Quantum Encryption - A Means to Perfect Security?

Bruce Auburn

Quantum Encryption – A Means to Perfect Security?

Bruce R. Auburn
GSEC v.1.4b

Introduction

In the past twenty years, the quantum properties of matter and light have been applied to the field of information security. Research has advanced to the point that actual devices using quantum properties are transmitting information over considerable distances. At this time, transmission speeds and hardware expense have generally limited the use of quantum devices to distribute keys rather than entire messages. There is controversy about how secure quantum messages are. It is possible to prove that the probability of message interception by an adversary is arbitrarily small, under ideal conditions. People and machines, however, can never be perfect, so there are many approaches to defeating quantum encryption. Some computer security experts have wondered why making the strongest link in a system even stronger will improve security overall. Since public key cryptography is so hard to decipher now, why spend so much time and money on an even more secure quantum encryption scheme? If deciphering is nearly impossible, why not use other techniques, such as social engineering, to eavesdrop? This paper will attempt to answer those questions.

Quantum Properties Explained

What are quantum properties? A rule called the Heisenberg uncertainty principle says that if you measure one thing, you cannot measure another thing accurately. For example, if you measure the position of an electron flying around an atom, you cannot accurately measure its velocity. If you measure the electron's velocity, you cannot accurately determine its position. If this principle applied to people, you could measure a person's height, but not his weight accurately, and vice versa. The odd thing about the uncertainty principle is that it only becomes true the instant you try to measure something. Until the point of measurement, the person's height and weight would be in an indeterminate, or "fuzzy" state. Fortunately, quantum properties become noticeable only in the realm of very small particles. In practice, these principles have been applied to photons. Photons have wavelike properties and are polarized, or tilted in a certain direction. These properties have been used to produce a powerful new way to encrypt messages that is theoretically unbreakable.

The quantum properties of matter extend through time and space. If a physical process creates a pair of photons, and this pair of photons travels in opposite directions at the speed of light for millions of years, a strange thing happens if one of the photons is examined by a human observer: if the polarity of the observed photon is vertical, the polarization of the photon that is millions of light years away, at the same instant, becomes horizontal. Up to the point of measurement, the polarization of both photons is unknown. It is hard to believe, but the act of measurement will actually cause the other photon to commit to a certain state. Many experiments have proved this concept. Einstein's famous quote, "God does not play dice with the universe" was a comment on the bizarre

effects of quantum mechanics. Even a great physicist like Einstein could not believe in quantum mechanics. Some scientists think that it will be possible in the future to teleport matter, in the manner of Star Trek, using quantum properties.

Quantum properties of matter are so strange that, even decades after their discovery, many scientists have a hard time understanding them. The quantum property of light that excites computer researchers is the fact that it is not possible to tamper with messages sent using light waves without changing the properties of the message. In other words, if a message has been tampered with, the tampering itself will change the message. Thus, quantum properties are ideal for key distribution. If a key has been tampered with, it is simply discarded and a new key sent. Since tampering is always discovered, it is theoretically possible to send a totally secure key over a distance.

Potential Weaknesses in Today's Keys

Why are researchers so interested in quantum properties? Although it is assumed that no one has broken the strongest encryption keys used in commerce and government, there is no guarantee that these keys, based on factoring large numbers, will be secure forever. Currently, very long keys such as 2048-bit keys are thought to be very safe, as it would take millions of years using the most advanced computers to break them. Recently, however, a key using RSA Security's RC5-64 algorithm was broken. A student at Notre Dame University, using 10,000 computers working around the clock for 549 days, broke a 109-bit key (Reuters, Notre Dame). This demonstrates both the difficulty of breaking keys and the fact that they can be broken given enough computer power. Someone may eventually discover a mathematical shortcut that allows rapid factoring of large numbers.

A computer scientist at the Indian Institute of Technology, Manindra Agrawal, recently solved a problem that has baffled mathematicians for centuries: how to tell if a number is prime without performing any factoring (Gomes). This does not mean that large numbers can now be factored easily and that today's encryption schemes can be broken, but solving this problem may open the door for mathematicians to figure out how to factor large numbers. Some mathematicians believe that Agrawal's discovery does not mean that we are any closer to being able to factor large numbers, but others believe that this discovery heralds new advances in the field.

