THE INCREASING THREAT TO DIGITAL ASSETS DUE TO THE DEVELOPMENT OF QUANTUM ALGORITHMS

Basil Hanafi, Mohammad Ubaidullah Bokhari, Imran Khan

Department of Computer Science, Aligarh Muslim University, Aligarh

ABSTRACT

The development in this digital era is fast pacing up to the future where machines will be able to perform tasks more efficiently and rapidly than even today's supercomputers aren't able to perform. Increasing technology and exponential development in the domain of Quantum Computing are leading humanity to the future where Computers will be able to solve unsolvable or exponential time-consuming problems in a span of short time. This will be proved advantageous in numerous ways but as every state of development has other aspects, this development will also be able to break down every possible cryptographic algorithm implemented in the classical computing era as they all are based on complex mathematical equations and calculations. A perfectly implemented Quantum Computer will be able to compute the mathematical calculations in parallel due to the phenomenon of Superposition and entanglement. All possible progress in Quantum Algorithms is discussed in the context of digital security in this paper which can be a possible threat to every executed cryptographic algorithm and securities instigated through them.

KEYWORDS

Quantum Computing, Quantum Computers, Quantum Algorithms, Cryptography, Security.

1. INTRODUCTION

Every technology today is being initiated to be established in a way such that it can solve the problems which a human wasn't able to solve in the past and will not be able to solve in the future as well. In this rapidly moving and the advancing world we are heading to a future with the minimized size of portable machines with significantly high computing Power. In the early stages of development, Gordon Moore stated and proved that every technology will get obsolete every two years as the number of transistors in a dense Integrated Circuit will get doubled within that span of time [1]. Although this development will get stopped somehow eventually in the near future as no one can go subatomic when it comes to using them for computational technology and related purposes. Here to overperform in this situation Quantum Computers and the concept of quantum computing can come into play. Quantum Computers work on the principles of quantum physics and Linear Algebra where the Qubits are the primary unit for Computation just like bits in the case of Classical Computing. The States are probabilistic in the case of Quantum computing, unlike Classical computing where the states are Deterministic as the Qubit can be in more than one state during computation and it can be evaluated on the basis of their respective probabilities along with their associated coefficient [2].

In present times, every problem is can be categorized into one of the three following categories:

1. P, Polynomial-time Problems that can be solved in Polynomial time. In the worst case, the size of the input will be the running time of the problem to get solved when executed.

2. NP, Nondeterministic Polynomial time problems are those problems in which the answer can be verified as correct or not in Polynomial-time.
3. NP-Complete, are the problem from a set belonging to P and the set equals NP.

The Problems which are can be solved in Polynomial time or less are termed Tractable, otherwise are termed Intractable. Classical Computing works pointedly well with Tractable problems, whereas Intractable problems can have potential solutions when implemented through Quantum Computing Concepts as using the superposition and entanglement concepts large exponential time calculations can be done very quickly due to simultaneous exploration of solutions.

The concept of Quantum computing is not very new but it was given years ago and now it is presently being applied to give a physical form of a machine for the purpose of computation. Humans might not be able to use the idea of Quantum computers as present-day desktop systems, but still, they will be able to surpass present-day computing machines in cases where classical computing requires exponential time to run an algorithm. Also, not always a Quantum computer will be performing better than the machines presently being used for the sake of computation, it will only perform better significantly when the complexity of an algorithm is exponential. There are a number of organizations that are working and researching the physical existence of Quantum Computers and providing the initial stage of the developed model to the users for academic and scientific purposes like IBM. Such initiatives are giving a huge hike in the development of Quantum Computers and related research in the domain [3].

