Paper Review: High-speed Hardware Architecture of KLEIN Cipher for IoT Image Encryption Applications

Jiahao Xiang

December 30, 2023

1 Review Comments

This paper introduces a high-speed hardware architecture, designed specifically for the KLEIN cipher, with a focus on image encryption applications within the Internet of Things (IoT) domain. The authors have successfully implemented the proposed architecture on both FPGA and ASIC platforms and have included an analysis of image security. However, there are concerns regarding the originality of the work and the comparison of experimental results, among other issues. Consequently, a major revision is recommended. The specific points for revision are as follows:

1. The first contribution includes an implementation that supports both encryption and decryption, a fundamental requirement for symmetric ciphers. However, the strategy of using multiple mutexes under control signals to direct the data flow for encryption or decryption is not unique, as it is also employed in other ciphers.

2. Furthermore, a more efficient implementation method is discussed in [1], which carries out the same MixColumn operation using a greater number of logic gates. It would be beneficial for the authors to compare the performance of these two implementations.

3. In Section 5.1, "Results for FPGA Implementation", the authors compare their implementation with another KLEIN implementation proposed in [2]. However, they only compare their work with Design 1 from [2], neglecting to compare it with Design 2. Given that Design 2 has a higher throughput (speed) than Design 1, the comparison with only Design 1 seems unfair.

4. In Section 5.2, "Results for ASIC Implementation", Figure 8 compares the throughput at a frequency of 100KHz for different ciphers. However, a comparison using the maximum frequency would be more beneficial.

At a specific frequency, throughput is mainly about latency. Therefore, the current comparison does not sufficiently demonstrate the high-speed advantage of the proposed design.

5. There are some issues with the figures and tables. In Figure 1, some symbols are missing, for example, the data flow in front of the $X4 << 1$. Additionally, an explanation for 'A' is needed. Table 6 could be removed, as it does not contain any comparative data.

6. The paper's structure could benefit from some improvements. Currently, the logical progression is from IoT to lightweight cryptography, then to cryptography, back to lightweight cryptography, then to hardware implementation, and finally to the KLEIN cipher. A more streamlined structure might be: IoT, cryptography, lightweight cryptography, hardware implementation, and then the KLEIN cipher. Furthermore, Sections 3.1 "Modification in Mix column" and 3.2 "Proposed Enc-Dec Architecture" appear to be discussing topics at different levels of detail.

7. Lastly, the references used are not recent. It is suggested that some newer references from the past three years be included.

References

[1] Karim Shahbazi and Seok-Bum Ko. Area-efficient nano-aes implementation for internet-of-things devices. *IEEE Trans. Very Large Scale Integr. Syst.*, 29(1):136–148, 2021.

[2] Pulkit Singh, B. Acharya, and R. K. Chaurasiya. High throughput architecture for klein block cipher in fpga, 2019.