Security Implications of Quantum Technologies

Jim Alves-Foss
Center for Secure and Dependable Software
Department of Computer Science
University of Idaho
Moscow, ID 83844-1010
email: jimaf@cs.uidaho.edu

Abstract

Quantum computing, first introduced in the early 70's, has taken on new life with the development of efficient algorithms, experimental quantum communication systems and basic quantum gates. This paper discusses the implications of quantum technologies, including both quantum communication and quantum computing, to the field of computer security. Although classical cryptography and security are still viable technologies, the introduction of quantum technology will force us to reevaluate some of our approaches to security. This paper provides an introduction to those issues that must be reevaluated.

Keywords: Quantum Computing, Cryptography, Security

1 Introduction

Quantum mechanics, since introduced, has provided us with a new look at the physical world. What classically has been seen as a deterministic world, where behavior of particles and systems is well defined, is actually composed of a collection of particles whose behavior is probabilistic. In addition, we can actually never know the true state of a particle since measurement of one aspect of the state may perturb the value of other aspects of the state. This perturbation affect is known as the Heisenburg uncertainty principle and is the basis of some of the security issues presented by quantum communication systems discussed in Section 2.

The probabilistic behavior of a particle of the system is typically modeled as the superposition of a collection of state values and their corresponding probability amplitudes. If a_i is the probability amplitude of state i and S_i is the values of state i, the superposition is represented as:

$$\sum_i a_i \left| S_i \right\rangle$$

where the amplitudes are complex numbers such that $\sum_i |a_i|^2=1$. In a quantum computer, calculations are performed on this superposition by the application of unitary transformations (reversible transformations). The benefit of quantum computation is that we can perform transformations (calculations) on all states simultaneously. The only drawback is that upon measuring the system to obtain a result the probability amplitudes collapse and we are only able to obtain one result per calculation. The result is based on the current probability amplitudes of

the system. For algorithms that involves a large search space with unique answers, such as factoring or cryptanalysis we can obtain answers on a quantum computer much faster than we can on a classical computer. Since the result is based on probability amplitudes, quantum algorithms are usually run a few times to provide a very high probability of obtaining the correct answer. The security ramifications of this are discussed in Section 3.

2 Quantum Communication and Computer Security

This section discusses the use of quantum technology for secure dissemination of information. In this section we assume the existence of two trustworthy parties Alice and Bob and an untrustworthy adversary Eve. In the discussions following, we assume that Alice initiates establish communication with Bob.

2.1 Quantum Key Distribution (a.k.a. Quantum Cryptography)

The central concept behind quantum key distribution is the use of quantum properties of signals to prevent eavesdropping on a message between two parties. The message contains the bits of a one-time pad (a use once encryption key) for secure communication. In general, Alice generates a random stream of bits, encodes them onto a communication channel using quantum techniques and sends the message to Bob. Bob measures the signal and then exchanges information with Alice to determine the key. The strength of this system is based on the fact that we can create quantum signals that consists of a superposition of values. Unless the signal is read correctly, a random value will be read. An exchange based on the approach outlined in [1] occurs as follows:

1. Alice creates photons in one of four non-orthogonal polarization states (e.g., horizontal, vertical, right circular or left circular) and sends them to Bob.
2. Bob measures the signal randomly using one of two bases (either circular or rectilinear).
3. Bob tells Alice which basis he used for each photon
4. Alice tells him which measurements matched the encoding.
5. Alice and Bob keep the data for the correct measurements (e.g., rectilinear has horizontal = 0 and vertical = 1; circular has left circular = 0 and right circular =1).
6. Bob and Alice check for tampering by publicly choosing a random subset of bits and comparing them through a hash or parity checking mechanism.

The strength of this type of scheme is based on the quantum nature of photons, where the measurement of the photon along one basis will result in a random value and will completely destroy the information along the other basis. If Alice encoded along the rectilinear basis and the photon was read on the circular basis, then not only is the resulting value random, but the encoded information lost.

There is no physical method for an eavesdropper to read the message stream without being detected, not even making a copy of the stream, since to make a copy you have to measure along the bases. Thus, the security of this type of key distribution holds.

Of course, there is no authentication in this scheme, so an active eavesdropper, Eve, can intercept all messages, both public and quantum encoded, between Alice and Bob, and insert all of her own messages, pretending to be Bob to Alice and Alice to Bob. No mechanism for authentication has yet been demonstrated for quantum computing systems. There have only been

references to unconditional authentication, with no analysis of the applicability of these approached to quantum technology. This is essential since the existence of a quantum computer will make all current public-key algorithms obsolete.