There are several Algorithms that are already developed and got deployed on the cloud services of Quantum Computers which are showing significant performances and got executed in a very minimal time when compared to machines based on classical computers. These algorithms are termed Quantum Algorithms and the deployment of Quantum Algorithms is one of the key achievements as Quantum computation works in parallel due to the concept of Superposition and entanglement [4]. These Quantum algorithms are proof the concept of computation will get revolutionized, whereas every technological development has its own bottlenecks. In a similar manner, Quantum Algorithms are also having some disadvantages when they come to practical implications. Quantum Algorithms will be a major threat to the digital security of the present-day era. As present-day security is based on cryptographic algorithms from maintaining integrity to confidentiality, spanning from Digital Signature to key Exchange. These Cryptographic algorithms work on complex mathematical and logical computation which requires time of enormous duration to break down without knowing the exact methodology to break the security based on that encryption Algorithm. Then there comes a situation where a Quantum computer comes into play that can compute calculations, which requires years of time with present-day computers, into seconds [5]. This scenario will lead to the compromise of every possible security position to all the highly sensitive organizations containing all kinds of digital assets around the globe. This Paper will be containing a thorough study related to such Quantum Algorithms which can be a possible threat to all the deployed Cryptographic Algorithms for maintaining security in the digital world. The whole paper will be composed into 6 different sections, namely Introduction, Related works, Quantum Computing and Quantum Computers, Quantum Algorithms, Idea of Compromising security in Post Quantum Era, Conclusion, and Future Extension.

2. RELATED WORK

The concept of Quantum Computing is based on the concepts of Quantum Physics. It works significantly fast when compared to classical computing and its related machines. The field is continuously growing and evolving with time as a Quantum Computer will be able to solve a number of problems. One of the Primary concerns to tackle is the idea of protecting security

systems in the post-Quantum Era as every possible security implemented will get compromised as everything is presently working on mathematical concepts executed on classical computing of Boolean Algebra. The Cryptographic Algorithms like RSA will get threatened as the calculations required will be done in a short span of time. RSA is can be bought down using 3 kinds of attack categories which are Protocol attacks, Mathematical attacks, and Side-Channel Attacks [6].

Quantum Algorithms are being used for various purposes, one of the applicability of Quantum Algorithms is for face detection and Recognition implemented through neural networks as it is significantly distinguishable from the execution of the NP-Complete Problem [7]. The concept of Quantum Algorithms is also applied to Monte Carlo Integration using Quantum Amplitude estimation since it provides substantial execution speed [8].

For the case of Machine Learning Algorithms and Evolutionary Algorithms, in most cases when data is quite large for Analytics the executed code takes enormous time to execute. Quantum Computers can execute such programs in a span of few minutes even if it requires a lot of time over classical computers. Because of this the results and predictions made by machine learning and the evolutionary algorithms can be optimized in an efficient manner [9].

Pattern Recognition is considered one of the most challenging tasks even with the powerful computers of present times because of its time-consuming behavior due to its multidimensionality. Grover's Search Algorithm and Quantum Wavelet Transform is can be used for the cause of Pattern Recognition in time efficient manner for data with high resolution and dimensionality [10].

The Physical existence might be recorded recently but conceptual studies are being done for a very long time back. The Quantum algorithms are can be used to solve Partially Observable Markov Decision-making Processes in various forms of applicability ranging from optimization to estimation and searching [11].

Quantum Amplitude Amplification is one of the ways which can be utilized for finding claws and collisions in functions of any order [12]. All of the above-mentioned claims are just the tip of the Ocean when it comes to the applications of Quantum Algorithms. There is a wide range of applicability of Quantum Algorithms in Security as well. Quantum algorithms are can be used for breaking Data Encryption Standards due to the swift speed of execution [13].

It is also proposed to use Quantum Computing for the purpose of creating Quantum-Safe Security solutions for IoT devices deploying through the network of drones termed the internet of drones IoD, which can be a huge leap for securing IoT devices in Post Quantum Era where all other algorithms working on Classical Cryptosystem Strategies, like Elliptic Curve Cryptography, RSA, Diffie Hellman, might get compromised using Shor's algorithm [14]. Quantum computing is also can be used for the process of Digital Signature using the CFS digital signature algorithm with slight variations which can reduce the storage space of the public key and improvise efficiency when Quasi-Cyclic Low-Density Parity Check (QC-LDPC) code and the Belief Propagation (BP) decoding algorithm is used for the process [15].

