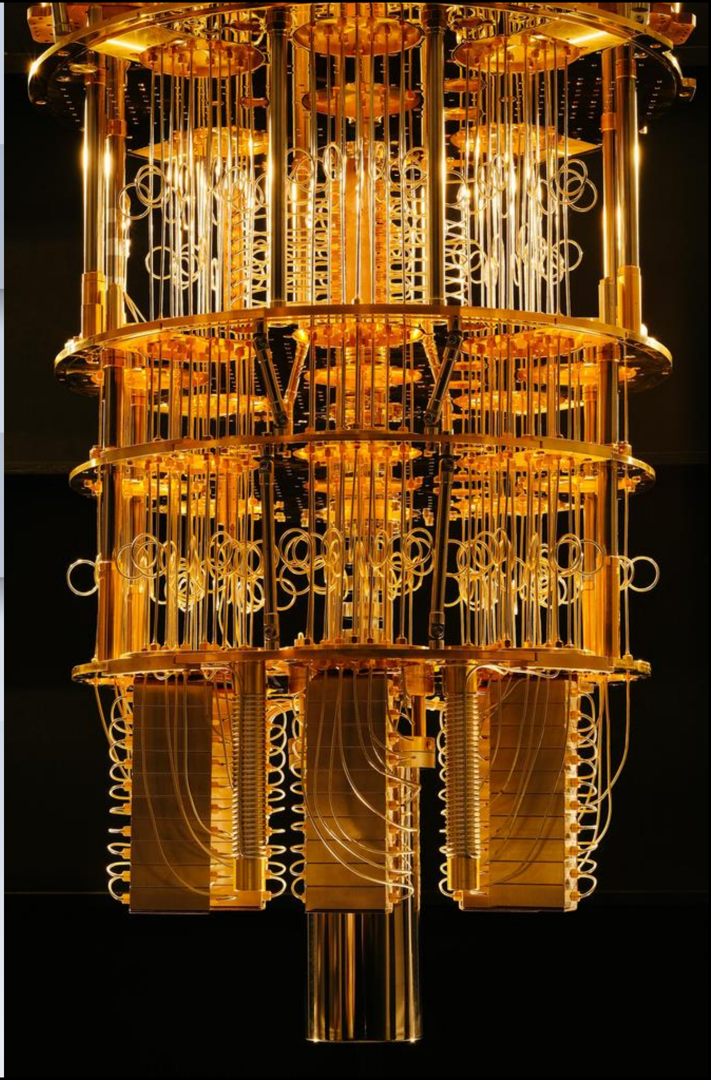
INTEGER FACTORIZATION USING SHOR'S ALGORITHM AND ITS IMPLEMENTATION ON A QUANTUM COMPUTER

