World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:17, No:05, 2023

A Real-World Roadmap and Exploration of Quantum Computers Capacity to Trivialise Internet Security

Authors : James Andrew Fitzjohn

Abstract : This paper intends to discuss and explore the practical aspects of cracking encrypted messages with quantum computers. The theory of this process has been shown and well described both in academic papers and headline-grabbing news articles, but with all theory and hyperbole, we must be careful to assess the practicalities of these claims. Therefore, we will use real-world devices and proof of concept code to prove or disprove the notion that quantum computers will render the encryption technologies used by many websites unfit for purpose. It is time to discuss and implement the practical aspects of the process as many advances in quantum computing hardware/software have recently been made. This paper will set expectations regarding the useful lifespan of RSA and cipher lengths and propose alternative encryption technologies. We will set out comprehensive roadmaps describing when and how encryption schemes can be used, including when they can no longer be trusted. The cost will also be factored into our investigation; for example, it would make little financial sense to spend millions of dollars on a quantum computer to factor a private key in seconds when a commodity GPU could perform the same task in hours. It is hoped that the real-world results depicted in this paper will help influence the owners of websites who can take appropriate actions to improve the security of their provisions.

Keywords : quantum computing, encryption, RSA, roadmap, real world
Conference Title : ICQCC 2023 : International Conference on Quantum Computing and Communication
Conference Location : London, United Kingdom
Conference Dates : May 15-16, 2023