Advances in computer hardware could also be instrumental in breaking keys. It has been shown that a computer utilizing quantum computing methods could quickly factor large numbers. In 1994, Peter Shor of AT&T Laboratories invented a quantum algorithm to quickly factor large numbers (Gottesman). Using such an algorithm on a quantum computer would reduce by many orders of magnitude the time spent to factor a large number. A one-time cipher would still be safe

because the information is totally random. Actual quantum computers may be decades away, but an eavesdropper could save messages containing vital secrets today and decrypt them in the future. As an example, a backwards nation could store encrypted data about weapons systems today, then decrypt the information twenty years later and develop dangerous weapons without doing any research. Many countries will never have the financial means to develop advanced weapons, so stealing information is the only way to build those weapons (Junnarkar).

Cipher History

An unbreakable cipher was invented in 1918 by Gilbert Vernam. It is called the Vernam cipher or one-time pad. The Vernam cipher uses a key that is as long as the message it is encrypting. The encrypted message is then totally random and unbreakable. The drawbacks to this type of encryption are caused by the difficulty of distributing the pads needed to encrypt messages and to the large volume of encryption material needed, since the key has to be as long as the message. Traditionally, couriers or secure communication channels have been used to distribute the one-time pads. The hot line from Washington D.C. to Moscow uses this type of encryption. In the 1940's, Claude Shannon of Bell Laboratories proved that if a key is shorter than the message it encrypts, some information could be inferred about the message. If a one-time key is reused for more than one message, it is possible to gain some knowledge about the messages. American code breakers caught the Russians reusing one-time pads during the Cold War and gained valuable information. Quantum encryption is an excellent means for distributing one-time pads.

Why Quantum Cryptography is So Secure

Quantum cryptography is thought to be secure for three main reasons (Lo). One, the quantum no-cloning theorem states that an unknown quantum state cannot be cloned. Theoretically, messages sent using quantum cryptography would be in an unknown quantum state, so they could not be copied and sent on. Two, in a quantum system, which can be in one of two states, any attempt to measure the quantum state will disturb the system. A quantum message that is intercepted and read by an eavesdropper will become garbled and useless to the intended recipient of the message. Three, the effects produced by measuring a quantum property are irreversible, which means an eavesdropper cannot "put back" a quantum message to its original state. These three properties provide the power of quantum cryptography. No amount of effort or genius can alter the fact that observing a quantum property irrevocably alters the object being observed. It is as if I mail a book to a friend, and someone in the post office opens the package and reads the book, and all of the letters become scrambled and the book is rendered unreadable. Furthermore, the book cannot be put back to the way it was. Now the book is of no use to the recipient, but it can be seen that someone broke into the package. This is why quantum cryptography is so

useful in distributing the keys used to encrypt messages. A lucky eavesdropper could intercept a quantum encrypted message, and if he made the correct measurement for each bit of the message he would have the key, although the likelihood of making the correct measurements is extremely low for longer messages. But keys are random strings of characters, so even a successful eavesdropper could not tell if he had successfully intercepted a key. For all of his work, the eavesdropper is still unsuccessful – he has altered the key by reading it, and the recipient can see that it has been tampered with, and new keys are sent until one is received that has not been tampered with.

Quantum Research History

Although the quantum properties of light and matter were discovered early in the twentieth century, the instruments and techniques necessary to produce and measure quantum states were not available until much later. The first person to write about applying quantum properties as a means of validating physical objects or messages was Stephen Wiesner of Columbia University in 1970. Wiesner proposed a scheme for using quantum properties to print paper money such that the serial numbers could not be duplicated, and another scheme to combine two ordinary messages into an undecipherable quantum message. His ideas were so far ahead of their time that they were not accepted by the publication he submitted them to. In 1983 his paper was finally published, after other researchers had become interested in quantum encryption, and Wiesner's contributions to the field were recognized (Dwyer). In 1979, Bennett and Brassard, who knew of Wiesner's ideas, proposed using quantum properties in conjunction with public key cryptography to produce more secure messages.

Public Key Cryptography

Public key cryptography was invented in the 1970s by Diffie, Hellman and Merkle. It differed from previous encryption systems in that the groups sending messages did not have to agree on a key beforehand. The encryption key is in the public domain, so anyone can encrypt a message, while the related decryption key is held privately so that one person or a trusted group of people are the only ones able to decrypt the message. In 1989, the first fully working prototype of an instrument that encrypted and decrypted quantum messages was produced at the IBM Thomas Watson Research Center. In this case, the information was transmitted over a distance of only a few inches and the transmission rate was very low (Dwyer).

