

CONTENTS

1. Introduction
2. Introduction to Quantum Computing
3. Qubits
4. History of cryptography.
5. Quantum cryptography
6. Difference between traditional and quantum cryptography
7. Quantum data representation.
8. Quantum key distribution.
9. BB-protocol.
10. Ekerts protocol.
11. Advantages and disadvantages.
12. Conclusion
13. References.

INTRODUCTION

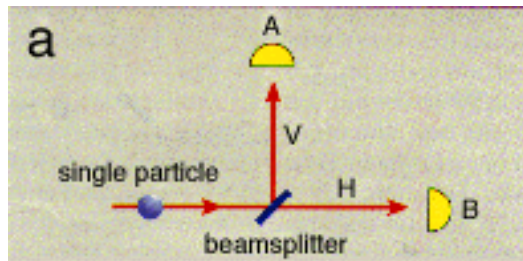
During the 20th century and a half, the contest between codemakers and code breakers has undergone reversals and complications. An unbreakable cipher was invented in 1918, although its unbreakability was not proved until the 1940s. This cipher was rather impractical because it required the sender and receiver to agree beforehand on a key - a large stockpile of secret random digits, some of which were used up each time a secret message was transmitted. More practical ciphers with short, reusable keys, or no secret key at all, were developed in the 1970s, but to this day they remain in a mathematical limbo, having neither been broken nor proved secure. A recent unexpected development is the use of quantum mechanics to perform cryptographic feats unachievable by mathematics alone. Quantum cryptographic devices typically employ individual photons of light and take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement. Eavesdropping on a quantum communications channel therefore causes an unavoidable disturbance, alerting the legitimate users. Quantum cryptography exploits this effect to allow two parties who have never met and who share no secret information beforehand to communicate in absolute secrecy under the nose of an adversary.

Introduction to Quantum Computer?

Behold your computer. Your computer represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage (1791-1871) and eventual creation of the first computer by German engineer Konrad Zuse in 1941. Surprisingly however, the high speed modern computer sitting in front of you is

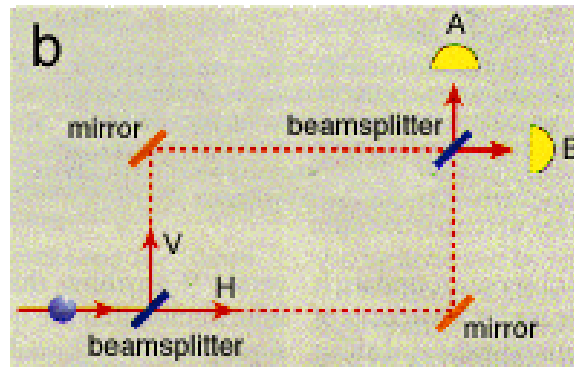
fundamentally no different from its gargantuan 30 ton ancestors, which were equipped with some 18000 vacuum tubes and 500 miles of wiring! Although computers have become more compact and considerably faster in performing their task, the task remains the same: to manipulate and interpret an encoding of binary bits into a useful computational result. A bit is a fundamental unit of information, classically represented as a 0 or 1 in your digital computer. Each classical bit is physically realized through a macroscopic physical system, such as the magnetization on a hard disk or the charge on a capacitor. A document, for example, comprised of n -characters stored on the hard drive of a typical computer is accordingly described by a string of $8n$ zeros and ones. Herein lies a key difference between your classical computer and a quantum computer. Where a classical computer obeys the well understood laws of classical physics, a quantum computer is a device that harnesses physical phenomenon unique to quantum mechanics (especially quantum interference) to realize a fundamentally new mode of information processing.

In a quantum computer, the fundamental unit of information (called a quantum bit or qubit), is not binary but rather more quaternary in nature. This qubit property arises as a direct consequence of its adherence to the laws of quantum mechanics which differ radically from the laws of classical physics. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical bit, but also in states corresponding to a blend or superposition of these classical states. In other words, a qubit can exist as a zero, a one, or simultaneously as both 0 and 1, with a numerical coefficient representing the probability for each state. This may seem counterintuitive because everyday phenomenon are governed by classical physics, not quantum mechanics -- which takes over at the atomic level. This rather difficult concept is perhaps best explained through an experiment. Consider figure a below:



Here a light source emits a photon along a path towards a half-silvered mirror. This mirror splits the light, reflecting half vertically toward detector A and transmitting half toward detector B. A photon, however, is a single quantized packet of light and cannot be split, so it is detected with equal probability at either A or B. Intuition would say that the photon randomly leaves the mirror in either the vertical or horizontal direction. However, quantum mechanics predicts that the photon actually travels both paths simultaneously! This is more clearly demonstrated in figure b.

In an experiment like that in figure a, where a photon is fired at a half-silvered mirror, it can be shown that the photon does not actually split by verifying that if one detector registers a signal, then no other detector does. With this piece of information, one might think that any given photon travels either vertically or horizontally, randomly choosing between the two paths. However, quantum mechanics predicts that the photon actually travels both paths simultaneously, collapsing down to one path only upon measurement. This effect, known as single-particle interference, can be better illustrated in a slightly more elaborate experiment, outlined in figure b below:



In this experiment, the photon first encounters a half-silvered mirror, then a fully silvered mirror, and finally another half-silvered mirror before reaching a detector, where each half-silvered mirror introduces the probability of the photon traveling down one path or the other. Once a photon strikes the mirror along either of the two paths after the first beam splitter, the arrangement is identical to that in figure a, and so one might hypothesize that the photon will reach either detector A or detector B with equal probability. However, experiment shows that in reality this arrangement causes detector A to register 100% of the time, and never at detector B! How can this be?

Figure b depicts an interesting experiment that demonstrates the phenomenon of single-particle interference. In this case, experiment shows that the photon always reaches detector A, never detector B! If a single photon travels vertically and strikes the mirror, then, by comparison to the experiment in figure a, there should be an equal probability that the photon will strike either detector A or detector B. The same goes for a photon traveling down the horizontal path. However, the actual result is drastically different. The only conceivable conclusion is therefore that the photon somehow traveled both paths simultaneously, creating an interference at the point of intersection that destroyed the possibility of the signal reaching B. This is known as

quantum interference and results from the superposition of the possible photon states, or potential paths. So although only a single photon is emitted, it appears as though an identical photon exists and travels the 'path not taken,' only detectable by the interference it causes with the original photon when their paths come together again. If, for example, either of the paths are blocked with an absorbing screen, then detector B begins registering hits again just as in the first experiment! This unique characteristic, among others, makes the current research in quantum computing not merely a continuation of today's idea of a computer, but rather an entirely new branch of thought. And it is because quantum computers harness these special characteristics that gives them the potential to be incredibly powerful computational devices.

