Paradigm Shifts in Information and Communication Technologies: Towards Quantum Computers

Kaushalesh Lal[1] and Shampa Paul[2]

Abstract

The paper delineates various paradigms and trajectories followed in information and communication technologies since the invention of first mechanical computer in 1822. The authors argue that next generation of computer could be based on quantum, a concept invented by Max Plank, a German Physicist in 1900. Computers in the new paradigm would be based on qubit rather than present day bit structure. This paradigm shift in computational technologies would not only enhance the speed of computers manifold but also allow parallel processing to a great extent. The authors demonstrate how the new technology would revolutionize the application of ICT with unprecedented security of data and information. The cloud computing could be very effective in the new ICT paradigm.

[1] Visiting Fellow, United Nations University-MERIT, Maastricht, The Netherlands; E:klal.mails@gmail.com
[2] Associate Professor, Society for Development Studies, Delhi; E:shampa.paul147@gmail.com

1. INTRODUCTION

Having invented the mechanical computer in 1822, Charles Babbage is regarded as father of the computer. Mechanical computers continued to be in use until middle of 20th century. These devices were subsequently replaced by calculators. Although Charles Babbage gave theoretical foundations (memory, arithmetic logic unit, conditional branching, and loops) in 1837, the computing devices based on his ideas came into existence in the middle of 20th century. In fact the first digital computer was invented in 1930 by John Vincent Atanasoff, an American Physicist. The first generation of computers were based on vacuum tubes technology while fifth generation (present day) computers are equipped with artificial intelligence. The other generations have been based on transistors, integrated circuits (Large Scale and Very Large Scale), and microprocessor technologies.

The digital computers have capacity to store input data, perform computations, and transfer results into transient memory of the system. Auxiliary memories (Magnetic tapes, Floppies, CD, DVD, and PD) are used to store data/information permanently. The smallest unit of memory is called ***bit.*** The name is derived from the capacity of memory to store data. A bit can store binary digit (0 or 1) hence known as bit. The single accessible unit of memory is called byte consisting of 8 bits. The earlier generation of computers were based on two-byte or 16 bit architecture. For instance the mini-computers of IBM in 1960s known as IBM-1620, was based on 16 bit architecture. The mainframe computers launched in mid-1970s (IBM 360 and 370) were based on 32 bit architecture. The larger size means more information could be stored in a single accessible unit of memory which leads to higher speed of computation. The personal computers were launched in mid-1980s and the first generation of PCs were based on 32 bit architecture. The trajectories of computational technologies have been changing by increasing the bits in a single unit of accessible memory. Presently computers are based on either 64 bit or 128 bit architecture.

During the last five decades, ICT (Information and Communication Technologies) have followed relatively a predictable path where the transistors were embedded onto silicon chips to make integrated circuits. This made the computer chips more and more powerful and devices smaller. In the near future, there is going to be a turning point in this predictable path to progress. In the coming decades, prediction of Moore's law that the number of transistors per square inch on integrated circuits would double every year since their invention would change and next generation technologies such as nanotechnologies would take centre stage.

In recent times, mathematicians and theoretical physicists have been working on new *bit* structure called quantum bit ***(qubit)***. The term is coined from Quantum Physics which is the basis of modern Physics. The quantum, invented by Max Plank, a German Physicist, is the smallest unit of energy in a matter. And quantum can exist in numerous states that are dependent on the state of matter. Scientists are working on the concept of quantum bit suggesting that smallest unit of memory could take more states rather than binary. The concept has got prominence in present day scientific literature.

The shift from vacuum tube to transistor based digital technologies may be regarded as first paradigm shift. The subsequent changes from transistors to very-very large integrated circuits may be regarded as trajectory changes in digital devices. The trajectory changes are illustrated as: transistors→ printed circuit boards → integrated circuits → very large integrated circuits → very-very large integrated circuits. Along with these trajectory changes, computer architecture also changed from 16 to 32 to 64 to 128 bit. Next paradigm shift would be caused by the modifications from bit to qubit. Quantum computing is an area of study that emphasises on developing computer technology based on the principles of quantum theory, which explains the nature and behaviour of energy (quantum) in a matter.

The development of a quantum computer would mark a leap forward in computing capabilities far greater than that from abacus to a modern day supercomputer, with performance gains in billion-fold realm and beyond. The quantum computer would gain enormous processing power through the ability to be in multiple states, and to perform tasks using all possible permutations simultaneously. Current centres of research in quantum computing include MIT, IBM, University of Oxford, and the Los Alamos National Laboratory (Department of Energy, US).

