Quantum Decryption using Shor's Algorithm

Shreshta Mishra
shubh134lve@gmail.com
Manipal University Jaipur

Ojusav Agarwal
ojha273@gmail.com
Manipal University Jaipur

Sunil Kumar
sunilpatel.bsb@gmail.com
Manipal University Jaipur

***Abstract*—This Paper presents the generalized Implementation of Quantum Circuit utilized in Shor's Algorithm simulated using Quantum Simulator offered by IBM. Shor's Algorithm is a ground breaking Quantum Algorithm which works on Integer Factorization; for a classical computer the following task would require an exponential amount of time whereas an Quantum Computer running Shor's Algorithm would only require Polynomial time. Using the principles of Quantum Superposition and Quantum Entanglement, the algorithm demonstrates the potential of quantum computing to solve complex mathematical problems efficiently. Experimental results show the effectiveness of the implemented algorithm in Integer Factorization and discrete logarithm, disturbing the safety of major encryption algorithms. This paper contributes to advancing the understanding and practical application of quantum algorithms in real-world scenarios.**

***Index Terms*—RSA, Quantum Computing, Shor's Algorithm, Integer Factorization**

I. Introduction

Quantum Computing is starting to seem like a possible threat to all the important encryption algorithms out there. It seems we are on the verge of a new technological revolution, from Basic Arithmetic to Cryptography! Quantum Algorithms are algorithms for a quantum computer, the most famous one being Shor's Algorithm, from 1994. It resolves an important problem the complexity-theoretic community has been struggling with for a long time: that integers can be factored or – even harder – that discrete logarithms can be calculated in polynomial time. These problems are currently impossible to solve for regular computers in polynomial time, so many cryptographic algorithms in use today, such as the Rivest-Shamir-Adleman (RSA) or the Digital Signature Algorithm (DSA), rely on that fact. Shor's Algorithm makes breaking RSA and other widely used cryptographic schemes possible. If you can factor large, randomly chosen semi-prime numbers in polynomial time, you can break the most commonly used schemes for encrypting information, and that means a huge amount of research has been going on in the area of quantum-resistant cryptography.

The motivation for our work stems from curiosity towards the field of Quantum Mechanics and a need for an approach addressing the limitations of traditional method, thus developing a generalized circuit construction approach, with an aim to enhance the scalability and applicability of the algorithm for factorizing numbers.

We present a generic implementation of Shor's Algorithm on ibmq-qasm-simulator [5] using generalised programmable circuit construction. Traditional implementations of Shor's Algorithm achieve exponential speed-ups by exploiting specialised circuit construction to speed up factorisation, where the circuit construction depends on the specific number that needs to be factored. The technique introduced here as opposed to the traditional approach, with its fixed circuits specialised for a fixed number to be factorised, proves to be scalable as the input integer bit size is now used to generate the required quantum circuits.

The Architecture of the article is as follows,

- Literature Review provides an overview of existing work and developments in the field of Quantum Computing, Shor's Algorithm, and more.
- Prelim introduces the foundational concepts required for better understanding of the work, such as - RSA, Qubits, Quantum Gates, and Shor's Algorithm
- Methodology describes the approach for implementation of the quantum circuit and approach used for development of generalized circuit for Shor's Algorithm.
- Experimental results and Discussion present the findings from running the compiled quantum circuit on quantum simulator and discusses the significance of achieved results.
- Conclusion & Results summarizes the work and outlines the potential direction, future work on the project might take.

II. Literature Review

Quantum Computing with its ability to perform tasks which are considered computationally expensive for a classical computer, has garnered a significant amount of attention - with various researches performed in the field in a nimble fashion. This section provides a review over some of the work relevant to Quantum Computing, Shor's Algorithm, Quantum Error Correction, and Experimental demonstration of Quantum Hardware.

a) Foundations of Quantum Computing: Nielsen et al. (2010), in their work "Quantum Computation and Quantum Information" [10] present a foundation for understanding principles of Quantum Computing and various Quantum Algorithms. The book covered various topics such as Quantum

Mechanics, Quantum Circuits, various Quantum Algorithms, and Quantum Information Theory.