Apart from all so much versatility in the applications of quantum computing, the major threat which is again being mentioned is the compromising of the classic cryptosystems. There are several ways through which it could be done using quantum algorithms. The new methodologies are can be developed to protect digital systems in the post-quantum era by working out on all the presently existing security systems and overcoming their respective bottlenecks in terms of quantum computing [16].

3. QUANTUM COMPUTING AND QUANTUM COMPUTERS

Quantum Computers are the ideas of a physically working machine working over the concept of Quantum Computing which performs computational tasks based on Linear Algebra instead of Boolean Algebra like traditional classical computers. The notion behind the concept was to develop a machine or a method to solve problems that today's computers will not be able to solve. Quantum Computing is different than Classical computing in numerous ways, it will be better to say it is a totally distinct method to design a highly powerful computational machine. There are some important points that differentiate between the two types of Computation, which are mentioned below:

1. The primary key difference between both kinds of computational methodology is its unit of computation which is Bit in Classical Computing and Qubit in Quantum Computing. Bits in Classical Computing can be in either of the two States (o or 1) where the States are deterministic. On the other hand, Quantum Computing works on the computational units known as Qubits which are Unit Vectors that can be in a state which is a linear combination of 0 and 1, labeled as a superposition. The Qubit q is can be represented as

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle$$

Where α and β are complex numbers as coefficients to measure probability, as the states are probabilistic.

2. One more important difference between the two computational methods is that the logical problems are solved using Gates based on the principles of Boolean Algebra. These Boolean gates like AND, OR, NOT, NAND, NOR, and XOR are the foundation pillar of Classical Computing. On the other hand, In Quantum Computing, Gates are represented by Matrices of Linear Algebra instead of Boolean Functions. To Change the State or make transitions of Logical decision making a Linear Transformation is performed for producing a new state. This gives similar results to classical computing but differs in internal mathematics running behind. In Quantum Computing there are also a number of gates available for performing computation and logical decision making like the Pauli-X Gate, Pauli-Y Gate, Pauli-Z Gate, Hadamard Gate, etc.

3. Another key difference between Classical and Quantum Computing is that the operations in Classical Computing are irreversible whereas when it comes to Quantum Computing the operations are reversible as they work on mathematical operations of linear algebra and linear transformation based on Matrices. Hence, the gates involved in computation in Quantum Computing are nothing but Matrices. For Example, the Classical Computing NOT gate is observed to give similar outputs as the Pauli-X gate of Quantum =Computing as illustrated in figure 1.

Figure 1. Comparison of Classical NOT gate in Boolean Algebra and equivalently performing Pauli-X gate.

4. QUANTUM ALGORITHMS

The term Quantum Algorithm is given to the algorithms and paradigms intended to be implemented on Quantum Computers for ominously fast computation and problems requiring years to give output. There was a very less in number of Algorithms available to be implemented on Quantum Computer long before its actual existence. Various research and mathematical calculations are being conducted to get something like Quantum Algorithm which can solve a problem exponentially fast compared to classical computers. Such Quantum Algorithms are designed such that they can be run efficiently on the realistic implementation of a Quantum Computer. These Quantum Algorithms are able to work proficiently because they are designed over the concepts of Quantum Physics like Superposition and Entanglement [18].

This notion of using Quantum Computers and executing Quantum Algorithms for solving almost impossible problems is termed Quantum Supremacy. In the present world scenario various Quantum Algorithms are available and more going to be added to the lists with each passing year. So, to confine everything to a single statement it will be better to say that Quantum Algorithms are defined in such a way that they could only be implemented on the Circuits made for Quantum Computation which take some Qubits as an Input and gives its corresponding measurement for some real values as Output or Answer [19].

There are a number of methods by which Quantum Algorithms can be characterized, one of them is to classify Quantum Algorithms into various categories on the basis of the technique which is being used for computation like Quantum Fourier Transformation, Amplitude Amplification, Quantum Walks, Phase estimation, etc. Another method is to categorize Quantum Algorithms on the basis of the usage or the problem which is being solved. The categorization is can be understood in detail by observing the following figure 2 [20].

Figure 2. Classification of Quantum Algorithm based on the technique used.

