A SURVEY OF QUANTUM AND CLASSICAL CRYPTOGRAPHY

Derrick Chait, Texas A&M University-Corpus Christi
Faculty Advisor: Ahmed Mahdy, Texas A&M University-Corpus Christi

ABSTRACT

Quantum cryptography can be used to unconditionally secure data communications by applying the laws of quantum physics. This is a major breakthrough because the cryptography currently in use, referred to as classical cryptography, relies solely on the hardness of a mathematical equation. The computational security of classical cryptography is being threatened by advances in quantum computing, which in theory can efficiently compute the hard mathematical problems classical cryptography relies on. This paper compares classical cryptography to quantum cryptography and outlines major problems quantum cryptography is currently facing.

INTRODUCTION

Securely transporting messages has been a goal of all major civilizations. The Mesopotamians, ancient Greeks, ancient Chinese, and the Spartans are just a few of the ancient civilizations that used some form of cryptography to keep their messages secret [12]. The ciphers used by these civilizations were advanced at the time, but were certainly not unbreakable. Cryptography has evolved over the years to a much more advanced state that our brains alone are incapable of breaking. The most advanced cryptography to date is quantum cryptography. It was first introduced by Stephen Wiesner in the 1970's, but the paper was not published until 1983 [15]. Quantum cryptography is currently a widely researched topic because of breakthroughs in quantum computing. These breakthroughs in quantum computing threaten the most widely used key distribution systems used today. Classical cryptography is directly affected by these breakthroughs because it relies solely on the hardness of computing a mathematical problem that can not be solved by current computers in polynomial time, but theoretically can be solved on a quantum computer. This realization is what spurred the research in quantum cryptography because quantum cryptography does not rely on computational security, but rather on the laws of quantum physics. This paper will first give a brief history of classical cryptography and discuss the different kinds, then move on to breaking classical cryptography with quantum computers, and finally discuss quantum cryptography. For quantum cryptography we will begin with a brief overview of what it is, then go over the most famous quantum key distribution protocol, next describe what eavesdropping is and how quantum cryptography defends against it, and finally go over practical quantum key distribution systems and the problems that arise.

CLASSICAL CRYPTOGRAPHY

Cryptography manages secret knowledge by taking a message in plaintext and converting it to an unintelligible message to any prying eyes. The need for cryptography is growing exponentially with the number of users that are relying on the internet for a multitude of things, with some of the most prominent uses being E-commerce and online banking. There are a number of security services that should be addressed by cryptography, with the most important being confidentiality, authenticity, and

accountability. Confidentiality protects against unauthorized release of the message, authenticity assures the recipient of the message that the sender is who they say they are, and accountability ensures the sender of the message is accountable for the contents. These goals are achieved by combining a plaintext message with a key and creating cipher text. This cipher text will be unusable to anyone unless they have the key to decode the message.

Classical cryptography systems are based on the NP-hardness of certain mathematical problems, such as factoring two large primes. These problems are said to be trapdoor functions because it is easy to compute the function one way, but extremely taxing to compute the reverse without some special information, known as the trapdoor [8]. Asymmetric cryptography and symmetric cryptography are the two main categories of classical cryptography. Symmetric cryptography, also known as secret key cryptography, uses one secret key for both encryption and decryption. Asymmetric cryptography, also known as public key cryptography, has both a public and a private key, either of which can be used for encryption/decryption [8]. Classical key cryptography relies on the NP-hardness of mathematical problems and does not offer theoretical security, but rather computational security. This poses a great security risk because a breakthrough in mathematics could potentially nullify public key cryptography, which would make transporting symmetric keys with asymmetric cryptography unsecure. This is a major concern considering most e-commerce and authentication services currently implemented use asymmetric cryptography to transfer the secret key to setup a secure connection between a client and a web server.

BREAKING CLASSICAL CRYPTOGRAPHY

Quantum Computers

The most widely used public key system is RSA, which relies on the fact that factoring two large prime numbers is an NP hard problem [1]. Factoring a number that is hundreds of digits long will take millions of years using even the fastest supercomputer. Relying on the hardness of mathematical problems has been the crutch of classical cryptography because whenever computers make gains in terms of computing power, classical cryptography can simply increase the key length, which effectively doubles the key space with each bit. A newly conceived computer, called a quantum computer, uses the laws of quantum physics and could possibly be able to crack any of the most sophisticated encryptions in use today in a year rather than millions of years. The main difference between quantum computers and classical computers is how information is stored. In a normal digital computer, information is stored in a bit and encoded as either a 1 or a 0. This means that an n-length word is stored as an n-length string of either 1's or 0's. Quantum computers on the other hand store information in quantum bits (qubits) which can be in a state of 0, 1, or most importantly exist simultaneously as 0 and 1. This means that n qubits actually requires 2^n numbers [13]. Quantum computers have the ability to be immensely powerful because of two major properties: it can be in multiple states at once as well as act on all of its states simultaneously. A quantum computer, in theory, could perform multiple operations at once on a single processing unit. In November 2007, a company named D-Wave Systems Incorporated unveiled the most

powerful quantum computer to date. The quantum computer contained 28-qubits and was running an image matching application [6].

