TECHNOLOGY

Quantum Technology and the Medical Librarian

Jason Bengtson

Texas Medical Center Library, Houston Academy of Medicine, Houston, Texas, USA.

INTRODUCTION

Some of the most exciting areas of computing research are quantum technologies. Relying on the counterintuitive laws which govern matter and energy at the smallest levels, quantum physics provides bold new answers to problems which current digital technologies cannot effectively solve. This article discusses the basis of these technologies and introduces two ways in which they may practically impact the environment of the medical librarian in the coming years as the technologies become more mature. By understanding something of these technologies and how they may manifest themselves in hospital or other healthcare environments, the hospital librarian can help prepare themselves for this exciting future.

SAFEGUARDING INFORMATION WITH QUANTUM TECHNOLOGIES

Information security has become one of the highest priorities for information providers in health care environments. Providers are legally obligated to take extreme steps to ensure that confidential medical information doesn't fall into the wrong hands.

Essential to this process are ways of protecting data to make it difficult for unauthorized parties who capture it in transit or remove it from a compromised digital environment to use or understand it. In fact, protecting data in such a fashion has become one of the central problems of our digital age. Essential to protecting modern data transfer is a process known as public key encryption.

Public Key Encryption

Modern communication channels are protected by *encrypting* them so that they can't be understood without *decrypting* the information they contain. Encryption takes a message (plaintext) and converts it into an encoded form (ciphertext), which must then be converted back into plaintext (decrypted) in order for it to be understood. *Symmetric encryption* relies upon complex algorithms (ciphers) and large alpha-numerical *keys* (similar to a very large password) to encrypt a message (1). Two users share a key that is pseudorandomly (a process not fully random, but which appears random under analysis) generated and exchanged between the users. Generally, the larger the key, the more difficult it is to decrypt a message without it.

However, there is a serious problem with this model of encryption. Namely, the parties involved must somehow secretly share a key that can be used to encrypt and decrypt all of their messages (2). If the key is intercepted, the eavesdropping party can use it to decrypt all of the private messages at will.

Most web encryption attempts to solve the key distribution problem using a technique called *public key encryption*. With this method, there are two keys, a public

and a private key. The public key is openly shared and is used to encrypt a message. However, the public key cannot decrypt messages. For decryption, a user must have the private key, which is not shared. Through this technique anyone can encrypt a message to be sent to a user, while only private key holders can read the message. Alternatively, the user can encrypt via the private key and users can decrypt the same message with the public key . . . ostensibly proving that the message came from the purported sender. In the commonly used RSA public key encryption scheme, the encryption protocols are based upon solving factorization problems for extraordinarily large prime numbers in order to decrypt the data (1). Because it requires so much computing power to find the large prime numbers that serve as the keys to encrypt and decrypt such communications, in the absence of those keys it becomes almost impossible for an attacker to access the message. There is, however, a technology on the horizon which may make this operation far more trivial to perform (more on that later).

Public Key Encryption is, however, very computing intensive, and so is really only suitable for users to send another key to each other that will be used for symmetric encryption (1, 2). Because symmetric encryption uses the same key for encryption and decryption of a message, and uses shorter keys, it also requires far more limited processing resources. This temporary key is then used for the duration of the communication session (2). Public key encryption is a powerful technique which forms the basis for secure communications on the modern web, but it's efficacy is predicated on the safety of private keys. This vulnerability of the public key encryption system has proven particularly worrisome in the last few years, as hackers, companies, and

governments have been caught improperly accessing private encryption keys through a variety of exploitation techniques. It is now public knowledge that the US Government regularly forces companies to surrender private encryption keys so that it may eavesdrop at will on private exchanges (3-5).

Private Key Encryption is based largely upon principles of the macroscopic world; that is to say, the world we all see and interact with. Most of us have at least a passing familiarity with the laws of this world, such as Newton's Laws of Motion. We may even know something about the more exotic of them, such as the effects of light and gravity described by the theories of Einstein. However, the world that seems so solid to us is actually a veneer, built upon much smaller building blocks that exist on the subatomic level. These building blocks follow different laws than those we are used to in the macroscopic world. In many ways, the logic of the physical world breaks down on this *quantum level*. Named for the theoretical, smallest unit of energy, the *quanta*, quantum physics describes the laws that operate at this level of reality. This branch of physics forms the basis of modern electronics, among other technologies. As scientists and researchers continue to explore the reality of this quantum world, some engineers have begun to expand the uses to which these discoveries have been put. One of the most exciting of these technologies may provide an unassailable way for users to exchange one-time, symmetric encryption keys.

