FPGA Implementation of AES-based Crypto Processor

Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen
Department of Information Technology
University of Turku
Turku, finalnd
{hasanw, masdan, masebr, juplos, hanten}@utu.fi

***Abstract*—Increased demand for data security is an undeniable fact. Towards achieving higher security, cryptographic algorithms play an important role in the protection of data from unapproved usage. In this paper, we present a crypto processor using Advanced Encryption Standard (AES). The AES is integrated with a 32-bit general purpose 5-stage pipelined MIPS processor. The integrated AES module is a fully pipelined module which follows inner round and outer round pipeline design. The results show that the presented pipeline version of the AES algorithm along with MIPS processor outperforms traditional methods. At the operating frequency of 553 MHz, the proposed design can achieve the throughput of 58 Gbps, the latency of 240 ns, and the minimum power consumption of 76 mw.**

Keywords—Cryptographic; Field Programmable Gate Array; AES pipeline; Throughput; Pipelining.

I. INTRODUCTION

The common goal of cryptographic algorithms is providing security. From last several years, Data Encryption Standard (DES) had been used as a cryptographic algorithm [1]. Due to the short key length of DES it is replaced by the Rijndael algorithm which has became as a standard in the cryptography domain, known as Advanced Encryption Standard (AES) [2]. Encryption is a transformation technique to change one form of data called plain text to an unreadable form of data, called cipher text. The hardware implementation of crypto algorithms, associated with keys, is by nature very secure and cannot be easily modified from outside [3]. After the Rijndael algorithm has become a standard encryption algorithm, many hardware implementations based on FPGA and ASIC have been proposed [3-9]. ASIC provides low power design but the design time and time to market is very high. Moreover, it has lack of flexibility for changing design parameters. FPGA provides the best platform for the hardware implementation of cryptographic algorithms because of its re-programmable capability and reconfigurability. This paper proposes an approach to combine general purpose processor with crypto co-processor. In this work, the general purpose processor is a MIPS-32 [10] which has five pipeline stages. We used AES-128 as a crypto algorithm acting as a crypto processor. We propose a system which is the integration of MIPS and AES Crypto processor, called MAC. MAC has the ability to run at different frequencies which gives flexibility and choice to end user to adjust the system with the throughput, latency, and power requirements.

Our design is implemented in such a way that crypto instructions do not block the instruction fetch cycle of the processor even though the crypto co-processor is running at the same time. By default, each instruction is fetched from the instruction memory unit and completed all its cycles on the MIPS processor if the instruction is designed for the processor. However, if the fetch instruction is not a MIPS instruction, it will be sent to the crypto co-processor in the next clock cycle after the decode stage. We incorporate crypto co-processor with MIPS and make this integration in a way that crypto co-processor runs by the MIPS without disturbing pipeline stages. The main contributions of this paper are follows:

- The pipeline version of AES is implemented, obtaining high throughput, low latency, and low power consumption.
- The integration of AES and MIPS is presented which has the ability to run at different frequencies.
- The implemented AES acts as a crypto processor controlled by MIPS instruction while it does not disturb the pipeline stages of the MIPS processor.

This paper is organized as follows: Section II presents the FPGA implementation of AES pipelined architecture. Section III describes MIPS based AES Crypto. In Section IV experimental results are discussed, while the conclusion is given in the last section.

II. FPGA IMPLEMENTATION OF AES PIPELINED ARCHITECTURE

The efficient implementation of the AES algorithm on FPGA is being under discussion from last several years in terms of throughput, minimum area requirement, and high speed [11-16]. The main reason to choose FPGA for the implementation of cryptographic algorithms is that it allows changing design with no additional time cost while the design cycle is also very short. An FPGA based AES implementation is presented in [3-14]. Fig. 1 shows the implementation technique of pipelined AES in which several procedures can

be run concurrently. Pipelining in the AES is performed for a high throughput while speed is increased by handling multiple rounds of AES concurrently. However, pipeline technique tends to consume a lot of area [15-21].

