Low-Power Implementation of a High-Throughput Multi-core AES Encryption Architecture

Pham-Khoi Dong[a], Hung K. Nguyen[a], Van-Phuc Hoang[b], Xuan-Tu Tran[a]*
[a)] SISLAB, University of Engineering and Technology – Vietnam National University, Hanoi
[b)] Institute of System Integration, Le Quy Don Technical University, Hanoi
* *Corresponding author's email: tutx@vnu.edu.vn*

***Abstract* - Nowadays, the Internet of Things (IoT) has been a focus of research that improves and optimizes our daily life based on intelligent sensors and smart objects working together. Thanks to Internet Protocol connectivity, devices can be connected to the Internet, thus allowing them to be read, controlled, and managed at any time and at any place. Security and privacy are the key issues for deploying IoT applications, and still face some enormous challenges; especially, for devices that require high throughput and low latency as IoT cameras, IoT gateways, high-quality video conferencing systems… In this paper, we proposed a 10-cores AES hardware architecture to achieve high throughput. These cores shared KeyExpansion Block so this architecture has high efficiency in term of area and power consumption. Fully parallel, outer round pipeline technique is also used to achieve low latency. The design has been modelled in RTL VHDL and then synthesized with a 45nm CMOS technology using Synopsys Design Compiler. On the other hand, clock gating technique is used to save power consumption. We use PrimeTime tool (Synopsys) to estimate the power consumption. Implementation results show that the proposed architecture achieves a throughput of 853.8 Gbps at the maximum operating frequency of 667 MHz and clock gating technique allows more power savings.**

Keywords— AES, multi-core AES, ASIC technology, security, high throughput, low latency, real-time applications.

I. INTRODUCTION

The Advanced Encryption Standard (AES) was accepted as a FIPS standard in November 2001 [1]. AES implementations can be broadly classified into software and hardware implementation. Compared to software implementation, hardware implementation of AES, by nature, provides more physical security and higher speed. In general, hardware implementation can be performed in either FPGA or ASIC platforms [2]. There have been many different hardware implementations for FPGA and ASIC. References [3], [4] [5], [6], [7], [8], [9], [10], [11] present architectures and results for ASIC implementation. On the other hand, references [12], [13], [14], [15], [16] present implementations of the AES algorithm on FPGA that can achieve a throughput rate from 2 to 130 Gbits/s.

The work in [3] presents hardware optimization strategies for high-speed ultralow-power AES architecture. First, the authors used AES 32-datapath to optimize area cost. Next, they utilized 8 S-Boxes to improve throughput. Finally, they applied a clock gating strategy into data storage registers to reduce power consumption. The test chip was fabricated using ST FDSOI 28nm technology. It achieved a power consumption of less than 20 µW for all key configurations with the energy consumption of less than 1 pJ/b and the throughput of 28 Mbps at 10 MHz.

In [4], the design of ultra-low power AES encryption cores by combining optimized architectures, using clock gating technique, and implementing on 65nm silicon on thin buried oxide (SOTB) CMOS process is presented. The implementation results show that by using two S-Boxes the AES encryption core requires the smallest number of clock cycles and achieves the lowest power consumption of 0.4 µW/MHz. Moreover, the proposed one S-Box AES encryption core consumes very low hardware resources of 2.4 kilo gate equivalent (kGEs).

Zhao *et al.* [5] present the architectural exploration of lightweight AES accelerators with the goal of minimizing energy consumption. The number of cycles per encryption in lightweight AES designs is estimated as a function of the number of available S-Boxes. This AES architecture was implemented in a 65nm test-chip and achieves 0.83 pJ/bit energy at 0.32 V with a throughput of 376 kbps.

Works [3], [4], [5] propose AES designs with an extremely low area and low power consumption, but due to the use of a looping architecture and low frequency, throughput is not high, and the latency is large. Therefore, these architectures are not suitable for high throughput applications and low latency requirements.

