Preface

Quantum computers from various established technology giants have demonstrated that they have the inherent potential to outperform classical computers in many areas. Especially in real-time analytics of big data, quantum computing (QC) has strongly established its superiority. Worldwide researchers in the past decade have built and deployed quantum computers for multiple use cases including homeland security, drug discovery, genome engineering, etc. Some researchers pursue quantum computing's potential to unlock the secrets of physics and to facilitate the development of new chemicals to aid the welfare of the humanity. Quantum computing is being increasingly used for artificial intelligence (AI) applications. With clouds being proclaimed as the one-stop IT solution for business automation needs, there is a rush of deploying quantum computers in cloud environments. Quantum computing as a service (QCaaS) is the latest service offering of cloud service providers.

The goal of this book is to facilitate and stimulate cross-disciplinary research initiatives and implementations in the cybersecurity domain due to the continuous advancements in the paradigm of quantum computing. Today, there are small-scale quantum computers getting produced and installed in hyperscale cloud environments in order to deliver quantum computing as a service. Industry professionals and academic researchers are able to access the distinct capabilities of quantum computing today without any hitch or hurdle. However, the rise of quantum computing has brought in a series of positive and negative implications. One of the major impacts is that the currently available cryptography algorithms are bound to be broken when a powerful quantum computer get built and released. Quantum computers can process big data easily. They can do computation thousands of times faster than the classical computers. Such a tremendous speed is being seen as a huge problem for traditional cryptographic algorithms. This book is to dig deep and dwell at length on the various impacts of quantum computing and how the impending challenges and concerns can be surmounted through quantum-resistant cryptography algorithms.

The main focus of this book is to bring all the related technologies, novel findings, and managerial applications of Quantum Information Science on a single platform to provide great readability, easy understanding, and smooth adaptability of various basic and advanced concepts to undergraduate and postgraduate students, researchers, managers, designers, academicians, and practitioners doing work in this domain.

https://doi.org/10.1515/9783110798159-202