Abstract

Recent advances in the development of quantum computing hardware have accelerated the interest of preparing information systems for the post-quantum world. Grover's unstructured search and Shor algorithm for period-finding have potential applications in security, cryptography, and communications in general. We present in this paper the evaluation and simulation of proofs of concepts, gates, and experiments for quantum circuits along with explanations of their potential applications to computing and security. The circuits explore several aspects of quantum computers such as superposition, parallel calculations, amplitude amplification and phase estimation. These circuits and gates were also tested on real quantum computers to assess their behavior.