Classical vs Quantum: What does the future hold for fully homomorphic encryption schemes?

Richard Omollo, Jackson Odote and Bernard Okello
Jaramogi Oginga Odinga University of Science and Technology, Kenya.
Technical University of Kenya, Nairobi, Kenya.

The construction of homomorphic encryption schemes has supported arbirtrary computations on outsourced data, without revealing their true contents. Recent introduction of fully homomorphic versions has further improved the remedy to security challenges that affect data especially when not in custody of its owners, by supporting computations including those of higher polynomials functions. Despite these positive developments, implementation of these fully homomorphic encryption schemes has impacted negatively on the computing resources. These developments also have been made both for classical computing systems that are based on assumed hardness of mathematical problems and quantum computing systems that are based on Heisenberg principle. This paper aim at comparing the two sets of fully homomorphic encryption schemes: classical and quantum, with a view of providing future state-of-the-art of computational needs on management of consumer data. The output of this paper shall be useful not only to the scholarly world but also to the production units that shall desire to adopt a more efficient computational approach that inexpensively safeguard consumer data.

Keywords: Fully Homomorphic Encryption Scheme; Quantum; Data security