81

An Overview of Quantum Cryptography

Ben Rothke

Quantum cryptography:

- Potentially solves significant key distribution and management problems
- Offers a highly secure cryptography solution
- Is not meant to replace, nor will it replace, existing cryptography technologies
- Is a new hybrid model that combines quantum cryptography and traditional encryption to create a much more secure system
- Although not really ready for widespread commercial use, is developing very fast.

81.1 Introduction

Over the past few years, much attention has been paid to the domains of quantum computing and quantum cryptography. Both quantum computing and quantum cryptography have huge potential, and when they are ultimately deployed in totality will require massive changes in the state of information security. As of late 2005, quantum cryptography is still an early commercial opportunity; however, actual commercial quantum computing devices will not appear on the scene for another 15 to 25 years. This chapter provides a brief overview on the topic of quantum cryptography and the effects it will have on the information security industry.

AU7495—Chapter81—29/1/2007—08:19—IRSHATH—14741—XML MODEL CRC12a – pp. 1045–1057.

81.2 Cryptography Overview

This section is not intended to be a comprehensive overview of cryptography; for that, the reader is advised to consult the references mentioned in Exhibit 81.1, Exhibit 81.2, and Exhibit 81.3. Nonetheless, before discussing the details of quantum cryptography, an initial overview of cryptography in general is necessary. Cryptography is the science of using mathematics to encrypt and decrypt data to be sure that communications between parties are indeed private. Specifically, it is the branch of cryptology dealing with the design of algorithms for encryption and decryption, which are used to ensure the secrecy and authenticity of data. Cryptography is derived from the Greek word *Kryptos*, meaning "hidden."

Cryptography is important in that it allows people to experience the same level of trust and confidence in the digital world as in the physical world. Today, cryptography allows millions of people to interact electronically via e-mail, E-commerce, ATMs, cell phones, etc. The continuous increase of data transmitted electronically has led to an increased need for and reliance on cryptography. Ironically, until 2000, the U.S. government considered strong cryptography to be an export-controlled munition, much like an M-16 or F-18. The four objectives of cryptography (see Exhibit 81.4) are:

- *Confidentiality*—Data cannot be read by anyone for whom it was not intended.
- *Integrity*—Data cannot be altered in storage of transit between sender and intended receiver without the alteration being detected.
- *Authentication*—Sender and receiver can confirm each other's identity.
- *Nonrepudiation*—It is not possible to deny at a later time one's involvement in a cryptographic process.

EXHIBIT 81.1 An Explanation of Photons

A photon is a finite unit of light, carrying a fixed amount of energy ($E=hf$), where f is the frequency of the light, and h is the value of planck's constant. No doubt you've heard that light may be *polarized*; polarization is a physical property that emerges when light is regarded as an electromagnetic wave. The direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter) and can be measured using a calcite crystal.

A photon that is rectilinearly polarized has a polarization direction at 0° or 90° with respect to the horizontal. A diagonally polarized photon has a polarization direction at 45° or 135°. It is possible to use polarized photons to represent individual bits in a key or a message, with the following conventions:

	0	**1**
Rectilinear	0°	90°
Diagonal	45°	135°

That is, a polarization direction of 0° or 45° may be taken to stand for binary 0, while the directions of 90° and 135° may be taken to stand for binary 1. This is the convention used in the quantum key distribution scheme BB84, which will be described shortly. The process of mapping a sequence of bits to a sequence of rectilinearly and diagonally polarized photons is referred to as *conjugate coding*, and the rectilinear and diagonal polarization are known as *conjugative variables*. Quantum theory stipulates that it is impossible to measure the values of any pair of conjugate variables simultaneously.

The position and momentum of a particle are the most common examples of conjugate variables. When experimenters try to measure the position of a particle, they have to project light on it of a very short wavelength; however, short-wavelength light has a direct impact on the momentum of the particle, making it impossible for the experimenter to measure momentum to any degree of accuracy. Similarly, to measure the momentum of a particle, long-wavelength light is used, and this necessarily makes the position of the particle uncertain. In quantum mechanics, position and momentum are also referred to as *incompatible observables*, by virtue of the impossibility of measuring both at the same time. This same impossibility applies to rectilinear and diagonal polarization for photons. If you try to measure a rectilinearly polarized photon with respect to the diagonal, all information about the rectilinear polarization of the photon is lost —permanently.

Source: Papanikolaou, N. 2005. *An introduction to Quantum Cryptography*, University of Warwick, Department of Computer Science, Conventry, U.K.

