ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

AES Implementation on Xtensa Processors

Ashlesha Karandikar (Menavlikar)

Tensilica, Cadence Design Systems, Inc. Pune, India

Abstract: This paper introduces implementation of AES on Tensilica's Xtensa processors. Advance Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). This paper illustrates the efficiency and performance of Tensilica Xtensa processors in accelerating encryption and decryption on Xilinx Kinex7 FPGA. Xtensa processors offer performance that competes with the hardware solutions at the same time provides the benefits of flexibility and programmability of software solutions.

Keywords: Xtensa, Processor, Configurable, Programmable, Cryptography, Encryption, Decryption, AES.

I. INTRODUCTION

Cryptography is a method of sending and receiving the data in such a form that only the person who is intended to use it can read, understand and process it. Advanced Encryption Standard is widely used cryptography standard and approved by NIST (U.S. Department of Commerce, National Institute of Standards and Technology).

This paper explains the process of designing an AES Engine, on the Xtensa processor developed by Tensilica, Cadence Design Systems, Inc. It illustrates the power of a configurable processor in accelerating the process of Encryption and Decryption. The Tensilica Instruction Extensions (TIE) language is used to design an optimized processor for AES. The focus of this paper is primarily on the AES implementation using 128-bit keys. However, the solution proposed here can be used to support AES encryption and decryption using 192- and 256-bit keys. Before going into the details of this Xtensa specific AES engine, take a moment to review and understand the AES standard.

II. ADVANCED ENCRYPTION STANDARD

AES algorithm is based on the block cipher developed by Dr. Joan Daemen and Dr. Vincent Rijmen. The AES standard has several advantages including simplicity, flexibility and security. The cipher structure can be implemented in parallelism with best possible performance optimization techniques.

The AES encryption is done by transforming the original message to block by block cipher. Each block is 128 bits in length and is conceptually stored and operated upon in a 4x4 byte state array. AES encryption is based on a secret 128-bit key to encrypt the plaintext block to ciphertext block. Prior to encryption the 128-bit key is expanded to 10 additional 128 bit keys.

AES encryption consists of basic four transformations that are described below.

- SubBytes – byte wise substitution transformation for each byte in the state array using a fixed table
- ShiftRows – transposition transformation which rearranges the placement of bytes within the state array
- MixColumns – permutation transformation, which treats each column of the state array as a polynomial and perform a Galois field multiplication with a fixed 4x4 matrix
- AddRoundKey –It performs byte wise Galois field addition with bytes of a key schedule

The flowchart for the AES encryption is given in Figure2.1. AES Decryption algorithm contains the inverse transformations of these encryption states.

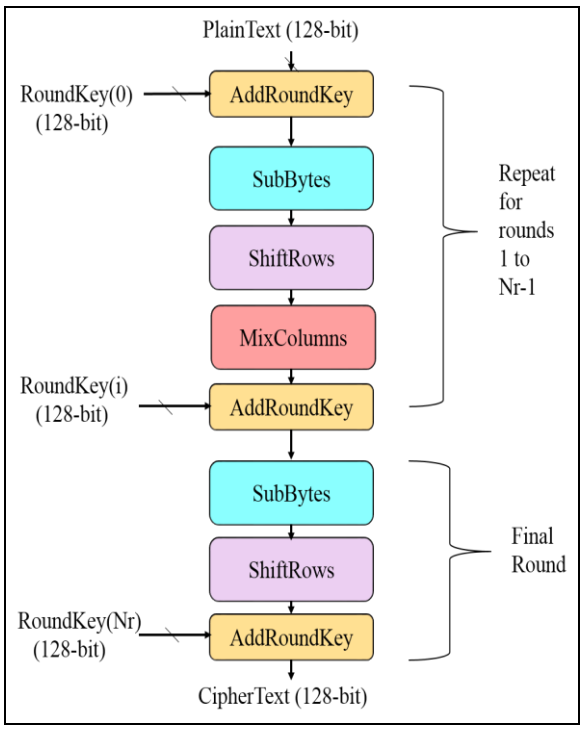

Figure 2-1 AES Encryption Flowchart

III. XTENSA CUSTOMIZABLE PROCESSORS

Xtensa processor architecture is extremely flexible by design. It provides widest range of customizable and programmable options. The unique features of Xtensa processors are -

- Configurability – The Xtensa Processor Generator create the pre verified customer specific processor with customized hardware and software toolsets.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

- Extensibility – It provides flexibility to customize instructions, registers and register files. The functional behavior of new data path can be specified using Tensilica Instruction Extention (TIE) methodology.

Xtensa processors can be used as 32-bit RISC controllers with minimal customization for memories and interfaces. By configuring and 6selecting pre-defined elements of the architecture and by inventing completely new instructions and hardware execution units, Xtensa processor can deliver performance levels that are orders of magnitude more efficient than other 32-bit processors. This this can be done in a fraction of the time it takes to develop and verify an RTL-based solution.

IV. AES WITH XTENSA PROCESSORS

The design of an application-specific processor for AES, which takes the advantage of the configurability and extensibility of the Xtensa processor is discussed here. A 128-bit data path is chosen for the processor. The processor is extended with a 128-bit AES register file and AES-specific instructions.

The Xtensa processor is extended with AES specific block implemented in TIE. The TIE language is used to describe processor extensions that are directly compiled into hardware and integrated into the Xtensa core. The encryption and decryption inputs are taken as interrupt requests to the processor.