Shor's Algorithm

Shor's algorithm, proposed by Peter Shor in 1994, is a quantum algorithm used to factor an integer and can be applied to cracking RSA. The first efficient algorithm to attack the factoring of the product of two large prime numbers, Shor's algorithm sparked a great deal of interest among the scientific community in the quantum computing field. Table 1 shows the performance break down of Shor's algorithm versus classical algorithms. To achieve these results, Shor's algorithm breaks down the factoring problem to an order-finding problem because an order finding problem can be computed concurrently. Once it is reduced to an order-find problem, the algorithm uses quantum Fourier transforms to find the period. The Quantum Fourier Transform is the reason for the computational speedup because the problem can be broken up and calculated simultaneously. The Big O of Shor's Algorithm for factoring an integer N is O((log N)^3) time with a O(log N) space[13]. This is a huge accomplishment because on a classical computer there is no algorithm that can solve the factoring problem in polynomial time. Shor's algorithm has been successfully tested on a quantum computer by IBM in 2001, when they factored 15 to find 3 and 5 [5]. The test was a proof of concept and the quantum computer used only contained 7 qubits.

Table 1: Comparison of Shor's algorithm versus other cryptanalysis algorithms [13]

Number of Digits (Public Key Size)	Number of Bits (Approximate)	Timeline	Years to Decipher	Algorithm
120	398	1993	830	Quadratic sieve
129	428	1994	5000	Quadratic sieve
130	431	1996	1000	Generalized number field sieve
140	465	1999	2000	Generalized number field sieve
155	512	1999	8000	Generalized number field sieve
300	1024	Yet to crack	10^11	Generalized number field sieve
300	1024	Yet to crack	10^7	Special number field sieve
300	1024	1994	< 1 second	Shor's algorithm

QUANTUM CRYPTOGRAPHY

Quantum cryptography offers perfectly secure data transmission because it relies on the laws of physics that we believe to be true, rather than relying on an unproven

mathematic problem. The idea was first proposed in the 1970's but was not applied to information security until the early 1990's. Quantum cryptography is only used to solve the key distribution problem, not actually transmit any useful data. It does so by transmitting photons of light through either fiber optics or free space [2]. These photons of light adhere to the Heisenberg uncertainty principle or quantum entanglement. The Heisenberg uncertainty principle is when special information is encoded into the properties of a photon so that any attempt to monitor the photon will change the properties and will be detectable. It relies on quantum theory that suggests certain pairs of physical properties are complementary so that measuring one will change the other. Quantum entanglement is a state of two or more photons that are strongly correlated physically even though they are separated spatially. This means even though they are separated, measurements performed on one system will appear to instantaneously influence the other systems that are strongly correlated [9].

Bennett-Brassard (BB84) Protocol

BB84 was the first quantum key distribution protocol and was developed by Charles Bennett and Gilles Brassard in 1984[3]. Mayer's proof proves that BB84 is unconditionally secure from an attacker that performs any operation allowed under quantum physics [9]. Mayer's proof guarantees the security of BB84 even in the event of a future development in quantum computing, which is a great advantage over all classical key distribution systems. A Vernam one-time pad is most often used in conjunction with the BB84 protocol because the one-time pad is a well known perfectly secure cryptosystem [11][14]. Although BB84 is mathematically proven secure, an implementation of the protocol is not. Problems may arise at the implementation level that will be impossible to foresee in the design level because the protocol may rely on some idealized piece of hardware that simply is not feasible at the time of implementation.

Eavesdropping

Eavesdropping is the act of an unintended receiver intercepting and reading a message between two communicating parties. Preventing eavesdropping is one of the main priorities of any key distribution system and quantum key distribution systems have an advantage. Quantum theory has a principle called the Heisenberg uncertainty principle that guarantees any effort to monitor the communication will disturb it in some detectable way. Although this does not prevent eavesdropping, it will allow the communicating parties to know if someone is eavesdropping. If someone is detected eavesdropping, the communicating parties can disregard the current key and not lose anything significant since it was a randomly generated key [2].

