# Commit

Ms. Ref. No.: COMPELECENG-D-24-00145R1

Title: Efficient Implementations of CRAFT Cipher For Internet of Things

Corresponding author: Professor lang li

Dear Professor li,

Following are the reviews for your paper referenced above. I invite you to revise your paper based on the reviewers' comments.

In preparing the revised version, please pay careful attention to the following instructions to prevent delay in processing.

\* EDIT THE PAPER CAREFULLY. It is recommended to use a professional native English-speaking editor. Papers with less than excellent English will not be published even if technically perfect. You will be given only one chance to improve the English writing!

\* Up front in your revised paper, describe how the comments of each reviewer are addressed.

\* Include a list of four to ten key words after the Abstract.

\* Make sure the Abstract succinctly describes the paper as it is used in abstracting and citation services. Keep the Abstract to about 200 words.

\* Make sure the Conclusion succinctly summarizes the paper. It should not repeat phrases from the Introduction! Keep the Conclusion to about 300 words.

\* Spell out each acronym the first time used in the Abstract as well as in the body of the paper.

\* Number references sequentially as they are used in the text (not alphabetically). Each reference must be referred to in the text. Limit the number of references to about 25 (but no more than 30) strongly relevant and recent ones. Provide complete information for all references (authors' names, journal name, pages, etc.; do not use et al for authors).

IMPORTANT: You do not need to include any reference(s) recommended by the reviewers if not strongly relevant and up to date. If a reviewer recommends rejection of your revised paper for not including the recommended reference(s), please inform me by email.

\* Make sure all figures and tables are referred to in the text.

\* Keep the paper size within 25 double-spaced pages (with font no less than 10), including any tables and figures.

\* Submit the revised version within 30 days independent of what the system shows.

Note: If our iThenticate system shows similarity of 25% or more between your submitted paper and published material, your paper will be rejected.

I look forward to receiving your revised manuscript.

Sincerely,

Debiao He

Editor-in-Chief

Computers and Electrical Engineering

Reviewer #1: Most of my comments are addressed but I advise you to add recent surveys on PQC to the paper and comment that you algorithm using Grover's still will be secure see below:

Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities

2023/10/18

Source

arXiv preprint arXiv:2310.12037

Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security

2023/5/22

Source

arXiv preprint arXiv:2305.13544

Reviewer #2: I recommend that the paper can be accepted.

Reviewer #3: I think this manuscript has been well revised and can be accepted.