Tear it Down and Build it Up:
A Quantum Twist on Information Decoding and Encoding

Written by Michael Gualtieri, April 2000
Seton Hall University - Computer Science Undergraduate Program

1. Abstract

The goal of this paper is to give the reader an understanding on the emerging field of quantum cryptography. A brief introduction to quantum computation is given followed by an overview of classical cryptography. This will give the basis for the remainder of the paper, which will explain quantum cryptography and some of its advances/standards. Concluding the paper will be drawbacks of using this method of encryption.

2. Introduction

Consider this situation. Bob and Alice are two classmates with a crush on each other. During a dull class, obviously not in the mathematical or computer field, they decide to pass each other love notes. The only problem is that another classmate Eve, who is a gossip, wants to read these notes. Bob and Alice are aware of this so they come up with a way to encode what they are writing, so no one, especially Eve, can read these notes. This may sound like childish behavior, but it is a common situation which, occurs on a second by second basis on the, newly dubbed, information superhighway. Between secret business information to top secret government files to your personal email, data is transmitted constantly and needs to remain secure and confidential. Thus we have

cryptography. Cryptography however, is a rapidly growing field, and advances are made daily to keep current encryption schemes strong, because as faster computers are built, it becomes quicker and more feasible to defeat these schemes.

Now consider this. What if Eve was also a brain, and could crack codes faster then anyone else in the class, and unlike any one else before. Would Bob and Alice's note be safe? Could Bob and Alice use their smarts to pick a more complicated code to one again outsmart Eve? Now enter the world of quantum computation and cryptography.

Quantum computation is shaking the world of classical computer science at and astounding rate. A relative new field, only beginning to gain support in the 1990's, it has already made developments which could be revolutionary, especially in the realm of encoding and decoding information, cryptography.

3. Quantum Computation

Quantum computation is based on *Hilbert Space*, or rather an infinite list of all possible realities, mathematically described as dimensions, all governed on the reactions of subatomic particles and quanta of light. While the classical method of approaching a problem would be to cycle through these "realities," or states, one by one, the quantum method can compute all these states in parallel. This means that a problem that requires billions upon billions of computations, before an answer can be given, can be solved instantly, instead of waiting until the end of the universe, literally, to receive the information requested, which is quite impractical, to say the least.

In the classical manner, all data can be represented by either *true* or *false*, *1* or *0*. This however is unacceptable when working in quantum spaces, due to the fact an atom can hold two polarization's, and hence is "fuzzy." Instead we have the invention of the *qubit*, invented by Dr. Schumacher, which is the smallest unit for quantum space, basically a quantum bit. In these qubits all states of data can be represented. For example we can have instead of 0 and 1, (0,0) (0,1) (1,0) and (1,1), and *n* quibits can hold 2^*n* states, at all times. Quantum computers work by taking a starting state of many numbers, instead of a single number, and performing a single operation on the entire set, thus producing the output instantly.

$$|0\rangle \rightarrow \tfrac{1}{2} * (|0\rangle + |1\rangle)$$

Fig I – A simple unary operation, mathematically represented, to transform qubits from the 0 state into another state.

$$\tfrac{1}{2}(|0\rangle + |1\rangle) \otimes \tfrac{1}{2}(|0\rangle + |1\rangle) = \tfrac{1}{4}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Fig II – A representation of an operation on a 2-bit quantum register.
Note: Binary representation is used, (10 = 2 and 11 = 3)

Interesting anomalies occur while working with these spaces. Before an interaction is made with the space, it does not even exist. Also, any further interaction causes its state to be permanently changed. These are complex topics to understand and are out of the scope of this paper, but although they may seem like weaknesses they can actually be used as advantages. Later on we will find how these features can be used practically and applied to cryptography.

4. Classic Cryptography

The situation presented above about *Bob*, *Alice*, and *Eve* was not chosen at random. These names are actually standard labels for certain aspects of cryptography. Alice is the party that encrypts and sends the message. Bob is the receiving party and decrypts the message. Eve is an unauthorized eavesdropper on the conversation between Bob and Alice.

Fig. III - Diagram of the roles Alice, Bob, and Eve take in communications.

The job of encryption is to stop Eve from listening to Bob and Alice, and there are numerous encryption schemes available today which will prevent Eve from listening to their conversation. Some of the more popular schemes are *public key* systems and *one time pad* schemes.