How Quantum Properties of Light are used to Produce Keys

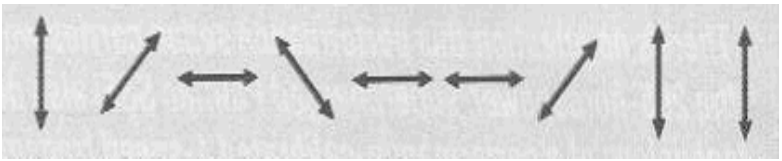
The quantum properties of light can be exploited to send secret messages. Light has wavelike properties, and the waves can be aligned, or polarized, in any direction. Ordinary sunlight consists of varying wavelengths of light (which produce the colors in a rainbow) polarized in a random fashion. Laser light,

however, consists of light of one wavelength that is polarized in one direction. These characteristics are what make lasers so powerful – the individual waves of light, since they are equal, combine to produce one very powerful wave of light. Lasers can be used to produce photons with a given polarization. Polarization can simply be thought of as the "tilt" of the light wave. The following examples will use photons polarized vertically, horizontally, at 45 degrees and 135 degrees, denoted | , —, / and \.

A calcite crystal can be used as a quantum filter. If the crystal is held in a vertical position, photons that are vertically or horizontally polarized (| or —) will pass through the filter unchanged. If a photon that is diagonally polarized (/ or \ ) passes through the vertical filter, however, the polarization will be changed to vertical or horizontal (| or —) in a totally random fashion. Thus, information is lost if the crystal is not aligned correctly, depending on the polarization of the incoming photon. This is what makes it difficult to steal a quantum message without detection. Even though there is a .75 probability of decoding a given bit (or photon), after only 10 bits of message there is only a 5 percent probability that the eavesdropper measured all of the photons correctly. If the eavesdropper then passes on the message to the intended recipient, it is easy to detect that an unauthorized person read the message because the original information and the received information will no longer agree.

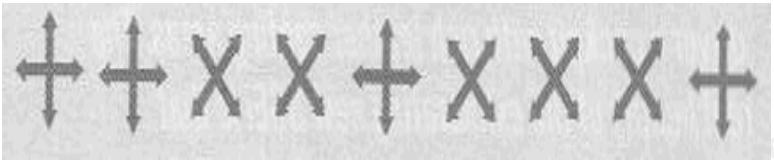
Following is an example of how polarized photons can be used to distribute keys, first proposed by Bennett and Brassard in 1984. In this example, Alice will send a key to Bob, while an eavesdropper named Eve tries to intercept the message. Alice codes the key using photon polarization to denote ones and zeroes. For example, a horizontally polarized photon could stand for a zero, and a vertically oriented photon could stand for a one. The same rule could be applied to the 45 degree and 135 degree photons. Symbolically, — or / equal 0, and | or \ equal 1.

Alice first encodes the key into a string of ones and zeroes. She can choose from one of two polarizations for each one or zero. It is important to note that Alice will use the "—" and "/" polarizations *randomly* to code the zeroes, and likewise the | and / polarizations *randomly* for ones. Thus the binary string "01" could be coded as — |, — \, / | or /\. Because Alice can choose two different polarizations to encode the ones and zeroes, it is hard for Eve to steal the message. If Alice sends a one as a vertically polarized photon, and Eve measures it with a tilted crystal (because Eve is guessing that it has a "/" or "\" polarization), the result Eve gets will be useless because she measured it incorrectly. The diagram below shows how Alice might send a message using the four different polarizations. The binary string sent is '100100011'.

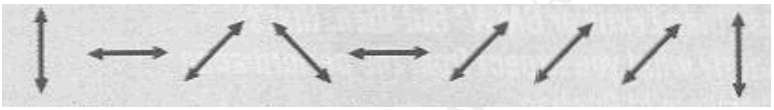


(Dwyer)

For each photon that Alice sends, Bob chooses at random a measurement type: either with the crystal vertical or slanted. The vertical crystal, which will correctly pass the vertical or horizontally polarized photons, is also known as a rectilinear measurement, and is designated as "+". Bob can also tilt the crystal at a 45 or 135-degree angle, which will correctly pass the correspondingly angled photons. This orientation is also called a diagonal measurement, designated "X". Bob's random measurements are shown in the diagram below.