Presenter
Aman Ganeju
Roll no:4080023

Supervisors
Om Krishna Suwal
Dibakar Sigdel,
Shree Krishna Bhattarai

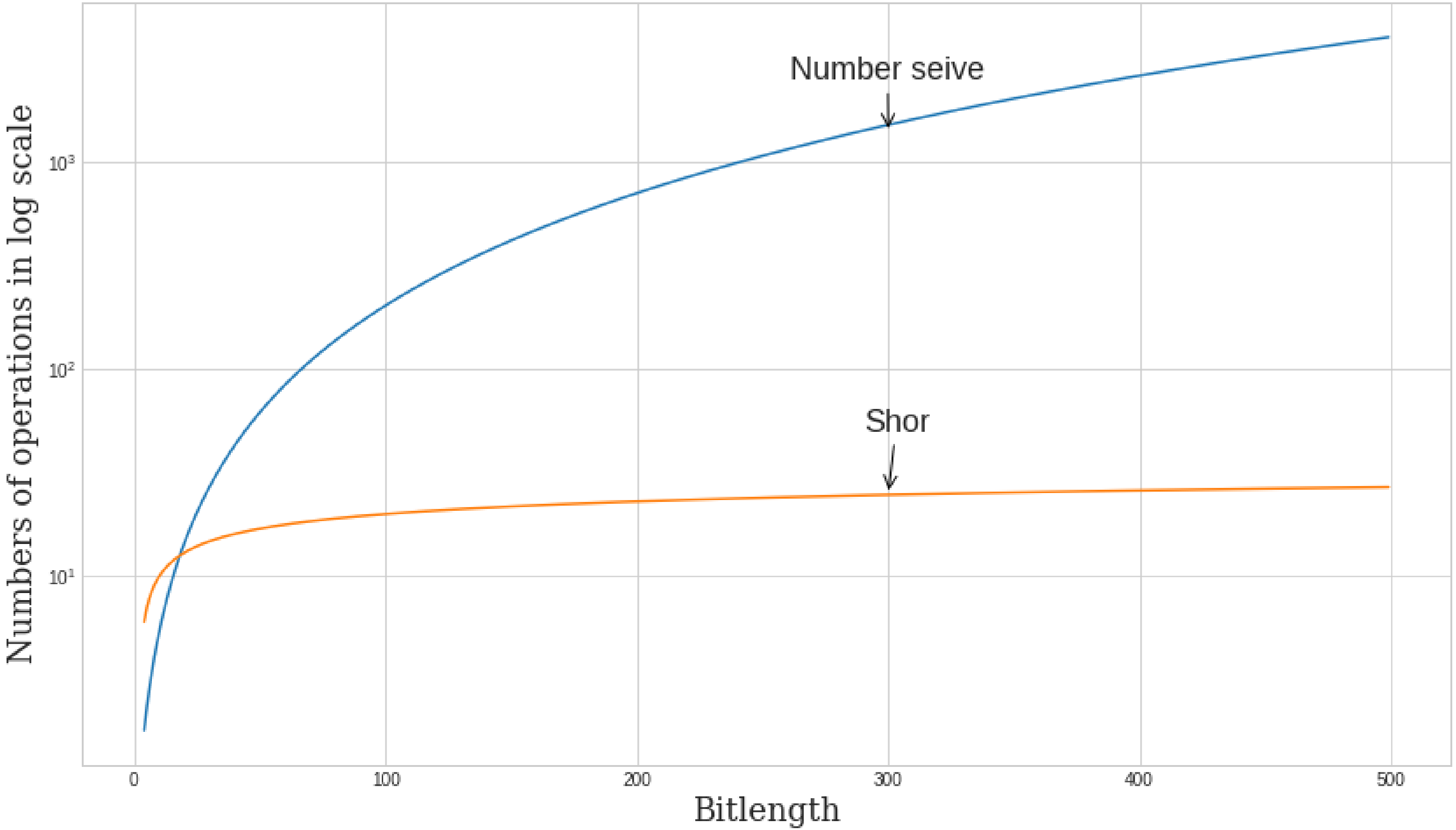


Integer Factorization

- An integer $I = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ 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 $2 \leq$ $\mathrm{x} < \sqrt{I}$ 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: $\mathcal{O}\left(\mathbf{exp}\left(\mathbf{cw^{\frac{1}{3}}(\log w)^{\frac{2}{3}}}\right)\right)$ [2](Hamdi et al.,2014)
- RSA cryptography is based on the difficulty of factoring problem