Pipelining and sub-pipelining techniques can be employed to increase operational frequency and throughput. Hodjat *et al.* [6] propose AES-128 core architectures with throughputs of 30 to 70 Gbps corresponding to area cost between 180 and 275 kGEs implemented on 180nm technology. With 30 Gbps throughput, the architecture uses outer round pipelining (one stage pipeline per round), takes 11 cycles to encrypt a 128-bit block. Therefore, the corresponding latency is 47 ns. With a throughput of 70 Gbps, the authors used a 4-stage pipeline architecture in each round, which took 41 cycles for each 128-bit block corresponding to a delay of 74.9 ns.

AES core in [8] running at 1000 MHz achieves the highest throughput of 128 Gbps. This architecture has 20 pipeline stages so it needs 20 clock cycles to encrypt one block of data; therefore, the latency is 20 ns. Despite achieving high throughput, the designs in [8] [9] and [10] have the large latency and is inefficient in terms of hardware resources and power consumption due to the excessive use of the pipeline.

Clock gating is very useful for reducing the power and energy consumed by digital systems. Authors in [17] fabricated and tested an energy recovery clocked pipelined multiplier with an integrated resonant clock generator, generating a sinusoidal clock. Results show a power reduction of 70% on the clock-tree and total power savings of 25% - 69% as compared to the same multiplier using

978-1-7281-9396-0/20/$31.00 ©2020 IEEE

conventional square-wave clocking scheme and corresponding flip-flops (FF). Shmuel Wimer *et al.* [18] present a novel method called Look-Ahead Clock Gating (LACG). Based on the present cycle data of FFs, this method calculates the clock enabling signals of each FF one cycle ahead of time. It is not only capable of stopping the majority of redundant clock pulses but also avoiding the tight timing constraints of AGFF and data-driven. The LACGs are modelled at RTL level, which significantly simplifies the gating clock implementation. The article also proposes to use one LACG for two FFs to reduce the hardware overheads and power consumption. LACG has been experimented on 22nm process technology. The experimental results have shown that this method reduces 22.6% of the clock power and 12.5% power consumption of the entire system.

Multi-core AES architectures can address the throughput limitations of single-core AES architectures. Multi-core AES running parallel on-chip increases throughput and is presented in some works as follows:

The work in [10] uses Multicore Processor (AMP-MP) to achieve high throughput and yet secure Advanced Encryption Standard based on Counter with Chaining Mode (AES-CCM). The proposed AMP-MP is realized on an 8-bit asynchronous 9-core processor fabricated based on 65nm CMOS process. The experimental results show that the throughput of the authentication is 13.54 Gbps.

In [19], the authors introduce a new parallelization strategy for Advanced Encryption Standard based on Galois/Counter Mode (AES-GCM). The approach enables the construction of scalable streaming cores that can process multiple separately-keyed packets per clock cycle in wide segmented busses. Authors demonstrate throughput of 482 Gbps in a single Xilinx Ultra scale FPGA and outline how the architecture can be used to achieve over 800 Gbps in a system comprising multiple FPGAs. Multi-FPGA systems are enabled because the architecture requires no core-to-core communication.

A detailed design for implementation of the AES algorithm on a multiprocessor platform has been provided in [20]. This research is to increase the processing speed of the AES encryption algorithm using the parallel and sequential mechanism. Authors have optimized both the encryption as well as the decryption algorithms. Parallelization in the source code has provided a huge difference of more than 80% in comparison with the sequential algorithms.

In [12], the authors have presented an efficient design methodology to implement the GCM combined with the AES for authenticated encryption in reconfigurable hardware devices. Using four AES cores and four binary field multipliers authors were able to demonstrate how to break the 100 Gbps speed bound in FPGA. In order to reduce the critical path of the GHASH operation, four pipeline stages have been inserted within the GF(2^{128}) multiplication. The final GCM architecture relies on a 4×4 construction and achieves 119 Gbps in Xilinx Virtex-5 devices.

Our target is to design a high-throughput AES encryption architecture with energy efficiency. To speed up encryption, we introduce a multi-core AES architecture. This architecture consists of single AES cores, which operate in parallel mode. To reduce power consumption, clock gating techniques are applied to the proposed architecture.

The remaining part of this paper is organized as follows. Section II describes the proposed hardware architecture with low power technique. The experimental results and discussions will be presented in Section III. Finally, conclusion and remarks are in Section IV.

