Paper Review: Optimized SM4 Hardware Implementations for Low Area Consumption

Jiahao Xiang

February 9, 2024

1 Review Comments

This paper introduces new, compact hardware architectures for the SM4 cipher, realized by minimizing the data path. The authors suggest two unique methods, "split-and-join" and "off-peak and stagger". These methods improve the usability of SM4 in environments with limited resources, allowing the cipher to function efficiently with low area usage. However, there are some errors in the figures and tables, and certain sentences are confusing. Here are some comments on the paper:

1. Section 1: The references to SIMON[3] and SPECK are unclear. Please clarify the reference for SPECK.
2. It would be helpful to add a table illustrating the differences between M-I, M-II, and M-III. The current numerical representation is hard to understand.
3. Section 2 (SM4): The details of the SM4's sbox are missing. Please include these details.
4. Section 3: Consider reorganizing the "Design and Analysis" section. Grouping the design and implementation together might make the design easier to understand.
5. Figure 2 needs a more detailed explanation. Some arrows associated with the XOR gate are missing.
6. The title of Figure 5 is incorrect. It should refer to both linear and non-linear transformation.
7. Table 1 should include the area consumption of the multiplexer.
8. Table 2: The S-box is loaded twice. Please clarify this with a footnote.
9. Figure 22 has an error in the middle subfigure and the third row. It currently reads "X35 X35", but it should be "X35 X33".

10. Table 7: The throughput is consistent across different frequencies. This is unusual for SM4-32bit and SM4-4bit on the SMIC 180 nm. Please provide an explanation if this is the case.