Efficient Implementations of CRAFT Cipher For Internet of Things-v1.16.0-Revise

Ms. Ref. No.: **COMPELECENG-D-24-00145**
Title: Efficient Implementations of CRAFT Cipher For Internet of Things
Corresponding author: Professor lang li

Reviewer #1: Good paper. Talk briefly about side channel attacks. Address the comments below for another revision.

The paper is moderately drafted, some comments:

A) References are not uniformly formatted.

B) Please add comparisons in a table (or subsection) so that one could fairly compare your work with similar previous works.

C) Papers related to crypto need to consider this: With the advent of post-quantum cryptography, it is better to add some relevant papers including the followings to make sure you cover that topic too. When PQC replaces ECC/RSA every security application from smart phones to block chains will be affected. So mention about PQC and its threats adding these 4 papers:

**High-performance fault diagnosis schemes for efficient hash algorithm blake, 2019 IEEE 10th Latin American Symposium on Circuits & Systems (LASCAS).

** CRC-oriented error detection architectures of post-quantum cryptography niederreiter key generator on FPGA, 2022 IEEE Nordic Circuits and Systems Conference (NorCAS), 2022.

**Error Detection Schemes Assessed in FPGA for Multipliers in Lattice-Based Key Encapsulation Mechanisms in post-quantum cryptography, IEEE Transactions on Emerging Topics in Computing, 2022.

**Hardware Constructions for Error Detection in WG-29 Stream Cipher Benchmarked on FPGA, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, to appear.

D) Again, any crypto paper needs to address this: Also add some previous works on side-channel attacks and lightweight cryptography or PQC. These attacks are critical when you want to implement your security and privacy usage model, mention these works:

**Education and Research Integration of Emerging Multidisciplinary Medical Devices Security, American Society for Engineering Education (ASEE), 2016.

**Multidisciplinary Approaches and Challenges in Integrating Emerging Medical Devices Security Research and Education, American Society for Engineering Education (ASEE),

2016.

**Fault Detection Schemes for High Performance VLSI Implementations of the Advanced Encryption Standard, The University of Western Ontario, 2007.

E) You could add a subsection for Discussions

F) Please add one or more future works for enhancing your presentation

G) Moreover, some works missing on lightweight cryptography LWC and building blocks. Implementations need to be low-energy and low-power, so it is essential to mention about such efficient ways to pursue with implementations using these 4 references:

** Optimized architectures for elliptic curve cryptography over Curve448, Cryptology ePrint Archive, 2020.

**Reliable architectures for finite field multipliers using cyclic codes on FPGA utilized in classic and post-quantum cryptography, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 31 (1), 2022.

**Work-in-progress: Hyflex hands-on hardware security education during covid-19, 2022 IEEE World Engineering Education Conference (EDUNINE).
arXiv preprint arXiv:2306.08178

**Guest Editorial: Introduction to the Special Section on Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures, IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2016.

- With the advent of post-quantum cryptography (PQC), it is better to add some relevant works to make sure you cover that topic too. This is the hottest topic in cryptography now. With PQC, add a paper on each of these six topics separately: (a) Curve448 and Ed448 on Cortex-M4, (b) SIKE on Cortex-M4, (c) SIKE Round 3 on ARM Cortex-M4, (d) Kyber on 64-Bit ARM Cortex-A, (e) Cryptographic accelerators on Ed25519, (f) Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM.

- NIST lightweight standardization was finalized in Feb. 2023. Also mention fault attacks as side-channel attacks, these topics to explore and add a reference on each of these separately: (a) Error Detection in Lightweight Welch-Gong (WG)-Oriented Streamcipher WAGE, (b) error detection reliable architectures of Camellia block cipher, (c) fault diagnosis of low-energy Midori cipher, (d) block cipher QARMA with error detection mechanisms.

Reviewer #2: The authors present two serial and unrolled architectures of CRAFT and effectively reduce area resources by optimizing the S-box and Mix-Columns of CRAFT. Overall, the quality of the paper is good.

Reviewer #3: This work implemented the CRAFT block cipher with two architectures proposed, the Serial architecture and the Unrolled architecture. Then, the efficiency of the implementations is tested on three FPGA platforms. The implementations proposed in this paper are interesting for the practical applications of CRAFT in IoT.

1. The reference format should be consistent with equations, such as, 'as shown in Equation 1' -> 'as shown in Equation (1)'.
2. The description of IA is not necessary to occupy a single subsection (Subsection 3.3). It is better to move it to Preliminaries. Meanwhile, the comparison between the IA, SA, and UA is not sufficient.
3. The definitions of SA and UA are not explicit, especially the implementation under UA. It is necessary to highlight their innovativeness in relation to previous architectures.
4. Can CRAFT be implemented under the Iterative architecture? If so, do implementations under UA or SA still have advantages over IA? On the other hand, can UA or SA be applied to other ciphers, such as PRESENT, and bring efficiency improvements?
5. It is better to combine the Section 4 with Section 5 in my opinion.
6. The data in Figure 9-13 is also demonstrated in Table 5-7, one approach is enough to compare the results.