b) Shor's Algorithm: Proposed by Peter Shor (1994), layed the ground-work for Shor's Algorithm - theoretically capable of efficiently factoring large composite numbers and solve discrete logarithm problem. Shor's original work [14] demonstrated theoretical architecture for the algorithm, with a polynomial time complexity, where a classical computer requires exponential time.

c) Experimental Demonstration: Experimental study performed by Amico et al. [2] presented implementation of Shor's Algorithm using IBM Q Experience, demonstrating Integer Factorization of composite numbers on quantum processor. Skosana et al. [15] demonstrated Integer Factorization of N=21 on IBM Quantum Processor, as well as an informative display on construction of various complex quantum gates using simpler quantum gates.

d) Quantum Error Correction: Quantum Error Correction provides a way for essentially mitigating errors and noise during Quantum Computation providing a reliable way of processing quantum information. Devitt et al. [7] provided a comprehensive review of quantum error correction techniques, while also covering topics such as error syndromes, fault tolerance, and quantum error correction codes. It also helped realize the need for efficient error correction codes for fault-tolerant Quantum Computers.

e) Quantum Circuit Optimizations: Optimized Quantum Circuits are helpful in maximizing computational efficiency and resource utilization. Markov et al. [9] proposed constant optimized quantum circuit for modular multiplication and modular exponentiation, effectively optimizing modular arithmetic operations by lowering the circuit complexity and gate count. Beauregard [4] presented quantum circuit for Shor's Algorithm consisting of 2n+3 qubits consisting of $O(n^3 lg(n))$ elementary gates with depth of $O(n^3)$.

f) Quantum Noise Model: Quantum Noise Models are useful in mitigating the effect of noise and error in Quantum Computations. Barenco et al. [3] showcased the advantages of using Approximate Quantum Fourier Transform (AQFT) when decoherence in present as compared to QFT. Dimitrov et al. [8] proposed an algorithm for modular exponentiation capable of improving performance, as well as discussed the challenges of noise and error management of in quantum computations.

III. Prelims

In this section, we provide a brief overview of the work in the fields relevant to our work, such as - RSA encryption, Quantum Computing Principles, Shor's Algorithm, and more.

A. Rivest, Shamir, and Adleman (RSA) Cryptography

The Rivest, Shamir, Adleman (RSA) encryption algorithm [12] is a profound Asymmetric Data Encryption algorithm which opens the world of secured data transfer over insecure channel using public-key cryptography concept. RSA crypto-system is an encryption algorithm developed back in 1978 by three researchers Ron Rivest, Adi Shamir and Leonard Adleman. This crypto-system offers high efficiency and Mathematically strong security to both military and the civilian world. RSA crypto-system provides secure storage of cryptography key over insecure communication channels or transfer operations. Mathematics in information security has existed long before the present day – RSA crypto-system is a high efficiency and Mathematically strong crypto-system that can be considered as a milestone in the history of information security, because it introduces symmetric-key crypto-systems.

At the centre of RSA cryptography are a family of computational complexity problems, for instance the question of how hard it is to factor large semi-prime numbers into their prime factors. RSA encryption rests on the assumption that it takes a long time for a classical computer to factor large numbers into primes, and so it is computationally infeasible for that kind of computer to carry out cryptanalysis of RSA encoded messages quickly enough to jeopardise communication sent by their recipients. The security of RSA cryptography hinges on the challenge of being able to factorize semi-primes constructed using large primes quickly, such that the result acts as the public key in the crypto-system. Despite substantial increases in computational power and the development of ingenious algorithms, so far no one has discovered a mathematically efficient algorithm for factoring large numbers using classical computers. Given this lack, and the fact that there are no efficient quantum algorithms to factor numbers quickly, the widespread use of the RSA crypto-system persists.

RSA security relies on a difficult math problem such as Integer Factorization, brute forcing depends on breaking the semi-primes into their constructive primes. The security of RSA directly relates to the key size. As computers get faster, bigger keys are needed to stay secure. Although, Quantum computers act as a huge threat as they can factor numbers quickly, breaking RSA's core math problem. Quantum algorithms like Shor's could make short work of cracking today's RSA encryption sizes.

