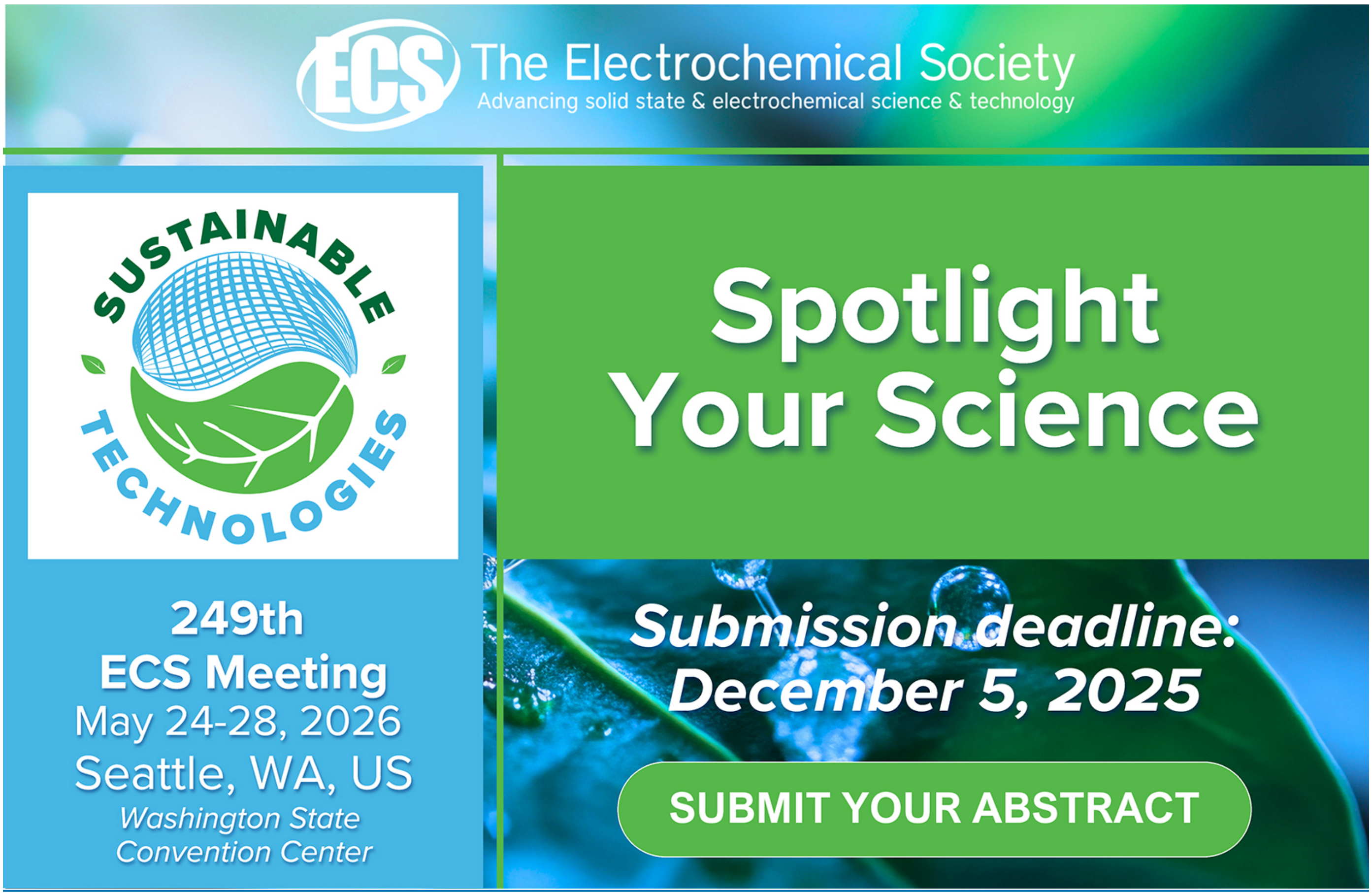
Journal of Physics:
Conference Series

PURPOSE-LED
PUBLISHING™

PAPER • **OPEN ACCESS**

Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods

To cite this article: Anshika Vaishnavi and Samaya Pillai 2021 *J. Phys.: Conf. Ser.* **1964** 042002



Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods

Anshika Vaishnavi and Samaya Pillai*
Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India
Email: *samaya.pillai@sidtm.edu.in

Abstract. Information security in communication networks is a persistent problem and essentially requires the usage of encryption methods. Quantum computing was first used to break encryption codes in the latter half of the 20th century with the introduction of the SHOR algorithm. Though the recent developments in QC capabilities have increased confidentiality, integrity, and availability of networks by protecting them against passive attacks like eavesdropping yet the transformation of classical to quantum computation can bear catastrophic implications as it has the potential to put the currently secure methods of transactions in jeopardy. This paper aims at the evaluation and comparison of traditional cryptographic techniques by the application of a SWOT framework. It takes up an exploratory study of the advanced quantum computing capabilities that can pose a massive risk to network security. The various security enhancements that can be adopted in data transmission to curtail these risks post-quantum are also discussed.