EXHIBIT 81.2 The Two-Slit Experiment

Clinton Davisson of Bell Labs originally performed the two-slit experiment in 1927. Davisson observed that, when you place a barrier with a single slit in it between a source of electrons and a fluorescent screen, a single line is illuminated on the screen. When you place a barrier with two parallel slits in it between the source and the screen, the illumination takes on the form of a series of parallel lines fading in intensity the farther away they are from the center. This is not surprising and is entirely consistent with a wave interpretation of electrons, which was the commonly held view at the time. However, Davisson discovered that when you turn down the intensity of the electron beam to the point where individual electrons can be observed striking the fluorescent screen, something entirely unexpected happens: the positions at which the electrons strike are points distributed randomly with a probability matching the illumination pattern observed at higher intensity. It is as if each electron has physical extent so that it actually passed through both slits, but when it is observed striking the screen, it collapses to a point whose position is randomly distributed according to a wave function. Waves and particles are both familiar concepts at the everyday scale, but, at the subatomic level, objects appear to possess properties of both.

This observation was one of the first to suggest that our classical theories were inadequate to explain events on the subatomic scale and eventually gave rise to quantum theory. It has now been discovered that objects on an extremely small scale behave in a manner that is quite different from objects on an everyday scale, such as a tennis ball. Perhaps the most surprising observation is that objects on this very small scale, such as subatomic particles and photons, have properties that can be described by probability functions and that they adopt concrete values only when they are observed. While the probability functions are entirely amenable to analysis, the concrete values they adopt when observed appear to be random.

One of the most dramatic illustrations of the probabilistic wave function representation of objects on the quantum scale is a thought experienment described by Erwin Schrödinger that is universally referred to as "Schrödinger's cat."[a] We are asked to imagine a box containing a cat, a vial of cyanide, a radioactive source, and a Geiger counter. The apparatus is arranged such that, if the Geiger counter detects the emission of an electron, then the vial is broken, the cyanide is released, and the cat dies. According to quantum theory, the two states in which the electron has been emitted and the electron has not been emitted exist simultaneously. So, the two states of cat dies and cat lives exist simultaneously until the box is opened and the fate of the cat is determined. What Davisson showed is that quantum objects adopt multiple states simultaneously, in a process called *superposition*, and that they collapse to a single random state only when they are observed.

[a] For more on this, see John Gribbin's *In Search of Schrödinger's Cat: Quantum Physics and Reality*, Toronto, Bantam Books, 1994.

Source: From Addison, TX: Entrust (www.entrust.com/resources/whitepapers.cfm).

The origin of cryptography is usually considered to date back to about 2000 B.C. The earliest form of cryptography was the Egyptian hieroglyphics, which consisted of complex pictograms, the full meaning of which was known to only an elite few. The first known use of a modern cipher was by Julius Caesar (100–44 B.C). Caesar did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. In addition to Caesar, myriad other historical figures have used cryptography, including Benedict Arnold, Mary Queen of Scotts, and Abraham Lincoln. Cryptography has long been a part of war, diplomacy, and politics.

The development and growth of cryptography in the last 20 years is directly tied to the development of the microprocessor. Cryptography is computationally intensive, and the PC revolution and the ubiquitous Intel x86 processor have allowed the economical and reasonable deployment of cryptography.

The concept of cryptography can be encapsulated in the following six terms:

- *Encryption*—Conversion of data into a pattern, called ciphertext, rendering it unreadable
- *Decryption*—Process of converting ciphertext data back into its original form so it can be read
- *Algorithm*—Formula used to transform the plaintext into ciphertext; also called a cipher
- *Key*—Complex sequence of alphanumeric characters produced by the algorithm that allows data encryption and decryption
- *Plaintext*—Decrypted or unencrypted data
- *Ciphertext*—Data that has been encrypted.

