The Future of Encryption in the Face of Advancing Quantum Computing Technology

Adhil Salim
Department of Computer Science and Engineering,
Amal Jyothi College of Engineering Kottayam

Advaith Manoj
Department of Computer Science and Engineering,
Amal Jyothi College of Engineering Kottayam

Alan Thomas Shaji
Department of Computer Science and Engineering,
Amal Jyothi College of Engineering Kottayam

Abstract—**Quantum computing is an emerging technology that significantly reduces calculation and processing time. Unlike classical computers that use binary bits with two states (0 or 1), quantum computers use qubits that can exist in two states simultaneously, known as superposition. Shor's algorithm takes advantage of quantum parallelism to easily break RSA encryption algorithms, which are widely used in modern online services and encryption. This presents a threat to personal information and data security. This paper discusses the threat of quantum computing to current encryption algorithms and proposes new algorithms to prevent it.**

I. INTRODUCTION

Quantum computing is a rapidly developing field that has the potential to revolutionize computing by enabling computers to solve complex mathematical problems that are currently considered impossible for classical computers [1]. Unlike classical computers, which use bits to represent information as either a 0 or 1, quantum computers use quantum bits, or qubits, which can exist in multiple states simultaneously. This allows quantum computers to perform certain types of calculations exponentially faster than classical computers [2].

However, the development of quantum computing also poses a significant threat to data security, particularly in the area of encryption. Many of the encryption methods that we currently use to protect sensitive information, such as RSA and AES, rely on the fact that factoring large numbers is a difficult problem for classical computers [3]. However, quantum computers are capable of performing this calculation much faster due to a quantum algorithm called Shor's algorithm [4]. This means that once quantum computers become powerful enough, they will be able to easily break many of the encryption methods that we currently use.

To address this threat, researchers are working on developing new encryption methods that are resistant to quantum attacks. These methods, known as post-quantum cryptography, use mathematical problems that are believed to be difficult for both classical and quantum computers to solve [5]. By doing so, they aim to provide a new generation of encryption methods that can withstand the power of quantum computers.

Overall, the potential impact of quantum computing on encryption is significant, and it is important for researchers and policymakers to be aware of the challenges and opportunities presented by this technology.

B. Thesis statement

Quantum computing is an emerging technology that poses a threat to current encryption algorithms used in online services and data security. Shor's algorithm can easily break RSA encryption algorithms by taking advantage of quantum parallelism. This paper proposes the need for new encryption algorithms to prevent the threat of quantum computing to personal information and data security.

II. OVERVIEW OF ENCRYPTION ALGORITHMS

Encryption is the process of converting conventional information or data into cipher text inorder to prevent it being accessed by an unauthorized party.The two different encryption methods that we currently use are symmetric encryption and asymmetric encryption.

Symmetric encryption uses a single key to both encrypt and decrypt data.This method requires the key to be secretly shared with the other party.Symmetric encryption is easier, faster and is suitable for large amount of data.however if the secret key is lost the encrypted data will be compromised.Most widely used symmetric encryption algorithms are AES-128, AES-192 and AES-256, AES stands for Advanced Encryption Standard and the size of the key in bits is denoted by the numbers.[6]

Asymmetric encryption uses two keys, one encrypts and the other decrypts.One of the keys is made public and the second one is kept private.Information is encrypted by the public key and is decrypted by the private key.It is slower, requires more resource but provides better security to the information transmitted.Commonly used asymmetric encryption are Rivest-Shamir-Adelman (RSA) algorithm,Digital Signature Standard (DSS) algorithm.[7],[8]

