Research Outlook of Crypto Systems in the Quantum Computing Era

Innovatus: A Journal on Computing Technology Innovations, Vol. 6, No. 1, 2023

Roselle S. Solitario[1]
roselle.delosreyes@ibrict.edu.om
[1] *IT Department Lecturer, University of Technology and Applied Sciences-Ibri, Sultanate of Oman*

ISSN (P) 2651-6993, ISSN (E) 2980-5031
Pre-print DOI No. 10.5281/zenodo.7519215

FOR PUBLISHERS ONLY:
Manuscript received: October 27, 2022; revised: January 8, 2023; accepted: January 10, 2023

ABSTRACT

This paper puts into perspective the directions of cybersecurity research with a goal of determining where it will lead us. Based on the analysis of the previous works, the author recommends adhering to the basic countermeasure principles as a solution to the long-standing dilemma of security researchers and experts in the endless race against the attackers. Secure communications are one of the necessities to humankind. It has been around for centuries, taking many different forms, from manual lock and keys to modern cryptographic systems, all aimed at one goal: to keep the data secret known only to its intended recipients. Globally, many attempts have been made to create an ultimately secure way to transport data, but the same number of efforts have been put by attackers to break these secure systems, thus the competition between crypto designers and the attackers.

KEYWORDS Cryptography, Key Distribution, Public Key exchange, Quantum Computing, QC-resistance.

1 INTRODUCTION

Computer security has been second nature to digital communications. Dating back to when the first commercial antivirus was created, experts from the IT industry as well as the academic research community incessantly pitch in new developments in the field of cybersecurity, with a few of the recent ones can be found in these papers [1] [2]. The opportunities become increasingly demanding and more competitive salaries offered in both private and public organizations, thus the demand for more cybersecurity professionals[1].

Yet, no matter the advances in the field of cybersecurity, all boils down to the 3 fundamentals goals of Computer Security – *Confidentiality*, *Integrity*, and *Availability*, collectively known as the CIA [3] in the cybersecurity world. Every modern security solution must exhibit the following characteristics:

- Confidentiality- or the ability of a system or network to limit access to authorized entities only;
- Integrity – the ability to detect unauthorized modifications, addition or deletions on a data or system settings; and,
- Availability – the resilience of a system or network to service its users with its computing requirements, whenever or wherever it is needed.

A lapse on any of the above–mentioned are unacceptable, and thereby, increases the vulnerability of a network or a system to security threats [4]. Over time, other security services emerged. Among them, non-repudiation is one of the areas well-sought for, as it protects the credibility of both the sender and receiver [5], hence, the assurance of trustworthiness of both. Modern security systems combine non-repudiation with CIA in varying levels, such as in the case of Cryptography [6].

Cryptography has been one of the most dynamic fields in computer security. The past two decades has seen numerous advances with respect to algorithm design and implementation in keeping abreast with the changing security requirements of secure digital communications [7]. For instance, WhatsApp, a popular messaging app in the middle eastern countries, uses Secure Hash Algorithm (SHA-256) for authentication and Advanced Encryption Standard (AES-256) for encryption. Google uses AES-256 as well. MS Outlook, on the other hand, uses different AES flavors in tandem with the classical Triple Data Encryption Standard (Triple DES or 3DES). Other enhancements followed the aforementioned cryptographic algorithms, producing newer algorithms such as Two-fish, Blowfish, ARC2, and CAST. Several published articles have claimed one algorithm is better than the others. However, comparing their results only led to the understanding that the differences really depend on the key performance measures being considered for every research conducted [8] [9] [6].

Perhaps, the most relatable use of cryptography is when we pay online transactions using our credit or debit cards. Imagine sharing your bank details over the internet? Thankfully, the financial institutions were mandated to implement security mechanisms to protect the banking details of their customers.

[1] https://www.netacad.com/courses/cybersecurity

Innovatus: A Journal on Computing Technology Innovations
UNIVERSITY OF ASIA AND THE PACIFIC
UA&P

Cryptographic algorithms have flavors, or variants, that tells the number of bits used for calculating the hash function and the cipher text. Thus, the numbers after the algorithm names, such as SHA-1,SHA-2, SHA-256[2], as well as AES-128, 292, 256-bit variants[3].

