A SYSTEMATIC SURVEY ON CRYPTO ALGORITHMS USING QUANTUM COMPUTING

GOVINDU SURLA[1], R. LAKSHMI[2], I. THAMARAI[3]

[1]Research Scholar, Pondicherry University, Department of Computer Science, India

[2]Assistant Professor, Pondicherry University, Department of Computer Science, India

[3]Associate Professor, Panimalar Engineering College, Department of Computer Science and Engineering, India

E-mail: [1]govindu561@gmail.com, [2]prof.rlakshmi@gmail.com, [3]thamarai.panimalar@gmail.com

ABSTRACT

The concept of a quantum computer is now well-established. It's the most cutting-edge tech out there, and every nation is competing for quantum supremacy. It is technology that will reduce computing time from decades to hours or minutes. Access to quantum computing capabilities will be a huge boon to the scientific community. The issue it raises, however, is one of the greatest cyber security dangers we face today. To that end, this paper will first present the reader to some fundamental post-quantum algorithms and then elaborate on the effects of quantum computing on modern cryptography. All cryptographic algorithms are theoretically susceptible to attack. When commercial quantum computers with billions of qubits of capacity become available, they will be able to decrypt virtually all existing public-key cryptosystems. The use of public key cryptography has enabled the conduct of secure online transactions. Yet, the security of the most widely used public key cryptography techniques in use today is threatened by breakthroughs in quantum computers. However, quantum cryptography is a promising technique that is set for widespread acceptance in actual cryptographic applications since it has been shown to be secure even in the most general assault allowed by the rules of physics. Using quantum cryptography, two people can build on an existing secret key. To accomplish this, several quantum cryptography techniques have been developed. We go over some of the concerns that protocol designers might need to take into account if it becomes necessary to employ these algorithms and give an overview of some of the developed cryptographic algorithms that, while not yet widely used, were thought to be resistant to quantum computing assaults.

Keywords: *Quantum Computation, Quantum Theory, Cryptography, And Quantum Public Key Distribution*

1. INTRODUCTION

Electronic communications, in particular, have benefited greatly from technical progress and are now one of the age's primary pillars of technology. Cryptography is one of the most pivotal areas of study in IT because of ensuring data privacy, integrity, validity, and non-repudiation during transmission and storage is critical. From the Greek for "hidden writing," cryptography refers to the practice of making information unreadable to unauthorized parties while it is in transit or storage. For the sake of online safety, cryptography is among the most vital building blocks. Both symmetric and asymmetric cryptosystems are in use today.

To ensure that only the sender and the intended recipient can decipher the message, cryptography combines the art of presentation techniques with the science of information security. Most contemporary cryptographic methods can be characterized as being based on elaborate mathematical formulas. During their development, cryptographic algorithms rely on assumptions about the nature of the underlying computational issues. An asymmetrical problem is, for instance, the factorization of an integer with a thousand digits; multiplying two integers is simple, but factoring such a number is difficult. The encryption process makes use of two keys, one of which is made public while the other is kept private. It is computationally impossible to determine the private key from the public key. Until now, the idea that a computer Programme can quickly multiply large prime numbers on its own has been the foundation of public key encryption, but that it would take hundreds of years to reverse the calculation. The capability to decrypt data encrypted with existing public key encryption methods will be greatly aided by quantum computing.

Richard Feynman introduced the idea of quantum computing in 1982; since then, it has been the subject of intense study and is widely seen as a threat to the security of existing forms of asymmetric cryptography. Compared to traditional computing methods, quantum computing's speed is a direct result of its foundation in quantum theory. Quantum computers can easily break classical cryptographic techniques. Existing information technology infrastructure will become fully vulnerable during the transition to the quantum computer, necessitating the creation of quantum-safe or subatomic cryptographic techniques. It is also true that certain quantum algorithms might compromise symmetric cryptography; nevertheless, this method's security can be improved by using larger key spaces. The security of current asymmetric crypto methods is based on the difficulty of factoring extremely large prime numbers as well as the discrete logarithm problem, algorithms have been developed that can crack them. It seems that even the most safe and effective system available today, elliptic curve cryptography, is vulnerable to quantum computers. Therefore, there is a requirement for cryptographic algorithms that can withstand attacks from quantum computers.

An actual quantum computer is now within reach. Many experts agree that this is the most important technological development of our time, and nations are competing to build the most advanced quantum computer possible, which can ensure their supremacy in the quantum computing arena. The USA, China, France, Britain, France, and Russia are the early front-runners, while other countries are making strong efforts to catch up. It's not just individual countries that are competing for dominance over "Quantum Computing"; major IT companies like Google, IBM, Facebook, D- Wave, Toshiba, etc., are also major drivers in this race. Using a quantum phenomenon for computation, an application of a quantum mechanism is quantum computing. Computing on a quantum level requires a special kind of machine called a quantum computer. To execute algorithms, it performs controlled manipulations of the states of qubits. If you're familiar with classical bits, you'll recognize the qubit (or quantum bit) as its quantum mechanical counterpart. A bit is the basic unit of information storage in traditional computers; bits can only take on the values zero or one. Quantum bits are the information storage units of choice in quantum computing. States of qubits are represented by the numbers 0 and 1, respectively. Qubits (quantum bits) can simultaneously be in the 0 or 1 state. Strange things happen at the quantum level. The following properties of quantum states are used in the construction of quantum computers.

i) **Superposition:** It is possible for quantum systems to simultaneously exist in two distinct but related states. A qubit can hold both the zero and one states simultaneously. The qubit will "collapse" to either 0 or 1 whenever the measurement is made.

ii) **Entanglement:** The quantum mechanical phenomenon of entanglement allows for a mutual description of the states of entangled particles. Every single measurement done on one entangled particle has an instantaneous effect on the other entangled particle, regardless of their relative positions.

iii) **Interference:** One of the main concepts underlying quantum computing is the regulation of the collapse probability of qubits into a specific measurement state. It's because of things like quantum interference that Quantum computing's development timeline.