2.2 Quantum Bit Commitment via Communication

A bit commitment protocol is used to enable Alice to commit to the choice of a value (which could be a single bit or a collection of bits) but keep that choice secret until a later time. One mechanism for this protocol, introduced by Bennett and Brassard [1], involves Alice choosing a bit value and encoding it in an entangled quantum state and sending the encoding to Bob. At some later time Alice declares the choice and provides Bob with sufficient information to decode the quantum state. Bob can then verify Alice's choice. Specifically, Alice takes a random string of bits $R = r_1, \ldots, r_n$ and encodes each bit in one of two bases, rectilinear R_+ if she wants a 0 or diagonal R_x if she wants a 11. Bob selects a random string of bases $b_1,\ldots,b_n \in \{+,x\}^*$ with which he reads *R'*. When Alice wishes to declare her choice of basis she announces the original bit string *R*. Bob can then determine the bit by looking at the bit locations *i* where his *R'* does not match *R*. It is these locations where Bob picked the wrong basis b_i. If all of the locations where $r'_i \neq r_i$ agree on the basis, then Bob interprets this as the correct choice.

Unfortunately, due to the uncertainty nature of quantum mechanics, Alice can always delay her choice until the time she declares it and thus forces Bob to correctly verify that new choice. Specifically, instead of sending a string of random values r_i, Alices sends a string of entangled states (encoded with equal probability in either basis. Prior to revealing her choice she reads the string on the basis according to her current (not original) bit choice. This current value is what she sends to Bob, and given the nature of entangled states, Bob will always have already read the "correct" value for the chosen basis.

Additionally Mayers [4] proved that unconditionally secure quantum bit commitment is not possible using any form quantum encoding to secure the value of the bit. There is a large class of cryptographic algorithms that have been shown to implement bit commitment. Since unconditionally secure quantum bit commitment is impossible using quantum encodings, these cryptographic algorithms must therefore not be realizable using quantum encodings.

2.3 Quantum Encryption via Communication

Data encryption is one use of quantum communication channels that has been suggested. Given that we have quantum key distribution, we can theorize the use of the one-time key to specify a quantum encryption of data. Unfortunately, further exploration shows that quantum communication provides limited benefits to this form of communication.

- One possible approach uses the bits of the key to specify which basis to use to transmit the data. A 1 in the key could specify rectilinear basis, while a 0 in the key could specify circular basis. Unfortunately, this approach is not secure. Although we could detect the presence of Eve as with the key distribution protocol, too much information would be released.

  Assume that Eve randomly chooses a basis for each bit and reads the message using that basis. If Eve was correct in choosing the basis, which occurs with probability 50%, Eve will obtain the correct value. If Eve was incorrect in choosing the basis, she obtains a random value, which is still correct 50% of the time. Standard probability calculations show that Eve obtains the correct value 75% of the time (.5*1 + .5*.5).

- Another more secure approach uses the bits of the key to specify the direction of the encoding in a single basis, where the basis is publicly known. Eve will thus always be correct in choosing the basis and will get the correct value only 50% of the time. This is exactly what classical secure communication does using the one-time pad. Unfortunately, since the basis is publicly known, Eve can retransmit the message completely masking the eavesdropping and thus providing no benefit over the use of classical communication.
- A third approach combines the two above approaches, using one bit of the one-time pad to specify which basis to use and uses the next bit to specify the direction of the encoding. Thus, when Eve selects the correct basis, she will get the correct answer only 50% of the time and her efforts can be detected through selected checksum mechanisms. Although this approach is secure, the additional overhead of two key bits per data bit may be unacceptable.

3 Quantum Computing and Computer Security

Quantum computing is derived via the construction of a quantum computer. That is, a device whose central computation engine is based on the concept of encoding information into quantum states, called *qubits*, or quantum bits. The benefit of such computation is that the values of the qubits are not necessarily fixed, but rather can encode a superposition of states. All operations on a quantum computer can therefore be executed on all states simultaneously.

Quantum computers are still theoretical, as only simple quantum gates have been constructed. Some of the difficulties in constructing large scale quantum computers still have to be overcome. Once these problems are solved the major limitation of the power of the quantum computer will be the number of bits manipulated by the computer. A quantum computer with n bits can manipulate 2^n simultaneous values. However, even with these limitations, it is not inconceivable that complex quantum computers could be constructed within a few decades.

3.1 Quantum Factoring

In [5], Shor energized the quantum computing community by presenting an algorithm that calculates the prime factorization of very large numbers in polynomial time. The algorithm requires a very large number of quantum gate operations for large number of bits in the number to be factored (on the order of hundreds of bits). To factor a number N the algorithm chooses a random number x and calculates $x^r \equiv 1 \bmod N$. Factors of N can now be computed, with high probability, by computing $\gcd(x^{r/2\pm1}, N)$. Of course, finding r is difficult and is at the heart of Shor's solution. First, the algorithm chooses a smooth number (one with small prime factors) $N^2 < q < 2N^2$ and builds the quantum state:

$$\left|\psi_1\right\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \left|a,0\right\rangle$$

This state represents an even probability distribution over q-a values. The algorithm then modifies this distribution to greatly increase the probability of reading the correct result and reducing the probability of reading an incorrect result. To do this, the quantum computer calculates:

$$\left|\psi_2\right\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \left|a, x^a \bmod N\right\rangle$$

from which we get, through application of Fourier transform:

$$\left|\psi_2\right\rangle = \frac{1}{q}\sum_{m=0}^{q-1}\sum_{a=0}^{q-1} e^{i2\pi am/q}\left|m, x^a \bmod N\right\rangle$$

Measuring both arguments of this superposition we obtain $c = m$ and x^k. The measurement gives, with high probability, $c = \lambda q/r$; where λ is an integer. Given q, with a few runs of the algorithm, we can compute r and thus factor N, with high probability. The run-time complexity of this form of quantum factoring is on the order of L^2 where L is the number of bits needed to represent N.