Keywords: Quantum computing, Cryptography, Encryption, AES, RSA, ECC, DH, Blowfish, Post-Quantum, Quantum-resistant, Quantum Key Distribution

1. Introduction

1.1 Need for Cybersecurity

Cybersecurity is the prevention of any damage to electronic communication systems and services and the protection of information involved along with maintaining integrity, availability, confidentiality, authentication and non-repudiation [1]. CISCO defines it as the practice of multiple layers of protection across systems and networks to prevent any attacks on sensitive information or business operations [2].

There has been a serious increase in the cyber threats owing to a surge in terms of the volume of data available, and therefore, a need of the hour is to secure personal, business and national information [3]. The major security challenges could be the complexity of network infrastructure, network threats like eavesdropping and wiretapping, increasing network capacity and infringement of the seven security parameters – authorization, availability, privacy, non-repudiation, integrity, and audit. As one can imagine, the impact of sensitive data being compromised can be massive, and businesses can suffer huge losses if details related to financial transactions, be it in e-commerce, bank transactions, credit card processing, or stock dealings [4].

No doubt, data security is a major concern in the world right now. For the secure transmission of data over an electronic medium, data should be encrypted. The science behind encryption is cryptology [5].

1.2 Cryptology

Cryptology is nothing but the phenomenon of deceiving a message. Initially, a sender transmits the message in an encoded form, known as cipher text so that it can only be understood by the proposed recipient. This prevents the misuse of this information if at all any unauthorized access was made. Decryption is just the opposite process, where the cipher text is decoded into the original text so that the message can now be read by the receiver. The aim of cryptology is not only to maintain data security but also to safeguard confidentiality, integrity also authentication of the information [6].

1.3 What is Quantum Computing?

As we leap forward with advancements in computing capabilities, we find ourselves moving closer to Quantum Computing. Its disruptive potential exceeds that of smartphones, the Internet and cloud computing combined. Quantum computers can perform complex calculations at a 100 million times faster speed than standard computers because it uses the 'superposition' property of a qubit which can not only identify dual states (e.g., 0 or 1, black or white, true or false) but can also compare and cope up with all the values in between these two states. This can change the paradigm of how mathematical operations are performed, thus making it possible to perform an infinite combination of calculations considering all options simultaneously [7].

1.4 Impact of Quantum Computing on modern-day cryptography

Some of the commonly used encryption algorithms are RSA, AES, ECC, Diffie-Hellman and Blowfish. Rivest, Shamir, Adleman (RSA) remains a worldwide standard and acts as a security backbone for well-known security infrastructure that is offered by companies like Microsoft, Nokia and Cisco [8]. The Advanced Encryption Standard (AES) is employed to provide client/server encryption for web traffic in a similar fashion [9]. In the field of IoT, Elliptic Curve Cryptography (ECC) is widely employed [10]. Blowfish is another method with a variable-length key which is replaceable with RSA, DES whereas the Diffie Hellman (DH) is an algorithm for sharing secret key among users [11].

So, currently, we rely on cryptographic keys, which are based on complex mathematical operations. Longer the key, more complex the mathematical computation, which makes it harder to crack the key and hence, making the network more secure. [42] These mathematical operations used by traditional cryptographic methods cannot be broken by classical computers. But this would not be the case in the future. Quantum computing processes data in quantum bits rather than two definite stages, changing how data can be encoded. It can exist in multiple stages at a particular time which makes operation upon all qubits simultaneously possible, the characteristic being known as quantum parallelism. Therefore, as the number of qubits increases, so does the computational speed of quantum computers, which can be illustrated as an n-qubit quantum computer being able to compute 2n values simultaneously [12].

1.5 Objective of the Study

Owing to the recent advancements in quantum computing, the conventional methods of cryptography will soon become unreliable. This paper aims at the evaluation and comparison of traditional cryptographic techniques by the application of a SWOT framework and takes up an exploratory study of the advanced quantum cryptography methods that would be employed in the future for network security.

