Project 5: Post-Quantum Cryptography

Chaoyun Li

December 2022

The task is to write a report on post-quantum cryptography. The report should cover the following aspects.

1. (30%) Outline the history and recent developments of quantum computers. The following questions should be covered.
   - Why quantum computers are powerful than classical ones?
   - What are the main approaches for building quantum computers?
   - What are the main problems in building practical quantum computers?
2. (30%) Describe the Grover's algorithm.
   - What are the main steps and how to implement them with quantum computers?
   - What are the time and memory complexities?
   - What are the impacts on the security of symmetric key cipher? How to mitigate quantum attacks based on Grover's algorithm?
3. (40%) Write an overview of post-quantum public key cryptosystems and the related hard problems. Give your recommendations of Public-Key Encryption/KEMs and Digital signature algorithms in the post-quantum settings and state your reasons. You may check the NIST PQC project [1].

[1] `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`

Requirements

1. The report should be written in **English**.
2. The report should have the following parts: Introduction, Main content, Summary and References[2]. When you describe an algorithm or an attack, please give technical details such as pseudocodes.

[2]Books, papers, websites, etc