Quantifying the Noise Tolerance of Quantum Factoring: A Study of Shor's Algorithm

Tung Yan YEUNG

This project investigates the impact of noise on Shor's algorithm, a quantum algorithm that could break RSA cryptography. Through software simulations on IBM quantum simulator, it aims to provide insights into the challenges of using quantum computers to threaten RSA security.

Introduction

Motivation

RSA encryption, widely used for online security, faces a threat that Quantum Computers (QC) could theoretically use Shor's algorithm to break RSA.

Objectives

- Model the imperfections, i.e. noises of superconducting architectures
- Explore Shor's algorithm performance under imperfections

Hypothesis

- Success rate ↓ as noise ↑
- Readout error least sensitive ∵ only occur at measurement
- Very low success rate factoring numbers larger than 15

How factoring crack RSA?

p · q = N

Step 1: Euler's totient function φ(n) = (p-1)(q-1)

Step 2: Generate random e that GCD(e, φ(n)) = 1

Step 3: Create d by e · d = 1 modφ(n)

Public key (e, N) & Private key (d, N)

Step 4: Encrypt message M by public key

C = M^e mod N

Step 5: Decrypt message by private key

M = C^d mod N

Know e, N, C → factor N → find out p & q → deduce value d → crack message M

Example to factor N=15 [1,2]

Step 1: Guess any numbers "a". Let a = 2.

Step 2: Find order of a^r = 1 mod N

2^0 % 15 = 1

2^1 % 15 = 2

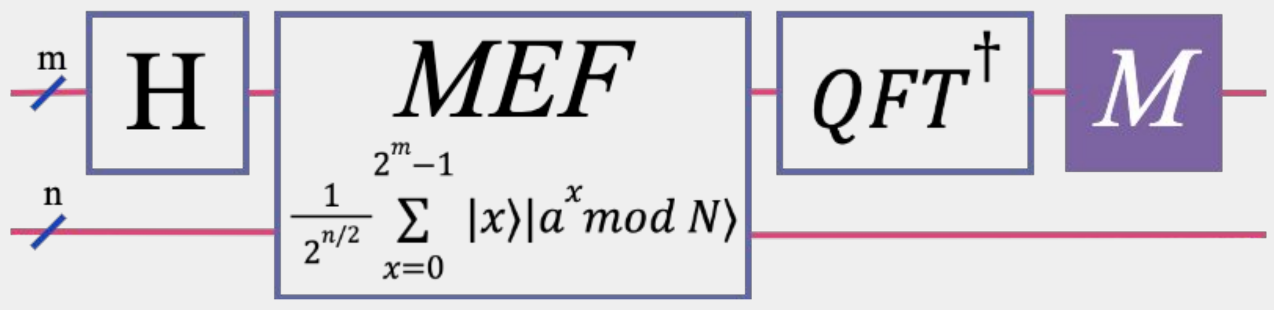
2^2 % 15 = 4

2^3 % 15 = 8

2^4 % 15 = 1 → ∴ r = 4

Step 3: GCD(n, a^(r/2)+1) → GCD(15, 5) = 5

GCD(n, a^(r/2)-1) → GCD(15, 3) = 3



Step 1: m qubits for control register

n qubits for work register stores |Ψ⟩. N=1111 → n=4

Circuit uses "2n+3" qubits → m=7

Step 2: Superposition (H)

$$[H|0\rangle]^{\otimes 7}|\Psi\rangle = \frac{1}{2^{n/2}}[|0\rangle + |1\rangle + |2\rangle + \cdots + |127\rangle]|1\rangle$$

Step 3: Modular Exponentiation Function

$$\tfrac{1}{4}[\,|0\rangle|1\rangle + |1\rangle|2\rangle + |2\rangle|4\rangle + |3\rangle|8\rangle + |4\rangle|1\rangle + \cdots + |124\rangle|1\rangle + |125\rangle|2\rangle + |126\rangle|4\rangle + |127\rangle|8\rangle\,]$$

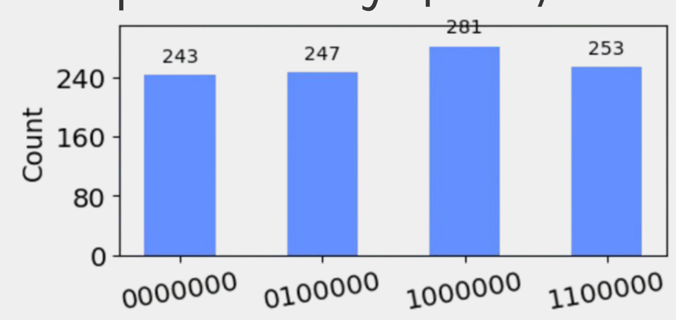
$$= \tfrac{1}{4}[\,(\,|0\rangle + |4\rangle + \cdots + |120\rangle + |124\rangle\,)\otimes|1\rangle + \cdots + (\,|3\rangle + |7\rangle + \cdots + |123\rangle + |127\rangle \otimes)|8\rangle\,]$$