2. Literature Review

2.1 Quantum Computing

M. A. Nielsen has stated that Richard Feynman was the first to reveal his idea of a quantum computer in 1982,acomputerthatworks on the properties of quantum mechanics[13].Aram Harrow pointed out another successive research by David Deutsch in 1985 wherein he proved that a quantum computer is faster than computing ordinary operations as well [14]. Lov Grover proposed a search algorithm that executes at a quadratically faster speed in quantum computers than a classical computer [15].Charles H. Bennett writes about how he and Gilles Brassard developed a quantum message exchange mechanism protocol for coin tossing in 1984. This mechanism is secure as it helps in the transmission of random key information between two unknown users [16].

However, the first physical breakthrough in this field was achieved in 1998 when Isaac Chuang, Almaden Research Center, IBM (San Jose, California, USA), and Neil Gershenfeld, Massachusetts Institute of Technology (Cambridge, Massachusetts, USA) developed a two-qubit quantum computer as highlighted by IBM news release [17]. Carey further explained with his research that this computer was given the task of finding the correct answer for a question with four possible options. As per the conventional norms, any classical computer would analyze each option sequentially/consecutively and then derives the correct solution in 2.25 tries. However, the quantum computer was able to do this in a single step by contemplating all the four options simultaneously [18].

2.2 Related Work

Peter Shor was successfully able to deduce an algorithm that could factor prime numbers at polynomial speed rather than what was earlier possible at exponential speed in classical computers [19]. Gottesman showed that the conventional public-key cryptography techniques are based on the principle of factoring, that is breaking down large numbers into prime numbers, but breaking this encryption was beyond today's computational power until now [20].This resonated with the theory already highlighted by Shannon that complete secrecy cannot be achieved by the current method of cryptosystem when faced with unlimited computing power [21]. Diffie W. also revealed in his work that it would not be right to ignore the fact that any public-key distribution scheme can be broken if advancements in computing are achieved [22].

Bhavesh Prajapati suggested that Shor's algorithm challenges the cryptographic methods dependant on factorization, and a need for quantum cryptography is felt. As an example, a 2048-bit RSA key takes billions of years to break using a classical computer, but a mature quantum computer algorithm can do it in seconds [23]. M. Dusekstated that the whole basis of why PKC is used as an encryption method lies in the difficulty in factorizing large prime numbers and logarithmic problems as they can be solved easily while encoding, but the decoding is extremely hard. Because of that, they are also known as one-way functions [24].

As stated in the literature review, significant work has been done around mathematical components of quantum computing or the risks associated with it. Lesser research was done on how it will affect modern-day cryptography and risks possessed by industries adopting traditional encryption algorithms or the countermeasures employed to prevent quantum risks. This paper aims to provide both the risks associated and measures that can be taken to prevent vulnerabilities caused by QC.

3. Research Methodology

The paper studies the various peer-reviewed literature in the fields of quantum computing, cryptography to reveal the effect of quantum computing on traditional cryptography and also introduces post-quantum cryptography. The online databases of Science Direct, IEEE, Emerald, Ebsco, etc., were employed for the research of related papers. The purpose of using qualitative research was to gain deeper insights into the study's topic. Relevant articles, blogs and whitepapers have also been referred, giving insights into the transformation that will be caused in the cybersecurity space due to quantum computing.

Ultimately, a SWOT framework was designed for five commonly used crypto algorithms from secondary research. This can provide an insight into the strengths and weaknesses of each algorithm with respect to quantum computing capabilities.

4. Vulnerabilities in Cryptography Methods Post-Quantum

4.1 RSA

Public Key algorithms are most widely used for encryption purposes. Algorithms like RSA, Elliptical Curve can initiate with just a public key and then computing the private key using mathematical models without having to consider all the possible scenarios. The private key can be computed by factoring in a number that is the product of two prime numbers. For example, a private key can be obtained by multiplying prime numbers like 7x3=21. The key length is what decides the security of any algorithm. RSA, for example, uses 2,048 bits which corresponds to 617 decimal digits which is unbreakable by current computing capabilities, but quantum computers can crack up to key pairs as long as the length of 4096-bit keys in just a few hours using Shor’s algorithm. Figure 1 represents SWOT analysis of Rivest, Shamir, Adleman (RSA). This can be termed as Return of Copper Smith Attack (ROCA) [25].