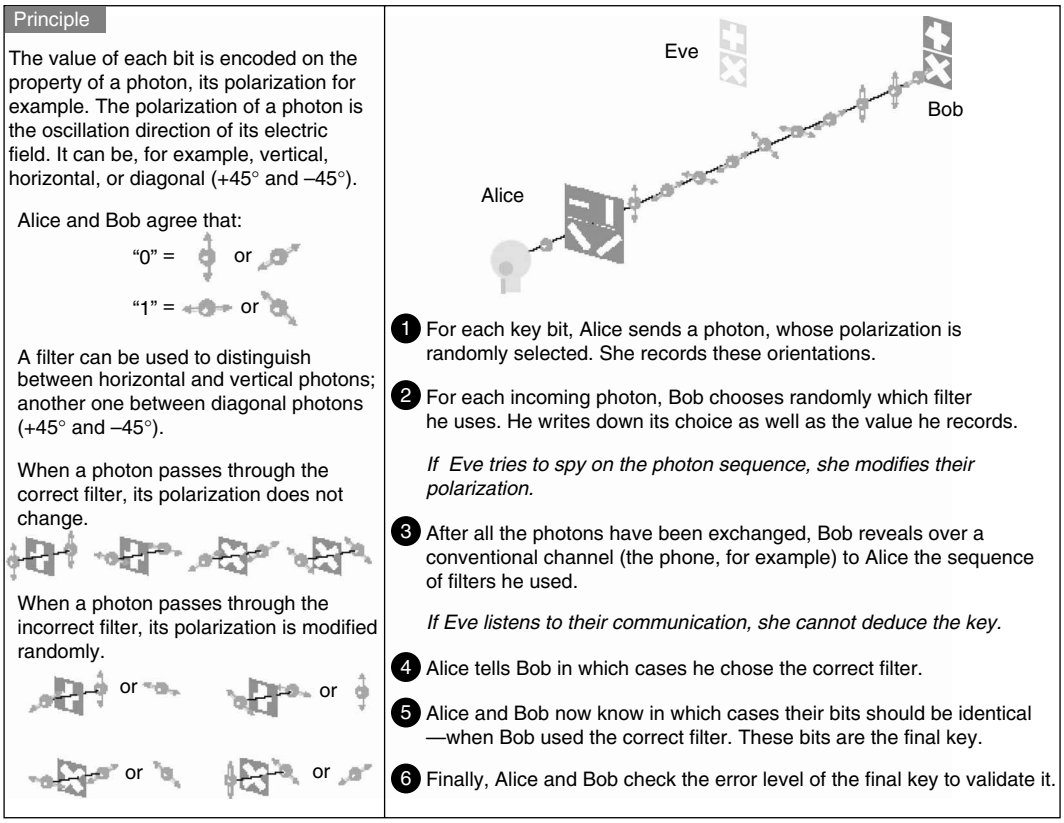

EXHIBIT 81.3 Quantum cryptography. (From IdQuantique. *A Quantum Leap for Cryptograhy*, p. 4, IdQuantique, Geneva. [www.idquantique.com/products/files/clavis-white.pdf].)

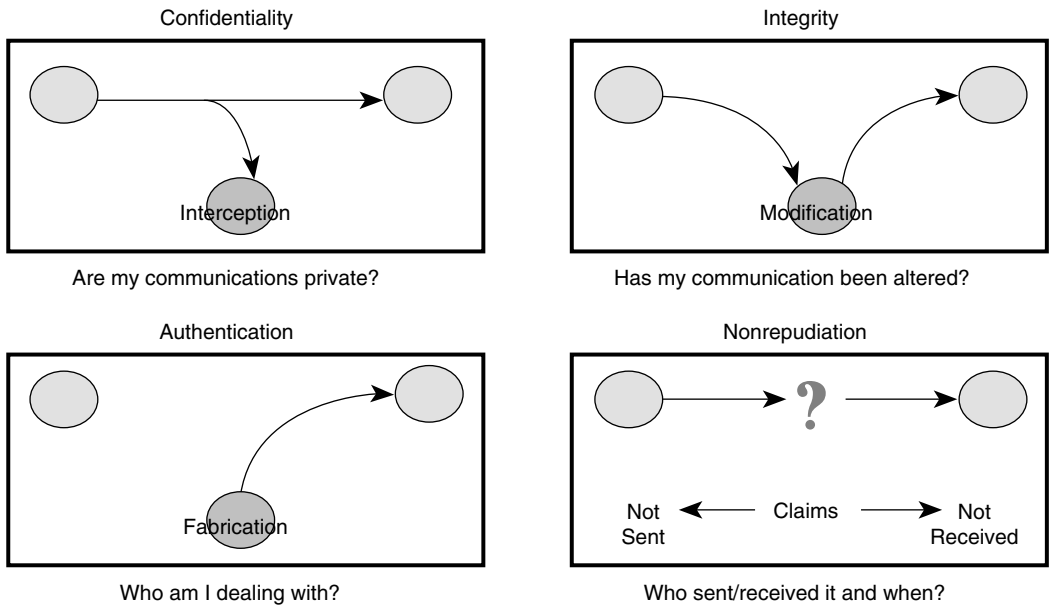

EXHIBIT 81.4 Four objectives of cryptography.

As stated earlier, one of the functions of digital cryptography is to allow people to experience the same level of trust and confidence in their information in the digital world as in the physical world. In a paper based society, we:

- Write a letter and sign it.
- Have a witness verify that the signature is authentic.
- Put the letter in an envelope and seal it.
- Send it by certified mail.

Correspondingly, this gives the recipient confidence that the:

- Contents have not been read by anyone else.
- Contents of the envelope are intact.
- Letter came from the person who claimed to have sent it.
- Person who sent it could not easily deny having sent it.

