Middle-East Journal of Scientific Research 24 (1): 128-133, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.01.228799

Design and Implementation of Low Power AES Based Crypto-Processor

[1]K. Kalaiselvi and [2]H. Mangalam

[1]Department of ECE, Hindusthan College of Engineering and Technology, Coimbatore, India
[2]Department of ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India

Abstract: Advanced Encryption Standard (AES) encryption algorithm has become a widely recognized standard in cryptographic applications. AES is a symmetric encryption algorithm which requires VLSI implementation to achieve high throughput with low power. In this paper, ASIC based AES crypto-processor is designed and implemented using 130 nm CMOS technology. Stream cipher of 8-bit is considered for crypto-processor with 128-bit keys and a throughput of 0.05 Gbit/S that incorporates parallel pipelines. These parallel pipelines are useful in reducing the operating frequency so that the power consumption is significantly reduced. Simulation and implementation results show that the proposed crypto-processor achieves high throughput, lower power dissipation and smaller chip area while comparing with other 8-bit stream implementations.

Key words: AES encryption · Crypto-processor · CMOS technology · Pipelining · Power dissipation

INTRODUCTION

Encryption has become a vital part in military applications, government agencies for secret information exchange. Due to the rapid advances in computer networks and communication, encryption needs to be applied for civilian systems to protect the information so that safety communication can be assured. In view of this information protection, there is a widespread interest in designing cryptographic systems. Though many algorithms are available in the literature for performing data encryption, Advance Encryption Standard (AES) Algorithm is the most preferred choice in wireless communication and wireless network related applications [1].

Crypto-processors are developed for encryption applications using very large scale integration (VLSI) technology so that the chip area, power consumption and performance can be optimized. VLSI implementations are either based on field programmable gate array (FPGA) technology or Application specific integrated circuit (ASIC) technology depending on the application. The important reason for opting VLSI technology is the hardware implementation of the crypto-processor. Hardware implementation of the cryptographic algorithms is more physically secure and cannot be attacked as easily by cryptanalysts [2].

Hardware encryption uses a general purpose FPGA chip or special purpose chip for encryption, while software encryption uses a general purpose computer to execute encryption as a program. Hardware encryption has the flexibility of changing the components and optimizing the system performance which is not possible in software encryption [3]. Hardware implementations provide significantly higher processing speed than software implementations. Hardware implementations can be designed to achieve certain requirements such as low power consumption, low area and high data rate. At the cost of increased area and power consumption, higher throughputs may be accomplished by using a loop-unrolled hardware structure. On the other hand, reducing the depth of the data path can decrease the size while compromising the throughput [4]. AES algorithm is a computationally intensive application which requires data-level parallelism (DLP) for performing encryption operations. Each round of the AES algorithm receives a new round key from the key expansion algorithm. The stream of data used in the encryption repeated over specific time duration. Decryption is performed by applying of the inverse transformations of the round functions [5]. Some of the parallelism types are instruction-level parallelism (ILP), thread-level parallelism (TLP) and DLP. The most popular form of parallelism available in many applications is DLP [6]. Exploiting DLP

Corresponding Authro: K. Kalaiselvi, Department of ECE, Hindusthan College of Engineering and Technology, Coimbatore, India.

existed in AES algorithm is the key to achieving high throughput by executing multiple, independent operations concurrently.

In this paper, ASIC based AES crypto-processor is designed and implemented using 130 nm CMOS technology. Stream cipher of 8-bit is considered for crypto-processor with 128-bit keys and a throughput of 0.05 Gbit/s that incorporates parallel pipelines. These parallel pipelines are useful in reducing the operating frequency so that the power consumption is significantly reduced. This paper is organized into five sections including this introductory section. Section 2 discusses some related work to our approach and other VLSI based cryptographic processors. The proposed crypto-processor is described in detail with architecture in Section 3. Section 4 presents the implementation results and performance comparison between the proposed approach and some related works. Finally, Section 5 concludes this paper and gives some directions for future work.

Related Work: In the literature, various approaches have been proposed for the VLSI implementation of cryptographic applications. One of the most widely used cryptographic algorithms is Rijndael algorithm. It operates on fixed size block ciphers rather than on a stream ciphers, so it is also known as block cipher algorithm. The key used in both the encryption and decryption modes is the same, which is the concept of private-key cryptosystems. Block ciphers are symmetric-key encryption algorithms that transform a fixed length plaintext into a fixed length cipher text using a single private key. The decryption is similar to the encryption except that the inverse transformations are applied in a reverse order using the same key used in the encryption. McLoone *et al.* discussed high performance single-chip FPGA implementations of the Rijndael [7]. These designs were implemented on the Virtex-E FPGA family of devices. Their encryptor core was capable of supporting different key sizes and was 21 times faster than the then known software implementation and was claimed as the fastest fully pipelined single chip FPGA Rijndael encryptor core.

