Unveiling Samsung Quantum Galaxy: Securing Smartphones With Quantum and Post-Quantum Cryptography

Martinho José Novo Caeiro (23917) and Paulo António Tavares Abade (23919)

I. Research Problem and Objectives

A. Problem Being Addressed

This article addresses the critical need to secure modern smartphones against quantum computing threats while maintaining compatibility with current cryptographic systems [1]. The research 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 research 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.

II. Article Analysis

This article will be analyzed by answering the questions on the *template* provided by the professor.

A. Basic Research Information

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

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

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.

B. Research Theory

The theory behind the 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.

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.

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

C. Strengths and Weaknesses

The study's strength points are based on how the author has managed to take advantage of the already existing hardware in Samsung Devices, and showing how it can be used to improve security in mobile communications, 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.

The study's weakness are based on a Samsung defect rather than the author, because the QRNG chip is very strong theoretically, but is weak in practice, because when it was tested with NIST SP800-22 and Dieharder, it can generate loads of ”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 it difficult 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.

D. Adopted Methodology

The methodology 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

Both authors are with the Instituto Politécnico de Beja, Escola Superior de Tecnologia e Gestão, Mestrado em Engenharia de Segurança Informática, Beja, Portugal. Supervisors: Rui Miguel Silva and Daniel José Da Graça Peceguinha Franco.

combines QRNG with post-quantum cryptographic algorithms.

E. Benchmark Used

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.

F. Results Presented

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 aren't going to be solid. 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.

G. Conclusions Presented

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.

H. Contribution to 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.

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