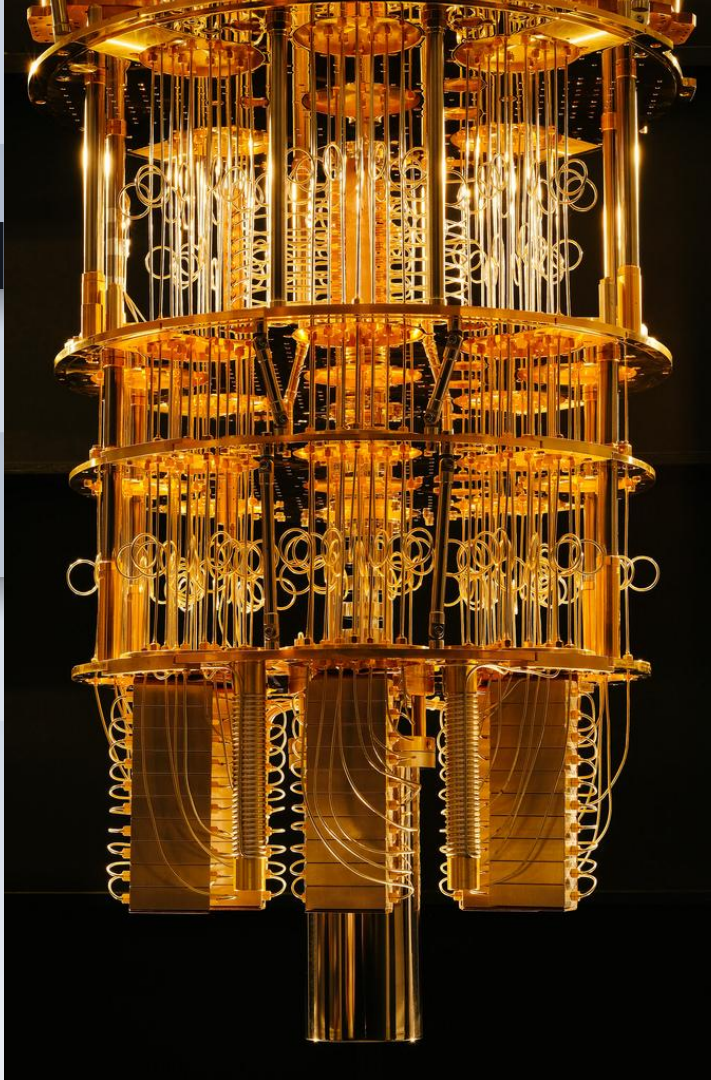
INTEGER FACTORIZATION USING SHOR'S ALGORITHM AND ITS IMPLEMENTATION ON A QUANTUM COMPUTER

Presenter
Aman Ganeju
Roll no:4080023

Supervisors
Om Krishna Suwal,PhD,
Dibakar Sigdel,PhD,
Shree Krishna Bhattarai,PhD.



Integer Factorization

- An integer $I = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$ can be decomposed into unique primes: $p_i's$ and $a_i's$ are their respective power.
- Question: what are the prime factors?
- Classical Method (a): Divide I by all the values $2 \leq x < I$ to find reminder.
- Classical method (b): Divide I by all the values $2 \leq x < \sqrt{I}$ to find reminder

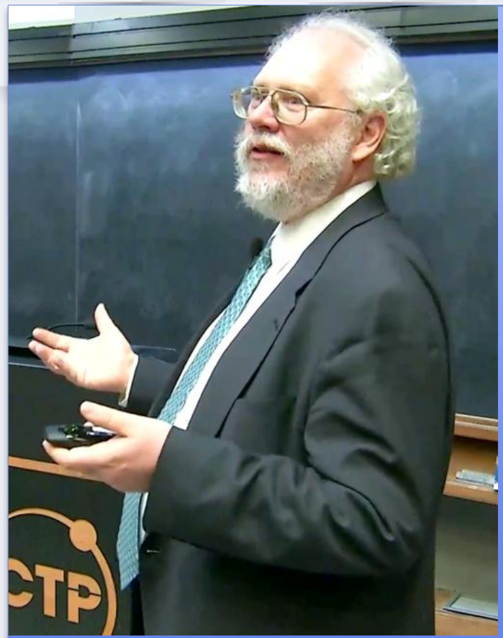
- Complexity: amount of resources(time or space needed)
- Method(a) takes $\mathcal{O}(2^w)$ time complexity where $w = log_2 I$
- Method(b) takes $\mathcal{O}(2^{w/2})$ time complexity
- The best known algorithm for factorization is General Number Field Sieve(GNFS):

  time complexity: $\mathcal{O}\left(\mathbf{exp}\left(\mathbf{cw}^{\frac{1}{3}}(\log \mathbf{w})^{\frac{2}{3}}\right)\right)$ [2](Hamdi et al.,2014)
- RSA cryptography is based on the difficulty of factoring problem