This result (which has been shown to be the optimal result) is tremendously faster than classical factoring techniques and as such places algorithms such as RSA in jeopardy. The only saving grace is that this technique requires a very large number of gates, although slower, less complex implementations may be possible.

3.2 Quantum Code Books

In [3] Brassard discussed the implementation of a quantum phone book. The phone book encodes into the quantum computer all the information in the phone book. The system is initialized and through a series of computations a result emerges. Boyer, et.al. [2] have proven that such an approach requires a minimum of roughly ½√N iterations to search the phone book. Although there are some restrictions on the usefulness of this approach, it is reasonable to assume that one could develop a code-book that can be used to launch a successful known-plaintext attack against an unknown encryption key. The system needs to be designed to implement the encryption algorithm with the input plain-text and output cipher text as parameters of the system. The system then executes the necessary number of iterations until the resulting key is generated. To break a block cipher that enciphers a 64-bit block using a 56-bit key (i.e., DES) would require roughly 2^{27} operations. Given the needs of the quantum computer to have unitary transformations we would need a quantum computer with at least 184-bit capability (64 bits output, 64 bit data input and the 56 bit key). To break the cipher, assuming the ability to calculate 2^{10} operations per second, the computer would require 36 hours. To break a cipher that uses 112 bits (i.e., triple-DES) would require 2^{55} operations, or 2^{45} seconds (1.1 million years). Therefore, it appears that even quantum computers have their limits when applied to use brute force algorithms. Current practice considers 100 bit keys a minimum level for security. A move to 200 bits would ensure security even for quantum computers (an ultra high speed quantum computer, operating at 2^{50} operations per second would still require 17.8 million years to break a cipher that uses a 200 bit key).

3.3 Bit Commitment and Encryption via Computing

The problem with quantum bit commitment, as pointed out by Mayers [4], is that Alice can always delay her choice of the bit until the time she reveals the value. With classical bit commitment, and subsequent communication, there are no probabilities involved. All data values are precise, and security is obtained through the computational infeasibility of breaking the system. Although quantum computers have been shown to be substantially faster than classical computers, there are limits to their computational power. This implies that there must still be a set of algorithms for which bit commitment is computationally secure.

Using quantum computers we can encrypt messages using very complex algorithms. To date no such algorithms have been proposed in the literature. We suspect that an algorithm to implement exponentiation (as used in RSA public key encryption) could execute much faster than current classical computer implementations and may be sufficiently secure so as to be computationally secure even on a large scale quantum computer.

3.4 Quantum Random Number Generator

In classical cryptography there is often a need for the generation of random numbers. There have been numerous reports in the literature of problems associated with the use of pseudo-random number generators that are implemented in software. These generators often exhibit patterns of behavior that can be exploited by an attacker to break the system. This section outlines quantum algorithm that implements a true random number generator.

The quantum search algorithm assumes the ability to generate a quantum state that is an equal superposition of all possible states. The unitary operation *A*:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

transforms a quantum bit |0> into a quantum state where both values |0> and |1> occur with equal probability. A simple random number generator consists of initializing an *n*-bit quantum register to |0>, applying *A* to each of the bits, resulting in the state:

$$\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}\left|x\right\rangle$$

Reading the value from this state gives a resulting value in the range 0, 2^n-1. Each value occurs with equal probability. Thus we get a true uniform *n*-bit random number generator.

4 Conclusions

Quantum computers and quantum communication will affect modern cryptographic systems. In some instances, as we have shown, modern cryptography will have to be either redefined, or at least implemented with a larger key space. However, as with any new technology there are certain approaches to implementing a solution are not appropriate for that technology, as we have seen with quantum encryption. Also, with any secure communication protocol we still need to worry about authentication of the end users. Quantum key distribution is fine, but is limited to non-authenticated key establishment. New algorithms or protocols will have to be developed to establish such authentication.

There is still much research to be done on quantum computing and quantum security to determine the capabilities and limitations of this new and exciting technology. For example it is not known if secure quantum protocols can be realized for coin-tossing or secure multi-party computations.

5 References

[1] C.H. Bennet and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175-179.

[2] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *PhysComp* 96.

[3] G. Brassard. Searching a Quantum Phone Book. *Science* 31, January 1997.

[4] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Letters.*, **78**, 1997, pp. 3414 – 3420.

[5] P.W. Shor. Algorithms for quantum computation: Discrete log and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science*, ed. S. Goldwasser. Nov. 1994, pp. 124-134.