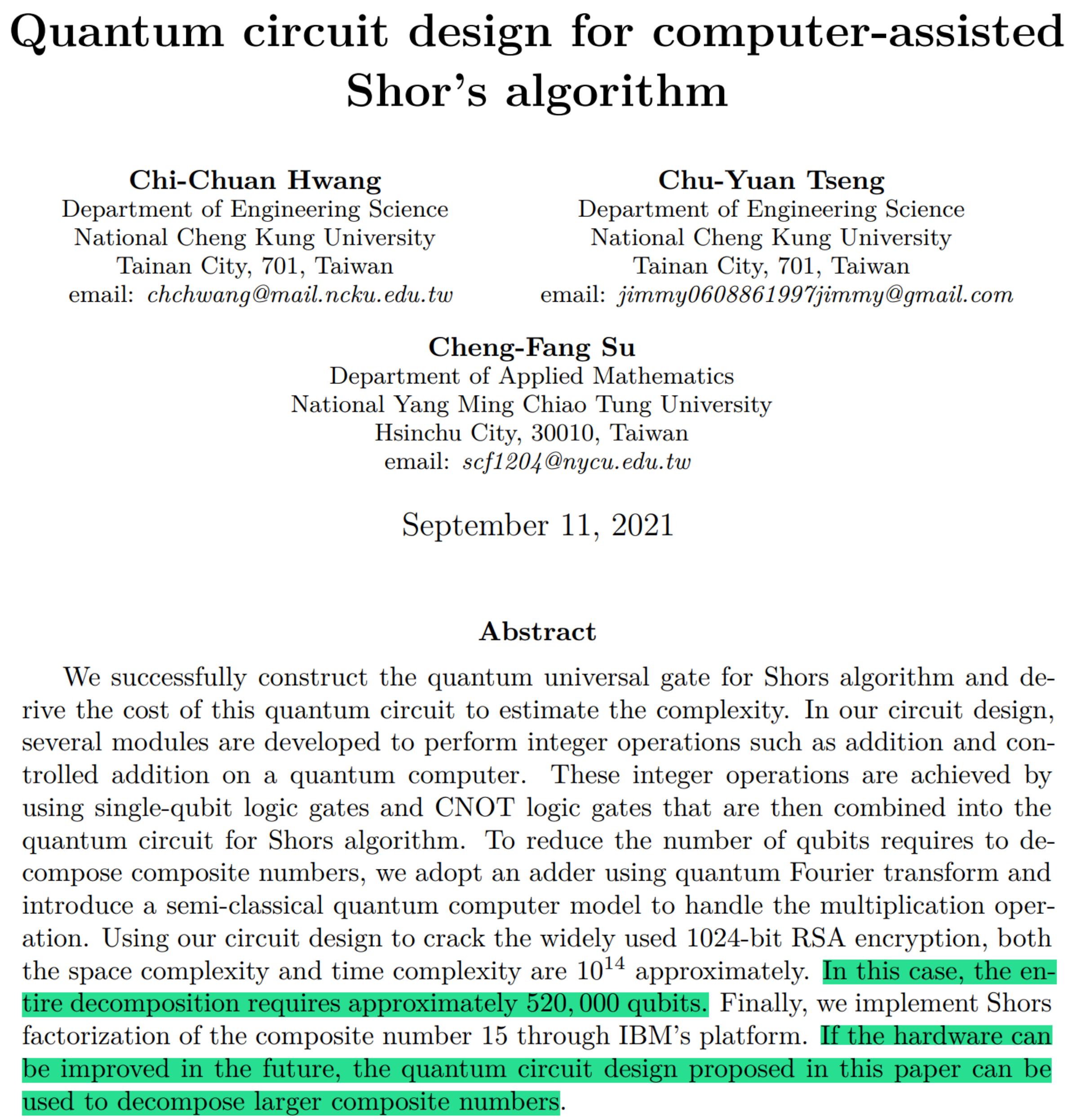
We first look at this paper.



Quantum circuit design for computer-assisted Shor's algorithm

Chi-Chuan Hwang
Department of Engineering Science
National Cheng Kung University
Tainan City, 701, Taiwan
email: *chchwang@mail.ncku.edu.tw*

Chu-Yuan Tseng
Department of Engineering Science
National Cheng Kung University
Tainan City, 701, Taiwan
email: *jimmy0608861997jimmy@gmail.com*

Cheng-Fang Su
Department of Applied Mathematics
National Yang Ming Chiao Tung University
Hsinchu City, 30010, Taiwan
email: *scf1204@nycu.edu.tw*

September 11, 2021

Abstract

We successfully construct the quantum universal gate for Shors algorithm and derive the cost of this quantum circuit to estimate the complexity. In our circuit design, several modules are developed to perform integer operations such as addition and controlled addition on a quantum computer. These integer operations are achieved by using single-qubit logic gates and CNOT logic gates that are then combined into the quantum circuit for Shors algorithm. To reduce the number of qubits requires to decompose composite numbers, we adopt an adder using quantum Fourier transform and introduce a semi-classical quantum computer model to handle the multiplication operation. Using our circuit design to crack the widely used 1024-bit RSA encryption, both the space complexity and time complexity are 10^{14} approximately. In this case, the entire decomposition requires approximately $520,000$ qubits. Finally, we implement Shors factorization of the composite number 15 through IBM's platform. If the hardware can be improved in the future, the quantum circuit design proposed in this paper can be used to decompose larger composite numbers.

1 Outline

1. Vector and Matrix
2. Hilbert space
3. Quantum postulates

2 Useful Reference

2.1 學測範圍

For some basic knowledge, please refer to the website 黑狗的家

- 3-1 平面向量的運算
- 3-2 平面向量的內積
- 3-3 平面向量內積的應用
- 1-1 空間概念
- 1-2 空間坐標系與空間向量
- 1-3 空間向量的內積
- 4-2 矩陣的運算
- 4-3 矩陣的應用

Please at least take a look at 3-1 3-2 and 4-2.

2.2 Linear space / Vector space

線代啓示錄（中文網站）