The Potential and Power of Quantum Computing

In a traditional computer, information is encoded in a series of bits, and these bits are manipulated via Boolean logic gates arranged in succession to produce an end result. Similarly, a quantum computer manipulates qubits by executing a series of quantum gates, each a unitary transformation acting on a single qubit or pair of qubits. In applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits in some initial state. The qubits can then be measured, with this measurement serving as the final computational result. This similarity in calculation between a classical and quantum computer affords that in theory, a classical computer can accurately simulate a quantum computer. In other words, a classical computer would be able to do anything a quantum computer can. So why bother with quantum computers? Although a classical computer can theoretically simulate a quantum computer, it is incredibly inefficient, so much so that a classical computer is effectively incapable of performing many tasks that a quantum computer could perform with ease. The simulation of a

quantum computer on a classical one is a computationally hard problem because the correlations among quantum bits are qualitatively different from correlations among classical bits, as first explained by John Bell. Take for example a system of only a few hundred qubits, this exists in a Hilbert space of dimension $\sim 10^90$ that in simulation would require a classical computer to work with exponentially large matrices (to perform calculations on each individual state, which is also represented as a matrix), meaning it would take an exponentially longer time than even a primitive quantum computer.

Richard Feynman was among the first to recognize the potential in quantum superposition for solving such problems much much faster. For example, a system of 500 qubits, which is impossible to simulate classically, represents a quantum superposition of as many as 2500 states. Each state would be classically equivalent to a single list of 500 1's and 0's. Any quantum operation on that system --a particular pulse of radio waves, for instance, whose action might be to execute a controlled-NOT operation on the 100th and 101st qubits-- would simultaneously operate on all 2500 states. Hence with one fell swoop, one tick of the computer clock, a quantum operation could compute not just on one machine state, as serial computers do, but on 2500 machine states at once! Eventually, however, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. The reason this is an exciting result is because this answer, derived from the massive quantum parallelism achieved through superposition, is the equivalent of performing the same operation on a classical super computer with $\sim 10^{15}0$ separate processors (which is of course impossible)!!

Early investigators in this field were naturally excited by the potential of such immense computing power, and soon after realizing its potential, the hunt was on to find something interesting for a quantum

computer to do. Peter Shor, a research and computer scientist at AT&T's Bell Laboratories in New Jersey, provided such an application by devising the first quantum computer algorithm. Shor's algorithm harnesses the power of quantum superposition to rapidly factor very large numbers (on the order ~10200 digits and greater) in a matter of seconds. The premier application of a quantum computer capable of implementing this algorithm lies in the field of encryption, where one common (and best) encryption code, known as RSA, relies heavily on the difficulty of factoring very large composite numbers into their primes. A computer which can do this easily is naturally of great interest to numerous government agencies that use RSA -- previously considered to be "uncrackable" -- and anyone interested in electronic and financial privacy.

Encryption, however, is only one application of a quantum computer. In addition, Shor has put together a toolbox of mathematical operations that can only be performed on a quantum computer, many of which he used in his factorization algorithm. Furthermore, Feynman asserted that a quantum computer could function as a kind of simulator for quantum physics, potentially opening the doors to many discoveries in the field. Currently the power and capability of a quantum computer is primarily theoretical speculation; the advent of the first fully functional quantum computer will undoubtedly bring many new and exciting applications.

A Brief History of Quantum Computing

The idea of a computational device based on quantum mechanics was first explored in the 1970's and early 1980's by physicists and computer scientists such as Charles H. Bennett of the IBM Thomas J. Watson Research Center, Paul A. Benioff of Argonne National Laboratory in Illinois, David Deutsch of the University of Oxford, and the late Richard P. Feynman of the California Institute of Technology (Caltech). The idea emerged when scientists were pondering

the fundamental limits of computation. They understood that if technology continued to abide by Moore's Law, then the continually shrinking size of circuitry packed onto silicon chips would eventually reach a point where individual elements would be no larger than a few atoms. Here a problem arose because at the atomic scale the physical laws that govern the behavior and properties of the circuit are inherently quantum mechanical in nature, not classical. This then raised the question of whether a new kind of computer could be devised based on the principles of quantum physics.

Feynman was among the first to attempt to provide an answer to this question by producing an abstract model in 1982 that showed how a quantum system could be used to do computations. He also explained how such a machine would be able to act as a simulator for quantum physics. In other words, a physicist would have the ability to carry out experiments in quantum physics inside a quantum mechanical computer.

Later, in 1985, Deutsch realized that Feynman's assertion could eventually lead to a general purpose quantum computer and published a crucial theoretical paper showing that any physical process, in principle, could be modeled perfectly by a quantum computer. Thus, a quantum computer would have capabilities far beyond those of any traditional classical computer. After Deutsch published this paper, the search began to find interesting applications for such a machine.

Unfortunately, all that could be found were a few rather contrived mathematical problems, until Shor circulated in 1994 a preprint of a paper in which he set out a method for using quantum computers to crack an important problem in number theory, namely factorization. He showed how an ensemble of mathematical operations, designed specifically for a quantum computer, could be organized to enable a such a machine to factor huge numbers extremely rapidly,

much faster than is possible on conventional computers. With this breakthrough, quantum computing transformed from a mere academic curiosity directly into a national and world interest.

Obstacles and Research

The field of quantum information processing has made numerous promising advancements since its conception, including the building of two- and three-qubit quantum computers capable of some simple arithmetic and data sorting. However, a few potentially large obstacles still remain that prevent us from "just building one," or more precisely, building a quantum computer that can rival today's modern digital computer. Among these difficulties, error correction, decoherence, and hardware architecture are probably the most formidable. Error correction is rather self explanatory, but what errors need correction? The answer is primarily those errors that arise as a direct result of decoherence, or the tendency of a quantum computer to decay from a given quantum state into an incoherent state as it interacts, or entangles, with the state of the environment. These interactions between the environment and qubits are unavoidable, and induce the breakdown of information stored in the quantum computer, and thus errors in computation. Before any quantum computer will be capable of solving hard problems, research must devise a way to maintain decoherence and other potential sources of error at an acceptable level. Thanks to the theory (and now reality) of quantum error correction, first proposed in 1995 and continually developed since, small scale quantum computers have been built and the prospects of large quantum computers are looking up. Probably the most important idea in this field is the application of error correction in phase coherence as a means to extract information and reduce error in a quantum system without actually measuring that system. In 1998, researches at Los Alamos National Laboratory and MIT led by Raymond Laflamme managed to spread a single bit of quantum information