The primary intention here is to focus on the Quantum Algorithms which can be used to break security and implemented cryptographic algorithms in the modern world scenario. The concept of Post Quantum Cryptography is introduced to tackle problems that can arise because of cryptanalytic attacks performed by Quantum Computers. The cryptographic notion applied to handle such Quantum Computer threat is termed Post Quantum Cryptography. The solutions offered to date are considered Quantum Safe Solutions, some of the basic types of Quantum Safe Solutions are

1. One-Time Signature (OTS) systems based on hash functions like Lamport-Diffie are offered by quantum-safe hash-based cryptosystems [21]. Instead of the difficulty of a mathematical problem, the security of such cryptosystems only depends on the collision resistance of the selected cryptographic hash function. Ralph Merkle, who suggested a signature method based on a one-way function [22], presented them originally. The Merkle tree method is the ancestor of contemporary hash-based cryptosystems, which are seen as good candidates for quantum-safe cryptosystems.

2. Quantum-safe based on code the principle of error-correction codes, which has been used to provide redundancy to digital communications, is basically being adopted by cryptosystems. By either introducing random mistakes into the transmission or encoding a message in the error sequence, the plain text is changed into a codeword. By erasing the mistakes or extracting the original input message from the errors, decryption is carried out. As a result, it is essential to hide the text's algebraic structure.

3. Miklos Ajtai [23] first presented quantum-safe lattice-based cryptosystems by creating stable cryptographic algorithms based on the hard lattice problem (NP). The lattices are collections of points having a periodic structure in n-dimensional spaces. The issue with the closest vector (CVP), the problem with the shortest vector (SVP), or the Shortest Independent Vectors Problem are often the foundations of lattice-based cryptosystems (SIVP). Lattice-based cryptographic algorithms provide a quick and easy implementation together with reliable security justifications. Lattice-based cryptography uses a number of straightforward issues, such as finding the shortest non-zero vector in the lattice using SVP, an NP-hard task that is often quantum-resistant, and

4. Quantum-safe Systems of multivariate equations that have been shown to be NP-hard or NP-complete serve as the foundation for multivariate cryptosystems [24]. Although quantum assaults may be tolerated, they nonetheless present a number of difficulties and inefficiencies for systems with limited resources. Due to the required "guesswork," their decryption performance is rather inefficient on devices with limited resources. Additionally, the presence of huge ciphertext overhead necessitates a considerable amount of processing power. In order to address the aforementioned issues, it is now essential to create and deploy optimized encryption and signature methods.

Other alternative systems, such as those that depend on pseudo-random multivariate quadratic equations [25] and rainbow-like digital signature schemes [26], should be taken into consideration for future development for resource-constrained applications. To meet the needs of memory-constrained devices, however, key-size optimizations and lightweight compression methods still need to be developed.

These 4 methods offer unique methods to keep the digital organization and respective digital resources safe in the Post Quantum Era. These all are continuously growing areas in terms of academics and research to solve the Post Quantum Situation. There can be a number of possibilities with which Quantum computing can be utilized for tearing down security in all aspects which are discussed in the forthcoming sections. To tackle those situations above description of approaches are initial approaches for survival in the coming future [27].

5. IDEA OF COMPROMISING SECURITY IN POST-QUANTUM ERA

The development of Quantum Algorithms is a very great leap of mankind toward a more developed future as they will be able to do what a present-day machine or human can't. But the increasing development in this direction is leading to a future where all security aspects will be at risk, this will be due to several reasons associated with Quantum Cryptography. The list can go towards a variety of applicability, a few of them are enlisted below

1. Quantum Fourier Transformation based Algorithms

All Present-Day Cryptographic Algorithms are based on large and complex mathematical calculations like prime numbers used for the RSA algorithm but it will be convenient to guess that exact number with the help of brute force due to the presence of Shor's Algorithm. Shor's Algorithm is a Quantum Algorithm to guess Large Numbers in seconds and is termed a Quantum Random Number Generator because of which a huge economy will be at Risk. Some other Fourier-based algorithms can also be used to detect the vulnerability and guess the encryption keys for risking the security on this digital web like Deutsch-Jozsa Algorithm for solving the black box problem, Bernstein-Vazirani Algorithm, Simon's Algorithm [28].