Practical Quantum Cryptography

There are still major problems associated with implementing quantum cryptography protocols. One of the most prominent problems is bit errors. The bit error rate of a quantum key distribution is several percent higher than an optical communication system, which can be devastating in terms of practicality. There is an error correction protocol called CASCADE that can correct the bit errors, but it also

opens the entire system up to new attacks. The problem with CASCADE is there is a chance that a number of the bits of the private key may be leaked to an attacker. One way to nullify these leaked bits is to use a process called privacy amplification. Privacy amplification takes the bit error corrected key and performs a compression function on it [4]. This will guarantee that the bits leaked to an eavesdropper will become useless and that both parties will have the same key. This solves one problem but at the same time it weakens the security of the actual key because it is compressing the number of bits. Another major problem with a practical quantum key distribution system is sending only one photon of light at a time. The only way the Heisenberg uncertainty principle will combat eavesdropping is if only one copy of the photon is sent. In practice, this is one challenge that has faced researchers. The final major problem is the length over which a connection can be made. The longest successful connection was created by NIST/Los Alamos in June 2006 which was recorded at 148.7km [10]. This distance limits the scope at which quantum key distribution systems can be used and until further advancement impedes its deployment in a global environment. One proposed solution to the problem is a quantum repeater that will transfer the state of one photon to another through quantum entanglement. Although quantum repeaters are being heavily researched, no fully functional prototype has yet to be released. In April 2007, physicists demonstrated quantum nodes and quantum channels may be used as segments in a quantum repeater [7].

CONCLUSION

Securing data and data communication is a top priority because the consequences of unsecure data can have grave effects on both the economy and national security. Classical key distribution systems are protected only by the limitations of the currently available computing power. With recent breakthroughs in quantum computing, classical key distribution systems are in danger of becoming entirely obsolete overnight. To combat the breakthroughs in quantum computing, researchers are also making breakthroughs in quantum cryptography that will provide unconditional security. The laws of quantum physics guarantee the security of quantum key distribution systems in theory, but do not guarantee the security of implementing such a system. A few of the problems associated with quantum key distribution completely replacing classical key distribution are as follows: high bit errors during the transfer of the quantum bits, no quantum repeater available so the distance over which communication can happen is too short for our globalized world, and finally sending one photon at a time is a challenge and if it is not met, the security of the system is compromised.

REFERENCES

1. Adleman, L., Rivest, R., Shamir, A., A method for obtaining digital signatures and public key cryptosystems, *Communications of the Association for Computing Machinery*, 21, (2), 120 – 126, 1978.

2. Bennett, C. H., Quantum cryptography using any two non orthogonal states, *Physical Review Letters*, 68, (21), 3121–3124, 1992.

3. Bennett, C. H., Brassard. G., Quantum cryptography: public key distribution and coin tossing, *Proceedings IEEE international conference on computers, systems, and*

signal processing, 175–179, 1984.

4. Bennett, C. H., Brassard, G., Crepeau, C., Maurer, U. M., Generalized privacy amplification, *IEEE Transactions on Information Theory*, 41, (6), 1915 - 1923, 1995.

5. Breyta, G., Chuang, I. L., Sherwood, M. H., Steffen, M., Vandersypen, L. M. K., Yannoni, S., Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, *Nature*, 414, 2001.

6. Burnette, E., D-Wave demonstrates latest quantum computer prototype at SC07, http://blogs.zdnet.com/Burnette/?p=456, 2007.

7. Choi, K. S., Chou, C. W., Deng, H., Felinto, D., Kimble, H. J., Laurat, J., Riedmatten, H., Functional quantum nodes for entanglement distribution over scalable quantum networks, *Science*, 316, (5829), 1316 - 1320, 2007.

8. Diffie, W., Hellman, M.E., New Directions in Cryptography, *IEEE Transactions on Information Theory*, IT-22, (6), 644 – 654, 1976.

9. Goel, R., Garuba, M., Girma, A., Research directions in quantum cryptography, *Information Technology 2007 ITNG '07 Fourth International Conference*, 779-784, 2007.

10. Hiskett, P., Hughes R., Lita, E., Miller A., Nam, S., Miller, A., Nordholt, J., Rosenberg, D., Long-distance quantum key distribution in optical fibre, *New Journal Of Physics*, 8, (193), 2006.

11. Inoue, K., Quantum Key Distribution Technologies, *IEEE journal of selected topics in quantum electronics*, 12, (4), 888 - 896, 2006.

12. Kartalopoulos, S.V., A primer on cryptography in communications, *IEEE Communications Magazine*, 44, (4), 146 - 151, 2006

13. Phaneendra, H.D., Shivakumar, M.S., Vidya, R.C., Quantum algorithms and hard problems, *5th IEEE International Conference on Cognitive Informatics*, 2, 783 -787, 2006

14. Vernam, G.S., Cipher printing telegraph systems for secret wire and radio telegraphic communications, *Journal of the IEEE*, 55, 109 – 115, 1926.

15. Wiesner, S., Conjugate Coding, *Sigact News*, 15, (1), 78 – 88, 1983.