Quantum Key Distribution

At the quantum level, the act of measurement changes things (6). As such, any information sent as quantum states will be changed if a third party intercepts and measures that information. By sending a one-time key as a series of bits encoded as particle quantum states, the sender allows the recipient the opportunity to verify the integrity of the information sent by comparing subsets of the message bits against the sender's data. If there are errors, the two parties will have reason to believe that their message (which will be used as the basis for their encryption key) has been at least partially intercepted (7, 8). This allows them the opportunity to switch communication channels and try again until they are able to successfully exchange an unaltered key for use during their communication session. Using this method, neither party must rely upon private keys which may be stolen by an unauthorized party. Quantum key distribution is already seeing limited use in Europe and, as security problems on the web proliferate, it is likely that we will see greater deployment in the future (7).

Quantum Key Distribution and HIPAA

Just as public key encryption is only as good as the security of private keys, HIPAA protections are often only as good as the encryption used to protect both communications and stored data. Through the use of quantum key distribution, health care providers have a way of of initiating a communication session using a one time key which expires at the end of the session, and which is exchanged between parties without relying on a private key which can be stolen. Indeed, each instance of key exchange is unique, and protected against unauthorized observation by one of the

foundational principles of modern physics. As such, the communicating parties may be assured of the security of their shared key, and, consequently, the likely security of their information exchange. Such security still relies on the use of symmetric encryption keys large enough to require unrealistic levels of computational work to discover. However, as long as such large keys are in use, and are generated through a secure, highly random mechanism, quantum key distribution could make unauthorized decryption of such messages a practical impossibility with current computing technology.

QUANTUM COMPUTING AND DIFFERENTIAL DIAGNOSIS

Using digital tools to aid in differential diagnosis is a tantalizing prospect. A new quantum technology could provide computer processing that is particularly conducive to this effort. The key to this technology lies in the way information operates on the quantum level; a fact that opens the door for something called *quantum computing*.

What is Quantum Computing?

Modern digital computers manipulate data built upon bits, which are the smallest unit of digital information. A bit can exist in two and only two possible states; zero or one. All modern computer processors are, at their most basic level, a pile of electronic switches (known as *transistors*) with off meaning zero and on meaning one. Strings of these binary digits can be used to represent any number. Digital computer processors

perform mathematical operations upon these numbers one at a time (although at incredibly high speeds). This process can sometimes be accelerated by breaking problems into smaller parts which can be solved in parallel, by using a processor that is actually several processors (called *cores*) in communication with each other. Even using parallel processing, however, most mathematical operations must follow a series of steps completed in order. Many problems (such as factorization) must be solved by trying every possible solution until the correct one is found. This limitation is the reason why even powerful computers find it practically impossible to decrypt messages asymmetrically encrypted with large, randomized keys without having access to the keys themselves.

Bits may be the smallest unit of information in computing, and they're easy for people to understand, but at the quantum level binary units are not the basis of information. At this level, the bit is replaced by the quantum bit, or *qubit*.

Qubits are a consequence of the curious way in which things exist at the quantum level. In the macroscopic world we are used to objects that only exist in one place at one time. Because of this familiarity, in school we are often introduced to subatomic particles as tiny spheres interacting with each other and flying rapidly through space. In reality, however, subatomic particles don't have a definite location and don't exist in a definite state. They exist in multiple locations and states at once, and only collapse into a definite state as a result of measurement. Instead of a tiny sphere, a subatomic particle is more like a cloud of possibilities, existing in what is known as a *superposition of states* (9, 10).

At its most basic level, this superposition is represented by a qubit, which can not only be a one or a zero, but can also represent any superposition of the states of one and zero (11). In this way, a single qubit can actually represent multiple states at once (9, 10, 12). To solve problems, the qubits in a quantum computer are set to an initial state, then manipulated with a quantum *algorithm* (a series of steps designed to solve a problem). Through a mysterious mode of interconnection called *quantum entanglement*, the qubits are able to share information amongst themselves (9, 10). At the end of this process the superpositions of the qubits are collapsed into a single state, now either one or zero. In essence, a quantum processor can simultaneously test many solutions to a problem, instead of testing them one at a time.

Quantum processors are currently at a highly experimental stage, and there are many engineering problems to be overcome before they become ready for practical use (10). However, the possibilities offered by quantum processors are already making some researchers nervous. Quantum computers employing a large number of qubits could easily solve the kinds of factorization problems that safeguard modern public key encryption schemes (12). Because Symmetric Key Encryption uses a different process to generate encrypted messages, most researchers believe that symmetric encryption, as long as sufficiently long, highly randomized keys are used, will remain too difficult for quantum computers to successfully crack. In addition to cryptographic applications, quantum computers have the potential to readily manipulate an enormous number of variables and solve problems based on incomplete information in ways that digital computers struggle with.

Can Quantum Computing Aid with Diagnosis?