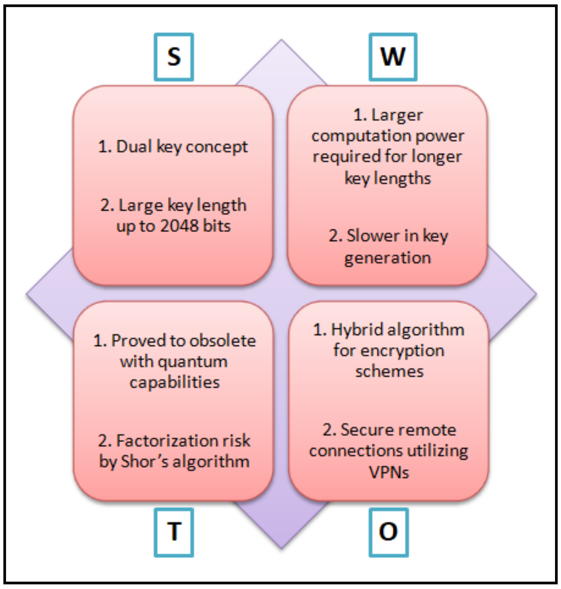

S
W
1. Dual key concept
2. Large key length up to 2048 bits
1. Larger computation power required for longer key lengths
2. Slower in key generation
1. Proved to obsolete with quantum capabilities
2. Factorization risk by Shor’s algorithm
1. Hybrid algorithm for encryption schemes
2. Secure remote connections utilizing VPNs
T
O

Figure 1: SWOT Analysis of Rivest, Shamir, Adleman (RSA)

4.2 ECC

Elliptical curve cryptography is employed to provide security in novel areas like IoT, blockchain. If we assume asymmetric key of 80 bitssize, then RSA needs 1024 bits while ECC requires only 60 bits. Thus, elliptical curve keys are lighter for longer keys. Shor’s and Grover’s Algorithm are essentially a threat to ECC. Shor’s algorithm will make factoring easy, which will eventually make the discovery of a private key almost certain by an intruder. Grover’s algorithm makes brute-forcing easier by creating uniform superposition over all the possible inputs, destructively interfering states that are invalid, and consequently, finding inputs satisfying the given function. Figure 2 represents SWOT analysis of Elliptical Curve Cryptography. The ECC's shorter key lengths will prove a major shortcoming in quantum computing. It will then become easier to crack this than the RSA [26].

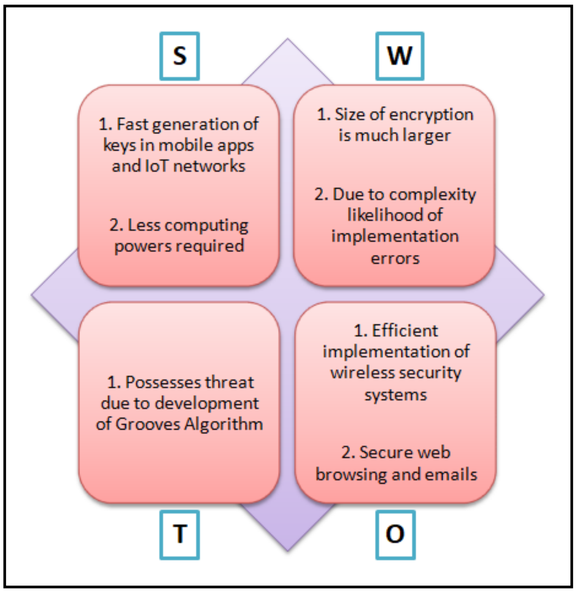

S
W
1. Fast generation of keys in mobile apps and IoT networks
2. Less computing powers required
1. Size of encryption is much larger
2. Due to complexity likelihood of implementation errors
1. Possesses threat due to development of Grooves Algorithm
1. Efficient implementation of wireless security systems
2. Secure web browsing and emails
T
O

Figure 2: SWOT Analysis of Elliptical Curve Cryptography (ECC)

4.3 AES

Advanced Encryption Standard was developed in 2001, it is a block cipher that works on symmetric-key cryptography providing confidentiality and integrity to the data. The key size generally used in AES is 128 bit or 16 bytes. The operation was carried out for 10 rounds. For a conventional computer, AES is a bit difficult to break as it requires 5x10^{21} years. But due to post-quantum era computing, this can be broken using Grover's Algorithm. Figure 3 represents SWOT Analysis of Advanced Encryption Standard (AES). But AES can be proved effective if the current key size is doubled and rounds of encryption are increased [27].