Both the research community and the industry experts in the commercial sector of cybersecurity are pitching in solutions to newly discovered threats. Interestingly, these modern security solutions are built on the classical algorithms; they are just improvements of their predecessors. The crypto systems that we know now were evolutions of the older ones. Having this in mind, let us revisit the basics of modern cryptosystems.

The modern cryptographic process can either be symmetric or asymmetric [10] [11]. The former, also known as secret-key cryptography, uses the same (shared) key to encrypt and to decrypt the data, while the latter, also known as public-key cryptography, uses a pair of private keys (secret code) and public key (shared secret). In asymmetric encryption (or public-key cryptography), the private key is known only to each participating nodes while the public key can be shared by both communicating parties over an insecure network.

Diffie Hellman (DH) is what usually will come to mind if we talk about public key cryptography. Deemed as one of the most significant developments in public-key cryptography, DH protocol is still frequently used to secure connections to websites, remotely accessing computers and encrypting emails [12]. DH protocol provides the means for two communicating parties to use a publicly shared codes to generate a key to encrypt on the sender's side and to decrypt on the receiver's side. It allows those who have never met before to safely create a shared secret key. Although it has been implemented in security protocols such as Transport Layer Security (TLS) [13] [14], IPsec [15], Secure Shell (SSH) [16] and many others, DH protocol still faces the problem of authentication [17]. A key sent over an insecure network can easily get to the hands of attackers. That said, a stronger security for key establishment is necessary.

2 CURRENT TRENDS

Cryptography is the cornerstone of secure communications over insecure networks like the internet. But there is more to cryptography than just transforming plain text data to cipher text; it also includes the secure transfer of cryptographic keys known as the key exchange. Key Exchange (KE) protocols play a significant role in enabling the use of shared key for asymmetric cryptography. It has been widely used in building secure channels over insecure network like the internet. Two important types of KE protocols are the Diffie Hellman (DH) and Rivest-Shameer-Adleman (RSA) algorithms, which have been widely studied and are continuously getting new developments, as seen in the works of [17] [18] [12] [19] [20] [21] [22] [23] . Some KE protocols are used in tandem with other cryptographic standards, while other KE schemes are embedded in the cryptographic algorithm itself [24]. Works have also been published about hardening the security of key exchange by combining more than one KE protocols and/or cryptographic algorithms [22] [21] .

Recently, the IT community is bracing for the possible repercussions of Quantum Computing (QC) [25] to the security of inter-network communications [26]. The Shor's algorithm, being one of the first applications of the quantum method in Cryptography [27], has also been extended to be used as an attack. The likes of Shor's algorithm will eventually arrive and will render many encryption algorithms ineffective in protecting the data being transmitted over a network. The problem lies not only in the security of transmitting the cryptographic key over insecure networks, but also to make cryptography as dynamic as possible, also called crypto agility [28], to avert the possible threats brought by the coming of the QC era.

This paper intends to give a synopsis of the developments in cryptosystems and its race with the equally evolving threats to cybersecurity in the Quantum Computing era.

3 OPPORTUNITIES

3.1 Cryptographic Algorithms Research

Cryptographic algorithm is one of the most popularly researched topics in the field of Cybersecurity. In fact, during the past 5 years, a search for Cryptosystem research from a single database (IEEE Xplore) yielded more than 16,000 search results[4]. Several categorizations arise, such as Classic Cryptography, Modern Cryptography, Cognitive Cryptography, Quantum Cryptography, and many more.

Classical cryptographic systems are systems that have been used in ancient times. They may be old, but they served their purposes well during their times. The likes of Caesar Cipher and Enigma, which were used prior to World War II [29], were in fact, the bases for modern cryptosystems.

Modern Cryptography systems are those that have been described in the introduction part of this paper. They are further classified into symmetric and asymmetric, which, differs in the way the communicating systems exchange keys. These classical cryptographic systems that have gained the attention of much research include Data Encryption Standards (DES), Triple DES (TDES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Diffie Hellman (DH) [10]. Some of them even evolved into multiple versions aiming to streamline the process or make the system more secure.