Public Key Encryption

Public key systems do not need a secret key exchange to send a message. Instead it works by having one public key to encrypt the message and a private key, to decrypt it. Anyone can have the public key to encrypt the message, but only one person can decrypt it. In essence, anyone can be Alice, but there is only one Bob. One of the most famous and widely used public key encryption schemes to date is RSA. Named after its inventors, Rivest, Shamir, and Adleman, it is based on the factorization of very large integer values. The public key in this case would be the two factors multiplied together,

and the private key would be the actual two numbers, which were used to generate the public key. RSA works under the assumption that it takes a very short time to generate the public key, for it is just one multiplication, however to generate all the factors of the public key and test them would take enormous amounts of time, therefore the private key can not be broken.

One Time Pad Encryption

The one time pad scheme is the only cryptography system that has been dubbed it will provide absolute secrecy. Alice, before transmitting the message adds it with a predetermined key. This in turn is transmitted to Bob who then subtracts the value of the key from the message. If Eve is able to intercept the message she will not be able to read it, because she does not have the secret key. This however does have drawbacks, despite its laude. If Bob and Alice keep using the same key to interact with each other, over time Eve could build up a "picture" of the key, and be able to decrypt messages. Also, the key must be first be distributed to both parties, which may not be feasible in all situations, such as in the case of satellite communications.

C = Encrypted Message $\mathbf{E_k}$ = set of functions used for encryption, where k is the amount of "key bits" or length of bits in the message **P** = Original Message **Encryption Applied**: $C = E_k (P)$ **Decryption Applied**: $P = E_k^{-1} (C)$

Fig. IV– A mathematical representation of one time pad encryption

5. Decoding Popular Encryption with Quantum Computation

By creating these *cryptograms*, or encoded messages, from such existing encryption schemes Eve will be thwarted by her attempts to listen to Bob and Alice's conversation. However remember in the second example given above, what if Eve could break codes faster than anyone? What would happen to Alice and Bob's note? This is a power that quantum computation can give to Eve.

Currently no matter how long a classical computer runs, certain encryption schemes will not falter. This is because there are so many possibilities to test before an answer can be returned. A good example is again, RSA encryption. To obtain a specific pair of factors from a large integer could take an eternity to compute, however with *quantum parallelism* the ability to compute many states at one time can be done instantaneously.

137 x 53 = 28907 => 1 step done quick 28907 = ? x ? => many steps, which eats time

Fig. V – An example of how factorization of large numbers is difficulty

In Figure V the number used was a mere 28907, which is feasible to factor and cycle through to get the correct combination of factors for the key, but what if the number for the factorization was hundreds or thousands of digits long? Then quantum parallelism is the only feasible way to break the code.

A man by the name of Dr. Peter Shor, an employee of AT&T Bell Laboratories, made this a reality. His algorithm based on quantum logic can factor numbers, which have an exponential growth with the number of factors and the size of the number being factored. It works by finding a common number, which is outputted by interference

within Hilbert space. Obviously it can be seen that this could end the security of current encryption schemes.

6. A New Encryption Solution: Quantum Cryptography or QKD

Now there is a problem for Bob and Alice, unless they can use the same technology that Eve uses, thus the emerging field of quantum cryptography. Quantum cryptography, or more correctly know as *QKD* (quantum key distribution) is the way to send encrypted messages over public channels and not worry what Eve may have up her sleeve.

One of the main standards for QKD is the *B92* protocol, invented by Charles Bennett, which is made up of the following steps. There are two channels needed, a private quantum one, usually fiber optic cable, and a public one, usually ethernet. Over the private channel Alice can send out photons from two polarizers, positioned vertically and at +45° to Bob. If she sends out the photon linearly, then this will be interpreted as a 0, otherwise she can send it out at a +45° angle, which would in turn be interpreted as a 1. Bob also has two polarizers, one which is horizontal interpreted as is 1 and one which is at a -45° angle interpreted as 0. During transmission Bob randomly selects a polarizer to receive the photon, and checks if the photon is passed to that polarizer, thus generating a yes or no each time. Bob is certain that he has the same bit value as Alice, because if he selects the vertical polarizer he will receive no photon, but if +45° is selected there is a 50% chance of it being received.

After the photon exchange Bob then sends to Alice his yes/no results. If Bob was unable to detect a photon, the “no’s”, it is thrown out and the resulting yes’s make up

the key in which Bob and Alice will use for further encryption. The bit rate has only a 25% efficiency rate, but that is the price which must be paid for greater security.