The essential elements of quantum computing originated from Argonne National Laboratory at University of Chicago in 1981 by Paul Benioff. But the general acceptance is that David Deutsch of University of Oxford provided the critical impetus for quantum computing research. In 1984, he was at a computation theory conference and began to wonder about the possibility of designing a computer that was based exclusively on quantum rules and published his breakthrough paper a few months later. With this, the race began to exploit his ideas.

Remainder of the paper is organised as follows. Second section presents the literature review while Section 3 discusses the structural change of bit configuration and its implication on speed of computers. The changes in memory configuration would have major implication of hardware architecture and system & application software and also on data security. Section 4 discusses implications on hardware and software while Section 5 delineates data and digital transaction security aspect. Finally the paper is summarised in Section 6.

2. REVIEW OF LITERATURE

The potential changes in the configuration of smallest unit of memory have drawn attention of theoretical physicists, mathematicians, and social scientists. Since the concept of new chip is still in laboratories, most of studies related to qubit computers are speculative in nature. A paper by Bhaskaran (2008) argues that a quantum computer (computer based on qubit) offers massive parallelism which derives from infinite states of a qubit. Another study by Menon and Ritwik (2014) find that quantum computers have a distinctive advantage over classical computers due to its ability to solve problems with large number of computations faster as a result the outputs are found in exponential speed. They also discuss the basics of quantum computing and the hardware on which these work upon. The study indicates that a quantum computing company called DWave with 512 qubit chipset system called DWave 2 has come out with actual working model of quantum computers.

Qubit concept is not only going to lead to paradigm shifts in computational technologies, but also has potential to lead breakthrough in auxiliary memories, i.e., storage devices. In this context a study by McAdams et al. (2017) reviewed the current state of the field of lanthanide and actinide *f*-SIMs and discusses the principal factors affecting the magnetic and quantum properties of such single-ion magnets. The authors also review the latest chemical approaches in designing *f*-SIMs with superior properties and highlight new trends in single molecule magnetism, including using *f*-SIMs as potential spin qubits for quantum computers.

Having realised the tremendous potential of quantum computers, few studies have focused on the impacts of new generation computers on various applications. In this context, Shemin and

Vipinkumar (2016) propose an e-payment method using quantum and visual cryptography and image steganography. This proposed system has the basis on two cryptographic mechanisms that provide security by preventing the payment system from hacking.

The design engineering got a big boost with the emergence of CAD/CAM during mid-1980s. The application packages were constrained by limited speed of computers and consequently many features could not be effectively incorporated leading to low functionalities. These application packages did not find much change since their emergence. Quantum computers offer a great opportunity for such computational-intensive application. A study by Horváth and Regine (2015) argue that application of ubiquitous technologies did not lead to radically new functionalities in CAD/CAM system. The authors expect that new functionalities in such application could come from new computing paradigm such as quantum computing.

3. FROM BIT TO QUBIT

The literature on computational technologies suggests that next generation of technology needs to focus on increasing the storage capacity of a bit rather than increasing number of bits in a single accessible unit of memory. The new technology is labelled as quantum technology as it is based on the concept of a quantum. The new technology would allow storing infinite digits, at least in principal, in a bit. If this can be achieved, it would lead to very rapid speed of computation and miniaturization of ICT products significantly. This would be a new paradigm of computational technologies. In a two-digit bit configuration, the electronic devices can store 2^8 (256) pieces of information in a single Byte while the storage capacity in three-digit bit configuration would be 3^8 (6561) thereby increasing the speed by more than 25 times (6561/256). The change in bit configuration would necessitate the major changes in all hardware devices as well as application and system software programmes that are discussed in the following section.

As rightly argued by Bhaskaran (2008) and Deutsch (2012), the architectures based on qubit would leads to higher speed and simultaneity in processing. Although parallel processing concept is not new, it has not been exploited to its full potential due to low speed of traditional computers based on bit structure. Quantum computers would allow n-parallel processes without much sacrificing the speed.

4. IMPLICATIONs on HARDWARE and SOFTWARE

As mentioned earlier quantum computers would necessitates not only changes in computer architecture but also in algorithm. The hardware structure includes arithmetic logic unit, central processing unit, transient memory structure, input/output devices interface, and parallel processing structures. Computers based on qubit structure would necessitate appropriate changes in all interfacing devices such as storage devises, network equipment, and only output devices. Going into too much detail of hardware changes in new generation computers would be beyond the scope of this paper.

