The Compatibility Analysis of AES Algorithm for Design Portability on FPGA

S. J. H. Pirzada, A. Murtaza, T. Xu, and L. Jianwei

***Abstract*—The increase in utilization of digital systems for rapid prototyping has compelled researcher to use Field Programmable Gate Array (FPGA) hardware. The Hardware description language (HDL) such as Verilog and VHDL, etc. are utilized for designing digital systems on FPGA. The HDL core can be designed either by the designing a core by indivisual or by using the ready-to-use cores provided by FPGA vendors. The cores provided by FPGA vendors are Intellectual Property core (IP-core) which provides an rapid prototyping option for implementation on FPGA. The IP-core provided by one FPGA vendor cannot be used on other vendors FPGAs. Therefore, designing an HDL core by indivisual provides the design portability on FPGA, as the core designed by indivisual can be used on FPGA of any vendor. Therefore, in scenarios where it is required to have FPGA platform independent solution, an individual designed HDL core is highly recommended instead of IP-core provided by FPGA vendors. Moreover, the licensing is required for many IP-cores; which makes it less feasible for low-cost design as licensed IP-core are available on payment. In this work, the Advanced Encryption Standard (AES) algorithm HDL core design is compared between HDL core designed by individual and IP-core provided by different FPGA vendors. Experimental results show that the comparison of implementations present quite similar results; however, design portability of an HDL core designed by an individual makes it more attractive in contrast to that is available by FPGA vendors.**

***Index Terms*—Advanced encryption standard, field programmable gate array, hardware description language, intellectual property core.**

I. Introduction

In the modern age, the computational power of computing systems is increasing for providing high-speed operations for a day to day usage. The increase in computational power has an impact on every walk of life, i.e., the communication systems, security algorithms, and information networks all are being designed for high-speed operations. The high-speed services are provided by utilization of either increase in computational power or by the parallel architectural implementation of systems. The parallel architecture implementations can utilize the ability of parallel processing hardware such as Field Programmable Gate Array (FPGA) for implementation. The FPGA provides parallel execution of algorithms as compared to other platforms; those provide sequential implementation on single or multicore processing. The algorithm implemented on FPGA is designed using Hardware Description Language (HDL). There are two significant HDL types available for the design of algorithms on FPGA; these are Verilog-HDL [1] and VHDL [2]. The hardware design implemented using HDL by FPGA vendor is the intellectual property of that company; therefore, it is known as Intellectual Property Core (IP-core). The IP-cores are provided by all FPGA manufacturers such as Xilinx [3], Microsemi ACTEL [4], Altera [5], etc. These IP-cores are optimized for a vendor-specific FPGA. So the IP-core designed by Xilinx can only work on Xilinx FPGAs. In addition to the IP-cores, individual designers can design their HDL core for implementation of an algorithm. The optimization of individually designed HDL core depends on the skills of the designer. There are certain advantages of individually designed HDL core as compared to the IP-cores. Specifically, in an application which requires the FPGA platform independent solution. For instance, in case of change of user requirements for a certain project can force the designer to change the use of FPGA from a specific vendor. Therefore the individual designed HDL core can be utilized in FPGA of any vendors but the IP-core of one vendor cannot be used with other vendors FPGA. Moreover, the IP-core provided by vendors is of two categories, either paid or free. The paid cores license can increase the cost of system implementation. Besides the IP-cores, many companies are working on providing a third party IP-core for implementation on FPGA platforms [6]. The increasing trend of providing third-party solution has provided an option for designers for utilizing the HDL core for their systems by purchasing the pre-designed IP-cores. These IP-cores provided by the third party sometimes are FPGA platform independent, and sometimes the third party provides FPGA platform specific IP-cores. There are also some online resources which provides free to use IP-cores, but these cores are not verified and may have errors / bugs in the cores.

The FPGA based systems are utilized for communication application for high-speed communications. The communication systems for terrestrial and air communication utilize Static Random Access Memory (SRAM) based FPGAs such as provided by Xilinx, Altera, etc. Although in space communication, special equipment is required for the protection of communication systems from extreme conditions [7]. The FLASH based FPGAs (such as provided by Microsemi ACTEL, etc.) are utilized in space communication. In addition to it, space-grade SRAM based FPGAs provided by Xilinx and Altera, etc. are also being used for space communications. The selection of FPGA

Manuscript received June 9, 2019; revised September 10, 2019. The work is supported by school of cyber science and technology, Beihang University, Beijing, China.

