ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 9, September 2020

A STUDY ON QUANTUM CRYPTOGRAPHY AND COMPUTATION

[1] Adithya Harish S M, [2] Priyadharshini G
[1][2] UG ScholarDepartment of Information Technology, PSG College of Technology, Coimbatore
1adithyaharish10@gmail.com,2priyadharshini6508@gmail

Abstract: The quest for reduced complexityand increased computing efficiency remains unsolved with present classical computers. Classical computers deal with problems whose complexity increase linearly. Most real-life problems have the complexity growing exponentially with the number of inputs rather than linearly. This poses a fundamental problem in our current computers. To achieve the pinnacle of speed, we require the necessity of quantum computers. Currently, there exist some algorithms utilizing the better side of quantum computers. For example, Shor's algorithm performs factoring of a large integer in Polynomial time, whereas classical factoring algorithms can do it in exponential time. On the other hand, cryptosystems such as RSA are no more secure with the era of quantum computers. In this paper we briefly survey the basic knowledge of quantum computers, quantum cryptography and the underlying algorithms and the application.

Keywords—Quantum cryptography, Exponential problems, Quantum public key distribution, RSA algorithm

I. INTRODUCTION

Despite providing us with the most spectacular wave of technological innovation in human history, there are still certain computational problems that the digital computers can't seem to unravel. Some key scientific breakthroughs and even the worldwide global economy is held back by these problems. Although conventional computers have been doubling in power and processing speed nearly every two years for decades, they still don't seem to be getting any closer to solve these persistent problems.Any computer scientist will probably give the same answer: The digital, conventional computers we use today are built on a classical, and very limited, model of computing. In the long run, to efficiently solve the world's most persistent computing problems, we are going to have to turn to an entirely new and more capable solution with quantum computers[4].

In 1981, the Nobel laureate Richard Feynman said that if one wants to make a simulation of Nature, it should be made quantum mechanical, because it doesn't look so easy. This idea opened door for the discovery of quantum computers using the quantum mechanical phenomena

Large numbers are not a cakewalk to factor even for the best computers in the world today. In fact, the required time for factoring large numbers is the basis for much of our present-day cryptography. It is based on mathematical problems that are too tough to solve. RSA encryption, the method used to encrypt the credit card number while shopping online, relies completely on the factoring problem. The website you use for purchasing gives you a large "public" key (which anyone can access) to encode your credit card information. But what if the factoring problem can be broken. It means an end to security and privacy. And that's what a quantum computer running shor's algorithm can do.

The rest of the paper is organized as follows: Background knowledge is covered in section 2,an overview of quantum is discussed in section 3, while section 4 concludes the paper with futures works overseen.

2. BACKGROUND KNOWLEDGE

This section questions the need quantum computers when we already have very efficient classical computers. It also deals with thefundamental ideason which quantum computes rely.

2.1 WHY QUANTUM COMPUTERS?

It is a riddle to achieve maximum efficiency in a classical computer. According to Moore's law, if the performance keeps improving by means of technological innovations, which has occurred over the previous couple of decades, the number of transistors per chip may be doubled every 18 months. Furthermore, processor clock frequency could reach the maximum amount as 40 GHz within 10 years [1]. By then, a single atom may represent one bit [1]. One of the possible problems could also be that, because electrons aren't described by classical physics but by quantum physics, quantum physical phenomenon may cause "tunneling" to occur on a chip. In such cases, electrons could leak from circuits. Taking under consideration the quantum mechanical characteristics of the one-atom-per bit level, quantum computers are proposed together thanks to effectively affect this predicament. In this way, quantum computers are often wont to solve certain computationally intense problems where classical computers require large amounts of time interval. Notwithstanding, further improvements are going to be necessary to make sure quantum computer's proper performance in future, but such improvements seem obtainable.

At present, there exist some algorithms making better use of quantum computers. For instance, the Polynomial-time algorithm for factoring a large integer with O(n3) time was proposed by Peter Shor [2]. This algorithm performs factoring exponentially faster than classical computers. This algorithm could factor a 512-bit product in about 3.5 hours with 1 GHz clock rate, whereas the classical computer could factor an equivalent product in 8400 MIPS years. (One MIPS year is the number of instructions that a processor can execute in a year, at the rate of millions of instructions per second.)

