort. Today's rising design costs and increasing system complexity make demands for improved design solutions. Another important issue is verification. Already 70 percent of the development time is burdened with verification. Especially for large System-on-Chips verification is the most critical part of the design cycle. One way to cope with the mentioned challenges is abstraction. Designing at a more abstract level than the register transfer level facilitates thinking in algorithms rather than hardware. A well-suited programming language for describing systems at this level is C because it is close to hardware and well-known from both the hardware and the software designers. Many dialects of C were developed in the last years, which extend C with constructs for description of

concurrency, timing and hardware data types: SystemC [1,2], SpecC, Handel-C [3], Rosetta a. o. They all allow a is to refine a system step by step from a behavioral description using pure C down to a hardware description by adding only those implementation details, that are needed at a particular stage in the design flow. Thus, bugs concerning the algorithm may be found at early design stages where simulation is very fast and the turn-around time is short.

4. BRIEF OVERVIEW OF AES ALGORITHM

In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the US government. The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES selection process under the name "Rijndael", a portmanteau comprised of the names of the inventors.

AES has a fixed block size of 128 bits and a key

Number of rounds (Nr)	128-bit Data	192-bit Data	256-bit Data
128-bit Key	10	12	14
192-bit Key	12	12	14
256-bit Key	14	14	14

size of 128, 192 or 256 bits, whereas Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. AES operates on a 4×4 array of bytes, termed the state. For encryption, each round of AES (except the last round) consists of four stages.

a) SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table (known as S Box).

b) ShiftRows - a transposition step where each row of the state is shifted cyclically a certain number of steps

c) MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation.

d) AddRoundKey - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

AES algorithm comprises of various rounds depending on the key size and blck size,(Fig No.2).Out of all the rounds the Pre- round comprises only AddRoundKey whereas the final round omits the MixColumns stage.

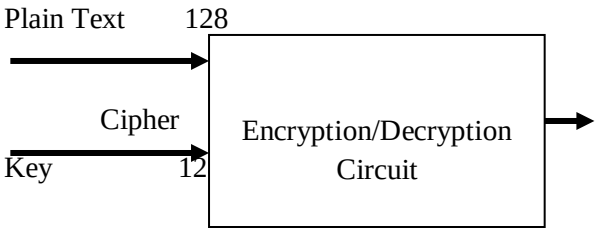

Figure 1: *An simple Block Diagram of AES-128.*

5. C-BASED DESIGN METHODOLOGY

Present design- and verification-techniques show in general a relatively strict separation between hardware and software. System architects sketch a specification and deliver this at hardware and software teams, who do their job with few interaction. The reason for that is the lack of methods, tools or uniform languages, that support the description of both software algorithms and hardware components. The co-simulation of hardware and software as well as gradual refinement of the design down to its components is strongly aggravated. In the last few years tools emerged, that are able to automatically translate algorithmic specification into a description on the register transfer level or even involve the synthesis step and generate a gate level net-list. Hence, the time-consuming and error-prone process of manual refinement is omitted. One example of such a tool is the Handel-C compiler from Celoxica[1]. It translates Handel-C code into either a RTL design with output formats VHDL and Verilog or a gate level EDIF net list. Handel-C is a language for implementing algorithms in hardware, architectural design space exploration, and hardware/software co-design. Based on ISO/ANSI-C, it has extensions required for hardware development. These include flexible data widths, parallel processing and communications between parallel elements. The language is designed around a simple timing model that makes it accessible to system architects and software engineers.