2. Amplitude Amplification-based Algorithms

With the evolution of the Information age, the concept of Big Data was introduced, to handle such a huge volume of data coming from various sources at very high velocity at a large server containing a wide variety of data. In this situation, data is being stored in an unstructured manner which is quite time-consuming when it comes to retrieving them from databases. Here, another Quantum Algorithm comes into role known as Grover's Algorithm which is used to search unstructured databases in a significantly lesser time. One more algorithm is can be used to solve the problem associated with generalization Searching in an unordered list known as Quantum Counting. Both of these algorithms are based on the categorization of Amplitude Amplification [29].

3. Hybrid Classical/Quantum-based Algorithm

There are some strategies that are available to use Classical and Quantum Computing together to solve complex problems. As was mentioned earlier that in some cases classical computing performs better than Quantum Computing. Hence, it will not be very ideal to use Quantum Computing in every possible method to break security implemented using cryptography. It is important to decide where to use what type of computation. Therefore, Hybrid Algorithms can be used to tackle situations to get optimized results required for solving complex mathematical problems. Some of the Hybrid Algorithms are Variational Quantum Eigensolver, Contracted Quantum Eigensolver, etc [30].

All these types of Quantum Algorithms possess enough potential to bring down security in post quantum era in several aspects. As for Instance, it is well aware that the whole security system of this prequantum Era is composed of factorization of huge Integer problems and Discrete Logarithmic problems and both of these can be cracked down using only Shor's Algorithm. Shor's Algorithm is itself powerful enough when implemented on Quantum Computers. As mentioned previously Shor's Algorithm is can be classified in Quantum Algorithms implemented using Quantum Fourier Transformation when any arbitrary function is given as input and the period of the function is can be obtained in Output.
Execution of Shor's Algorithms is illustrated below:

1. Take any random positive integers m and n where m<n, and calculate,greatest common divisor, gcd(m,n) using Euclidean Algorithm. If gcd(m,n) $\neq$ 1, the result is a prime factor, and if gcd(m,n) =1, then go to step 2.
2. Unknown period P is obtained of the sequence using Quantum Computing and expressed as x mod n, x2 mod n, x3 mod n, x4 mod n, and so on.
3. If P is odd go to step 1, but if P is even, go to step 4 where P is $(m^{P/2}-1)(m^{P/2}-1) = m^{P}-1 = 0$ mod n,
4. Evaluate $m^{P/2}+1$ and equate it to 0 mod n, if found equal go to step 1, and if $m^{P/2}+1 \neq 0$, then go to step 5,
5. Evaluate d = gcd $(m^{P/2}-1, n)$ using Euclidean Algorithm, as $m^{P/2}+1 \neq 0$ proven previously, d is the prime factor of n.

A number of researches are being done to implement Shor's Algorithm in an efficient manner so that it can give the desired output, but a satisfactory implementation is yet to be achieved to bring down the security systems of the present era as Nobody has achieved scalability with even more than just few quantum bits.[31].

When it comes to the Quantum Computing execution of Shor's Algorithm, the complexity is can be expressed as

$$(log\ logn)^{2+e}$$

where e is the exponent of RSA [32].

Apart from the above-discussed Algorithms, Machine Learning Algorithms are being developed at a very fast pace for attacking and detecting the vulnerabilities in a system to tear down the security of any digital infrastructure. With the evolution of Quantum Computers, these Machine Learning Algorithms will be executing and finding the vulnerabilities of the systems in a span of seconds. Quantum Computers and Quantum Algorithms have a wide spectrum of applicability which can result in either constructive or destructive depending on the usage of the technology [33].