S. J. H. Pirzada, T. Xu, and L. Jianwei are with the School of Cyber Science and Technology, Beihang University, Beijing, China (e-mail: jahanzebp@ hotmail.com, xutg@buaa.edu.cn, liujianwei@buaa.edu.cn).

A. Murtaza is with the School of Electronics and Information Engineering, Beihang University, Beijing, China (e-mail: abid_murtaza47@hotmail.com).

DOI: 10.7763/IJCTE.2019.V11.1253

vendor depends on the application area and FPGA hardware architecture. Therefore, the FPGA platform independent HDL core helps in shifting design and saving precious design time quickly.

The Advanced Encryption Standard (AES) algorithm is used for providing data security for communication systems [8]. The AES algorithm is the state-of-the-art algorithm which is utilized in many applications such as space communication [9]. The AES algorithm provides options for different key sizes of 128-bits, 192-bits, and 256-bits. The AES algorithm takes 10 rounds for 128-bits key, 12 rounds for 192-bits key, and 14 rounds for 256-bits key. The key size determined by the level of security required by the specific application. The input message to the AES algorithm is called the plaintext and output is called ciphertext. The AES algorithm consists of four sub-algorithms; these are substitution byte, shift row, mix column, and add round key. There are many modes of implementation of AES algorithms [10]. The AES algorithm can be implemented on FPGA using IP-core or individually designed HDL core. The AES algorithm not only utilized in provided data encryption, but it is also utilized in providing data authentication services such as Cipher-based Message Authentication Code (CMAC) algorithm [11]. Many researchers have implemented the CMAC algorithm on FPGA by designing their HDL core [12], [13]. The AES algorithm is also utilized in the provision of Authenticated Encryption (AE) algorithms such as GCM [14] and PCMAC [15] etc. Hence, the AES algorithm finds its application in almost every data security application. The AES algorithm flow diagram is shown in Fig. 1.

Rest of the paper is organized as follows. Section II presents previous work; Section III presents the comparative analysis of HDL cores. Section IV presents experimental results, and Section V concludes this paper.

II. Previous Work

The requirements of the implementation of different algorithms for communication systems are increasing with the increase of electronics devices for daily use. This requirement has motivated designers to develop HDL cores for implementation of different algorithms for rapid prototyping. L. Sekanina [16] presented the idea of evolvable IP cores for FPGAs. The evolvable IP-core can provide independent evolution of an internal circuit. L. Shannon [17] has provided a detailed study on the impact of IP-cores on FPGA design. He explained the advantages and disadvantages of using IP-core based design and market trend associated with it.

The AES algorithm is a widely used data security algorithm for many applications. The HDL core for AES algorithm is provided by almost all the FPGA manufacturers for providing data security. Also, the AES algorithm is implemented by many researchers on FPGA by designing their own IP-core. H. Zodpe *et al*. [18] presented an AES algorithm implementation using an efficient method for advances in the security features. Their work proposed, the design of HDL core and implementation of design using PN sequence generator for implementation of substitution box. T. good *et al*. [19] has presented the review of AES algorithm implementation of FPGA. Their work has reviewed all the implementations for fastest as well as the smallest implementation on FPGA for AES algorithm. G. P. Saggese *et al*. [20] has presented the optimization techniques used for efficient implementation of AES algorithm such as pipelining, tiling, and unrolling of the algorithm on FPGA. Their implementation is focused on modification of algorithm implementation for increase speed and efficiency of the algorithm. All the research work discussed is focused on optimization of AES algorithm on FPGA by modification of HDL core. In addition to it, F. Durvaux *et al*. [21] has presented their work on the security issues related to the development of HDL cores on FPGA. Their work provided a survey on the security of hardware implementation using FPGA and discussed significant attacks on the security HDL core of the AES algorithm.

