

Dear Editors and Reviewers:

Thank you very much for reviewing my manuscript titled "*Lightweight and Efficient Architecture for AES Algorithm based on FPGA*" 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's Comment about manuscript contents.

:

The manuscript presents an important topic.

Most sections are well written.

The analysis of results is presented in an unclear way.

Response: thank you very much for your comments. Based on the comments, the result analysis is written in a more clear way at the result analysis section of the manuscript.

A1. Is the subject of the article suitable for publication in the i-ETC journal?:

4=Almost Yes

Response: thank you very much.

A2. Are the facts, arguments and conclusions in the paper technically valid and accurate?:

3=More or Less

Response: thank you very much.

A3. Is the previous work adequately referenced and integrated with the new results:

5= Definitely Yes

Response: thank you very much.

B. STRUCTURE

Reviewer's Comment about manuscript structure.

The manuscript is well structured but could be improved.

The reviewer suggests some improvements in various sections of the manuscript (please see the pdf file uploaded by reviewer, which has some annotations).

Response: Thank you very much for the comments. I have revised and edited the manuscript based on the comments, even though I didn't get the said pdf file.

B1. Is the title brief yet clear enough to identify the paper?:

5= Definitely Yes

Response: thank you very much.

B2. Does the list of keywords index all the features of interest in the paper?

:

5= Definitely Yes

Response: thank you very much.

B3. Does the abstract indicate the main topics and results?:

4=Almost Yes

Response: thank you very much.

B4. Are the main results and conclusions properly given and explained in the paper?:

3=More or Less

Response: thank you very much.

C. LANGUAGE

Reviewer's Comment about language quality and clarity.

Most sections are well written.

The analysis of results is presented in an unclear way.

Response: thank you very much. Based on the comments, the result analysis is written in a more clear way.

D1. Refree comments to the authors (this will be forwarded to the contact author):

The reviewer suggests some improvements in various sections of the manuscript (please see the pdf file uploaded by reviewer, which has some annotations).

Reviewer D:

In general, the article just implements two lanes of the A3ES algorithm in parallel in FPGA.

No novelty is introduced in the design of each A3ES lane, using a previous design.

Response: The proposed method varies from other existing analogous designs in that it combines several methodologies to provide a compact and efficient AES-128 architecture based on a hybrid approach. In addition to two AES cores working in parallel, outer full parallel pipelining and inner partial parallel pipelining methods have been applied to make the design different. This is used so as to enable message execution fast. The use of DSP48E and DSP48E1 for execution of XOR operations and some logical and simple control operations also make the proposed approach different.

Utilizing DSP slices and BRAM hard-cores, as well as balanced resources from generic FPGA fabrics rather than employing all traditional logic parts or all FPGA hard-cores entirely, could balance the usage of both hardware resources. This enhances implementation flexibility while utilizing contemporary FPGA resources for appropriate sections of the algorithm. The proposed architecture's combined impact is intended to generate a balanced trade-off between speed and area, with more emphasis given to speed.

About the results in table 2, the author report frequencies of around 800 MHz. The speed grade of the used FPGA is not mentioned. Even so, the maximum operating frequency of a BRAM and DSP of a Virtex-6 FPGA is 600 MHz for the highest speed grade (not used). Assuming an IoT application, you should consider a -1L speed grade with a maximum frequency of 410 MHz. Knowing that this frequency easily degrades with routing, there is no way to achieve 800 MHz. The same applies to the Virtex-7 device.

So, with a real frequency, your results are no better than the previous works.

Response: Thank you very much for the comments.

In an FPGA design, throughput is proportional to the frequency at which the FPGA runs; being able to run the FPGA at a higher frequency results in higher throughput. The highest frequency is limited by the combinational logic and routing delays. These delays are eliminated by adding registers between the logic, which raises the maximum frequency and consequently the throughput. Pipelining is the term for this technique, and used in the proposed method for both parallel AES cores.

Since the implementation considered both the modern FPGA hard-cores (DSPs (DSP48E and DSP48E1) and BRAMs) and also the traditional FPGA logic elements (LUTs and related logic elements) together, the maximum frequency recorded is the overall frequency achieved for the implementation of the algorithm based on the FPGA resources from both categories, and not limited to the capabilities of the hard-cores only.

Regarding the higher frequency impact on constrained IoT devices, it is noted that IoT network may consist three different layers including, the Cloud computing layer, Fog computing layer and end-devices layer. This means that it consists both high performance and constrained platforms. High performance layers require high throughput AES, while constrained devices use lightweight and compact architectures with lower throughput. So, the achieved results will target these different requirements and not only the constrained devices.

Regarding the speed-grade, for high throughput outcomes, speed-grade -3 is used.

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 Editors'/Reviewers' commitments and warm work earnestly, and hope that the corrections will meet the expected requirements.

Thank you again!

Best regards,

sincerely,

Abiy Tadesse,