any responsibility–if you do choose to install PGP, it is up to you check that your computer is capable of running it, that the software is not infected with a virus, and so on. Also, you should check that you are in a country that permits the use of strong encryption. Finally, you should ensure that you are downloading the appropriate version of PGP: individuals living outside America should not download the American version of PGP, because this would violate American export laws. The international version of PGP does not suffer from export restrictions.

I still remember the Sunday afternoon when I first downloaded a copy of PGP from the Internet. Ever since, I have been able to guarantee my e-mails against being intercepted and read, because I can now encrypt sensitive material to Alice, Bob and anybody else who possesses PGP software. My laptop and its PGP software provide me with a level of security that is beyond the combined efforts of all the world's code-breaking establishments.

FROM
"THE CODE BOOK"
BY S. SINGH

8 A Quantum Leap into the Future

For two thousand years, codemakers have fought to preserve secrets while codebreakers have tried their best to reveal them. It has always been a neck-and-neck race, with codebreakers battling back when codemakers seemed to be in command, and codemakers inventing new and stronger forms of encryption when previous methods had been compromised. The invention of public key cryptography and the political debate that surrounds the use of strong cryptography bring us up to the present day, and it is clear that the cryptographers are winning the information war. According to Phil Zimmermann, we live in a golden age of cryptography: "It is now possible to make ciphers in modern cryptography that are really, really out of reach of all known forms of cryptanalysis. And I think it's going to stay that way." Zimmermann's view is supported by William Crowell, Deputy Director of the NSA: "If all the personal computers in the world–approximately 260 million computers–were to be put to work on a single PGP encrypted message, it would take on average an estimated 12 million times the age of the universe to break a single message."

Previous experience, however, tells us that every so-called unbreakable cipher has, sooner or later, succumbed to cryptanalysis. The Vigenère cipher was called "le chiffre indéchiffrable," but Babbage broke it; Enigma was considered invulnerable, until the Poles revealed its weaknesses. So, are cryptanalysts on the verge of another breakthrough, or is Zimmermann right? Predicting future developments in any technology is always a precarious task, but with ciphers it is particularly risky. Not only do we have to guess which discoveries lie in the future, but we also have to guess which discoveries lie in the present. The tale of James Ellis and GCHQ warns us that there may already be remarkable breakthroughs hidden behind the veil of government secrecy.

This final chapter examines a few of the futuristic ideas that may enhance or destroy privacy in the twenty-first century. The next section looks at the future of cryptanalysis, and one idea in particular that might enable cryptanalysts to break all today's ciphers. In contrast, the final section of the book looks at the most exciting cryptographic prospect, a system that has the potential to guarantee absolute privacy.

The Future of Cryptanalysis

Despite the enormous strength of RSA and other modern ciphers, cryptanalysts are still able to play a valuable role in intelligence gathering. Their success is demonstrated by the fact that cryptanalysts are in greater demand than ever before–the NSA is still the world's largest employer of mathematicians.

Only a small fraction of the information flowing around the world is securely encrypted, and the remainder is poorly encrypted, or not encrypted at all. This is because the number of Internet users is rapidly increasing, and yet few of these people take adequate precautions in terms of privacy. In turn, this means that national security organizations, law enforcers and anybody else with a curious mind can get their hands on more information than they can cope with.

Even if users employ the RSA cipher properly, there is still plenty that codebreakers can do to glean information from intercepted messages. Codebreakers continue to use old-fashioned techniques like traffic analysis; if codebreakers cannot fathom the contents of a message, at least they might be able to find out who is sending it, and to whom it is being sent, which in itself can be telling. A more recent development is the so-called *tempest attack*, which aims to detect the electromagnetic signals emitted by the electronics in a computer's display unit. If Eve parks a van outside Alice's house, she can use sensitive tempest equipment to identify each individual keystroke that Alice makes on her computer. This would allow Eve to intercept the message as it is typed into the computer, before it is encrypted. To defend against tempest attacks, companies are already supplying shielding material that can be used to line the walls of a room to prevent the escape of electromagnetic signals. In America, it is necessary to obtain a government license before buying such shielding material,

which suggests that organizations such as the FBI regularly rely on tempest surveillance.

Other attacks include the use of viruses and Trojan horses. Eve might design a virus that infects PGP software and sits quietly inside Alice's computer. When Alice uses her private key to decrypt a message, the virus would wake up and make a note of it. The next time that Alice connects to the Internet, the virus would surreptitiously send the private key to Eve, thereby allowing her to decipher all subsequent messages sent to Alice. The Trojan horse, another software trick, involves Eve designing a program that appears to act like a genuine encryption product, but which actually betrays the user. For example, Alice might believe that she is downloading an authentic copy of PGP, whereas in reality she is downloading a Trojan horse version. This modified version looks just like the genuine PGP program, but contains instructions to send plaintext copies of all Alice's correspondence to Eve. As Phil Zimmermann puts it: "Anyone could modify the source code and produce a lobotomized zombie imitation of PGP that looks real but does the bidding of its diabolical master. This Trojan horse version of PGP could then be widely circulated, claiming to be from me. How insidious! You should make every effort to get your copy of PGP from a reliable source, whatever that means."

A variation on the Trojan horse is a brand-new piece of encryption software that seems secure, but which actually contains a *backdoor*, something that allows its designers to decrypt everybody's messages. In 1998, a report by Wayne Madsen revealed that the Swiss cryptographic company Crypto AG had built backdoors into some of its products, and had provided the U.S. Government with details of how to exploit these backdoors. As a result, America was able to read the communications of several countries. In 1991 the assassins who killed Shahpour Bakhtiar, the exiled former Iranian prime minister, were caught thanks to the interception and backdoor decipherment of Iranian messages encrypted using Crypto AG equipment.

Although traffic analysis, tempest attacks, viruses and Trojan horses are all useful techniques for gathering information, cryptanalysts realize that their real goal is to find a way of cracking the RSA cipher, the cornerstone of modern encryption. The RSA cipher is used to protect the most important military, diplomatic, commercial and criminal communications

–exactly the messages that intelligence gathering organizations want to decipher. If they are to challenge strong RSA encryption, cryptanalysts will need to make a major theoretical or technological breakthrough.

A theoretical breakthrough would be a fundamentally new way of finding Alice's private key. Alice's private key consists of p and q, and these are found by factoring the public key, N. The standard approach is to check each prime number one at a time to see if it divides into N, but we know that this takes an unreasonable amount of time. Cryptanalysts have tried to find a shortcut to factoring, a method that drastically reduces the number of steps required to find p and q, but so far all attempts to develop a fast-factoring recipe have ended in failure. Mathematicians have been studying factoring for centuries, and modern factoring techniques are not significantly better than ancient techniques. Indeed, it could be that the laws of mathematics forbid the existence of a significant shortcut for factoring.

