IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOGRAPHY IN QUANTUM COMPUTING

[1]Name Kashmira Avinash Patil

[1]Designation of 1st Author:Student

Bharti Vidyapeeth Institute of Management and Information Technology,Navi Mumbai,India

Abstract: Quantum cryptography is based on using photons and theirfundamental Quantum properties develop an indestructible cryptosystem because it is not possible to measure the quantum state of any system without alarming the system. Classical cryptography is built upon classical information theory and the Turing model of computation. The development of Quantum information theory and computing amounts to a paradigm shift. In many respects, Quantum information processing is radically different from classical information processing. A Quantum computer with hundreds or thousands of qubits is needed to solve problems beyond the capability of conventional computers, and it is not known when such a computer might be built. Identifying new cryptanalytic improvements that make use of Quantum algorithms and expanding the applicability is known cryptanalytic attacks by means of Quantum technology

Keywords:Cryptographic, Qubits, Quantum Circuit, Quantum Key Exchange, Advanced Encryption Standard, Artificial Intelligence, Quantum algorithms.

I. INTRODUCTION

Quantum computing is based on a sequence of unitary operations acting on the wave function or the density matrix ρ for a number of Quantum spins or qubits. Computers these days offer all types of services for us. Having and using computers ease up so many tasks in our lives. But computers also have a risk of security with every each task that they perform .Quantum computations are inherently probabilistic. Quantum operations or gates can be performed by using spins or classical bits, within a classical statistical setting. Classical systems realizing Quantum computing have to be truly probabilistic. e practical realization of the unitary transformations needed for Quantum gates. It is not the purpose of this work to challenge the high potential of Quantum computations employing isolated Quantum systems.

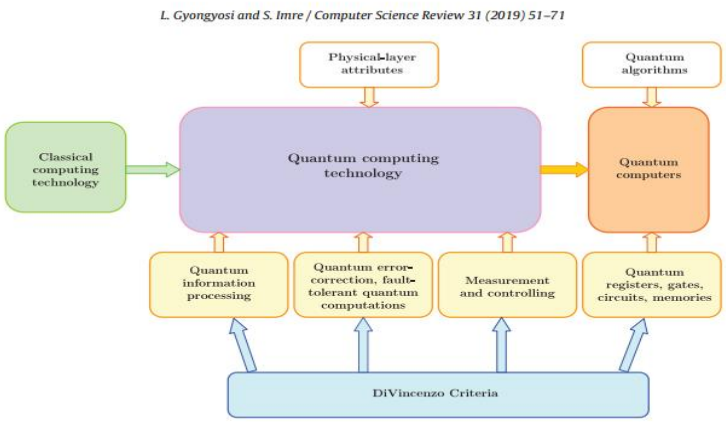

Fig. 1. The conceptual diagram of the evolution of quantum computing technology from classical computing technology. Quantum computers employ the results integrated by quantum computing technologies.

Quantum cryptography is a very interesting field that makes use of the rules of Quantum mechanics to deve lop cryptosystem that is believed to be the most secure system. Quantum cryptography is based on photons and their fundamental quantum properties to develop an fundamental Quantum properties to develop an indestructible cryptosystem because it is not possible to mea sure the Quantum state of any system without alarming the system. Quantum computing technology offers fundamentally different solutions to computational problems and enables more efficient problem-solving than what is possible with classical computations. A Quantum computer has reversible Quantum gates that perform a unitary operation on the Quantum systems. everyone knows that Quantum computers will likely be capable of breaking most forms of traditional public key encryption and digital signatures. Everything protected by RSA, Diffie-Hellman . every major application of cryptography a careful review of the impact of Quantum computing needs to be performed without delay.

III.Literature Review:

1.Quantum Algorithms:

commonly used circuit model of Quantum computation, by a Quantum circuit which acts on some input qubits and terminates with a measurement. A Quantum circuit consists of simple Quantum gates which act on at most a fixed number of qubits. The number of qubits has to be fixed because a changing number of qubits implies non-unitary evolution.