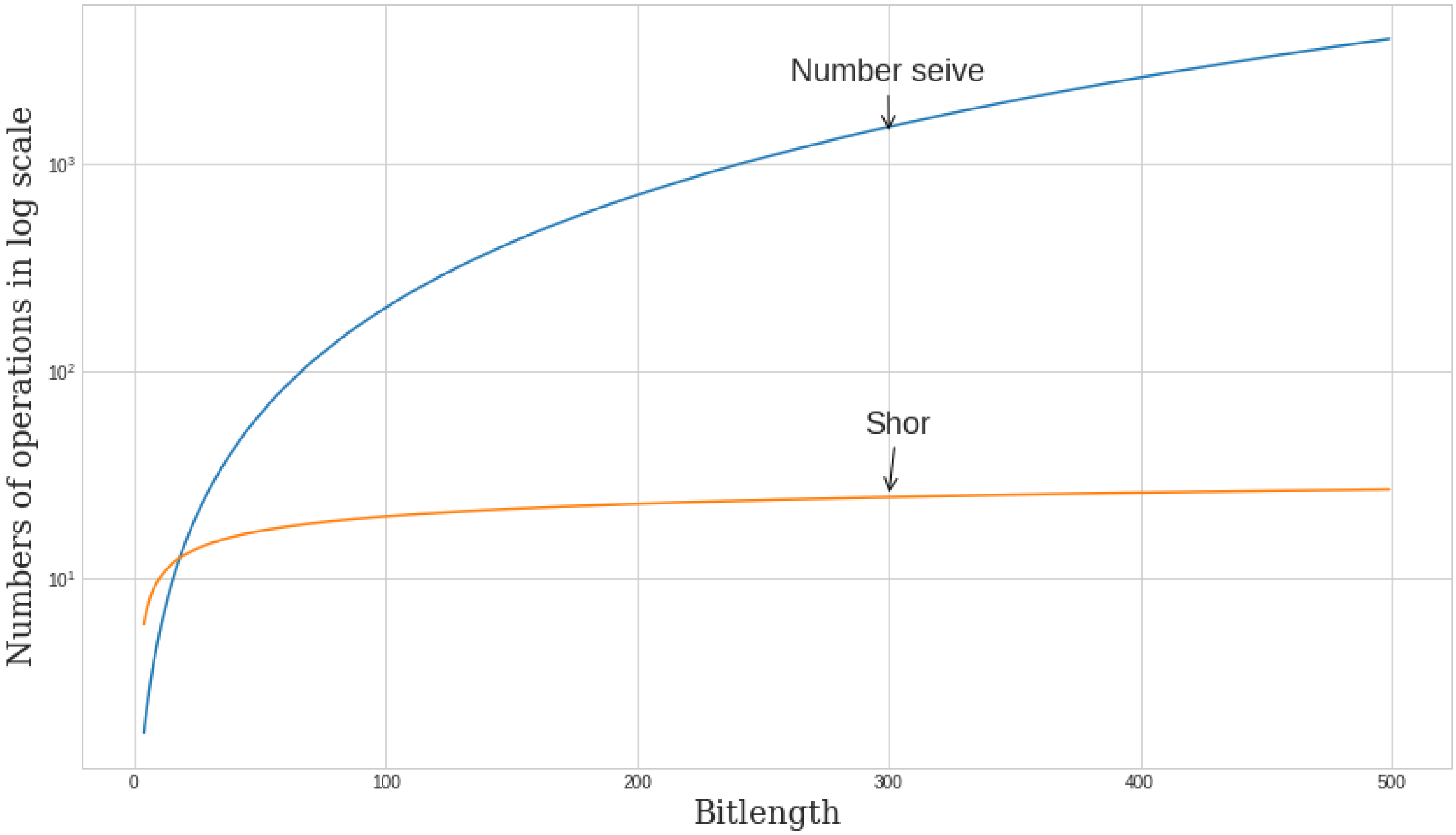
Shor’s Algorithm

It is a

- ❑ Quantum Algorithm
- ❑ Developed by Peter Shor in 1994
- ❑ For composite integer factorization
- ❑ In polynomial time with bounded error.