The two basic forms of cryptography are *symmetric* and *asymmetric*. Symmetric cryptography is the oldest form of cryptography, where a single key is used both for encryption and decryption. Exhibit 81.5 shows how a single key is used within symmetric cryptography to encrypt the plaintext. Both the party encrypting the data and decrypting the data share the key. While effective, the difficulty with symmetric cryptography is that of key management. With symmetric cryptography, as the number of users increases, the number of keys required to provide secure communications among those users increases rapidly For a group of n users, we must have a total of $1/2(n^2-n)$ keys to communicate. The number of parties (n) can increases to a point where the number of symmetric keys becomes unreasonably large for practical use. This is known as the n^2 problem. Exhibit 81.6 shows how many keys can be required. For 1,000 users (which is a very small number in today's distributed computing environments), an unmanageable 499,500 keys are required to share to share communications.

The key management problem created the need for a better solution, which has arrived in the form of symmetrical or public-key cryptography. Public-key cryptography is a form of encryption based on the use of two mathematically related keys (the *public key* and the *private key*) such that one key cannot be derived from the other. The public key is used to encrypt data and verify a digital signature, and the private key is used to decrypt data and digitally sign a document. The five main concepts of public-key cryptography are:

- Users publish their public keys to the world but keep their private keys secret.
- Anyone with a copy of a user's public key can encrypt information that only the user can read, even people the user has never met.

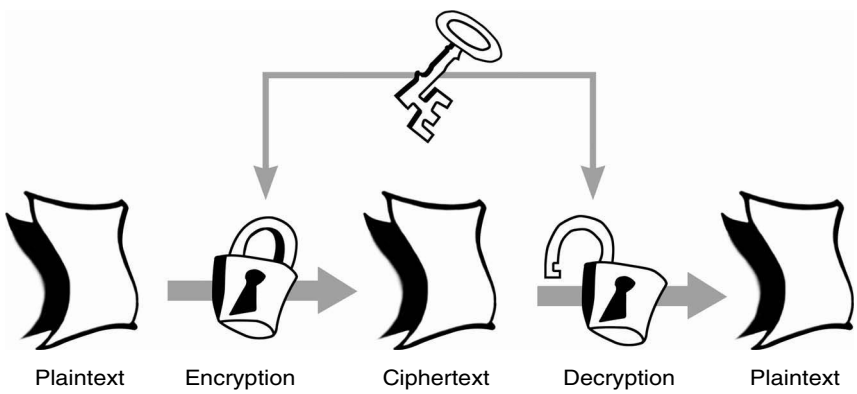

EXHIBIT 81.5 Single-key symmetric cryptography.

EXHIBIT 81.6 Keys Needed

Users	$1/2(n^2-n)$	Shared Key Pairs Required
2	$1/2(4-2)$	1
3	$1/2(9-3)$	3
10	$1/2(100-10)$	45
100	$1/2(10{,}000-100)$	4,950
1,000	$1/2(1{,}000{,}000-1000)$	499,500

- It is not possible to deduce the private key from the public key.
- Anyone with a public key can encrypt information but cannot decrypt it.
- Only the person who has the corresponding private key can decrypt the information.

Exhibit 81.7 shows how asymmetric cryptography is used to encrypt the plaintext. The parties encrypting the data and decrypting the data use different keys.

The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via a secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

It should be noted that an intrinsic flaw with public-key cryptography is that it is vulnerable to a large-scale brute force attack. In addition, because it is based on hard mathematics, if a simple way to solve the mathematical problem is ever found, then the security of public-key cryptography would be immediately compromised. From a mathematical perspective, public-key cryptography is still not provably secure. This means that algorithms such as RSA (which obtains its security from the difficulty of factoring large numbers) have not been proven mathematically to be secure. The fact that it is not a proven system does not mean that it is not capable, but if and when mathematicians comes up with a fast procedure for factoring large integers, then RSA-based cryptosystems could vanish overnight.

From a security functionality perspective, symmetric cryptography is for the most part just as strong as asymmetric crytography, but symmetric is much quicker. Where asymmetric shines is in solving the key management issues. In the absence of key management issues, there is no compelling reason to use asymmetric cryptography.

81.3 Quantum Mechanics and Quantum Theory

Two observations about quantum mechanics are notable. Nobel prize-winning physicist Richard Feynman stated that, "Nobody understands quantum theory," and fellow physicist Niels Bohr noted decades earlier that, "If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet." With that in mind, let us attempt to uncover the basic ideas about quantum theory and quantum cryptography.

For the most part, classical physics applies to systems that are larger than 1 micron (1 millionth of a meter) in size and was able to work quite handily when attempting to describe macroscopic objects.

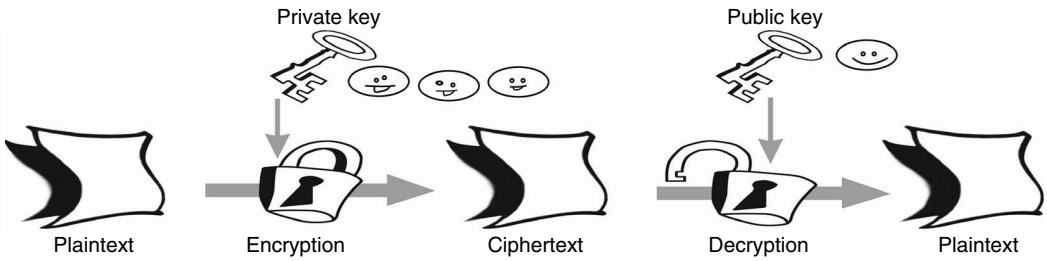

EXHIBIT 81.7 Asymmetric cryptography.