The field of quantum computing is expanding rapidly. Expansion in this area is skyrocketing over the world. Researchers are only interested in one thing: developing a quantum computer with more than one qubit and extremely fine error control. The last 22 years have seen amazing progress in this area (Fig. 1). It is possible that a 2-qubit quantum computer will be developed by the likes of MIT, Oxford, Berkeley, and IBM by early 1998. This year, Google unveiled its 72- qubit quantum computer. In 2019, Rigetti declared [1-3] that they will create a 128- qubit quantum computer within a year. There have been three distinct generations of quantum computers.

i) **First Generation:** The initial generation of quantum computers is created for experimental, non-commercial purposes.

These somewhat sophisticated models were developed for working prototype purposes.

ii) **Second Generation:** In the future, it's possible for many teams to make the basic research breakthrough and to have the hardware infrastructure needed to build a quantum computer with more qubits and complexity. The second generation of quantum computers is being developed in response to high-end commercial and academic applications that require more scalability and processing speed. These quantum computers might be farmed out to fulfill increased computational needs, like how cloud computing handles peak demand.

iii) **Third Generation:** As the hardware cost continues to decrease as a result of exponential growth and development, the third generation will usher in full quantum supremacy. In the not-too-distant future, everyone will be able to afford and have easy access to a quantum computer. When compared to classical computers and programs, the 3rd quantum computer will provide a superior solution for a wide range of non-commercial uses.

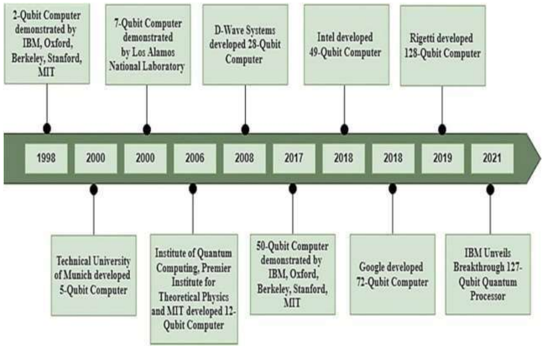
2-Qubit Computer demonstrated by IBM, Oxford, Berkeley, Stanford, MIT
7-Qubit Computer demonstrated by Los Alamos National Laboratory
D-Wave Systems developed 28-Qubit Computer
Intel developed 49-Qubit Computer
Rigetti developed 128-Qubit Computer
1998
2000
2000
2006
2008
2017
2018
2018
2019
2021
Technical University of Munich developed 5-Qubit Computer
Institute of Quantum Computing, Premier Institute for Theoretical Physics and MIT developed 12-Qubit Computer
50-Qubit Computer demonstrated by IBM, Oxford, Berkeley, Stanford, MIT
Google developed 72-Qubit Computer
IBM Unveils Breakthrough 127-Qubit Quantum Processor

Figure 1: Growth of Quantum Computing [4]

The remaining part of the paper is organized as follows. Section2 primarily highlights the driving forces for our work in the field of quantum cryptography.Section3 Discusses about the key differences among the Quantum computing and classical Computing.Section4 provides traditional and latest survey on Quantum Cryptography.Section5 discusses about the key issues in quantum cryptography which forms a basis for our research.section6 provides the key Research Areas in Crypto algorithms and Quantum Computing followed by section 7 which provides

us the objectives of proposed research and finally section8 concludes the paper.

2. MOTIVATION

The field of quantum communication uses quantum physics to offer a variety of possibilities for securely sharing sensitive information between parties that are separated by distance. Since then, quantum key distribution techniques have become commonplace for secure two-way communication. It may also be easily expanded to include more than two participants, allowing for a wider range of multiparty quantum communication applications. Since its implementation in mobile phone networks & fiber optical networks, the four-party quantum key secret image sharing protocol has attracted significant interest in multiparty quantum communication. Insecure communication can result from this protocol's susceptibility to a collective eavesdropping attack. Quantum key distribution techniques like BB84, B92, and so on have been the subject of much study, with researchers analyzing their resistance to a wide range of attacks. The robustness of the four-party Quantum Secret Sharing (QSS) protocol and the ability to counteract eavesdropping attacks are not standardized areas of study. Elliptic Curve Cryptography (ECC) oriented QSS & Hyper-Elliptic Curve Cryptography (HECC) oriented QSS are required to enhance the safe operation of the four-party quantum secret exchange protocol.

