

Dear Editor and Reviewers:

Thank you very much for reviewing my manuscript titled “*A New Lightweight and Efficient FPGA based Architecture for AES Algorithm Targeting IoT Security*” and providing me valuable comments as well as helpful and encouraging feedback. The comments have greatly helped to improve the quality of the paper. Below, I present responses to address all the review comments. Accordingly, I have modified the manuscript based on the review comments that require actions.

Reviewer A:

The author made some improvements in 2-nd version of the manuscript. He tried to respond to my comments in the review form of the first-round.

However, in the first-round revision, I made some handwriting comments/suggestions over the PDF file of the manuscript, that should improve the quality of the paper. The mentioned PDF was uploaded by the reviewer, but the author said that he didn't receive it.

Dear author: I'm up-loading the same PDF file of the first-round revision (that, for some unknown reason, you didn't receive it), that includes some handwriting comments/suggestions over the PDF of 1-st version of the manuscript. Please consider using this information to improve the manuscript.

Best Regards

Your Reviewer

Response: Thank you very much for all the insightful comments. I really appreciate your commitment, patience and insightful considerations you made when reviewing my paper. Your valuable review comments have greatly helped to improve the quality of the manuscript. Thank you very much. I have considered all of your comments and changed the manuscript accordingly.

Reviewer B:

- 1) Which particular FPGA are you using?
- 2) Have you tested the circuit on an FPGA board or just synthesized and simulated it?
- 3) How do you receive the external data?
- 4) Once again, you cannot achieve such frequencies in a Virtex-5 or Virtex-6 FPGA.
- 5) What are you mapping in the FPGA? Is the source available?
- 6) At what frequencies are the BRAMs and DSPs working?

Response: Thank you very much for your useful comments.

- 1) The FPGA devices used are: Xilinx Virtex-7 (Part: XC7VX690T, speed-grade -3), Virtex-5 (XC5VLX155T) and Virtex-6 (XC6VLX75T).
- 2) The circuit is not tested on FPGA board. Only post synthesis and implementation was performed.
- 3) Just post synthesis and implementation were performed, and no external data was needed or no device interface was done.
- 4) The frequencies achieved on Virtex-5 and Virtex-6 were post synthesis results obtained based on the parallel-pipelined architecture, but not a test result of device interface and device programming.
- 5) As the Vivado HLS accepts hardware oriented c-based design entry, first, c-simulation was done for functional verification of the specification. Then, synthesis, c/RTL co-simulation, and implementation on Virtex-7 device were done. The resulting RTL was also implemented using ISIM for older versions FPGA devices. The source is available.
- 6) The maximum frequencies achieved are the overall frequencies calculated based on the clock periods at which the optimized design was synthesized and implemented, so it depends on the achieved clock periods.

Reviewer C:

From the technical point of view, I find that the paper addresses an interesting topic that fits in the scope of the ISEL Academic Journal of Electronics Telecommunications and Computers (i-ETC) and that the presented work is technically sound. Nevertheless, I believe that there are a couple of aspects that should be improved before the paper is accepted for publication, namely:

1. The title of paper should be reviewed to make it clear that the paper presents a new FPGA-based architecture for AES.
2. The goal of the research work is not clear. Is the proposed architecture targeted for constrained devices or for high-performance ones?

Pipelined architectures are not suitable for implementations in hardware and power constrained devices...

3. The implementation approach adopted by the author considered a Virtex-7 device but did not consider Kintex-7 or Artix-7 devices, which are the ones suitable for constrained implementations. This should be justified.
4. The obtained implementation results should be discussed to properly present the advantages of the proposed architecture regarding the state of the art.

In what concerns the presentation, I find that the submitted manuscript is of easy reading. Nevertheless, I consider that it can be better structured and that the English language can be further improved.

Specific comments and suggestions can be found in the PDF file attached to my review form.

In conclusion, IMO, the manuscript addresses an interesting topic but there are a couple of aspects that must be improved before the manuscript is accepted for publication.

Response: Thank you very much for your valuable and insightful comments as well as constructive feedback that greatly helped to improve the quality of the manuscript. I really appreciate your commitment and patience to deeply read the text and provide such useful comments.

- 1) Based on the comment I have modified the title to: *“A New Lightweight and Efficient FPGA based Architecture for AES Algorithm Targeting IoT Security”*
- 2) Lower number of FPGA resource utilization with moderate throughput results achieved on Virtex-5 device are intended for constrained devices, and high throughput result achieved on Virtex-7 device is intended for high performance applications. This is because the IoT network incorporates both constrained devices (end devices) and high performance platforms such as Fog/Cloud platforms.
- 3) From the Xilinx 7-series device families (Kintex-7, Artix-7 and Virtex-7 devices), Virtex-7 was selected for implementing the proposed architecture targeting the security of high performance applications. For constrained devices, Virtex-5 implementation was considered.
- 4) The result analysis is modified based on your comment and, the result discussion and analysis section of the revised manuscript was changed accordingly.
- 5) Based on your comments, the structure of some parts of the manuscript has been reorganized including Section I, Section II and Section III of the manuscript. Moreover, improvements have been done on the language used for the writings.

I meticulously tried to improve the quality of the manuscript based on the comments, and made some modifications in the manuscript. The modifications will not change the main content and the paper's framework. I appreciate for Editor's/Reviewers' commitments and warm work earnestly, and hope that the corrections will meet the expected requirements.

Thank you again!

Best regards,

sincerely,

Abiy Tadesse Abebe.