(qubit) across three nuclear spins in each molecule of a liquid solution of alanine or trichloroethylene molecules. They accomplished this using the techniques of nuclear magnetic resonance (NMR). This experiment is significant because spreading out the information actually made it harder to corrupt. Quantum mechanics tells us that directly measuring the state of a qubit invariably destroys the superposition of states in which it exists, forcing it to become either a 0 or 1. The technique of spreading out the information allows researchers to utilize the property of entanglement to study the interactions between states as an indirect method for analyzing the quantum information. Rather than a direct measurement, the group compared the spins to see if any new differences arose between them without learning the information itself. This technique gave them the ability to detect and fix errors in a qubit's phase coherence, and thus maintain a higher level of coherence in the quantum system. This milestone has provided argument against skeptics, and hope for believers. Currently, research in quantum error correction continues with groups at Caltech (Preskill, Kimble), Microsoft, Los Alamos, and elsewhere.

At this point, only a few of the benefits of quantum computation and quantum computers are readily obvious, but before more possibilities are uncovered theory must be put to the test. In order to do this, devices capable of quantum computation must be constructed. Quantum computing hardware is, however, still in its infancy. As a result of several significant experiments, nuclear magnetic resonance (NMR) has become the most popular component in quantum hardware architecture. Only within the past year, a group from Los Alamos National Laboratory and MIT constructed the first experimental demonstrations of a quantum computer using nuclear magnetic resonance (NMR) technology. Currently, research is underway to discover methods for battling the destructive effects of decoherence, to develop an optimal hardware architecture for designing and building a quantum computer, and to further uncover quantum algorithms to

utilize the immense computing power available in these devices. Naturally this pursuit is intimately related to quantum error correction codes and quantum algorithms, so a number of groups are doing simultaneous research in a number of these fields. To date, designs have involved ion traps, cavity quantum electrodynamics (QED), and NMR. Though these devices have had mild success in performing interesting experiments, the technologies each have serious limitations. Ion trap computers are limited in speed by the vibration frequency of the modes in the trap. NMR devices have an exponential attenuation of signal to noise as the number of qubits in a system increases. Cavity QED is slightly more promising; however, it still has only been demonstrated with a few qubits. Seth Lloyd of MIT is currently a prominent researcher in quantum hardware. The future of quantum computer hardware architecture is likely to be very different from what we know today; however, the current research has helped to provide insight as to what obstacles the future will hold for these devices.

Future Outlook

At present, quantum computers and quantum information technology remains in its pioneering stage. At this very moment obstacles are being surmounted that will provide the knowledge needed to thrust quantum computers up to their rightful position as the fastest computational machines in existence. Error correction has made promising progress to date, nearing a point now where we may have the tools required to build a computer robust enough to adequately withstand the effects of decoherence. Quantum hardware, on the other hand, remains an emerging field, but the work done thus far suggests that it will only be a matter time before we have devices large enough to test Shor's and other quantum algorithms. Thereby, quantum computers will emerge as the superior computational devices at the very least, and perhaps one day make today's modern computer obsolete. Quantum computation has its origins in highly specialized fields of

theoretical physics, but its future undoubtedly lies in the profound effect it will have on the lives of all mankind.

Qubits

The first step for implementing QIP is to have a physical system that can carry quantum information. The preferred system for realizing

qubits in liquid-state NMR consists of spin- $\frac{1}{2}$ nuclei, which are naturally equivalent to qubits. The nuclear-spin degree of freedom of a

spin- $\frac{1}{2}$ nucleus defines a quantum mechanical two-state system. Once the direction along the strong external magnetic field is fixed, its state space consists of the superpositions of "up" and "down" states. That is, we can imagine that the nucleus behaves somewhat like a small magnet, with a definite axis, which can point either "up" (logical state

$|0\rangle$) or "down" (logical state $|1\rangle$). By the superposition principle, every

quantum state of the form $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ is a

possible (pure) state for the nuclear spin. In the external magnetic field, the two logical states have different energies. The energy difference

results in a time evolution of $|\psi_0\rangle$ given by

The constant ω is the precession frequency of the nuclear spin in the external magnetic field in units of radians per second if t is in seconds. The frequency is proportional to the energy difference ϵ between the

"up" and "down" states:
$$\omega = 2\pi\epsilon/\hbar$$
, where \hbar is Planck's constant.

Although a spin- $\frac{1}{2}$ nucleus' state space is the same as that of a qubit, the precession implies that the state is not constant. We would like the realization of a qubit to retain its state over time when we are not intentionally modifying it. For this reason, in the next section, the qubit state realized by the nuclear spin will be defined so as to compensate for the precession.

Precession frequencies for nuclear spins can vary substantially depending on the nuclei's magnetic moments. For example, at **11.7T**, the precession frequency for protons is **500Mhz** and for ^{13}C it is **125Mhz**. These frequency differences are exploited in measurement and control to distinguish between the types of nuclei. The effective magnetic field seen by nuclear spins also depends on their chemical environment. This dependence causes small variations in the spins' precession frequencies that can be used to distinguish, for example, the two ^{13}C nuclei in TCE: The frequency difference (called the "chemical shift") is **600- 900Hz** at **11.7T**, depending on the solvent, the temperature and the TCE concentration.

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Using the Pauli matrix σ_z , the time evolution can be

expressed as $|\psi_t\rangle = e^{i\omega\sigma_z t/2}|\psi_0\rangle$. The operator $\omega\sigma_z/2$ is the internal Hamiltonian (that is, the energy observable, in units for which $\hbar/(2\pi) = 1$) of the nuclear spin. The direction of the external magnetic

field determines the z -axis. Given a choice of axes, the idea that a

single nuclear spin- $\frac{1}{2}$ has a spin direction (as would be expected for a tiny magnet) can be made explicit by means of the Bloch sphere

representation of a nuclear spin's state (Fig. 3). The Pauli matrix σ_z can be thought of as the observable that measures the nuclear spin along

the z -axis. Observables for spin along the x - and y -axis are given by

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

the other two Pauli matrices and

Given a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ of the nuclear spin, one can form the

density matrix $|\psi\rangle\langle\psi|$ and express it in the form

$$\vec{c} = (\alpha_x, \alpha_y, \alpha_z)$$

The vector then is a point on the unit sphere in three-dimensional space. Conversely, every point on the unit sphere corresponds to a pure state of the nuclear spin. The representation also works for "mixed" states, which correspond to points in the interior of the sphere. As a representation of spin states, the unit sphere is called the "Bloch sphere". Because quantum evolutions of a spin correspond to rotations of the Bloch sphere, this sphere is a useful tool for thinking about one- and sometimes about two-qubit processes.