3. QUANTUM COMPUTING VS CLASSICAL COMPUTING

Richard Feynman proposed the concept of a quantum computer in 1982. This is a computer that takes advantage of the phenomena associated with quantum mechanics. As a branch of physics concerned with subatomic particles and their peculiar behavior, quantum mechanics is relevant at the tiny scale. Bits are the basic building pieces of a classic computer, and they have just two observable states: 0 and 1. On the other hand, quantum computers use qubits, often known as quantum bits [5]. Qubits can exist simultaneously in the 0 and 1 states because of superposition, which broadens the range of possible uses. When a particle is examined, it transitions into one of these states. Complex issues can be simplified by using this characteristic of quantum computers. A qubit under superposition undergoes an operation that affects both values simultaneously. Another physics phenomenon used in quantum computing is quantum entanglement. Once two qubits become entangled, their quantum superposition can be represented only collectively, as if describing a single entity with four possible states. Furthermore, regardless of their separation in space, the tangled qubit will undergo a corresponding change in state. When this happens, we get genuine parallel computing power [6]. The total number of values that may be processed in a single operation grows exponentially as the number of entangled qubits increases as a result of the aforementioned phenomena. As a result, 2n operations can be processed simultaneously by an n- qubit quantum computer.

In the realm of quantum computing, we find both universal and non-universal machines. The non-universal quantum computers are made for specialized tasks, while the universal quantum computers are developed to tackle any task. D-non- universal Wave's quantum computer with over 2,000 qubits [7] and IBM's universal qubit with 17 qubits and accurate error correction are two such examples. As far as universal quantum computers go, IBM's is the best there is right now [8]. Quantum computing resources are available online for study purposes from both D-Wave and IBM. A 17-qubit universal quantum computer was also disclosed by Intel and QuTech in October 2017 [8]. According to Bone and Castro [9], a quantum computer's architecture is fundamentally different from that of a classical computer, which employs more conventional components like transistors and diodes. Researchers have experimented with a variety of alternative architectures, including quantum dots, in which electrons exist in a superposition state, and computing liquids. Furthermore, they highlighted that the employment of algorithms that take use of quantum parallelism is essential for quantum computers to demonstrate their superiority over classical computers. A quantum computer wouldn't be any faster than a classical one at multiplying, for example.

4. SURVEY OF QUANTUM COMPUTING

Because to its reliance on a physical concept, quantum cryptography introduces a novel form of secure encryption that is invulnerable to attack without the sender's and receiver's knowledge. Quantum computers use entanglement and superposition, among other quantum phenomena, to execute calculations. It belongs to the realm of quantum communication and information sciences. Quantum key distribution is based on quantum physics and classical information theory (QKD). Public and private parts make up the two halves of the shared key. With QKD, you may rest assured that your sent data will remain secure. QKD's main and distinctive feature is that its users can use the concepts of quantum state or quantum entanglement to identify the presence of any unauthorized individuals attempting to steal the key.

As opposed to the bits employed in classical systems, the quantum key exchange encrypts the message in states of qubits. Quantum states are frequently represented by photons. There are two main approaches that have been put into practice: a) prepare & measure protocols, and b) entanglement-based protocols. We have done a Systematic literature survey as shown in Figure.2.

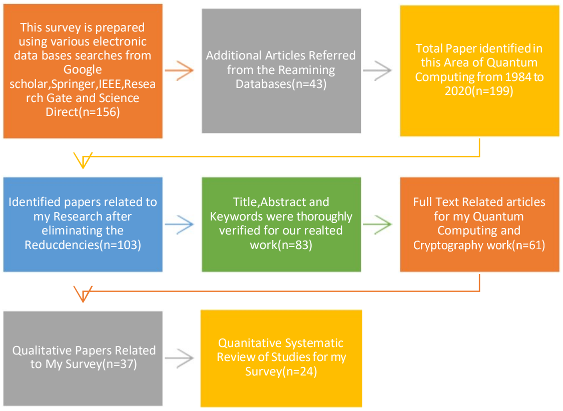
This survey is prepared using various electronic data bases searches from Google scholar,Springer,IEEE,Research Gate and Science Direct(n=156)
Additional Articles Referred from the Reamining Databases(n=43)
Total Paper identified in this Area of Quantum Computing from 1984 to 2020(n=199)
Identified papers related to my Research after eliminating the Reducdencies(n=103)
Title,Abstract and Keywords were thoroughly verified for our realted work(n=83)
Full Text Related articles for my Quantum Computing and Cryptography work(n=61)
Qualitative Papers Related to My Survey(n=37)
Quanitative Systematic Review of Studies for my Survey(n=24)

Figure 2: Literature Survey on My proposed Research

The first proposal for quantum cryptography using "Heisenberg's Uncertainty Principle" was made in 1984 by Bennett and Brassard [10]. The designation "BB84" was chosen for it. The method works on the premise that any secret key can be transmitted by sending a specific sequence of photons to the receiver. It is the polarisation of the photons that conceals the key's individual bits. So that the attacker cannot detect these photons and transmit those to the recipient with disturbing the state of the light in a measurable way, "Heisenberg's Uncertainty Principle" is then used to take proper care of the attackers. When using BB84, you can choose between four different polarization modes. In the beginning, the sender establishes contact with the recipient via a virtual medium by picking random strings. The receiver then communicates across an unreliable channel his choice of reference frames for determining the quantum states of individual photons.

Bennett [11] proposed a streamlined variant of BB84 in 1992; he called it B92. The theory that describes the power of quantum computers in terms of processing speed was first introduced in 1997 by Bennett, Cohen, Brassard, and Vazirani [12]. Shor's algorithm was used to efficiently solve exponent in polynomial time.