B. Quantum Computing

Quantum computing works on the fundamental concepts of quantum mechanics to carry-out computations in ways that are logically different from classical computers. Quantum Computing [11] utilizes a qubit rather than bits, the quantum counterpart of the classical bit. Dissimilar to classical bits which are capable of taking a discrete value 0 or 1, qubits on the other hand, are two-level system with the capability to be in states $|0\rangle$, $|1\rangle$, and super-position (linear combination) between both states. This property allows quantum computers to explore multiple computational paths simultaneously, providing exponential speedup for certain algorithms compared to classical counterparts. Another key concept in Quantum computing is Quantum Entanglement, a phenomena in which, independent of their distance from one another, the states of several qubits are connected in such a way that the states of one qubit simultaneously influence the states of another. Entanglement enables quantum computers to perform parallel

computations and achieve remarkable computational capability.

Quantum gates are the fundamental components of a quantum circuit, quantum counter-part to classical logic gates. These gates manipulate the states of qubits, allowing quantum computations to be performed. Some of the major quantum gates include the Hadamard gate, CNOT gate, phase gate, and more. The realization of practical quantum computers faces some major challenges, including qubit coherence times, gate fidelity, and error correction. Despite these challenges, advances in quantum hardware and algorithmic research hold promise for realizing the potential of quantum computing in solving real-world problems. A process chart showing working of IBM quantum computer is shown in Figure 1 [1].

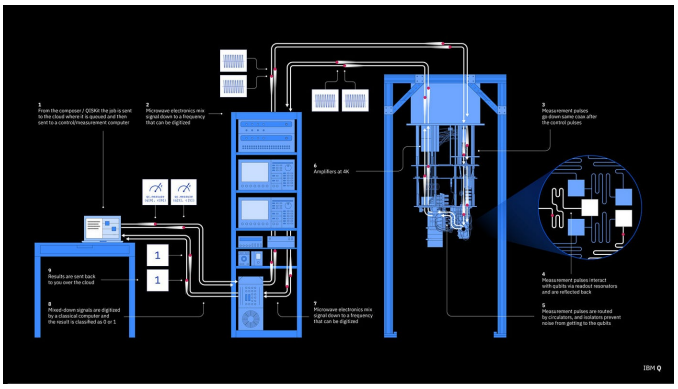

Fig. 1: IBM-Q

C. Shor's Algorithm

Peter Shor in 1994, designed a quantum algorithm named Shor's Algorithm [13], capable of efficiently performing Integer Factorization and computing discrete logarithms — two computationally expensive problems which make most cryptographic protocols secure. The algorithm's groundbreaking feature comes from its ability to factorize integer in Polynomial time unlike classical computers which require exponential time for the same task.

The classical Integer Factorization problem involves decomposing a composite number into its prime factors. Some classical algorithms used for Integer Factorization are as follows, Trial Division Algorithm, General Number Field Sieve (GNFS), have sub-exponential time complexity, making them computationally impossible for sufficiently large integers due to their exponential growth in runtime. This limitation forms the basis of many widely-used cryptographic schemes, including the RSA encryption algorithm.

Shor's Algorithm utilizes the principles of Quantum Parallelism and Quantum Phase Estimator (QPE) with Quantum Fourier Transform (QFT) to achieve exponential speedup over classical algorithms for Integer Factorization. The algorithm's key steps involve period finding in a quantum superposition and subsequent classical post-processing to extract the factors efficiently.

In the context of cryptography, Shor's Algorithm poses a major threat to the security of asymmetric cryptographic algorithms, such as Diffie-Hellman, Elliptic Curve Cryptography (ECC), and RSA, which rely on the laborious nature of Integer Factorization and discrete logarithm problems. Consequently, the development of quantum-resistant cryptographic schemes has become imperative to alleviate the potential impact of quantum computing on information security.

IV. Methodology

In this section, we describe the methodology used during implementation of generalized quantum circuit on Quantum Simulator.