Diagnosis is a notoriously difficult process requiring both an expansive knowledge base and the ability to sort through a large number presenting symptoms. Doctors must cope with incomplete or incorrect information from patients, symptoms common among many ailments, and the possibility that a patient is suffering from many illnesses (including opportunistic ones) at the time of their examination. Numerous attempts have been made to use computerized tools to aid in the diagnostic process. Perhaps the most notable of these efforts has been Watson, the IBM supercomputer that used a combination of natural language analysis techniques to win a *Jeopardy!* competition. Since thrilling audiences with this feat, IBM has worked with the Memorial Sloane-Kettering Cancer Center to employ the tool in Oncology (13).

Early results from Watson's use in diagnosing cancer have been highly promising. But Watson, despite being a remarkable technology, suffers from a number of shortcomings. Watson is a supercomputer, requiring significant digital resources to accomplish what it does. That means Watson needs even more significant resources to be scaled up for widespread use. It would be impractical to have a Watson supercomputer at every healthcare institution, even if those institutions could afford the investment in hardware and licensing, so Watson will be likely available to most of them only on a subscription basis. That means that those institutions will lose Watson's advantages in the event of an internet outage, and may suffer severe slowdowns at peak times when the Watson service is being inundated with traffic.

With its ability to perform operations on many variables simultaneously, and deal easily with incomplete information, quantum computing offers a compelling possible alternative to even the most sophisticated artificially intelligent applications running on digital processors. Such capabilities will potentially make quantum computers more scalable and less resource-intensive when solving difficult problems such as differential diagnosis. As such computers become more powerful and decrease in size, they could be deployed to infrastructure poor areas suffering pandemic conditions, providing local power equivalent to a digital supercomputer to aid in diagnosis and the elucidation of treatment options.

CONCLUSION

Quantum technologies are still in development, but may soon provide powerful new tools to protect private healthcare information and assist medical professionals in diagnosing and treating patients. This article provided a general overview of two of these technologies: quantum key distribution and quantum computing, both of which may, within the foreseeable future, revolutionize the way that information works in health care environments. By better understanding the basis of these technologies, hospital librarians will be better positioned to deal with them when they begin to make an appearance at health care providers.

REFERENCES

1. The Apache Software Foundation. (2015). SSL/TLS Strong Encryption: An Introduction - Apache HTTP Server Version 2.2.http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html#cryptographictech (22 Feb 2015)
2. Kinney S. Cryptographic Basics. In: Kinney S, editor. Trusted Platform Module Basics. Burlington: Newnes; 2006 p. 11–9.
3. Brodkin J. (2013). CryptoSeal VPN shuts down rather than risk NSA demands for crypto keys. *Ars Technica*. http://arstechnica.com/information-technology/2013/10/cryptoseal-vpn-shuts-down-rather-than-risk-nsa-demands-for-crypto-keys/ (23 Feb 2015)
4. Twitter EP. (2013). Reports: NSA Has Keys To Most Internet Encryption. http://www.npr.org/blogs/thetwo-way/2013/09/05/219367716/reports-nsa-has-keys-to-most-internet-encryption (23 Feb 2015)
5. Geuss M. (2015). SIM card makers hacked by NSA and GCHQ leaving cell networks wide open. *Ars Technica*. http://arstechnica.com/tech-policy/2015/02/sim-card-makers-hacked-by-nsa-and-gchq-leaving-cell-networks-wide-open/ (23 Feb 2015)
6. Weizman Institute of Science. (1998). Quantum Theory Demonstrated: Observation Affects Reality. http://www.sciencedaily.com/releases/1998/02/980227055013.htm (23 Feb 2015)
7. Battelle DH. (2014). The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution. *WIRED*. http://www.wired.com/2014/09/quantum-key-distribution/ (23 Feb 2015)

8. Chan P, Lucio-Martínez I, Mo X, others. (2011). Quantum Key Distribution. http://arxiv.org/abs/1111.4501 (23 Feb 2015)

9. Galchen R. (2011). The Mind-Expanding World of Quantum Computing. *The New Yorker*. http://www.newyorker.com/magazine/2011/05/02/dream-machine (23 Feb 2015)

10. Simonite T. (2012). The CIA and Jeff Bezos Bet on Quantum Computing. *MIT Technology Review*. http://www.technologyreview.com/news/429429/the-cia-and-jeff-bezos-bet-on-quantum-computing/ (23 Feb 2015)

11. Altepeter J. (2010). A tale of two qubits: how quantum computers work. *Ars Technica*. http://arstechnica.com/science/guides/2010/01/a-tale-of-two-qubits-how-quantum-computers-work.ars (23 Feb 2015)

12. Rich S, Gellman B. (2014). NSA seeks to build quantum computer that could crack most types of encryption. *The Washington Post*. http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html (23 Feb 2015)

13. Steadman I. (2013). IBM's Watson is better at diagnosing cancer than human doctors. *Wired UK*. http://www.wired.co.uk/news/archive/2013-02/11/ibm-watson-medical-doctor (14 Feb 2015)