Peter Shor

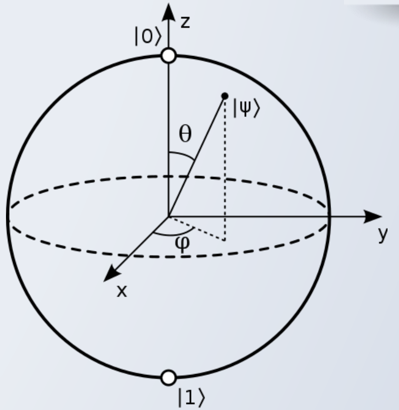

Number seive
Shor
Numbers of operations in log scale
10^3
10^2
10^1
0
100
200
300
400
500
Bitlength

Introduction to Quantum Computing

- Act of leveraging quantum mechanical properties to perform computing [3](Hidary, 2019)
- Qubit

  Basic unit of information

  Superposition of $|0\rangle$ and $|1\rangle$ states



$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\, where |\alpha|^2 + |\beta|^2 = 1$$
$$= \left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right)$$

- Measurement of $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ collapse superposition to single

$$P(|0\rangle) = |\alpha|^2 \qquad P(|1\rangle) = |\beta|^2$$

- For 2 qubit system, system can have superposition of all four states

$$|0\rangle|0\rangle \quad |0\rangle|1\rangle \quad |1\rangle|0\rangle \quad |1\rangle|1\rangle$$

- For n qubit system, there are 2^n different possible states

$$|\Psi\rangle = \sum_{m=0}^{2^n-1} a_m |m\rangle$$