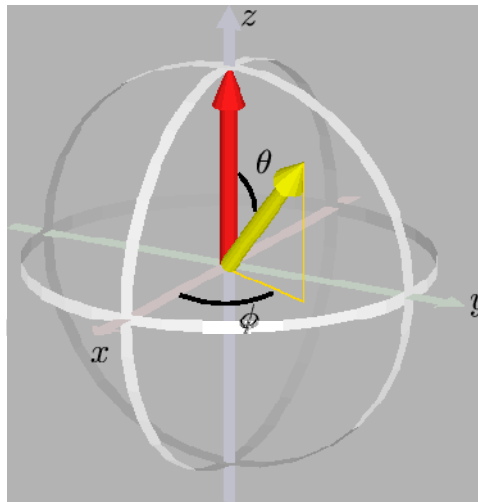


FIG. 3: Bloch sphere representation of a qubit state. The yellow arrow represents a pure state $|\psi\rangle$ for the qubit or nuclear spin- $\frac{1}{2}$. The Euler angles are indicated and determine the state according to the formula

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$$

. The red arrow along the z -axis indicates the orientation of the magnetic field and the vector for $|0\rangle$. If

we write the state as a density matrix ρ and expand it in terms of Pauli matrices,

$$\rho = |\psi\rangle\langle\psi| = (\mathbb{1} + x\sigma_x + y\sigma_y + z\sigma_z)/2$$

$$= \frac{1}{2} (\mathbb{1} + \sin(\theta) \cos(\phi) \sigma_x + \sin(\theta) \sin(\phi) \sigma_y + \cos(\theta) \sigma_z), \quad (3)$$

then the coefficients $(x, y, z) = (\sin(\theta) \cos(\phi), \sin(\theta) \sin(\phi), \cos(\theta))$ of the Pauli matrices form the vector for the state. For a pure state this vector is on the surface of the unit sphere, and for a mixed state, it is inside the unit sphere. The Pauli matrices are associated with spin observables in the laboratory frame, so that all axes of the representation are meaningful with respect to real space.

HISTORY OF CRYPTOGRAPHY

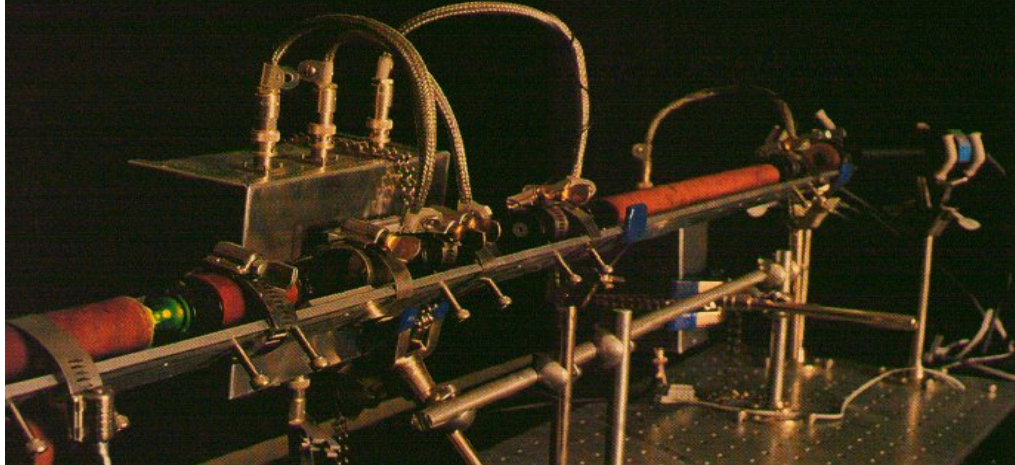
The art of cryptography began at least 2,500 years ago and has played an important role in history ever since. Perhaps one of the most famous cryptograms, the Zimmerman Note propelled the U.S. into World War I. When the cryptogram was broken in 1917. Around this time Gilbert S. Vernam of American Telephone and Telegraph Company and Major Joseph O. Mauborgne of the U.S. Army Signal Corps developed the first truly unbreakable code called the Vernam cipher. One distinctive feature of the code is its need for a key that is as long as the message being transmitted and is never reused to send another message. (The Vernam cipher is also known as the one-time pad from the practice of furnishing the key to spies in the form of a tear-off pad, each sheet of which was to be used once and then carefully destroyed.) The discovery of the Vernam cipher did not create much of a stir at the time, probably because the cipher's unbreakability was not definitively proved until later and because its massive key requirements made it impractical for general use. Because of this limitation, soldiers and diplomats continued to rely on weaker ciphers using shorter keys. Academic interest in cryptology grew more intense in the mid-1970s,

when Whitfield Diffie, Martin E. Hellman and Ralph C. Merkle, then at Stanford University, discovered the principle of public-key cryptography (PKC). Soon afterward, in 1977, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, then at the Massachusetts Institute of Technology, devised a practical implementation the RSA algorithm.