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

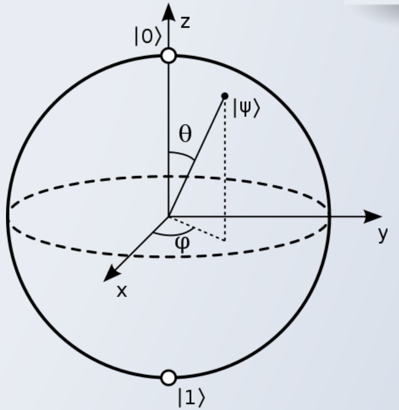
Introduction to Quantum Computing

- 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

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



- 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:

$$p = GCD\left(x^{a/2} + 1, M\right) \text{ or/and } q = GCD(x^{a/2} - 1, M)$$

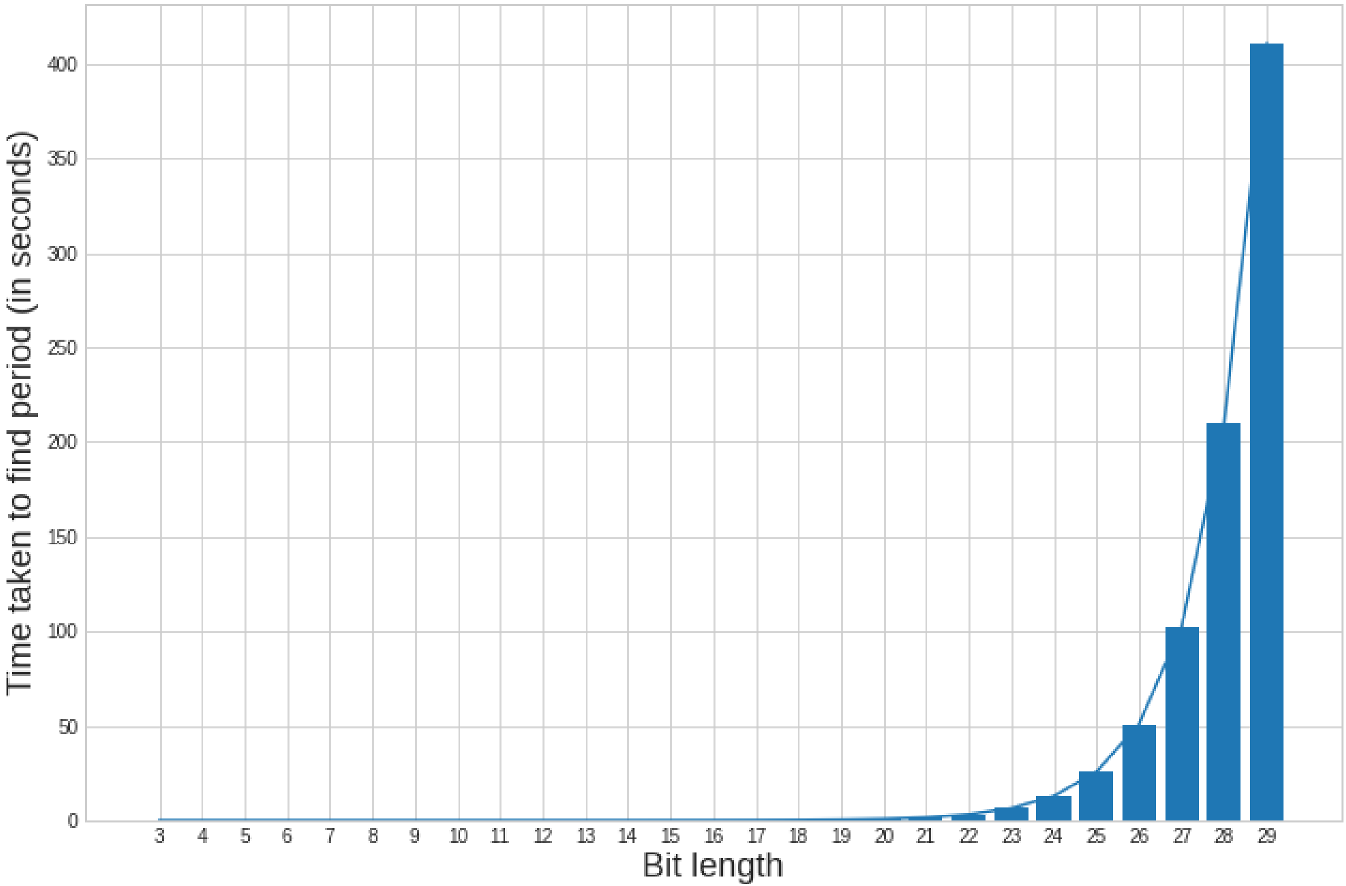


Fig: Amount of time required to find period of integer of increasing bit length

Shor's algorithm on quantum computer

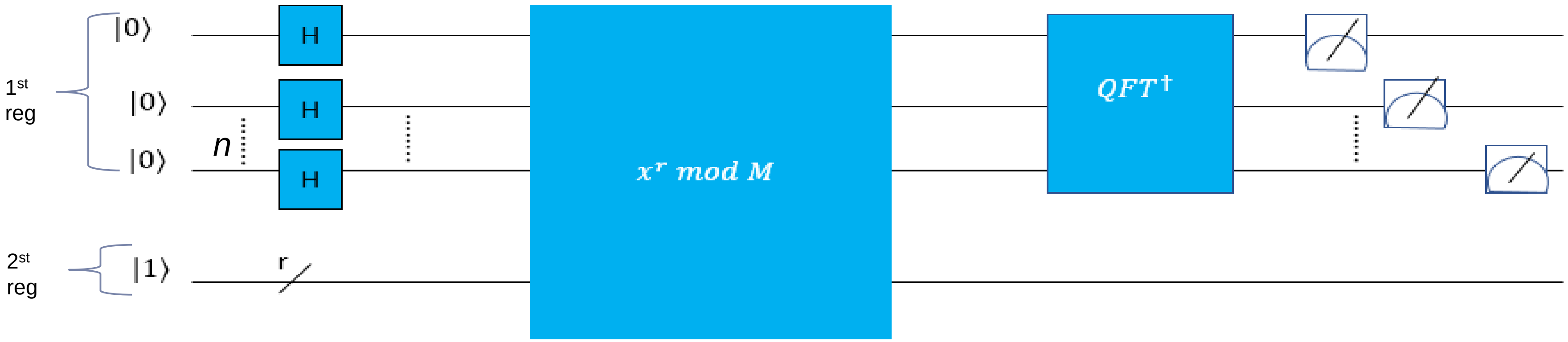


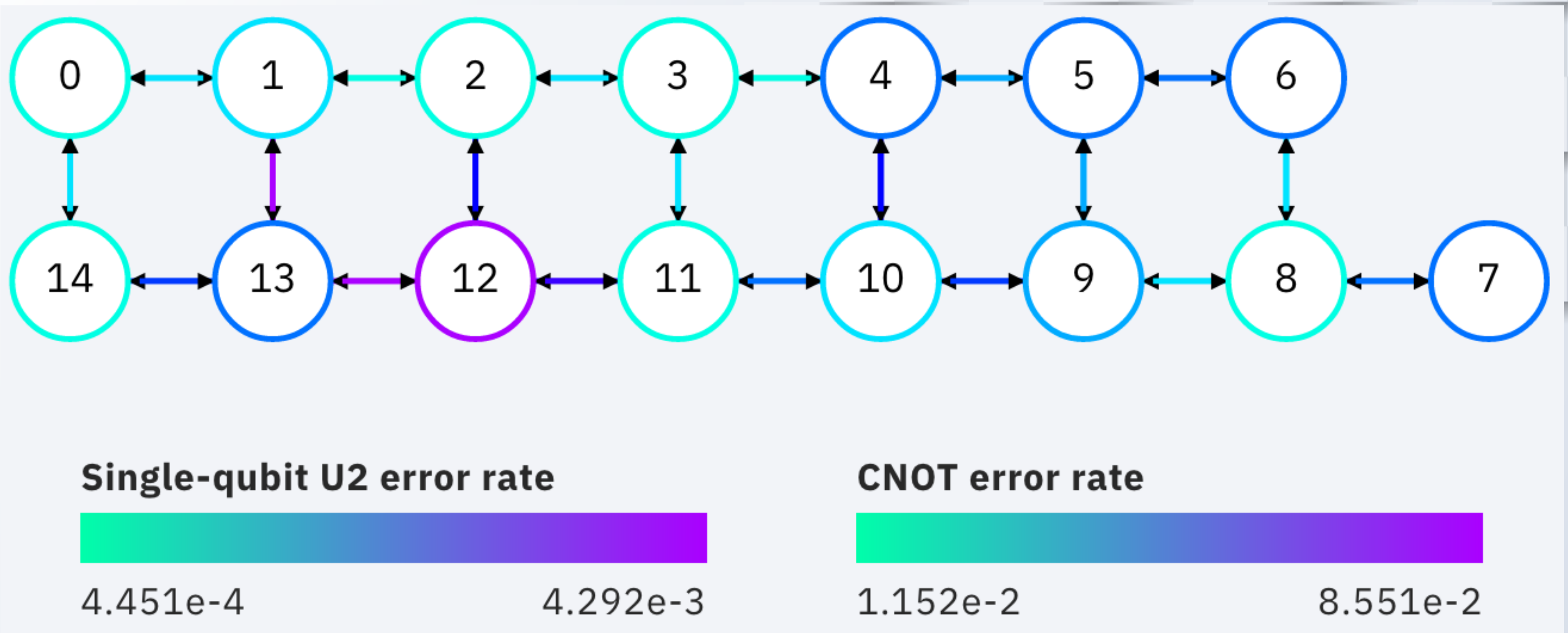