2.Simon's algorithm:

Simon's algorithm solves a black-box problem exponentially faster than any classical algorithm, including bounded-error probabilistic algorithms. This algorithm, which achieves an exponential speedup over all classical algorithms that we consider efficient, was the motivation for Shor's factoring algorithm.

3.Quantum phase estimation algorithm:

The Quantum phase estimation algorithm is used to determine the eigen phase of an eigenvector of a unitary gate given a Quantum state proportional to the eigenvector and access to the gate. The algorithm is frequently used as a subroutine in other algorithms.

2.1.Shor's algorithm:

Shor's algorithm work on the discrete logarithm problem and the integer factorization problem in polynomial time, the best known classical algorithms take super-polynomial time. These problems are not known to be in P or NP-complete. It is also one of the few Quantum algorithms that solves a non–black-box problem in polynomial time .It is known as classical algorithms run in super-polynomial time.

All current experimental activity in Quantum cryptography is in Quantum key exchange (QKE). Classical cryptography is built upon classical information theory and the Turing model of computation. Classical factoring difficulty underlies the RSA public key cryptosystem, become easy on a Quantum computer. range of specifically Quantum communication primitives that have important consequences for cryptography. the Quantum no-cloning theorem implies the existence of Quantum keys that cannot be copied, even by the key's owner. Quantum key distribution forces eavesdroppers to invest in Quantum technology, leading to a new arms race between code-breakers and codemakers. Today's computers are based on a foundation of binary digits, with data encoded as a string of bits within electronic circuitry. Each bit must be either a zero or a one; it cannot exist as both at the same time. Shor's Algorithm factor large numbers in polynomial time, in effect breaking some commonly used forms of public-key encryption.The most unusual concepts in its characteristics are described as fuzzy probabilities by a wave function.Once a particle is measured, its characteristics become fixed at specific values, effectively collapsing the particle's wave function..Factoring is the hard problem upon which robust public key cryptographic systems are based. In schemes such as the RSA algorithm, the public encryption key and the private decryption key are mathematically related, but it is computationally infeasible to calculate one from the other without knowing the underlying prime factors.

1.Determine if n is even, prime or a prime power. If so, exit.

2. Pick a random integer $x < n$ and calculate gcd(x, n). If this is not 1, then we have obtained a factor of n.

3. Quantum algorithm Pick q as the smallest power of 2 with $n\ 2 \leq q < 2n\ 2$. Find period r of x a mod n. Measurement gives us a variable c which has the property $c\ q \approx d\ r$ where $d \in N$.

4. Determine d, r via continued fraction expansion algorithm. d, r only determined if gcd(d, r) = 1 (reduced fraction).

5. If r is odd, go back to 2. If $x\ r\ 2 \equiv -1 \bmod n$ go back to 2. Otherwise the factors p, q = gcd(x r 2 ± 1, n).

6.Factorization algorithm with polynomial complexity .
7. Runs only partially on quantum computer with complexity
O (log n) 2 (log log n)(log log log n)
8.Pre- and post-processing on a classical computer .
9.Makes use of reduction of factorization problem to order-finding problem . Achieves polynomial time with efficiency of Quantum Fourier Transform.

2.1.1.How it works?

Quantum computing:

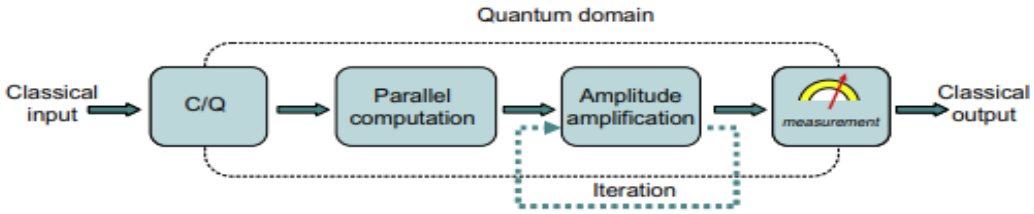

Fig. 3. General model of quantum algorithms.