QUANTUM CRYPTOGRAPHY

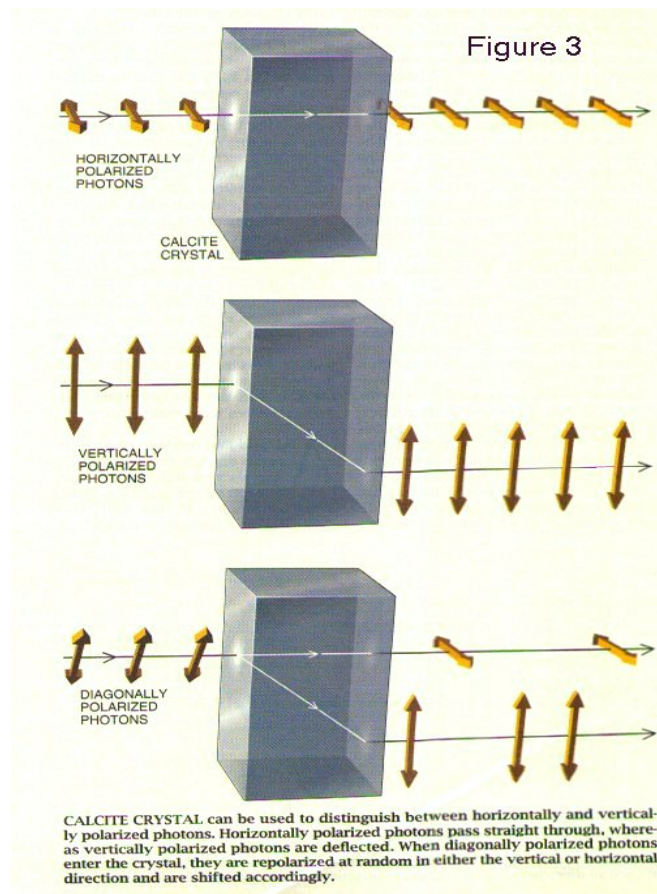
Several years before the discovery of public-key cryptography, another striking development had quietly taken place: the union of cryptography with quantum mechanics. Around 1970 Stephen J. Wiesner, then at Columbia University, wrote a paper entitled "Conjugate Coding," explaining how quantum physics could be used, at least in principle, to accomplish two tasks that were impossible from the perspective of classical physics. One task was a way to produce bank notes that would be physically impossible to counterfeit. The other was a scheme for combining two classical messages into a single quantum transmission from which the receiver could extract either message but not both. Unfortunately, Wiesner's paper was rejected by the journal to which he sent it, and it went unpublished until 1983. Meanwhile, in 1979, two of us (Bennett and Brassard) who knew of Wiesner's ideas began thinking of how to combine them with public-key cryptography. We soon realized that they could be used as a substitute for PKC: two users, who shared no secret initially, could communicate Secretly, but now with absolute and provable security, barring violations of accepted physical laws.

Quantum device generates & measures faint flashes of polarized light, providing a secure way to transmit information. On average, each flash consists of one tenth of a photon.



Our early quantum cryptographic schemes, developed between 1982 and 1984, were somewhat impractical, but refinements over the next few years culminated in the building of a fully working prototype at the IBM Thomas J. Watson Research Center in 1989. John Smolin, now at the University of California at Los Angeles, helped to build the electronics and optics for the apparatus, and Francois Bessette and Louis Salvail of the University of Montreal assisted in writing the software. At about the same time, the theoretical ideas of David Deutsch of the University of Oxford led one of us (Ekert) to conceive of a slightly different cryptosystem based on quantum correlation's. In early 1991, utilizing ideas conceived by Massimo Palma of the University of Palermo, John Rarity and Paul Tapster of the British Defense Research Agency started experiments implementing Ekert's cryptosystem. Quantum theory, which forms the basis for quantum cryptography. Quantum theory is believed to govern all objects, large and small, but its consequences are most conspicuous in microscopic systems such as individual atoms or subatomic particles. The act of measurement is an integral part of quantum mechanics, not just a passive, external process as in classical physics. So it is possible to design a quantum channel – one that carries signals based on quantum phenomena - in such a way that any effort to monitor the channel necessarily disturbs the signal in some detectable way. The effect arises because in quantum

theory, certain pairs of physical properties are complementary in the sense that measuring one property necessarily disturbs the other. This statement, known as the Heisenberg uncertainty principle, does not refer merely to the limitations of a particular measurement technology: it holds for all possible measurements. The uncertainty principle can be applied to design a completely secure channel based on the quantum properties of light. The smallest unit or quantum, of light is the photon, which can be thought of as a tiny, oscillating electric field.



To construct a quantum channel, one needs a polarizing filter or other means for the sender to prepare photons of selected polarizations and a way for the receiver to measure the polarization of the photons.

The latter job could be accomplished by another polarizing filter, which would absorb some of the photons crossing it. But the task is most conveniently done by a birefringent crystal (such as calcite), which sends incident photons, depending on their polarization, into one of two paths without absorbing any [see fig-3]. A photon encountering a calcite crystal behaves in one of two ways depending on its polarization in relation to the crystal. The photon may pass straight through the crystal and emerge polarized perpendicular to the crystal's optic axis, or it may be shifted and emerge polarized along that axis. If the photon entering the crystal is already polarized in one of these two directions, it will undergo no change of polarization but will be deterministically routed into the straight or shifted path, respectively. If a photon polarized at some intermediate direction enters the crystal, however, it will have some probability of going into each beam and will be repolarized according to which beam it goes into, forgetting its original polarization. The most random behavior occurs when the photon is polarized halfway between these two directions, that is, at 45 or 135 degrees. Such photons are equally likely to go into either beam, revealing nothing about their original polarization and losing all memory of it. Suppose Bob is told in advance that a given photon is polarized in one of the two "rectilinear" directions, vertical (90 degrees) or horizontal (0 degrees) without being informed of the specific polarization. Then he can reliably tell which direction by sending the photon into an apparatus consisting of a vertically oriented calcite crystal and two detectors, such as photomultiplier tubes, that can record single photons. The calcite crystal directs the incoming photon to the upper detector if it was horizontally polarized and to the lower detector if it was vertically polarized. Such an apparatus is useless for distinguishing diagonal (45 or 135-degree) photons, but these can be reliably distinguished by a similar apparatus that has been rotated 45 degrees from the original orientation. The rotated apparatus, in turn, is useless for distinguishing vertical from horizontal photons. According to the uncertainty principle these limitations apply not just to the

particular measuring apparatus described here but to any measuring device whatsoever. Rectilinear and diagonal polarizations are complementary properties in the sense that measuring either property necessarily randomizes the other.

The direction of the oscillation is known as the photon's polarization. Ordinary light consists of photons that have many different polarizations. But if the light passes through a polarizing filter, such as those used in sunglasses, only photons having a particular polarization will make it through. Which polarization is transmitted depends on the orientation of the filter. In sunglasses the filters are oriented to transmit vertically polarized light because such light reflects off most horizontal surfaces with less glare. But if the glasses are turned 90 degrees, so that one lens is directly above the other, they will transmit horizontally polarized light, augmenting the glare instead of diminishing it.

DIFFERENCE BETWEEN CLASSICAL&QUANTUM CRYPTOGRAPHY

While classical cryptography employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted messages, in quantum mechanics the information is protected by the laws of physics .In classical cryptography an absolute security of information cannot be guaranteed. The Heisenberg uncertainty principle and quantum entanglement can be exploited in a system of secure communication, often referred to as “quantum cryptography”. Quantum cryptography provides means for two parties to exchange a enciphering key over a private channel with complete security of communication.

