How do Quantum Algorithms influence Cyber Security in the NISQ era?

Arman Rudar

Received September 14, 2023
Accepted February 11, 2024
Electronic access February 29, 2024

Quantum algorithms have emerged to be a promising technology with the potential to revolutionize various fields such as optimization, financial modeling, and drug discovery by offering computational advantages that classical algorithms struggle to match. However, quantum algorithms also have key implications regarding cyber-security where some algorithms have the potential to compromise currently used encryption schemes, leading to the theft of data. As a result, quantum algorithms will pose a threat to cyber-security in the NISQ era if quantum resistant cryptographic schemes are not implemented fast enough. This paper provides a surface-level background on quantum computing and discusses the intersection of quantum algorithms with cybersecurity in today's era as well as the future.

Introduction

Quantum computers are potentially revolutionary devices that leverage the properties of quantum systems to outperform classical computers, which are the computers we use today. Modern computers use binary digits (bits). These bits are similar to a switch where there are two possible values, a 0 or 1, and can be connected and communicated with in long chains in order to perform arithmetics. Quantum computers develop this practice through utilizing superposition and entanglement. Superposition is a phenomenon that can occur when a qubit (Quantum bit) exists simultaneously in both a 0 and 1 state allowing for the exploration of multiple solutions at the same time. Specifically, the number of solutions considered at once could be up to 2^N where N is the number of bits [1]. Entanglement, in essence, is a phenomenon that interconnects qubits with each other, rendering the state of one qubit inseparable and dependent on the state of the other. Culminating these properties together allows quantum computers to work incredibly fast, so fast that modern-day encryption schemes such as the RSA can be broken with Shor's algorithm in a few hours as opposed to quadrillions of years by its classical counterpart [2]. This therefore highlights their potential in specialized applications and their influence over cyber-security which will be discussed throughout this paper.

What are Quantum Algorithms?

Quantum Algorithms are algorithms that solve problems using a quantum system/computer. They are designed to solve specific problems where their quantum properties help provide a substantial advantage over classical algorithms. When quantum algorithms are run on a quantum computer, speedups or efficiency improvements can be realized and help solve problems in much less time [3]. A great example of a speedup is in Shor's algorithm. The task is to factorize a number of thousands of bits long into its prime factors. For a classical computer, the task's exponential complexity renders it impossible to solve in a realistic time frame; however, a quantum computer using Shor's algorithm can solve it within three hours [4]. The factorization of large numbers becomes significant when used to decrypt modern encryption schemes such as RSA: leading to private emails and confidential information to be public. Grover's algorithm, which will be discussed further later, also achieves the same effect on AES-128 (another widely used modern encryption scheme.)

However, there are currently multiple obstacles preventing quantum algorithms from reaching their full potential, most notably qubit stability, error correction, and scalability [5,6]. Qubit stability refers to the high sensitivity experienced by qubits through interference with environmental factors such as temperature fluctuations and electromagnetic radiation. Sufficient interference with these external factors can cause the qubit to lose its information. As a result, shielding qubits from these external influences proves to be an ongoing challenge due to the highly sensitive nature of qubits. Furthermore, quantum computers are prone to errors due to the inherent fragility of quantum states. Quantum error correction is crucial for ensuring the fidelity of the computational process, however, implementing error correction techniques increases the number of qubits needed for a given computation which causes problems in scalability as the quantum system becomes more complex and demanding in terms of resources. These limitations aren't problems with the algorithms themselves but instead the hardware of the quantum computers used today. Despite these problems, further research on limitations will hopefully spur the creation of more practical

quantum algorithms.