The Advanced Encryption Standard (AES) is a symmetric block cipher that can encrypt and decrypt electronic data with a high level of security. It is a variation of the DataSecDE standard adopted by the US Government in 2001 and developed by two cryptographers from Belgium, Joan Daemen and Vincent Rijman. For blocks of 128 bits, the AES program will use 256, 192 or 256 bit encryption codes. The total number of decryption and encryption sessions, which are 10, 12 or 14, shall be determined by the key. Four steps shall be taken in each round: byte substitution, row shift, column mix and key addition. These actions aim at converting the input information to output which is capable of dealing with various types of attacks. The AES is widely used for a variety of purposes, e.g. secure communication, data storage, electronically signed signatures and authentication.[9], [10]

Two different keys, a public key and a private key generated from two big prime numbers, are used in the Rivest &ShamirAdleman algorithm. You can share a public key with anyone, but the private key has to be kept secret. Encryption and decryption of encrypted messages, signing and validation of Digital Signatures may be carried out using the RSA algorithm. The difficulty of factoring large numbers is a complex mathematical problem that has not yet been solved successfully, and therefore the security of the RSA algorithm relies on it.

III. QUANTUM COMPUTING AND ITS IMPACT ON ENCRYPTION

Quantum computing is a revolutionary technology that uses quantum-mechanical phenomena to perform operations on data [11]. While it has the potential to solve problems that classical computers cannot, it also poses a threat to the security of current encryption methods. Encryption methods used by classical computers rely on the difficulty of factoring large numbers or computing discrete logarithms [12]. In contrast, quantum computers use quantum bits that can exist in multiple states at once, allowing for parallel processing and faster problem-solving. This makes many encryption methods that are currently considered secure susceptible to attack by quantum computers [13].

A. Comparison of classical computing vs. quantum computing in terms of encryption breaking capabilities

Current research is focused on developing new encryption methods that are resistant to quantum attacks. One approach is post-quantum cryptography, which uses mathematical problems believed to be difficult even for quantum computers to solve [14]. Another approach is to develop quantum-resistant versions of current encryption methods, such as lattice-based cryptography or code-based cryptography [15]. Additionally, researchers are exploring the use of quantum key distribution, which uses the principles of quantum mechanics to securely distribute encryption keys [16].

B. Current research on quantum computing and its impact on encryption

In conclusion, the field of quantum computing and its impact on encryption is an active area of research with significant implications for the future of cybersecurity. The development of new encryption methods that are resistant to quantum attacks is crucial to ensuring the security of sensitive information in the era of quantum computing.

IV. POSSIBILITY OF ENCRYPTION BREAKING BY 2030

Quantum computing has undergone rapid development in recent years. Owing to limitations on scalability, personal quantum computers still seem slightly unrealistic in the near future. The first practical quantum computer for ordinary users is likely to be on the cloud. However, the adoption of cloud computing is possible only if security is ensured.[17]

The concern among cybersecurity researchers and analysts is justified as a novel form of computing, utilizing quantum physics instead of traditional electronics, has the potential to compromise the majority of modern encryption techniques. Consequently, communication could become vulnerable and unsecured, similar to transmitting information without any encryption.

Fortunately, the threat so far is hypothetical. The quantum computers that exist today are not capable of breaking any commonly used encryption methods. Significant technical advances are required before they will be able to break the strong codes in widespread use around the internet, according to a 2018 report from the National Academies of Sciences, Engineering, and Medicine. [18]

But still there are several reasons to worry. Once the computing power becomes strong enough to break current encryption technologies, modern internet communications and e-commerce could someday succumb to a quantum attack, leading to a massive breach.

A. Explanation of current progress in quantum computing technology

Current implementations of quantum computers require large, expensive infrastructure for supercooling and electromagnetic shielding, and even then, we have been able to assemble only a handful of qubits in a single processor. However, the history of computing shows that although conventional computers began by requiring similar infrastructure, size soon shrank dramatically and the environmental requirements for today's machines allow for domestic operation. The pattern can already be seen with a company in Canada, D-Wave Systems Inc. [19]

Rieffel echoes one key potential area for quantum computing – the factoring of integers. As of the year 2000, the most efficient factoring algorithm was developed by Lenstra and Lenstra, but in 1994, Peter Shor created a quantum algorithm for factoring n-digit numbers. [20] Shor's algorithm, if implemented, could be very useful for breaking cryptographic codes. [21]