Fig : Circuit diagram for Shor's Algorithm Implementation

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

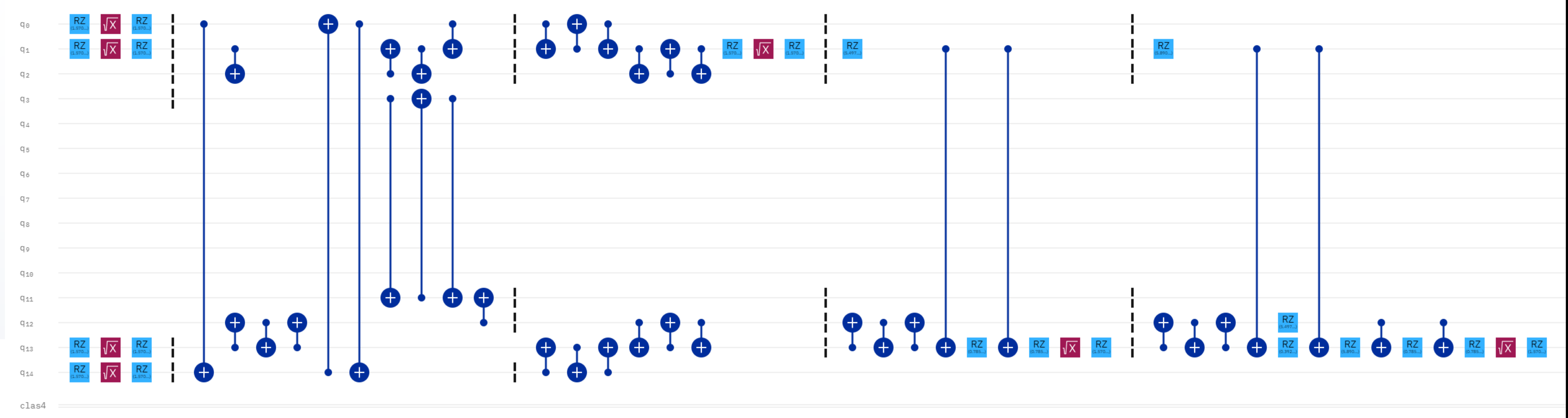
- Hadamard gates($H^{\otimes n}$) : $O(log\, M)$ - Oracle Function : $O(log^3 M)$
- QFT: $O(log^2 M)$ - Euclidian Algorithm: $O(log^3 M)$