Wu *et al*., (2001) have designed CryptoManiac, which is a cryptographic coprocessor design based on Very Long Instruction Word (VLIW) so that four instruction per cycle can be executed [8]. In addition, bitwise logical and arithmetic instructions are combined to execute in a single instruction cycle. Oliva *et al*., (2003) presented a programmable cryptonite processor which is specifically designed to implement crypto algorithms [9]. It comprises of VLIW architecture with two 64-bit datapaths, that can run at clock rate 400 MHz and providing a throughput of 700 Mb/s. Kim *et al*. [10] presented a fully integrated and synthesizable cipher core supporting the AES. The core which designed and fabricated was key scheduler, encipher and decipher. The core operating frequency was 465 MHz and was able to deliver a throughput upto 2.3 Gb/s.

The hardware implementation of AES algorithm with key expansion capability has been proposed which utilized pipelined design for implementation [11]. It provides a throughput rate of 2.38 Gb/s with pipelining while 128-bit keys are used. A multiple Gb/s rate AES coprocessor has been designed and implemented, which has the programming capability with Gigabit throughput for cryptographic applications [12]. Another crypto coprocessor has been presented which can perform AES-128 encryption and decryption in both feedback and nonfeedback modes of operation [13]. It achieved the maximum throughput of 3.84 Gb/s at the frequency 330 MHz. This crypto coprocessor was programmed using the memory mapped interface of an embedded CPU core and is tested using a LEON 32-bit SPARC V8 processor. Kuo and Verbauwhede described an ASIC implementation of the AES algorithm, which gives a maximum throughput of around 1.82 Gb/s at 100 MHz [14]. They described different pipelined implementations of the AES algorithm with area and speed optimizations that lead to a low area and high throughput AES encryption processor.

Proposed Crypto-Processor Design: The literature review motivates us to design a new crypto-processor that improves the system performance with less power consumption. Power efficient implementation of our previous work has been utilized [15]. In that work, a low power implementation of AES algorithm was achieved using key expansion approach. The designed architecture also reduced the critical path delay for improved performance. It supports both encryption and decryption with a throughput of 0.05Gbps. In this work, ASIC based AES crypto-processor is designed using the low power AES unit and implemented using 130 nm CMOS technology.

The proposed crypto-processor includes some general purpose processor components so that the single processor can be used for entire processing. Figure 1 depicts the components of the ASIC based crypto-processor design. It comprises of the general purpose processing units such as instruction register, queue, control unit and address generation unit.

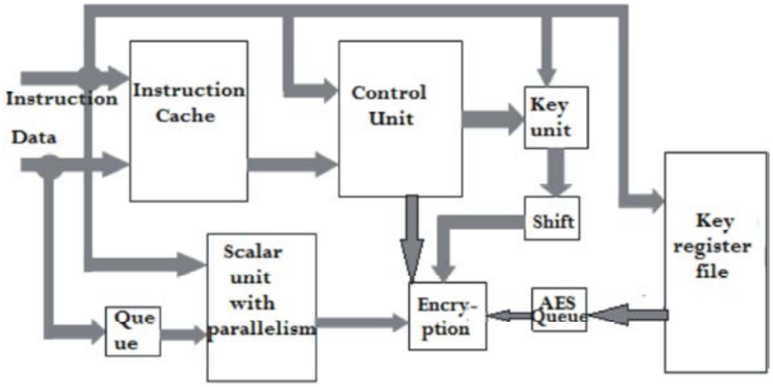

Fig. 1: Block diagram of proposed crypto-processor

The AES queue deals with the encryption key and key register files. The low power AES encryption is performed by the encryption unit. In this encryption unit, the key expansion unit is incorporated. In order to support the different words flexibility of the Key expansion unit, the flexible Key expansion is designed based on a simple circuit on the chip, which refer the Key expansion algorithm. Stream cipher of 8-bit is considered for crypto-processor with 128-bit keys and a throughput of 0.05 Gbit/s that incorporates parallel pipelines. These parallel pipelines are useful in reducing the operating frequency so that the power consumption is significantly reduced.

