Dear Editor and Reviewers:

Thank you for your letter and the reviewers’ comments concerning our manuscript entitled "Efficient Implementations of CRAFT Cipher For Internet of Things" (ID: COMPELECENG-D-24-00145). We have reviewed your comments carefully and made corrections in accordance with them. We have revised portion marked in blue in our paper. We hope our revised manuscript can be accepted for publication.

The main corrections and responses to the comments are shown as below:

Response to the reviewers’ comments:

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

Response: We have included recent surveys on Post-Quantum Cryptography (PQC) in our paper and noted that our algorithm, which uses Grover's method, maintains security. The detailed revision is as follows:

Although quantum computing has enhanced capabilities to attack ciphers, as highlighted by Darzi et al. [27] and Canto et al. [28], it’s noteworthy that the probabilistic algorithm based on quantum computing, proposed by Grover et al. [29], could reduce the key space from 128-bit to 64-bit. However, this reduction is not sufficient to brute force attack the CRAFT cipher with current computational capabilities.

[27] S. Darzi, K. Ahmadi, S. Aghapour, A. A. Yavuz, M. M. Kermani, Envisioning the future of cyber security in post-quantum era: A survey on PQ standardization, applications, challenges and opportunities, CoRR abs/2310.12037 (2023). arXiv:2310.12037, doi:10.48550/ARXIV.2310.12037.

[28] A. C. Canto, J. Kaur, M. M. Kermani, R. Azarderakhsh, Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security, CoRR abs/2305.13544 (2023). arXiv:2305.13544, doi:10.48550/ARXIV.2305.13544.

[29] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96, STOC '96, ACM Press, 1996. doi:10.1145/237814.237866.

We tried our best to improve the manuscript and made some changes in the manuscript. These changes will not influence the main content and framework of the paper. Thank you very much for your comments and suggestions.

Best regards,

Lang Li