Leuenberger & Loss, (2001) [13] presented a mechanism for quantum computing that would be superior to classical computer in searching databases or factoring numbers. It employs the parallelism of quantum systems to speed up database searches. They discussed how Grover's algorithm can be used to entangle a state with a single particle in superposition and Shor's algorithm can be used to entangle states with multiple particles using molecular magnets in their paper. They theoretically proved that molecule magnets are excellent candidates for building a powerful and compact storage device.

In 2002, Ching-Nung Yang & Chen-Chin Kuo [14] proposed a method that combined BB84 and B92 to provide a fresh approach to QKE. Two QKE protocols were proposed by them. The first goal was to increase QKE efficiency by 42.9%, while the second was to increase theoretical maximum efficiency to 28.6% with an order 2 mean complexity. Their final complexity was O after this process (n2.86).

To this end, Scarani, Acin, Ribordy, and Gisin [15] developed the "SARG04" quantum cryptography protocol in 2004. The number of states in the procedure and in "BB84" is the same in both cases. The sender declares two non-orthogonal states, one of which is used for encoding the bit but does not expose the bases, before the receiver and transmitter decide which bits share the same bases. An accurate measurement of the condition can be made if the receiver employs a suitable basis. And if he picks the wrong one, he won't be able to determine the bit or measure the sender's states.

QKD performance and security can both be enhanced by employing a decoy state, as proposed by Y. Zhao, B. Yi, X. Ma, H. Lo. L. Qiang [16] in 2006. In their work, they presented the results of the first experiments to distribute quantum keys using a decoy state. They demonstrated two distinct decoy state QKD algorithms, one operating over a 15-kilometer telecom fiber and the other operating over a 60-kilometer weak suction telecom fiber. When performed in a decoy state, QKD yielded a zero-key- generation-rate security proof. Using fake state QKD ensured the method's robustness and usefulness for secure data transmission over great distances.

In 2011, Houshmand & Hosseini [17] connected the method to "BB84" using the Dynamic Key Distribution (QKD) rules described by Cabello [18]. By decoding the quantum data stream, a set of qubit pairs can be prepared in advance. In compared to "BB84," their technique conceals less information

about the key bit because both sides confirm on a two-qubit unified operation, U1 and U2, before the process even begins. In their algorithm, none of the transmitted qubits are wasted, whereas in "BB84," half of them are thrown away. Here, one bit is used to denote the reception of a single qubit, while another bit is employed to determine the state of a single qubit collection.

Two transmitting participants connected via a two-way quantum channel are needed for the QKD method described by Zamani and Verma [19] in 2011. Since the approach does not rely on any conventional routes for communication, the time and resources spent on key reconciliation & key shifting are reduced to a minimum. Increased key exchange speed is one of the benefits of this protocol.

In 2012, R. D. Sharma and A. De [20] investigated the weaknesses of existing schemes such lack of sender and receiver authentication, no pre-processing, and no approximation of intruder's information, and presented an improved QKD protocol that employs both classical and quantum channels. There were nine procedures that were carried out to accomplish this. Client authentication, initialization, quantum communications, shifting, error resolution, attacker information guessing, resolution on continuing, confidentiality strengthening, and error-free key acquisition are the procedures involved in enhancing security. M. Razavi [21] proposed a multi-user, multi-access QKD network in 2012. The participants can exchange secret keys with one another without involving any nodes. Instead of a full mesh network, they use the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

switching concept in what is known as a "Wavelength Division Multiplexing" (WDM) network. By associating a positive wavelength with both nodes, the wavelength router links those who wish to swap keys. By reserving two separate wavelength groups at both nodes, a single communication channel can be used for transporting both quantum and conventional signals. WDM networks are combined with either a "Time Division Multiple Access" (TDMA) or a "Code Division Multiple Access" (CDMA) network to form hybrid networks. Each WDM node in such a network architecture can act as a hub for a TDMA or CDMA network with multiple users.

By proposing a new QKD diagram to be circulated between three parties, Odeh, Elleithy, Alshowkan, and Abdelfattah [22] in 2013 offered a strategy for secure communication seen between sender and the receiver. By removing the need for many rounds of inspection and verification of the quantum bases, a trustworthy center makes it easier for clients to exchange the secret message. Their algorithm is divided into two parts: a) user authentication and quantum key distribution; and b) data transfer across a quantum channel. For instance, if the sender wants to establish a connection with the recipient, he must provide QKD with a request that includes his key. QKD then questions the recipient to ensure authenticity. Once both parties have been verified, QKD will begin releasing quantum keys in the some predetermined order, allowing the sender to encrypt the input-text as well as the receiver to decrypt it using his and the sender's public keys.

In 2014, Aldhaheri, Elleithy, etc al. [23] proposed a session key exchange process over the quantum network as a solution to the problems with "BB84" and "B92." The current state and a random state were substituted to ensure the authentication secrets of all users remain secure. A concept is made during the construction of "BB84" to compensate for the signal loss, such as a weak signal source, an almost perfect broadcast line, delicate yet firm quantum sensors, repeaters, and amplifiers. To put their theories into practice, they employ a highly muted laser source to generate multi-photon quantum signals.