Step 4: QFT† → measure

Inverse Quantum Fourier Transform (QFT†) to perform Quantum Phase Estimation (QPE) → determine the phase of eigenvalues of operators by $\phi = \ell/2^m$

Peaks ℓ occur at 0, 32, 64, 96

Phases φ (s/r) are 0, 1/4, 1/2, 3/4



Methodology

1. **Implement Shor's algorithm**
   Develop quantum circuit & post-quantum processing procedure

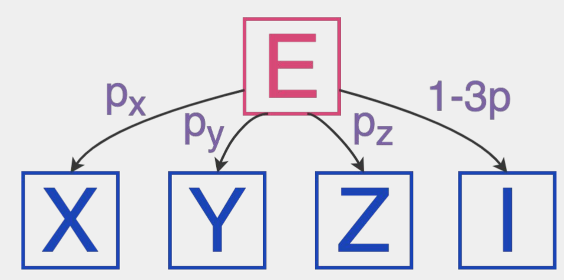
2. **Build 3 types of noise models**
   Sample IBM 15 real QC error data [3] & research findings [4]

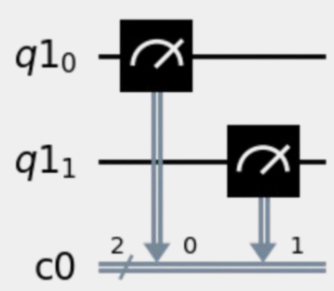
3. **Vary error rates**
   Vary error rates between min. & max. to implement circuit

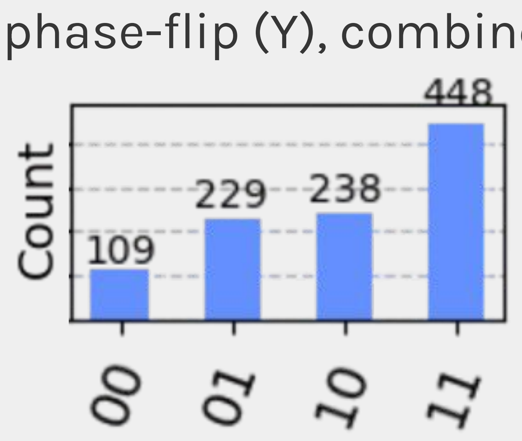
4. **Analysis**
   Analyse factoring success rate and compare to noise-free results

Types of noise

Depolarising Bit-flip (X), phase-flip (Y), combined flip (Z) occurs with same probability







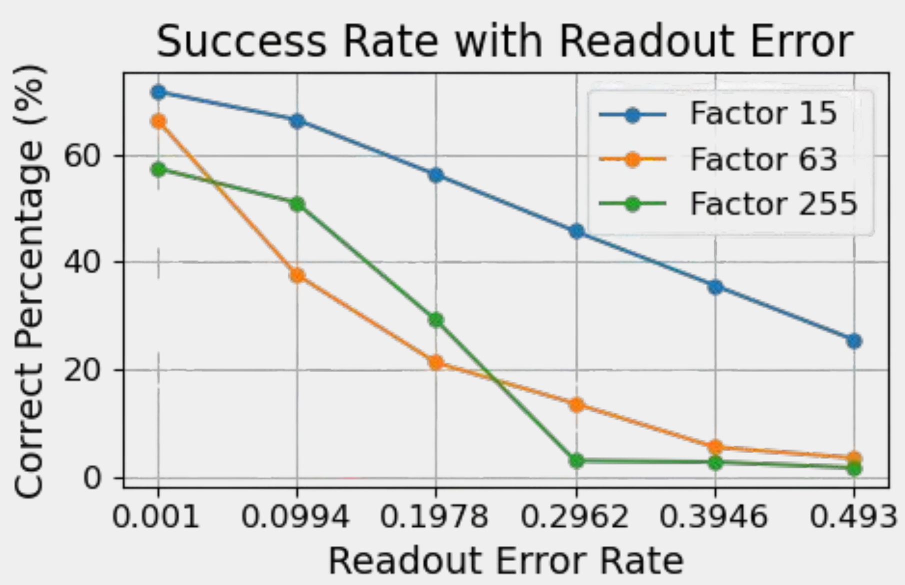
State	Theoretical	Simulated
|00⟩	⅓ · ⅓ = 0.111	109/1024 = 0.106
|01>	⅓ · ⅔ = 0.222	229/1024 = 0.224
|10⟩	⅔ · ⅓ = 0.222	238/1024 = 0.232
|11⟩	⅔ · ⅔ = 0.444	448/1024 = 0.438

