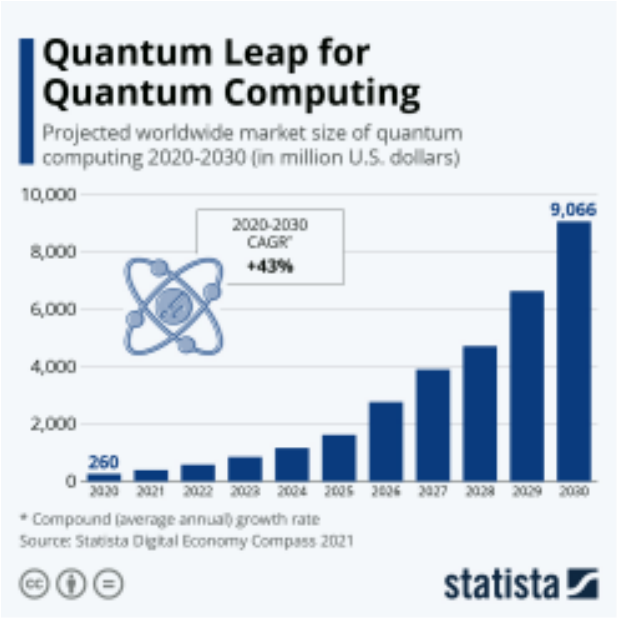
Authored by: Sriharini Vedula, Sai Ganesh Manda, Duru Ozmal, Krishna Meda, Rokia Ossama, Nahed Abdelgaber

Introduction

"*There are things that are so serious that you can only joke about them.*" *– Werner Heisenberg*

Until the past century, when many of the world's most renowned scientists (physicists) and philosophers had thought they knew nearly everything about the universe and had had a satisfying explanation of almost all natural phenomena and events like the motion of the planets, the secrets of electro-magnetism, and the spectrum of the Sun's light, one phenomenon was left unexplained: the behavior of the universe on the scale of the atoms and electrons, the bizarre nature and the subsequent implications of which the great minds of the time were neither able to comprehend nor debunk the fallacies that underlay.

This was like an engine that empowered all minds to stay curious, to be persistently inquisitive about the truth of the reality, and demystify the universe at every scale once and for all. So came the revolution of quantum mechanics - the science of probabilities and uncertainty. Quantum mechanics revolutionized the world of physics, later rippling its influences into the fields of its applications that followed, by its inherently mind-baffling truths such as partial existence (superposition), wave-particle duality (interference), and entanglement. These effects are seen today in quantum computing and light transmission technologies.



Like the industrial revolution changed the earth and affected everyone's life aspects, the quantum revolution is going to simply create what was thought of as a kind of magic years ago. Many scientists encourage while others discourage the fact that it's happening, it must be understood that this is going to take the industry by a storm. The key industrial insights in the quantum market claim that in terms of revenue, the global quantum computing market size was valued at around $457.9 million in 2021 and is projected to reach $5274.9 million by 2030 **as shown in figure 1.**

The market is predicted to grow at a significant rate due to the sheer potential of quantum computers in solving complex problems efficiently with promising exponential speed-ups over classical computations in terms of the logical overheads involved.

Classical Cryptography

The encryption methods of classical cryptography are based purely on the complexity of the mathematics involved; more specifically, the computational difficulty of factoring large numbers

is where the security of encryption in classical cryptography lies. Quantum cryptography on the other hand, is a more recently developed method of encryption such that two parties can establish for themselves a secure communication entirely reliant on the immutable laws of quantum mechanics, whose properties are utilized in order to transmit data through theoretically unhackable means. Both forms of cryptography have their own approaches and solutions to the key exchange problem (which says that, to build a secure communication channel where no one else may access a copy of the key(s)/data, it is necessary to share any keys or other information).

One of the arguably strongest classical cryptographic algorithms is RSA. It entirely revolves around logarithmic functions to stay computationally convoluted enough to resist brute force attacks and yet remain streamlined enough to be swift post-deployment. For the encryption and decryption of general data, RSA switches the order in which the key sets are used; to encrypt and decrypt the data, the recipient's public and private keys are used respectively, thereby eliminating any need for key exchange in scenarios where RSA is employed. The algorithm works as follows:

1. Key Generation: This first step of generating a pair of keys involves selecting two large prime numbers, p and q, and computing their product, $n = p \times q$. The totient of n, given by the Euler's totient function $\varphi(n)$, is computed as $\varphi(n) = (p-1)(q-1)$. The public key is the pair (e, n), e being a small, odd integer that is relatively prime to $\varphi(n)$. The private key is the pair (d, n), d being the multiplicative inverse of e modulo $\varphi(n)$.
2. Encryption: To encrypt a message m, the sender uses the recipient's public key (e, n) to compute the ciphertext $c = m^e \bmod n$.
3. Decryption: To decrypt a ciphertext c, the recipient uses their private key (d, n) to compute the plaintext $m = c^d \bmod n$, recovering the original message.