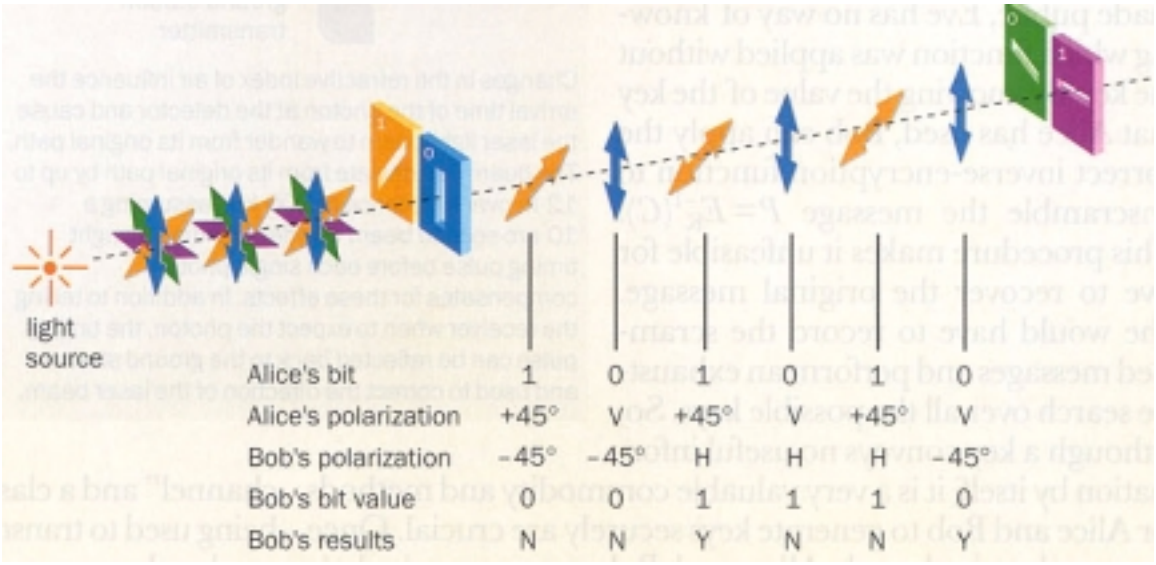

Fig. VI – A visual example of the B92 system.

Error checking can then ensue over a public channel. A subset of the new key bits from both Bob and Alice are then packed into several bit "words" and are then compared. The error checking can also help in detecting Eve lurking about. The photons are received from Alice to Bob at about 50%, however if Eve was interfering with this exchange, Bob's results would be off by 25%. This is due to the mechanics of quantum computation, every state once touched if changed forever.

QKD is a more efficient way of transmitting trusted keys between hosts. The key can not be found before usage, because if doesn't even exist before it is needed. Also snoopers are exposed much easier, allowing proper measures to be taken in dealing with them.

Advances

Thus far experiments at Los Alamos National Labratory, a primary researcher in Quantum Cryptography, have been able to send encrypted messages over 48km. Also experiments have been done with *free space,* or sending photons over distances without the uses of fiber optics. This is an ideal solution for satellites. So far the greatest distance covered in the daytime has been 0.5km, but this distance is expected to increase soon.

7. Shortcomings of Quantum Cryptography

Although the quantum system for cryptography seems ideal there are several shortcomings upon implementing it. Even though tests have reduced positive results, full-scale quantum computations will most likely not be around for some time. Factors such as thermal noise and imperfections within the hardware used could render a system useless. Quantum cryptography, however is a very new field and many ground-breaking advances continue to be made. When the realities of Hilbert Space can be mastered and used computations will be faster than ever and Quantum cryptography will protect us better than ever.

Sources Used

About Quantum Cryptography - http://www.ecst.csuchico.edu/~atman/Crypto/quantum/quantum-crypto-inf.html

About Quantum Devices - http://www.ecst.csuchico.edu/~atman/Crypto/quantum/quantum-devices.html

A Quantum Leap For Computers? - http://www.ecst.csuchico.edu/~atman/Crypto/quantum/qc-leap.html

A Quick Introduction to Quantum Information - http://p23.lanl.gov/Quantum/infointr.html

Beyond Bits - http://www.ecst.csuchico.edu/~atman/Crypto/quantum/beyond-bits.html

Center for Quantum Computation - http://www.qubit.org/intros/cryptana.html

Problems with Quantum Cryptography - http://www.ecst.csuchico.edu/~atman/Crypto/quantum/quantum-probs-inf.html

Secure communications using quantum cryptography - http://p23.lanl.gov/Quantum/papers/aerosense.pdf

Quantum Cryptography takes to the Air, Physics World , May 1999 - http://p23.lanl.gov/Quantum/papers.html