Cognitive Cryptography uses the strategy of combining classical systems with modern (cognitive) approaches [30].

[2] https://www.sslauthority.com/the-difference-between-sha-1-sha-2-and-sha-256-hash-algorithms

[3] https://www.n-able.com/blog/aes-256-encryption-algorithm#:~:text=The%20National%20Institute%20of%20Standards,bit%2C%20and%20256%2Dbit.

[4] https://ieeexplore.ieee.org/search/searchresult.jsp?queryText=cryptography&highlight=true&returnFacets=ALL&returnType=SEARCH&matchPubs=true&ranges=2018_2023_Year

3.2 Quantum Computing

Quantum Computing (QC), or the use of superposition, interventions, and complicated calculations, brought communication security risks to new heights [25]. It is said that QC can make existing cryptographic schemes useless unless modified to address the challenges that it will bring. Several studies have been conducted to see how QC affects cryptography. Those studies evaluates the resistance of existing algorithms to learn how to retain the level of security that it guarantees at present [26] [31] [32] when QC era arrives.

4 THREATS

Quantum computing is already a work in progress. But the National Institute of Standards and Technology (NIST) believes that a fully functional Quantum computer will not be available until 2036 [33]. Even though it is not yet here, cryptographers are starting to provide solutions that will be ready by the time it is needed. The perceived computational power of quantum computers can exponentially break any strong cryptographic algorithm.

The security of cryptographic systems depended on the difficulty of solving the discrete logarithmic problem, which was eventually broken by Number Field Sieve (NFS) algorithm. New developments in cryptosystems are evolving towards more complex computations. For instance, there was an enhancement of the former version of DH using Elliptical curve (ECDH) to increase the computation complexity [33]. The problem, however, when using a large prime number (P), there is tradeoff on the processing time. Using small P numbers on the other hand makes it susceptible to Pollard's Rho algorithm. Therefore, making more complex the computations is no guarantee that what is secure right now will be ultimately secure when QC arrives [34]. Besides. Rios [35]mentioned that any computational secure protocol night be insecure in a matter of years or decades because it depends on the similarly advancing computational resources.

5 CRITICAL ISSUES AND FUTURE SCOPE

The ever-changing needs for secure communications make the IT security community busy since two decades ago. They continue to find alternatives that would ensure the security of the cryptographic algorithm without a trade off on the computational speed it requires. There are published modifications on modern algorithms to improve in one aspect or the other (speed or security) such as the works of [36] [37], but the challenge is how to balance between both. Combining existing cryptographic methods is one of the solutions seen, as demonstrated in the works of [21] that combines DH and RSA, or the paper of [23] that combines DH with AES, and the works of [38] that combines AES with MD5 to get the best features of both to enhance processing speed while maintaining its security.

This paper was written after an in-depth review of published works and the analysis of their proposed cryptosystems. The analysis gave insights on the different techniques used by different researchers to improve cryptosystems – both key establishment and encryption algorithms.

The modern cryptosystems are sufficiently secure until a successful attack happens. For this reason, continuous efforts are being done to update how they work. For instance, the DH protocol, considered one of the most important developments in internet security, is only safe until QC arrives.

To date, researchers are scrambling to develop Quantum-resistant cryptographic algorithms. Complex mathematical functions, combinatorial algorithms, and modifications of formula or parameters are among the common research methodologies used, trying to outsmart the possible attacks in the Quantum world. However, there is no guarantee that more complex mathematical functions can be ultimately secure when the QC era arrives.

This said, the author recommends that instead keeping up with the race for increasing complexity of mathematical functions used in cryptographic algorithms, why not try "diversity" as a good a strategy for countering attacks? For instance, we can modify DH's key exchange functions by introducing secret codes that comes from one or both communicating parties and use it as security bits to be padded to the shared key. It makes the cryptographic key diverse in the sense that it makes unique keys for every transaction, thus, no two keys will be the same for different transactions even for parties who have previously communicated with each other.