A. Circuit Implementation

a) Initialization: For qubits in control register and work register - denoted as $|0\rangle^{\circledast n} |0\rangle^{\circledast m}$, Apply Hadamard gate on control register to get $H^{\circledast n}$, and apply Phase Gate on work register to get a linear combination of 2^n states in the control register with $|1\rangle$ in work register.

$$|0\rangle^{\circledast n} |0\rangle^{\circledast m} \rightarrow \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |1\rangle$$

b) Quantum Modular Exponentiation: Perform $a^x mod N$ on work registers with state $|x\rangle$ using UROT(Unitary Rotation) Gates, where $a \in Nand 1 < a < N$, $N = 2^n$:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |1\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |a^x mod N\rangle$$

$$= \frac{1}{rN} \sum_{s=0}^{r-1} \sum_{x=0}^{N-1} e^{\frac{2\pi i s x}{r}} |x\rangle |u_s\rangle$$

The following operation can be applied to Quantum Circuit using U^x operation on working register with state $|x\rangle$.

c) Quantum Phase Estimation (QPE): Perform Controlled Unitary Rotation operation on all qubits in controlled register.

$$|\psi_0\rangle = |0\rangle^{\circledast n} |v\rangle \tag{1}$$

$$|\psi_1\rangle = [(\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \circledast (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \circledast ... \circledast \frac{|0\rangle + e^{i\theta} |1\rangle}{\sqrt{2}}] |v\rangle \tag{2}$$

$$|\psi_2\rangle = [(\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \circledast (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \circledast ... \circledast (\frac{|0\rangle + e^{2i\theta} |1\rangle}{\sqrt{2}}) \circledast (\frac{|0\rangle + e^{i\theta} |1\rangle}{\sqrt{2}})] |v\rangle \tag{3}$$

...

$$|\psi_n\rangle = [(\frac{|0\rangle + e^{2^{n-1} i\theta} |1\rangle}{\sqrt{2}}) \circledast (\frac{|0\rangle + e^{2^{n-2} i\theta} |1\rangle}{\sqrt{2}}) \circledast ... \circledast (\frac{|0\rangle + e^{2i\theta} |1\rangle}{\sqrt{2}}) \circledast (\frac{|0\rangle + e^{i\theta} |1\rangle}{\sqrt{2}})] |v\rangle \tag{4}$$

where, $|\psi_0\rangle \rightarrow$ eigen-state prior first unitary operation, $|\psi_1\rangle \rightarrow$ eigen-state after first unitary operation, $|\psi_2\rangle \rightarrow$ eigen-state after second unitary operation, $|\psi_n\rangle \rightarrow$ eigen-state after nth unitary operation, and $|v\rangle \rightarrow$ eigen-state mth qubit in work register.

After which, Inverse Quantum Fourier Transform [6] is to be applied as shown below and in Figure 4.

d) Quantum Fourier Transform (QFT) and Inverse QFT: Apply Inverse Quantum Fourier Transform to get period from the equation,

$$QFT\,|x\rangle = |\widetilde{x}\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle \tag{5}$$

Let,

$$|\widetilde{x}\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i x \sum_{k=1}^{n} \frac{y^k}{2^k}} |y_1 y_2 ... y_n\rangle \tag{6}$$

$$|\widetilde{x}\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \prod_{k=1}^{n} e^{\frac{2\pi i x y k}{2^k}} |y_1 y_2 ... y_n\rangle \tag{7}$$

$$Since, |y\rangle = |y_1 y_2 ... yn\rangle = |y_1\rangle \circledast |y_2\rangle \circledast ... \circledast |y_n\rangle$$

$$|\widetilde{x}\rangle = \frac{1}{2^{\frac{n}{2}}}[(|0\rangle + e^{\frac{2\pi i x}{2}} |1\rangle) \circledast (|0\rangle + e^{\frac{2\pi i x}{4}} |1\rangle) \circledast ... \circledast (|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle)] \tag{8}$$

Hence, Signifying that Unitary Rotation Operation can be used to apply Quantum Fourier Transform and Inverse Quantum Fourier Transform.

Inverse Quantum Fourier Transform is conjugate transpose of Quantum Fourier Transform as shown below in Figure 3.