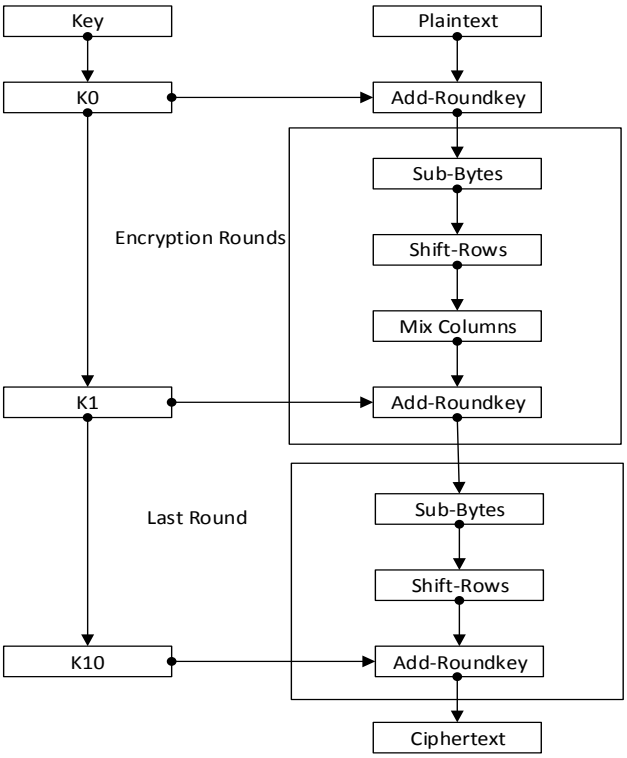

Fig. 1. The AES algorithm flow.

Hence the implementation of HDL core for AES algorithm has been implemented using many modifications for improvement for various applications. The comparison of FPGA vendor provided IP-cores with the individually designed HDL core have not yet been provided. This work provides the limitations of IP-cores to compare the HDL cores developed by individuals with IP-cores.

III. The Comparative Analysis of HDL Cores

The IP-cores provided by FPGA vendors are designed to provide the functional requirement of a specific algorithm as per the standard implementation. The IP-cores provides options for variations of the algorithm implementation, i.e., the AES algorithm IP-core provides options for 128bits, 192bits, and 256bits key size implementation selection. Although the HDL is not visible for modification of IP-cores, therefore it cannot be used in any other FPGA vendor. This

feature of IP-core protects the specific FPGA vendors business, but it poses certain limitations.

A. Utilization of IP-Cores for Research Work

Firstly, the IP-cores cannot be utilized for modification of algorithms for research purpose. The implementation of substitution-box in AES algorithm is performed on Look-up Table (LUT) instead of using Block Random Access Memory (BRAM). In space communication implementation of AES algorithm for implementing Substitution-box using BRAM instead of LUT [7] cannot be performed using IP-cores. The IP-cores cannot be used to conduct further research, and implementation must be done by designing the HDL core by an individual.

B. Time to Market vs. Controllability

Secondly, the IP-cores provide the easy to design and fast implementation option, but it does not provide control over all parameters of the algorithm. The AES algorithm inputs and outputs can be configured in the IP-core, but the intermediate implementation parameters cannot be configured. Some researcher proposed the modification in the algorithm for increasing randomness in cipher-text [22]. These changes cannot be implemented as the intermediate states are not accessible.

C. Architecture Variations in FPGAs

Thirdly, the IP-cores provided by an FPGA vendor is limited for certain families of FPGA manufacturer with certain hardware architecture. The compatibility of different cores among various device families in the same FPGA manufacturer is specified by the manufacturer. Most of the time, size limits the usability of cores in different families.

D. Design Portability

Fourthly, the possibility of using cores of one FPGA manufacturer with another FPGA manufacturer is nearly impossible because of the change of format of core and design architecture. Besides, the IP-cores are locked with a particular FPGA vendor, and HDL files are not available. Therefore, design portability is not possible.

E. IP-Core Licensing Issues

Fifthly, a significant issue is the licensing issue, which restricts the designer to use the IP-core developed by the FPGA vendor. The IP-cores require licensing are not free and can cost much money for using it. In the case of IP-cores provided by third-party IP-core developer, the cores cannot be implementable of FPGAs of two different manufacturers, and it also costs money. The payment of an additional amount of money reduces the cost-effectiveness of the design.

On the other hand, HDL core designed by individual provides the advantage of design portability and design modification according to the application requirements. Therefore, the HDL core design by an individual has been widely adopted instead of IP-cores.