The changes in computer architecture would necessitate appropriate modification is system software commonly referred as operating systems. The phenomenon would be much more complex than what we experienced in year 2000, popularly known as Y2K problem. Although asynchronous communication is highly unlikely to disappear, all device drivers would need to be rewritten to accommodate high computational speed. Another consequence could be increase in more buffer storage of only output devices such as printers.

Due to changes in operating systems, application software systems would also require appropriate changes. The changes in application software would depend on their dependency of use of auxiliary memory. The software systems that process large volume of data are usually designed in such a way that they use auxiliary memory rather than transient memory. Use of auxiliary memory allow systems to process data constrained by the storage devices attached with system. It is not the common practice to use computer memory (transient) for storage of entire data needed for a particular application. That constraint would not be there in qubit computers thereby increasing the computation speed manifold. It may be worth mentioning that retrieval of data from transient memory to arithmetic logic unit is many times faster than retrieval from auxiliary memory. But transient memory is limited. This aspect compelled software developers to use auxiliary memory to accommodate large volume of data at the cost of processing speed. All such application software would need to be rewritten in qubit computer paradigm.

The new paradigm would have implication of data and information management. The present day encryption and decryption techniques would change. The new techniques called quantum encryption are not prone to decryption and hence would provide strong security of data and information. These techniques are discussed in detail in the following section.

5. SECURITY of DATA and DIGITAL TRANSACTION

The quantum computers (QC) would be a major leap into the future especially in artificial intelligence and online security. QC can provide breakthrough in artificial intelligence as it would analyse large quantities of data with exponential speed required to improve the performance of computers. Regarding online security, the hackers can crack the coding in today’s system easily on the other hand QC would be able to provide online security to financial institutions using quantum encryption methods that are ultra-secure communication methods. It is important to discuss these techniques before they are applied in any application.

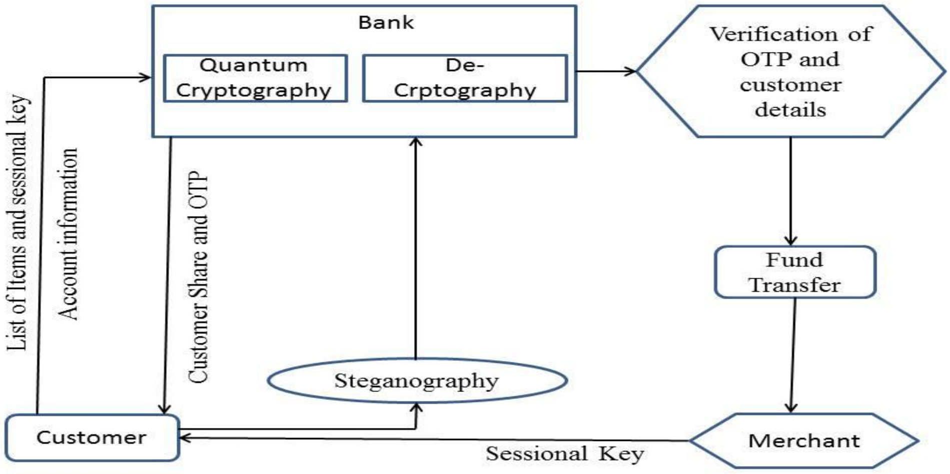
Quantum cryptography: It is a cryptographic technique based on qubit structure where quantum can be in any state rather than bit structure where it can take only two states. It is this property of qubit that prohibits eavesdropper to clone or measure it. Hence the information encrypted through quantum cryptography cannot be decrypted by hackers or any unauthorised person.

Visual cryptography: The technique is proposed by Moni Naor and Adi Shamir in 1994 (Zhou et. al., 2006). The technique encrypts images into number of meaningless pieces. And original image can be retained after combining all the pieces.

Steganography: This is the process of hiding data in another data in ways that prevents the detection of hidden data from human’s casual eye contact (Shemin and Vipinkumar, 2016). The technique requires two files for embedding hidden message in another data. The first one is cover media that holds hidden message and the other one is data to be hidden. It can be classified into text or image steganography depending on the type of cover media.

Figure 1 demonstrates how most secured e-commerce transaction can take place using quantum cryptography. As can be seen in the figure, a customer initiates the process by going to e-commerce company website and receives a transaction. The customer then searches the items to be purchased from the merchant. After that he/she sends the list of items along with bank account details to the customer bank. This information is sent to the bank using image or text steganography installed at customer computer by the bank. At the bank the information, i.e., list of items and bank details are separated by reverse steganography and account details are matched with the information available with the bank. If the verification process is successful, the bank system proceeds further.