Different Classes of Problems

The problem classes of P, NP, NP-complete, and NP-Hard (Figure 1) are crucial to understanding the complexity of certain computational problems. They allow us to gain a better insight into the capabilities, limitations, and efficiency of the algorithms used today to solve a specific type of problem. An example of this would be Shor's integer factorization algorithm: considered NP. All the problems in all the complexity classes utilize the two common resources of time and space where time refers to how long an algorithm takes to solve a problem and space refers to the total amount of memory required [7,8]. However, as the difficulty of the problem increases the time and space complexity also increases, demonstrating that different complexity classes require different amounts of resources. Solving these problems efficiently has the potential to be transformative in various fields including optimization and cryptography while also aiding to advance medicine and even finance [9]. So why haven't we solved them yet?

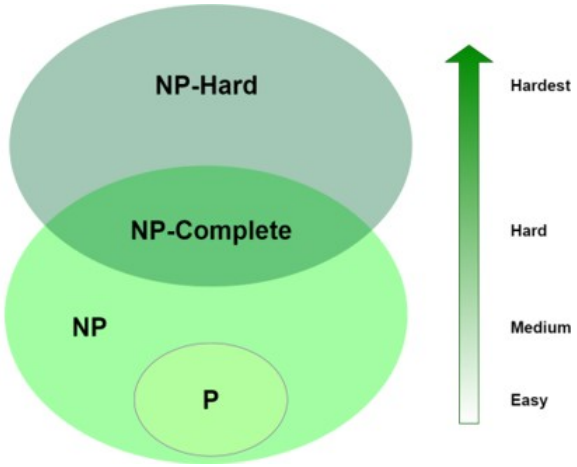

Fig. 1 Visualized relationship of P, NP, NP-Complete and NP-Hard Problems [10]

NP (nondeterministic polynomial) problems prove challenging to solve classically as they currently cannot be solved in polynomial time. By nature, NP problems have an exponential search space which creates an exponential number of possible solutions to explore. As a result, classical computers will have to undergo long searches to determine the optimal solution which will exponentially increase as the problem size/search space increases [8]. One way to solve exponentially growing problems is with exponentially growing systems, like quantum entangled systems as it can offer a potential speedup. Quantum computers/algorithms for example can harness their unique ability for quantum superposition to consider 2^N solutions at once: allowing for the ability to explore a larger solution space simultaneously, potentially leading to a faster solution. However, in today's era, problems with scaling, decoherence, and low gate fidelity prevent the usage of one [11]. Quite simply, quantum computers today aren't good enough. Without leveraging the properties of quantum systems, classical computers will find it difficult as their processing speed isn't advanced enough. Furthermore, there is a lack of known efficient algorithms to help classical computers overcome NP problems. Until new algorithms are discovered or our development of quantum computers improves to a certain degree, NP problems will remain unsolvable.

What is the NISQ era?

NISQ stands for Noisy Intermediate-Scale Quantum [12]. It refers to today's quantum computers being susceptible to noise with "Intermediate-Scale" relating to the size of quantum computers ranging from 10 to a few hundred qubits [12]. Limitations arise from the quantum computers being "Noisy" which indicates there isn't full control of each individual qubit due to the limitations in the system's hardware and control. This NISQ era is represented as a stepping stone for a more efficient era of quantum computers that are not limited by or prone to errors. To overcome this challenge, advancements in error-mitigation techniques, hardware, and algorithms must be made. These can be done by developing more sophisticated error mitigation techniques that can mitigate the impact of errors. Following this will be an era where fault-tolerant quantum computers will solve hard problems such as factorizing numbers thousands of bits long which would have to require the overcoming of the "intermediate scale" found in today's quantum computers. The idea of the innovation to develop and solve problems like these is what makes quantum computing a fast-growing field of research.

Quantum Algorithms Post NISQ

With today's faulty and inaccurate quantum computers, what development can we expect in the future? In the proceeding years, advancements in qubit quality, scalability, and error correction techniques will help quantum algorithms tackle complex problems with high efficiency and fidelity. Quantum algorithms would be expected to solve once infeasible problems exponentially faster than any other classical algorithm. Optimization in various fields would become simple: helping businesses save costs as well as improve efficiency [13]. Furthermore, quantum machine learning would be more practical and useful; providing computational advantages in many ways [14]. One step to transitioning past the NISQ era would be to improve the error rate. Physicists believe that for a practical large-scale quantum computer, an error rate of about one in a million is needed [15].