Without much hope of a theoretical breakthrough, cryptanalysts have been forced to look for a technological innovation. If there is no obvious way to reduce the number of steps required for factoring, then cryptanalysts need a technology that will perform these steps more quickly. Silicon chips will continue to get faster as the years pass, doubling in speed roughly every eighteen months, but this is not enough to make a real impact on the speed of factoring–cryptanalysts require a technology that is billions of times faster than current computers. Consequently, cryptanalysts are looking toward a radically new form of computer, the *quantum computer*. If scientists could build a quantum computer, it would be able to perform calculations with such enormous speed that it would make a modern supercomputer look like a broken abacus.

The remainder of this section discusses the concept of a quantum computer, and therefore it introduces some of the principles of quantum physics, sometimes called quantum mechanics. Before going any further, please heed a warning originally given by Niels Bohr, one of the fathers of quantum mechanics: "Anyone who can contemplate quantum mechanics without getting dizzy hasn't understood it." In other words, prepare to meet some rather bizarre ideas.

In order to explain the principles of quantum computing, it helps to return to the end of the eighteenth century and the work of Thomas Young, the English polymath who made the first breakthrough in deciphering Egyptian hieroglyphics. A fellow of Emmanuel College, Cambridge, Young would often spend his afternoons relaxing near the college duck pond. On one particular day, so the story goes, he noticed two ducks happily swimming alongside each other. He observed that the two ducks left two trails of ripples behind them, which interacted and formed a peculiar pattern of rough and calm patches. The two sets of ripples fanned out behind the two ducks, and when a peak from one duck met a trough from the other duck, the result was a tiny patch of calm water–the peak and the trough canceled each other out. Alternatively, if two peaks arrived at the same spot simultaneously, then the result was an even higher peak, and if two troughs arrived at the same spot simultaneously, the result was an even deeper trough. He was particularly fascinated, because the ducks reminded him of an experiment concerning the nature of light which he conducted in 1799.

In Young's earlier experiment he had shone light at a partition in which there were two narrow vertical slits, as shown in Figure 71(a). On a screen some distance beyond the slits, Young expected to see two bright stripes, projections of the slits. Instead he observed that the light fanned out from the two slits and formed a pattern of several light and dark stripes on the screen. The striped pattern of light on the screen had puzzled him, but now he believed he could explain it wholly in terms of what he had seen on the duck pond.

Young began by assuming that light was a form of wave. If the light emanating from the two slits behaved like waves, then it was just like the ripples behind the two ducks. Furthermore, the light and dark stripes on the screen were caused by the same interactions that caused the water waves to form high peaks, deep troughs and patches of calm. Young could imagine points on the screen where a trough met a peak, resulting in cancelation and a dark stripe, and points on the screen where two peaks (or two troughs) met, resulting in reinforcement and a bright stripe, as shown in Figure 71(b). The ducks had provided Young with a deeper insight into the true nature of light, and he eventually published "The Undulatory Theory of Light," an all-time classic among physics papers.

Nowadays, we know that light does indeed behave like a wave, but we know that it can also behave like a particle. Whether we perceive light as a wave or as a particle depends on the circumstances, and this ambiguity

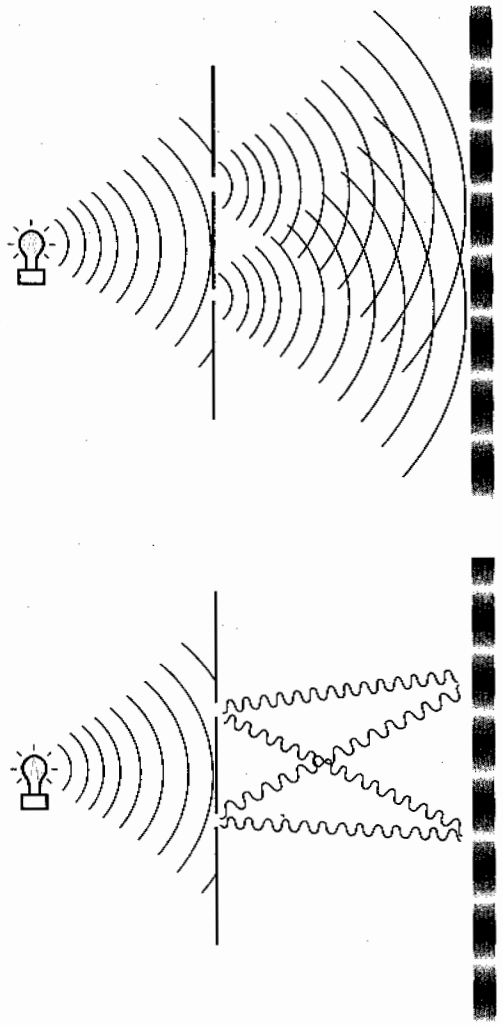

Figure 71 Young's slits experiment viewed from above. Diagram (a) shows light fanning out from the two slits in the partition, interacting and creating a striped pattern on the screen. Diagram (b) shows how individual waves interact. If a trough meets a peak at the screen, the result is a dark stripe. If two troughs (or two peaks) meet at the screen, the result is a bright stripe.

of light is known as wave–particle duality. We do not need to discuss this duality any further, except to say that modern physics thinks of a beam of light as consisting of countless individual particles, known as photons, which exhibit wave-like properties. Looked at this way, we can interpret Young's experiment in terms of photons flooding the slits, and then interacting on the other side of the partition.

So far, there is nothing particularly strange about Young's experiment. However, modern technology allows physicists to repeat Young's experiment using a filament that is so dim that it emits single photons of light. Photons are produced individually at a rate of, say, one per minute, and each photon travels alone toward the partition. Sometimes a photon will pass through one of the two slits, and strike the screen. Although our eyes are not sensitive enough to see the individual photons, they can be observed with the help of a special detector, and over a period of hours we could build up an overall picture of where the photons are striking the screen. With only one photon at a time passing through the slits, we would not expect to see the striped pattern observed by Young, because that phenomenon seems to depend on two photons simultaneously traveling through different slits and interacting with each other on the other side. Instead we might expect to see just two light stripes, simply projections of the slits in the partition. However, for some extraordinary reason, even with single photons the result on the screen is still a pattern of light and dark stripes, just as if photons had been interacting.

This weird result defies common sense. There is no way to explain the phenomenon in terms of the classical laws of physics, by which we mean the traditional laws that were developed to explain how everyday objects behave. Classical physics can explain the orbits of planets or the trajectory of a cannonball, but cannot fully describe the world of the truly tiny, such as the trajectory of a photon. In order to explain such photon phenomena, physicists resort to quantum theory, an explanation of how objects behave at the microscopic level. However, even quantum theorists cannot agree on how to interpret this experiment. They tend to split into two opposing camps, each with their own interpretation.