Table 1. Comparison of classical vs quantum computers

Classical computer	Quantum computer
Factor 193 digits using a 2.2 GHZ machine: 30 CPU years	Factor 193 digits using a 2.2 GHZ machine: 0.01 seconds
Factor 232 digits using a 2.2 GHZ machine: 2000 CPU years*	No estimates available
Factor 500 digits using a 2.2 GHZ machine: 10^2 CPU years	Factor 193 digits using a 2.2 GHZ machine: 2 seconds

*Largest number currently factorable; special hardware using a distributed system of computers

2.2 DOMAIN

We experience the advantages of classical computing each day. However, there are challenges that today's systems will never be ready to solve. For problems exceeding a particular size and complexity, we don't have enough computational power on Earth to tackle them. To stand an opportunity at solving a number of these problems, we'd like a replacementquite computing.

Universal quantum computers leverage the quantum mechanical phenomena of superposition and entanglement to make states that scale exponentially with number of qubits, or quantum bits.

Let's consider '2' bit system whose possible combination of '2' bit data system {(00)(01)(10)(11)} contain '4' possible states. Here, a '2' bit classic computer can at most simultaneously perform '1' of these '4' possible function. In order to see all of them, the pc would wish to repeat function separately. Whereas due to phenomenon of superposition a '2' quantum bit quantum computer is able to analyse all of the operation at a time. '2' quantum bit system contains information about 4 states. Then a machine with 'n' quantum bit systemcontains information about 2n states simultaneously. Hence, the storage, computation and analysis increase with increase in data. Quantum Computing entirely depends upon the rule and property of quantum physics to unravel the matter.

All computing systems believe a fundamental ability to store and manipulate information. Classical computers work with bits (0 and 1). Quantum computers on the other hand, work with Q-bits (0 and 1 at the same time). Classical computers are based on classical phenomena. Quantum computers are supported quantum phenomena like superposition, entanglement. In conventional computers, data processing is done in Central Processing Unit or CPU, which consists of Arithmetic and Logic Unit

(ALU), processor registers and a control unit. In quantum computers, processing is completed in Quantum Processing Unit or QPU, which consists of variety of interconnected qubits.

3. TYPES OF CRYPTOGRAPHY

In symmetric cryptography, the sender and the receiver use the identical secret key and also the same cryptographic algorithm to encrypt and decrypt data. as an example, Alice can encrypt a plain text message using her shared secret key and Bob can decryptthe message using the identical cryptographic algorithm Alice used and alsoshared the same secret key. The key must be kept secret, meaning that only Alice and Bob should know it; therefore, an efficient way for exchanging secret keys over public networks is demanded[10].
Asymmetric cryptography or public key cryptography (PKC) where the keys are available pairs. Each party should have its own private and public key. For example, if alice wants to encrypt a message, bob would send his public key to Alice and so Alice can encrypt the message with bob's public key. Next, Alice would transmit the encrypted message to bob who is in a position to decrypt the message along with his private key. Thus, we encrypt the message with a public key and only the one who owns the private key can decrypt the message.

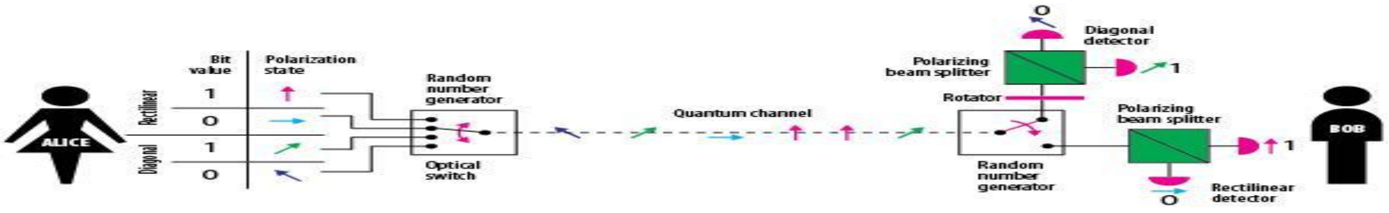
3.1 QUANTUM CRYPTOGRAPHY

This section says how quantum computers can act as a threat to the current cryptographic techniques and how this problem can be overcome by using quantum cryptography and public key distribution.