Additionally, future researchers can explore other ways of strengthening the security of cryptographic systems by way of layering that can be achieved, for instance, by key encapsulation - that is, to wrap the cryptographic key into another layer of encryption algorithm. You could combine algorithms such as the key exchange algorithm of DH or RSA, but after the key generation, wrap it with another layer of security by using existing cryptographic standards, such as SHA-256 or SHA3.

There is no telling whether any of those strategies can withstand Quantum attacks, or how long it can stand unbroken. But the idea of sticking to some of the basic strategies of countering attacks, such as diversity and layering, could be worth a try.

REFERENCES

[1] A. Al-Far, A. Qusef and S. Almajali, "Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics," in *2018 International Arab Conference on Information Technology (ACIT)*, Werdanye, Lebanon, 2019.

[2] T. P. Thao, A. Miyaji, M. S. Rahman, S. Kiyomoto and A. Kubota, "Robust ORAM: Enhancing Availability, Confidentiality and Integrity," in *2017*, Christchurch, New Zealand, 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC).

[3] M. Ciampa, COMPTIASecurity+ Guide to Network Security Fundamentals, Fourth Edition., USA: Cengage, 2012.

[4] M. Kumar, J. Meena, R. Singh and M. Vardhan, "Data outsourcing: A threat to confidentiality, integrity, and

availability," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, India, 2015.

[5] X. Li, Q. Guo and Q. Zheng, "Formal Analysis and Improvement of ZG Non-repudiation Protocol," in *2010 Second International Workshop on Education Technology and Computer Science*, Wuhan, China, 2010.

[6] V. Poonia and N. S. Yadav, "Analysis of modified Blowfish algorithm in different cases with various parameters," in *2015 International Conference on Advanced Computing and Communication Systems*, Coimbatore, India, 2015.

[7] S. Katsikeas, P. Johnson, M. Ekstedt and R. Lagerström, "Research Communities in cyber security: A Comprehensive Literature Review," arXiv.org; Ithaca, United States, Ithaca, 2021.

[8] A. Kubadia, D. Idnani and Y. Jain, "Performance Evaluation of AES, ARC2, Blowfish, CAST and DES3 for Standalone Systems : Symmetric Keying Algorithms," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2019.

[9] E. M. Mohamed, S. El-Etriby and H. S. Abdul-kader, "Randomness testing of modern encryption techniques in cloud environment," in *2012 8th International Conference on Informatics and Systems (INFOS)*, Giza, Egypt, 2012.

[10] P. S. Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, 2017.

[11] V. S. Igumnov and V. N. Lis, "Influence of Quantum Computers on Classical Cryptography," in *2007 8th Siberian Russian Workshop and Tutorial on Electron Devices and Materials*, Novosibirsk, Russia, 2007.

[12] A. S. Rawat and M. Deshmukh., "Efficient Extended Diffie-Hellman Key Exchange Protocol," in *2019 International Conference on Computing, Power and Communication Technologies (GUCON)*, India, 2019.

[13] D. E. Simos, K. Kleine, A. G. Voyiatzis, R. Kuhn and R. Kacker, "TLS Cipher Suites Recommendations: A Combinatorial Coverage Measurement Approach," in *2016 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, Vienna, Austria, 2016.

[14] S.-M. Kim, Y.-H. Goo, M.-S. Kim, S.-G. Choi and M.-J. Choi, "A method for service identification of SSL/TLS encrypted traffic with the relation of session ID and Server IP," in *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Busan, Korea (South), 2015.

[15] V. HASHIYANA, T. HAIDUWA, N. SURESH, A. BRATHA and F. K. OUMA, "Design and Implementation of an IPSec Virtual Private Network: A Case Study at the University of Namibia," in *2020 IST-Africa Conference (IST-Africa)*, Kampala, Uganda, 2020.

[16] T. Ylonen, "SSH Key Management Challenges and Requirements," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Canary Islands, Spain, 2019.

[17] A. Taparia, S. K. Panigrahy and S. K. Jena., "Secure key exchange using enhanced Diffie-Hellman protocol based on string comparison," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017.

