Quantum Cryptography – Current Methods and Technology

Jeremy Goldman

December 11, 2014

Abstract

If properly harnessed, the application of quantum particles will dramatically alter the computing world. This power will be particularly important in the field of cryptography, which has thus far relies on the complexity of classical operations to encrypt data or hide keys. The quantum bit would exponentially decrease the computing time necessary to find a key. In addition, the no-cloning property of quantum particles can be utilized to ensure eavesdroppers are not present in communication channels. Our technology is not able to deploy mass-produced, reliable machines or channels with quantum capabilities, but significant advances have been made in the past decade. This paper examines how computers will take advantage the unique properties of quantum particles to both ensure greater security, and break existing cryptographic algorithms.

A Look into Quantum Mechanics

Quantum mechanics is the study of the small particles that make up the universe – for instance photons and electrons. At the low level of physics, the general laws and equations that govern how objects move, known as classical mechanics, ceases to explain observed phenomenon. A number of properties have been attributed to quantum particles, some of which are quite useful for our purposes:

- Uncertainty principle – the more precisely you measure one aspect of a quantum particle, such as momentum, the less reliably you can measure another aspect, such as location
- Observer effect – the location of quantum particles can be described as a wave function, and upon observation the function appears to collapse into a deterministic state.
- Quantum entanglement – particles can be generated in such a way that they can be described as a system, rather than as one individual particle. For instance, if total spin equals zero, altering the spin of one particle affects the other.

Nonetheless, we do not know everything there is to know about this complex science. In the words of physicist Richard Feynman: “I can safely say that nobody understands quantum mechanics”. This uncertainty partially explains the difficulty engineers and scientists alike have encountered in the task of building a quantum computer.

To the community

The purpose of this paper is to characterize the current and potential applications of quantum particles in the field of cryptography. It does not to give a detailed description in to the laws of quantum mechanics; people have earned their PHDs for less. A precise understanding of the multivariate equations behind the theories is helpful, but for the sake of our higher-level algorithms and time they are mostly kept out of the paper. For those who desire a higher understanding of lower mechanics, helpful sources can be found at the end of this article.

The Importance of Qubits

The implementation of quantum bits, known as qubits, into computer architecture, would dramatically affect the field of computer science. More research is being done on qubits than ever before, and they have already emerged in limited systems, mostly for the purpose of research and development. In many regards, the introduction of bits with quantum properties will make classical computers, which rely solely on deterministic electronic currents for calculation, obsolete. Because of the complexity and uncertainty of these particles, their potential applications cannot be fully enumerated; nonetheless, there are clear cryptographic techniques and technologies that stand poised to take advantage of this new science.

Encryption: Quantum Key Distribution

To use the standard example, say Alice and Bob are communicating privately, and Eve is attempting to eavesdrop. Using the ‘safest’ encryption there is, Alice can generate a one-time-pad for her message and send the key to Bob. Alice then exclusive-or’s the bits of her message with the pad, so when Bob receives the encrypted message, he can exclusive-or with the same pad.

While incredibly difficult to break computationally, this technique is still vulnerable to man-in-the middle attacks. Eve might be intercepting Alice’s messages, including the key itself, and either sending duplicates or forwarding them to Bob. If the attack is done well, Bob may have no idea that his keys have been viewed by an eavesdropper.

Quantum Key Distribution (QKD) involves sending decryption keys as quantum particles. Using these particles will enable both the sender and receiver to clearly notice when a third party is intercepting their message.

- Entanglement principle: Two copies of the same key can be generated using a light polarization filter, which only allows a small bottleneck of photons to pass through. Two photons passing through at the same time will exhibit an equal entanglement state, in which an effect on one will be do the same to the other, regardless of their distance in space.
- Observation effect: When Eve measures the state of the particle, its wave function will collapse and the state will change. Because Alice's photons are entangled, the change will register on her end as well.
- No-Cloning theorem: This theorem states that it is impossible to create a tool that takes an entire quantum state as input, and outputs a particle with that same state. Essentially, we have not yet devised a way to copy qubits, and it is generally believed to be impossible. Thus the attacker could not copy the photons, which would store their information in un-entangled particles, before sending them to Bob.