signal detection on air interfaces can be regarded as optimization of function . Transmitter radiates a carefully produced signal, but the noisy radio channel disturbs it. Furthermore, other customers generate interference during their conversations. The quality of the detection in receiver can be improved significantly if he also takes signals from account instead of only focusing on sent information. This approach is called multiuser detection and poses hard computational challenges. Quantum computing is a process of manipulating Quantum mechanical systems for information processing using superposition and entanglement. Quantum computer performs calculations Quantum-mechanically using qubits, far more efficiently than foreseeable classical computer. A qubit is a special system in Quantum computing world with signal detection on air interfaces can be regarded as optimization of function . Transmitter radiates a carefully produced signal, but the noisy radio channel disturbs it. Furthermore, other customers generate interference during their conversations. The quality of the detection in receiver can be improved significantly if he also takes signals from account instead of only focusing on sent information. This approach is called multiuser detection and poses hard computational challenges. Quantum computing is a process of manipulating Quantum mechanical systems for information processing using superposition and entanglement. Quantum computer performs calculations Quantum-mechanically using qubits, far more efficiently than foreseeable classical computer. A qubit is a special system in Quantum computing world with two degrees of freedom and state of a Quantum system is represented using qubits with 0 and 1 in the superposition. A Quantum computer operates on qubits using Quantum gates , represented by a matrix that is applied to a state vector of the qubit. Any information out of a Quantum system is extracted using physical measurement on the qubits. A Quantum computer operates on qubits using Quantum gates , represented by a matrix that is applied to a state vector of the qubit. All the Quantum operations are reversible and hence always given by unitary matrix Quantum circuit is a sequence of operations in the form of gates on a Quantum system.The unitary operation transforms the qubit state to a different desired state.

Quantum Domain:

Number of domain-wall excitations created for different quench parameters, in a regime that is difficult to model with classical computers. This work demonstrates the capability of Quantum simulators for investigating high-energy physics phenomena, such as quark collision and string breaking.

Cryptanalysis:

Quantum computers, which are still in the early phases of research, have potential use in cryptanalysis. For example, Shor's Algorithm could factor large numbers in polynomial time, in effect breaking some commonly used forms of public-key encryption.

Quantum Cryptanalytic Progress: Identifying new cryptanalytic improvements that make use of Quantum algorithms and expanding the applicability is known cryptanalytic attacks by means of Quantum technology. Different Quantum attack models can be considered here, and attack models that are close to being realizable with today's technology are particularly relevant. We want to fully leverage Quantum computing, including expected mid-term advancements.

Quantum Resource Estimation: Establishing reasonably precise Quantum resource counts for cryptanalytic attacks against symmetric and asymmetric schemes, especially for problem instances and parameter choices that are actually deployed or considered for standardization for future deployment.

2.3.Challenges:

Any practical implementation of Shor's algorithm is years away. To date, seven qubit Quantum computers have been constructed. It may be more than a decade before a 20- or 30-qubit Quantum computer is built. A Quantum computer with hundreds or thousands of qubits is needed to solve problems beyond the capability of conventional computers, and it is not known when such a computer might be built.

Any interaction between a quantum system and the external environment results in unintentional measurements that corrupt the quantum states and makes further Quantum calculation impossible. Quantum Key Distribution or QKD is being put forward as a secure mechanism to tackle the issue of security by helping users encrypt data while also enabling them to share that with a limited number of resources. So not only can messages/data is secure but also distributed among personnel thus helping with secure distribution.

2.4.Problems in Quantum Computation:

- ***Decoherence***

Decoherence leads to errors in Quantum computational systems where information is lost.It gives qubits more computational power because theoretically as extra qubits are added to a system, it doubles the amount of parallel operations that can be done.

