Chapter 16
Future of Quantum Computing in Cyber Security

Geeta N. Brijwani
KC College, India

Prafulla E. Ajmire
GS College, India

Pragati V. Thawani
KC College, India

ABSTRACT

Quantum computing leverages the probabilistic nature of the universe to harness computing capabilities, superseding classical and even supercomputers to solve complex problems in areas including drug development, financial modelling, etc. It is all about metadata and algorithms. This chapter per the authors aims to examine the field quantum computing in the context of cybersecurity. Through a thorough study of the timeline of developments in cybersecurity, modern cybersecurity schemes have been examined and conclusions pertaining to their vulnerabilities due to the emergence of quantum computers have been drawn. Breaking modern cryptographic schemes is equivalent to solving the underlying mathematical problems that these schemes are based on, which can be significantly sped up with a quantum computer. Hence, this chapter conveys the need for enterprises to adopt post quantum cryptographic schemes, which are not easily vulnerable to attacks by a quantum computer.

INTRODUCTION

Quantum

Quantum is the smallest and a discrete physical entity in the universe. Study of quantum led to a new branch of physics known as “Quantum Mechanics”. It deals with the behaviour of particles at the subatomic level. Everything in the universe has a particle and wave nature. This forms the bedrock of

DOI: 10.4018/978-1-6684-6697-1.ch016

Quantum Mechanics which is largely based on the notion that the Universe is probabilistic in nature. Quantum Computers exploit the laws of Quantum mechanics to speed up computation substantially. It gives a Quantum Computer the power to solve problems that are generally intractable with a classical computer (Griffiths, 2023).

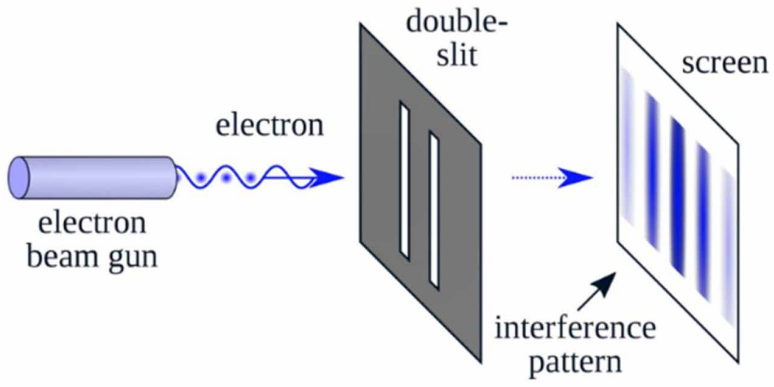
Computing

It refers to the act of performing calculation or computation using a computer. Investigating and testing algorithms, developing the hardware and software forms the basis of the idea of computing.

Quantum Technology

Unlike quantum technology, quantum computers run parallel computations. This technology works on quantum mechanisms (as discussed earlier in Section 1.1) with its superposition and entanglement.

Figure 1. Illustration of Thomas Young's Double Slit Experiment



Quantum Computing

Quantum Computing is defined as a technology which rapidly changes or emerges and a type of computation whose operations harness the laws i.e. rules of quantum mechanics to solve complex problems easily as compared to classic or normal usage computers.

Fundamental Concepts

Qubits

Qubits are the smallest unit of a Quantum Computer. A classical computer stores data in the form of bits which are discrete, i.e 1s and 0s. A bit can exist in only one of those two states at a time. However, the laws of quantum mechanics (Mainly, Superposition, Entanglement and Quantum interference) permit Qubits to exist in a combination of the two states (Gervin, 2011, p. 1).