III. MIPS BASED AES CRYPTO (MAC)

In our proposed design, shown in Fig. 2, we integrate the crypto co-processor based on the AES algorithm with the MIPS processor in such a way that AES is executed as the crypto co-processor. This method is called MAC (MIPS-AES Crypto). The hardware implementation using FPGA provides significant performance gains compared to the software implementation using general purpose processor (microprocessor) in terms of parallel processing, pipelining, word size, and speed [22]. Throughput up to several Gbps can be easily achieved by using FPGA. The crypto algorithm agility is also possible using FPGA [9]. In our design if the fetched instruction is a crypto instruction it will be sent to the pipeline stages of crypto co-processor for execution through the decode stage without affecting the pipeline stages of the MIPS processor. There are five different stages named IF, ID, EX, MEM, and WB. If the fetch instruction is a MIPS instruction it runs on MIPS and completes all its cycle on the pipeline stages. However, if the fetched instruction is a crypto instruction it is forwarded to the crypto co-processor from the decode stage as shown in Fig. 2. One of the contributions of this paper is to extend the general purpose processor with the AES crypto co-processor. If the instruction fetched from the instruction memory is a MIPS instruction, it will run on the pipeline stages of the MIPS processor (decode, execute, and write back). However, if the instruction is crypto-instruction, it will run on the crypto co-processor. The crypto-instruction fetched from instruction memory is decoded during the decode stages and sent to crypto co-processor. The proposed design is also flexible to run on different frequencies to achieve different throughputs and power consumptions.

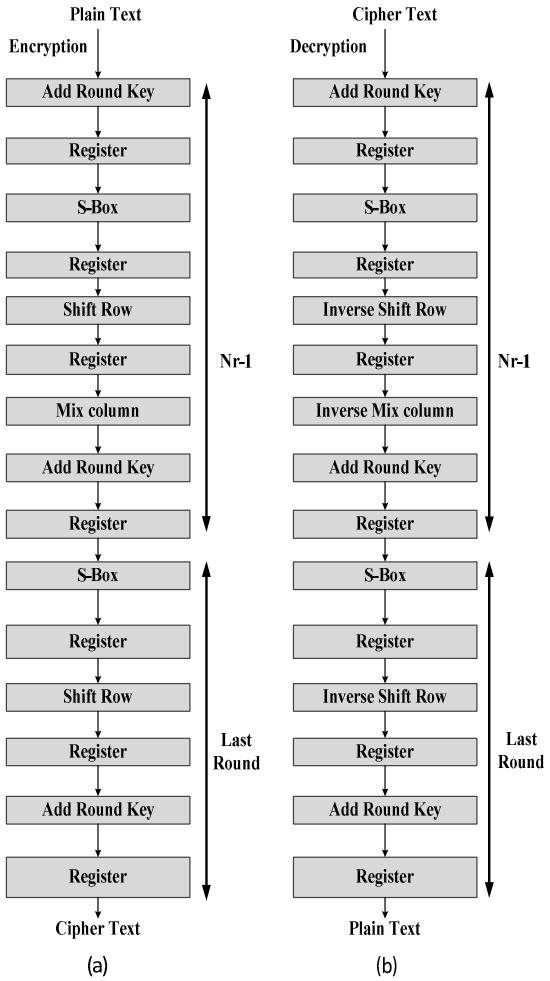

Fig. 1. (a) Pipelined AES Encryption (b) AES Decryption.