[18] P. Deshpande, S. Santhanalakshmi, P. Lakshmi and A. Vishwa, "Experimental study of Diffie-Hellman key exchange algorithm on embedded devices," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, 2017.

[19] A. Karakra and A. Alsadeh, "A-RSA: Augmented RSA," in *2016 SAI Computing Conference (SAI)*, London, UK, 2016.

[20] Q. Liu, Y. Li, L. Hao and H. Peng, "Two efficient variants of the RSA cryptosystem," in *2010 International Conference On Computer Design and Applications*, Qinhuangdao, China, 2010.

[21] J. E. Avestro, A. M. Sison and R. P. Medina., "Hybrid Algorithm Combining Modified Diffie Hellman and RSA," in *2019 IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E)*, Bali, Indonesia, 2019.

[22] T. K. Hazra, A. Mahato, A. Mandal and A. K. Chakraborty, "A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques," in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, Bangkok, Thailand, 2017.

[23] Y. Yusfrizal, A. Meizar, H. Kurniawan and F. Agustin., "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption," in *The 6th International Conference on Cyber and IT Service Management (CITSM 2018)*, Parapat, Indonesia, 2018.

[24] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," 2001. [Online]. Available: https://iacr.org/archive/eurocrypt2001/20450451.pdf. [Accessed 29 Sept 2021].

[25] A. Vaishnavi and S. Pillai., "Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods," *Journal of Physics: Conference Series,* vol. 1964, no. 4, 2021.

[26] A. Raya and K. Mariyappn., "Diffie-Hellman Instantiations in Pre- and Post-Quantum World: A Review Paper," in *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, India, 2020.

[27] N. Chouhan, H. K. Saini and S. C. Jain., "A novel technique to modify the SHOR'S algorithm — Scaling the encryption scheme," in *2017 Second International*

Conference on Electrical, Computer and Communication Technologies (ICECCT), India, 2017.

[28] O. Grote, A. Ahrens and C. Benavente-Peces., "A Review of Post-quantum Cryptography and Crypto-agility Strategies," in *2019 International Interdisciplinary PhD Workshop (IIPhDW)*, Wismar, Germany, 2019.

[29] A. A. Bruen, M. A. Forcinito and J. M. McQuillan, "Classical Ciphers and Their Cryptanalysis," in *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*, Wiley Data and Cybersecurity, 2021, pp. 21-45.

[30] M. R. Ogiela and L. Ogiela, "Cognitive Cryptography in Advanced Data Security," in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, Krakow, Poland, 2018.

[31] M. Stipcevic, "Quantum random number generators and their use in cryptography," arXiv.org;, United States, Ithaca, 2011.

[32] G. Mogos, "Use quantum random number generator in Diffie-Hellman key exchange protocol," in *2016 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, Cluj-Napoca, Romania, 2016.

[33] A. Raya and K. Mariyappn, "Diffie-hellman Instantiations in Pre- and Post-Quantum World," in *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Bangalore, India, 2020.

[34] R. A. Grimes, "How Can Quantum Computing Break Today's Cryptography?," in *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*, Wiley Data and Cybersecurity, 2020, pp. 59-83.

[35] C. Rios, "Experimental Characterization of a Discrete Gaussian-Modulated Quantum Key Distribution System," University of Arizona, 2021.

[36] U. Coruh and O. Bayat, "Hybrid Secure Authentication and Key Exchange Scheme for M2M Home Networks," *Security and Communication Networks; London,* vol. 2018, p. 25, 2018.

[37] C. Diwan and S. K. Singh, "AN APPROACH TO REVAMP THE DATA SECURITY USING CRYPTOGRAPHIC TECHNIQUES," in *International Journal of Advanced Research in Computer Science;*, Udaipur,India, 2017.

[38] H. Pasaribu, D. Sitanggang, R. R. Damanik and A. C. R. Sitompul., "Combination of advanced encryption standard 256 bits with md5 to secure documents on android smartphone," *Journal of Physics: Conference Series; Bristol,* vol. 1007, no. 1, 2018.