The first camp posits an idea known as *superposition*. The superpositionists begin by stating that we know only two things for certain about the photon–it leaves the filament and it strikes the screen. Everything else

is a complete mystery, including whether the photon passed through the left slit or the right slit. Because the exact path of the photon is unknown, superpositionists take the peculiar view that the photon somehow passes through both slits simultaneously, which would then allow it to interfere with itself and create the striped pattern observed on the screen. But how can one photon pass through both slits?

Superpositionists argue along the following lines. If we do not know what a particle is doing, then it is allowed to do everything possible simultaneously. In the case of the photon, we do not know whether it passed through the left slit or the right slit, so we assume that it passed through both slits simultaneously. Each possibility is called a *state*, and because the photon fulfills both possibilities it is said to be in a *superposition of states*. We know that one photon left the filament and we know that one photon hit the screen on the other side of the partition, but in between it somehow split into two "ghost photons" that passed through both slits. Superposition might sound silly, but at least it explains the striped pattern that results from Young's experiment performed with individual photons. In comparison, the old-fashioned classical view is that the photon must have passed through one of the two slits, and we simply do not know which one–this seems much more sensible than the quantum view, but unfortunately it cannot explain the observed result.

Erwin Schrödinger, who won the Nobel Prize for Physics in 1933, invented a parable known as "Schrödinger's cat," which is often used to help explain the concept of superposition. Imagine a cat in a box. There are two possible states for the cat, namely dead or alive. Initially, we know that the cat is definitely in one particular state, because we can see that it is alive. At this point, the cat is not in a superposition of states. Next, we place a vial of cyanide in the box along with the cat and close the lid. We now enter a period of ignorance, because we cannot see or measure the state of the cat. Is it still alive, or has it trodden on the vial of cyanide and died? Traditionally we would say that the cat is either dead or alive, we just do not know which. However, quantum theory says that the cat is in a superposition of two states–it is both dead and alive, it satisfies all possibilities. Superposition occurs only when we lose sight of an object, and it is a way of describing an object during a period of ambiguity. When we eventually open the box, we can see whether the cat is alive or dead. The act of looking at the cat forces it to be in one particular state, and at that very moment the superposition disappears.

For readers who feel uncomfortable with superposition, there is the second quantum camp, who favor a different interpretation of Young's experiment. Unfortunately, this alternative view is equally bizarre. The *many-worlds interpretation* claims that upon leaving the filament the photon has two choices–either it passes through the left slit or the right slit–at which point the universe divides into two universes, and in one universe the photon goes through the left slit, and in the other universe the photon goes through the right slit. These two universes somehow interfere with each other, which accounts for the striped pattern. Followers of the many-worlds interpretation believe that whenever an object has the potential to enter one of several possible states, the universe splits into many universes, so that each potential is fulfilled in a different universe. This proliferation of universes is referred to as the *multiverse*.

Whether we adopt superposition or the many-worlds interpretation, quantum theory is a perplexing philosophy. Nevertheless, it has shown itself to be the most successful and practical scientific theory ever conceived. Besides its unique capacity to explain the result of Young's experiment, quantum theory successfully explains many other phenomena. Only quantum theory allows physicists to calculate the consequences of nuclear reactions in power stations; only quantum theory can explain the wonders of DNA; only quantum theory explains how the sun shines; only quantum theory can be used to design the laser that reads the CDs in your stereo. Thus, like it or not, we live in a quantum world.

Of all the consequences of quantum theory, the most technologically important is potentially the quantum computer. As well as destroying the security of all modern ciphers, the quantum computer would herald a new era of computing power. One of the pioneers of quantum computing is David Deutsch, a British physicist who began working on the concept in 1984, when he attended a conference on the theory of computation. While listening to a lecture at the conference, Deutsch spotted something that had previously been overlooked. The tacit assumption was that all computers essentially operated according to the laws of classical physics, but Deutsch was convinced that computers ought to obey the laws of quantum physics instead, because quantum laws are more fundamental.

Ordinary computers operate at a relatively macroscopic level, and at that level quantum laws and classical laws are almost indistinguishable. It did not therefore matter that scientists had generally thought of ordinary computers in terms of classical physics. However, at the microscopic level the two sets of laws diverge, and at this level only the laws of quantum physics hold true. At the microscopic level, quantum laws reveal their true weirdness, and a computer constructed to exploit these laws would behave in a drastically new way. After the conference, Deutsch returned home and began to recast the theory of computers in the light of quantum physics. In a paper published in 1985 he described his vision of a quantum computer operating according to the laws of quantum physics. In particular, he explained how his quantum computer differed from an ordinary computer.

Imagine that you have two versions of a question. To answer both questions using an ordinary computer, you would have to input the first

Figure 72 David Deutsch.

version and wait for the answer, then input the second version and wait for the answer. In other words, an ordinary computer can address only one question at a time, and if there are several questions it has to address them sequentially. However, with a quantum computer, the two questions could be combined as a superposition of two states and inputted simultaneously–the machine itself would then enter a superposition of two states, one for each question. Or, according to the many-worlds interpretation, the machine would enter two different universes, and answer each version of the question in a different universe. Regardless of the interpretation, the quantum computer can address two questions at the same time by exploiting the laws of quantum physics.

To get some idea of the power of a quantum computer, we can compare its performance with that of a traditional computer by seeing what happens when each is used to tackle a particular problem. For example, the two types of computer could tackle the problem of finding a number whose square and cube together use all the digits from 0 to 9 once and only once. If we test the number 19, we find that $19^2 = 361$ and $19^3 = 6{,}859$. The number 19 does not fit the requirement because its square and cube include only the digits: 1, 3, 5, 6, 6, 8, 9, i.e., the digits 0, 2, 4, 7 are missing and the digit 6 is repeated.

To solve this problem with a traditional computer, the operator would have to adopt the following approach. The operator inputs the number 1 and then allows the computer to test it. Once the computer has done the necessary calculations, it declares whether or not the number fulfills the criterion. The number 1 does not fulfill the criterion, so the operator inputs the number 2 and allows the computer to carry out another test, and so on, until the appropriate number is eventually found. It turns out that the answer is 69, because $69^2 = 4{,}761$ and $69^3 = 328{,}509$, and these numbers do indeed include each of the ten digits once and only once. In fact, 69 is the only number that satisfies this requirement. It is clear that this process is time-consuming, because a traditional computer can test only one number at a time. If the computer takes one second to test each number, then it would have taken 69 seconds to find the answer. In contrast, a quantum computer would find the answer in just 1 second.

The operator begins by representing the numbers in a special way so as to exploit the power of the quantum computer. One way to represent the

numbers is in terms of spinning particles–many fundamental particles possess an inherent spin, and they can either spin eastward or westward, rather like a basketball spinning on the end of a finger. When a particle is spinning eastward it represents 1, and when it is spinning westward it represents 0. Hence, a sequence of spinning particles represents a sequence of 1's and 0's, or a binary number. For example, seven particles, spinning east, east, west, east, west, west, west respectively, together represent the binary number 1101000, which is equivalent to the decimal number 104. Depending on their spins, a combination of seven particles can represent any number between 0 and 127.