Besides RSA, there are also many other strong cryptographic techniques/protocols such as the Advanced Encryption Standard (AES), widely used in online banking, file encryption, and VPNs; Elliptic Curve Cryptography (EEC), a PKE algorithm that uses elliptic curves to generate keys, widely used in mobile devices and embedded systems; the Secure Hash Algorithm (SHA), a family of hash functions that are used for digital signatures and message authentication codes; and many more.

Quantum Cryptography

BB84 Protocol

Likewise in quantum cryptography, one of the strongest working QKD protocols today is BB84, as it's based on [the properties/phenomena of] quantum entanglement. When using polarization qubits in said protocol, Alice arranges an arbitrary series of four states. The Z basis is generally chosen, and as a result, the users of this protocol equate the binary digits 0 and 1 with the nonorthogonal states of |0|, |+|, and |1|, |-|. We have the nonorthogonality condition in place so that we can ensure that Eve (any eavesdropper) is unable to clone with perfect fidelity the chosen states (as stated by the no-cloning theorem). The implication here is that Eve thereby cannot

perfectly retrieve the information encoded by Alice, and Eve's action causes a disturbance on the quantum states that is detectable by the legitimate users.

Alice's prepared states are then sent to Bob, who measures them in his chosen basis, selected at random. Keep in mind that, should Bob select the same basis as Alice, then Bob can accurately decode Alice's input. On the other hand, should Bob select the wrong basis, his result, and thus the bit he reads, will be random. It's because of this possibility that, when the quantum communication is over, Bob exploits a classical public channel to tell Alice about which basis he used to measure each photon. Alice reports back her own basis, and they discard all the events correlating to the use of different bases. After this sifting operation, both parties should have two identical strings of bits, forming the so-called "sifted key."

E91 Protocol

Also called the Ekert Protocol, it is another QKD protocol, like BB84, that uses the properties of entangled particles to establish a shared secret key between two parties. It was introduced by the British-Polish professor of quantum physics at the Mathematical Institute, University of Oxford, Artur Ekert in 1991.

The advantages of having quantum protocols like the above are (but are not limited to):

1. Security: The so-called "factoring assumption" in the classical cryptography, which is based on the assumption that it is insanely difficult to factor large numbers, is broken by quantum computers (with the advent of quantum algorithms such as the Shor's Algorithm), which have the potential to solve such mathematically hard problems much faster than classical computers.
2. Ability to detect eavesdroppers: Any attempt to intercept a message will not go undetected, in contrast to the classical cryptography where an eavesdropper can intercept a message without being detected.

The disadvantages of quantum cryptography are (but are not limited to):

1. Complexity and Cost: Quantum cryptography requires specialized equipment, such as single-photon detectors and QKD systems, which are expensive and difficult to implement on a large scale.
2. Distance limitations: Quantum cryptography has distance limitations due to the nature of quantum entanglement, which means that it is currently limited to short-range communication; the distance between the two parties is also limited by the attenuation of the photons during transmission, which can affect the quality of the communication channel.

Despite the drawbacks, this is still a budding area of research with many ongoing efforts to develop more efficient and practical quantum encryption methods.

Post-Quantum Cryptography

Post quantum cryptography aims to build strong encryption methods that algorithms cannot break and which obstructs undetected eavesdropping. Theoretically, it's impossible to hack quantum cryptography but its practical uses are limited. Existing protocols might have to be modified to handle larger signatures or key sizes. Current challenges are mostly surrounded by transmission rates and application limitations. These are hard challenges to overcome as there is a need for transmittable quantum states in long distances, sustainable communication networks, and understanding the utilization of emerging technologies and public adaptation.

Up until now, many of the challenges in secure quantum information have been solved in regard to post quantum cryptography. Within its cost and complexity, quantum migration takes time. It's crucial to begin planning the next steps of this replacement for a safe actualization.

Post-quantum cryptography is, more specifically, a type of cryptography that is designed to be resistant to attacks by quantum computers. This is important because quantum computers have the potential to break many of the cryptographic algorithms that are currently in use by classical computers.

One of the main issues associated with quantum computing is that it can easily factor large numbers, which is the basis of many cryptographic algorithms. Post-quantum cryptography uses mathematical problems that are believed to be resistant to quantum computers, such as lattice-based cryptography and code-based cryptography.