However, today's error correction technology can only achieve rates of about one in a thousand[15]. Until we develop fault-tolerant quantum computers, we will be stuck in the NISQ era for an unforeseeable amount of time, glimpsing at the potential of quantum algorithms.

Cybersecurity Post NISQ

Increasing reliance on digitalization has caused individuals and firms to become even more vulnerable to cyber-attacks[16]. Paired with the development of fault-tolerant quantum computers, will data be secure?

Most of the threat lies within the potential for quantum computers to break certain classical cryptographic schemes. Shor's and Grover's algorithms, discussed in the proceeding section, are examples of quantum algorithms that can be utilized by quantum computers to break such cryptographic schemes. When possible, information intercepted in the past by hackers, if recorded and stored properly, can be decrypted in the future by quantum computers[17]. Many refer to this as Store Now, Decrypt Later, or SNDL for short[17]. Hackers can exploit this for ransomware or espionage when quantum computers become available. Unfortunately, the only way to prevent SNDL is for firms or individuals to migrate to quantum-resistant encryption. However, currently, there are over 4.1 billion internet users so migrating to Quantum-resistant encryption will be a massive and global undertaking, and one that is complicated by the layered complexity and heterogeneity of the worldwide compute infrastructure we operate in[18]. Researchers estimate it may take a few years to implement quantum-resistant encryption, but, this all depends on the rate of quantum computing advancement[19].

Shor's Algorithm

Shor's algorithm for integer factorization was one of the first planned applications for quantum computers[4]. The goal of the factorization problem is to find an integer's two prime products, represented as $n = pq$. The most efficient classical algorithm known to date is the general number field sieve and runs in time $O(exp((logN)1/3(loglogN)2/3)))$ while Shor's quantum algorithm solves this in time $O((logN)3)$ with N being the length of the integer in bits[20]. The RSA asymmetric encryption is the most commonly used cryptographic system for secure data transfer and relies on the assumption that it is computationally infeasible to factor large numbers into their prime factors in a reasonable amount of time[21]. A comparison of time estimation to decrypt different-size RSA encryptions can be seen in Table I which reflects the advanced efficiency of quantum computers in this case. Evidently, Shor's algorithm demonstrates that the RSA cryptosystem is vulnerable to an attack with a fully scaled quantum computer, being able to crack the RSA-2048 within 3 hours.

RSA Key Size	Classical Computer	Quantum Computer
2048	6×10^{15} years	3.00 hours
3072	1.1×10^{25} years	3.53 hours
4096	7×10^{33} years	3.94 hours

Table 1 Classical Computer Vs. Quantum Computer - Time Estimation to Decrypt Different $Size^2$ RSA Encryptions

Through a combination of classical lattice reduction and a quantum approximate optimization algorithm (QAOA), researchers in China have been able to successfully factor a 48-bit integer with 10 superconducting qubits, marking it as the largest integer factored on a quantum device to date[11]. It has been theorized that only 372 physical qubits are necessary to challenge the RSA-2048 through this new technique, illustrating its potential superiority over Shor's algorithm which requires around 10,000 qubits to factor[?]. Apart from the new algorithm being potentially simpler to implement due to needing fewer qubits, it's also much more efficient than any previous factorization algorithm. As a result, the RSA encryption technique may become obsolete sooner than anticipated.

