

Abstract—This paper presents a comprehensive analysis of Samsung’s Quantum Galaxy framework [1], which integrates Quantum Random Number Generation (QRNG) and Post-Quantum Cryptography (PQC) techniques to enhance mobile device security against emerging quantum computing threats. Through reverse engineering, digital forensics, and cryptographic analysis, we evaluate the effectiveness of these quantum-resistant mechanisms on commercial smartphone hardware. Our findings demonstrate that quantum-resistant cryptography is not only theoretically sound but also practically viable for widespread mobile device deployment, offering enhanced security while maintaining compatibility with existing communication standards. We discuss the methodology, present key findings regarding the integration of QRNG and PQC, and critically evaluate the research limitations and future directions for quantum-safe mobile security.

Index Terms—Quantum random number generator (QRNG), post-quantum cryptography (PQC), reverse engineering, digital forensics, secure mobile communications, mobile application security, quantum-resistant cryptography.

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 made 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 Advancement 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 technologies 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?

H. What are the study’s weaknesses?

I. Which type of methodology was adopted?

J. Clearly identify the adopted research design method.

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

L. Clearly identify the criteria/equations that were used to validate results.

M. Critically analyze the presented results

N. 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.

O. What is the contribution to the existing knowledge?

P. Can you accept the findings as true? Discuss any failing and shortcomings of the method used to support the findings.

Q. Summarize your conclusion on the analyzing the benchmark.

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

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

T. Conclude by summarizing the Research Problem + Research Gap+ Purpose of the study (MAXIMUM 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>