6. CONCLUSION AND FUTURE EXTENSION

The concept of Quantum Algorithms is not new, as they are being developed and researched for more than the past three decades. The list of Quantum Algorithms is being increased with each passing year. The tendency of these algorithms possesses the capabilities to perform computations at a very elevated fast rate which can result in a major threat to all the systems protected with highly advanced Cryptographic Algorithms. As present-day Algorithms are based on very powerful mathematical computations which will require years of computation to get output will all be compromised in an instance of a few seconds with the emergence of Quantum Computers and associated Quantum algorithms. The whole world is in need of more dynamic and robust methods to secure the digital assets of all organizations in the post-Quantum Era. To develop such techniques, it is required to get a good insight into all the Quantum Algorithms which will be the possible menace in such situations apart from all the vulnerabilities present to develop Quantum-proof, Quantum-safe, or Quantum-resistant Cryptosystems. There will be a huge range of applicability and scope of advancements in the future of Quantum Computers to solve the problems which are yet to be solved and have more reliable techniques to protect information and assets available in digital environments, for which research is needed to be continued in this dimension.

REFERENCES

[1] Bobra, M. (2022). The Shrinking Transistor. *Physics*, *15*, s75.

[2] [Hota, L., & Dash, P. K. (2022). A Taxonomy of Quantum Computing Algorithms: Advancements and Anticipations. In *Technology Road Mapping for Quantum Computing and Engineering* (pp. 36-56). IGI Global.

[3] Kanamori, Y., &Yoo, S. M. (2020). Quantum computing: principles and applications. *Journal of International Technology and Information Management*, *29*(2), 43-71.

[4] Montanaro, A. (2016). Quantum algorithms: an overview. *npj Quantum Information*, *2*(1), 1-8.

[5] Farik, M., & Ali, S. (2016, December). The need for quantum-resistant cryptography in classical computers. In *2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)* (pp. 98-105). IEEE.

[6] Fossen-Helle, A. (2020). *Quantum Computing, how it is jeopardizing RSA, and Post-Quantum Cryptography* (Master's thesis, The University of Bergen).

[7] S. Gushanskiy and V. Potapov, "Investigation of Quantum Algorithms for Face Detection and Recognition Using a Quantum Neural Network," 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 2021, pp. 791-796, doi: 10.1109/ICIEAM51226.2021.9446325.

[8] K. Miyamoto, "Quantum algorithms for Monte Carlo integration using pseudo-random numbers," 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), 2021, pp. 454-455, doi: 10.1109/QCE52317.2021.00075.

[9] S. P and P. Kumari, "Quantum Algorithms for Machine Learning and Optimization," 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), 2020, pp. 1-2, doi: 10.1109/PhDEDITS51180.2020.9315301.

[10] N. Mahmud and E. El-Araby, "Dimension Reduction for Efficient Pattern Recognition in High Spatial Resolution Data Using Quantum Algorithms," 2019 32nd IEEE International System-on-Chip Conference (SOCC), 2019, pp. 126-131, doi: 10.1109/SOCC46988.2019.1570558150.

[11] R. D. Rosenwald, D. A. Meyer and H. A. Schmitt, "Applications of quantum algorithms to partially observable Markov decision processes," 2004 5th Asian Control Conference (IEEE Cat. No.04EX904), 2004, pp. 420-427 Vol.1.

[12] H. Buhrman et al., "Quantum algorithms for element distinctness," Proceedings 16th Annual IEEE Conference on Computational Complexity, 2001, pp. 131-137, doi: 10.1109/CCC.2001.933880.

[13] W. -L. Chang, "Fast Quantum Algorithms of Breaking the Data Encryption Standard," International Symposium on Parallel and Distributed Processing with Applications, 2010, pp. 520-527, doi: 10.1109/ISPA.2010.27.

[14] H. Abulkasim, B. Goncalves, A. Mashatan and S. Ghose, "Authenticated Secure Quantum-based Communication Scheme in Internet-of-Drones Deployment," in IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3204793.

[15] F. Ren, X. Yang and D. Zheng, "A QC-LDPC Code Based Digital Signature Algorithm," 2018 International Conference on Networking and Network Applications (NaNA), 2018, pp. 257-262, doi: 10.1109/NANA.2018.8648750.

[16] M. Roetteler and K. M. Svore, "Quantum Computing: Codebreaking and Beyond," in IEEE Security & Privacy, vol. 16, no. 5, pp. 22-36, September/October 2018, doi: 10.1109/MSP.2018.3761710.