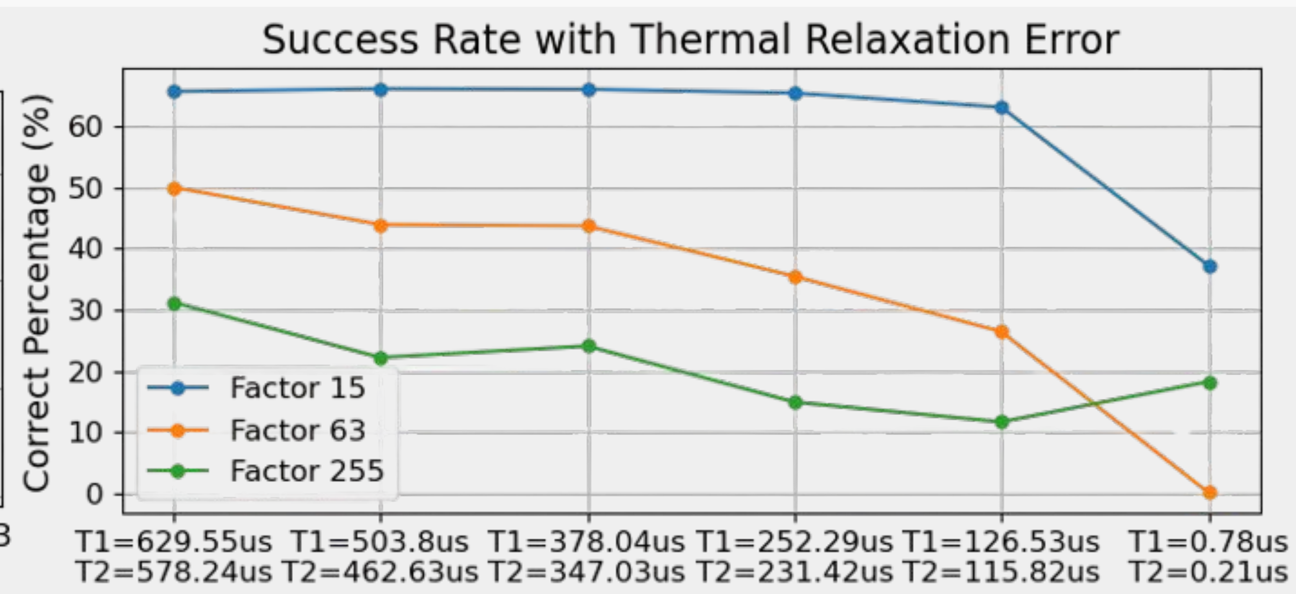
Thermal Relaxation (i) Thermal relaxation occurs over time in the form of excitation / de-excitation (T1 = relaxation constant) (ii) Dephasing of qubit overtime (T2 = dephasing constant)