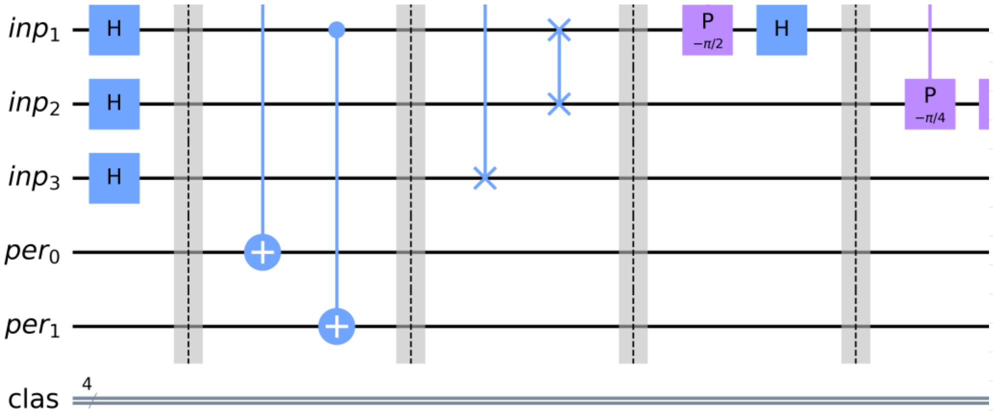
- Complexity of algorithm=$\mathcal{O}(log^3 M)$
- Hence Shor's algorithm is a Bounded error Quantum polynomial (BQP) algorithm.



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

- Qubits used: 0,1,2,3,13,14





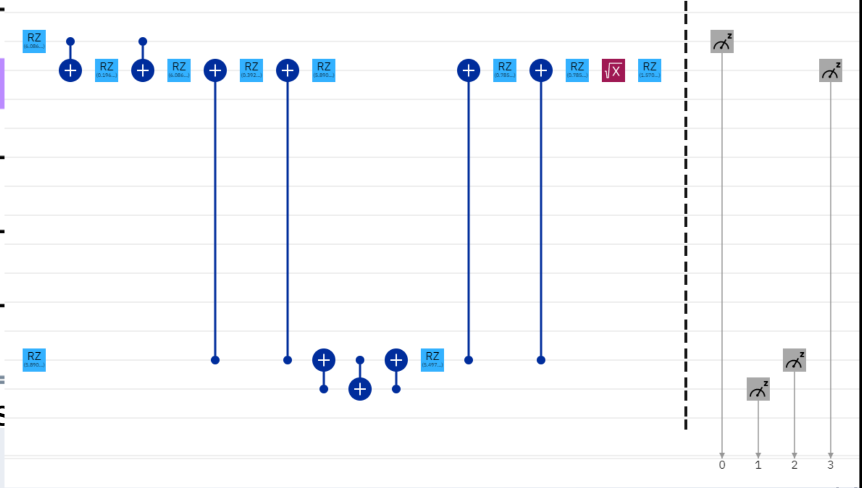
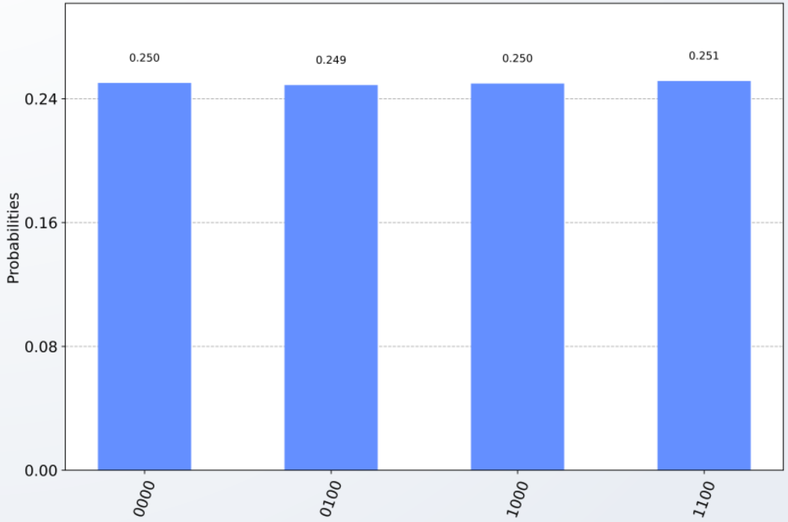