- Entanglement between qubits is a special type of correlation such that change in one instantaneously triggers an effect on other.[4]

Theory of Shor's Algorithm

Say M= $p.q$ be a composite odd integer and M $\neq p^k$, for prime p,

1. Choose a random number : $1 < x < M$
2. If $\mathrm{GCD}(x, M) \neq 1$, then factor = $\mathrm{GCD}(x, M)$ where GCD = greatest common divisor
3. If $\gcd(x, M) = 1$, find period, a of MEF function
$$f(r) = x^r \; mod \; M \qquad , r \in \mathbb{Z}(M)$$
4. If period: a is odd or $x^{a/2} \equiv 1 \; (modM)$, we restart the algorithm from step 1
5. If a is even and $x^{a/2} \not\equiv 1 \; (modM)$ then, factors of M are:
$p = GCD\left(x^{a/2} + 1, M\right)$ or/and $q = GCD(x^{a/2} - 1, M)$

An example

- Let M = 15 and x = 2 then GCD(2,15)=1,
- $f(r) = \ 2^r \, mod \, 15, r \in \mathbb{Z}(15)$ would give

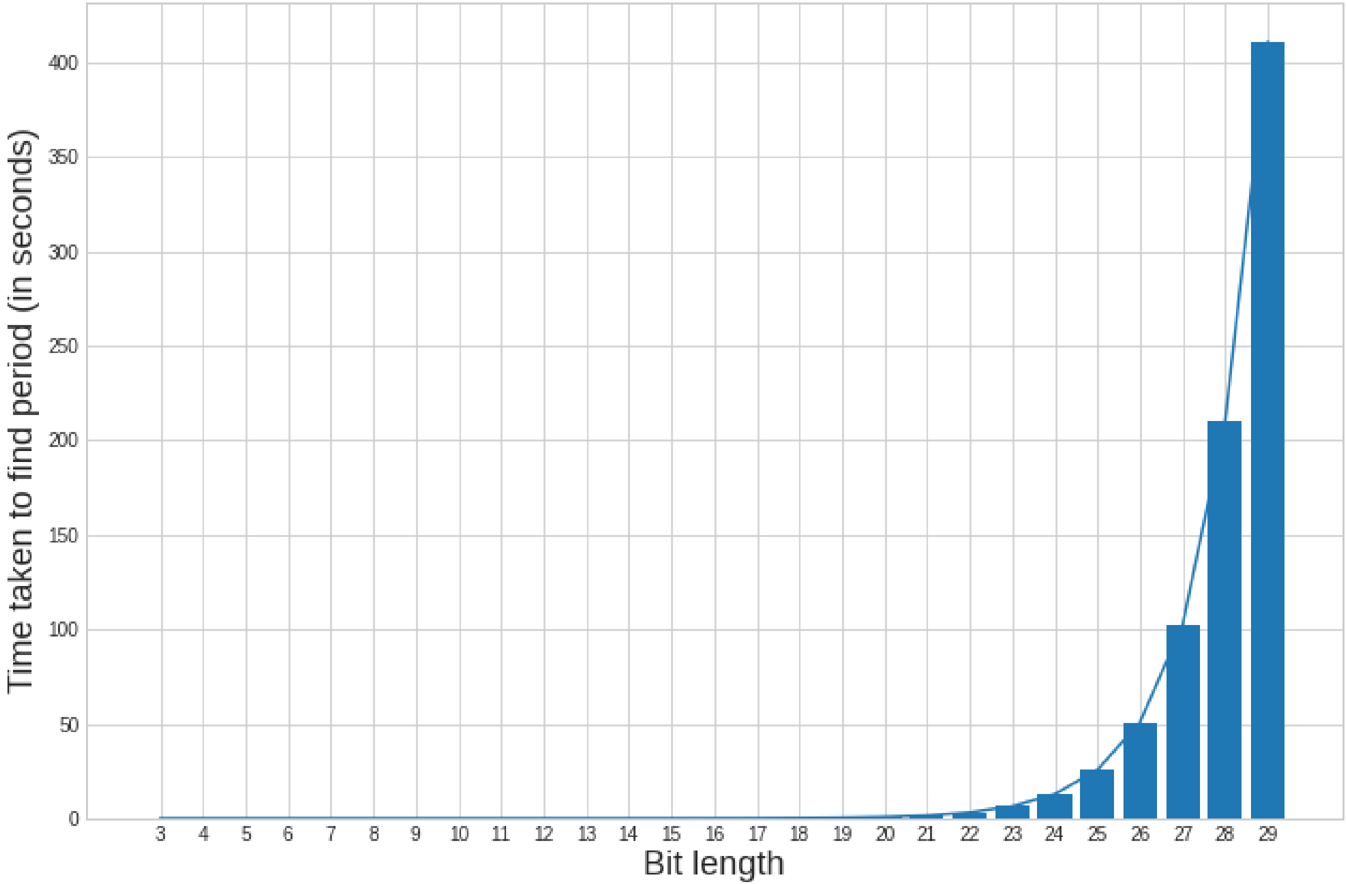
  $f(0) = \ \ 1 \, mod \, 15 = 1,\ f(1) = 2 \, mod \, 15 = 2, f(2) =$ $4 \, mod \, 15$ =4, . . .