Another area of opportunity is the simulation of quantum systems. One such application would be the efficient solving of quantum problems of strongly interacting particles [18] Dyakonov skeptically remarks that after 15 years of imagining the potential of quantum computing, these are the only two application areas suitable for quantum information processing. [21]

In conclusion, the true potential for quantum computing is not yet known. Will it be limited to a small domain of problems as espoused by Dyakonov, or limited only by the imagination of computer scientists? An interesting observation comes from Nielson and Chung who remark that one of the biggest challenges is for computer scientists to design algorithms in a non-classical manner.[21]

B. Projections for the future of quantum computing and its potential for encryption breaking

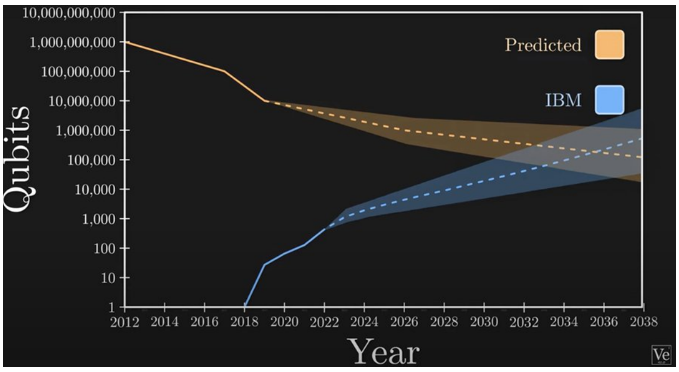
RSA is only one of the public key encryption schemes in use today. However, following his factoring algorithm, Shor quickly developed a quantum algorithm for solving the discrete logarithm problem. [22] Which showed that quantum computing poses a similar risk to other major encryption schemes.

Also, a recent study from National Institute of Standards and Technology (NIST) [23] shows quantum computing will mark the end of current encryption algorithms. It also shows that if the key lengths are sufficient, symmetric key encryption (specifically the Advanced Encryption Standard AES) is quantum resistant.

There are a range of alternative mathematical problems to those used in RSA and ECDSA that have already been implemented as public key cryptographic schemes, and for which the HSP does not apply. That is, they appear to be quantum resistant. These implementations include: [22]

1. Buchmann–Williams Key Establishment
2. The NTRU Cryptosystem
3. The Goldreich–Goldwasser–Halevi Cryptosystem
4. The Ajtai–Dwork Cryptosystem
5. The McEliece Cryptosystem

The below graph shows that, if the trends in quantum computing continues as it is now, by around 2036 our quantum computing power will be much enough to break all our currently existing encryptions algorithms.



source: veritasium, Veritasium - YouTube, "How Quantum Computers Break The Internet... Starting Now"

In 2012, it was estimated that it would take around a billion qubits to break the RSA algorithm, but five years later, that number dropped to 230 million. In 2019, it is estimated that it would only take 20 million qubits to break the encryption. Comparing that with the number of physical qubits available today, of course we are nowhere near that number of qubits. But considering this exponential progress and our prediction, by around 2036 quantum computers will be able to break all the currently existing encryption algorithms.

V. IMPLICATIONS OF ENCRYPTION BREAKING

Even though quantum computers are capable to break our current encryption algorithms, there are a number of barriers that prevent them to becoming fully developed in the status quo:

Accuracy: A quantum computers is a probabilistic machine, which means that in a single trial it might return the correct solution along with 10,000 other possibilities.28 Higher accuracy can be done with numerous trials of the same problem, but this diminishes the speed advantage of quantum computing[24]

Environmental Factors: Qubits can be altered by heat, noise, stray magnetic couplings. In order to minimize this, the qubits need to be totally isolated and in near-absolute zero temperatures. When doing so, there is still some extraneous noise, but another issue arises: when the qubits are totally isolated, it is difficult to control them without contaminating the environment and contributing additional noise and heat to the system.[24]

phase errors: In addition to the errors that plague regular bits like bit flip error, qubits are susceptible to other changes in data, like phase error, which can incorrectly flip the superposition sign of the phase relationship and cause errors in measurement. [24]

but still, it’s not the case that quantum computers are not successful. Google recently announced that its D-Wave quantum computer was functional and contained over 1,000 qubits. it is also possible that there could be an unexpected growth in the advancement in quantum computing.