With a traditional computer, the operator would then input one particular sequence of spins, such as west, west, west, west, west, west, east, which represents 0000001, which is simply the decimal number 1. The operator would then wait for the computer to test the number to see whether it fits the criterion mentioned earlier. Next the operator would input 0000010, which would be a sequence of spinning particles representing 2, and so on. As before, the numbers would have to be entered one at a time, which we know to be time-consuming. However, if we are dealing with a quantum computer, the operator has an alternative way of inputting numbers which is much faster. Because each particle is fundamental, it obeys the laws of quantum physics. Hence, when a particle is not being observed it can enter a superposition of states, which means that it is spinning in both directions at the same time, and so is representing both 0 and 1 at the same time. Alternatively, we can think of the particle entering two different universes: in one universe it spins eastward and represents 1, while in the other it spins westward and represents 0.

The superposition is achieved as follows. Imagine that we can observe one of the particles, and it is spinning westward. To change its spin, we would fire a sufficiently powerful pulse of energy, enough to kick the particle into spinning eastward. If we were to fire a weaker pulse, then sometimes we would be lucky and the particle would change its spin, and sometimes we would be unlucky and the particle would keep its westward spin. So far the particle has been in clear view all along, and we have been able to follow its progress. However, if the particle is spinning westward and put in a box out of our view, and we fire a weak pulse of energy at it,

then we have no idea whether its spin has been changed. The particle enters a superposition of eastward and westward spins, just as the cat entered a superposition of being dead and alive. By taking seven westward-spinning particles, placing them in a box, and firing seven weak pulses of energy at them, then all seven particles enter a superposition.

With all seven particles in a superposition, they effectively represent all possible combinations of eastward and westward spins. The seven particles simultaneously represent 128 different states, or 128 different numbers. The operator inputs the seven particles, while they are still in a superposition of states, into the quantum computer, which then performs its calculations as if it were testing all 128 numbers simultaneously. After 1 second the computer outputs the number, 69, which fulfills the requested criterion. The operator gets 128 computations for the price of one.

A quantum computer defies common sense. Ignoring the details for a moment, a quantum computer can be thought of in two different ways, depending on which quantum interpretation you prefer. Some physicists view the quantum computer as a single entity that performs the same calculation simultaneously on 128 numbers. Others view it as 128 entities, each in a separate universe, each performing just one calculation. Quantum computing is *Twilight Zone* technology.

When traditional computers operate on 1's and 0's, the 1's and 0's are called bits, which is short for binary digits. Because a quantum computer deals with 1's and 0's that are in a quantum superposition, they are called quantum bits, or *qubits* (pronounced "cubits"). The advantage of qubits becomes even clearer when we consider more particles. With 250 spinning particles, or 250 qubits, it is possible to represent roughly 10^{75} combinations, which is greater than the number of atoms in the universe. If it were possible to achieve the appropriate superposition with 250 particles, then a quantum computer could perform 10^{75} simultaneous computations, completing them all in just one second.

The exploitation of quantum effects could give rise to quantum computers of unimaginable power. Unfortunately, when Deutsch created his vision of a quantum computer in the mid-1980s, nobody could quite envisage how to create a solid, practical machine. For example, scientists could not actually build anything that could calculate with spinning particles in a superposition of states. One of the greatest hurdles was

maintaining a superposition of states throughout the calculation. A superposition exists only while it is not being observed, but an observation in the most general sense includes any interaction with anything external to the superposition. A single stray atom interacting with one of the spinning particles would cause the superposition to collapse into a single state and cause the quantum calculation to fail.

Another problem was that scientists could not work out how to program a quantum computer, and were therefore not sure what sort of computations it might be capable of doing. However, in 1994 Peter Shor of AT&T Bell Laboratories in New Jersey did succeed in defining a useful program for a quantum computer. The remarkable news for cryptanalysts was that Shor's program defined a series of steps that could be used by a quantum computer to factor a giant number–just what was required to crack the RSA cipher. When Martin Gardner set his RSA challenge in *Scientific American*, it took six hundred computers several months to factor a 129-digit number. In comparison, Shor's program could factor a number a million times bigger in one-millionth of the time. Unfortunately, Shor could not demonstrate his factorization program, because there was still no such thing as a quantum computer.

Then, in 1996, Lov Grover, also at Bell Labs, discovered another powerful program. Grover's program is a way of searching a list at incredibly high speed, which might not sound particularly interesting until you realize that this is exactly what is required to crack a DES cipher. To crack a DES cipher it is necessary to search a list of all possible keys in order to find the correct one. If a conventional computer can check a million keys a second, it would take over a thousand years to crack a DES cipher, whereas a quantum computer using Grover's program could find the key in less than four minutes.

It is purely coincidental that the first two quantum computer programs to be invented have been exactly what cryptanalysts would have put at the top of their wish lists. Although Shor's and Grover's programs generated tremendous optimism among codebreakers, there was also immense frustration, because there was still no such thing as a working quantum computer that could run these programs. Not surprisingly, the potential of the ultimate weapon in decryption technology has whetted the appetite of organizations such as America's Defense Advanced Research Projects Agency (DARPA) and the Los Alamos National Laboratory, who are desperately trying to build devices that can handle qubits, in the same way that silicon chips handle bits. Although a number of recent breakthroughs have boosted morale among researchers, it is fair to say that the technology remains remarkably primitive. In 1998, Serge Haroche at the University of Paris VI put the hype surrounding the breakthroughs into perspective when he dispelled claims that a real quantum computer is only a few years away. He said this was like painstakingly assembling the first layer of a house of cards, then boasting that the next 15,000 layers were a mere formality.

Only time will tell if and when the problems of building a quantum computer can be overcome. In the meantime, we can merely speculate as to what impact it would have on the world of cryptography. Ever since the 1970s, codemakers have had a clear lead in the race against codebreakers, thanks to ciphers such as DES and RSA. These sorts of ciphers are a precious resource, because we have come to trust them to encrypt our e-mails and guard our privacy. Similarly, as we enter the twenty-first century more and more commerce will be conducted on the Internet, and the electronic marketplace will rely on strong ciphers to protect and verify financial transactions. As information becomes the world's most valuable commodity, the economic, political and military fate of nations will depend on the strength of ciphers.

Consequently, the development of a fully operational quantum computer would imperil our personal privacy, destroy electronic commerce and demolish the concept of national security. A quantum computer would jeopardize the stability of the world. Whichever country gets there first will have the ability to monitor the communications of its citizens, read the minds of its commercial rivals and eavesdrop on the plans of its enemies. Although it is still in its infancy, quantum computing presents a potential threat to the individual, to international business and to global security.