Photonic quantum technologies have shown great promise through their high-speed transmission and low-noise specialized photons. Photon-based quantum technologies can be explained as providing secure communication by encoding a variety of the BB84 protocol discussed earlier. The use of single-photon sources is important in these protocols, as it enables the creation of a secure key and is caused by the unavailability of single photon sources since today's cryptography systems are relying on photons from laser pulses. Another alternative might be quantum cryptography based on entangled photon pairs with low power consumptions and small device footprints. Optical communications could have a visible effect on reducing power consumption.

There is no direct relation between quantum-proof encryption and distance limitation. Quantum-proof encryption (also known as post-quantum cryptography) is designed to be resistant to attacks by quantum computers, whereas distance limitation refers to the maximum distance over which a quantum communication channel can reliably transmit quantum information. However, it is worth noting that some post-quantum cryptography schemes may require a quantum communication channel to securely distribute the encryption keys, in which case, the distance limitation of the quantum communication channel may become a limiting facet.

Quantum-Proof or Quantum-Resistant VPNs

Quantum-proof VPNs are VPNs that encrypt data as they move over the network by making use of post-quantum cryptography (PQC). In the near future, quantum computers are predicted to be

able to crack the present public key encryption techniques. PQC is a paradigm that is meant to withstand attacks from these machines. Quantum-proof VPNs work to prevent hackers from decrypting today's encrypted data so that they can be stored until quantum computers are strong enough to break the encryption. PQC algorithms are based on supposedly challenging mathematical issues for quantum computers, as we know them today, to solve efficiently, albeit lacking enough practical evidence to support this argument.

For the time being, we can still use QKD to encrypt a VPN connection. This can be done by encrypting the VPN traffic first with a conventional encryption algorithm such as AES or RSA. The encryption key for this algorithm is then distributed using QKD to ensure its security. The QKD system will generate a random key, which is then transmitted over a quantum channel to the other end of the VPN connection. Once the key is received, the conventional encryption algorithm can be used to encrypt and decrypt the VPN traffic.

QKD can be used to provide an additional layer of security to a VPN connection, making it more resistant to attacks from quantum computers or other advanced cryptographic attacks. However, QKD is currently more expensive and less practical and scalable than conventional encryption methods, and is typically only used in high-security applications where the cost and complexity are justified by the need for maximum security.

Moreover, PQC algorithms are still being developed and tested, so they could contain defects or vulnerabilities that adversaries, whether quantum or classical, might take advantage of. As a result, quantum-proof VPNs only offer a greater degree of security than the present encryption techniques and are not immune to quantum assaults. Instead, they are quantum-resistant or quantum-safe.

Conclusion

Quantum cryptography offers new and exciting paradigms for secure communications that have the potential to revolutionize the way we think about data protection. Unlike classical cryptography, which relies solely on mathematics, quantum cryptography uses the principles of quantum mechanics to provide a level of security that is theoretically unbreakable. While there are still some challenges to work through, such as scalability and cost, recent advances in quantum technologies have brought us closer than ever to realizing the full potential of quantum cryptography.

A particularly promising application regarding cybersecurity is of course the use of quantum key distribution (QKD) to encrypt VPNs specifically. This technology offers a new level of security that’s resistant to attacks from even the most powerful adversaries, making it an

attractive option for organizations that require the highest level of security for their communications (such as with the military and government; they can use quantum cryptography to securely transmit sensitive info without worrying about interception from third parties; in the medical and healthcare field as well, quantum cryptography can be used to send patient records, healthcare data, and medical research in secure ways). With the ongoing development of quantum technologies, it's likely that we'll see even more powerful and efficient applications of quantum cryptography in various other fields in the near future.

Overall, quantum cryptography represents an exciting new frontier in the field of cybersecurity, and has the potential to transform the way we communicate and secure our information.

Citations

Basset, F. B., Valeri, M., Roccia, E., Murreda, V., Poderini, D., Neuwirth, J., Spagnolo, N., Rota, M. B., Carvacho, G., Sciarrino, F., & Trotta, R. (2021, March 19). *Quantum key distribution with entangled photons generated on ... - science*. science.org. Retrieved April 9, 2023, from https://www.science.org/doi/10.1126/sciadv.abe6379 Volume 7, Issue 12

Buchmann, J., Lindner, R., Rukert, M., & Schneider, M. (2009, May 26). *Post-quantum cryptography: Lattice Signatures - Springer*. Springer Link. Retrieved April 9, 2023, from https://link.springer.com/content/pdf/10.1007/s00607-009-0042-y.pdf