Additionally, as part of risk analysis, it is important to discuss the potential enemies behind quantum-based attacks. Fortunately, while these attacks could cause inordinate damage, the cost of building and maintaining a quantum computer is cost prohibitive to web thieves and other black hat hackers.[24]

Therefore, the question arises: who could be behind these attacks? According to current research and development, governments and large organizations are the best possible guess. Thus, it is crucial to invest in research and development of post-quantum cryptography to ensure that sensitive information and data remain secure, even in the face of quantum-based attacks. As the threat of quantum computing becomes increasingly real, it is important for governments, organizations, and individuals to take action now to prepare for a future in which quantum-based attacks are a real possibility.

VI. POSSIBLE SOLUTIONS

As quantum computers become more and more powerful, they will be able to break many of the public key encryption algorithms that we use today. This could have a major impact on our existing communication and online services. We're currently working to develop encrypted systems that are safe for both quantum computers and classic computers, able to communicate with today's communication protocols and networks.

The branch of cryptography that uses a mathematical structure known as lattices for designing and analyzing cryptographic schemes is Lattice Based Cryptography. Lattices are lines in a multi dimensional space, which give rise to an ordinary gridlike pattern. Unlike more widely used and known public-key algorithm such as the RSA which could, theoretically, be defeated using Shor's algorithm on a quantum computer—some lattice-based constructions appear to be resistant to attack by both classical and quantum computers.It relies upon complex problems which are thought to be able to cope with Quantum Attack, and this makes it a promising candidate for Post Quantum encryption.Basis provide the information necessary to create a lattice.The two important lattice problems used to base security on are: Short Basis problem and Closest Vector problem.In Short Vector Problem we are given a long basis for a lattice and is asked to find a point on the lattice as close as possible to the origin. Closest Vector problem asks to find the lattice point closest to a target point.When it comes to cryptography lattices have much higher dimensions up to 1000 dimensions which becomes extremely hard for both quantum and classical computers to efficiently solve.[25]

Multivariate cryptography is a type of cryptographic system in which various polynomials may be used to construct Public Key Cryptography Systems. Multivariate encryption is based upon the hardness of solving mathematical systems consisting of multinomial equations.[25]

A type of post quantum cryptography based on the security of the hash function is called hash cryptography. Hash functions are mathematical operations that map any input to a fixed-length output, such that it is easy to compute the output given the input, but hard to find the input given the output. You could build digital signature schemes that are impenetrable to quantum attacks with the use of hashbase cryptography, e.g. Merkle's Signature System.[14]

Code based cryptography, which relies upon the hardness of decode error correcting codes, is a branch of Post quantum Cryptography. It was developed at the end of the 1970s and early 1980s by McEliece and Niederreiter, who provided a high level of security against quantum attacks. Code Based Cryptography uses public key encryption systems, which encrypt a message with random errors added to the codeword, decrypting it using secret codes for correcting those errors.[14]

VII. CONCLUSION

Quantum computing is an emerging technology that can perform computations at an unprecedented rate, offering exceptional benefits to society. However, it is crucial to examine the security implications of this technology. Quantum computing presents serious threats to commonly used encryption methods like RSA and AES. Rather than impeding innovation, we should shift to post-quantum cryptography and replace insecure encryption methods with those that are more robust and challenging to crack.