Quantum Cryptography

While cryptanalysts anticipate the arrival of quantum computers, cryptographers are working on their own technological miracle–an encryption system that would reestablish privacy, even when confronted

with the might of a quantum computer. This new form of encryption is fundamentally different from any that we have previously encountered in that it offers the hope of perfect privacy. In other words, this system would be flawless and would guarantee absolute security for eternity. Furthermore, it is based on quantum theory, the same theory that is the foundation for quantum computers. So while quantum theory is the inspiration for a computer that could crack all current ciphers, it is also at the heart of a new unbreakable cipher called *quantum cryptography*.

The story of quantum cryptography dates back to a curious idea developed in the late 1960s by Stephen Wiesner, then a graduate student at Columbia University. Sadly, it was Wiesner's misfortune to invent an idea so ahead of its time that nobody took it seriously. He still recalls the reaction of his seniors: "I didn't get any support from my thesis adviser–he showed no interest in it at all. I showed it to several other people, and they all pulled a strange face, and went straight back to what they were already doing." Wiesner was proposing the bizarre concept of quantum money, which had the great advantage of being impossible to counterfeit.

Wiesner's quantum money relied heavily on the physics of photons. When a photon travels through space it vibrates, as shown in Figure 73(a). All four photons are traveling in the same direction, but the angle of vibration is different in each case. The angle of vibration is known as the polarization of the photon, and a lightbulb generates photons of all polarizations, which means that some photons will vibrate up and down, some from side to side, and others at all angles in between. To simplify matters, we shall assume that photons have only four possible polarizations, which we label ↕, ↔, ↖↘ and ↗↙.

By placing a filter known as a Polaroid in the path of the photons, it is possible to ensure that the emerging beam of light consists of photons that vibrate in one particular direction; in other words, the photons all have the same polarization. To some extent, we can think of the Polaroid filter as a grating, and photons as matchsticks randomly scattered onto the grating. The matchsticks will slip through the grating only if they are at the correct angle. Any photon that is already polarized in the same direction as the Polaroid filter will automatically pass through it unchanged, and photons that are polarized perpendicular to the filter will be blocked.

Unfortunately, the matchstick analogy breaks down when we think about diagonally polarized photons approaching a vertical Polaroid filter. Although matchsticks oriented diagonally would be blocked by a vertical grating, this is not necessarily the case with diagonally polarized photons approaching a vertical Polaroid filter. In fact, diagonally polarized photons are in a quantum quandary when confronted by a vertical Polaroid filter. What happens is that, half of them at random will be blocked, and half will pass through, and those that do pass through will be reoriented with a vertical polarization. Figure 73(b) shows eight photons approaching a vertical Polaroid filter, and Figure 73(c) shows that only four of them successfully pass through it. All the vertically polarized photons have passed through, all the horizontally polarized photons have been blocked, and half of the diagonally polarized photons have passed through.

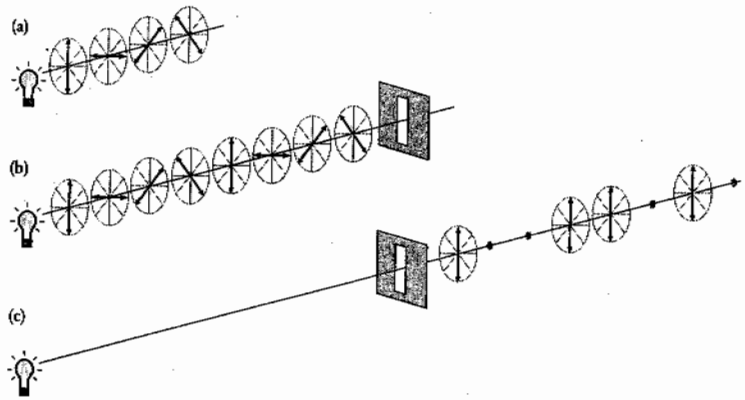

Figure 73 (a) Although photons of light vibrate in all directions, we assume for simplicity that there are just four distinct directions, as shown in this diagram. (b) The lamp has emitted eight photons, which are vibrating in various directions. Each photon is said to have a polarization. The photons are heading toward a vertical Polaroid filter. (c) On the other side of the filter, only half the photons have survived. The vertically polarized photons have passed through, and the horizontally polarized photons have not. Half the diagonally polarized photons have passed through, and are thereafter vertically polarized.

It is this ability to block certain photons that explains how Polaroid sunglasses work. In fact, you can demonstrate the effect of Polaroid filters by experimenting with a pair of Polaroid sunglasses. First remove one lens, and close that eye so that you are looking with just the other eye through the remaining lens. Not surprisingly, the world looks quite dark because the lens blocks many of the photons that would otherwise have reached your eye. At this point, all the photons reaching your eye have the same polarization. Next, hold the other lens in front of the lens you are looking through, and rotate it slowly. At one point in the rotation, the loose lens will have no effect on the amount of light reaching your eye because its orientation is the same as the fixed lens–all the photons that get through the loose lens also pass through the fixed lens. If you now rotate the loose lens through 90°, it will turn completely black. In this configuration, the polarization of the loose lens is perpendicular to the polarization of the fixed lens, so that any photons that get through the loose lens are blocked by the fixed lens. If you now rotate the loose lens by 45°, then you reach an intermediate stage in which the lenses are partially misaligned, and half of the photons that pass through the loose lens manage to get through the fixed lens.

Wiesner planned to use the polarization of photons as a way of creating dollar bills that can never be forged. His idea was that dollar bills should each contain 20 light traps, tiny devices that are capable of capturing and retaining a photon. He suggested that banks could use four Polaroid filters oriented in four different ways (↕, ↔, ↖↘, ↗↙) to fill the 20 light traps with a sequence of 20 polarized photons, using a different sequence for each dollar bill. For example, Figure 74 shows a bill with the polarization sequence (↖↘ ↕ ↗↙ ↗↙ ↔ ↕ ↕ ↖↘ ↕ ↖↘ ↔↔ ↗↙ ↔ ↖↘ ↗↙ ↔ ↗↙ ↕ ↕). Although the polarizations are explicitly shown in Figure 74, in reality they would be hidden from view. Each note also carries a traditional serial number, which is B2801695E for the dollar bill shown. The issuing bank can identify each dollar bill according to its polarization sequence and its printed serial number, and would keep a master list of serial numbers and the corresponding polarization sequences.

A counterfeiter is now faced with a problem–he cannot merely forge a dollar bill which carries an arbitrary serial number and a random polarization sequence in the light traps, because this pairing will not appear on the bank's master list, and the bank will spot that the dollar bill is a fake. To create an effective forgery, the counterfeiter must use a genuine bill as a sample, somehow measure its 20 polarizations, and then make a duplicate dollar bill, copying across the serial number and loading the light traps in the appropriate way. However, measuring photon polarizations is a notoriously tricky task, and if the counterfeiter cannot accurately measure them in the genuine sample bill, then he cannot hope to make a duplicate.