  i.e. $f(r) =$ 1, 2, 4, 8, 1, 2, 4, 8, 1, 2, 4, 8 …

  So period, a = 4
- Factors are $GCD\left(2^{\frac{4}{2}} + 1{,}15\right) = GCD(5{,}15)$ = 5,

  $GCD\left(2^{\frac{4}{2}} - 1{,}15\right)$= $GCD(3{,}15)$= 3
- Hence factors are 5 and 3 : 5*3 =15

Fig: Amount of time required to find period of integer of increasing bit length


Time taken to find period (in seconds)
400
350
300
250
200
150
100
50
0
3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
Bit length

Shor's algorithm on quantum computer

1. Initialize two quantum registers $|0\rangle^n |1\rangle^r$
   Where $M^2 < 2^n < 2M^2$, *r > log(M) +1*
2. Prepare uniform superposition by applying Hadamard gates
   ($H^{\otimes n}$)in first register
3. Apply the periodic function $f(x) = z^x(mod\ M)$ on second register
4. Apply QFT on first register to obtain the frequency of the superimposed state in 1st register and
5. Measure the input register

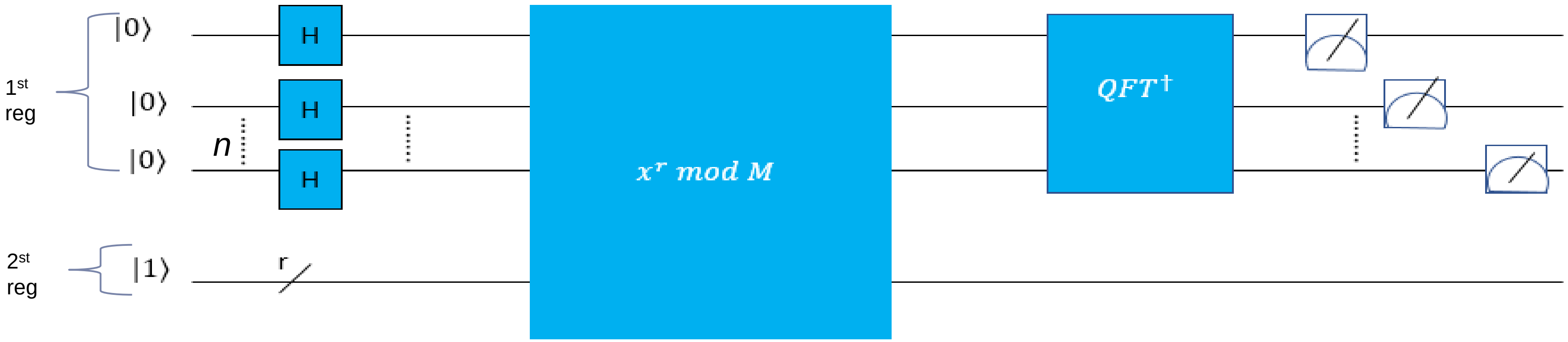


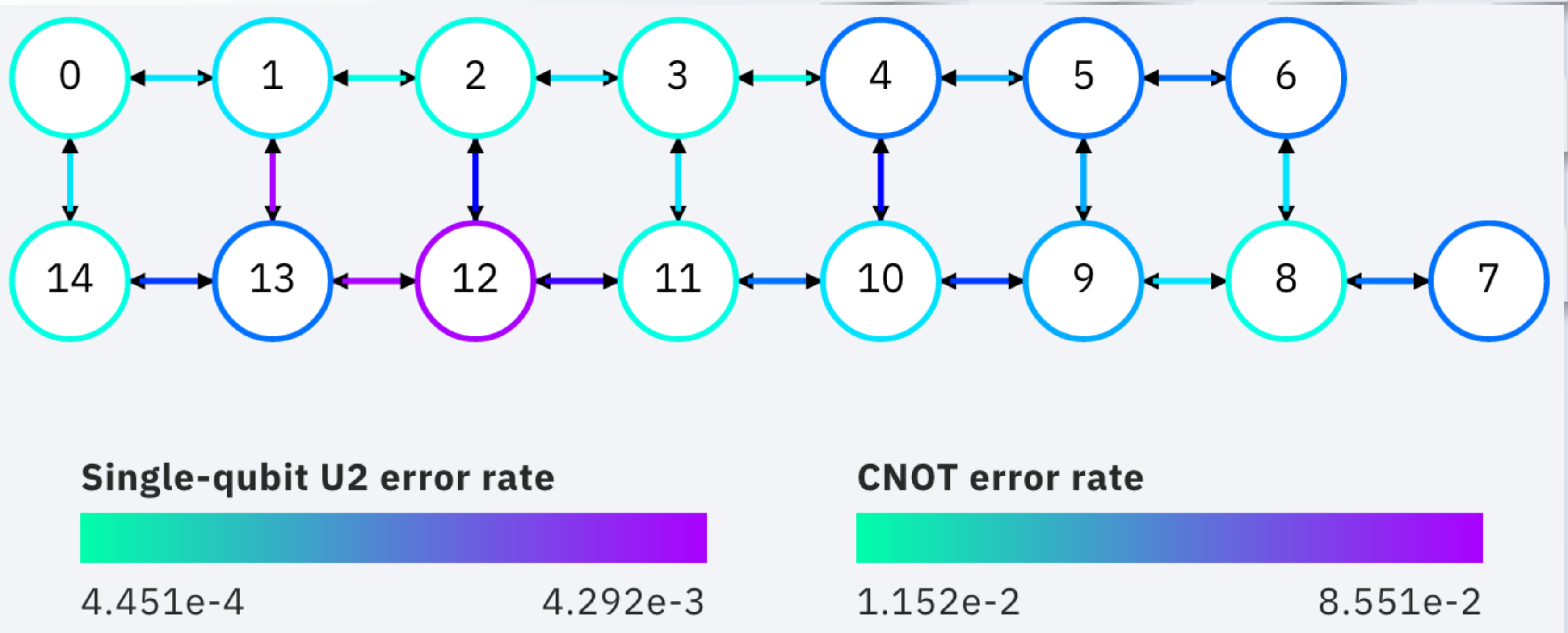
Fig : Circuit diagram for Shor's Algorithm Implementation

5. Classical analysis: Use Continued Fraction Algorithm and Euclidean Algorithm to find period a and then find the factors

- Shor's algorithm has a bounded error
- Complexity
  - Hadamard gates($H^{\otimes n}$) : $O(log\, M)$ - Oracle Function : $O(log^3 M)$
  - QFT: $O(log^2 M)$ - Euclidian Algorithm: $O(log^3 M)$
- Complexity of algorithm=$\mathcal{O}(log^3 M)$
- Hence Shor's algorithm is a Bounded error Quantum polynomial (BQP) algorithm.

