OUTSIDE THE BOX – THE "TAP" BOX

RISK ANALYSIS PERSPECTIVE ON THE EMERGENCE OF QUANTUM COMPUTING

An Undergraduate Thesis Portfolio

Presented to the Faculty of the

School of Engineering and Applied Science

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science in Electrical Engineering

By

William Sivolella

December 14, 2022

A SOCIOTECHNICAL SYNTHESIS

The emergence of quantum computers will drastically change the world and benefit it in many ways, but it will also pose security risks that will affect major institutions in society as well as the general population. The technical research will aim to research the direct solution to such security risks through finding optimal quantum-proof encryption algorithms. Meanwhile, the science, technology and society (STS) topic aims to create a proper analysis of when optimal quantum-proof algorithms will be implemented into societal institutions and if this implementation will occur before the emergence of practical quantum computers. This analysis will provide one with an understanding of the time window as well as the potential severity of the described security risk. After the technical research is complete, it will provide important evidence for the STS research and provide context for not only when the world will be able to begin the implementation of quantum-proof algorithms but also for how safe these algorithms will be.

The technical report will aim to find the current optimal quantum-proof encryption algorithms and understand how they work. The National Institute of Standards and Technology (NIST) is holding an open competition for individuals to submit their quantum-proof algorithms. This competition is a great resource to find the best algorithms and thoroughly analyze them. The technical research will create an understanding of how these algorithms work and how safe they are in order to properly determine the risk of the emergence of quantum computers. NIST will also standardize and approve of algorithms, which provides context for when institutions will begin to integrate these algorithms into their security systems.

One of the leaders in the NIST competition is International Business Machines (IBM) which has developed the algorithm Cryptographic Suite for Algebraic Lattices (CRYSTALS). This lattice algorithm is deemed quantum-proof for the following simplified explanation: there is a myriad of answers that fit the criteria for solving a CRYSTALS problem, but only one of those answers will actually decrypt what the algorithm is protecting since quantum computers can only produce one answer every time they are run. The winners of the competition are expected to be announced in the next two years, and by then the winners' algorithms will be approved and standardized for widespread implementation.

The STS research uses risk analysis, which is a form of Pinch and Bijker's Social Construction of Technology (SCOT) and provides a framework to understand the severity of the risks of quantum computing and whether or not the world will be ready for the emergence of quantum computers. By viewing the problem from the risk analysis perspective, it appears that quantum-proof algorithms will be integrated into society by the time useful quantum computers emerge. The major factors considered are when will quantum-proof algorithms be optimized, how long would it take for major entities to implement these algorithms into their security systems, when will quantum computers capable of hacking emerge and what are biases that could affect these factors.

Although there are some quantum-proof algorithms already in use, like IBM's CRYSTALS, most entities, especially non-tech entities, will not change their security infrastructure until these algorithms are modified and approved by a reputable source. The vast majority of sources predict NIST to release these algorithms by 2022 to 2024. Consultants at Accenture and experts at MIT Technology Review believe the implementation of these

algorithms will be completed by 2025-2028 and 2030-2040 respectively. Accenture and MIT Technology review also expect useful quantum computers will be present in society by 2025 and 2030 respectively. Although these projections expect a world that will have a small window of major security risks due to quantum computing, one can conclude that the world will be ready for quantum computers since tech industry public figures often underestimate the timing of new projects.

It is admirable that institutions like NIST have created a platform where anyone can contribute to solving the problem of protecting everyone's information. At an age where technology is improving exponentially, complications improve exponentially. Thus, society cannot just focus on current problems, but also need to prepare for future problems, which may have even greater consequences.

TABLE OF CONTENTS