

FROM INFORMATION TECHNOLOGIST TO QUANTUM SPECIALIST

By Jeremiah K. Jones

The roles of an Information Technologist can range anywhere from system administrative work, to developing communications systems, to data management. Among all of the various duties an IT specialist may have, there are two responsibilities that will always remain constant: to adapt to change and to acquire new skills in response to those changes.

In the IT industry, we hardly have time to adapt to the latest technology before the next wave of progress sweeps over us. Amidst the tumult of constant change, it remains our duty to offer some stability to the professional world by quietly and quickly learning new skills in order to apply new technologies accordingly. Fortunately, we sometimes have some insight as to what developments are approaching, so that we can properly prepare for their deployment.

Even with advanced notice, the next major paradigm shift in the industry may still appear as a foreign subject to many Information Technologists. So what is the next revolution in IT? The answer to that question may be simple—Quantum Information (QI). Thus it is beneficial for IT specialists to begin brushing up on some basic Quantum Physics. Although the words ‘basic’ and ‘quantum’ never seem appropriate together, QI is rapidly approaching

the IT industry and needs to be better understood by Information Technologists everywhere.

A problem of quantum proportion

Quantum mechanics come into play where classical Newtonian physics begin to break down. As objects become smaller and smaller (such as an electron or a photon), Newtonian physics cannot be used to accurately calculate the properties of the body (location, acceleration, etc). Instead, according to Heisenberg’s uncertainty principle, these properties can only be calculated as a probability.

Additionally, in measuring a property, the value of that property will be changed by the measurement. For example, if a measurement is made to determine the speed of a photon, while taking the measurement, the speed of the photon will be altered so that the measurement is only valid for that single moment. The same is true for finding position.

These constantly changing values would seem to make utilizing quantum mechanics impossible. However, it ends up that this very principle of uncertainty is what allows quantum mechanics to become useful in data systems [1].

Bits and qubits

Through the use of superposition and entanglement, the properties of a quantum body can simultaneously represent many different values. These new states of being then represent ‘qubits’ rather than ordinary binary bits. One photon, for example, can contain an infinite amount of qubit information [1].

This leads us to one of the fundamental differences between a classical computer and a quantum computer. In a classical computer, n number of bits can represent any one integer k , where $0 \leq k \leq 2^n - 1$. By using the principle of superposition, it is possible for n qubits of quantum information to represent all integers in that range simultaneously [2].

Using qubits as the basis for a computational system creates an entirely new form of logic with unique algorithms to power the system. This new set of quantum rules has been elaborated upon in the theoretical design of the famous Feynmann processor [1].

From theory to application

Although quantum computing is a fascinating concept, as of now, it remains only that—a concept. It is true that there have been some cases of simple quantum calculations (on Dec. 19, 2001 Scientists at IBM's Almaden Research Center successfully used a 7-qubit quantum computer to factor the number 15 [3]), however, the public is still far from seeing any practical application of these theories. On the other hand, Quantum Information (QI) is something that is much closer to becoming a standard in the IT industry.

Rather than using quantum mechanics to perform complex calculations on data, there have already been some amazing breakthroughs in the use of quantum mechanics to represent and encrypt data [4]. By using quantum theories in data encryption and transmission, it is possible to create an unbreakable encryption algorithm. This would allow for data to be transmitted at high rates through optical lines without the possibility of an eavesdropper being able to intelligibly “listen” to the data.

Recently, id Quantique was able to implement an encryption system using quantum-key distribution (QKD). This is a scheme that allows for the encryption keys to change rapidly, so that a hacker would have to crack multiple AES codes used throughout the data transmission. This type of technology is already feasible, and there is already talk of working quantum security into satellite communications.

Other companies have also been able to successfully implement a variety of quantum security systems [5]. This is a sure sign that the use of QI is not far from implementation in more public environments.

A quantum example

As these methods approach application in the industry, it becomes important not only to recognize their existence, but also to understand some basic examples of how these systems might be implemented. There are currently many different theories and ideas on how to use quantum mechanics in the IT industry, but many of them are similar enough that the fundamental concepts are the same. Therefore we will only

look at one example of how QI is proposed to be implemented. The example we will look at is the BB84 protocol [6].