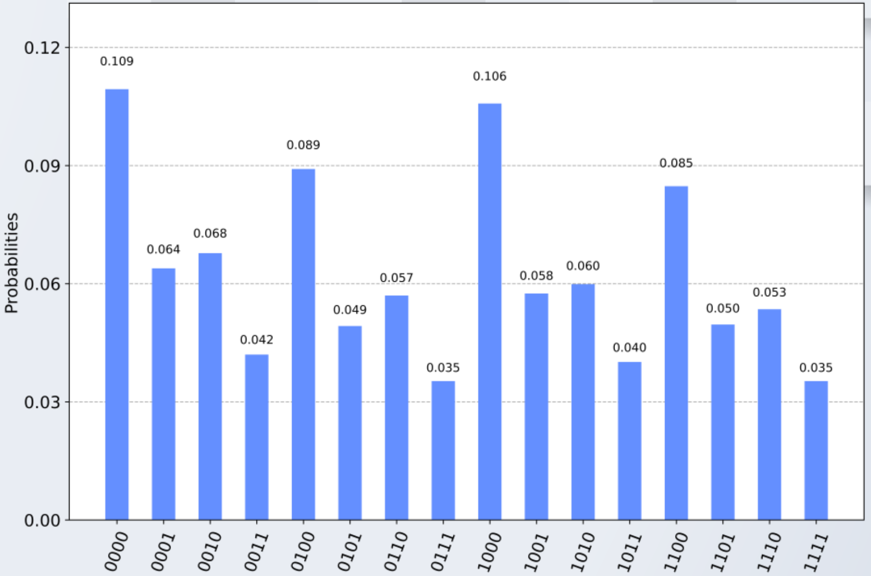
Fig: Quantum Circuit diagram for Shor's

Result

On *ibmq_qasm_simulator*



On *ibmq_16_Melbourne* QC

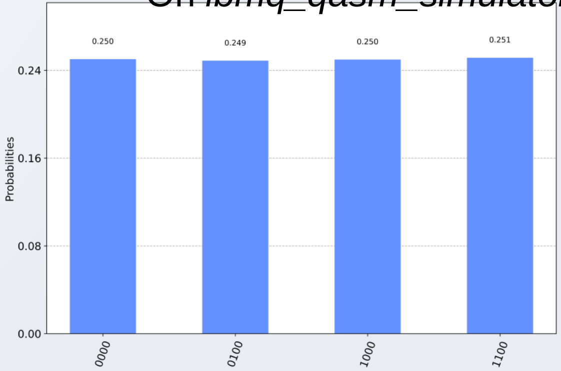


- Peaks at decimal equivalents: 0,4,8,12
- By classical processing, order a = 4
- And factors = $\mathrm{GCD}(2^2 + 1,15) = 5$ and $\mathrm{GCD}(2^2 - 1,15) = 3$
- Validation: 3*5=15.

