Karlsruher Institut für Technologie

Institut für Industrielle Informationstechnik
Hertzstraße 16, Geb. 06.35
76187 Karlsruhe
www.iiit.kit.edu

Masterarbeit

Unveiling the Power and Peril of Shor's Algorithm in Quantum Computing

Abstract

Quantum computing is revolutionizing the computational landscape, and Shor's algorithm stands as a prime example of its transformative potential. This thesis delves into the intricate workings of Shor's algorithm, its exponential speedup for integer factorization compared to classical methods, and its far-reaching implications, particularly in the realm of cryptography.

Developed by Peter Shor in 1994, this algorithm harnesses the power of quantum mechanics to factorize integers significantly faster than any known classical algorithm. This exponential speedup [e.g., $O(2^{\sqrt{n}})$ vs. $O\left(e^{(n^{(1/3)})}\right)$] poses a significant challenge to the security of widely used encryption schemes like RSA, which rely on the difficulty of integer factorization.

The research will be structured into several key areas:

The first part of this thesis will present a detailed understanding of Shor's algorithm, including its quantum circuit representation and mathematical foundations.
This section will also discuss the quantum Fourier transform, a key component of the algorithm, and how it contributes to the efficiency of the algorithm.
The second part will focus on the computational power of Shor's algorithm. It will include a comparative analysis with classical factorization algorithms, demonstrating the quantum advantage.
This section will also discuss the conditions under which Shor's algorithm outperforms classical algorithms and the practical challenges of implementing Shor's algorithm on a quantum computer.
The third part of this thesis will focus on the practical implementation of Shor's algorithm on hybrid quantum computing systems.
Hybrid quantum computing systems, which combine classical and quantum computing elements, represent a promising avenue for the realization of complex quantum algorithms.
The final part of the thesis will explore the implications of Shor's algorithm, with a particular focus on cryptography.
It will discuss how the algorithm threatens the security of RSA encryption, a widely used public-key encryption scheme.
This section will also explore potential countermeasures and alternatives to RSA, such as lattice-based cryptography and quantum key distribution.

The work can be done in German or English.

Prior knowledge

- Basic understanding of quantum mechanical concepts
- Programming skills (Python)
- Strong interest in and enthusiasm for research

Research area

- Quantum Computing
- Implementation of quantum algorithms
- Comparison of algorithms

Studiengang

☒ Elektro- und Informationstechnik
☒ Mathematik
☒ Informatik
☒ Physik

Alignment

☒ Research
☒ Implementation
☒ Analysis and evaluation
☒ Method development

Start

At any time

Links

Mitarbeiterseite

Ansprechpartner

Dr. Hamza Gardi
Westhochschule, Hertzstr. 16
Geb. 06.35, Zimmer 115
hamza.gardi@kit.edu
Tel.: (0721) 608 - 4451759