# PROJECT PROGRESS REPORT

Student name: Ayush Keshar Prasai

Student name: Ronit Ashok Maheshwori

Student name: Jalay Shah

Student name: Virajsinh Jeetendra Sinh Rahevar

Unit: COIT20265

Unit mentor: Mohammed Mohammed

Unit coordinator: Fariza Sabrina

# Introduction

This progress report has been forged to relay information about the progress of tasks listed in the project plan. This progress report contains information regarding the individual contribution of team members on the tasks of the project with everyone contributing to production of at least one technical artefact to aid the project progress.

# GitHub link: https://github.com/ayush12198371/Quantum-Safe-Cryptography-Mitigating-Vulnerabilities-in-Post-Quantum-Era.git

# Technical artefacts

|  |  |
| --- | --- |
| Student | Technical Artefact |
| 1. Ayush Keshar Prasai | -Documentation of the report  -GANTT chart  -Kanban board |
| 1. Ronit Ashok Maheshwori | -Documentation of task 3, 5, 6. |
| 1. Jalay Shah | -presented descriptive list of present-day algorithms task 4 |
| 1. Virajsinh Jeetendra Sinh Rahevar | -Documented task 1 and 2. |

# Task completed

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| s/n. Tasks from the Project Plan | Deliverables | Student contribution | Start-Date of completion | Task progress |
| 1. Research post-quantum computational ability. |  | Virajsinh Jeetendra Sinh Rahevar/ Jalay Shah | 30/07/2024-05/08/2024 | 80% |
| 1. Outline post-quantum computational limit. |  | Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 30/07/2024-05/08/2024 | 80% |
| 1. Research present day computational ability | -vulnerability  -risks from threat actors | Ayush keshar Prasai/ Ronit Ashok Maheshwori | 10/07/2024-14/07/2024 | 80% |
| 1. List present day algorithms. | -present day cryptography  -algorithms in use | Jalay Shah/Ayush Keshar Prasai | 14/07/2024-16/07/2024 | 80% |
| 1. Outline present day computational limit. | -widely accepted vulnerabilities | Ronit Ashok Maheshwori/ Ayush keshar Prasai | 16/07/2024-19/07/2024 | 80% |
| 1. Compare present day computational limit to post-quantum computational ability. | limitation of modern computers  -post-quantum vulnerabilities list | Ronit Ashok Maheshwori/ Jalay Shah | 19/07/2024-23/07/2024 | 80% |
| 1. Review of the tasks completed | Draft documentation | Ronit Ashok Maheshwori/ Jalay Shah/ Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 24/07/2024-05/08/2024 | 40% |
| 1. Project Plan | Documentation | Ayush Keshar Prasai | 19/07/2024-24/07/2024 | 100% |
| 1. Progress report | Documentation | Ayush Keshar Prasai | 24/07/2024-05/08/2024 | 100% |

# Changed from Project Plan

As the project progresses, some of the key tasks assigned have been required to change in addition to the team member for this project group. With equally assigned tasks and expected outputs, the addition of team members has led to tasks being reassigned and scheduled to another completion date. Furthermore, progression of tasks has also brough upon attention to the need for REVIEW as an addition to the scheduled tasks where noncontributing team members of the task review completed tasks to add or remove information for draft documentation. The team believes that this process shall give more authenticity and integrity to the report thus forged.

1. Schedules:

Addition to the contributing team member has led to the need of rescheduling task at hand. The team, although clouded with uncertainty, has managed to assign tasks to the new team members so that they can contribute to the project with changes depicted in the Kanban board.

## Tasks:

New task Review has been added to the scheduled tasks from the project plan. The need for this task arose when all the team members contributed to the task, yet the authenticity and accuracy of the information relayed to the project had no means to be documented or represented. The task description and deliverable are listed below:

|  |  |  |
| --- | --- | --- |
| Task | Description | Deliverable |
| 1. Review | -cross checking accuracy of relayed information.  - new angle of thought on task at hand | -references  -authenticity to report  -availability of the report |

# Issues and challenges

It is expected for the project to face issues and challenges to come to a certain conclusion. Moreover, issues and challenges thus faced while on this report until this day has been taken by the team as a motivating factor to signify integrity to the contributions. Some of the issues and challenges for this project faced are:

## Issues:

The team defines issues as personal or professional hurdles that they faced during this project. Such issues hinder the completion of the task yet also underline the need for improvement or changes that the progress of the project asks, individually or collectively. Some of such issues are:

|  |  |
| --- | --- |
| Issues | Description |
| 1. Scheduling Conflicts | One of the newly added team members has had a hard time regarding the contribution to the project plan. For the time being, he has been scheduled task at his own will such that significant contribution can be made to the progress report and the project. |
| 1. Communication chain | An effective communication chain is to be established such that the remote team member can be incorporated to the weekly team meetings. |

## Challenges:

Challenges are referred to in this project as technical inadequacies as an individual or a team that hinder the progress of the Project. Some of the challenges faced are:

|  |  |
| --- | --- |
| Challenges | Description |
| 1. Inadequate knowledge of the lattice and code-based quantum algorithms. | Some of the concept of quantum computing is so foreign that each team member must get accustomed to at least some knowledge of quantum physics to know the operational and functional process of quantum cryptography. |
| 1. Depiction of quantum computing and cryptography | Basic knowledge of quantum computing through free courses from IBM and Azure Quantum. |

# Addressing challenges

These issues and challenges can be addressed effectively by:

|  |  |
| --- | --- |
| Issues and challenges | Ways to address it effectively |
| 1. Scheduling Conflicts | -regular team meetings in MS teams |
| 1. Communication chain | -activity in MS teams is must for all teams’ members |
| 1. Inadequate knowledge of the lattice and code-based quantum algorithms | -research on this topic to be scheduled immediately preferably IBM documentation |
| 1. Depiction of quantum computing and cryptography | -use of Azure quantum and IBM developer |

# Priority tasks

The task at hand now would be the following:

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Student 1 | Student 2 | Student 3 |
| 1. Derive risk associated with present algorithms relating to post-quantum ability. | Jalay Shah/Ayush Keshar Prasai | Ronit Ashok Maheshwori | Virajsinh Jeetendra Sinh Rahevar |
| 1. Identify and outline vulnerabilities in present computational ability and cryptographic techniques. | Ronit Ashok Maheshwori | Jalay Shah | Virajsinh Jeetendra Sinh Rahevar |
| 1. Explain the need for transition from present cryptographic techniques in relation to risk. | Ayush Keshar Prasai | Jalay Shah | Virajsinh Jeetendra Sinh Rahevar |
| 1. Propose such transition. | Virajsinh Jeetendra Sinh Rahevar | Ronit Ashok Maheshwori | Jalay Shah/Ayush Keshar Prasai |