RESULTS AND DISCUSSION

The functional verification of the proposed design can be done with any commercial software packages. Once the functional verification is completed, the design is ready for physical implementation. The first step in physical implementation is to convert the hardware description language (HDL) model to register transfer level (RTL) code so that the design can be synthesized. In this work, the RTL model is synthesized using Design Compiler (DC) from Synopsys which is an industry standard EDA tool. In DC compiler, the RTL model is converted into gate level netlist. The gate level netlist should be able to meet area, timing and power requirements. Optimization constraints include operating frequency (clock period), input and output delays at the IOs. In this implementation, TSMC 130 nanometer target technology is adopted for better performance. Figure 2 shows the schematic, which was generated after synthesizing the RTL code.

Table 1 provides the power report obtained from the design compiler unit. The total dynamic power is 49.49 mW.

Table 1: Power report of crypto-processor architecture

Power Specific Information	Values
Global operating voltage	1.2 V
Cell internal power	32.17mW
Net switching power	17.32mW
Cell leakage power	0.11mW
Total Dynamic power	49.49mW

Figure 3 shows the design of the floor-planned view. In the perimeter, 130 I/O cells are placed along with the cell utilization of 80% with flip chip and double back. The I/O cells and core area of the power supply are separated, as both require different power supplies. Five metal layers are used for routing the entire design, power supply and ground connects are on the top layer.

The floor-planned design is used for automatic placement. It is a process of placing the standard cells in suitable locations in the core area. The core area should be free from any obstacles like power routes, macros and hot spots. Figure 4 shows the placed cells with no violations.

The cells in the core area of the design has to be connected with clock supply, since, the die receives clock from one source or one input pad, this clock pad has to drive the flip flops placed in the entire core area. The clocks reaching all the flip-flops should have minimum latency and zero skew. In order to meet these requirements clock tree network is identified that can carry clock from the pad to all the flip-flops. Figure 5 shows the clock-routed design with minimum latency and skew.

The final stage in the design process is routing all the cells in the core area and to the I/O cells. Routing contain two step process, initially global routing is carried out and then detailed routing is followed which ensures that all the cells are interconnected as per the netlist. Figure 6 shows the routed design of the proposed work.

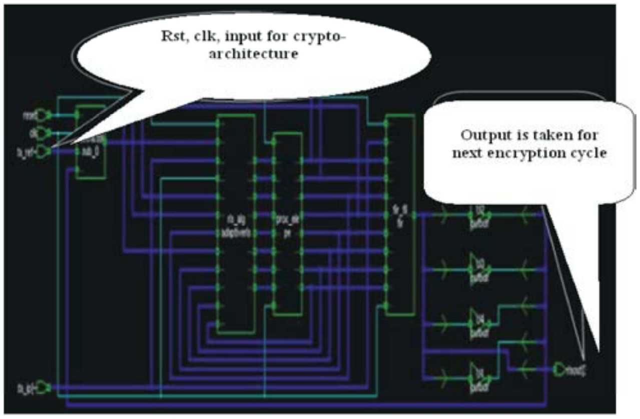
Rst, clk, input for crypto-architecture
Output is taken for next encryption cycle