II. Hardware Architecture Proposal

A. Proposed Clock Gating Multi-Core AES Architecture

The Clock Gating Multi-Core AES architecture is proposed in Fig. 1. This architecture consists of *N* single AES cores that work in parallel to speed up the encryption. Data bus consists of *N*×*128* parallel lines, each core uses 128 independent data lines. So, each clock cycle encrypts *128*×*N* bits of input data. Typically, each AES core has a Key Expansion block used to generate round keys for each round of AES. However, with AES multi-core architecture on chip, we only use one Key Expansion block for all single AES cores to reduce area and power consumption.

To reduce power consumption, we used "local clock gating" technique. This feature causes inactive clocked elements to have clock gating logic automatically inserted which reduces power consumption on those elements when the values stored by those elements are not changing. The RTL clock gating feature allows easily configurable,

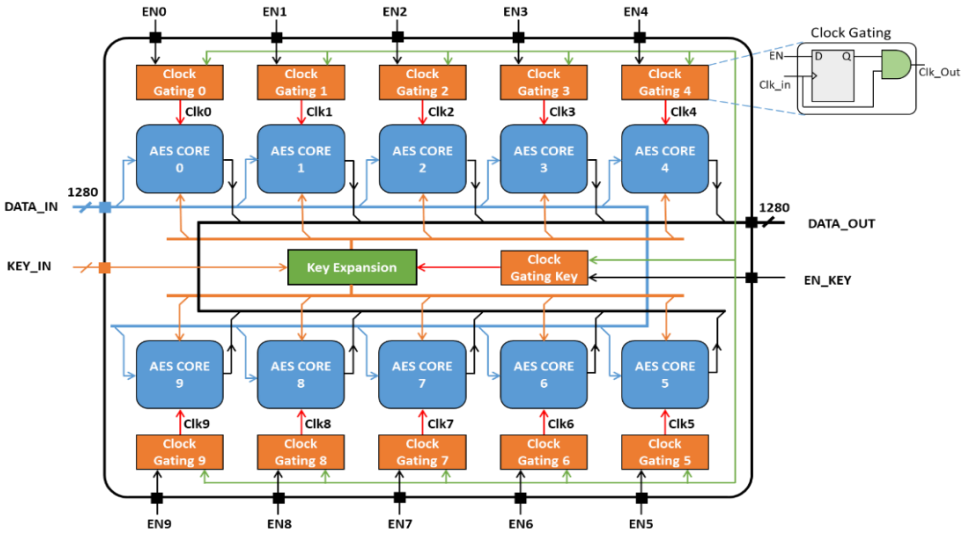

Fig. 1. Clock Gating Multi-Core AES Architecture.

TABLE I. IMPLEMENTATION RESULTS OF MULTI-CORE AES ON 45NM CMOS TECHNOLOGY

Active cores	CLK (MHz)	Clock Gating			Non Clock Gating			Saving Power (%)	Throughput/ Core (Gbps/core)
		Total Power (mW)	Throughput (Gbps)	Energy Efficiency (Gbps/W)	Total Power (mW)	Throughput (Gbps)	Energy Efficiency (Gbps/W)		
No core	667	24.5	0	0	104.7	0	0	76.6	0
One core	667	230.3	85.38	370.7	302.1	85.38	282.6	23.8	8.5
Two cores	667	419.4	170.76	407.2	500.1	170.76	341.5	16.1	17.0
Three cores	667	618.3	256.14	414.3	698.1	256.14	366.9	11.4	25.6
Four cores	667	817.2	341.52	417.9	897.0	341.52	380.7	8.9	34.2
Five cores	667	1014.9	426.90	420.6	1094.7	426.90	330.4	7.3	42.7
Six cores	667	1212.4	512.28	422.5	1291.9	512.28	343.7	6.2	52.2
Seven cores	667	1412.0	597.66	423.3	1490.3	597.66	353.1	5.3	57.8
Eight cores	667	1611.7	683.04	423.8	1692.8	683.04	403.5	4.8	68.3
Nine cores	667	1809.2	768.42	424.7	1891.0	768.42	406.4	4.3	76.8
Ten cores	667	2015.0	853.80	423.7	2084.8	853.80	409.5	3.3	85.4

automatically implemented clock gating which allows a maximal reduction in power requirements.