In order to further detect intruders, the photons can be randomly sampled for different properties. Remember that a certain measurement of one property means uncertainty of the others. Alice and Bob independently choose to measure each proton for different properties, say polarization or spin. The then exchange which property they measured on each photon, and examine whether the values are the same on photons that they measured

the same property. If there is a large difference, it is likely the signal was intercepted, and the communication should be dropped. If results are similar, then the values can be stored as binary data; for instance, left spin = 0, right spin = 1. This is the shared key.

There is a trade off here between security, efficiency, and time. Efficiency in this context means the number of photons whose properties translate into key values. It is possible to have two of the three.

- Security and time: Include a wide variety of possible measurement types, but this would result in most photons being wasted.
- Efficiency and time: conduct the same measurement on each photon
- Security and Efficiency: Conduct the random measurements again on the unused photons, logarithmically increasing efficiency with each full iteration. Most academic papers and modern companies suggest this method, recommending one or two extra iterations through the unused photons.

Use Today

Largely a European phenomenon, professional QKD systems made their first appearances around ten years ago. The need for secure key distribution has sparked much research into the field from private industry. Thus far, elementary systems have been implemented in cities such as Geneva and Dublin.

There are, however, some limitations on the practical implementation of QKD that have yet to be overcome. Each particle in QKD is significant, but transporting photons over long distances without interference has been an engineering issue. Fiber-optic cables can carry photons for around 50 miles, but beyond that over 90% of the

particles become absorbed by the cables themselves, which is below the desired mean photon rate of 0.1. This is likely the reason discrete systems must be set up within each city. Generating and measuring the photons requires specialized equipment as well; equipment which is not likely to be found within a personal computer anytime soon. Because of this, intermediate facilities, euphemistically referred to in the industry as "trusted nodes" must be established to receive the messages. Concern has been expressed over the possibility of a leak or identity forgery within the intermediate step. But the overall belief within the QKD community seems to be that these obstacles can be overcome.

Quantum Computing: breaking modern cryptographic algorithms

Much of today's encryption relies on the arithmetic complexity of operations required to decrypt a key. Consider, for instance, the modern RSA encryption algorithm. The length of the key influences how long it will take to decrypt the message, both with a known and an unknown private key. Given a private key, doubling the length of the key slows down decryption by a factor of six or seven. Without the private key, decryption takes a vastly longer amount of time, and doubling the key size exponentially increases the time required. In fact, it is often more efficient to wait for an improvement in technology than to spend years of CPU time to break a single key. In 2003, the NSA estimated that it could spend tens of millions of dollars on a machine that could break a 1024-bit RSA key in a year. Yet today, cryptographers warn that processing power has been increasing such that the 1024-bit key is no longer up to par.

The next leap in this decryption technology may come from different computation mechanisms entirely. On classical computers, where all bits are stored as transistors that can be in a position either representing 0 or 1, simple brute force attempts to break keys involve guessing the value of each bit, testing if that combination works, and trying another value if it does not.

Quantum computers rely on the same idea, but will take advantage of the properties of quantum particles to speed up the computation. Before a particle is observed, its aspects (polarization, spin, momentum, position, etc) are not determined. This is the fundamental principle: it is not that we do not know the value of a quantum bit before we look at it; rather, its value can be superimposed between zero and one. Thus one qubit can store 2 values at once, 2 qubits can correlate 4, and 100 can correlate 10^{29}. Thus quantum computers would largely be comprised of classical bits, with a few crucial qubits. With this capability fully harnessed, solving non-deterministic algorithms in polynomial time would become a reality.