To understand the difficulty of measuring the polarization of photons, we need to consider how we would go about trying to perform such a measurement. The only way to learn anything about the polarization of a photon is by using a Polaroid filter. To measure the polarization of the photon in a particular light trap, the counterfeiter selects a Polaroid filter and orients it in a particular way, say vertically, ↕. If the photon emerging from the light trap happens to be vertically polarized, it will pass through the vertical Polaroid filter and the counterfeiter will correctly assume that

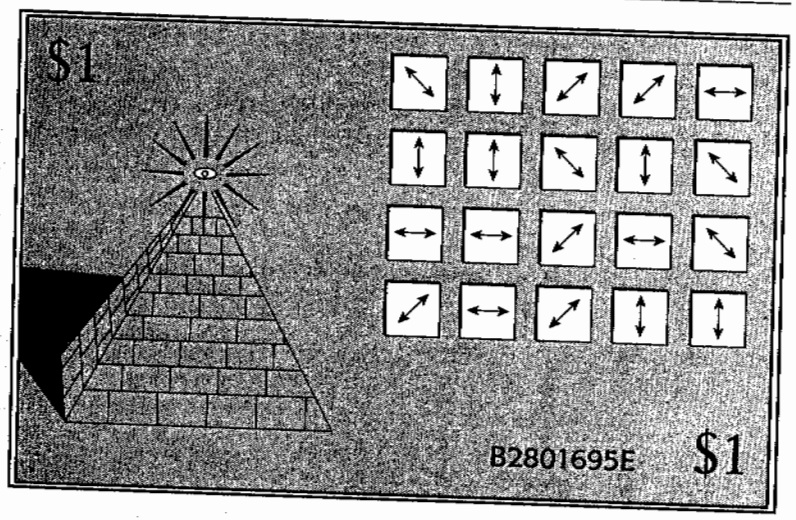

Figure 74 Stephen Wiesner's quantum money. Each note is unique because of its serial number, which can be seen easily, and the 20 light traps, whose contents are a mystery. The light traps contain photons of various polarizations. The bank knows the sequence of polarizations corresponding to each serial number, but a counterfeiter does not.

it is a vertically polarized photon. If the emerging photon is horizontally polarized, it will not pass through the vertical Polaroid filter, and the counterfeiter will correctly assume that it is a horizontally polarized photon. However, if the emerging photon happens to be diagonally polarized (↘ or ↗), it might or might not pass through the filter, and in either case the counterfeiter will fail to identify its true nature. A ↘ photon might pass through the vertical Polaroid filter, in which case the counterfeiter will wrongly assume that it is a vertically polarized photon, or the same photon might not pass through the filter, in which case he will wrongly assume that it is a horizontally polarized photon. Alternatively, if the counterfeiter chooses to measure the photon in another light trap by orientating the filter diagonally, say ↖, then this would correctly identify the nature of a diagonally polarized photon, but it would fail to accurately identify a vertically or horizontally polarized photon.

The counterfeiter's problem is that he must use the correct orientation of Polaroid filter to identify a photon's polarization, but he does not know which orientation to use because he does not know the polarization of the photon. This catch-22 is an inherent part of the physics of photons. Imagine that the counterfeiter chooses a ↖-filter to measure the photon emerging from the second light trap, and the photon does not pass through the filter. The counterfeiter can be sure that the photon was not ↖-polarized, because that type of photon would have passed through. However, the counterfeiter cannot tell whether the photon was ↗-polarized, which would certainly not have passed through the filter, or whether it was ↕- or ↔-polarized, either of which stood a fifty-fifty chance of being blocked.

This difficulty in measuring photons is one aspect of the uncertainty principle, developed in the 1920s by the German physicist Werner Heisenberg. He translated his highly technical proposition into a simple statement: "We *cannot* know, as a matter of principle, the present in all its details." This does not mean that we cannot know everything because we do not have enough measuring equipment, or because our equipment is poorly designed. Instead, Heisenberg was stating that it is logically impossible to measure every aspect of a particular object with perfect accuracy. In this particular case, we cannot measure every aspect of the photons within the light traps with perfect accuracy. The uncertainty principle is another weird consequence of quantum theory.

Wiesner's quantum money relied on the fact that counterfeiting is a two-stage process: first the counterfeiter needs to measure the original note with great accuracy, and then he has to replicate it. By incorporating photons in the design of the dollar bill, Wiesner was making the bill impossible to measure accurately, and hence creating a barrier to counterfeiting.

A naive counterfeiter might think that if he cannot measure the polarizations of the photons in the light traps, then neither can the bank. He might try manufacturing dollar bills by filling the light traps with an arbitrary sequence of polarizations. However, the bank is able to verify which bills are genuine. The bank looks at the serial number, then consults its confidential master list to see which photons should be in which light traps. Because the bank knows which polarizations to expect in each light trap, it can correctly orient the Polaroid filter for each light trap and perform an accurate measurement. If the bill is counterfeit, the counterfeiter's arbitrary polarizations will lead to incorrect measurements and the bill will stand out as a forgery. For example, if the bank uses a ↕-filter to measure what should be a ↕-polarized photon, but finds that the filter blocks the photon, then it knows that a counterfeiter has filled the trap with the wrong photon. If, however, the bill turns out to be genuine, then the bank refills the light traps with the appropriate photons and puts it back into circulation.

In short, the counterfeiter cannot measure the polarizations in a genuine bill because he does not know which type of photon is in each light trap, and cannot therefore know how to orient the Polaroid filter in order to measure it correctly. On the other hand, the bank is able to check the polarizations in a genuine bill, because it originally chose the polarizations, and so knows how to orient the Polaroid filter for each one.

Quantum money is a brilliant idea. It is also wholly impractical. To start with, engineers have not yet developed the technology for trapping photons in a particular polarized state for a sufficiently long period of time. Even if the technology did exist, it would be too expensive to implement it. It might cost in the region of $1 million to protect each dollar bill. Despite its impracticality, quantum money applied quantum theory in an intriguing and imaginative way, so despite the lack of encouragement from his thesis adviser, Wiesner submitted a paper to a scientific journal. It was rejected. He submitted it to three other journals, and it was rejected three

more times. Wiesner claims that they simply did not understand the physics.