In the early 1900s, however, a radically new set of theories was created in the form of quantum physics. The quantum theory of matter developed at the turn of the century in response to a series of unexpected experimental results that did not conform to the previously accepted Newtonian model of the universe. The core of quantum theory is that elementary particles (e.g., electrons, protons, neutrons) have the ability to behave as waves. When Albert Einstein developed his general theory of relatively, he showed that space-time is curved by the presence of mass. This is true for large objects, as well as smaller objects encountered in everyday living (see Exhibit 81.2 for more details).

Quantum physics describes the microscopic world of subatomic particles such as molecules, atoms, quarks, and elementary particles, whereas classical physics describes the macroscopic world. Quantum physics also differs drastically from classical physics in that it is not a deterministic science; rather, it includes concepts such as randomness.

Quantum cryptography deals extensively with photons (see Exhibit 81.1), which are elementary quantum particles that lack mass and are the fundamental light particles. For the discussion at hand, quantum cryptography uses Heisenberg's uncertainty principle to allow two remote parties to exchange a cryptography key. One of the main laws of quantum mechanics manifest in Heisenberg's uncertainty principle is that every measurement perturbs the system; therefore, a lack of perturbation indicates that no measurement or eavesdropping has occurred. This is a potentially powerful tool within the realm of information security if it can be fully utilized.

One of the many applications of quantum mechanics is quantum computing. Standard computers use bits that are set to either one or zero. Quantum computers use electrons spinning either clockwise or counterclockwise to represent one and zeroes. These quantum bits are known as *qubits*. If these are in a superposition of states and have not been observed, all the possible states can be evaluated simultaneously and the solution obtained in a fraction of the time required by a standard computer, This generational leap in processing power is a huge threat to the security of all currently existing ciphers, as they are based on hard mathematical problems. The current security of the RSA algorithm would be eliminated.

The era of quantum cryptography began in the mid-1970s when researchers Charles Bennett at IBM and Gilles Brassard at the University of Montreal published a series of papers on its feasibility. They displayed the first prototype in 1989. In 1984, they created the first and, to date, best-known quantum cryptographic protocol which is known as BB84. Exhibit 81.8 demonstrates how BB84 carries out a quantum cryptographic key exchange.

81.4 Quantum Computing *versus* Quantum Cryptography

It should be noted that quantum computing and quantum cryptography are two discrete areas sharing a common term. Quantum computing is still in the theoretical state, but quantum cryptography is a functional, commercial solution. A quantum computer is a theoretical computer based on ideas from quantum theory; theoretically, it is capable of operating nondeterministically. According to the RSA Crypto FAQ,[1] quantum computing is a new field in computer science that has been developed in concert with the increased understanding of quantum mechanics. It holds the key to computers that are exponentially faster than conventional computers (for certain problems). A Quantum computer is based on the idea of a quantum bit or qubit. In classical computers, a bit has a discrete range and can represent either a zero state or a one state. A qubit can be in a linear superposition of the two states; hence, when a qubit is measured, the result will be zero with a certain probability and one with the complementary probability. A quantum register consists of n qubits. Because of superposition, a phenomenon known as quantum parallelism allows exponentially many computations to take place simultaneously, thus vastly increasing the speed of computation. It has been proven that a quantum computer will be able to factor and compute discrete logarithms in polynomial time. Unfortunately, the development of a practical quantum computer is still decades away.

[1]Refer to http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

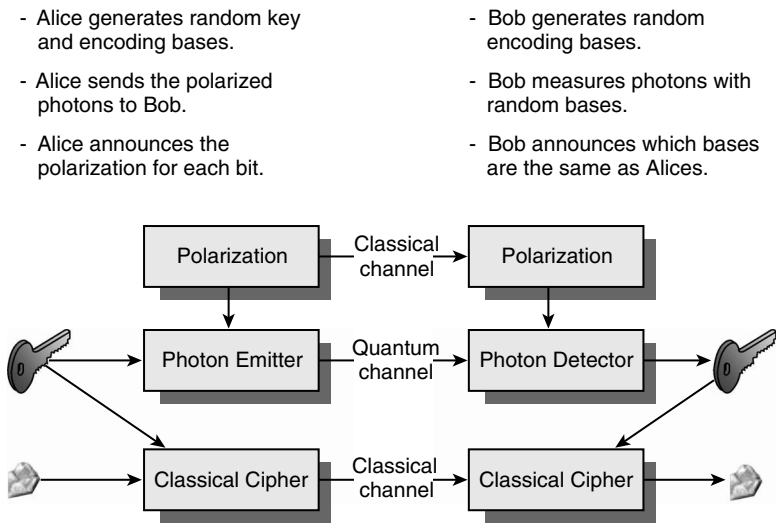

EXHIBIT 81.8 BB84. (From Sosonkin, M. 2005. *Introduction to Quantum Cryptography*, Polytechnic University, New York [http://sfs.poly.edu/presentations/MikeSpres.pdf].)