Fig. 2: Synthesized schematic of crypto-processor architecture

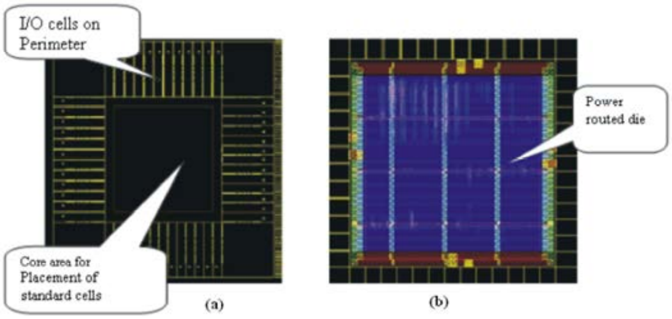

Fig. 3: Floor planned die (a) Standard cells & I/O cells (b) Power routing

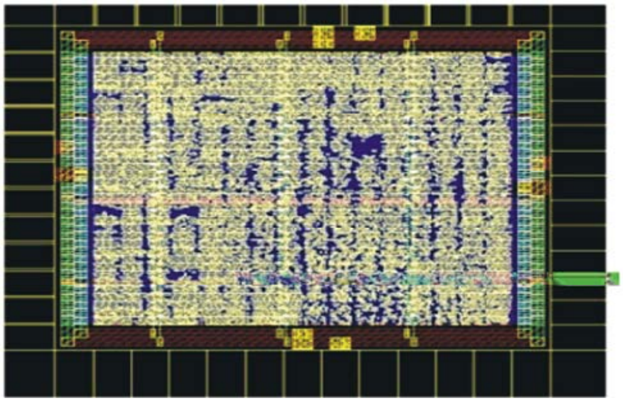

Fig. 4: Placed cells with no violations

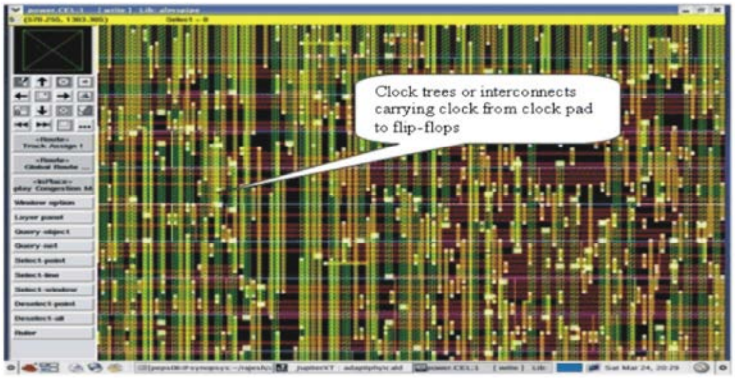
Clock trees or interconnects carrying clock from clock pad to flip-flops

Fig. 5: Clock routed design

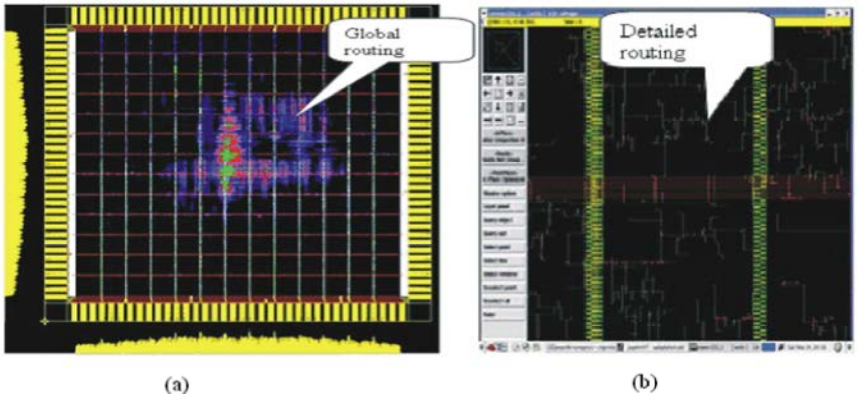

Fig. 6: Routed design (a) Global routing (b) Detailed routing

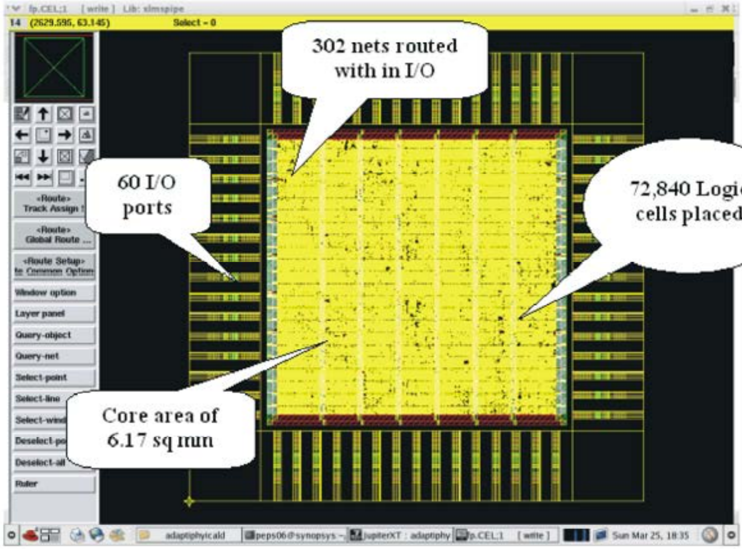

Fig. 7: Layout of final chip of crypto-processor

Table 1: Performance comparison of proposed design

Scheme	Supply voltage (v)	Technology (nm)	Critical Path (ns)	Area (sq. mm)	Total power (mW)
[11]	1.2	130	6.78	8.92	67.54
[14]	1.2	130	6.62	7.81	63.33
Proposed	1.2	130	5.64	6.17	49.49

The layout of the final chip for Cryptoprocessor is shown in Figure 7. The proposed design is free from DRC violations, meeting all the constraints as identified in the specifications. This is converted to GDSII file and it is made ready for fabrication. The entire design is verified using sign off tools from Synopsys.