(Dwyer)

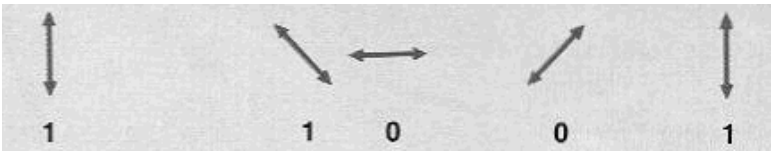
If Bob measures a vertical or horizontal photon with a rectilinear measurement, as in the first measurement in the above diagram, his measurement will be "correct", in that the measurement will not change the polarization. In the second measurement above, Bob makes the wrong measurement, and the 45-degree photon will come through the crystal *randomly* as either a horizontal or vertical photon. Thus, the information for the second bit that Alice sends is irretrievably lost. The following diagram shows the results of Bob's measurements.


(Dwyer)

The next step is for Bob to publicly to announce which measurements he made (*not* the results of the measurements). Alice publicly tells Bob for which photons he made the correct type of measurement. The correct measurements made by Bob are checked below.


(Dwyer)

Bob keeps all of the results for which he has made the correct measurement and discards the rest. Some photons will also be lost because the detectors are not 100% efficient. The remaining ones and zeroes will make up the key, as seen in the next diagram. The ones and zeroes that are left will contain secret information.



(Dwyer)

Testing for Eavesdropping

Alice and Bob can test for eavesdropping by selecting a random subset of results and comparing them. This can be done publicly because this subset will not be used for the key. If Eve has intercepted the message, by the rules of probability she will have made the wrong measurement about half the time, and the photons she sends on to Bob will have a good probability of being wrong. So it is easy to detect eavesdropping in this manner.

In practice, for Bob and Alice to compare bits one by one is fairly inefficient, and there are better ways to detect eavesdropping. One method of detection is to take random subsets of the photons received, for example, photons one, three, five, seven and so on, and add up the quantity of ones in the sample, also known as a parity check. There has to be either an even or an odd number of ones in the sample. It has been proven that if Alice and Bob's parity numbers differ, which means eavesdropping has taken place, that there is a 50% probability that any parity check will detect the eavesdropping. It is easy to use a computer to quickly check thirty subsets, which would yield a 1 in 2^{30} chance of *not* detecting eavesdropping, or about one in a billion.

What Causes Errors Besides Eavesdroppers

Eavesdroppers are not the only reason for transmission errors. This is why the reliability of quantum transmissions cannot be said to be 100% secure, even with parity checking. Transmitting and receiving equipment can introduce errors. The transmission medium, whether air or optical fiber, can also cause errors. Random noise is present in all electronic devices. To hinder interception and possible splitting of light waves, very low levels are used to transmit data – as low as 1/10 of a photon per transmitted bit. These low levels can cause lost bits or reception errors. It is impossible to separate errors introduced by eavesdropping from errors produced by other things. Statistical methods can be used to estimate the number of errors so that only a very small probability remains that information was leaked to an eavesdropper. These statistical

techniques are called privacy amplification, and much research has been done on this subject (Thomson ISI). The advantage of privacy amplification over existing public keys is that the probability of information leakage can be proved to be at a certain level, for example one in a billion, while public keys have never been proven secure. It is just widely believed that no one has learned how to factor large prime numbers yet.

Reducing Effects of Errors

Using a two-step process of error correction and privacy amplification, a known fraction of secure information can be derived from a quantum transmission. This fraction is known as gain. There are four factors involved in gain: the observed error rate, the probability that Alice's source indicated that a valid signal was created, the probability that Alice sent a multi-photon pulse, and the probability that a pulse sent by Alice leads to a successful detection by Bob. These factors are combined into an equation to calculate the gain factor for a given quantum implementation. The equation is beyond the scope of this paper. What is important about the equation is that is possible to derive a reliably secure amount of information from a given transmission and that useful improvements can be made by manipulation the equipment to produce better gain. As an example, it is possible to determine if a signal contains multiple photons. Using this type of detector would allow Alice to not send any information containing multiple photons. Thus the gain, or percentage of secure information transmitted, would increase. The gain equation gives researchers a concrete method to test the security of their implementations (Walton).