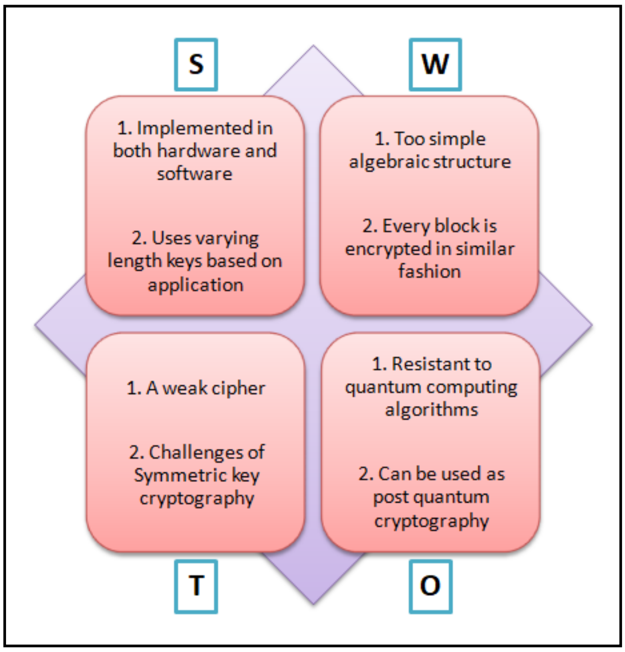

S
W
1. Implemented in both hardware and software
2. Uses varying length keys based on application
1. Too simple algebraic structure
2. Every block is encrypted in similar fashion
1. A weak cipher
2. Challenges of Symmetric key cryptography
1. Resistant to quantum computing algorithms
2. Can be used as post quantum cryptography
T
O

Figure 3: SWOT Analysis of Advanced Encryption Standard (AES)

4.4 Blowfish

Another symmetric cryptographic block cipher created by Bruce Schneier in 1993, Blowfish ranges from 32 to 448 bits. It is believed to have a better performance than commonly used encryption methods like AES, DES, RSA and has a lesser time and power consumption. It can create longer keys and each key, in turn, generates subkeys. Also, each subkey generated is somewhat different from the other. This way a much longer key is made which increases the complexity and prevents any attack. In fact, there is no proof of the Blowfish algorithm being hacked up till now. Even with quantum computing technology, the Blowfish algorithm will only be broken by a factor of one or two supposedly. So, even in the QC era, we can simply rely on this by using a longer key, such as switching to a 256 bit key in quantum when compared to 128 bit in classical [28] [29]. Figure 4 represents SWOT Analysis of Blowfish.

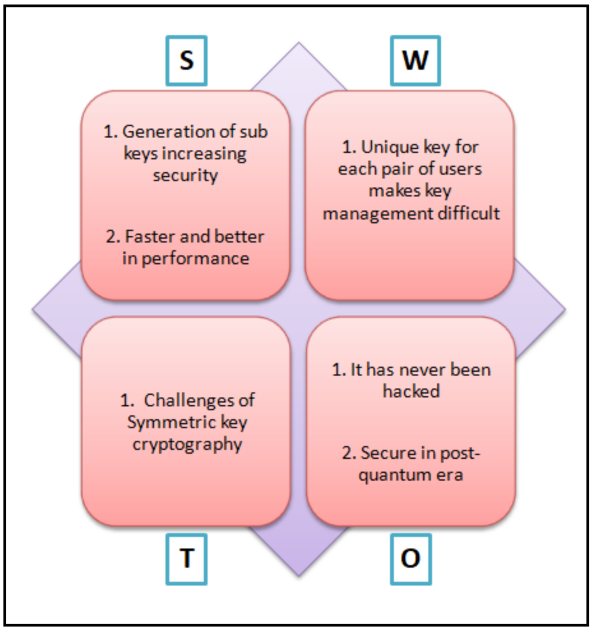

S
W
1. Generation of sub keys increasing security
2. Faster and better in performance
1. Unique key for each pair of users makes key management difficult
1. Challenges of Symmetric key cryptography
1. It has never been hacked
2. Secure in post-quantum era
T
O

Figure 4: SWOT Analysis of Blowfish

4.5 Diffie-Hellman

Developed in 1976 by Whitefield Diffie and Martin Hellman, the objective of Diffie-Hellman key exchange was to cater to the key agreement and exchange limitation not possible in other encryption methods. In this algorithm, two users decide upon a key pair and once that is done, share the public key to communicate with each other over an insecure channel. The sender or receiver need not have any knowledge about the person on the other side of the network link. The only drawback is that since there is no way of authenticating the users, the system becomes susceptible to eavesdropping, mostly man-in-middle attacks, inside, outsider attacks. Apart from this, Shor’s algorithm can render this method useless by cracking its factorization in no time [30]. Figure 5 represents SWOT analysis of Diffie-Hellman (DH).

4.6 Comparison of modern-day cryptography methods

It is clear that public key cryptography is endangered by quantum computing as deduced from Table 1. This leaves us with only a few encryption methods to fall back on, like AES, 3DES and Blowfish. These methods are symmetric, which brings us to address the same major limitation which was felt in the symmetric cryptography methods which had eventually led to the development of asymmetric cryptography or Public Key Cryptography (PKC). This shortcoming was that the key to be used in transmission had to be shared between users through a communication channel that could be intercepted [31].