VIII. ACKNOWLEDGMENT

I would like to acknowledge the institutional support provided by the Department of Computer Science at Amal Jyothi College of Engineering. I am grateful to the anonymous reviewers and editors for their insightful comments and suggestions that helped to improve this manuscript. I would also like to acknowledge Derek Muller and his YouTube channel Veritasium for inspiring the topic of this study. Finally, I extend my thanks to the community of quantum computing researchers and scientists whose work inspired and informed this study.

References

[1] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.

[2] D. DiVincenzo, "The Physical Implementation of Quantum Computation," Fortschritte der Physik, vol. 48, no. 9-11, pp. 771-783, 2000.

[3] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[4] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[5] D. Jao and V. Soukharev, "Isogeny-based cryptography," in Advances in Cryptology – CRYPTO 2011, 2011, pp. 553–572.

[6] “Symmetric vs Asymmetric Encryption: What’s the difference?” https://blog.mailfence.com/symmetric-vs-asymmetric-encryption/ (accessed Apr. 10, 2023).

[7] “Asymmetric Encryption: Definition, Architecture, Usage | Okta.” https://www.okta.com/identity-101/asymmetric-encryption/ (accessed Apr. 10, 2023).

[8] “What is Asymmetric Cryptography? Definition from SearchSecurity.” https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography (accessed Apr. 10, 2023).

[9] “Advanced Encryption Standard (AES) - GeeksforGeeks.” https://www.geeksforgeeks.org/advanced-encryption-standard-aes/ (accessed Apr. 10, 2023).

[10] “Advanced Encryption Standard - Wikipedia.” https://en.wikipedia.org/wiki/Advanced_Encryption_Standard (accessed Apr. 10, 2023).

[11] Feynman, R. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7), 467-488.

[12] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on 1 Foundations of Computer Science (pp. 124-134). IEEE

[13] Ekert, A., & Jozsa, R. (1996). Quantum computation and Shor's factoring algorithm. Reviews of Modern Physics, 68(3), 733-753.

[14] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.

[15] Gentry, C., & Peikert, C. (2019). Lattice cryptography for the internet. Notices of the American Mathematical Society, 66(3), 337-351

[16] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[17] H. L. Huang et al., “Homomorphic encryption experiments on IBM’s cloud quantum computing platform,” Front Phys (Beijing), vol. 12, no. 1, pp. 1–6, Feb. 2017, doi: 10.1007/S11467-016-0643-9/METRICS.

[18] “Is Quantum Computing a Cybersecurity Threat? Although quantum computers currently don’t have enough processing power to break encryption keys, future versions might - Document - Gale Academic OneFile.”https://go.gale.com/ps/i.do?id=GALE%7CA580224313&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00030996&p=AONE&sw=w&userGroupName=anon%7Ec0fa77eb (accessed Apr. 09, 2023).

[19] J. Myers, “The Current State and Potential of Quantum Computing”.

[20] E. Rieffel and W. Polak, “An introduction to quantum computing for non-physicists,” ACM Computing Surveys, 32(3), Sep. 2000 [Online]. Available: doi: 10.1145/367701.367709

[21] M. Dyakonov, “State of the art and prospects for quantum computing,” 14 Dec. 2012 [Online]. Available: arXiv:1212.3562.

[22] W. Buchanan and A. Woodward, “Will quantum computers be the end of public key encryption?,” https://doi.org/10.1080/23742917.2016.1226650, vol. 1, no. 1, pp. 1–22, Jan. 2016, doi: 10.1080/23742917.2016.1226650.

[23] L. Chen et al., “NISTIR 8105 Report on Post-Quantum Cryptography”, doi: 10.6028/NIST.IR.8105.

[24] Z. Kirsch, “Quantum Computing: The Risk to Existing Encryption Methods Zach Kirsch Quantum Computing: The Risk to Existing Encryption Methods,” 2015.

[25] “Lattice-based cryptography - Wikipedia.” https://en.wikipedia.org/wiki/Lattice-based_cryptography (accessed Apr. 10, 2023).