This protocol utilizes the quantum properties of photons to share a cryptographic key. Photons will each have one of four polarization states: horizontal, vertical, +45 degrees (diagonal), or -45 degrees (the opposite diagonal). These states are then predetermined to represent the binary states of '1' and '0'. In our example, we will have the horizontal and the +45 degree diagonal represent a '1', while the vertical and the -45 degree diagonal will represent a '0'.

Using the classical cryptographic example of "Alice and Bob," Alice and Bob will use the BB84 protocol to determine the cryptographic key that they will use in their system. First, Alice sends Bob a random series of bits, each in one of the four polarization states. In order to determine the polarization of the photons, two types of detectors are used. The first type will correctly detect a horizontal or vertical polarization (detector A), while the second will correctly detect either of the diagonal polarizations (detector B). Only one detector may be used per photon bit, and the detector can only be trusted to correctly determine the two polarizations it was intended for. As an example, if a horizontal photon is detected by detector B, then the polarization state could be read to be either of the diagonal directions, but it will not be correctly detected as a horizontal polarization.

Bob will then randomly select a series of detectors to retrieve the data. Upon retrieval,

there will be many bits in error. Again, this is because a random series of detectors was used, and each detector can only correctly determine two of the four possible polarizations. Bob has no method of his own to be able to determine which bits were correct. He then must tell Alice the series of detectors he used to retrieve the data, and Alice can respond by letting him know which if his detectors were correct in determining the polarizations. They will then use the correctly detected bits as the cryptographic key in their system.

If an eavesdropper is listening to the bits in the system, then Alice and Bob will be able to detect the eavesdropper's presence. This is also a benefit of quantum encryption. As an eavesdropper attempts to detect the bits using a random sequence of detectors, the properties of the bits are changed, and thus errors will be introduced into the correct data. As Alice and Bob detect the increased number of errors, they will be able to determine the presence of the eavesdropper.

A new standard

As QI technology becomes more affordable to smaller businesses, the IT industry will surely see some dramatic changes. The transmission and protection of data will take on a new perspective, and it will become very useful for the IT specialist to become familiar with the workings of QI.

Some of the current uses of QI that are being researched include: cryptography, data teleportation, faster computation times, and quantum sorting algorithms. Because each of

these applications would become a great asset to anybody working in a technology-related field, it is beneficial to begin looking into this growing field early on in its progress.

Although it may not be necessary for an Information Technologist to carry on a comprehensive conversation with a quantum physicist, it will become very useful to be acquainted with the background of this information, so that he may be able to quickly adapt to the new technologies that will surely be coming into adaptation.

As the duties of the Information Technologist seem to increase daily, it is strongly suggested that the role of “Quantum Specialist” be added to the list. This will ensure a quick and nearly painless shift into the new era that seems to be looming above the industry.

References

- [1] Gerard J. Milburn, “The Feynmann Processor”, Helix Books, pp. 28 - 37, 1998.

- [2] Arthur O. Pittenger, “An Introduction to Quantum Computing Algorithms”, Birkhauser Boston, pp. 22-23, 2000

- [3] IBM Research News, “First demonstration of Shor’s historic factoring algorithm”, http://www.research.ibm.com/resources/news/20011219_quantum.shtml.

- [4] Geraldo A. Barbosa, Eric Corndorf, and Prem Kumar, “Quantum cryptography with coherent-state light: Demonstration of a secure data encryption scheme operating at 100kb/s”, Presented at QELS’02, Long Beach, CA, May 19-24, 2002.

- [5] R. Colin Johnson, “Hackers beware: quantum encryption is coming”, EE Times, <http://www.eetimes.com/story/OEG20021111S0036>, 2002.

- [6] Justin Mullins, “Making Unbreakable Code”, IEEE Spectrum, pp. 41 – 45, May 2002

Other Resources

Michael Brooks, “Quantum Computing and Communications”, Springer, 1999

Michael A. Nielsen and Isaac L. Chuang, “Quantum Computation and Quantum Information”, Cambridge, 2000

H. P. Yuen, “Quantum versus classical noise cryptography”, in Quantum Communications and Measurements II, ed. P. Kumar et al., Plenum Press, 2000