The "Global clock gating" technique is used by inserting the Clock Gating Cells. Each single AES core has a Clock Gating Cell to turns off the clock in case this AES core is not used. Depending on the throughput of the application, users can configure the chip to run all of the N cores or only run some cores. Other cores are tuned off the clock signal by setting the core's EN pins to '0' logic to reduce the power consumption of the unused cores.

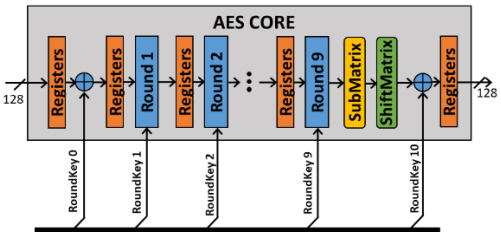

Fig. 2. Architecture of Single Core AES.

The structure of the Single Core AES is shown in Fig. 2. In each AES core there are 10 CipherRounds, to speed up encryption, between rounds we insert registers to create the pipeline architecture. The pipeline and parallel architecture ensures that when data is filled full in the pipeline stages, after clock cycle a block of 128-bit is encrypted.

III. RESULTS AND DISCUSSION

We implemented hardware for two multi-core AES architectures on 45nm ASIC technology. In the first architecture, we didn't use local clock gating and global clock gating. For the second architecture, we used local clock gating with the *insert_clock_gating* command in DC Compiler. After synthesizing with DC Compiler, we use Synopsys PrimeTime tool to estimate power consumption in 11 cases (active from 0 to 10 cores via EN pin). Depending on the input data rate to enable the clock for each core, for example, when there is no input data, interrupt the clock for all 10 cores, when the input data rate is 85 Gbps, turn on the clock for 1 core, when the input data rate is 170 Gbps, turn on the clock for 2 cores.

The results of hardware synthesis on 45nm CMOS technology are presented in Table I. With 10 cores on the chip, our architecture achieves high efficiency in terms of power consumption, extremely throughput (853.8 Gbps). Although the throughput of the multi-core AES architecture without clock gating is the same, the multi-core AES architecture that uses the clock gating technique has lower power consumption. Summary, the clock gating technique applied in our AES multi-core design saves 3.3% to 76.6% of power consumption (Fig. 3).

TABLE II. THROUGHPUT OF MULTI CORE AES ENCRYPTION COMPARISON

Design	Platform	Number of cores	Throughput (Gbps)
[10] 2019	65nm CMOS	9 cores	13.54
[19] 2015	multiple FPGAs	20 core	883
[12] 2010	FPGA Xilinx Virtex-5	4 cores	119.3
Our work	45nm CMOS	10 cores	853.8

In terms of throughput, our design provides a higher throughput than related works using ASIC [10] and FPGA [12] technologies (TABLE II). In [19], although the throughput is higher than our design, however 20 AES cores are required over multi FPGAs. Our design has so high throughput that it can be used to develop high speed access networks.

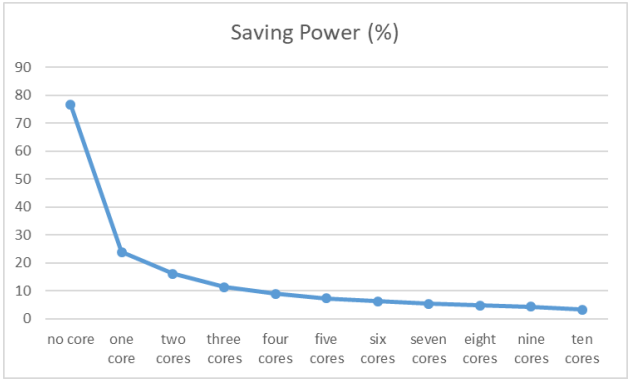

Fig. 3. Power Consumption with Clock Gating vs. without Clock Gating.

IV. CONCLUSION

In this paper we have proposed two multi-core AES architectures. On the first architecture we used clock gating techniques to reduce the power consumption, on the second architecture we did not use clock gating. In both architectures, KeyExpansion blocks are shared between AES cores to reduce area cost, pipeline technique is used in each single core to

increase throughput. The hardware synthesis results on 45nm CMOS technology show that our designs achieve ultra-high throughput (853.8 Gbps). On the other hand, the clock gating technique applied in the first multi-core AES design saves 3.3% to 76.6% of power consumption than second design.