In 2018, Gueddana & Lakshminarayanan [24] contrasted "BB84" Quantum Key Transmission with the improved form of "Quantum Dense Coding," and they provided recommendations for circuit applications and theoretical modeling based on their findings. A basic detention mechanism involving a small number of states was proposed in 2018 by Davide Rusca, Ernesto Boaron, et al. [25]. The security proof included a comprehensive analysis of attack divergence.

In 2019, Bacco, Vagniluca, et al. [26] shown how to put up a straightforward inexpensive QKD arrangement over a metro fiber link using co-propagation of a weak quantum beam via a linked fiber. Using time-bin ciphering, it was shown that the three-state "BB84" process is valid. In 2019, Huawang, Raylin, and Yuewei [27] proposed a method of quantum secret sharing based on orbital angular momentum measurement. The sender creates isolated particles at a chosen angle, and the receiver decrypts them using Fourier transformation. The sender generates the shared key using the single- particle observations.

By weakening the protections of the BB84 protocol, Price, Rarity, and Erven [28] showed that DOS attacks might be easily uncovered in the year 2020. They planned a QKD process that might identify unauthenticated users attempting to intervene in the medium by taking command of the nodes and refusing service if the amount of substituted qubits exceeded the finite key limit. They did this by weakening the BB84 protocol in order to create a safe key from two photon polarizations. The below

Table 1: Summarizes the Recent Works in the Area of Quantum Cryptography.

S.N o	Name of the Authors	Proposed Algorithm/ Security Procedure	sults Found	dvantages	isadvantages	Journal
	nnett and assard[10]	isenberg's certainty nciple-based ntum ptography.	nsidered a cific mple of ce and bob shown	blic Key yptography	ck of Security e to Public y	EE ernational nference on mputers stems and

		honor of 84, its ne.	w to do ptography using antum coin sing method			nal cessing, ngalore, lia, cember 34, pp. 175-79
	nnett[11]	dated and amed as 2, this tem is a eamlined sion of 84.	erferometric antum key tribution been alized for ure ptography	le to transfer cret Key ficiently	ctical plementation es some ficulty	antum ptography ng any two n-thogonal tes, ysical view tters, 1992, 3121—24
	nnett, Bernstein, Brassard, and Vazirani[12]	or's algorithm, they solved discrete logarithms in polynomial time	nsidered the cryptographic theorems and proved them in this work	le to implement in Lower Bounds of Quantum Search also	ny of the Lower Bounds are Missing then it remaining may not be traced	engths and weaknesses of quantum computing, SIAM journal on Computing. 26(5), 1510-23,1997
	uenberger and Loss[13]	over's algorithm in super-positioning of the single-particle state and also about the application of Shor's orithm	ved the Grover's algorithm by using Feynman diagrams	le to implement Parallelism in quantum Computing	y not be feasible for larger applications.	antum computing in molecular magnets, Nature, 410(6830), 9,2001.
	ing-Nung ng and en-Chin o[14]	egrated 84 with B92 d crated a brid orithm	plied BB84 tocol on 30 bits with nbinations	e BB84 chanism's uble-layer sign will aid h in data-cordance d privacy ancement.	provements Security ects is eded for uble level 84	hanced antum Key stribution tocols ing BB84 d B92, ceedings the 2002 ernational mputer mposium, 951—9,2002.
	rani, Acin, ordy and sin[15]	bust antum ptographic	thors have monstrated t quantum	onger than 84 in the sence of any	encoding is a versally own quantum	antum yptography tocols

		tocol and ned it as ARG04”.	ptography be greatly engthened encoding a ssical bit in ups of non-hogonal bit states. in face of acks based the splitting photon mbers	ors when jected to S attacks	enomenon t can be egrated with re mplicated cedures, perior coding hniques are cessary.	bust inst oton mber litting acks for eak Laser lse plementatio Physical view tters. 92 : 7901,2004.
	Zhao, B. X. Ma, H. L. an[16]	ggested a coy state D that proves the formance as ll as the urity of the D setup	ed decoy thod tocol and formed merical nulation to form ximum ure	hance the ety and iciency of l-world QKD plementations nificantly.	other words, decoy state proach will y be ective for rter tances if perior QKD ups are used.	nulation d plementatio f Decoy te antum Key stribution er 60km lecom
			stance by the bits			er, ISIT, Seattle, USA, y 2006
	o Yu and Jia[17][18]	D using Cabello’s principle	formed security analysis for quantum error correcting codes for bits which transmits long distances	hen used to QKD, quantum cipher space design (CSS) codes boost key transmission security and confidentiality over noisy quantum channels.	lidity and Security of the Protocol may be enhanced	Entanglement - base Quantum Key Distribution Protocol, Information Security and cryptology (ISCISC), 8th ernational ISC nference, IEEE, pp. —48,2011