Methodology: Implementation

- Programming language: Python; package :Qiskit
- Qiskit: an open source SDK to work with quantum circuits and algorithms, and acts as interface for running quantum circuits on quantum computers at IBM [8]
- Hardware: *ibmq_qasm_simulator* and *ibmq _16_Melbourne*
- *ibmq_qasm_simulator* : quantum simulator at IBM
- *ibmq _16_Melbourne* : a 15 qubit quantum computer at IBM
- Qubits used: 0,1,2,3,13,14



Topography diagram and coupling map of *ibmq_16_Melbourne* [8]

Circuit design

- Factor an integer I=15 with base z = 2 for MEF
- Created a simplified compiled version of Shor's algorithm (Geller and Zhau,2013)

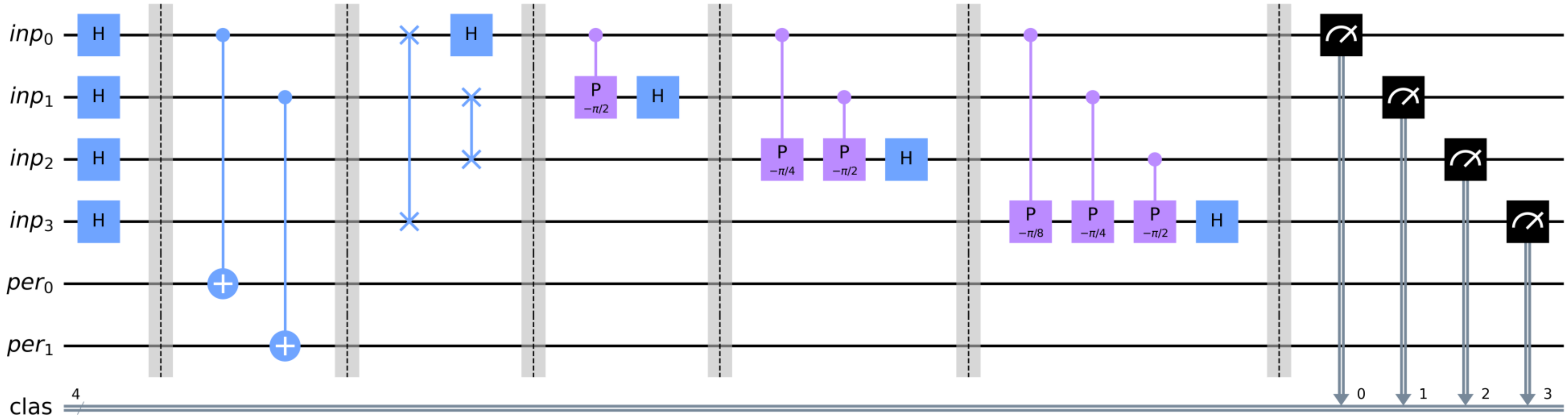
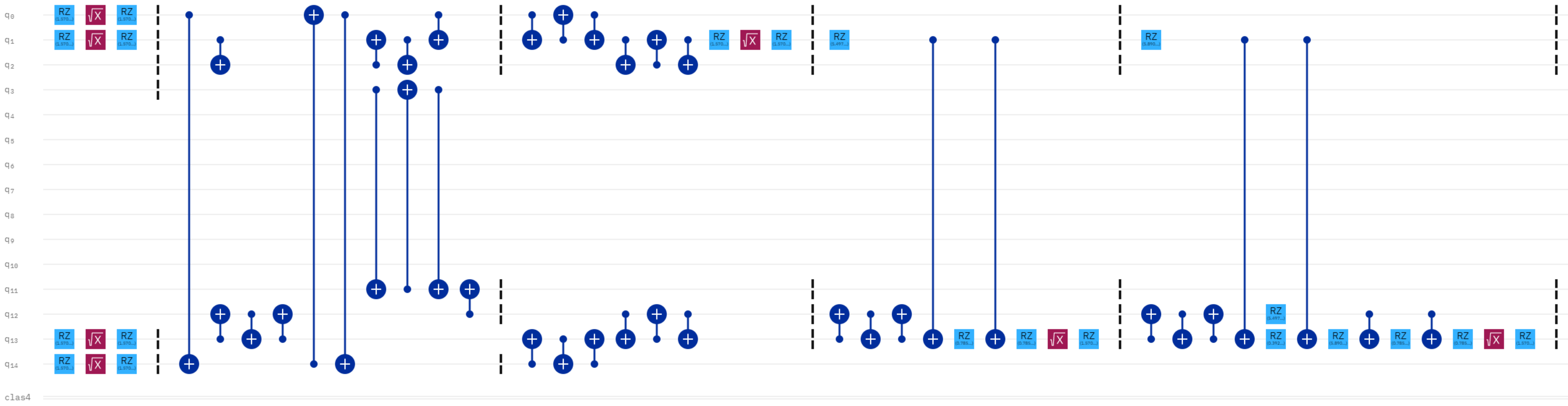
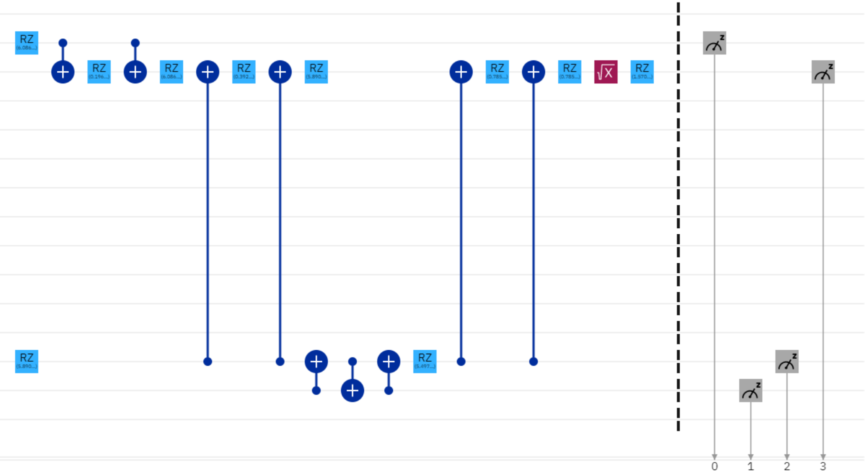