6. DESIGN FLOW

The tools used to implement the required functionality and their progression are shown in Figure 1. The SOPC-Builder from Altera was used to create a standard Nios 16 bit processor core with port input/outputs for communication with the external AES core. With Celoxica's DK1

design suite the AES algorithm as well as the interface for data input and output were programmed and verified. The VHDL output from the Celoxica Handel-C compiler was synthesized with Leonardo from Mentor Graphics. Same was done with the generated Nios core. At least the top level schematic including instantiations of the previously generated EDIF netlists and some periphery was drawn and implemented on a FPGA using Altera's Quartus Place and Route tools

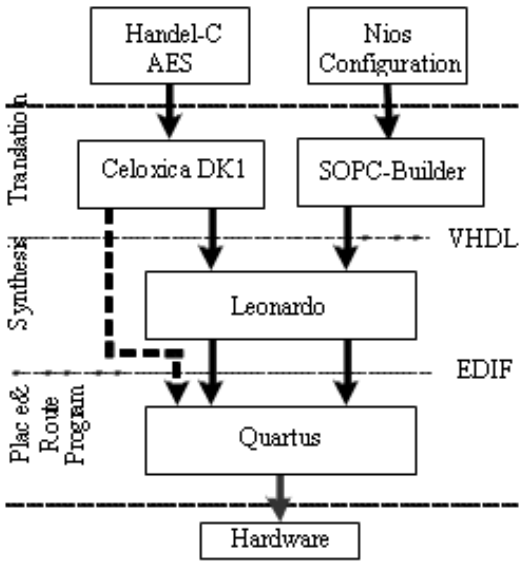

Figure 1: Toolflow

7. OBJECTIVE

The design goal of this paper was to create a demonstration of the AES for the end user and not for integration into a communication or data storage device; however this design could be modified to such ends. Since the goal was to create a demonstration, two human interface devices (HIDs), a regular PS2 keyboard and a 4x20 line LCD comprise the inputs and outputs to the system. A top level block diagram is shown in Figure 1 to illustrate

REFERENCES

[1] H. Muhr, "Einsatz von SystemC im Hardware/Software-Codesign",diploma thesis, http://agcad.ict.tuwien.ac.at/lehre/diplomarbeiten/muhr/muhr.pdf, 2000

[2] H. Muhr, G. Cadek, J. Notbauer and G. Niedrist, "Einsatz von C-basierten Methoden in der Systementwicklung", http://agcad.ict.tu-wien.ac.at/agcad/events/austrochip/muhr00.pdf, Austrochip 2000.

[3] Handel-C Language Reference Manual, Version 2.1, http://www.celoxica.com, 2001

[4] Federal Information Processing Standards Publication 197, Advanced Encryption Standard, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, November 26, 2001

[5] R.L. Rivest, "The RC5 Encryption Algorithm," Proceed ings of Fast Software Encryption - 2nd International Workshop, Leuven, Belgium, Springer Verlag LNCS 1008, pp. 86-96, 1995.

[6] J.-P. Kaps and C. Paar, "Fast DES Implementation for FPGAs and its Application to a Universal Key-search Machine," presented at Workshop in Selected Areas of Cryptography (SAC'98), Kingston, Ont., Aug. 1998. http://www.xess.com/manuals/xsa-3S-manual-v1_0.pdf. 2005

[7] H. Feistel, W.A. Notz, and J.L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Communi- cations," Proceedings of IEEE, Vol. 63, No. 11, pp. 1545-1554, 1975.

[8] C.M. Adams and S.E. Tavares, "Designing S-boxes for Ciphers Resistant to Differential Cryptanalysis," Pro- ceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, pp. 181-190, 15-16 Feb. 1993.

[9] Doran, R. W., "Variants on an Improved Carry Look- ahead Adder," IEEE Trans. on Computers, Vol. 37, No. 9, pp. 1110-1113, 1988.

[10] Wallace, C. S., "A Suggestion for a Fast Multiplier," IEEE Trans. on Computer, Vol. EC-13, pp.14-17, 1964.

[11] "Active-HDL Getting Started" available at website http://ece.gmu.edu/labs/Active_HDL.pdf (manual)

[12] "XSA-3S1000 FPGA Board v. 1.0 User Manual," Xess Cor poration, availabl website