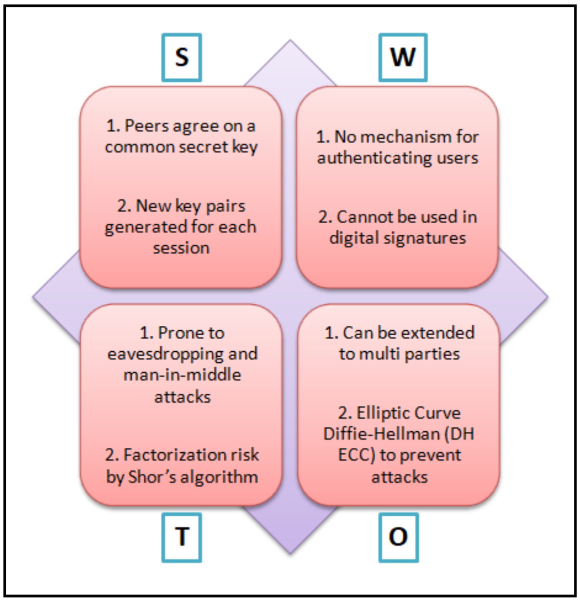

S
1. Peers agree on a common secret key
2. New key pairs generated for each session
W
1. No mechanism for authenticating users
2. Cannot be used in digital signatures
T
1. Prone to eavesdropping and man-in-middle attacks
2. Factorization risk by Shor's algorithm
O
1. Can be extended to multi parties
2. Elliptic Curve Diffie-Hellman (DH ECC) to prevent attacks

Figure 5: SWOT Analysis of Diffie-Hellman (DH)

Table 1: Comparison of modern-day cryptography methods

Cryptography	Founded	No. of bits	Type	Post-quantum impact
RSA	1997	1024-4096	Public key	Breakable
ECC	1985	Variable	Public key	Breakable
AES	2001	128, 192, 256	Symmetric	Secure (with longer key length)
Blowfish	1993	32-448	Symmetric	Secure (with longer key length)
Diffie-Hellman	1976	Variable	Public key	Breakable

5. Future Scope

5.1 Advancements in Quantum Computing

Currently, experiments are being conducted in quantum Fourier transforms, which can increase the performance of current QC algorithms exponentially when coupled with today's powerful supercomputers. In response, a shift in post-quantum cryptography is occurring. Two novel areas are emerging in cryptography, namely quantum-resistant algorithms and quantum key distribution [32]. Further study is done to achieve perfect secrecy by using laws of quantum mechanics to distribute private-based sharing keys based on a one-time-pad (OTP) [33]. Thus, an IT infrastructure that supports QC configurations will soon be an hour of need.

Quantum computers might be as soon as five years from now or even take twenty more years but it will not be long when the most popular cryptographic methods used today especially RSA, ECC, DH, will be broken. Possessing the ability to quickly factor prime numbers, all communication systems dependent on public key encryption (using asymmetric keys) will be cracked, and huge amounts of sensitive data will be compromised [34].

5.2 Challenges

There is no complete picture as to when quantum computers will become a reality.

There is no certainty if we will even be able to build quantum computers as it is important to isolate them from the external environment as any interaction with atoms outside the system inducing errors in the calculation which leads to impaired measurements. Commonly known as de-coherence, this is where the quantum states are meddled with and it is impossible to calculate further [35]. Quantum cryptography possesses a major limitation as it fails to offer a digital signature and related features, like certified mail or settling a dispute before the judge [22].

5.3 Post-Quantum Cryptography

So, if traditional PKI fails to keep up with quantum computers then what the future is?

Quantum Cryptography paved the way to a quantum channel that could be the future of communication where passive eavesdropping has a limited probability. Any even if any tampering is done, it can be detected. This makes hacking or copying quantum almost impossible. They would be completely unbreakable [36].

The fact that conventional cryptography has never been completely safe implies that digital communications can be taped, copied even when the intruder has no intention of doing so but can later use it for decrypting future communications with the same secret key. But when this elementary method gets replaced by a quantum system which is based on the principle of polarized photons gives rise to uncertainty. This prevents data theft because an eavesdropper cannot manage to intercept the channel without altering it in one way or another. This intrusion can be easily detected by the legitimate users of that channel [37].