81.5 Quantum Cryptography *versus* Traditional Cryptography

A fundamental difference between traditional cryptography and quantum cryptography is that traditional cryptography primarily uses difficult mathematical techniques (such as integer factorization in RSA) as its fundamental mechanism. Quantum cryptography, on the other hand, uses physics to secure data. Whereas traditional cryptography stands on a foundation of strong math, quantum cryptography has a radically different premise in that the security should be based on known physical laws rather than on mathematical problems (see Exhibit 81.9). Quantum cryptography, also known as quantum key distribution or (QKD), is built on quantum physics. Perhaps the most well-known aspect of quantum physic is the uncertainty principle of Werner Heisenberg, which states that we cannot know both the position and momentum of a particle with absolute accuracy at the same time.

Specifically, quantum cryptography is a set of protocols, systems, and procedures that make it possible to create and distribute secret keys. Quantum cryptography can be used to generate and distribute secret keys, which can then be used together with traditional cryptography algorithms and protocols to encrypt and transfer data. It is important to note that quantum cryptography is not used to encrypt data, transfer encrypted data, or store encrypted data.

As noted early, the need for asymmetric key systems arose from the issue of key distribution. The quandary is that it is necessary to have a secure channel to set up a secure channel. Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with complete security as dictated by the laws of physics. When the key exchange takes place, conventional cryptographic algorithms are used. For that reason, many prefer the term *quantum key distribution* as opposed to *quantum cryptography*.

The following is a basic and overly simplistic explanation of how quantum cryptography can be used in a commercial setting:

- Two parties need to exchange data electronically in a highly secure manner.
- They choose standard cryptography algorithms, protocols, systems, and transport technologies to exchange the data in an encrypted form.
- They use a quantum cryptography channel to generate and exchange the secret keys required by the algorithms.

EXHIBIT 81.9 Comparison between QKD and Public/Private Key Protocols

Quantum Key Distribution	Pro/Con	Public/Private Key	Pro/Con
Requires dedicated hardware and communication lines	Con	Can be implemented in software; very portable	Pro
Mathematically proven secure based on basic physics laws	Pro	Mathematically undecided; based on mathematical problems for which an easy solution is not known (but could be discovered)	Con
Security is based on basic principles; does not require changes in future	Pro	Requires using longer private and public keys as computer power increases	Con
Will still be secure even when a quantum computer is built	Pro	Can be broken by a quantum computer, when and if one is built	Con
Very expensive	Con	Affordable by anyone	Pro
Still young and in development	Con	Extensively tested and deployed	Pro
Works only at limited distances and only with (direct) optical fibers	Con	Works at any distance and with any kind of network connection	Pro
Bit rate for key creation still low for some kinds of applications, but it will improve soon (when technical problems are solved)	?	Requires considerable amount of computing power, which is not a problem with data such as normal secret keys but not practical with larger data	?
Can be used with one-time pad, the only mathematically proven secure cryptographical algorithm	Pro	Cannot be used with one-time pad	Con

Source: From Pasquinucci, A. 2004. *Quantum Cryptography: Pros and Cons*, Lecco, Italy: UTTI.IC (http://www.ucci.it/en/qc/whitepapers/).

- They use the secret keys generated by quantum cryptography and the classical algorithms to encrypt the data.
- They exchange the encrypted data using the chosen classical protocols and transfer technologies.

Within quantum cryptography are two distinct channels. One channel is used for the transmission of the quantum key material via single photon light pulses; the other channel carries all message traffic, including the cryptographic protocols, encrypted user traffic, and more.

According to the laws of quantum physics, when a photon has been observed, its state changes. This makes quantum cryptography ideal for security purposes, because when someone tries to eavesdrop on a secure channel it will cause a disturbance in the flow of the photons that can be easily identified to provide extra security.

Quantum algorithms are orders of magnitude better than current systems. It is estimated that quantum factorization can factor a number a million times longer than any used for RSA in a millionth of the time. In addition, it can crack a Data Encryption Standard (DES) cipher in less than four minutes! The increased speed is due to the superposition of numbers. Quantum computers are able to perform calculations on various superpositions simultaneously, which creates the effect of a massive parallel computation.