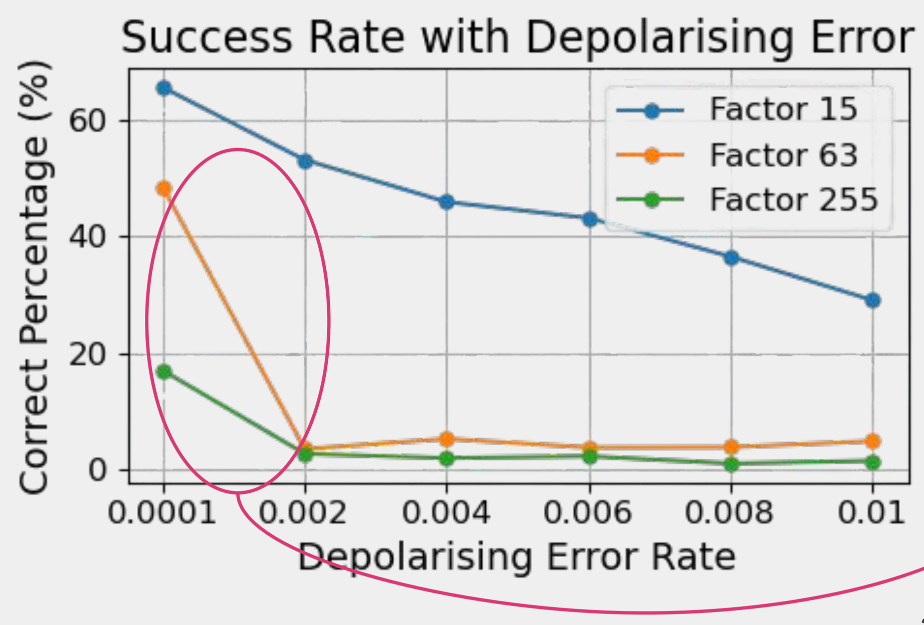
Readout Error in measuring qubits

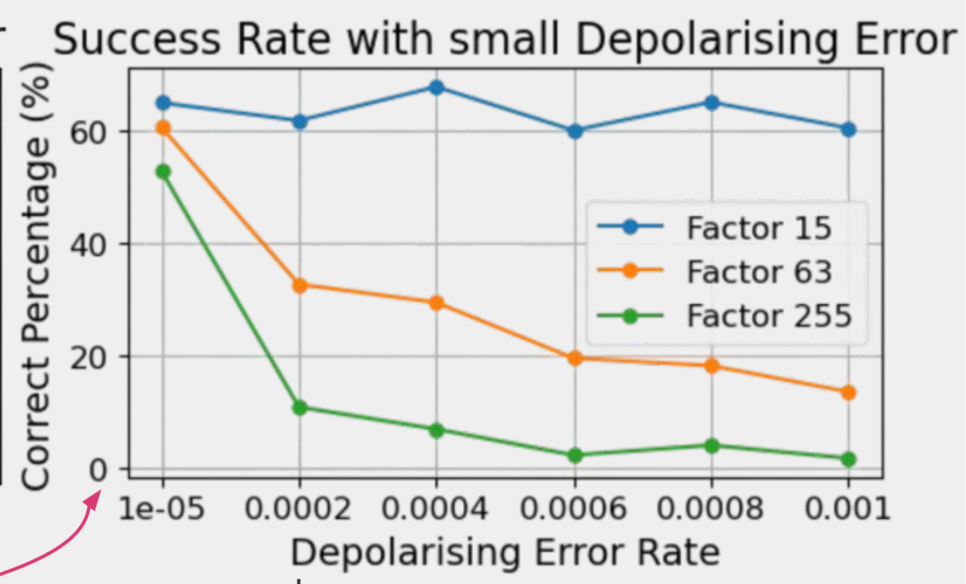
Results

- ➢ Line Graphs Analysis
  - Readout Error:
    - Significantly drop close to 0 since median error rate for factoring 255
  - Thermal Relaxation Error:
    - Non sensitive to small circuit
  - Depolarising Error:
    - Biggest impact among the three errors
    - Sensitive between error = 1e-5 to 2e-3
- ➢ Table Analysis
  - Readout is the least impact among the three errors
  - Real noisy QC has <5% success rate for factoring 63, 255.
  - Experimental noise models reveals depolarising error is the major challenge to Shor's algorithm









* Real QC backend *ibm_brisbane*	Factor success rate
15 (1111)	70.65%
63 (111111)	4.96%
255 (11111111)	2.55%

* median error rate	Factor success rate		
	15	63	255
Noise Free	66.67%	56.44%	59.71%
Depolarising	47.57%	3.47%	2.40%
Thermal relaxation	64.14%	26.99%	10.49%
Readout	65.05%	56.40%	52.92%

Discussion

- Fluctuation see in line graphs could be due to the nature of gates are not perfect, e.g. Hadamard gates ✘ produce 50/50 outcomes.
- Still far away from breaking RSA-2048.
- Future plan: error mitigation for depolarising error.

I would like to thank Dr. Imad Faruque and Dr. Jorge Barreto for their support throughout this research.

Contact ansontyyeung@gmail.com
UK: +44 (0) 7444 295480 | HK: +852 5622 2301
https://github.com/ansontyyeung

[1] https://doi.org/10.1137/S0097539795293172
[2] Nielsen, M. A., Chuang, I. L. (2000). Quantum Computation and Quantum Information. Cambridge University Press.
[3] https://quantum.ibm.com/services/resources
[4] https://doi.org/10.1103/PhysRevA.103.042603

University of BRISTOL