	mani and Verma[19]	D algorithm on a 2-way quantum network	mpared the existing with BB84 protocol	y exchange rates can be improved by decreasing the classical channel's overhead. cause to the lack of a traditional method of contact,Cuts down on the cost of doing siness.	sts will increase as more time and effort will be required to ensure the proposed protocol works as intended.	QKD otocol with a Two-way Quantum Channel, Advanced Networks and Telecommun i cation systems (ANTS), 5th ernational Conference IEEE, pp 1-011.
	D. Sharma and Ashok de[20]	hanced QKD protocol that uses both the classical as well as quantum channels	this study, improvement s are made to the quantum key distribution protocol in the areas of error correction, authenticatio n, attack-information estimation, and data secrecy. plifier	thout relying on Computational assumptions, this can ensure the secrecy of encrypted data for an extended period of time..	ta Filtration and Rectification will take more time.	New Secure Model for Quantum Key Distribution Protocol, Industrial and Information system (ICIIS), 6th IEEE ernational Conference, pp 462-6,2012.
	Razavi[21]	stributed Quantum Key Infrastructures with Multiple Access	brid WDM-T/CDMA up has been used in this work across Quantum Key Distribution Networks	th the goal of supporting a high number of users, a hybrid architecture using wavelength routers with passive Optical networks is died and evaluated.	le to apply only on CDMA and FDMA.	ltiple- Access Quantum Key Distribution Networks, IEEE nsactions on Communicati on, vol. 60, 10,2012.
	eh, eithy,	w schematic QKD that is	th the pose of	this body of rk, we have	addition, we y reach a	antum Key stribution

	showkan, Abdelfattah[22]	be mutual circulated amongst three parties.	stering protections for quantum communicati o ns, the authors of this work proposed a novel security quantum algorithm that makes use of public key encryption method to produce keys.	sented a new model for the distribution of quantum keys between three or more parties. is approach requires the presence of a trusted center that supplies the clients with the essential confidential information that will allow for secure communicatio n h each other	w degree of user identification and information privacy protection with this effort.	Using Public Key Algorithm (RSA), ndon, United Kingdom: third International Conference on Innovative Computing Technology (INTECH), IEEE,2013.
	dhaheri, Elleithy[23]	ssion key exchange procedure over the quantum network	order to guarantee that a key is supplied to the conversing parties, this suggested protocol avoids the unnecessary redundancy created by earlier methods.	stributing or exchanging the key that can identify any part of the quantum channel of communicatio n is made safe by the suggested approach.	ta Transmission and Security Mechanisms may be enhanced.	dul rahman Aldhaheri, Khaled Elleithy, Majid Alshammari, Hussam (2014), A vel Secure Quantum Key Distribution Algorithm, University of dgeport,20 14.
	eddana and Lakshminara y anan[24]	graded form of “Quantum Dense Coding”	formed Numerical simulation and physical realisability ng BB84-QKD and BB84-QDC tocols	proves the Security in quantum Circuits	nultiple attacks are happened this may not work properly	ysical Feasibility of QKD based on Probabilistic Quantum Circuits, IET Information Security, Volume 12, ue 6, November 2018, pp. 1– 5,2018.

	vide Rusca, Alberto Boaron[25]	nnett and Brassard's 1984 simplified quantum public key protocol has been proven secure.	signed an Efficient Encoding Scheme and done decoy-state parameter estimation ng with urity proof	ding only three distinct states achieves the same private key rate as sending four states, and the approach is resistant against potential state paration flaws.	urity against coherent attacks may not be possible.	urity proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol, Physical Review A, 5:052336,2 8.
	cco, Vagniluca[26]	w-cost QKD arrangement determined on a metropolitan fiber link	antum key distribution (QKD) scheme stability. We have confirmed the accuracy of error rates, raw data rates, and secret key rates obtained over the course of several hours using two distinct channel nditions.	nonstrating the system's reliability for more than four hours	pensive prices and poor performance, which prohibit widespread use of this new technology in cellular networks.	ld trial of a three-state quantum key distribution scheme in the Florence metropolitan area, EPJ Quantum Technology 6.1: 5,2019.
	awang, Raylin and Yuewei[27]	ret sharing technique via the observation of orbital angular momentum.	rified the correctness, confidentiality, efficiency of the proposed scheme	aler generates random OAM or ANG basis single particles. Quantum Fourier transformations are used to encode the participants' private keys into the particles.	lculations in Fourier Transforms consumes time and more human effort is needed.	antum Secret Sharing by using Fourier Transform on Orbital Angular Momentum, IET ormation Security, (Volume 13, ue 2, rch 2019), 104—8,2019.

	ce, Rarity and Erven[28]	D cedure for detecting unauthenticated users to avoid DDoS attacks	curity of BB84 is verified and applicability of this protocol for DDoS attacks is done	hout any additional tweaks, two-photon pulses can be used to generate a secure key.	mplexity in terms of Key calculations and takes more time for this process.	uantum key distribution protocol for rapid denial of service detection, EPJ Quantum Technology, 2 0.

Quantum cryptography relies solely on quantum physics for decoding, rather than on mathematical algorithms. Quantum cryptography's key benefits are that it is I almost impossible to hack, ii) easy to implement, iii) low-maintenance, iv) effective at solving factorization and discrete logarithm problems, and v) facilitated by the use of quantum computers.

One major drawback is that the range of radio signals is now capped at just 90 miles. Doesn't solve authentication problem Doesn't address a few of the weakest areas in data security, like hacking and key storage, but requires replacing existing hardware arrangement.