QUANTUM DATA REPRESENTATION

Data can be represented in many different forms without changing its meaning. For example the letter 'A' is represented by the ASCII number 65 and 65 is in turn represented by sequence of binary digits which is the native form of today's computer. This simply means a machine is capable of processing any data that can be represented in an alternate form. In quantum computing, standard bits are represented using atoms or photons. The quantum bit, or qubit, can exist in one of two distinguishable states as in traditional systems. Atoms and photons have a spin associated with them. The spin is either up or down (see figure 1).



Figure 1. Atomic/photon up and down spin.

Some quantum cryptographic protocols make direct use of a property of qubits, known as Quantum entanglement. Quantum entanglement was first proposed and studied by famous scientists Einstein, Podolsky and Rosen (the EPR theorem). It is the co-relationship between two quantum particle's states (the up and down spin). This relationship is distance independent. A change in the state of one quantum particle will affect the state of other co-related particles. This quantum entanglement property is what makes a quantum computer more powerful than a von Neumon computer. The state of von Neumon computer may be represented by the state of all the sub-systems. In quantum computers this not true, the interaction between multiple subsystems introduce properties that would otherwise not be

part of the system (entanglement properties). However it should be noted any system that does not use quantum entanglement can be simulated using current technology. Current computers *"can simulate any quantum system, unless the system is separated and the correlations break the Bell Inequality/Theorem"*. The beauty of a quantum representation of information for cryptography lies in its conditional reading property. Any attempt at measuring a quantum state, unavoidably disturbs the state, unless some prior information of the state is known. Laws of physics - namely Heisenburgs uncertainty principle, therefore protect the data.

QUANTUM KEY DISTRIBUTION

In the case of PKC, no previously shared information is required, however as stated above, it is based on unproven maths. Security provided by PKC is likely to be threatened by the completion of the first quantum computer in the not too distant future. Traditional symmetric cryptography relies on a shared key that has to be established in an out of band manner. Both these methods rely on a physical transformation, encryption of the plain text. The ciphered text can then be read and copied by any person, but only the intended recipients can decrypt and understand the message.

Quantum cryptography is a completely different approach with this regard. Quantum information cannot be read unless some information is known beforehand about the state in which the information was prepared. Any attempt to read and hence copy the data with out the required information, disturbs the data in such away as to change its values.

Quantum key distribution aims to generate a truly random key between two principles wishing to communicate in a secure manner. The two principles require no prior shared information. Once a key of arbitrary length is shared, the secret information can be transmitted

through public communication channels, having been encrypted using a symmetric encryption.

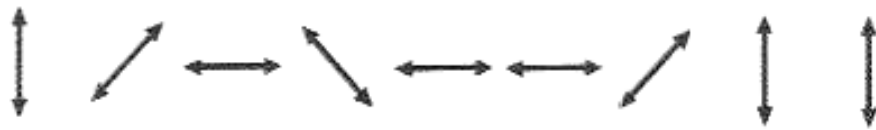
Current quantum key distribution uses one of three main cryptographic systems with encoding based on:

1. Two non-commuting observables
2. Quantum entanglement and Bells inequality/theorem
3. Two non-orthogonal state vectors

The cryptographic systems based on two non-commuting observables have been realized. The protocols used in a system of this type were originally proposed by Bennett and Brassard (the BB protocol). Another prototype, based on quantum entanglement, is currently being built. The protocols used for this system were originally developed by Ekert (Ekert protocol).

Quantum Key Distribution

A quantum cryptographic system will allow two people, say, Alice and Bob, to exchange a secret key. The system includes a transmitter and a receiver. Alice uses the transmitter to send photons in one of four polarizations: 0, 45, 90 or 135 degrees. Bob uses the receiver to measure the polarization. According to the laws of quantum mechanics, the receiver can distinguish between rectilinear polarizations (0 and 90), or it can quickly be reconfigured to discriminate between diagonal polarizations (45 and 135); it can never, however, distinguish both types. The key distribution requires several steps. Alice sends photons with one of four polarizations, which she has chosen at random.



For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (x).



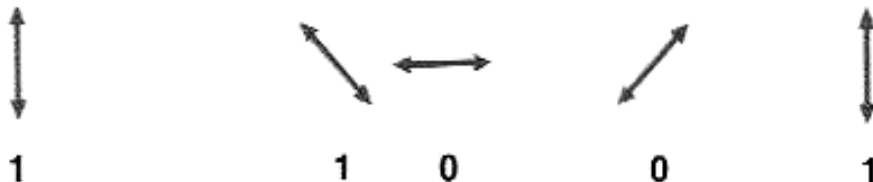
Bob records the result of his measurement but keeps it a secret.



Bob publicly announces the type of measurements he made, and Alice tells him which measurements were of the correct type.



Alice and Bob keep all cases in which Bob measured the correct type. These cases are then translated into bits (1's and 0's) and thereby become the key.



ENCODING BASED ON TWO NON-COMMUTING OBSERVABLES - BB PROTOCOL

This protocol uses polarised photons as the information carriers. Photons can be polarised to many different angles. This algorithm makes use of 4 different polarisation to achieve secure communication. The four angles of polarisation are 0, 45, 90 and 135 degrees. According to quantum physics, a photon can be measured to determine whether its polarisation is at 0 or 90 degrees. With a slight reconfiguration of the apparatus, a photon can be measured to decide whether it is at a polarisation of 45 or 135 degrees. The two configurations however cannot both be used to measure the polarisation. The process of measuring the polarisation changes a photon's polarisation in a random manner. Attempting to measure a photon's polarisation at the wrong angle produces truly random results.

This means both parties in a communication must agree on the angle of polarisation to use, for the correct information to be transferred. Lets examine how two principles would us this result to securely distribute a key.