3.2 AS A THREAT

Recent research in the field of quantum computing has proved that some problems that are considered difficult or impossible to solve using conventional computation platforms become fairly trivial for a quantum computer. Any information that has been encrypted, or will be encrypted using manyof the industry's state-of-the-artcryptosystems based on computational-hardness is now under threat of both eavesdropping and attack by future adversaries who have access to quantum computers[9].
This means that even encrypted information sitting in a database for some 20 years, will be subjected to opensource by those with access to quantum computing platforms. The discovery of the content of such data could lead to very serious consequences. These include the misuse of bank account numbers, identity information, items relating to military security and other sensitive information. Without safe encryption against quantum, everything that has been transmitted, or will ever be transmitted, over any network is vulnerable to eavesdropping.
Quantum computers can be a major threat to the current encryption techniques that we use to secure the data and passwords as they can factor very large numbers potentially. It is true that if we had a large powerful enough system right now, we could factor very large numbers. But to get there you'd need a system probably in the thousands of qubits, or even millions. Those would have to be very robust, very error-free qubits, which we don't have today. We have at least 10 years, if not 15 or 20, before we have a system large enough to do that. No immediate concern there.

3.3 QUANTUM PUBLIC KEY DISTRIBUTION



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	✛ Rect	✕ Diag	✕ Diag	✛ Rect	✕ Diag	✕ Diag	✕ Diag	✕ Diag
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB's shared sifted key	—	1	—	1	—	1	0	—

Intraditional public-key cryptography, trapdoor functions are used to conceal the meaning of messages between two users from a passive eavesdropper,

Despite the lack of any initial shared secret information between the two users. In quantum public key distribution, the quantum channel is used to transmit a supply of random bits between two users rather than directly sending meaningful messages. The users share no secret information initially, and by subsequent consultation over an ordinary non-quantum channel which is subjected to passive eavesdropping, can tell with high accuracy whether the original quantum transmission has been disturbed in the transmission. (it is the quantum channel's peculiar virtue to compel eaves-dropping to be active). If the transmission has not been disturbed, they agree to use these shared secret bits in the well-known way as a one-time pad (OTP)

to conceal the meaning of subsequent meaningful communications, or for other cryptographic applications (e.g. authentication tags) requiring shared secret random information. If transmission has been disturbed, they

discard it and try again,deferring any meaningful communications until they have succeeded in transmitting enough random bits through the quantum channel to serve as a one-time pad. Figure 1 describes the working of public key distribution[10].

The QKD sender transmits photons, one at a time to the receiving unit. A quantum property like polarization, phase or position is applied to each photon to designate whether that photon represents a one or a zero.

Because of its nature at this quantum level, the photons can be sent in a state where they represent both one and zero simultaneously called the superposition state. It's only when the photon is observed or measured that it settles into one of the fixed states.

If a third party intercepts the key transmission and tries to read it, he won't be able to re-transmit it to the intended receiver in exactly the same state that it was initially sent in. If he tries, the receiver will get a meaningless data and it's apparent that someone is tapping the line.

3.4 RSA ALGORITHM:

RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key[8]. The keys for the RSA algorithm 'M' are generated the following way:

1. Choosetwo different large random prime numbers P and Q. Let 'M' be the secret key.

2. Calculate n=P*Q

3.2.1 n is the modulus for the public key and the private keys

i) Calculate the totient:
F(N) = (P-1)*(Q-1)

ii) Choose an integer 'e' such that
1 < e<F(N) and e is coprime to F(N)

(N), i.e.: e and F (N) share no factors other than 1; gcd (e,F (n)) = 1

➢ e is released as the public key exponent

5. Compute 'dtosatisfy

the congruence relation i.e.: d*e=1 mod(F (N)) for some integer x.

[1] d is kept as the private key exponent

ENCRYPTING MESSAGE:

c = M^e mod n

DECRYPTING MESSAGE:

Alice can recover M from e by using her private key d in the following procedure:

M = c^d mod n

BOB	**ATTACK**	**ALICE**
P, Q: Prime numbers	**(N) -------------**	**M: secret**

N=P x Q	□	**N**
F(N) = (P-1) (Q-1)		
1 < e <F(N)	**(e)**	
		e
GCD (e, F(N)) =1		

	□	**C=M^e**
C		
		mod N
(Bob needs d)		
	□------------ -	
d. e mod(F(N)) =1		
M=C^d mod N		
Bob got the key!		

3.4.1 EXAMPLE:

Alice wants to send a secret key to Bob.
Table 2. Illustration of RSA algorithm

Say the key is M=123. Bob choses two random prime numbers say p=53 and Q=61

and compute n = p*q (The parameters usedhere are artificially small).