- ***Error Correction***

a noisy error corrupts the three-bit state so that one bit is equal to zero but the other two are equal to one. If we assume that noisy errors are independent and occur with some probability *p*, it is most likely that the error is a single-bit error and the transmitted message is three ones.

- ***Output observance***

Retrieving output data after a Quantum calculation is complete risks corrupting the data. Developments have since been made, such as a database search algorithm that relies on the special wave shape of the probability curve in Quantum computers.

III.Conclusion:

Shor's algorithm work on the discrete logarithm problem and the integer factorization problem in polynomial time. in effect breaking some commonly used forms of public-key encryption. Quantum computing is based on a sequence of unitary operations acting on the wave function or the density matrix ρ for a number of Quantum spins or qubits. While the technology already influences the above-mentioned fields and the Quantum computing benefits and applications go on, the list is by no means complete and that is the most amazing part. As with all new technologies, applications that are currently unimaginable will be there as the hardware keeps evolving and creating new opportunities. Shor's algorithm is very important for cryptography, as it can factor large numbers much faster than classical algorithms (polynomial instead of exponential) . powerful motivator for quantum computers . no practical use yet, as it is not possible yet to design quantum computers that are large enough to factor big numbers2011).Six month T-bills rate is used as proxy of interest rate. As investors arevery sensitive about profit and where the signals turn into red they definitely sell the shares. And this sensitivity of the investors towards profit effects the relationship of the stock prices and interest rate, so the more volatility will be there in the market if the behaviors of the investors are more sensitive. Plethora (2002)has tested interest rate sensitivity to stock market returns, and concluded an inverse relationship between interest rate and stock returns. Nguyen (2010) studies Thailand market and found thatInterest rate has aninverse relationship with stock prices.

Iv.References

[1]https://www.quora.com/How-much-does-a-quantum-computer-cost
[2]https://en.wikipedia.org/wiki/Quantum_error_correction
[3]https://ca.search.yahoo.com/search?fr=mcafee&type=E211CA826G91504&p=conlusion+of+quantum+computing
[4]https://ca.search.yahoo.com/search?fr=mcafee&type=E211CA826G91504&p=science+direct
[5]https://ca.search.yahoo.com/search?fr=mcafee&type=E211CA826G91504&p=sci+hub
[6]Quantum Cryptography for Internet of Things Security Alekha Parimal Bhatt | Anand Sharma*
[7]Quantum computing with classical bits C. Wetterich
[8]Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave quantum computer Feng Hu a,b, Lucas Lamata c,d, Mikel Sanz d, Xi Chen d,e, Xingyuan Chen f , Chao Wang a,b,g, Enrique Solano d,h,
[9]Promise From the Future — Quantum Cryptography Interview with Dr. Hoi Kwong Lo Senior Vice President MagiQ Technologies.
[10]The Impact of Quantum Computing on Cryptography Marie A.Wright
[11]Some trends in research in cryptography and security mechanisms Fred Piper.
[12]Quantum computing's impact on security The Sandbox Roger A Grimes, KnowBe4
[13]A Survey on quantum computing technology☆,☆☆ Laszlo Gyongyosi a,b,c,∗ , Sandor Imre b
[14]Quantum computing and communications – Introduction and challenges q Sándor Imre
[15]Is quantum computing becoming relevant to cyber-security? Keegan Keplinger Keegan Keplinger, eSentire
[16]The impact of quantum computing on real-world security: A 5G case study Chris J. Mitchell
[17]Training an Artificial Neural Network Using Qubits as Artificial Neurons: A Quantum Computing Approach Avinash Chalumuria , Raghavendra Kuneb, B. S. Manoj.
[18]Quantum computing and supervised
[19]machine learning: Training, model selection, and error estimation L. Oneto, S. Ridella, D. Anguita.
[20]Google Takes a Big Step Toward Quantum Computing Chris Palmer Senior Technology Writer
[21]https://qudev.phys.ethz.ch/static/content/QSIT15/Shors%20Algorithm.pdf
[22]Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM journal on computing 26.5 (1997): 1484-1509.