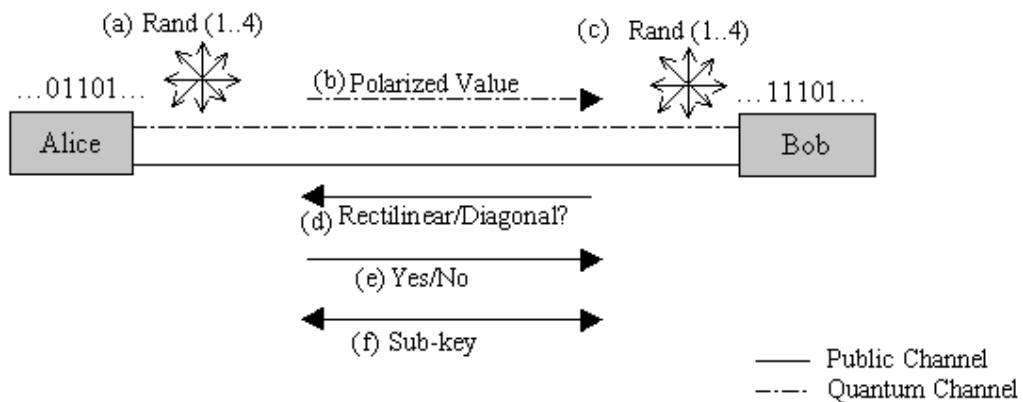


Figure 2. The BB key-distribution protocol in action

HOW IT WORKS

- (a) Alice initiates the communication by generating a random sequence of binary digits.
- (b) She proceeds to transmit each digit using one of the four polarisations at random.
- (c) Bob randomly picks one of the polarisations and makes a measurement to determine the photons "value" (up or down spin).
- (d) Bob then tells Alice which of the rectilinear (0 and 90 degrees) or diagonal polarisation (45 and 135 degrees) he used in his measurement. Note, however that he does not reveal the actual value he received.
- (e) Alice responds with a yes or no. Both Bob and Alice save the value of the bits on which their measurement types agreed. The sequence of saved values forms the key, which is later used for further encrypted public communications.
- (f) Before completing the key distribution Alice and Bob compare a small random subset of the generated key. Any discrepancies indicate heavy eavesdropping and the entire process is repeated. When the process eventually ends Bob and Alice can be assured that there are few or no errors in the exchanged key, and that an eavesdropper knows little or none of it.

The protocol as described above is rather simplified. Certain assumptions were made when it was initially proposed. One of the assumptions was lack of noise on the quantum channel this has since been dealt with by using a fairly complex error correcting protocol. The protocol also caters for any information that may have been leaked to an eavesdropper, Eve, during the public correction stage. Briefly, the

error correction protocol involves estimating the average error rate, then dividing the received data up into K random blocks which are publicly agreed upon, so that on average only 1 error occurs in a block. Alice and Bob calculate each block's parity. The parity of each block is then compared, if both parties agree on the block's parity, the block is accepted. If not, the block is divided into two halves. This process is then repeated recursively. During this process an eavesdropper may learn at most $\log(K)$ bits of information. To avoid leaking too much information, every time the parity bits are communicated, the last bit of a block is discarded! This process is repeated N times until both Alice and Bob are happy that there are very few errors. Alice and Bob then use the public communications channel to randomly choose a hashing function, which is then applied to the received data to generate the key. It can be guaranteed that Eve knows nothing about the final key established between Alice and Bob. One of the practical limits of a quantum system is the difficulty in producing single photons. To illuminate this problem a series of pulses are generated. Unfortunately these pulses can easily be sampled using beam-splitting techniques by an eavesdropper, without detection. The eavesdropper would more than likely use this information to assist in crypto-analysis. However, the error correction protocol just discussed changes the mapping between the original transmission and final key to such an extent that any of the partial information gained, will to all means and purposes be useless. While on the topic of attacks. There are two general attacks that rely on quantum mechanics.

1. The N photons transmitted between Alice and Bob are measured as a complete N state system. The public communication channel is monitored simultaneously. The net result is that the eavesdropper can determine exactly what the key is.
2. The small photon pulses generated are sampled and the photons are stored in perfect reflectors (similar to the ones used by Weisner) until direction of polarisation is announced on the

public channel. This information is then used to read the "value" of the photon if it is going to be used as part of the key.

Both these attacks are thought to be practically infeasible. In the BB protocol the most problematic assumption is that an eavesdropper cannot corrupt the public communication channel. In practice this can be implemented using an un-jamable public channel or alternatively the use of an authentication scheme, to verify the sender and receiver. The last technique however requires a key to be initially shared, so it no longer is a distribution mechanism but rather a key expansion mechanism. Note that a determined eavesdropper can repeatedly interfere and eventually exhaust all the shared keys before any "safe" communication is

established. This denial of service attack is more of a problem associated with all quantum cryptography in general. If this assumption is ignored an eavesdropper can establish itself between Alice and Bob, with principles been none the wiser.

For interest, a schematic diagram of the physical apparatus used in the first prototype of a quantum key-distribution system is given above (figure 3). Image 1, near the front of this paper, is an actual photo of the system. The quantum device illustrated was onnected to a desktop workstation, which was used to control it. The software on the workstation simulated both users of the system Bob and Alice and optionally an eavesdropper Eve. Although all the users where on same system, they were only allowed to communicate via public communication channel, as required by the protocol. A more detailed description of the apparatus used can be found in [14].

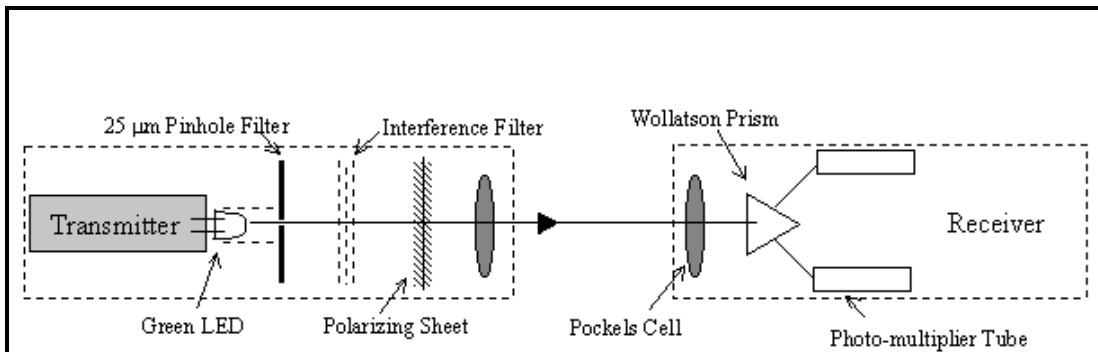


Figure 3. Schematic diagram of the original prototype

CRYPTOGRAPHIC SYSTEM WITH ENCODING BUILT UPON QUANTUM ENTANGLEMENT AND BELLS THEOREM

EKERTS PROTOCOL

Ekerts protocol takes advantage of quantum entanglement and the non-locality properties of quantum systems. Polarised photons are once again used as the information carriers. The protocol seems initially a bit odd, as the receiver is the initiator of the communication. The communication starts with Bob generating two co-related photons. Each particle is kept isolated from the environment to prevent any external quantum entanglement. Bob knows the quantum spin on the generated photons. He sends 1 of the photons to Alice, who wishes to transmit information. Alice performs one of 4 operation on the sent photon. The four operation Alice can perform are: to do nothing, or to rotate the photon by 180 degrees around one of the 3 axis (x, y, z). These are special operations, known as unitary operations, which can be applied the photon without destroying the coherence between the two tangled particles. Alice then sends the photon back to Bob who then recombines the 2 entangled particles. Bob then makes a measurement of the combined state using a quantum gate. The result

can be used to determine which operation Alice performed on the photon. The entire process has been illustrated in figure 4.