IV. The Experimental Results

Many vendors offer different types of FPGA for commercial use. These FPGAs are either SRAM based FPGAs or FLASH based FPGAs. Also, the logic resources and architecture of FPGA varies in all FPGAs vendors. The IP-cores provided for any specific FPGA vendor are different for different families of FPGAs with different architecture. In this work, the HDL core of the AES algorithm is implemented on SRAM and FLASH based FPGAs. The implementation is performed to compare the resources and analysis of the design.

The implementation of the AES algorithm on SRAM based FPGA is performed on Xilinx Virtex-6 FPGA (XC6VLX75T). The AES algorithm IP-core for the Xilinx Virtex-6 FPGA [23] is implemented, and resource utilization is compared with HDL core design implementation by an individual. The implementation is performed using Xilinx ISE 12.1 using Modelsim simulation software. The implementation of AES IP-core is performed for a key size of 128bits, 192bits, and 256 bits. The implementation of the HDL core is implemented for 128bits key size. The comparison of resource utilization is shown in Table I. The resource utilization of HDL core and IP-core implementation has approximately the same resources.

TABLE I: Comparison of Resource Utilization on SRAM FPGA

Implementation	LUT	Block RAM	*Clock Frequency*
AES IP Core [23]	946	4	345
AES HDL Core	635	5	307

The implementation of the AES algorithm on FLASH based FPGA is performed on ACTEL ProASIC3E FPGA. The AES algorithm IP-core for the ACTEL ProASIC3E FPGA [24] is implemented, and resource utilization is compared with HDL core design implementation by an individual. The implementation is performed using Libero SoC 11.8 using Modelsim simulation software. The implementation of AES IP-core and HDL core is performed for a key size of 128bits. The comparison of resource utilization is shown in Table II.

TABLE II: Comparison of Resource Utilization on Flash FPGA

Implementation	LUT	Block RAM	*Clock Frequency*
AES IP Core [23]	4049	8	84
AES HDL Core	4615	0	98.5

The resource utilization of HDL core and IP-core implementation has approximately the same resources. The simulation results of the implementation of the AES algorithm on FPGA is shown in Fig. 2.

V. Conclusion

In this work, a comparison between the HDL core designed by individual and IP-core provided by FPGA vendors is presented. The comparison of resource utilization for AES algorithm implementation on FPGA by both methods is performed. The comparison is provided on Xilinx SRAM based FPGA and Microsemi ACTEL FLASH based FPGA. Although, similar resources were utilized HDL core

designed by individual provides better design portability as compared to IP-cores.

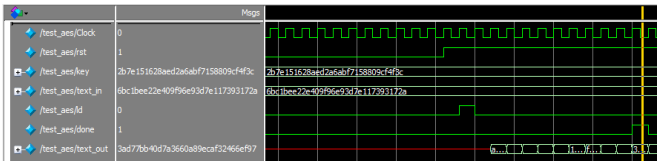

Fig. 2. The AES algorithm simulation.

REFERENCES

[1] "IEEE standard for Verilog hardware description language," IEEE Std 1364-2005 (Revision of IEEE Std 1364-2001), April 7, 2006, pp. 1-590.

[2] "IEC/IEEE international standard - behavioural languages - part 1-1: VHDL language reference manual," in IEC 61691-1-1: 2011(E) IEEE Std 1076-2008, May 19, 2011, pp.1-648.

[3] Xilinx. Intellectual Property. [Online]. Available: https://www.xilinx.com/products/intellectual- property.html

[4] Microsemi ACTEL. [Online]. Available: https://www.microsemi.com/product-directory/design-resources/5092-IP-cores

[5] Altera. [Online]. Available: https://www.intel.com/content/www/us/en/products/programmable/intellectual-property.html

[6] Helion. [Online]. Available: https://www.heliontech.com.

[7] S. J. H. Pirzada, A. Murtaza, L. Jianwei, and T. Xu, "The AES implementation for avoiding single event effects for satellite application," in *Proc. the 9th IEEE on Electronic Information and Emergency Communication Conference (ICEIEC 2019)*, Beijing, China, July 2019.