Comparing Different Methods of Privacy Amplification

The gain equation was applied to three types of quantum implementations. The first was a weak coherent pulse (WCP), whereby a laser beam is attenuated to produce a very low number of photons per pulse. The second was a correlated photon source (CPS), in which spontaneous parametric down conversion is used to ensure that only single photons are sent. The third method was CPS with a photon-number resolving detector (CPS/PNR), which is a better way to generate single photons than using CPS alone, although this method requires bulky equipment. For the three methods, the best performance over a distance was calculated, with the third method (CPS/PNR) showing the best results. The following chart shows the bits per second rate using the three methods over different transmission mediums (Walton).

	1 Km free space	**50 Km fiber**	**Satellite, low earth orbit**
CPS or WCP	50 kbits/sec	1 bit/second	0 bits/second
CPS/PNR	400 kbits/sec	100 bits/second	100 bits/second

Current Quantum Encryption Distances and Speeds

The state of quantum encryption has reached the point where it is useful in real situations, as opposed to just in laboratories. Recently, teams of British and German researchers sent a key between two mountains in Germany for a distance of 14.5 miles (Reuters, Keys). The Los Alamos National Laboratory is thought to hold the distance record for optical fiber at 30 miles (DeJesus). Current fiber systems are thought to be limited to about 60 miles, which rules out use in a global network. One might think that repeaters could be used to extend the network, but, as stated before, quantum signals cannot be duplicated without changing their properties in some way.

Research is also being conducted to speed up the rate of quantum transmissions. At Northwestern University in Illinois, Prem Kumar and Horace Yuen have used standard lasers and existing optical technology to transmit encrypted data at 250 megabits per second over a fiber optic cable (Junnarkar). These researchers came up with the idea of transmitting photons in bundles, rather than single or fractional photons. It is much easier to detect multiple photons, so inexpensive equipment can be used. It was not stated whether using photon bundles increased the likelihood of eavesdropping. Kumar and Yuen are also working on a technique to amplify the bundles of photons using optical amplifiers, which would allow much greater transmission distances, even to the extent of internet-wide use. This would entail a lot of new equipment, however, as the current Internet transmission medium contains large amounts of copper wire, which cannot pass quantum signals cleanly. It must be stressed that this is a research effort, and current quantum transmissions consist of single or fractional photons.

More Research about Vulnerabilities Needed

The field of quantum encryption is so new that more thought and research has gone into producing quantum transmissions than to what kinds of vulnerabilities may be present. Research is needed to verify the security of quantum transmissions from source to receiver. Optimal attack strategies need to be identified for all types of quantum systems, along with methods for defending against these attacks (Meystre). Error correcting codes and privacy amplification are two methods that have been used, and there are certain to be new strategies invented over time. Considering the massive security holes in today's software, it is evident that security tends to lag behind application and hardware development.

Current quantum systems using as little as .1 photons per bit are thought to be secure, but it has been shown that eavesdropper armed with foreseeable but not currently available technology may be able to successfully intercept these low-level signals (Walton).

Why Encryption does not Ensure Absolute Security

Long encryptions keys might be compared, in military terms, to a mile-high mountain that that has an enemy behind it. The attacking army could go straight over the mountain to reach the enemy, or it might attack by going around the mountain. It has been said that quantum cryptography merely creates a higher mountain, and that the enemy has been concentrating for a long while not on defeating encryption schemes, but in attacking in other ways. Although success in breaking enemy codes during World War II by the United States were instrumental in winning the war, encryption has advanced to the point that other means may be necessary to find out what the enemy is doing. The best way to get around encryption systems may be to exploit human weaknesses, also known as social engineering.

Social Engineering Techniques

If a bank had a vault of six-foot thick steel, would it make sense to cut through it with torches or to try to blow it up? It might make more sense for a robber to convince the bank owner to open up the vault for him. Of course, the robber may have to use violent means to convince someone to open the vault, but such action must be expected from the criminal element. In a similar manner, it is usually easier to break into any organization from the inside. Passwords are easily stolen by rummaging around employees' desks. Many people write their passwords down and hide them under their keyboards. Many other people will tell their passwords to somebody on the telephone impersonating an executive or a technical person. Password files can be stolen and password-cracking programs applied to the files. It is often easy to guess a password, given the tendency of people to use the names of their children or pets. The quantum key that was so painstakingly created and transmitted from Alice to Bob in the previous example could reside on somebody's networked computer, vulnerable to an attacker using a stolen password.