5.3.1 Quantum Key Distribution (QKD): Based on the concept of quantum physics, forms the basis of this. It solves a very serious problem in modern cryptography methods that is the key distribution. It helps in securely exchanging a random key between users over an unprotected channel which ultimately helps in securing the data [38]. The basic working principle is that the sender will randomly generate a sequence of ones and zeroes. When this string is transmitted, each value is encoded by a photon in one of the polarization states – horizontal and vertical or two diagonals, the relationship established by the sender itself. The receiver will also configure its receiver for photons. The probability of both configurations matching is half. So, if it matches, the receiver receives the exact message sent by the sender. If it doesn’t match, the receiver cannot determine the sequence and cannot even attempt to re-determine the polarization because any such attempt would lead to its destruction. Both the users discuss over any public communication link to check which times the receiver was set, but the polarization state that the photons were set to, is not disclosed. The values which match at both ends are the shared secret key. Eaves dropping, the polarization of transmitted photons changes, and users can detect this as their secret keys will no longer match. This brings us to the uncertainty principle, which states that if something is measured, the result will be influenced [39] [40].

5.3.2 Quantum-Resistant Cryptography: There are mathematical algorithms already in existence that can replace public key cryptography like RSA, DH, and ECC.

These are resistant to classical computing but are also quantum-safe as an exponential speedup of search algorithms is believed to be impossible even by using Grover’s algorithm [41].

Four such methods have been proposed for post-quantum encryption: [41]

- Lattice-based cryptography
- Code-based cryptography
- Hash-based signatures
- Multivariate-based cryptography

6. Managerial Implications

This study exhibits how the advancements in quantum computing will affect the existing modern-day cryptography. The paper can act as a guide to the security professionals on how the traditional cryptology framework will prove unproductive when exposed to quantum computing. The primarily used algorithms like RSA, DES, AES, and Blowfish have been analyzed in detail, and a SWOT framework is charted in reference to the impact of quantum computing on each of these. The opportunities and challenges post-quantum are also discussed. A comparison between all the algorithms is drawn, and a consolidated list is provided, which can be used as a quick reference check for evaluating the security state of each of these cryptographic algorithms. Finally, the methods of post-quantum cryptography are described that can effectively replace the conventional methods in future and are also considered safe with respect to the current quantum capabilities.

7. Conclusion

It has become utterly common for some or the other data hack case coming to light every day. Even the large organizations with optimum infrastructure in place are not spared. This brings us to a stark realization that the complete safety of our data is still a myth. The data breach maybe due to an insider attack, third-party vendor, or system incapability. The causes are many and the methods numerous, but the problem remains the same – data loss.

With Quantum Computing becoming a reality, the traditional methods of cryptography will take a major hit. This brings us to the concept of Quantum Cryptography as there is a need for a cryptographic ecosystem that is resistant to not only our classical present but also to our quantum future!

Only time will tell if quantum is something that will be achieved soon or will it only remain a concept for many years to come. If quantum computers become a reality with our computing systems undergoing massive changes, will we be prepared for efficient data protection methods or will it be another major disruption like the Y2K, only this time it will have the entire population's information at stake!

References

[1] NIST Glossary, "Cybersecurity," Nist.gov

[2] https://csrc.nist.gov/glossary/term/cybersecurity(Accessed Jul. 10, 2020)

[3] CISCO, "What is Cybersecurity?," Cisco.com

[4] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html (Accessed Jul. 10, 2020)

[5] R. Kumar Goutam, "Importance of cybersecurity,"*International Journal of Computer Applications,* vol. 111, no. 7, pp. 14-17, Feb. 2015.

[6] B. Kapoor, P. Pandya and J. S Sheriff, "Cryptograhy – A security pillar of privacy, integrity and authenticity of data communication," *Kybernetes*, vol. 40, no. 9/10, pp. 1422-1439, Oct. 2011.

[7] O.G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *International Journal of Scientific and Research Publications (IJSRP),* vol. 8, no. 7, pp. 495-516, Jul. 2018.

[8] C. P.Pfleeger, S. L. Pfleeger and J. Margulies, "Details of Cryptography", *Security in Computing*, 4th ed. New York, USA: Pearson, 2015, pp. 786-788. [Online]. Available: https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/security-in-computing-5-e.pdf

[9] S. Vernacchia, "Advancing a strategy for quantum computing that will inspire, support and safeguard economic growth in the Middle East,"*Quantum Leap*

[10] https://www.pwc.com/m1/en/world-government-summit/documents/wgs-quantum-leap.pdf (Accessed Jun. 05, 2020)

[11] E. Tittel, J. Michael Stewart and M. Chapple, "Asymmetric Cryptography,"*Certified Information Systems Security Professional Study Guide*, 2nd ed. USA: Sybex, 2004, pp. 289. [Online]. Available: https://manpreetstorage.files.wordpress.com/2016/07/official-isc2-guide-to-the-cissp-cbk-fourth-edition-2015.pdf