ACKNOWLEDGEMENT

This research is supported by Ministry of Science and Technology (MoST) of Vietnam under grant number KC.01.21/16-20.

REFERENCES

[1] *FIPS 197: Advanced Encryption Standard. National Institute of Standards and Technology, available at http://csrc.nist.gov/publications/,* 2001.

[2] P. Chodowiec, "FPGA and ASIC implementations of AES," in *Cryptographic engineering*, Springer, 2009, p. 235–294.

[3] D.-H. Bui, D. Puschini, S. Bacles-Min, E. Beigne and X.-T. Tran, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 25, no. 12, pp. 3281-3290, 12/2017.

[4] V.-. Hoang, V.-. Dao and C.-. Pham, "Design of ultra-low power AES encryption cores with silicon demonstration in SOTB CMOS process," *Electronics Letters,* vol. 53, no. 23, pp. 1512-1514, 2017.

[5] W. Zhao, Y. Ha and M. Alioto, "Novel Self-Body-Biasing and Statistical Design for Near-Threshold Circuits With Ultra Energy-Efficient AES as Case Study," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 23, no. 8, pp. 1390-1401, August 2015.

[6] A. Hodjat and I. Verbauwhede, "Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors," *IEEE Transactions on Computers,* vol. 55, pp. 366-372, April 2006.

[7] S. K. Mathew, F. Sheikh, M. Kounavis, S. Gueron and A. Agarwal, "53 Gbps Native GF(2^4)^2 Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors," *IEEE Journal of Solid-State Circuits,* vol. 46, pp. 767-776, April 2011.

[8] G. Sayilar and D. Chiou, "Cryptoraptor: High throughput reconfigurable cryptographic processor," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2014.

[9] L. Ali, I. Aris, F. S. Hossain and N. Roy, "Design of an ultra high speed AES processor for next generation IT security," *Computers & Electrical Engineering,* vol. 37, no. 6, pp. 1160-1170, November 1, 2011.

[10] A. A. Pammu, W. Ho, N. K. Z. Lwin, K. Chong and B. Gwee, "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 4, pp. 1023-1036, April 2019.

[11] Pham-Khoi Dong, Xuan-Tu Tran and Hung K. Nguyen, "A 45nm High-Throughput and Low Latency AES Encryption for Real-Time Applications," in *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*, Sep. 2019.

[12] L. Henzen and W. Fichtner, "FPGA parallel-pipelined AES-GCM core for 100G Ethernet applications," in *2010 Proceedings of ESSCIRC*, Sept 2010.

[13] K. B. Anuroop and M. Neema, "Fully pipelined-loop unrolled AES with enhanced key expansion," in *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, May 2016.

[14] S. Hesham, M. A. A. E. Ghany and K. Hofmann, "High throughput architecture for the Advanced Encryption Standard Algorithm," in *17th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, April 2014.

[15] J. Vliegen, O. Reparaz and N. Mentens, "Maximizing the throughput of threshold-protected AES-GCM implementations on FPGA," in *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, July 2017.

[16] Y. Wang and Y. Ha, "High throughput and resource efficient AES encryption/decryption for SANs," in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2016.

[17] H. Mahmoodi, V. Tirumalashetty, M. Cooke and K. Roy, "Ultra Low-Power Clocking Scheme Using Energy Recovery and Clock Gating," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 17, no. 1, pp. 33-44, January 2009.

[18] S. Wimer and A. Albahari, "A Look-Ahead Clock Gating Based on Auto-Gated Flip-Flops," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 61, no. 5, pp. 1465-1472, May 2014.

[19] B. Buhrow, K. Fristz and E. Daniel, "A highly parallel AES-GCM core for authenticated encryption of 400 Gb/s network protocols," in *2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, December 2015.

[20] M. S. Al-Bahri, A. J. AiShebani, K. Gupta and O. K. AlAwaisi, "AES Parallel Implementation on a Homogeneous Multi-Core Microcontroller," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, March 2018.