Quantum and Lattices

S. I. Anyanwu
Fed. Univ. of Tech., Akure,
Dept. of Computer Science,
Ondo State.

B. K. Alese
Fed. Univ. of Tech., Akure,
Dept. of Computer Science,
Ondo State.

O. O. Obe
Fed. Univ. of Tech., Akure,
Dept. of Computer Science,
Ondo State.

ABSTRACT
This research work considers the properties of quantum computer and lattices and their relationship in cryptography.

General Terms
Quantum, Lattice

Keywords
Quantum, Lattice, Quantum Computers

1. INTRODUCTION
In this digital age and with the ever increasing machines processing power, the best thing to do is to create quantum computers. Quantum computer (QC) is a computer that makes use of quantum physics to perform operations on data. Quantum computer has a lot of benefits over the classical computer as it makes use of the power of atoms and molecules operations. A quantum refers to a specified quantity of an entity. In physics, it can be defined as the smallest amount of any physical entity that can exist independently.

Recent field of study now combine quantum and lattice for various results. Lattice has to do with a set points, particles or objects. Lattice has several definitions as it has made its roots in different fields. It can be defined in mathematics as a partially ordered set in which every subset containing elements has a greatest lower bound or intersection and a least upper bound.

2. PROPERTIES OF QUANTUM COMPUTER
Superposition: A qubit can exist not just in one state or another but in a superposition of different states. QC with 500 qubits gives 2^{500} superposition states. Each state would be classically equivalent to a single list of 500 1's and 0's. Such computer could operate on 2^{500} states simultaneously. According to [1], observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. This kind of computer is equivalent to a classical computer with approximately 10^{150} processors.

Entanglement: This ties qubits inextricably to each other over the course of operations. According to [2], the fact that entanglement implies a tensor product rather than Cartesian product means that a system of multiple qubits has a state space that grows exponentially in the number of qubits.

Memory: The memory of a classical computer is a string of 0s and 1s, and it can perform calculations on only one set of numbers simultaneously. The memory of a quantum computer is a quantum state that can be a superposition of different numbers.

Reversible: All operations are reversible since reversible quantum gates exist that permit the full complement of familiar logical operations. [2] stated that on one level, this is due to the fact that classical computations dissipate heat, and with it information, whereas quantum operations dissipate no heat and therefore retain all information across each calculation.

2.2 Cryptographic Benefits
Artificial Intelligence: Increasing the speed of operation will help computers to learn faster even using the one of the simplest methods – mistake bound model for learning.

Operations: QC is much faster and consequently will perform a large amount of operations in a very short period of time. According to [3], performing a computation on many different numbers at the same time and then interfering all the results to get a single answer, makes a quantum computer much powerful than a classical one.

High performance: High performance according to [1] will allow for the development of complex compression algorithms, voice and image recognition, molecular simulations and true randomness (randomness is important in simulations). Molecular simulations are important for developing simulation applications for chemistry and biology.

Quantum communication: With the help of quantum communication both the receiver and sender are alerted when an eavesdropper tries to catch the signal. Quantum bits also allow more information to be communicated per bit. QCs make communication more secure.

3. LATTICE
3.1 Properties of Lattice
Properties of lattice that lead to interesting special classes of lattices [4].

Bounded lattice: A bounded lattice is an algebraic structure of the form $(L, \vee, \wedge, 1, 0)$ such that $(L, \vee, \wedge)$ is a lattice, 0 (the lattice's bottom) is the identity element for the join operation $\vee$, and 1 (the lattice's top) is the identity element for the meet operation $\wedge$.

Completeness: A poset is called a complete lattice if all its subsets have both a join and a meet. In particular, every complete lattice is a bounded lattice. While bounded lattice homomorphisms in general preserve only finite joins and meets, complete lattice homomorphisms are required to preserve arbitrary joins and meets.

A conditionally complete lattice is a poset in which every nonempty subset that has an upper bound has a join (i.e., a least upper bound). Such lattices provide the most direct generalization of the completeness axiom of the real numbers. A conditionally complete lattice is either a complete lattice, or a complete lattice without its maximum element 1, its minimum element 0, or both.

Distributivity: Since lattices come with two binary operations, it is natural to ask whether one of them distributes over the other, i.e. whether one or the other of the following dual laws holds for any three elements a, b, c of L:

Distributivity of ∨ over ∧: a∨(b∧c) = (a∨b) ∧ (a∨c).

Distributivity of ∧ over ∨: a∧(b∨c) = (a∧b) ∨ (a∧c).

A lattice that satisfies the first or, equivalently (as it turns out), the second axiom, is called a distributive lattice.

Modularity: For some applications the distributivity condition is too strong, and the following weaker property is often useful. A lattice (L, ∨, ∧) is modular if, for all elements a, b, c of L, the following identity holds.

