UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Seminar

Friday October 13, 2023 at 1PM in Reynolds 1101

Vaideeshwaran Saravanan

Using Complex Number Algebra to alleviate threats of Contemporary Cryptography from Shor's Quantum threat

Advisor: Dr. Charlie Obimbo
Advisory: Dr. Ritu Chaturvedi

Abstract:

As technology continues to advance, the need for robust data protection through cryptography has become increasingly vital. The purpose of cryptography is to ensure the confidentiality, integrity, and authenticity of data, especially during transmission or storage, in the presence of potential adversaries. However, the intensified rise of quantum computing, accompanied by quantum algorithms like Shor's algorithm, which can quickly factorize large numbers, presents a significant threat to classical encryption systems, such as RSA, which rely on the difficulty of prime factorization.

This research is centred on developing alternative methodologies to enhance security and prepare the technology for the post-quantum era. Our research is based on Post-Quantum Cryptography, and rather than relying solely on prime factorization, our algorithm uses complex number algebra that can withstand quantum attacks with proper testing, and with a focus on seamless transitions from vulnerable cryptographic systems. By exploring these alternatives, we aim to contribute to the ongoing evolution of cryptography and its resilience in an increasingly complex digital landscape.