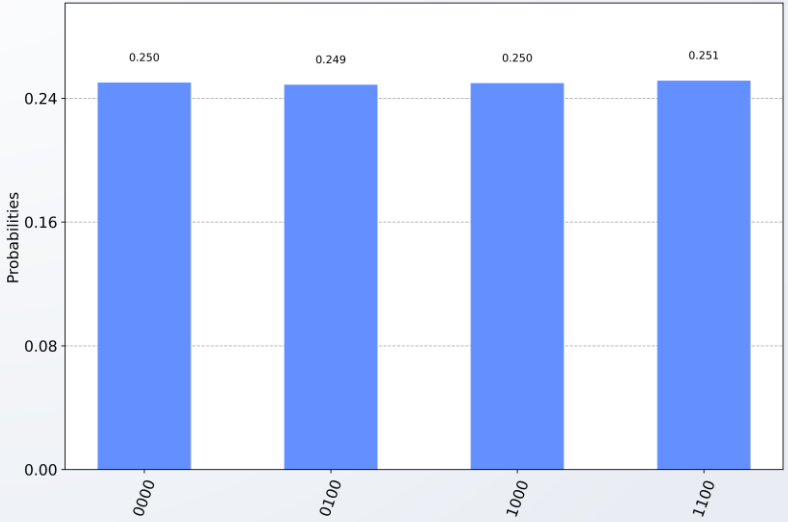
Fig: Quantum Circuit diagram for Shor's Algorithm to factor integer 15