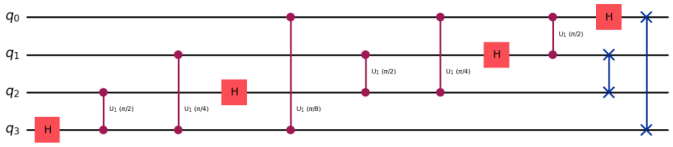

Fig. 2: Compiled Quantum Circuit for QFT

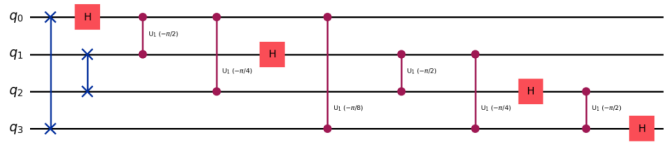

Fig. 3: Compiled Quantum Circuit for IQFT

e) Probability Measurement: For the resulting equation,

$$|\psi\rangle = [(\frac{|0\rangle + e^{2\pi i(\frac{j_{m-1}}{2})} |1\rangle}{\sqrt{2}}) \circledast (\frac{|0\rangle + e^{2\pi i(\frac{j_{m-2}}{2} + \frac{j_{m-1}}{4})} |1\rangle}{\sqrt{2}}) \circledast ... \circledast (\frac{|0\rangle + e^{2\pi i(\frac{j_0}{2} + \frac{j_1}{4} + ... + \frac{j_{m-1}}{2^m})}}{\sqrt{2}})] |v\rangle \tag{9}$$

$$Probability of\,|0\rangle = |\tfrac{1}{2}(1 + e^{i\theta_\psi})|^2$$

$$Probability of\,|1\rangle = |\tfrac{1}{2}(1 - e^{i\theta_\psi})|^2$$

Thus, The outcome of Shor's Algorithm is probabilistic in nature, with the precision directly proportional to number of qubits(in control register).

f) Period Measurement: Using continuous fractions, The resulting equation converges to $\frac{z}{r}$, where $r \rightarrow$ period.

B. Generalized Circuit

In this section, we present our implementation of Shor's Algorithm using a generalized approach. Traditional approach for Shor's Algorithm utilize predefined circuits constructed

a) States: The total states are divided into two separate states based on the following conditions,

(i) Fundamental States : Consisting of 2^k, where $k \in Z$ and $0 < k < \lceil \log_2 N \rceil$

(ii) Derived States : Consisting of $N - 2^k$, where $k \in Z$ and $0 < k < \lceil log_2 N \rceil$

b) Modular Exponentiation: For a random integer a, We apply Left Shift or Right Shift on qubits based on their relative value for bit_1 and bit_2 fundamental state and derived state.

- If the value of Fundamental state is greater than Derived state : We set bit_1 equal to 0 and bit_2 equal to 1. Then, we swap the value of qubit at bit_1 and bit_2 to perform right shift and increment the value of both bit_1 and bit_2 by 1 until the value of bit_2 is less than position of last qubit.
- If the value of Derived state is less than Fundamental State : We set bit_1 equal to index of last qubit and bit_2 with value of bit_1 decreased by number of work bits, decrementing by 1 at every iteration until bit_1 is greater than 0.
- If a is a Derived state : Append an X-Gate in quantum circuit at the position of current qubit.

V. Experimental Results and Discussion

In this section, we present the results achieved using our generalized implementation on Shor's Algorithm, as well as the finalized circuit .

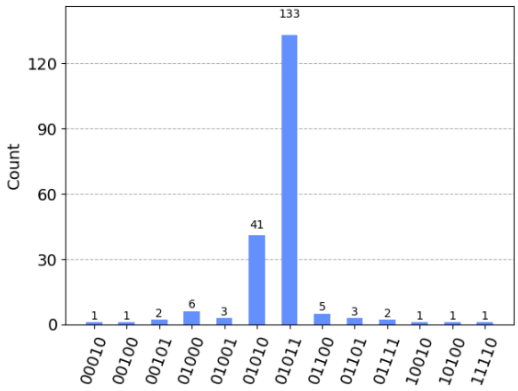

Fig. 4: Hits for Compiled Quantum Circuits

The hits achieved on quantum simulator upon running compiled quantum circuit running for 200 shots are shown above in Figure 4.