So, n = 53*61= 3233.

He then computes the totient,

F (n) = (p-1) * (q-1) = 3120 and chooses esuch that 1<e<F (n) and e is coprime to 3120. So, e=17.

Bob sends the value of n and e to alice. Even if an attacker oversees it, he would not be able to find p and q with n being known. This is because conventional computers take thousands of years to find prime factors of a large number.

Alice then computes value of C using formula, **c= M^e mod n** and sends it to Bob. **c=855** Bob computes his secret key d by applying

d*e=1 mod (F (N)) i.e. (d multiplied by e and applying its modulus over F (n) should give 1)

d=2753

Finally, M is found using **M= c^{d}mod n= 123**

During the process, an eavesdropper can track value of n and e, but it would turn out to be of no use.

3.4.2 PROBLEM WITH RSA PROTOCOL:

RSA algorithm (named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) is the most widely used public key encryption protocol at the moment. RSA algorithm is a public key encryption scheme. That is, the encryption key is known to public, while the decryption key is known only to the intended receiver. Its security relies on the fact that of factoring large numbers is highly complex. As of today, there is no conventional computer with a code-breaking algorithm that can prime factor large numbers with polynomial time. Breaking an RSA-encrypted message with current conventional computerswill take an enormous time.

RSA protocol has notable limits. First, unconventional computers, most likely the quantum computers, may break it efficiently with the discovery of Shor's algorithm[8].

It is shown that with a quantum computer, large numbers can be factored with polynomial complexity. Shor's algorithm was experimentally demonstrated in 2001 [5] Second, even with a conventional computer, although an efficient code-breaking algorithm has not been reported yet, it doesn't mean that such an algorithm does not exist. Third, the hardware of conventional computers has been developing very fast and is expected to continue this trend according to Moore's law [6]. Due to the above three threats, the RSA algorithm may not be able to provide future security for certainapplications that require long-term information confidentiality. However, by implementing quantum phenomena in RSA algorithm, we can arrive at security system that is not breakable even by Shor's algorithm. This can be applied to the public key or the private key or to the two prime numbers or to the 'c' value.

CONCLUSION AND FUTURE OF QUANTUM COMPUTERS:

Quantum computers could spur the development of new breakthroughs in all aspects of life. Examples are science, medications to save lives, machine learning methods to diagnose illnesses sooner, materials to make more efficient devices and structures, financial strategies to live well in retirement, and algorithms to quickly direct resources such as ambulances.

We don't have the key to expose the whole quantum mystery yet. It is highly possible that nature sealed the door and isnot accessible from outside. So, our focus is to develop a mathematical model for the superposition and use it to develop a quantum computer and we are not doing it in blind faith. The future is not foreseen yet, but it is definitely promising.

AKNOWLEDGEMENT

We would like to express our deep gratitude to Dr. Anitha Kumari and Mrs.Shyamala Gowri, Professor, Department of Information Technology, PSG College of Technology for their valuable support and encouragement throughout the study.

REFERENCES

[1]C.P. Williams & S.H. Clearwater, "Exploration in quantum computing", *NewYork: Springer-Verlag, 1997*).

[2]P.W. Shor, Algorithm for quantum computation: Discrete logarithm and factoring, Proc. 35th IEEE Annual Symp. On Foundations of Computer Science, Santa Fe, NM, November 1994, 24–134.

[3]W.H. Zurek, "Decoherence and transition from quantum to classical", *Physics Today,October 1991.*

[4]Online:https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing

[5]Online:https://medium.com/@jonathan_hui/qc-what-are-qubits-in-quantum-computing-cdb3cb566595

[6]Online:https://venturebeat.com/2019/07/14/ibm-research-explains-how-quantum-computing-works-and-could-be-the-the-supercomputer-of-the-future

[7]Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: public key distribution and coin tossing." *Theor. Comput. Sci.* 560, no. 12 (2014): 7-11.

[8]Sarthak R Patel, Khushbu Shah, Gaurav R Patel, "Study on Improvements in RSA Algorithm", *International journal ofengineering Development and Research.*

[9]Zhao, Yi. "Quantum cryptography in real-life applications: assumptions and security". *University of Toronto, 2009.*

[10]Mavroeidis, Vasileios, Kamer Vishi, Mateusz D. Zych, and AudunJøsang. "The impact of quantum computing on present cryptography." *arXiv preprint arXiv:1804.00200* (2018)