Figure 1: Proposed e-commerce model using quantum cryptography



In the second step, using visual cryptography two shares of account information are generated. Subsequently one share of account information and one time password (OTP) are sent to the customer using steganography. At the customer end, the information is separated and OTP is displayed to the customer. The customer then sends the same OTP to the bank. The OTP does not travel to the bank as it is. Rather using visual steganography, the half share of account information and OTP by customer is sent to the bank. On receiving this visual steganography information, the OTP sent by the customer and half share of bank account image are separated at the bank. Subsequently, the bank system joins both the pieces of quantum encrypted bank account information and verify it with details of the customer's account available with bank. The bank also verifies OTP sent by the customers. If both the pieces of information match then bank makes the transaction into the merchant bank account. The advantage of the proposed system is the use of visual quantum encryption technology and image steganography. In this method of e-commerce, eavesdropper cannot decrypt bank account details of customer and OTP as the relevant data is encrypted by using quantum cryptography.

The visual cryptography used in the system, safeguards the customer's data and quantum cryptography and image steganography prevents security threats such as phishing, identity theft etc. This system could be extended to other financial sector applications.

6. SUMMARY

Since invention of first mechanical computer in 1822, the computational technologies have experienced rapid changes particularly since the emergence of digital computers in the middle of 20th century. The information technology has two main components. One, the design and components used in data processing and storage devices and second, the display devices. The first component has evolved from vacuum tube technology to very-very large integrated circuits while the display technologies changed from Cathode Ray Tubes (CRT) to Liquid Crystal Display (LCD). Although digital technologies have changed drastically for the last several decades, the structure of smallest unit of memory called bit has not changed. Therefore the evolution of digital technologies may be regarded as trajectory shifts.

In recent times, scientists, mathematicians, and science labs have focussed on the structure of bit. They argue that if the bit states can be changed from binary to many, it could lead to breakthrough in information technology. The concept is based on quantum; the smallest unit of energy is a matter. The concept of quantum was invented by Max Plank, a German Physicist, in 1900. Plank's theory suggests that a quantum can take (infinite in principal) as many states as the matter. Drawing on this idea, physicist, computer scientists, and mathematicians are working on a new bit structure called quantum bit (qubit). The computer based on qubit could be called as quantum computers. This technological breakthrough would be a paradigm shift in digital technologies.

This paper investigates the consequences of quantum computers on speed of computation, simultaneity in data processing and its impact on data security. The paper also examines the impact of quantum computers on business applications such as e-commerce, net banking, and other financial transactions. The proposed systems are likely to contribute drastically towards speed of computations. The paper demonstrates that speed would be a function of qubit structure. The new systems are expected to bring significant improvement in data and system security which would boost ICT application in all spheres of human activities. Quantum cryptography, visual cryptography, and image steganography are few techniques that could provide unprecedented data security.

References

Bhaskaran, G. (2008). "Scientific Developments: A vision", In: S R Hashim and N S Siddharthan, (Eds) *High Tech Industries, Employment and Global Competitiveness*, Routledge, London: New York and New Delhi, 219-237.

Deutsch, David (2012). T*he Beginning of Infinity*, Penguin: London.

Menon, Pranav Santosh and Ritwik, M. (2014). A Comprehensive but not Complicated Survey on Quantum Computing, *IERI Procedia*, 10, 144 – 152

Shemin, P.A. and Vipinkumar, K.S. (2016). E-Payment System using Visual and Quantum Cryptography. *Procedia Technology*, 24, 1623 – 1628.

McAdams, Simon G., Ariciu, Ana-Maria, K. Kostopoulos, Andreas, P.S., Walsh, James and Tuna, Flouriana (2017). Molecular single-ion magnets based on lanthanides and actinides: Design considerations and new advances in the context of quantum technologies. *Coordination Chemistry Reviews*, vol. 346, 216-239.

Horváth, Imre and Regine, W.Vroom (2015). Ubiquitous computer aided design: A broken promise or a sleeping beauty. *Computer-Aided Design*, Vol. 59, 161-175.

Zhou, Zhi, Arce, Gonzalo R., and Crescenzo, Giovanni Di, 2006, Halftone Visual Cryptography, *IEEE Transactions on Image Processing*, Vol. 15(8).