Table 2 provides the various performance measures for the proposed work and other related references [11] and [14]. The CMOS technology and supply voltage for the design are 130nm and 1.2 volt respectively. The proposed design consumes a total dynamic power of 49.49 mW which is less than other referred works. Similarly the area and critical path are reduced in this scheme.

CONCLUSION

Power efficient implementation of AES algorithm has been utilized to design the high performance crypto-processor. It supports both encryption and decryption with a throughput of 0.05Gbps. ASIC based AES crypto-processor is designed using the low power AES unit and implemented using 130 nm CMOS technology. The proposed design consumes a total dynamic power of

49.49 mW which is less than existing schemes. The proposed scheme reduces the critical path and area for improved performance.

REFERENCES

1. Hodjat, A., P. Schaumont and I. Verbauwhede, 2004. Architectural design features of a programmable high throughput AES coprocessor, Proc. of the International Conference on Information Technology: Coding and Computing, ITCC'04, 2: 498-502.
2. Ahmad, N. and S.M. Rezaul Hasan, 2012. Low-power compact composite field AES S-Box/Inv S-Box design in 65nm CMOS using novel XOR gate, Integration, the VLSI journal, http://www.sciencedirect.com/science/article/pii/S0167926012000375.
3. Hamalainen, P., T. Alho, M. Hannikainen and T.D. Hamalainen, 2006. Design and implementation of low-area and low-power AES encryption hardware, Conf. on Digital System Design: Architectures, Methods and Tools, Dubrovnik, Croatia, pp: 577-583.
4. Hsiao, S.F. and M.C. Chen, 2005. Efficient substructure sharing methods for optimizing the inner-product operations in Rijndael advanced encryption, IEE Proc., Comput. Digit. Tech., 152(5): 653-665.
5. NIST, Advanced encryption standard (AES), 2001. Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
6. Hodjat, A. and I. Verbauwhede, 2006. Area-throughput trade-offs for fully pipelined 30 to 70 Gb/s AES processors, IEEE Transactions on Computers, 55(4): 366-372.
7. McLoone M. and J. McCanny, 2001. High Performance Single-Chip FPGA Rijndael Algorithm Implementations, Proc. Workshops Cryptographic Hardware and Embedded Systems., CHES, pp: 65-76.
8. Wu, L., C. Weaver and T. Austin, 2001. Cryptomaniac: A fast flexible architecture for secure communication, Proc. of the 28th Annual International Symposium on Computer Architecture, ISCA 2001, pp: 110-119.
9. Oliva, D., R. Buchty and N. Heintze, 2003. AES and the cryptonite crypto processor, Proc. of the 2003 International Conference on Compilers, Architecture and Synthesis for Embedded Systems, pp: 198-209.
10. Kim, N.S., T. Mudge and R. Brown, 2003. A 2.3 Gb/s fully integrated and synthesizable AES Rijndael core, Proc. IEEE Custom Integrated Circuits Conference, pp: 193-196.
11. Su, C., T. Lin, C. Huang and C. Wu, 2003. A high-throughput low-cost AES processor, IEEE Communication Magazine, 41(12): 86-91.
12. Hodjat, A. and I. Verbauwhede, 2004. A 21.54 Gb/s fully pipelined AES processor on FPGA, Proc. of 12th Annual IEEE Symposium on Field — Programmable Custom Computing Machines, pp: 308-309.
13. Kozyrakis, C., D. Judd, J. Gebis, S. Williams, D. Patterson and K. Yelick, 2001. Hardware/compiler codevelopment for an embedded media processor, Proceedings of the IEEE, 89(11): 1694-1709.
14. Kuo, H. and I. Verbauwhede, 2001. Architectural optimization for a 1.82 Gb/s VLSI implementation of the AES Rijndael algorithm, Proc. of Cryptographic Hardware and Embedded Systems CHES 2001, Paris, France, in: LNCS, 2162: 51-64.
15. Kalaiselvi, K. and H. Mangalam, 2015. Power efficient and high performance VLSI architecture for AES algorithm, Journal of Electrical Systems and Information Technology.