What if Alice was having financial difficulties and an adversary knew about it? Alice could simply be paid off, and no amount of quantum cryptographic techniques would be of help. Alice would simply sell the key and it would be in the hands of the enemy. This happens all of the time in the spy business. During the cold war between the Soviet Union and the United States, a brilliant means was devised for tapping into Soviet oceanic cables used for communication between various Russian naval installations. American submarines located Russian cables buried in the Barents Sea, fastened a large tap around the cable and recorded the plain and encrypted transmissions. This was very successful for a time, but an American named Aldrich Ames sold out to the Russians, which rendered much of the American effort useless.

Blackmail is another means that spies use to gather information. A person is put into a compromising situation, which is then recorded and used to convince the person to perform unsavory acts, such as treason. It has been proposed that J. Edgar Hoover, the longtime head of the F.B.I., neither acknowledged the existence of the Mafia nor did much about it because some compromising photographs existed.

Miniature cameras have become small enough to be hidden almost anywhere. Alice may be sending Bob a message using a quantum key that has perfect security, but the camera could simply record Alice typing a message to Bob before the encryption had a chance to be applied. Keyboards themselves generate signals that can be tapped. Americans in general are not known for their security consciousness. We have a history of losing important scientific and nuclear secrets that have been useful to our enemies.

Quantum keys must be stored safely or they are not effective. No means for ensuring total security have yet been found. In theory, quantum entanglement has been proposed as a solution. This is a method that could use pairs of photons generated at the same time, where one photon is not read until the key is needed, thus ensuring that the other photon, which was used to generate the key, had not been tampered with. Unfortunately, no method of storing photons has been found where quantum states can be preserved for more than a fraction of a second.

In summary, quantum techniques should meet the encryption needs of users, perhaps indefinitely. It is uncertain if or when someone will discover a fast way to factor large numbers. It is equally important to look at the human weaknesses inherent in any system and try to eliminate them as much as possible.

References

BBN Technologies. "Quantum Cryptography." URL: http://www.bbn.com/networking/quantumcryptography.html (21 Oct. 2002).

DeJesus, Edmund X. "Quantum Leap." Information Security Online. Aug. 2001. URL: http://www.infosecuritymag.com/articles/august01/features_crypto.shtml (10 Nov. 2002).

Dwyer, Jeffrey. "Quantum Cryptography." URL: http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum1.htm (23 Oct. 2002).

Fisher, Dennis. "Turning the Key on Data." eWEEK Magazine 18 Nov. 2002: 89

Gomes, Lee. "A Beautiful Mind from India is putting the Internet on Alert." Wall Street Journal Online. 4 Nov. 2002. URL: http://www.iitbombay.org/misc/press/wsj100402.htm (13 Jan. 2003).

Gottesman, Daniel & Lo, Hoi-Kwong. "From Quantum Cheating to Quantum Security." Physics Today. Nov. 2000. URL: http://www.aip.org/web2/aiphome/pt/vol-53/iss-11/p22.html (29 Oct. 2002).

Junnarkar, Sandeep. "Noisy Light is New Key to Encryption." CNET News Online. 15 Nov. 2002. URL: http://news.com.com/2100-1001-965957.html?tag=fd_top (10 Dec. 2002).

Lo, Hoi-Kwong. "Quantum Cryptology." Hewlett-Packard Labs. 17 Nov. 1997. URL: http://fog.hpl.external.hp.com/techreports/97/HPL-97-151.pdf (12 Dec. 2002).

Meystre, Pierre. "Future Issues in Theoretical Quantum Cryptography." 15 Feb 1995. URL: http://www.aro.army.mil/phys/proceed.htm#Future%20Issues (10 Nov. 2002).

Reuters Group PLC. "Keys for Deciphering Code Sent Record Distance." 2 Oct. 2002. Technology News – Reuters. URL: http://emoglen.law.columbia.edu/CPC/archive/crypto/news_article%5BStoryID=1526934%5D.html (13 Jan. 2003).

Reuters Group PLC. "Notre Dame Math Whiz Cracks Certicom Code Contest." The Mercury News Online. 6 Nov. 2002. URL: http://zdnet.com.com/2100-1104-964798.html (10 Dec. 2002).

Thomson ISI. “Quantum Privacy Amplification and the Security of Quantum Cryptography Over Noisy Channels.” 31 May 2001. URL: http://www.esi-topics.com/enc/interviews/Dr-David-Deutsch.html (17 Dec. 2002).

Walton, Z., et al. “Performance of Photon-Pair Quantum Key Distribution Systems.” URL: http://arxiv.org/PS_cache/quant-ph/pdf/0103/0103145.pdf (10 Dec. 2002).