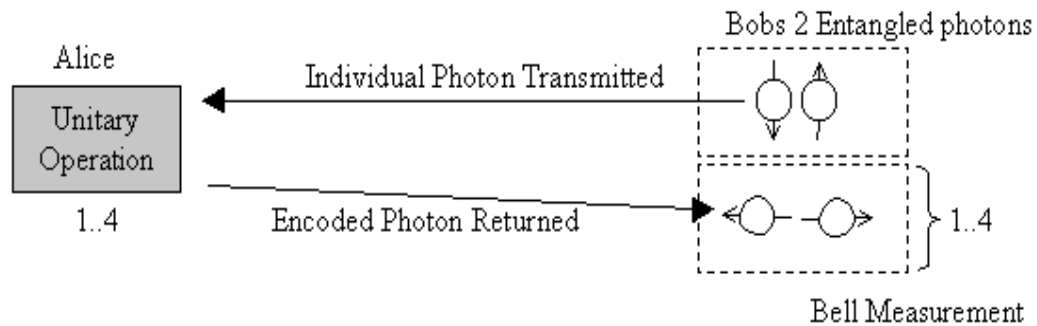


Figure 4. Ekerts protocol in action.

The quantum gates used by Alice to alter the state of the photon are available and have been so for quite some time. However the quantum gate used by Bob is still in development. Bob's quantum device is performing an operation more commonly known as a "Bell measurement". This device is allowed by quantum mechanics, as it does not try to calculate the state of the individual photons, but rather their combined state. This gate is presently beyond our technology but the idea is being experimentally reviewed [12].

There are several advantages to using Ekerts protocols. One of the advantages is increased communication capacity. For the cost of transferring one photon twice we can transfer 4 pieces of information. Another benefit is a cleaner and more efficient mechanism to handle noise in the quantum channel. Privacy amplification (discussed very briefly above) is used to handle the errors. If the amount of eavesdropping is too significant there will be a large number of errors, even after the error correction. If this is the case the cryptographic system can drop the key on the basis that Eve knows too much information. The key distribution process starts all over again and continues, until a secure transmission is achieved.

ADVANTAGES OF QUANTUM CRYPTOGRAPHY

- Secure method of communication of the information.
- Can detect eavesdropping.
- Unbreakable cryptosystem.

DISADVANTAGES OF QUANTUM CRYPTOGRAPHY

The wide spread use and acceptance of quantum cryptography is just a matter of time. Currently the size and expense of the quantum equipment makes it infeasible for use in a home environment. What is required is a technological leap similar to the discovery of the transistor to push it along the inevitable path. The claim of complete security in current quantum system is unsubstantiated. A form of authentication is still required to prove that a trusted principle is not just a masquerading enemy. Quantum key-distribution is also susceptible to denial of service attacks, where, by repeatedly interfering an eavesdropper can prevent the distribution of a key, that is required to complete a secure communication.

CONCLUSIONS

According to David DiVincenzo of the IBM Watson Research Center, the technical ability for widespread practical application of entangled cryptography is a long way off. Nevertheless, he says, "this is a small, but notable, step towards qualitatively more powerful forms of long-distance cryptography." QKD could be used for real-time key generation in cryptographic applications where this long-term risk is unacceptable.

Quantum cryptography is likely to be the first practical application of the foundations of quantum mechanics, which illustrates the often unexpected value of basic research. The still young field of quantum information has already achieved a multitude of exciting and surprising insights-both in the foundation of the quantum mechanics and its application to the problem of communication.

In practice, quantum cryptography has been demonstrated in the laboratory by IBM and others, but over relatively short distances. Recently, over longer distances, fiber optic cables with incredibly pure optic properties have successfully transmitted photon bits up to 60 kilometers. Beyond that, BERs (bit error rates) caused by a combination of the Heisenberg Uncertainty Principle and microscopic impurities in the fiber make the system unworkable. Some research has seen successful transmission through the air, but this has been over short distances in ideal weather conditions. It remains to be seen how much further technology can push forward the distances at which quantum cryptography is practical.

Practical applications in the US are suspected to include a dedicated line between the White House and Pentagon in Washington, and some links between key military sites and major defense contractors and research laboratories in close proximity. With many dedicated groups working in this field you can expect surprising results and breakthroughs.

REFERENCES

www . hitchiker's guide to quantum cryptography.

www . magiq technology

www . qcintro files.

www . new releases.

www . optical processing.

www. Askjeeves a theoretical assertion of the quantum

cryptography part 1 & part 2.

Abstract

Quantum cryptography

INTRODUCTION

Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated. One that is completely secure against being compromised without knowledge of the sender or the receiver of the message.

Quantum cryptography is different from the traditional cryptographic system in that it relies more on physics, rather than mathematics, as a key aspect of its security model. In classical cryptography an absolute security of the information cannot be guaranteed. The Heisenberg uncertainty principle and the quantum entanglement can be exploited in a system of secure communication. Quantum cryptography provides a means for two parties to exchange an enciphering key over a private channel with complete security of communication. This was first suggested by S.Wiesner and C.Bennet to use quantum mechanics to achieve provably secure key distribution.

TOPICS DISCUSSED

- Introduction to quantum information processing
- Need for quantum cryptography
- History of the introduction of this technique
- Types of quantum cryptosystems
- Advantages & disadvantages
- Applications of this technique

Basri Rasheed

Roll No. 3

ACKNOWLEDGEMENT

I thank God Almighty for the successful completion of my seminar.

I express my sincere gratitude to Dr. M N Agnisharman Namboothiri, Head of the Department, Information Technology. I am deeply indebted to Staff-in-charge, Miss. Sangeetha Jose and Mr. Biju, for their valuable advice and guidance. I am also grateful to all other members of the faculty of Information Technology department for their cooperation.

Finally, I wish to thank all my dear friends, for their whole-hearted cooperation, support and encouragement.