# Response to the Reviews

**Title: Efficient Implementations of CRAFT Cipher For Internet of Things**

**Manuscript Reference Number:**
**COMPELECENG-D-24-00145**

**Authors:**
Jiahao Xiang
Lang Li

Date: February 12, 2024

# Message from the Authors

Dear Editors and Reviewers,

We appreciate your constructive comments, which have significantly enhanced our manuscript. Each comment has been addressed, and your valuable suggestions have been included in the revised manuscript. The manuscript has been updated accordingly. For clarity, all updates have been colored in blue to distinguish them from the original content.
We have addressed each comment individually in the detailed response that follows. Each comment we received is boxed for clarity, with our responses written immediately after. Please note that all page and reference numbers in our response correspond to the revised manuscript, unless stated otherwise. The page and reference numbers in the reviewers' comments remain as they were in the original manuscript. We eagerly await your feedback and hope that our revisions meet your satisfaction.

Sincerely,
Jiahao Xiang and Lang Li.

# Response To Reviewer #1

## Overall Comments

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

### Response

We greatly value your detailed feedback and careful review. In response to your suggestions, we have expanded our discussion on side channel attacks. Additionally, we have included relevant references to support this new content. We trust that these revisions satisfactorily address your concerns.

---

### Reviewer Comment

> Reviewer # 1.1 - References are not uniformly formatted

### Response

We appreciate your feedback. We have meticulously reviewed the .bib file and the references, and made the necessary adjustments to ensure uniform formatting. We believe these revisions adequately address the concerns.

---

### Reviewer Comment

> Reviewer # 1.2 - Please add comparisons in a table (or subsection) so that one could fairly compare your work with similar previous works.

### Response

Thank you for your suggestion. In response, we have added a new table in the Results section of our revised manuscript. This table offers a comprehensive comparison between our work and similar previous studies. We trust that this addition effectively addresses your concerns. The detailed revisions are as follows:

add compare table in here

---

### Reviewer Comment

> Reviewer # 1.3 - 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.

### Response

We value your feedback. Accordingly, we've added a discussion about post-quantum cryptography in the Introduction section of our updated manuscript. To support this new content, we've also included pertinent references. We believe these modifications adequately address your concerns. The detailed revisions are as follows:

XXXX detailed revisions XXXX

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

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

[xx] 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.

[xx] 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.

---

### Reviewer Comment

Reviewer # 1.4 - Again, any crypto paper needs to address this: Also add some previous works on side-channel attacks and lightweight cryptography or PQC.

### Response

We appreciate your expert suggestion. In response, we have expanded our discussion to include previous works on side-channel attacks and have added relevant references to support this content. We trust that these modifications adequately address your concerns. The detailed revisions are as follows:

detailed content of SCA in Introduction

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

[xx] Multidisciplinary Approaches and Challenges in Integrating Emerging Medical Devices Security Research and Education, American Society for Engineering Education (ASEE), 2016.

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

---

### Reviewer Comment

Reviewer # 1.5 - You could add a subsection for Discussions.

### Response

We value your expert suggestion. In response, we have added a Discussions section to improve the quality of our manuscript. The detailed revisions are as follows:

section of discussion

---

### Reviewer Comment

> Reviewer # 1.6 - Please add one or more future works for enhancing your presentation

### Response

We appreciate your insightful suggestion. In response, we have included a discussion of potential future work in the Discussions section to enhance the quality of our manuscript. The detailed revisions are as follows:

future work, section of discussion

---

### Reviewer Comment

> Reviewer # 1.7 - Moreover, some works missing on lightweight cryptography LWC and building blocks.

### Response

We value your insightful suggestion. In response, we have included the previously missing implementation work and added the necessary references to support this addition. The detailed revisions are as follows:

similar work on the introduction

[xx] Optimized architectures for elliptic curve cryptography over Curve448, Cryptology ePrint Archive, 2020.

[xx] 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.

[xx] Hyflex hands-on hardware security education during covid-19, 2022 IEEE World Engineering Education Conference (EDUNINE). arXiv preprint arXiv:2306.08178

[xx] Introduction to the Special Section on Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures, IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2016.

---

# Response To Reviewer #2

## Overall Comments

Reviewer # 2 - Overall Comments here

### Response

We would like to thank you for you positive feedback. Your detailed comments have considerably helped with improving the clarity of the revised manuscript.

---

## Reviewer Comment

Reviewer # 2 - First Comment here

### Response

Your Response here. We modified the introduction as

> "We further performed simulations in which the topology changes are based on the robots' proximity. Since performance was similar to the results presented here, we do not report the results.

---

## Reviewer Comment

- Reviewer # 2 - Second Comment here

### Response

Your Response

---

## Reviewer Summary

Reviewer # 2 - Summary if present here

### Response

Your Response

---

# Response To Reviewer #3

## Overall Comments

Reviewer # 3 - Overall Comments here

### Response

We would like to thank you for you positive feedback. Your detailed comments have considerably helped with improving the clarity of the revised manuscript.

---

## Reviewer Comment

Reviewer # 3 - First Comment here

### Response

Your Response here. We modified the introduction as

> "We further performed simulations in which the topology changes are based on the robots' proximity. Since performance was similar to the results presented here, we do not report the results.

---

## Reviewer Comment

- Reviewer # 3 - Second Comment here

### Response

Your Response

---

## Reviewer Summary

Reviewer # 3 - Summary if present here

### Response

Your Response

---