5. ISSUES IN QUANTUM CRYPTOGRAPHY

Some of the problems with quantum cryptography are illustrated below:

- **Raw key generation:** Raw For the purpose of key generation, a bit sequence can be sent across the quantum channel and then generated. The size of the key generation depends on the protocol used, the channel characteristics, and whether Eve is monitoring the quantum channel.
- **Sifting:** By filtering out potentially noisy bits, the sifting function makes it unnecessary to provide information about the bits' values over the classical channel. The size of the key is affected by whether Eve is listening, and the resulting "sifted" key is the same for Alice and Bob.
- **Error correction or key reconciliation** [29]: In order to determine if Eve was listening on the transmission medium, the final step of the protocol, key reconciliation, corrects the sifted key for errors and guesstimates the error rate using either the bits that were sacrificed in the previous step or the bits that were sifted out of the key in the previous step. When the rate of errors exceeds a certain threshold, Alice and Bob conclude that Eve has already been listening.
- **Privacy amplification** [30]: If the amount of noise is below the threshold, Eve will continue to listen, but she will choose to make very few inferences. To further reduce Eve's data, Alice and Bob can engage in "privacy amplification," a technique that involves giving up a few bits in exchange for more privacy.
- **Authentication** [31]: After Alice and Bob have transmitted and received messages on the classical channel, they must be authenticated to ensure that no tampering has occurred on Eve's part. To generate an authentication tag, the sender utilizes selected bits of the secret key that was previously exchanged. After a key has been utilized, its associated bits are discarded. Sending the tag with the message allows the recipient to create a new tag using his own private copy of the key. If the labels match, the message is accepted, and the newly generated key is appended to the previous key. If the verification fails, Eve is considered to be attempting to intervene, and the round is terminated.

6. RESEARCH AREA IN CRYPTO ALGORITHMS AND QUANTUM COMPUTING

As an alternative foundation for public-key cryptography, many other approaches have been tested [32], in addition to the standard classical cryptographic methods that are already in use. Progress in these areas may one day lead to public key schemes that are useful, secure, and resistant to quantum computing, even though most of the resulting methods are either unknown or have been cracked. Several NP-complete problems have been used in public-key cryptography, but the knapsack problem was one of the first. The first knapsack-based cryptosystem was suggested by Merkle and Hellman in 1978 [33], but it was quickly proved to be weak against approximation lattice reducing attacks [34]. Since then, many similar schemes have been cracked, with the final one being Chor Rivest [35], which was cracked in 1995 [36].

Replacements for factoring or discrete logarithm have also been proposed, although they are more involved algebraic issues. Some examples are finding solutions to multivariate system of polynomials in galois field, and the conjugacy conducted in order to investigate in braid group. In recent times, both have seen significant attention from mathematicians and cryptologists. The New European Systems for Signatures, Integrity, and Encryption (NESSIE) collaboration adopted SFLASH as a solution to the latter problem in 2003; however, this system was cracked in 2007 [38]. We still don't know when these and other mathematical difficulties will be understood well enough to produce useable public key cryptography primitives with plausible security estimates.

7. OBJECTIVES

By considering the above survey the main objectives of proposed work are as follows:

- One goal is to validate and evaluate conventional algorithms like genetic, cuckoo search, and tabu search that were inspired by quantum computing.
- The current protocol for communicating quantum secrets will be evaluated for its security flaws, and a new, better protocol will be created as a result.
- Multiparty communication performance analysis using metrics like processing time and error rate.

8. CONCLUSION

In today's world, where information is so important, it is critical that data transmission and storage be as secure as possible. Quantum computers can easily break conventional public key methods like RSA and El Gamal as well as symmetric key techniques like DES (3DES, AES). The development of a fully functional universal computing device that can implement robust quantum algorithms appears to be drawing closer every year. All currently used public key algorithms, including RSA & Elliptic Curve Cryptosystems, will be rendered completely insecure as a result of this technological development. As demonstrated by this review, the development of quantum-resistant cryptographic techniques such as lattice-based encryption, hash-based signatures, and code-based encryption is a major concern.

REFERENCES

[1] Gibney E. Quantum computer race intensifies as alternative technology gains steam. Nature 2020;587(7834):342–3.

[2] Help Net Security. Quantum computers: how to prepare for this great threat to information security. Published, Helpnetsecurity.com. [Accessed 24 April 2021].

[3] LaMacchia B. The long road ahead to transition to post-quantum cryptography. Communication ACM 2022;65(1):28–30. https://doi.org/10.1145/3498706.

[4] Kumar, Manish. "Post-Quantum Cryptography Algorithms Standardization and Performance Analysis." Array 15 (2022): 100242.

[5] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th ed. New York, NY, USA: Cambridge University Press, 2011.

[6] R. Jozsa, "Entanglement and Quantum Computation," in Geometric Issues in the Foundations of Science, S. Huggett, L. Mason,

K. Tod,S. Tsou, and N. Woodhouse, Eds. Oxford University Press, July 1997.

[7] W. Tichy, "Is quantum computing for real?: An interview with catherine mcgeoch of d-wave systems," Ubiquity, vol. 2017, no. July, pp. 2:1–2:20, Jul. 2017. [Online].

[8] M. Soeken, T. Ha¨ner, and M. Roetteler, "Programming quantum com- puters using design automation," arXiv preprint arXiv:1803.01022, 2018.

[9] S. Bone and M. Castro, "A Brief History of

Quantum Computing," Surveys and Presentations in Information Systems Engineering (SUR- PRISE), vol. 4, no. 3, pp. 20– 45, 1997.

[10] Bennett. C. H. and Brassard. G. (1984), Quantum Cryptography: Public Key Distribution and Coin Tossing, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, December 1984, pp. 175--179.