Modular identity

$$(a \wedge c) \vee (b \wedge c) = [(a \wedge c) \vee b] \wedge c$$

This condition is equivalent to the following axiom.

Modular law: $a \leq c$ implies $a \vee (b \wedge c) = (a \vee b) \wedge c$

Besides distributive lattices, examples of modular lattices are the lattice of sub-modules of a module, and the lattice of normal subgroups of a group.

3.2 Cryptographic Benefits

Lattice is used for cryptography for a number of reasons such as [5]:

a) Simple and efficient: linear, parallelizable
b) Resists sub-exponential & quantum attacks (so far)
c) Security from worst-case assumptions
d) Lattice problems offer the possibility of faster encryption and decryption algorithms.

4. RELATIONSHIP OF QC AND LATTICE

Lattice-based cryptography: The field of lattice-based cryptography has been developed based on the assumption that lattice problems are hard but up till date, there are no known quantum algorithms for solving lattice problems that perform significantly better than the best known classical algorithms. This is despite the fact as stated by [6] that lattice problems seem like a natural candidate to attempt to solve using quantum algorithms since they are believed not to be NP-hard for typical approximation factors, because of their periodic structure, and the Fourier transform, which is used so successfully in quantum algorithms, is tightly related to the notion of lattice duality. Since Shor's discovery of the quantum factoring algorithm in the mid-1990s attempts to solve lattice problems by quantum algorithms have been made. With the continuous advancements in the field of quantum computing, the security of many existing asymmetric key cryptosystems has been demonstrated to be broken in the theoretical sense [7].

Lattice QCD: It is a well-established non-perturbative approach to solving the quantum chromodynamics (QCD) theory of quarks and gluons. It is a lattice gauge theory formulated on a grid or lattice of points in space and time. It is important to note when the size of the lattice is taken infinitely large and its sites infinitesimally close to each other, the continuum QCD is recovered [8].

In lattice QCD, fields representing quarks are defined at lattice sites (which leads to fermion doubling), while the gluon fields are defined on the links connecting neighbouring sites. This approximation approaches continuum QCD as the spacing between lattice sites is reduced to zero. Numerical lattice QCD calculations using Monte Carlo methods can be extremely computationally intensive, requiring the use of the largest available supercomputers. To reduce the computational burden, the so-called quenched approximation can be used, in which the quark fields are treated as non-dynamic "frozen" variables.

Lattice field theory is an area of theoretical physics, specifically quantum field theory, which deals with field theories defined on a spatial or space-time lattice. In modern quantum field theory, the introduction of a space-time lattice is part of an approach different from the operator formalism. This is lattice field theory. Its main ingredients are:

- functional integrals,
- Euclidean field theory and
- The space-time discretization of fields.

Lattice field theory has turned out to be very successful for the non-perturbative calculation of physical quantities.

Superlattice is a periodic structure of layers of two (or more) materials. Typically, the thickness of one layer is several nanometers. It can also refer to a lower-dimensional structure such as an array of quantum dots or quantum wires.

5. CONCLUSION

The combination of quantum and lattices in various fields has proofed to be of greater performance among others. Yet a major obstacle in the production of a QC is decoherence that is the interaction of the quantum system with the environment, disturbing the quantum state and leading to errors in the computation. Although techniques of quantum error correction have been used successfully to combat some effects of decoherence, there is still a long way to go before building a large-scale quantum computer will be possible.

6. REFERENCE

[1] Avaliani, A. (2002). *Quantum Computers.* International University, Germany.

[2] Barreno, M. A. (2002). *The Future of Cryptography Under Quantum Computers.* Department of Computer Science, Dartmouth College, Hanover, New Hampshire, USA. Technical Report TR'02 – 425.

[3] West, J. (2000). *Quantum Computers.* http://www.cs.caltech.edu/~westside/quantum-intro.html#qc

[4] Lattice (Order) (2012). Retrieved from en.wikipedia.org/wiki/Lattice_(order).

[5] Peikert, C. (2009). *Some Recent Progress in Lattice-Based Cryptography.* In Proceedings of Theory of Cryptography Conference - TCC'09, San Francisco, CA, USA. LNCS, Vol. 5444, pp 72, Springer-Verlag.

[6] Micciancio, D. and O. Regev (2008). *Lattice-Based Cryptography.* In Post Quantum Cryptography, D. J. Bernstein; E. Dahmen (eds.), pp 147 - 191, Springer (2009).

[7] Plantard, T., M. Rose, and W. Susilo (2009). *Improvement of Lattice-Based Cryptography using CRT.* School of Computer Science and Software Engineering, University of Wollongong, Wollongong NSW, Australia.

[8] Wilson, K. (1974). "Confinement of quarks". Physical Review D 10 (8): 2445. Bibcode 1974PhRvD..10.2445W. doi:10.1103/PhysRevD.10.2445.