It seemed that only one person shared Wiesner's excitement for the concept of quantum money. This was an old friend by the name of Charles Bennett, who several years earlier had been an undergraduate with him at Brandeis University. Bennett's curiosity about every aspect of science is one of the most remarkable things about his personality. He says he knew at the age of three that he wanted to be a scientist, and his childhood enthusiasm for the subject was not lost on his mother. One day she returned home to find a pan containing a weird stew bubbling on the cooker. Fortunately she was not tempted to taste it, as it turned out to be the remains of a turtle that the young Bennett was boiling in alkali in order to strip the flesh from the bones, thereby obtaining a perfect specimen of a turtle skeleton. During his teenage years, Bennett's curiosity

Figure 75 Charles Bennett.

moved from biology to biochemistry, and by the time he got to Brandeis he had decided to major in chemistry. At graduate school he concentrated on physical chemistry, then went on to do research in physics, mathematics, logic and, finally, computer science.

Aware of Bennett's broad range of interests, Wiesner hoped that he would appreciate quantum money, and handed him a copy of his rejected manuscript. Bennett was immediately fascinated by the concept, and considered it one of most beautiful ideas he had ever seen. Over the next decade he would occasionally reread the manuscript, wondering if there was a way to turn something so ingenious into something that was also useful. Even when he became a research fellow at IBM's Thomas J. Watson Laboratories in the early 1980s, Bennett still could not stop thinking about Wiesner's idea. The journals might not want to publish it, but Bennett was obsessed by it.

One day, Bennett explained the concept of quantum money to Gilles Brassard, a computer scientist at the University of Montreal. Bennett and Brassard, who had collaborated on various research projects, discussed the intricacies of Wiesner's paper over and over again. Gradually they began to see that Wiesner's idea might have an application in cryptography. For Eve to decipher an encrypted message between Alice and Bob, she must first intercept it, which means that she must somehow accurately perceive the contents of the transmission. Wiesner's quantum money was secure because it was impossible to accurately perceive the polarizations of the photons trapped in the dollar bill. Bennett and Brassard wondered what would happen if an encrypted message was represented and transmitted by a series of polarized photons. In theory, it seemed that Eve would be unable to accurately read the encrypted message, and if she could not read the encrypted message, then she could not decipher it.

Bennett and Brassard began to concoct a system based on the following principle. Imagine that Alice wants to send Bob an encrypted message, which consists of a series of 1's and 0's. She represents the 1's and 0's by sending photons with certain polarizations. Alice has two possible schemes for associating photon polarizations with 1 or 0. In the first scheme, called the *rectilinear* or +-scheme, she sends ↕ to represent 1, and ↔ to represent 0. In the other scheme, called the *diagonal* or ×-scheme, she sends ↗ to represent 1, and ↖ to represent 0. To send a binary

message, she switches between these two schemes in an unpredictable way. Hence, the binary message 1101101001 could be transmitted as follows:

Message	1	1	0	1	1	0	1	0	0	1
Scheme	+	×	+	×	×	×	+	+	×	×
Transmission	↕	↗	↔	↗	↗	↖	↕	↔	↖	↗

Alice transmits the first 1 using the +-scheme, and the second 1 using the ×-scheme. Hence, 1 is being transmitted in both cases, but it is represented by differently polarized photons each time.

If Eve wants to intercept this message, she needs to identify the polarization of each photon, just as the counterfeiter needs to identify the polarization of each photon in the dollar bill's light traps. To measure the polarization of each photon Eve must decide how to orient her Polaroid filter as each one approaches. She cannot know for sure which scheme Alice will be using for each photon, so her choice of Polaroid filter will be haphazard and wrong half the time. Hence, she cannot have complete knowledge of the transmission.

An easier way to think of Eve's dilemma is to pretend that she has two types of Polaroid detector at her disposal. The +-detector is capable of measuring horizontally and vertically polarized photons with perfect accuracy, but is not capable of measuring diagonally polarized photons with certainty, and merely misinterprets them as vertically or horizontally polarized photons. On the other hand, the ×-detector can measure diagonally polarized photons with perfect accuracy, but cannot measure horizontally and vertically polarized photons with certainty, misinterpreting them as diagonally polarized photons. For example, if she uses the ×-detector to measure the first photon, which is ↕, she will misinterpret it as ↗ or ↖. If she misinterprets it as ↗, then she does not have a problem, because this also represents 1, but if she misinterprets it as ↖ then she is in trouble, because this represents 0. To make matters worse for Eve, she only gets one chance to measure the photon accurately. A photon is indivisible, and so she cannot split it into two photons and measure it using both schemes.

This system seems to have some pleasant features. Eve cannot be sure of accurately intercepting the encrypted message, so she has no hope of deciphering it. However, the system suffers from a severe and apparently insurmountable problem–Bob is in the same position as Eve, inasmuch as he has no way of knowing which polarization scheme Alice is using for each photon, so he too will misinterpret the message. The obvious solution to the problem is for Alice and Bob to agree on which polarization scheme they will use for each photon. For the example above, Alice and Bob would share a list, or key, that reads + × + × × × + + × ×. However, we are now back to the same old problem of key distribution–somehow Alice has to get the list of polarization schemes securely to Bob.

Of course, Alice could encrypt the list of schemes by employing a public key cipher such as RSA, and then transmit it to Bob. However, imagine that we are now in an era when RSA has been broken, perhaps following the development of powerful quantum computers. Bennett and Brassard's system has to be self-sufficient and not rely on RSA. For months, Bennett and Brassard tried to think of a way around the key distribution problem. Then, in 1984, the two found themselves standing on the platform at Croton-Harmon station, near IBM's Thomas J. Watson Laboratories. They were waiting for the train that would take Brassard back to Montreal, and passed the time by chatting about the trials and tribulations of Alice, Bob and Eve. Had the train arrived a few minutes early, they would have waved each other goodbye, having made no progress on the problem of key distribution. Instead, in a *eureka!* moment, they created quantum cryptography, the most secure form of cryptography ever devised.

Their recipe for quantum cryptography requires three preparatory stages. Although these stages do not involve sending an encrypted message, they do allow the secure exchange of a key which can later be used to encrypt a message.

Stage 1. Alice begins by transmitting a random sequence of 1's and 0's (bits), using a random choice of rectilinear (horizontal and vertical) and diagonal polarization schemes. Figure 76 shows such a sequence of photons on their way to Bob.

Stage 2. Bob has to measure the polarization of these photons. Since he has no idea what polarization scheme Alice has used for each one, he randomly swaps between his +-detector and his ×-detector. Sometimes Bob picks the correct detector, and sometimes he picks the wrong one.

If Bob uses the wrong detector he may well misinterpret Alice's photon. Table 27 covers all the possibilities. For example, in the top line, Alice uses the rectilinear scheme to send **1**, and thus transmits ↕; then Bob uses the correct detector, so he detects ↕, and correctly notes down 1 as the first bit of the sequence. In the next line, Alice does the same thing, but Bob uses the incorrect detector, so he might detect ⤢ or ⤡, which means that he might correctly note down 1 or incorrectly note down **0**.

