Abstract

The introduction of Quantum Technologies (QTs) has a dual impact on cybersecurity: on the one hand, Quantum Computing jeopardises current classical public-key cryptosystems, such as RSA and ECDH, and on the other hand, Quantum Cryptography can be a powerful countermeasure against quantum attacks and also a building block for next-generation cryptography. The objective of this thesis work is to explore the current relationship between QTs and cybersecurity in three central aspects: the use of Quantum Cryptography and Quantum Key Distribution (QKD) to protect modern Software-Defined infrastructures (SDIs) against quantum attacks, the adoption of Quantum Annealing techniques to optimise SDIs that can be used as a mean to deploy and manage responsive on-demand network security services, and the analysis of the impact of Quantum Computing on current cryptosystems. As the first result of this work, the reader can appreciate the design and development of a software stack to integrate QKD in SDIs, the Quantum Software Stack (QSS). The QSS is a cloud-native application that can be easily integrated into SDIs and includes a QKD simulator based on a quantum circuit model simulation. A second result is the introduction of a generic Quadratic Unconstrained Binary Optimisation (QUBO) formulation to describe Virtual Network Functions Embedding Problems (VNFEPs). These optimisation problems are part of SDIs, and solving them helps telecommunication providers optimise the management of their infrastructures. The presented QUBO formulation has been validated using a quantum annealer, compatible with this type of formulation, and classical solvers. The final result, even if it can be considered as a preliminary study, regards the analysis of Shor's algorithm for solving Discrete Logarithm Problem (DLP) and Elliptic Curve DLP (ECDLP). The main objective is to analyse the available optimisation for Shor's algorithm and estimate the required resources to run it on real hardware. The implementation of the related quantum algorithms uses Qiskit as a toolkit for describing and simulating quantum circuits.