81.6 Quantum Key Generation and Distribution

One current use of quantum cryptography is for key distribution. Because it is based on quantum mechanics, the keys generated and disseminated using quantum cryptography have been proven to be completely random and secure. The crypto keys are encoded on an individual photon basis, and the laws of quantum mechanics guarantee that an eavesdropper attempting to intercept even a single photon will permanently change the information encoded on that photon; therefore, the eavesdropper cannot copy or even read the photon and the data on it without modifying it. This enables quantum cryptography to detect this type of attack.

Before the advent of a public-key infrastructure, the only way to distribute keys securely was via trusted courier or some physical medium (keys on a floppy disk or CD-ROM). Much of the security of public-key cryptography is based on one-way functions. A mathematical one-way function is one that is easy to compute but difficult to reverse; however, reversing a one-way function can indeed be done if one has adequate time and computing resources. The resources necessary to crack an algorithm depend on the length of the key, but with the advent of distributed computing and increasing computer speeds this is becoming less of an issue.

In the late 1970s, the inventors of the RSA algorithm issued a challenge to crack a 129-bit RSA key. They predicted at the time that such a brute force attack would take roughly 40 quadrillion years, but it did not take quite that long. By 1994, a group of scientists working over the Internet solved RSA-129. In essence, the security of public keys would quickly be undermined if there was a way to quickly process the large numbers.

Quantum cryptography has the potential to solve this vexing aspect of the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security guaranteed by the laws of physics (again, if the keys can be kept secret, then the underlying security is vastly improved). Quantum key distribution exploits the fact, as mentioned earlier, that according to quantum physics the mere fact of observing a system will perturb it in an irreparable way. The simple act of reading this article alters it in a way that cannot be observed by the reader. Although this alteration cannot be observed at the macroscopic level, it can be observed at the microscopic level. A crucial factor is that it is provably impossible to intercept the key without introducing perturbations.

This characteristic has vast value to cryptography. If a system encodes the value of a bit on a quantum system, any interception will automatically create a perturbation due to the effect of the observer. This perturbation then causes errors in the sequence of bits shared by the two endpoints. When the quantum cryptographic system finds such an error, it will assume that the key pair was intercepted and then create a new key pair. Because the perturbation can only be determined after the interception, this explains why to date quantum cryptography has been used to exchange keys only and not the data itself.

What does it mean in practice to encode the value of a digital bit on a quantum system?[2] In telecommunications, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber to the receiver where it is registered and transformed back into an electronic form. These pulses typically contain millions of particles of light, called photons. In quantum cryptography, one can follow the same approach, with the only difference being that the pulses contain only a single photon. A single photon represents a very tiny amount of light (when reading this article, your eyes are registering billions of photons every second) and follows the laws of quantum physics. In particular, it cannot be split in half. This means that an eavesdropper cannot take half of a photon to measure the value of the bit it carries, while letting the other half continue on its course. To obtain the value of the bit, an eavesdropper must detect the photon which will affect the communication and reveal its being observed.

81.7 Quantum Cryptography *versus* Public-Key Cryptography

In many ways, quantum cryptography and public-key cryptography are similar. Both address the fundamental problem of creating and distributing keys to remote parties in a highly secure manner; they both solve the key distribution problem encountered by any two entities wishing to communicate using a cryptographically protected channel. But, quantum cryptography obtains its fundamental security from the fact that each qubit is carried by a single photon, and these photons are altered as soon as they are read, which makes it impossible to intercept messages without being detected.

[2] See IdQuantique, *A Quantum Leap for Cryptography.*, p. 4, Geneva, IdQuantique, (www.idquantique.com/products/files/clavis-white.pdf).

81.8 Quantum Cryptography and Heisenberg's Uncertainty Principle

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. This law, put forward in 1927 by German physicist Werner Heisenberg, suggests that the mere act of observing or measuring a particle will ultimately change its behavior. At the macroscopic levels, we do not notice this occurring.

Under the laws of quantum physics, a moving photon has one of four orientations; vertical, horizontal, or diagonal in opposing directions. Quantum cryptographic devices emit photons one at a time, and each photon has a particular orientation. Photon sniffers are able to record the orientation of each photon, but, according to Heisenberg's uncertainty principle, doing so will change the orientation of some of the particles which in turn will warn both the sender and the recipient that their channel is being monitored. Where Heisenberg's uncertainty principle is of huge benefit to information security is that, if quantum cryptography is used to send keys via photons then perfect encryption is assured. If it is found that the keys have been observed and are therefore at risk, then it is a simple matter to create a new set of keys. In traditional key exchange, it is not possible to know if a key has been tampered with to the same degree of certainty as with quantum cryptography.

Many of the quantum cryptography proponents and vendors publicly state that quantum cryptography provides absolute security; however, for those with a background in cryptography, the only provably secure cryptosystems are one-time pads.[3] Can quantum cryptography really create a scheme that provides absolute security? Traditional cryptographic schemes, such as RSA, are based on hard mathematical problems; quantum cryptography is based on the laws of physics and Heisenberg's uncertainty principle, which would seem to provide absolute security.