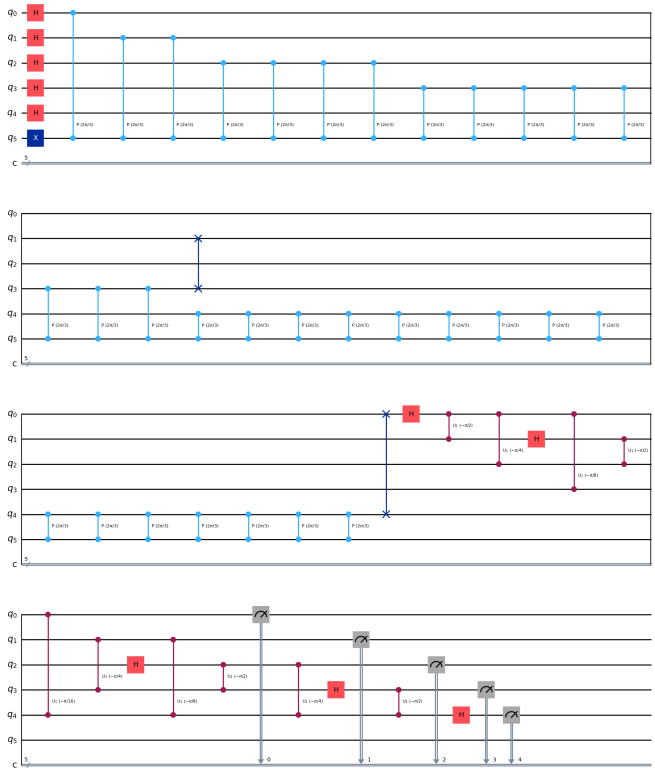

Fig. 5: Compiled Quantum Circuit showing the final circuit for N=15

The finalized circuit generated using generalized approach for $N = 15$ is shown above, consisting of quantum gates used for implementation of Quantum Phase Estimator (QPE), Inverse Quantum Fourier Transform (IQFT) according to circuit shown in Figure 3.

Upon running the circuit for N=15 shown in Figure 5, multiple attempts using random integers are required for Integer Factorization. In final attempt, for a random integer - multiple qubit swap operations are performed effectively performing modular exponentiation as shown below,

- Random Integer $= 13$
- Fundamental States $= (2, 4, 8)$
- Derived States $= (7, 11, 13)$
  Applied Qubit Swap between (2, 3)
  Applied Qubit Swap between (1, 2)
  Applied Qubit Swap between (0, 1)
  ...
  Applied Qubit Swap between (2, 3)
  Applied Qubit Swap between (1, 2)
  Applied Qubit Swap between (0, 1)
- Qubits $= 4$
- Register Reading $= 10111110$
- Corresponding Phase $= 0.7421875$
- Estimated Period $= 4$
- Estimated Factor $= (3, 5)$

Hence, giving the final non-trivial estimated factors for N=15 as 3 and 5.

A. Discussion

In this section, we discuss the findings when using the proposed approach as well as various challenges faced during implementation.

a) Limitations and Challenges: 1. Circuit Depth and Qubit Coherence: As the size of input number increases, the depth of quantum circuit required for factorization also increases, resulting in potential challenges to maintain and balance qubit coherence during the computation process.
2. Gate Fidelity and Error Correction: High gate fidelity is crucial for accurate computations in quantum mechanics. During quantum gate operations, errors pop up in the circuit which can impact the reliability of the algorithm. Correction techniques are required to mitigate these errors and improve gate fidelity to overcome these challenges in quantum algorithm design and implementation.
*3. Resource Constraints:*Building Quantum hardware is very complicated and resource intensive and not Quantum Simulation softwares are not widely available. Computation resources like qubits and quantum gates are very limited. Factorizing large numbers may require significant computational resources beyond the capabilities of current quantum platforms, emphasising the need for scalable and efficient algorithms.

b) Practical Implications: 1. Circuit Depth and Qubit Coherence: There are certain limitations in the implementation of Shor's Algorithm on current quantum simulators due to circuit depth restrictions and qubit coherence times as already discussed above, when the size of the input number increases, the depth of the quantum circuit required for factorization also increases which leads to difficulty in maintaining qubit coherence.
2. Key Exchange and Secure Communication: Advances in Quantum computing presents opportunities for enhancing key exchange protocols and secure communication mechanisms. Quantum Key Distribution (QKD) protocols utilizes the laws of quantum mechanics, such as No-Cloning theorem (which

states that it is not possible produce identical copy of unknown state) to establish safe communication channels resistant to eavesdropping attacks as the system will change upon observation due to intervention of photon particles in optical cables. The deployment of quantum networks in the communication domain could revolutionize secure data transmission in various sectors, including government, finance and healthcare.

3. Cryptography Standardization Efforts: We need to standardise quantum cryptographic algorithm after the emergence of quantum computing. The development and assessment of cryptographic systems that are resistant to attacks from both classical and quantum adversaries requires a global effort. Standardization guarantees security, compatibility, and interoperability in upcoming cryptographic systems.