[12] M. Hassankashi, “Security on the Web by Advanced Encryption Standard (AES) and Security Assertion Markup Language (SAML),” Codeproject.com

[13] https://www.codeproject.com/Articles/1023379/Security-on-the-Web-by-Advanced-Encryption-Standar

[14] P. Grubbs, “Why ECC is the Solution for IoT Security,” Securew2.com

[15] https://www.securew2.com/blog/ecc-solution-iot-security/ (Accessed Jun. 05, 2020)

[16] A. Majot and R. Yampolskiy, “Global Catastrophic Risk and Security Implications of Quantum Computers,” *Futures*, vol. 72, pp. 17-26, Sep. 2015.

[17] M. A. Wright, “The Impact of Quantum Computing on Cryptography,” *Network Security*, vol. 2000, no. 9, pp. 13-15, Sep. 2000.

[18] M. A. Nielsen and I. L. Chuang, “Introduction and overview,” *Quantum Computation and Quantum Information*, 10th ed. New York, USA: Cambridge University Press, 2011, p. 7. [Online]. Available:http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf

[19] A. Harrow, “Why Now is the right time to study quantum computing,” *Crossroads*, vol. 18, no. 3, pp. 32-37, Mar. 2012.

[20] L. K. Grover, “Quantum Mechanics Helps in Searching for a Needle in a Haystack,” *Physical Review Letters*, vol. 79, no. 2, pp. 325–328, Jul. 1997.

[21] C. H. Bennett, G. Brassard and A. K. Ekert, “Quantum Cryptography,” *Scientific American*, vol. 267, no. 4, pp. 50-57, Oct. 1992.

[22] IBM, “IBM’s Test-Tube Quantum Computer Makes Histroy,” Ibm.com

[23] https://www-03.ibm.com/press/us/en/pressrelease/965.wss (Accessed Jun. 28, 2020)

[24] P. Carey, “Quantum Computing Breakthrough,” *Mercury News*, May18, 1998. [Online]. Available: https://www.infowar.com/(Accessed Jul. 16, 2020)

[25] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, ser. SFCS ’94. Washington, DC, USA: IEEE Computer Society, 1994, pp. 124–134

[26] D. Gottesman, “Quantum Computers,”

[27] https://qso.lanl.gov/~gottesma/QComputers.%20Html(Accessed Jun. 17, 2020)

[28] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[29] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[30] B. Prajapati, “Limit of Privacy and Quantum Cryptography,” *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, vol. 4, no. 4, pp. 1567-1571, Apr. 2018.

[31] M. Dusek, N. Lutkenhaus and M. Hendrych, “Quantum cryptography,” *Progress in Optics*, vol. 49, pp. 381–454, Mar. 2006.

[32] D. Denning, “Is quantum computing a cybersecurity threat?,” Theconversation.com

[33] https://theconversation.com/is-quantum-computing-a-cybersecurity-threat-107411 (Accessed Jun. 17, 2020)

[34] V. Stolbikova, “Can Elliptic Curve Cryptography be Trusted? A Brief Analysis of the Security of a Popular Cryptosystem,” ISACA Journal, vol. 3, May. 2016.

[35] A. Muhammad Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data,” *Cryptography and Network Security*, Jun. 2017.

[36] N. Abdul Wahid, A. Ali, B. Esparham and M. Marwan, “A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention,” *Journal of Computer Science Applications and Information Technology*, vol. 3, no. 2, pp. 1-7, Aug. 2018.

[37] A. Gupta and N. Kaur Walia, “Cryptography Algorithms: A Review,” *International Journal of Engineering Development and Research (IJEDR)*, vol. 2, no. 2, pp. 1667-1672, 2014.

[38] K. Imamoto and K. Sakurai, “Design and Analysis of Diffie-Hellman-Based Key Exchange Using One-time ID by SVO Logic,” *Electronic Notes in Theoretical Computer Science,* vol. 135, no. 1, pp. 79-94, Jul. 2005.

[39] V. Mavroeidis, K. Vishi, M. D. Zych, A. Josang, “The Impact of Quantum Computing on Present Cryptography,” *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 3, Mar. 2018.

[40] R. A. Perlner and D. A. Cooper, “Quantum Resistant Public Key Cryptography: A survey,” *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, Gaithersburg, Maryland, USA: IDtrust, 2009.

[41] A. Broadbent and C. Schaffner, “Quantum Cryptography Beyond Quantum Key Distribution,” *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 351-382, Oct. 2015.

[42] E. Williams, “Quantum Computing Kills Encryption,” Hackday.com