81.9 Disadvantages of Quantum Cryptography

Like everything else in the world of information security, quantum cryptography is no panacea. The main drawbacks of quantum cryptography are:

- It is slow.
- It is expensive.
- It works only over relatively short distances.
- It is new and unproven.
- It requires a dedicated connection.
- It lacks digital signatures.
- The speed of the actual key exchange is roughly 100 kbps.

Also, because it must transfer the actual physical properties of photons, it only works over relatively short distances. Current limitations now mean that the cryptographic devices can be a maximum of 75 miles apart. The reason for the short distance is that optical amplification destroys the qubit state. A repeater cannot be used to extend the distance because the repeater would change the state of the photon. In addition, attenuation of the fiber-optic links would degrade the quality of the signal and ultimately make the transmitted photon unreadable.

The photon emitters and detectors themselves are currently far from perfect and can cause errors that often require retransmission of the keys. The signals themselves are currently a significant problem for those implementing quantum cryptography, due to the presence of noise in all of the communications

[3]For more information on why, see http://world.std.com/~franl/crypto/one-time-pad.html.

channels, most prominently in the optical fibers themselves. As the systems evolve, however, noise is less likely to be a problem.

In order to transmit the photon, both parties must have a live, unbroken, and continuous communications channel between them. Although no quantum routers now exist, research is being conducted on how to build them. The value of a quantum router is that it would enable quantum cryptography to be used on a network. Finally, quantum cryptography today does not have a seamless method for obtaining a digital signature. Quantum digital signature schemes are in development but are still not ready for the commercial environment.

81.10 Effects of Quantum Computing and Cryptography on Information Security

It is clear that if a functioning quantum computer was to be constructed, it would immediately undermine the security provided by both symmetric-key algorithms and public-key algorithms. Quantum computing would be able to break public-key cryptosystems in inconsequential amounts of time. It is estimated that a 1024-bit RSA key could be broken with roughly 3,000 qubits. Given that current quantum computers have less than 10 qubits, public-key cryptography is safe for the foreseeable future, but this is not an absolute guarantee.

81.11 Conclusion

Quantum cryptography, while still in a nascent state, is certain to have a huge and revolutionary effect on the world of cryptography and secure communications. As of late 2005, quantum cryptography was not in heavy use in the Fortune 1000 community, but it will likely find much greater application in the coming years as it matures and the price drops.

81.12 Glossary of Quantum Physics Terms

Entanglement—The phenomenon that two quantum systems that have been prepared in a state such that they interacted in the past may still have some locally inaccessible information in common.

Interference—The outcome of a quantum process depends on all of the possible histories of that process.

Observable—Anything within a quantum mechanical system that can be observed, measured, and quantitatively defined (e.g., electron spin, polarization).

Quanta—Discrete packets or entities in quantum systems; observables in quantum systems tend to vary discretely, not continuously.

Superposition—The concept that a quantum system may be simultaneously in any number of possible states at once.

Additional Resources

Ekert, A. 1995. *CQC Introductions: Quantum Cryptography*, Centre for Quantum Computation, Oxford, (www.qubit.org/library/intros/crypt.html).

MagiQ. 2004. *Perfectly Secure Key Management System Using Quantum Key Distribution*, MagiQ Technologies, New York. (www.magiqtech.com/registration/MagiQWhitePaper.pdf).

Oxford Centre for Quantum Computation, www.qubit.org.

Moses, T. and Zuccherato, R. 2005. *Quantum Computing and Quantum Cryptography: What Do They Mean for Traditional Cryptography?* Entrust White Paper, January 13 (https://www.entrust.com/contact/index.cfm?action=wpdownload&tp1=resources&resource=quantum.pdf&id=21190).

Quantum cryptography tutorial, www.cs.dartmouth.edu/~jford/crypto.html.
Sosonkin, M. 2005. *Introduction to Quantum Cryptography*, Polytechnic University, New York. (http://sfs.poly.edu/presentations/MikeSpres.pdf).
Wikipedia, http://en.wikipedia.org/wiki/Quantum_Cryptography.

Cryptography References

Kahn, D. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, New York.
Nichols, R. 1998. *ICSA Guide to Cryptography*, McGraw-Hill, New York.
RSA cryptography FAQ, www.rsasecurity.com/rsalabs/faq.
Schneier, B. 1996. *Applied Cryptography*, John Wiley & Sons, New York.
Singh, S. 2000. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, Lancaster, VA.

Commercial Quantum Cryptography Solutions

MagiQ Technologies, www.magiqtech.com.
id Quantique, www.idquantique.com.
Qinetiq, www.qinetiq.com.
NEC, www.nec.com.