Grover's Algorithm

The Advanced Encryption Standard (AES) is another commonly used encryption technique to protect and secure sensitive data such as messages and passwords. The symmetric block cipher algorithm transforms information into gibberish and can only be converted back using a specific and personalized key. Through multiple rounds of encryption, decoding back to the original data becomes very challenging. Classical computers would have to try every single possible key one at a time until the right one is found. With AES-256 there are a total of 2^{256} potential secret keys and would take the fastest supercomputers billions of years to crack the encryption. However, by leveraging the properties of quantum systems, Grover's algorithm can potentially threaten AES encryption by providing a quadratic speedup[22]. The advantage is that Grover's algorithm can find the right encryption key in fewer iterations. For instance, if a classical computer were to try to crack the AES-128, it would require taking 2^{128} steps. Grover's algorithm however would require 2^{64} steps. While this improvement is significant, performing 2^{64} steps remains unachievable using our present quantum technology due to excessively long-time requirements. A preemptive measure to counter the use Grover's algorithm for when it inevitably becomes disposable, would be to double the number of bits the AES-256 uses to 512: creating the AES-512. This new encryption scheme contains 2^{256} times more keys which means that Grover's algorithm would need to complete 2^{128} times more steps than the AES-256. However, transitioning to AES-512

would be extremely expensive and require a long time to implement. For now, Grover's algorithm doesn't pose a direct threat, but eventually, more sophisticated quantum computers will eventually be built and most likely reduce the time to perform 2^{64} steps.

Challenges faced by quantum algorithms in the NISQ era

While there is great potential for quantum computing in the NISQ era, multiple limitations arise regarding the reliability of quantum algorithms[23]. As mentioned before, quantum systems are very sensitive and when they interact with their surroundings such as other atoms, temperature changes, or even stray electromagnetic fields, they start to lose their coherence[24]. As a result, their ability to maintain superposition and engagement starts to degrade which can be responsible for causing possible errors in the algorithm. Although it is impossible to entirely eliminate environmental interactions, there are ways to mitigate and reduce decoherence through error correction, quantum gate optimization, and shielding[25,26]. This paper won't discuss solving these problems but instead, provides a short and simple background for them.

Qubit quality refers to how well a qubit can maintain its quantum properties. The reliability of quantum computers is directly correlated with qubit quality; the higher the qubit quality the higher the reliability of the system. However, achieving good-quality qubits can prove to be difficult. As mentioned before, the interaction between qubits and the environment can cause decoherence, reducing the qubit quality, but also reducing the fidelity of quantum gates. It is important to maintain high gate fidelity as it assures that its intended operation has been carried out successfully. For example, if a gate were designed to flip a qubit's state from $|0>to|1>$, high fidelity (over 99%) would indicate that this transition occurred with minimal errors. Unfortunately, when a gate operates on a qubit, some of the energy used on the qubit could unintentionally disperse into neighboring qubits and change their state thus altering their qubit quality. This is referred to as crosstalk and can lead to disruptions in the quantum computer[27].

To mitigate crosstalk, more advanced physical isolation and shielding techniques can be employed to reduce unwanted interactions between qubits. For example, superconducting qubits are often placed within a cryogenic environment and shielded with materials that attenuate electromagnetic interference[28]. Further research into the types of materials used for shielding could lead to discoveries in diminishing electromagnetic interference thus reducing crosstalk. Alternatively, error correction could be advanced to correct the errors induced by crosstalk, gate fidelity and other sources of noise.

However, through the advancements of these challenges, cybersecurity could be left vulnerable as operating algorithms like Shor's and Grover's would be feasible. As a result, it would be imperative to implement quantum-resistant cryptographic schemes before these algorithms are fully functional.

Quantum Resistant Cryptographic Schemes

Although cryptography is secure now, in the future when quantum computers advance, encryption schemes such as RSA and AES will not provide security or protection for data anymore. As a result, quantum-resistant cryptographic schemes (QRCS) must be implemented to prevent potential mass data leaks. QRCS prove resilient to attacks from both classical and quantum computers which make them great for securing data. They do this by increasing the problem complexity to decode/decrypt translated data by utilizing mathematical problems that require computations that are not sped up greatly by quantum computers[19]. Additionally, QRCS have much larger key sizes compared to classical cryptographic schemes thus adding an additional layer of complexity which increases the difficulty of the problem. Even if a quantum computer could successfully crack a smaller key size such as AES-256, a much larger key size like AES-512 can be used in QRC and would still remain secure due to the exponential difficulty brought when key sizes increase. Some QRCS are also specifically constructed in a way to inhibit the strengths of some quantum algorithms but also exploit the limitations within them as well. For example, Shor's algorithm for factorization wouldn't prove useful to certain quantum resistant cryptophic schemes as they might not even involve the use of factorization to solve. Shor's very specific task proves itself as a limitation due to the fact it doesn't have versatility thus providing a lack of quantum advantage which ensures QRCS' security.

