Integer Factorization using Shor's Quantum Algorithm

Minor Project ESA
Team No: S3

Team Members:
Raj Jain 01FE18BCS002
Aayush Rajwade 01FE18BCS005
Aman Kumar 01FE18BCS029
Ayush Utsav 01FE18BCS059
Under the Guidance of: Mr. KMM Rajashekharaiah

KLE Technological University, Hubli

School of CSE

July 20, 2021

Outline of presentation

- Project Overview
- Literature Survey
- Goals/Objectives
- Methodology
- Circuit Design
- Results
- References

Project Overview

Domain/Problem Space :

- Number Theory
- Quantum Computing

Problem Definition :

To do Integer Factorisation by using Shor's Quantum Algorithm.

Applications :

- Breaking public key RSA Cryptography.
- Enabling Quantum Cryptography.

Literature Survey

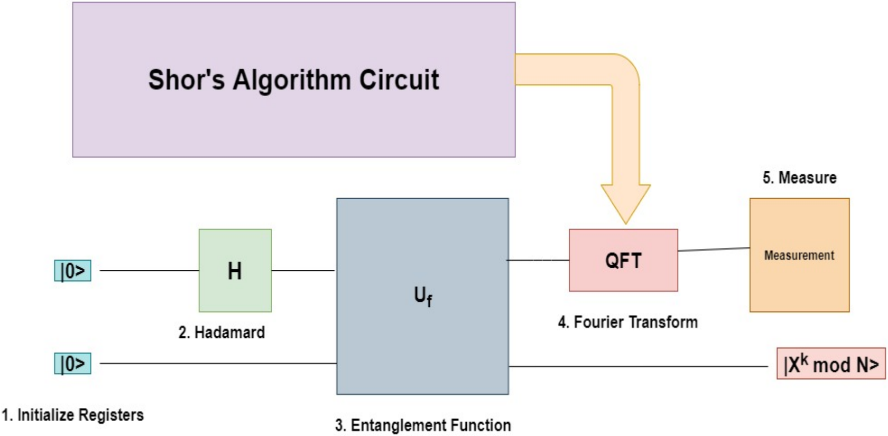
Paper Name	Author Name
QFT, Period Finding and Shor's Algorithm.	William Casper
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer	Peter W Shor.
A Note on Shor's Quantum Algorithm for Prime Factorization	Zhengjun Cao
Quantum Algorithm Implementations for Beginners	Adetokunbo adedoyin and john ambrosiano

Goals / Objectives

- To do integer factorization using Shor's Quantum algorithm.
- To achieve maximum probability success rate while factoring this integer.
- To reduce the number of iterations for which the algorithm runs.

Methodology

Component level diagram



Circuit Design

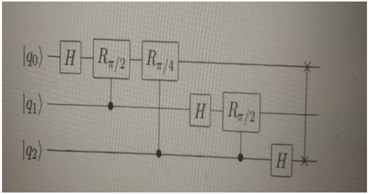


Figure: Quantum Fourier Transform

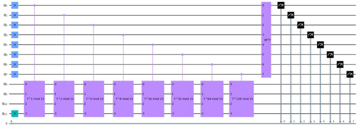


Figure: Sequential Quantum Fourier Transform

Results

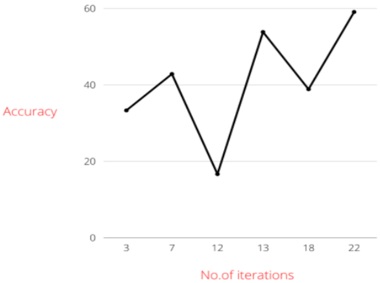


Figure: Accuracy vs. no. of iterations graph

- This graph represents Accuracy (Probability success rate) VS no of iterations the algorithm ran.
- The maximum accuracy achieved using SQFT is 59.0909% with iteration count of 22.

References

- Abhijith, J., et al. "Quantum algorithm implementations for beginners." arXiv e-prints (2018): arXiv-1804.
- Speiser, Jacqueline. "Implementing and Comparing Integer Factorization Algorithms."
- Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete loga- rithms on a quantum computer."SIAM review41, no. 2 (1999): 303-332.

Thank You