[8] NIST, FIPS 197. (November, 2001). Advanced Encryption Standard (AES). [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips- 197.pdf

[9] CCSDS, CCSDS 352.0-B-1. (November, 2012). CCSDS Cryptographic Algorithms. [Online]. Available: https://public.ccsds.org/Pubs/352x0b2.pdf

[10] NIST, Special Publication 800-38A. (December, 2001). Recommendation for Block Cipher Modes of Operation: Methods and Techniques. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-38a/final

[11] NIST, Special Publication 800-38B. (May, 2005). Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/index.html#sp800-38B1998.

[12] I. B. Dhaou, T.N. Gia, P. Liljeberg, and H. Tenhunen, "Low-latency hardware architecture for cipher-based message authentication code," in *Proc. Circuits and Systems (ISCAS*), 2017.

[13] S. J. H. Pirzada, A. Murtaza, and L. Jianwei, "Implementation of CMAC authentication algorithm on fpga for satellite communication," in *Proc. Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chengdu, China, March 15-17, 2019.

[14] M. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC," National Institute of Standards and Technology SP 800-38D, November, 2007.

[15] S. J. H. Pirzada, A. Murtaza, L. Jianwei, and T. Xu, "The parallel CMAC authenticated encryption algorithm for satellite communication," in *Proc. Electronic Information and Emergency Communication Conference (ICEIEC 2019)*, Beijing, China, July, 2019.

[16] L. Sekanina, "Towards evolvable IP cores for FPGAs," in *Proc. NASA/DoD Conference on Evolvable Hardware*, Chicago, USA, 2003, pp. 145-154.

[17] L. Shannon, "Impact of intellectual property cores on field programmable gate array design," Master's degree thesis.

[18] H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," *Trans. of Journal of King Saud University–Engineering Sciences*, 2018.

[19] T. Good and M. Benaissa, "AES on FPGA from the fastest to the smallest," *Lecture Notes in Computer Science*, vol. 3659, 2005.

[20] G. P. Saggese, A. Mazzeo, N. Mazzocca, and A. G. M. Strollo, "An FPGA-based performance analysis of the unrolling, tiling, and pipelining of the AES algorithm," *Lecture Notes in Computer Science*, vol. 2778, 2003.

[21] F. Durvaux, S. Kerckhof, F. Regazzoni, and F. X. Standaert, "A survey of recent results in FPGA security and intellectual property protection," *Secure Smart Embedded Devices, Platforms, and Applications*.

[22] A. S. Bader and A. M. Sagheer, "Modification on AES-GCM to increment ciphertext randomness," *Trans. of International Journal of Mathematical Sciences and Computing*, vol. 4, pp. 34-40, November 2018.

[23] Xilinx. Cryptography Intellectual Property. [Online]. Available: https://www.xilinx.com/products/intellectual-property/nav-dsp-and-math/nav-cryptography.html

[24] Microsemi-Actel. [Online]. Available: http://www.actel.com/ipdocs/CoreAES128_RN.pdf

S. J. H. Pirzada was born in Attock, Pakistan. In 2007, he received his BE degree in electronics engineering from NED University of engineering and technology, Karachi, Pakistan. In 2012, he received an MS degree in electrical, electronics, control and instrumentation engineering from Hanyang University, Seoul, South Korea. Since 2018 he is enrolled for the Ph.D. degree in the School of Cyber Science and Technology at Beihang University, Beijing, China. His research interest is in the field of cryptography for satellite applications.

A. Murtaza was born in Karachi, Pakistan. In 2010, he received the M.Sc. electronics degree from the University of Karachi, Karachi, Pakistan. He is working with Pakistan's National Space Agency SUPARCO since 2010. He is currently working towards the Ph.D. degree in space technology applications at Beihang University, Beijing, China. His research interests include information security, space information network, and applications.

T. Xu graduated from Beijing University of Aeronautics and Astronautics in 1993 with a master's degree in engineering. He is now an associate professor of School of Cyber Science and Technology at Beihang University, Beijing, China. His research areas are network management and flow / protocol analysis technology, UNIX / Linux system development, large information system design and development technology, public opinion big data analysis and mining.

L. Jianwei was born in Shandong, China. He received the BS and MS degrees in electronics and information engineering from Shandong University, Shandong, China in 1985 and 1988 respectively. He received his Ph.D. degree in electronics and communication systems from Xidian University, Shaanxi, China in 1998. He is now the dean of the School of Cyber Science and Technology at Beihang University, Beijing, China. His current research interests include wireless communication networks, cryptography, and information and network security.