Review Form 3

Journal Name:	**Archives of Current Research International**
Manuscript Number:	**Ms_ACRI_131412**
Title of the Manuscript:	**Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate 'Harvest Now, Decrypt Later' Attacks**
Type of the Article	

PART 1: Comments

	Reviewer's comment **Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.**	**Author's Feedback** *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Please write a few sentences regarding the importance of this manuscript for the scientific community. A minimum of 3-4 sentences may be required for this part.	It is an interesting and helpful article. The general presentation is very legible, correct and full of interesting data. Some details should be corrected but there is no fundamental objection over this paper. With minor revision, it would be acceptable for publication.	
Is the title of the article suitable? (If not please suggest an alternative title)	The title is suitable.	
Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.	Remove numerical results from the abstract, they should not be included to improve readability.	
Is the manuscript scientifically, correct? Please write here.	The manuscript is correct, no objections made.	
Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.	The references are recent, but they should include classical attacks published about (NIST PQC) ML-CRYSTALS-KYBER as mentioned in my review report below. Additionally it is suggested to change references to IEEE format.	

Review Form 3

Is the language/English quality of the article suitable for scholarly communications?	Yes, the article is suitable and well written.	
Optional/General comments	**Observations that should be corrected:** • Remove numerical results from the abstract, they should not be included to improve readability. • It is recommended to change the references in the text. To do so, each bibliography cited at the end should be numbered in square brackets and those numbered brackets should be inserted in the text to reference the paragraphs, instead of using name and year of reference (IEEE Standards). • When mentioning CRYSTALS-Kyber (FIPS 203) as a promising solution proposed by NIST, it is necessary to point out that there must be continuous monitoring on the proposed standards given the constant threat of classical cryptanalytic attacks [1-22]. One must be very careful in betting on a specific PQC solution as a panacea (even if it is recommended by NIST), the evidence is there for all to see. For example, alternative PQC solutions for KEM protocols not based on LWE lattices and purely algebraic in nature are being developed (it is suggested to explore cs.CS preprints in arXiv of recent appearance). • The expression “PQC adoption (P(A)P(A)P(A)P(A)) ?” is not understood, please clarify. • Are the equations mentioned in methodology and the consequent statistical analysis all original or should they be referenced? • In Table 1 it is convenient to include in the description the size of the plain text and the detail of the hardware used to obtain these data. • In Figure 1 the units of measurement of the ordinate axis are missing. • In Figure 2 it is recommended to change the bullets or highlight the colors because they are not legible. • In Table 2, add the reference of the origin of the data. • In Figure 4 it is recommended to change the plotting to a more understandable system. • In Table 3 add the data source reference. • In Table 4 add the data source reference. • In Figure 6 add data source reference. • In Table 5 add data source reference. **References cited here (locate pdf’s with Google Scholar)** [1] 2022-Ma-Vulnerable PQC against Side Channel Analysis on Kyber.pdf [2] 2022-Park-PQC-SEP-Power Side-channel Evaluation for PQC algorithms.pdf [3] 2023-Grunfeld-Side-Channel Attacks on CRYSTALS.pdf [4] 2023-Ji-A Side-Channel Attack on a Masked Hardware KYBER.pdf [5] 2023-Rajendran-Pushing the limits of generic side-channel attacks on KYBER.pdf [6]2023-Rodriguez-Correlation Electromagnetic Analysis on an FPGA Implementation of CRYSTALS-Kyber.pdf [7] 2023-Wang-A Side-Channel Attack on a Bitsliced KYBER.pdf [8] 2024-Ravi-Defeating Low Cost Countermeasures against SCA on KYBER.pdf [9] 2019-Qin-An Efficient Key Mismatch Attack on the NIST Candidate KYBER.pdf [10] 2020-Sim-Single-Trace Attacks on Message Encoding in latice-based KEMs.pdf [11] 2021-Hamburg-Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber.pdf [12] 2021-Hermelink-Fault-Enabled Chosen-Ciphertext Attacks on KYBER.pdf [13] 2021-Okada-Recovery Attack on Bob's Reused Randomness in Crystals-Kyber.pdf [14] 2021-Xagawa-Fault-Injection Attacks against NIST's PQC candidates.pdf [15] 2022-Azouaoui-Systematic Study of Decryption and Re-Encryption Leakage on KYBER.pdf [16]2022-Sim-Chosen-Ciphertext_Clustering_Attack_on_CRYSTALS-KYBER.pdf [17]2023-Backlund-Secret Key Recovery Attacks on Masked and Shuffled KYBER.pdf [18]2023-Jendral-A Single-Trace Message Recovery Attack on CRYSTALS-KYBER.pdf	

Review Form 3

	[19] 2023-Kuo-A Lattice Attack on CRYSTALS-Kyber with CPA.pdf [20] 2023-Li-Overview and Discussion of Attacks on CRYSTALS-KYBER.pdf [21]2024-Iavich-Investigating CRYSTALS-Kyber Vulnerabilities-Attack Analysis.pdf [22] 2024-Ravi-Generic_Message_Recovery_Attacks_on Kyber.pdf	

PART 2:

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Are there ethical issues in this manuscript?	*(If yes, Kindly please write down the ethical issues here in details)*	

Reviewer Details:

Name:	**Juan Pedro Hecht**
Department, University & Country	**University of Buenos Aires, Argentina**