I. Research Problem and Objectives

A. Problem Being Addressed

The article addresses the critical need to secure modern smartphones against quantum computing threats while maintaining compatibility with current cryptographic systems [1]. The research problem focuses on analyzing Samsung's Quantum Galaxy implementation, which integrates both Quantum Random Number Generation (QRNG) and Post-Quantum Cryptography (PQC) techniques to enhance mobile device security. This problem is highly relevant as quantum computers pose an existential threat to current RSA and ECC-based encryption schemes. The clarity of the problem is well-established through the investigation of both the security mechanisms employed and their practical implementation on consumer mobile devices, making it accessible and important for the cybersecurity and mobile technology communities.

B. Research Objectives and Hypothesis

The primary research objectives are to:

II. Article Analysis

The analysis of the article will be make through the answers to the questions on the *template* that was provided by the professor.

A. What is the name of the research?

The name of the research is "Unveiling Samsung Quantum Galaxy: Securing Smartphones With Quantum and Post-Quantum Cryptography".

B. Where the research was published?

The research was published in the journal "IEEE Access", which is a multidisciplinary, open access journal of the Institute of Electrical and Electronics Engineers (IEEE).

C. Who is the author?

The name of the author is Omar Alibrahim, a researcher with support from Kuwait Foundation for the Advancemente of Sciences (KFAS). The research was published on 2nd of May 2025.

D. What's the theory of research?

The theory of research is based on the integration of quantum tecnologies in enhancing mobile communication security, all thanks to the new features of the Samsung Galaxy Series.

E. What's the problem being addressed in this study?

The study explains that Samsung has a lack of effective implementation of Quantum Random Number Generator (QRNG) utilization in existing applications, something that could enhance security in mobile communications.

F. What are the objectives addressed?

The author has addressed this gap by developing a secure instant messaging and VoIP application that combines QRNG with post-quantum cryptographic algorithms.

G. What are the study's strength points?

The study's strength points are how the author has managed to take advantage of the already existing hardware in the Samsung, and showing how it can be used to improve security in mobile comunications, specially in instant messaging and VoIP applications, by that is a solid and possible solution for the future of mobile security without making the user waste more money when you can use the already existing hardware.

H. What are the study's weaknesses?

The study's weakness, is more a defect of Samsung than the author, because the QRNG chip is very strong theorically, but is weak in practice, because when it was tested with NIST SP800-22 and Dieharder, it can generate very "1" bits in a row or alternating "0" and "1" bits, which isn't good for a random number generator, because it can be predicted by an attacker.

And this makes a problem for the author, because if the QRNG isn't good, the security of the applications that use it, can be compromised and won't be as secure as it should be theoretically.

I. Which type of methodology was adopted?

The methodoly adopted was a dissection of the Samsung Quantum Galaxy's security features, focusing on the integration of QRNG and PQC in mobile applications. That was done through digital forensics at the phone's file system and reverse engineering of its binaries and Android applications, where they discovered the mechanisms to invoke the chip's random byte generation capabilities.

To be more specific, the author planned a three-phase approach:

- ***Discover***: Understand how the QRNG is integraded and how it can be accessed by applications.
- ***Research***: Evaluation of QRNG chip's performance, assets its randomness quality, and investigate its utilization in existing mobile applications.
- ***Development***: After discovering that no meaningful use of the QRNG was being made, the author developed a secure instant messaging and VoIP application that combines QRNG with post-quantum cryptographic algorithms.

J. Briefly explain the variable of analysis used on this study.

The study used three test suites to evaluate the randomness quality of the QRNG chip:

- ***NIST SP800-90b***: A standard for the generation of random numbers using deterministic and non-deterministic methods.
- ***NIST SP800-22***: A widely used suite of statistical tests for evaluating the randomness of binary sequences.
- ***Dieharder***: A comprehensive suite of statistical tests for random number generators, providing a more extensive analysis of randomness quality.

K. Critically analyze the presented results

As we said before, the QRNG chip used in the Samsung Quantum Galaxy has some problems when it comes to randomness quality, because when it was tested with NIST SP800-22 and Dieharder, so the results presented by the author are good and represent a good step forward in mobile security, whoever it is limited by the quality of the QRNG chip used in the phone, because if the QRNG isn't good, the security of the applications that use it. We are sure that if the QRNG chip was better, the results would be even better. After all, the author was honest about the problems of the QRNG chip, so we can trust the results presented.

L. What are the conclusions presented by the author?

The solution/conclusion that the author has achieved demonstrates that leveraging QRNG-generated randomness alongside PQC significantly improves security against emerging quantum threats, establishing a foundation for enhanced mobile data protection.

M. What is the contribution to the existing knowledge?

It shows that the integration of QRNG and PQC in mobile applications is feasible and can be effectively implemented using existing hardware, paving the way for future advancements in mobile security technologies.

N. Summarize your conclusion on the analyzing the benchmark.

O. What is the main gap that you have identified on this study, and that you are willing to address on your research?

P. Which part of the benchmark will you use in your study, in order to compare your results with their outcomes?

Q. Conclude by summarizing the Research Problem + Research Gap+ Purpose of the study (MAXIMIUM 40 WORDS)

References

[1] O. Alibrahim. "Unveiling samsung quantum galaxy: Securing smartphones with quantum and post-quantum cryptography." IEEE Access, vol. 13, pp. 73202 - 73218, 2025, Accessed: Jan. 21, 2026. [Online]. Available: https://ieeexplore.ieee.org/document/10974970