q0
q1
q2
q3
q4
q5
q6
q7
q8
q9
q10
q11
q12
q13
q14
clas4

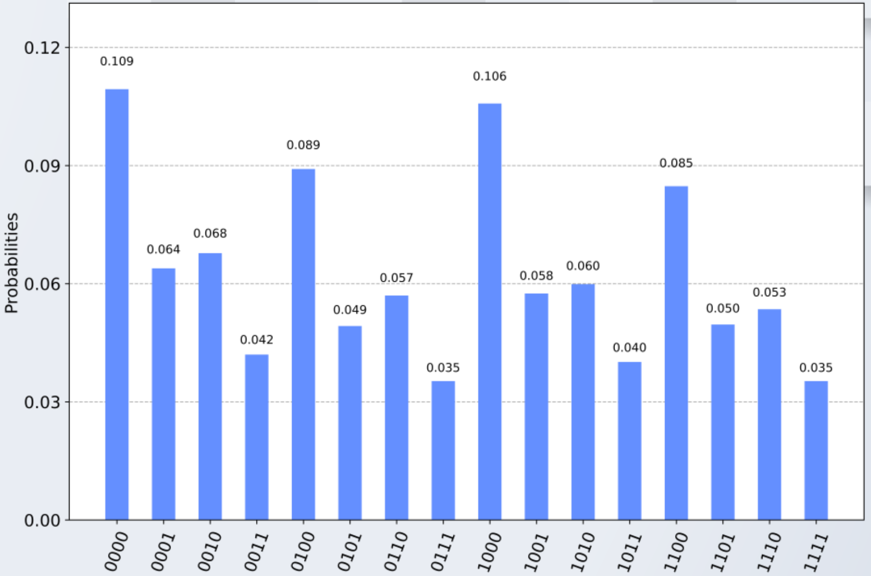

0
1
2
3

Result

On *ibmq_qasm_simulator*



On *ibmq_16_Melbourne* QC

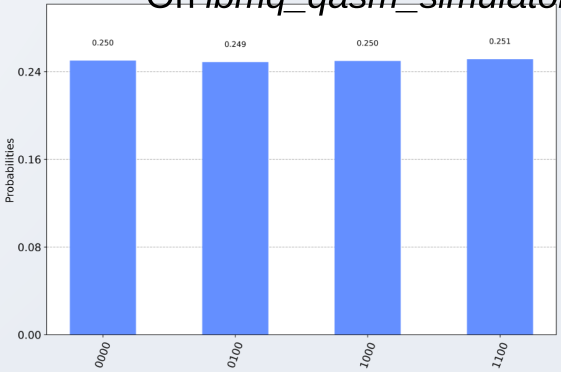


- Peaks at decimal equivalents: 0,4,8,12
- By classical processing, order a = 4
- And factors = $\mathrm{GCD}(2^2+1,15)=5$ and $\mathrm{GCD}(2^2-1,15)=3$
- Validation: $3*5=15$.

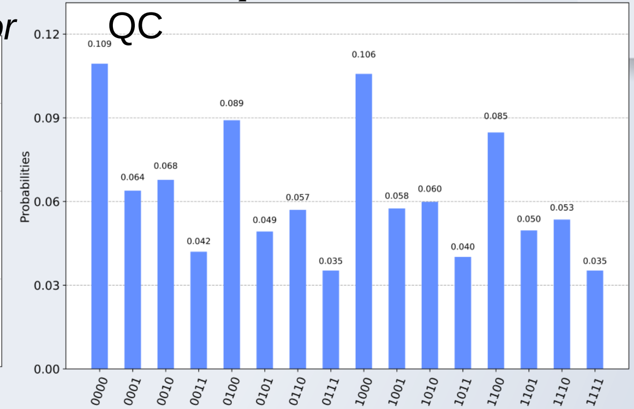
Discussion

- Dissimilarities in results
- Quantum Errors
- Scalability

On *ibmq_qasm_simulator*



On *ibmq_16_Melbourne* QC



Significance: Break RSA cryptography

- A widely used cryptographic system for online data transmission including emails and online payments
- Based upon the difficulty of factoring a large number
- 300 trillion years for classical computer to break 2048 bit key while it takes 10 secs for 4099 qubit QC(Zhang, 2020)
- Largest experimentally factored number by quantum computer using Shor’s algorithm: ‘21’ (Martin-Lopez,2012)

```
RSA-(2048) = 25195908475657893494027183240048398571429282126204032027777137783
             60436620207075955562640185258807844069182906412495150821892985591
             49176184502808489120072844992687392807287776735971418347270261896
             37501497182469116507761337985909570009733045974880842840179742910
             06424586918171951187461215151726546322822168699875491824224336372
             59085141865462043576798423387184774447920739934236584823824281198
             16381501067481045166037730605620161967625613384414360383390441495
             26344321901146575444541784240209246165157233507787077498171257724
             67962926386356373289912154831438167899885040445364023527381951378
             636564391212010397122822120720357
```

Figure: RSA-(2048)

THANK You

Acknowledgment

- Supervisors: Dibakar Sigdel, Om Krishna Suwal, Shree Krishna Bhattarai
- Association of Nepali Physicists in America (ANPA)
- Khwopa College
- Friends: Rodip Datheputhe, Supriya Dhakal, Anis Gautam, Sagar Ganeju

References

1. Cheung, D. (2003). Using generalized quantum Fourier transforms in quantum phase estimation algorithms (Doctoral dissertation, University of Waterloo [Department of Combinatorics and Optimization]).
2. Hamdi, S. M., Zuhori, S. T., Mahmud, F., & Pal, B. (2014). A compare between Shor's quantum factoring algorithm and general number field sieve. *2014 International Conference on Electrical Engineering and Information & Communication Technology*. doi:10.1109/iceeict.2014.6919115
3. Hidary, J. D. (2019). *Quantum Computing: An Applied Approach* (pp. 1-351). Cham: Springer
4. Loceff, M. (2016). A Course in Quantum Computing.
5. Martin-Lopez, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X. Q., & O'brien, J. L. (2012). Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature photonics, 6(11), 773-776.
6. Monz, T., Nigg, D., Martinez, E. A., Brandl, M. F., Schindler, P., Rines, R., ... & Blatt, R. (2016). Realization of a scalable Shor algorithm. Science, 351(6277), 1068-1070.
7. Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.
8. Open-source quantum development. (n.d.). Retrieved February 20, 2021, from https://qiskit.org/
9. Zhang, L., Miranskyy, A., & Rjaibi, W. (2020). Quantum Advantage and Y2K Bug: Comparison. IEEE Software.