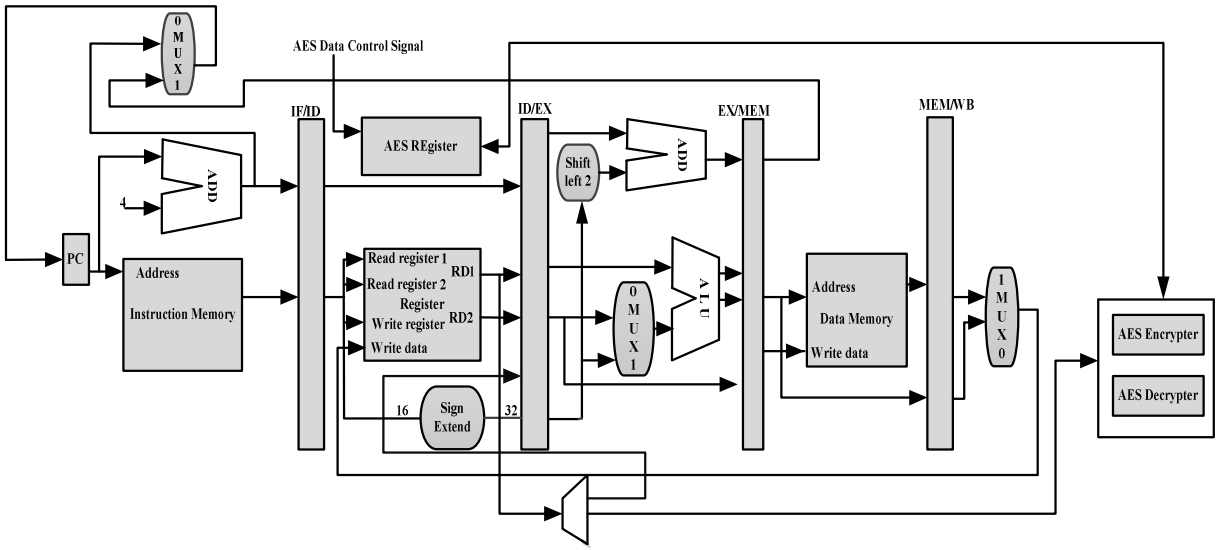

Fig. 2. Crypto processor with MIPS.

IV. EXPERIMENTAL RESULT

In order to implement the design on FPGA, we have used Xilinx ISE 14.4. For power measurement, we have used Xilinx XPower tool and the design is implemented on Virtex 6 ML605. Table I shows hardware and timing statistics. MAC runs on different frequencies, throughput has been measured for different frequencies which have been illustrated in Fig. 3. The best throughput is 58 Gbps obtained at the maximum frequency of 553 MHz. The minimum latency of the design is 240 ns as shown in Fig. 4. As depicted in Fig. 5 the minimum power consumption is 76 mw observed at 50 MHz and maximum power consumption is 813 mw observed at 553 MHz. The hardware resource utilizations for MIPS and AES are shown in Fig. 6. According to this figure, the occupied area for AES and MIPS is 662 and 1885, respectively.

Table I . Hardware timing and statistics.

Resources	Usage
I/O pins	418
Block RAMs	204
Slices Register	2547
Critical Path Delay	1.808ns
Frequency	553 MHz
Throughput	58 Gbps
Register	1015
Multiplexer	176
Minimum input required time	3.89ns
Maximum output required time	0.77ns

We have compared the proposed approach with other implementations reported in the literature in terms of power consumption and throughput. Results are shown in Fig. 7 and Fig. 8. The power consumed by the method presented in [21] is 1.313 watt at the frequency of 210 MHz. The power consumption of a methods proposed in [3] is 1.029 and 2.083

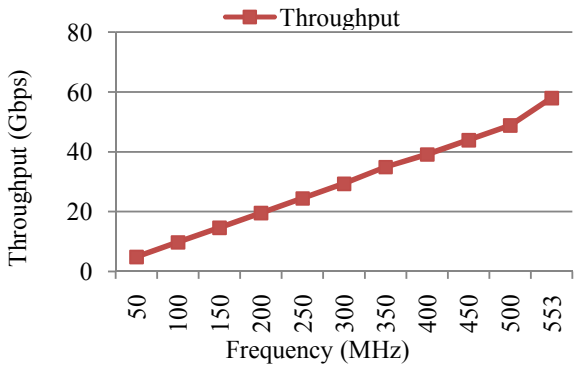

Fig. 3. Effect on throughput for different frequencies.

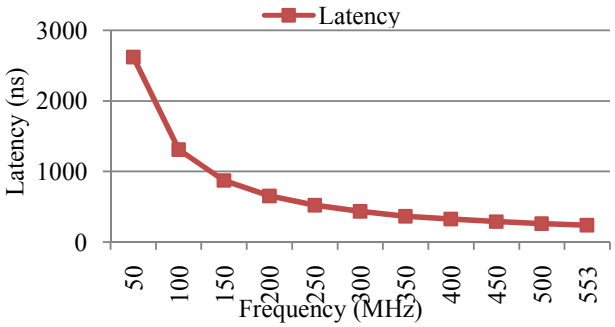

Fig. 4. Effect on latency for different frequencies.