VI. Conclusion & Future Scope

In conclusion, this paper presents a generalized implementation of Shor's Algorithm for Integer Factorization on a quantum simulator, using a novel approach based on generalized circuit construction. By leveraging the principles of quantum mechanics and utilizing the Qiskit library, Shor's Algorithm demonstrates the exponential speedup in time complexity and computation over classical factorization methods, highlighting the transformative potential of quantum computing in solving computationally challenging problems.

The algorithm's efficacy in factorizing huge numbers is demonstrated by the experimental results, spot-lighting the probable applications of quantum computing in cryptography and other computational domains.

However, the implementation of Shor's Algorithm also faces some challenges, including circuit depth restrictions, qubit coherence times, and gate fidelity issues. Looking ahead, the practical implications of Shor's Algorithm extend beyond cryptographic security including exchange protocols, secure communication mechanisms, and cryptography standardization efforts.

As quantum computing technology develops, businesses and industries have to start preparing for the transition to quantum technologies and invest into research, education and infrastructure, making the quantum computing global benefits a reality.

Overall, this study is a contribution to the quantum computing frontier, towards improving the design and practical implementation of quantum algorithms. In particular, on engineering quantum computers to factorise large integers, and towards a quantum cryptography future. By addressing the current challenges, it opens up dimensions for going beyond the current limitations to quantum computing to new opportunities. It is a way towards an alternative future of quantum technologies remaking our world.

A. Future Scope

a) Integration of Quantum Bit Adder: Future research into the addition of a quantum bit adder component to Shor's Algorithm seems very promising. Further studies could investigate the possibility of improving computing efficiency in Integer Factorization problems by integrating quantum adder circuits into the already existing implementations. Exciting prospects for improving quantum algorithms and optimization arise from this study.

b) Development of Quantum Noise Model: A trace-preserving transformation is a characteristic of a noisy quantum channel. In the quantum communication channel, decoherence is inevitable, which causes the quality of entangled states to generally decline with channel length. Quantum noise is crucial for improving practical quantum computing systems. We could focus on the development and refinement of quantum noise models to capture the effects of noise and errors in quantum computing accurately. Incorporation of realistic noise models into quantum simulators and hardware platforms can give deeper insights into the behavior of quantum systems and devise strategies for error mitigation and fault tolerance. This integration can help advance quantum systems and enhance computing technologies.

References

[1] 2019. Electronics360.

[2] Mirko Amico, Zain H Saleem, and Muir Kumph. Experimental study of shor's factoring algorithm using the ibm q experience. *Physical Review A*, 100(1):012305, 2019.

[3] Adriano Barenco, Artur Ekert, Kalle-Antti Suominen, and Päivi Törmä. Approximate quantum fourier transform and decoherence. *Physical Review A*, 54(1):139, 1996.

[4] Stephane Beauregard. Circuit for shor's algorithm using 2n+ 3 qubits. *arXiv preprint quant-ph/0205095*, 2002.

[5] Andrew Cross. The ibm q experience and qiskit open-source quantum computing software. In *APS March meeting abstracts*, volume 2018, pages L58–003, 2018.

[6] GM D'Ariano, Chiara Macchiavello, and MF Sacchi. On the general problem of quantum phase estimation. *Physics Letters A*, 248(2-4):103–108, 1998.

[7] Simon J. Devitt, Ashley M. Stephens, William J. Munro, and Kae Nemoto. Quantum error correction for beginners. *Reports on Progress in Physics*, 76(7):076001, 2016.

[8] Vassil S Dimitrov, Graham A Jullien, and William C Miller. An algorithm for modular exponentiation. *Information Processing Letters*, 66(3):155–159, 1998.

[9] Igor L Markov and Mehdi Saeedi. Constant-optimized quantum circuits for modular multiplication and exponentiation. *arXiv preprint arXiv:1202.6614*, 2012.

[10] Michael A. Nielsen and Isaac L. Chuang. Quantum computation and quantum information. *Cambridge University Press*, 2010.

[11] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[12] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[13] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[14] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[15] Unathi Skosana and Mark Tame. Demonstration of shor's factoring algorithm for n= 21 on ibm quantum processors. *Scientific reports*, 11(1):16599, 2021.