[17] Rieffel, E., &Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys (CSUR)*, *32*(3), 300-335.

[18] Montanaro, A. (2016). Quantum algorithms: an overview. *npj Quantum Information*, *2*(1), 1-8.

[19] Markov, I. L., Fatima, A., Isakov, S. V., &Boixo, S. (2018). Quantum supremacy is both closer and farther than it appears. *arXiv preprint arXiv:1807.10749*.

[20] Smith, J., &Mosca, M. (2010). Algorithms for quantum computers. *arXiv preprint arXiv:1001.0767*.

[21] Lamport, L. (1979). Constructing digital signatures from a one way function.

[22] R. C. Merkle, "A certified digital signature," in Conference on the Theory and Application of Cryptology, 1989, pp. 218-238.

[23] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," Deep Space Network Progress Report1978.

[24] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, pp. 188-194, 2017

[25] N. T. Courtois, "On multivariate signature-only public key cryptosystems," IACR Cryptol. ePrint Arch., vol. 2001, p. 29, 2001.

[26] J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng, "New differentialalgebraic attacks and reparametrization of rainbow," in International Conference on Applied Cryptography and Network Security, 2008, pp. 242-257.

[27] Abuarqoub, A., Abuarqoub, S., Alzu'bi, A., & Muthanna, A. (2021, December). The Impact of Quantum Computing on Security in Emerging Technologies. In *The 5th International Conference on Future Networks & Distributed Systems* (pp. 171-176).

[28] Zhou, S. S., Loke, T., Izaac, J. A., & Wang, J. B. (2017). Quantum Fourier transform in computational basis. *Quantum Information Processing*, *16*(3), 1-19.

[29] Ambainis, A. (2010). Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations. *arXiv preprint arXiv:1010.4458*.

[30] Shukla, A., &Vedula, P. (2021). A hybrid classical-quantum algorithm for solution of nonlinear ordinary differential equations. *arXiv preprint arXiv:2112.00602*.

[31] T. Monz, D. Nigg, E.A. Martinez, M.F. Brandl, P. Schindler, R. Rines, S.X. Wang, I.L. Chuang, and R. Blatt. "Realization of a scalable Shor algorithm." Science, 2016, 351(6277), pp.1068-1070.

[32] P. W. Shor, ''Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,'' SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, Oct. 1997

[33] Gao, X., Zhang, Z., & Duan, L. (2017). An efficient quantum algorithm for generative machine learning. *arXiv preprint arXiv:1711.02038*

AUTHORS

Mr. Basil Hanafi is presently a Research Scholar at the Department of Computer Science, Aligarh Muslim University, Aligarh. He completed his Post Graduation in Computer Science and Application in 2018 from Aligarh Muslim University. The working domain expands to Neural Cryptography and Quantum Algorithms. He is an active sportsman who represented the University at various District and State level events in equestrian Sports. He also worked as Data Analyst at Major Research Project on the person with disability Act 1995: Study and Survey of Human Rights Judicial and State Protection for Differently abled people U.P. India before getting enrolled in Ph.D. Programme.

Prof. Mohammad Ubaidullah Bokhari is presently working as Professor in the Department of Computer Science, AMU, Aligarh, (INDIA) and Principal Investigator (PI) of the ambitious project, NMEICT ERP Mission Project (Govt. of India). He worked as Chairman Department of Computer Science for about 6 Years. He has also worked as an Associate Professor and Director of Studies in Australian Institute of Engineering & Technology, Victoria, Melbourne (Australia). Prof.Bokhari has a vast teaching experience of more than thirty-two years. He is having significant amount of Published Research work in various well reputed Journals.

Imran Khanis a Ph.D. candidate in the Department of Computer Science at Aligarh Muslim University, Aligarh. He was trained as a machine learning engineer at the same department through a master's program and as an interaction researcher through his involvement in various projects, such as cancer detection, Drowsiness detection system, financial fraud detection, and Graph neural networks. His research interests lie in the fields of synthetic identity detection in financial networks, and other kind of identity theft detection. His Ph.D. research aims to establish a theoretical model to detect the synthetic identities in financial networks using deep learning.