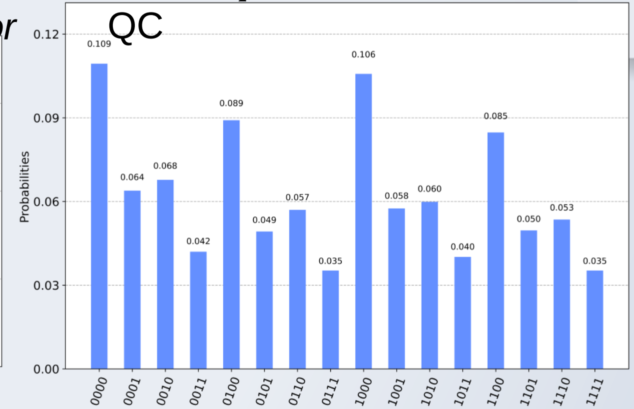
Discussion

- Dissimilarities in results
- Quantum Errors
- Scalability

On *ibmq_qasm_simulator*



On *ibmq_16_Melbourne* QC



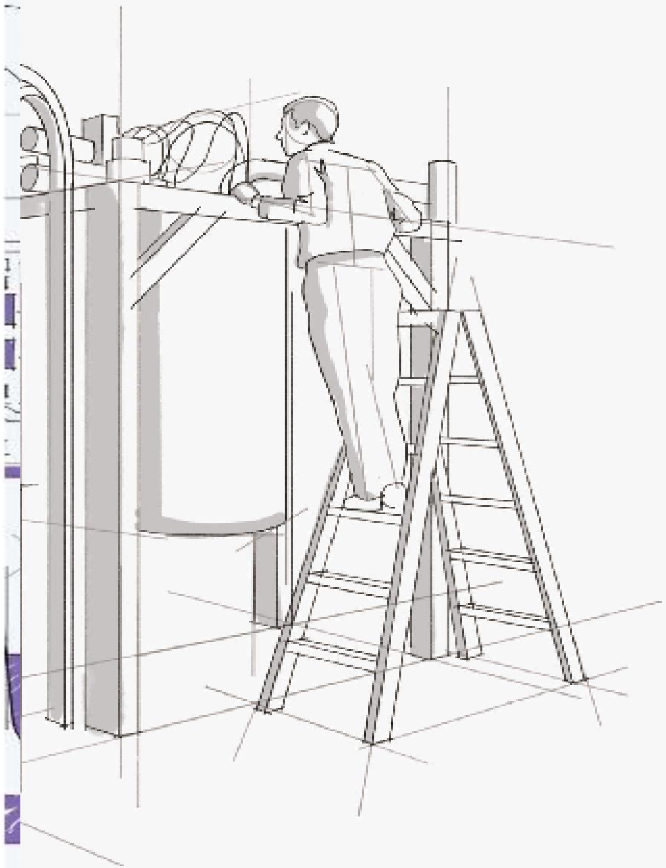
Significance: Break RSA cryptography

- A widely used cryptographic system for online data transmission including emails and online payments

```
RSA-(2048) = 2519590847565789349402718324004839857142928212620403202777713783
               6043662020707595556264018525880784406918290641249515082189298559 1
               4917618450280848912007284499268739280728777673597141834727026189 6
               3750149718246911650776133798590957000973304597488084284017974291 0
               0642458691817195118746121515172654632282216869987549182422433637 2
               5908514186546204357679842338718477444792073993423658482382428119 8
               1638150106748104516603773060562016196762561338441436038339044149 5
               2634432190114657544454178424020924616515723350778707749817125772 4
               6796292638635637328991215483143816789988504044536402352738195137 8
               636564391212010397122822120720357
```

Figure: RSA-(2048)

THANK You



Qiskit

Certificate of Proficiency

This is to certify that

Aman Ganeju

has successfully completed and received a passing score during
the final challenge of Qiskit Challenge India, demonstrating an applied
understanding of the basics of Quantum Computing using Qiskit,
plus the ability to apply and experiment with classical machine learning
techniques and the Variational Quantum Classifier (VQC) algorithm.

September 16, 2020
Date

Abraham Asfaw
Quantum Education and Open Science
IBM Quantum

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.