[11] Bennett. C. H. (1992), Quantum cryptography using any two non- Orthogonal States, Physical Review Letters, 68, pp 3121–-3124.

[12] Bennett, C. H., Bernstein, E., Brassard, G., Vazirani, U. (1997), Strengths and weaknesses of quantum computing, SIAM journal on Computing, 26(5), 1510-1523.

[13] Leuenberger, M. N., Loss, D. (2001), Quantum computing in molecular magnets, Nature, 410(6830), 789.

[14] Yang. Ching-Nung and Kuo. Chen-Chin (2002), Enhanced Quantum Key Distribution Protocols Using BB84 and B92, Proceedings of the 2002 International Computer Symposium, pp. 951-- 959.

[15] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin (2004). Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, Physical Review Letters. 92 (5): 057901.

[16] Y. Zhao, B. Qi, X. Ma, H. Lo. L. Qian (2006), Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber, ISIT, Seattle, USA, July 2006.

[17] Houshmand. M. and Hosseini-Khayat. S. (2011), An Entanglement- base Quantum Key Distribution Protocol, Information Security and cryptology (ISCISC), 8th International ISC Conference, IEEE, pp. 45--48.

[18] Cabello Adan, Quantum key distribution in the Holevo limit, https://arxiv.org/abs/quant-ph/0007064v4

[19] Farnaz Zamani, P. K. Verma (2011), A QKD Protocol with a Two-way Quantum Channel, Advanced Networks and Telecommunication systems (ANTS), 5th International Conference IEEE, pp 1-6.

[20] R. D. Sharma, A. De (2012), A New Secure Model for Quantum Key Distribution Protocol, Industrial and Information system (ICIIS), 6th IEEE International Conference, pp 462-466.

[21] M. Razavi (2012), Multiple-Access Quantum Key Distribution Networks, IEEE Transactions on Communication, vol. 60, no. 10.

[22] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah (2013), Quantum Key Distribution by Using Public Key Algorithm (RSA), London, United Kingdom: third International Conference on Innovative Computing Technology (INTECH), IEEE.

[23] Abdulrahman Aldhaheri, Khaled Elleithy, Majid Alshammari, Hussam (2014), A Novel Secure Quantum Key Distribution Algorithm, University of Bridgeport.

[24] Gueddana. A., and Lakshminarayanan. V. (2018), Physical Feasibility of QKD based on Probabilistic Quantum Circuits, IET Information Security, Volume 12, Issue 6, November 2018, pp. 521–-526.

[25] Davide Rusca, Alberto Boaron, Marcos Curty, Anthony Martin, and Hugo Zbinden (2018), Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol, Physical Review A, 98.5:052336.

[26] Davide Bacco, Ilaria Vagniluca, Beatrice Da Lio, Nicola Biagi, Adriano Della Frera, Davide Calonico, Costanza Toninelli, Francesco S. Cataliotti, Marco Bellini, Leif K. Oxenløwe, Alessandro Zavatta (2019), Field trial of a three- state quantum key distribution scheme in the Florence metropolitan area, EPJ Quantum Technology 6.1: 5.

[27] Huawang. Q., Tso. R., Dai. Y. (2019), Quantum Secret Sharing by using Fourier Transform on Orbital Angular Momentum, IET Information Security, (Volume 13, Issue 2, March 2019), pp. 104-–108.

[28] Alasdair B. Price, John G. Rarity, Chris Erven (2020), A quantum key distribution protocol for rapid denial of service detection, EPJ Quantum Technology.

[29] Bennett, CH, Bessette, F, Brassard, G, Salvail, L & Smolin, J 1992, 'Experimental quantum cryptography', Journal of Cryptology, vol. 5(1), pp. 3-28.

[30] Bennett, CH, Brassard, G, Crepeau, C & Maurer, UM 1995, 'Generalized privacy amplification', IEEE Trans. Inf. Theory, vol. 41, no. 6, pt. 2, pp. 1915–1923.60km Telecom

Fiber, ISIT, Seattle, USA, July 2006.

[31] Wegman, MN & Carter, JL 1979, 'Universal classes of hash functions', J. Comput. Syst. Sci., vol. 18, pp. 143–154.

[32] J. Buchmann, C. Coronado, M. D¨oring, D. Engelbert, C. Ludwig, R. Overbeck, A. Schmidt,

U. Vollmer, and R.-P. Weinmann. Post-quantum signatures. Cryptology ePrint Archive, Report 2004/297, 2004.

[33] R. C. Merkle and M. E. Hellman. Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory, 24(5):525–530, Sept. 1978.

[34] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In Advances in Cryptology: Proceedings of CRYPTO '82, pages 279–288, 1982.

[35] B. Chor and R. L. Rivest. A knapsack type public key cryptosystem based on arithmetic in finite fields. IEEE Transactions on Information Theory, 34(5):901–909, Sept. 1988.

[36] C.-P. Schnorr and H. H. H¨orner. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In Advances in Cryptology – EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, pages 1–12, 1995.

[37] N. T. Courtois, L. Goubin, and J. Patarin. SFLASHv3, a fast asymmetric signature scheme. Cryptology ePrint Archive, Report 2003/211, 2003.

[38] V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical cryptanalysis of SFLASH. In Advances in Cryptology – CRYPTO 2007, 27th Annual International Cryptology Conference, pages 1–12, 2007.