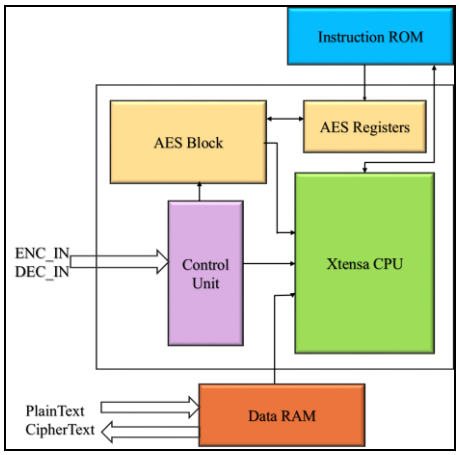

Figure 4-1 AES Block Diagram with Xtensa

The block diagram of AES specific Xtensa processor is shown in Figure 4.1. The Xtensa core is connected to instruction ROM and Data RAM memories through 128-bit data bus. The wide data paths inside and outside the processor ensure high throughput for the AES cipher. The instructions are fetched from the instruction ROM through a dedicated instruction bus. The data into and from the data RAM is connected through Xtensa local memory interface (XLMI). The input plain text data and the encrypted cipher text output are transferred to the external blocks of SOC through data RAM.

V. IMPLEMENTATION DETAILS AND ANALYSIS

The AES algorithm with Xtensa processors uses TIE language. TIE is used to design the customized processor in the most optimized form. The design is implemented with the highly integrated design environment called Xtensa Processor Development Toolkit. The Xtensa Processor Development Toolkit contains C/C++ source code editor, compiler tool chain, debugger and profiling Tools.

The TIE instructions are used to accelerate the AES transformation functionality. The hardware design challenge of adding instructions to a processor are greatly simplified by the TIE compiler. The TIE compiler takes a text description of the custom instruction and automatically interfaces the instruction to the Xtensa processor. These instructions look and act like any other core instruction. These instructions use the same format, interrupts, or exceptions which occur in a pipelined processor. The TIE compiler also extends the software development tools so that designers can quickly test and benchmark the code using the TIE instructions without having to write any assembly code.

The complete system is prototyped using Xilinx Kintex-7 FPGA KC705 evaluation kit along with the Xtensa Debug Module. The prototype board is connected through USB port of PC into the UART port of KC705.

The performance is observed with AES implemented in software C language along with Base Xtensa CPU versus customized AES Xtensa processor using TIE language.

The hardware profiling of both the implementations is done with the help of Xtensa Processor Development Toolkit. The number of instruction cycles required to encrypt and decrypt ten blocks of AES with C language are 10000 times more than that implemented with TIE as shown in the figure 5.1.

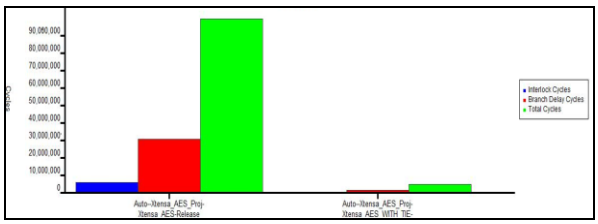

Figure 5-1 AES Performance comparison with SW and TIE Implementation

VI. CONCLUSION

The Xtensa processor offers significant advantages in almost any application. The Xtensa architecture combines a powerful general-purpose 32-bit instruction set design, with a unique configuration and extension process. These are used to handle general-purpose processing as well as the most compute intensive requirements in communication system design, including security algorithms.

In this paper we discussed the methods to customize Xtensa processor for the AES cipher transformations. An AES engine based on the Xtensa processor can provide performance which is comparable with the most hardware solutions, but retains the ease of design and flexibility found in software based solutions.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

REFERENCES

[1] FIPS197, The official Advance Encryption Standard, Federal Information Processing Standards Publications 197, Issued by NIST at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, PP 5-34
[2] Implementing the XTS-AES Standard on Xtensa Processors, Application Note, Tensilica Cadence Design Systems, Inc. pp 1-42
[3] Handbook on applied cryptography - Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Aug 1996, pp 223-271
[4] Applied cryptography, By Bruce Schneier, WILEY India edition, pp 1, 130
[5] Xtensa LX6 DataSheet , pp 1-13
[6] Xtensa Processor Developer's Toolkit DataSheet, pp 1-4 Xtensa processor documents available at http://ip.cadence.com/ipportfolio/tensilica-ip
[7] Xtensa Software Developer's Toolkit, User Guide , PP 1-43
[8] Xtensa Hardware User's Guide, pp 1-200
[9] Tensilica Instruction Language user's guide, pp 1-197
[10] Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter, Chih-Chung Lu, Shau-Yin Tseng, Year 2002, PP 277-282
[11] Parallel AES Encryption Engines for Many-Core Processor Arrays, Bin Liu, Baas, B.M. Year 2013, Volume 62, pp 536-547 High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion, Qiang Liu, Zhenyu Xu, Ye Yuan, October 2014, Published in IET Computers & Digital Techniques, pp.175 – 184
[12] 692-nW Advanced Encryption Standard (AES) on a 0.13- m CMOS Tim Good and Mohammed Benaissa,IEEE Transactions on Very Large Scale Integration Systems, Vol 18, No. 12, Dec 2010, pp 1753 – 1757
[13] Generic architecture and semiconductor intellectual property cores for advanced encryption standard cryptography M. McLoone and J.V. McCanny, Tech., Vol. 150, No. 4, July 2003, pp 239-244.
[14] AES Encryption Algorithm Based on the High Performance Computing of GPU, Fei Shao, Zinan Chang, Yi Zhang Department of Information Technology Jinling Institute of Technology Nanjing, China, 2010 Second International Conference on Communication Software and Networks, pp- 1,6
[15] Study of the AES Realization Method on the Reconfigurable Hardware, 2013 International Conference on Computer Sciences and Applications, Yuwen Zhu, Hongqi Zhang, Yibao Bao, pp 72-76