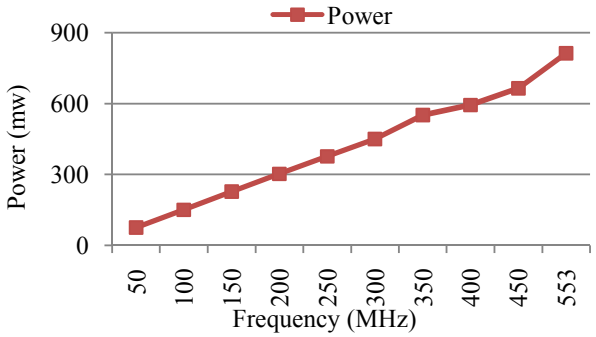

Fig. 5. Effect on power for different frequencies.

watt at the frequency of 142.8 and 125.3 MHz, respectively. The power consumption of MAC is 0.813 watt at the maximum operating frequency of 553 MHz. Similarly, the maximum throughput of MAC is 58 Gbps which is higher than the throughput reported in each of approaches in [3] and [21]. Similarly, power consumption of MAC is lower than the design presented in [3] and [21]. Table II summarize all the comparisons and results.

Table II. Result comparison.

The proposed method	Frequency (MHz)	Throughput (Gbps)	Power (W)
[21]	210	0.546	1.313
[3] approach 1	142.8	18.8	1.029
[3] approach 2	125.3	16.09	2.083
Ours	553	58	0.813

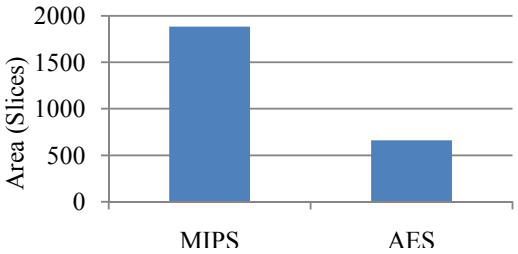

Fig. 6. Area consumption of MIPS and AES.

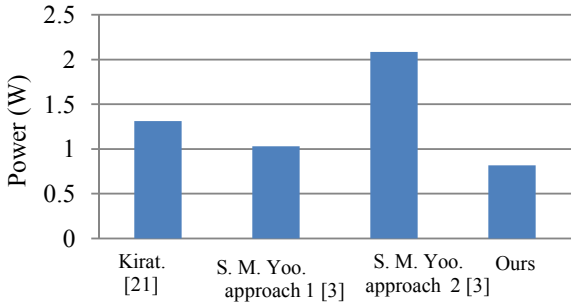

Fig. 7. Power comparison.

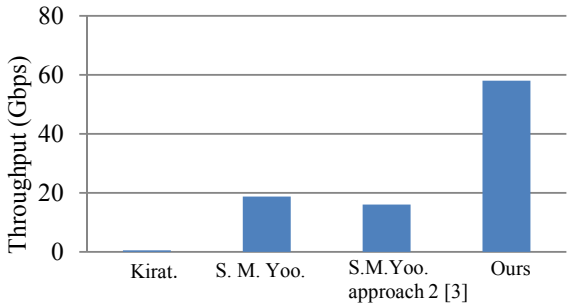

Fig. 8. Throughput comparison.

V. CONCLUSION

Encryption algorithm is being used by military and government over a last couple of decades for secure communication. The main purpose of encryption is to hide data from unauthorized usage. In this paper, we purposed a method to employ the crypto processor run in an integration with a General Purpose Processor. In this direction, we have presented a pipeline version of AES algorithm that can encrypt data. The high performance and high configurability of the combination of General Purpose Processor and crypto processor makes it pertinent to various security applications. The proposed design, MAC, has the ability to run on different frequencies and provide flexibility to user adjusting the frequency to meet the throughput, latency, and power consumption requirements.

REFERENCES

[1] B. Schneier, Applied Cryptography, Wiley, New York, 1996.

[2] National Institute of Standard and Technology (USA, Advanced Encryption Standard). FIPS 197, Available at, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, September 1999.

[3] S. M. Yoo et. al., "An AES crypto chip using a high-speed parallel pipelined architecture," Elsevier, Microprocessor and Microsystem, vol. 29, pp. 317-236, January 2005.

[4] P. Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware," Master's thesis, George Mason University, March 2002.

[5] H. Kuo and I. Verbauwhede, "Architectural optimization for 1.82 Gbits/sec VSLI implementation of the AES Rijindael algorithm," in processdings of Cryptographic Hardware and embedded systems (CHES'01), France, vol. 2162, pp. 51-64, Springer-Verlag, May 2001.