So why aren't all systems already using QRCS? First of all, establishing trust in new quantum resistant cryptographic schemes is a very slow and extensive process that requires a lot of time[19]. To establish trust in QRCS, meticulous peer review, testing, and extended research must be conducted to an extreme in order to ensure that new QRCS are robust and resistant to a wide range of potential attacks — both classical and quantum. Implementing QRCS will require transitioning from previous cryptography. However, this could serve to be difficult as transitioning involves updating hardware, software, and protocols which if avoided can cause a multitude of incompatibility errors. Furthermore, as QRCS will most likely require larger key sizes, they will also require more computational resources which can cause a decrease in performance for different applications such as sending messages[19]. Figuring out how to correctly balance security and performance is crucial and will take time to perfect.

Lattice-Based Cryptography

As the potential threat of quantum computers breaking current cryptographic schemes has been long known, the National Institute of Standards and Technology (NIST) launched a competition in 2016 for researchers to produce encryption algorithms that are secure from both classical and quantum attacks[29]. Cryptographers from all around the world submitted 82 different encryption schemes and in July of 2022, after years of relentless testing to determine the most secure, 4 proposals were selected to be part of NISTs post-quantum cryptographic standard with 3 of them based around the properties of lattices[30].

Lattices are geometrical structures formed by a regular arrangement of points in a multi-dimensional space. Lattice-based cryptography utilizes this in order to create secure encryption and key exchange[31]. A key benefit of using lattice-based cryptography over other QRCS is that lattice-based cryptographic schemes are known for their efficiency in terms of computational requirements and key sizes[32]. They typically have smaller key sizes in comparison to other QRCS which results in less overhead and lower resource consumption. As a result, improvements in performance, resource consumption, scalability and cost-effectiveness could be realized[32].

The encryption process works by the sender using a public lattice basis to create a lattice that encodes the plaintext message. To make it difficult for attackers to decrypt the cipher text, a layer of noise is added to the lattice representation of the plaintext. The noisy lattice is then encoded to create the ciphertext which is then sent to the receiver. The whole encryption process is done by a single key that is shared between the sender and recipient. Since the recipient has this private key, they can decode the ciphertext using the same key and recover the original plaintext. The inherent difficulty of solving certain lattice problems stems from the fact that the number of lattice points grows exponentially as the number of dimensions increases. Furthermore, it is believed that the mathematical problems associated with lattices are computationally intractable: not even the most powerful quantum computers can solve them. Proposed future encryption schemes will use around 1000 dimensions and will present resistance against both classical and quantum attacks. However, as mentioned before, the implementation of these quantum-resistant cryptographic schemes will require time and patience.

Conclusion & Outlook

Although quantum computers have the potential to revolutionize various fields, their effect on cybersecurity in the future can prove to be a double-edged sword. As fault-tolerant quantum computers will inevitably become available in the post-NISQ era, individuals exploiting SNDL can cause the leakage of vast amounts of data and unfortunately, there is no way to prevent it. Only the damage caused can be mitigated by implementing QRC schemes as fast as possible which could take years. Fortunately, in current times, due to the limitations of quantum computers regarding NISQ, and problems with qubit stability, error correction, and scalability, our current quantum computers don't pose an immediate threat to current cryptography. For now, classical cryptographic schemes remain strong, however, if QRC schemes aren't implemented before major advancements in quantum computing are made, Shor's and Grover's algorithms along with newly created techniques can prove to be detrimental.