Clark, R., Bartlett, S., Bremner, M., Lam, P. K., & Ralph, T. (2021). POST-QUANTUM CRYPTOGRAPHY: A SECURITY PATCH FOR THE INTERNET. In The impact of quantum technologies on secure communications (pp. 25–26). Australian Strategic Policy Institute. http://www.jstor.org/stable/resrep31261.9

De Feo, L., Jhao, D., & Plut, J. (n.d.). *Towards quantum-resistant cryptosystems from supersingular ... - IACR*. eprint iacr. Retrieved April 9, 2023, from https://eprint.iacr.org/2011/506.pdf

Ekert, A. K. (1991, August 5). *Quantum cryptography based on Bell's theorem*. Physical Review Letters. Retrieved April 9, 2023, from https://doi.org/10.1103/PhysRevLett.67.661

GeeksforGeeks. (2022, June 22). *Differences between classical and quantum cryptography*. GeeksforGeeks. Retrieved April 9, 2023, from https://www.geeksforgeeks.org/differences-between-classical-and-quantum-cryptography

Gillis, A. S. (2022, January 28). *What is quantum cryptography?* Security. Retrieved April 9, 2023, from

https://www.techtarget.com/searchsecurity/definition/quantum-cryptography#:~:text=Quantum%20cryptography%20is%20a%20method,secret%20key%20can%20decrypt%20it.

Magnuson, S. (2019). THE RACE FOR QUANTUM RESISTANT CRYPTOGRAPHY. National Defense, 103(784), 25–25. https://www.jstor.org/stable/27022510

Nasedkin, B., Kiselev, F., Filipov, I., Tolochko, D., Ismagilov, A., Chistiakov, V., Gaidash, A., Tcypkin, A., Kozubov, A., & Egorov, V. (2022, November 30). *Quantum key distribution component loopholes in 1500-2100 nm range perspective for trojan-horse attacks*. arXiv.org. Retrieved April 10, 2023, from https://arxiv.org/abs/2211.16815

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020, December 14). Advances in quantum cryptography. Washington DC; Optical Society of America.

Simplilearn. (2023, February 13). *What is RSA algorithm in cryptography?: Simplilearn*. Simplilearn.com. Retrieved April 9, 2023, from https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm#:~:text=When%20using%20RSA%20for%20encryption,any%20keys%20in%20this%20scenario.

Stebila, D., & Mosca, M. (2017, July 28). *Post-Quantum Key Exchange for the internet and the open quantum ... - IACR*. Retrieved April 9, 2023, from https://eprint.iacr.org/2016/1017.pdf

Sutherland, A. (2017, February 8). *MIT Mathematics*. math.MIT.edu. Retrieved April 9, 2023, from https://math.mit.edu/classes/18.783/2017/Lecture1.pdf

Xu, F., Sajeed, S., Kaiser, S., & Wei, K. (n.d.). *Experimental quantum key distribution with source flaws*. APS Physics Journal. Retrieved April 9, 2023, from https://link.aps.org/accepted/10.1103/PhysRevA.92.032305

Zbinden, H., Bechmann-Pasquinucci, H., Gisin, N., & Ribordy, G. (1998). Quantum Cryptography. *Applied Physics B Lasers and Optics*, 1–6. https://doi.org/03.67.Dd; 85.60; 42.25; 33.55.A

Reflecting Questions

1. What course concepts does your project connect to and how?
    a. We discuss topics such as quantum cryptography, quantum protocols, and quantum algorithms/QKD. This is done prior to our discussion of these concepts in the context of VPNs as it provides insight into where quantum is headed in the future regarding applications in cybersecurity.

2. How does this project relate to your interests or career goals?
    a. Our interests all lie in fields such as cybersecurity, artificial intelligence/machine learning, and robotics. As such, quantum computing expands our interests as its new and different applications, methodologies, and sub-disciplines continue to emerge in all these fields, as a result, driving the job market in the industry and the future of our tiny world.
3. How does this project relate to the societal or ethical impact of quantum/AI in the future?
    a. Since this paper was about quantum cryptography, it relates to the ideas of code-making/breaking, hacking, data protection, and privacy. With quantum computers on the rise, the strongest encryption algorithms and protocols we have today will be essentially rendered useless, so we need to find new ways to protect ourselves and our data from malicious actors and also be mindful of our own capabilities of endangering the privacy of others. All in all, we have to do our best to not abuse the power that comes with greater technology that will become more widely available.
4. What did you most enjoy about this project?
    a. Doing deep dives into the actual algorithms/protocols and getting into the nitty-gritty details of how exactly they work. It is absolutely fascinating to look at the inner workings of these schemes and know that not only can one secure data with some fancy math (and now we can add quantum mechanics to that equation), but also know *how* exactly to secure that data.