Theoretical Implementations

In order to transform a quantum particle into a qubit, its properties must be discretized into two possible values. For instance, whether a photon has a right or left handed circular polarization. A number of other particles and measurements have been proposed for this purpose:

Measurement	0 / 1	Physical Element(s)
Spin	Up / Down, Left / Right, 45^{o} / 135^{o}	Electron, Nucleus, Optical Lattice, Josephson Junction, Quantum dot (nanocrystal)
Charge	Uncharged / Charged	Electron (determined by presence), Josephson Junction

Practical Challenges

Because of the observation effect, observing at a qubit before it is finished computing will collapse the wave function, effectively terminating the qubit's superposition. No method has been established to monitor the state of a qubit during execution of a program, at least during the parts when it is calculating in a superimposed state. One implication of this is that computations involving qubits prove quite difficult to debug; one cannot go through the assembly code line-by-line and examine the values of qubits during the process. In addition, the observation effect does not only account for sentient observers such as humans. Other particles can unintentionally interfere with the quantum element at the atomic level (or lower down), and condense the superposed qubit. Minimizing collisions is part of the reason that many experimental quantum computers cool the temperatures of the quantum particles to almost absolute zero.

In similar spirit to the photons in QKD, qubits can become absorbed by their surrounding environment if not handled properly. Entanglement can also be an issue in computers with multiple qubits. When two or more qubits entangle, their individual positions describe the positions of the other. Thus, processing power is decreased because the two cease to act as individual actors but rather as a unit.

The Development Process

There is also the complexity of incorporating these qubits into a functioning computer with classical bits, but this has already been achieved, to a limited degree. Google, Microsoft, IBM, and other hardware firms are looking into the potential structure and application of these machines. Engineers working on building these machines understand them to varying degrees before implementation. In the style of the uncharted quantum arena, Google has taken to throwing small systems together and testing them after the fact to see what they are capable of accomplishing.

This is to say that the first quantum computers will be tremendously powerful, but equally expensive. Powerful organizations will have first access to these non-deterministic machines before the general population. Developers of encryption algorithms will therefore have to take into account the superimposed threat and potential of qubits. The result may well be an algorithm that runs in increasingly complex polynomial-time algorithms or nested encryption whose runtime is NP^{P}, or NP^{NP}.

Conclusion

The inclusion of quantum physics into computing tools has potential to effect many aspects of cryptography. The unique laws of quantum particles can be incorporated into cryptographic systems, both aiding the security and vulnerability of sensitive information. Relying on the observer effect and no-cloning principle, Quantum Key Distribution offers a method to ensure that communications are not intercepted. The

introduction of the qubit may drastically reduce the time required for NP-complete problems, many of which are used as encryption schemes.

Moore's Law predicts an exponential rise in computing power over time. As transistors near the size of the electrons they hold, perhaps the next leap will come from a fundamentally engineering mechanism. Cryptography will be largely effected by these infinitesimally small particles, and security firms large and small are preparing for their advent.

Works Cited

[1] Shor, Peter R. “Polynomial-Time Alrogithms for Prime Factorization and Discrete Logarithms on a Quantum Computer” *SIAM* 26 (1997):1484 http://arxiv.org/pdf/quant-ph/9508027v2.pdf. 28 Nov. 2014

[2] “RSA Key Lengths” Jaxamex 2 Dec 2014 <http://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml>

[3] “Is the future of cryptography in qubits” SANS Institude 29 September 2002, 26 Nov. 2014 <http://www.sans.org/reading-room/whitepapers/vpns/future-cryptography-qubits-885>

[4] Rambabu Saini “Quantum Cryptography Enhancement of QKD EPR Protocol and Identity Verification” *International Journal of engineering sciences and Research Technology 27 November 2014*
http://www.academia.edu/2120175/Quantum_Cryptography_Enhancement_of_QKD_EP

[5] Goran Lindblad “A General No-clning Theorem” 1998, 9 Dec. 2014
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.44.827

[6] Toshihiko Sasaki, Yoshihisa Yamamoto & Masato Koashi “Practical quantum key distribution protocol without monitoring signal disturbance” Nature 509, 475–478
http://www.nature.com/nature/journal/v509/n7501/full/nature13303.html 28 Nov 2014

[7] William Jackson “Can quantum cryptography work in the real world?” GCN Oct 28, 2013, Nov 28 2014 <http://gcn.com/Articles/2013/10/28/quantum-cryptography.aspx?Page=2>