References

1 A. Childs and W. Dam, https://arxiv.org/abs/0812.0380, Quantum algorithms for algebraic problems. arXiv.org.

2 S. Harshvardhan, N. Tran, C. McIrvin, J. McClure and S. Jain, *Simulating noisy quantum circuits for cryptographic algorithms*, https://arxiv.org/pdf/2306.02111.pdf.

3 F. Brandao and K. Svore, Quantum speed-ups for semidefinite programming. arXiv.org.

4 P. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, https://arxiv.org/abs/quant-ph/9508027, arXiv.org.

5 E. Knill, *Scalable quantum computation in the presence of large detected-error rates*, https://arxiv.org/abs/quant-ph/0312190, arXiv.org.

6 A. Steane, https://arxiv.org/abs/quant-ph/9708022, Quantum computing. arXiv.org.

7 W. H am al ainen, *Class NP-complete, and NP-Hard problems*, https://cs.joensuu.fi/pages/whamalai/daa/npsession.pdf.

8 H. Izadkhah, *SpringerLink*.

9 D. Herman, C. Googin, X. Liu, Y. Sun, A. Galda, I. Safro, M. Pistoia and Y. Alexeev, https://arxiv.org/abs/2307.11230, Quantum Computing for Finance. arXiv.org.

10 W. baeldung, *P, NP, NP-complete and NP-hard problems in computer science*, Baeldung on Computer Science.

11 A. Papageorgiou and J. Traub, *Measures of quantum computing speedup*, arXiv.org.

12 J. Preskill, *Quantum Computing in the NISQ era and beyond*, arXiv.org.

13 A. Ajagekar and F. You, *Quantum computing for Energy Systems Optimization: Challenges and opportunities*, arXiv.org.

14 J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe and S. Lloyd, Quantum Machine Learning. arXiv.org.

15 N. Author, *Breakthrough in quantum error correction could lead to large-scale quantum computers*, Physics World.

16 P. Lis and J. Mendel, *Economics and Business Review*, **5**, 24–47.

17 *Nature*.

18 D. Ott, C. Peikert and O. Participants, *Identifying research challenges in post quantum cryptography migration and cryptographic agility*, arXiv.org.

19 J. Mattsson, B. Smeets and E. Thormarker, https://arxiv.org/abs/2112.00399, Quantum-resistant cryptography. arXiv.org.

20 J. Buhler, H. Lenstra and C. Pomerance, *SpringerLink*.

21 R. Rivest, A. Shamir and L. Adleman, *Communications of the ACM*.

22 M. Grassl, B. Langenberg, M. Roetteler and R. Steinwandt, *SpringerLink*.

23 Y. Cao, J. Romero and A. Aspuru-Guzik, *Potential of quantum computing for Drug Discovery - IEEE Xplore*.

24 Y.-C. Liu, J. Shang and X. Zhang, *MDPI*.

25 S. Devitt, K. Nemoto and W. Munro, https://arxiv.org/abs/0905.2794, Quantum error correction for beginners. arXiv.org.

26 K. Heya, Y. Suzuki, Y. Nakamura and K. Fujii, *Variational Quantum Gate Optimization*, arXiv.org.

27 A. Ash-Saki, M. Alam and S. Ghosh, *Experimental characterization, modeling, and analysis of Crosstalk in a*, https://www.researchgate.net/publication/348671380_Experimental_Characterization_Modeling_and_Analysis_of_Crosstalk_in_a_Quantum_Computer.

28 C. Murray, *Material matters in superconducting qubits*, https://arxiv.org/abs/2106.05919, arXiv.org.

29 *NIST*.

30 *NIST*.

31 D. Micciancio and O. Regev, *Lattice-based cryptography*, https://link.springer.com/chapter/10.1007/978-3-540-88702-7_5, SpringerLink.

32 M. Sabani, I. Savvas, D. Poulakis, G. Garani and G. Makris, *Evaluation and comparison of lattice-based cryptosystems for a secure quantum computing era*, https://www.mdpi.com/2079-9292/12/12/2643, MDPI.