[6] N. Sklavos and O. Koufopavlou, "Architecture and VLSI implementation of the AES-proposal Rijndael," IEEE Trans. Computers, vol. 51, pp. 1454-1459, 2002.

[7] P. R Schaumont et. al., "Unlocking the design secrets of a 2.29 Gb/s Rijndael processor," in processdings of ACM Conference on Design Automation (DAC 2002), USA, pp. 634-639, 2002.

[8] S. Morioko and A. Satoh, "A 10 Gbps full-AES crypto design with twisted BSS s-box architecture," in processdings of IEEE International Conference on Computer Design VLSI in Computers and Processors, Germany, pp. 98-103, September 2002.

[9] U. Mayer et. al., "Evaluation of different Rijndael implementaion for high end servers," in processdings of IEEE International Symposium on Circuits and Systems ,USA, vol. 2, pp. 348-351, May 2002.

[10] MIPS 32 Architecture for programmers, vol . I, "Introduction to MIPS Architecture," Available at http://www.mips.com/products/product-materials/processor/mips-architecture/2008.

[11] V. Fischer, M. Drutarovsky, P. Chodowiec and F. Gramain, "Inv mixcolumn decomposition and multilevel resource sharing in AES implementations," IEEE trans. VLSI syst, vol. 13, pp. 989-992, 2005.

[12] A. C Zigiotto and R. d'Amore, "A low-cost FPGA implementation of the advanced encryption standards algorithm," in processdings of 15th International International Symposium on Integrated Circuits and System Design, Brazil, pp. 191-196, September 2002.

[13] A. Satoch, S. Morioka, K. Takano and S. Munetoh, "A compact Rijndal hardware architecture with s-box optimization," in processdings of 7th International Conference on Theory and Application of Cryptology and Information Security, Australia, vol. 2, pp. 239-254, Springer-Verlag, 2001.

[14] T. Good and M. Benaissa. "AES FPGA from fastest to smallest," in processdings of 7th International Workshop on Cryptographic Hardware and Embedded System, United Kingdom, vol. 3659, pp. 427-440, Springer-Verlag, September 2005.

[15] S. McMillan and C. Patterson, "JBits implementation of the advanced encryption standard(Rijndael)," in processdings of 11th International Conference on Filed–Programmable Logic and Applications, United Kingdom, vol. 2147, pp. 162-171, Springer-Verlag, August 2001.

[16] Y. Zhang and X. Wang, "Pipelined implementation of AES encryption based on FPGA," in processdings of IEEE International Conference on Information theory and Information Security, pp. 170-173, December 2010.

[17] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989. I. Verbauwhede, P. Schaumont and H. kuo, "Design and performance testing of a 2.29-Gb /s rijndael processor," IEEE J. Solid State Circuits, vol. 38, pp. 569-572, 2003.

[18] N. C Iyer, P. V Anandmohan , D. V Poornaiah and V. D Kulkarni, "High through put, low cost, fully pipelined architecture for AES crypto chip," in processdings of Annual IEEE India Conference, pp. 1-6, September 2006.

[19] A. Dandalis et. al. , "A comparative study of performance of AES candidates using FPGA's," in proce. of The third Advanced Encryption Standard (AES3) Candidate Conference,pp 124 -140, April 2000.

[20] G.P Saggese, A. Mazzro, N. Mazzocca and A. Strollo. "An FPGA-based performance analysis of the unrolling , tiling, and pipelining of the AES algorithm," In proceeding of 13th International Conference on Field-Programmable Logic and Applications, Portugal, vol. 2778 of LNCS, pp. 292-302, Springer-Verlag, September 2003.

[21] K. Pal Singh, S. Parmar, "Low Power Encrypted MIPS Processor Based on AES Algorithm," Journal of Global Research in Computer Science, vol. 3 No. 4, pp. 63-67, April 2012.

[22] L. Gaspar et. al., "Cryptographic extension for soft general purpose processors with secure key management," in processdings of 21st IEEE International conference on Field Programmable Logic and Applications, Greece, pp. 500-505, September 2011.

[23] J. Carabaño et. al., "An Exploration of Heterogeneous Systems," in Proceedings of 8th IEEE 8th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), pp. 1-7, July 2013, Germany.