Stage 3. At this point, Alice has sent a series of 1's and 0's and Bob has detected some of them correctly and some of them incorrectly. To clarify the situation, Alice then telephones Bob on an ordinary insecure line, and tells Bob which polarization scheme she used for each photon–but not how she polarized each photon. So she might say that the first photon was sent using the rectilinear scheme, but she will not

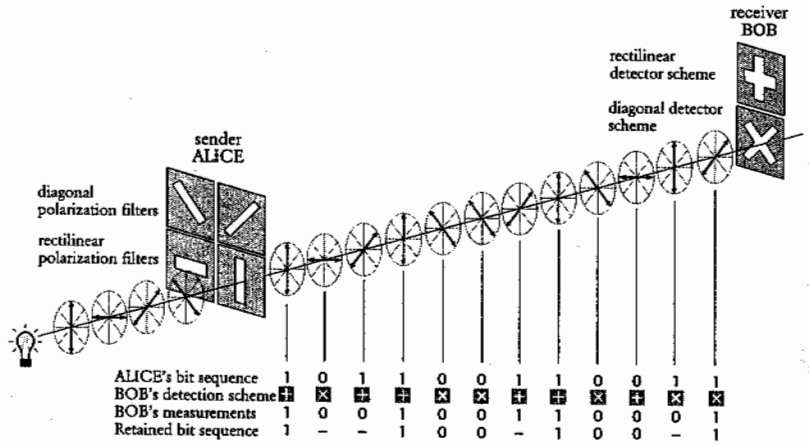

Figure 76 Alice transmits a series of 1's and 0's to Bob. Each 1 and each 0 is represented by a polarized photon, according to either the rectilinear (horizontal/vertical) or diagonal polarization scheme. Bob measures each photon using either his rectilinear or his diagonal detector. He chooses the correct detector for the leftmost photon and correctly interprets it as 1. However, he chooses the incorrect detector for the next photon. He happens to interpret it correctly as 0, but this bit is nevertheless later discarded because Bob cannot be sure that he has measured it correctly.

say whether she sent ↕ or ↔. Bob then tells Alice on which occasions he guessed the correct polarization scheme. On these occasions he definitely measured the correct polarization and correctly noted down 1 or 0. Finally, Alice and Bob ignore all the photons for which Bob used the wrong scheme, and concentrate only on those for which he guessed the right scheme. In effect, they have generated a new shorter sequence of bits, consisting only of Bob's correct measurements. This whole stage is illustrated in the table at the bottom of Figure 76.

These three stages have allowed Alice and Bob to establish a common series of digits, such as the sequence **11001001** agreed in Figure 76. The crucial property of this sequence is that it is random, because it is derived

Table 27 The various possibilities in stage 2 of photon exchange between Alice and Bob.

Alice's scheme	Alice's bit	Alice sends	Bob's detector	Correct detector?	Bob detects	Bob's bit	Is Bob's bit correct?
Rectilinear	1	↕	+	Yes	↕	1	Yes
			×	No	⤢	1	Yes
					⤡	0	No
	0	↔	+	Yes	↔	0	Yes
			×	No	⤢	1	No
					⤡	0	Yes
Diagonal	1	⤢	+	No	↕	1	Yes
					↔	0	No
			×	Yes	⤢	1	Yes
	0	⤡	+	No	↕	1	No
					↔	0	Yes
			×	Yes	⤡	0	Yes

from Alice's initial sequence, which was itself random. Furthermore, the occasions when Bob uses the correct detector are also random. The agreed sequence does not therefore constitute a message, but it could act as a random key. At last, the actual process of secure encryption can begin.

This agreed random sequence can be used as the key for a onetime pad cipher. Chapter 3 described how a random series of letters or numbers, the onetime pad, can give rise to an unbreakable cipher–not just practically unbreakable, but absolutely unbreakable. Previously, the only problem with the onetime pad cipher was the difficulty of securely distributing the random series, but Bennett and Brassard's arrangement overcomes this problem. Alice and Bob have agreed on a onetime pad, and the laws of quantum physics actually forbid Eve from successfully intercepting it. It is now time to put ourselves in Eve's position, and then we will see why she is unable to intercept the key.

As Alice transmits the polarized photons, Eve attempts to measure them, but she does not know whether to use the +-detector or the ×-detector. On half the occasions she will choose the wrong detector. This is exactly the same position that Bob is in, because he too picks the wrong detector half the time. However, after the transmission Alice tells Bob which scheme he should have used for each photon and they agree to use only the photons which were measured when Bob used the right detector. However, this does not help Eve, because for half these photons she will have measured them using the incorrect detector, and so will have misinterpreted some of the photons that make up the final key.

Another way to think about quantum cryptography is in terms of a pack of cards rather than polarized photons. Every playing card has a value and a suit, such as the jack of hearts or the six of clubs, and usually we can look at a card and see both the value and the suit at the same time. However, imagine that it is only possible to measure either the value or the suit, but not both. Alice picks a card from the pack, and must decide whether to measure the value or the suit. Suppose that she chooses to measure the suit, which is "spades," which she notes. The card happens to be the four of spades, but Alice knows only that it is a spade. Then she transmits the card down a phone line to Bob. While this is happening, Eve tries to measure the card, but unfortunately she chooses to measure its value, which is "four." When the card reaches Bob he decides to measure its suit, which is still "spades," and he notes this down. Afterward, Alice calls Bob and asks him if he measured the suit, which he did, so Alice and Bob now know that they share some common knowledge–they both have "spades" written on their notepads. However, Eve has "four" written on her notepad, which is of no use at all.

Next, Alice picks another card from the pack, say the king of diamonds, but, again, she can measure only one property. This time she chooses to measure its value, which is "king," and transmits the card down a phone line to Bob. Eve tries to measure the card, and she also chooses to measure its value, "king." When the card reaches Bob, he decides to measure its suit, which is "diamonds." Afterward, Alice calls Bob and asks him if he measured the card's value, and he has to admit that he guessed wrong and measured its suit. Alice and Bob are not bothered because they can ignore this particular card completely, and try again with another card chosen at random from the pack. On this last occasion Eve guessed right, and measured the same as Alice, "king," but the card was discarded because Bob did not measure it correctly. So Bob does not have to worry about his mistakes, because Alice and he can agree to ignore them, but Eve is stuck with her mistakes. By sending several cards, Alice and Bob can agree on a sequence of suits and values which can then be used as the basis for some kind of key.

Quantum cryptography allows Alice and Bob to agree on a key, and Eve cannot intercept this key without making errors. Furthermore, quantum cryptography has an additional benefit: it provides a way for Alice and Bob to find out if Eve is eavesdropping. Eve's presence on the line becomes apparent because every time that she measures a photon, she risks altering it, and these alterations become obvious to Alice and Bob.

Imagine that Alice sends ↖↘, and Eve measures it with the wrong detector, the +-detector. In effect, the +-detector forces the incoming ↖↘ photon to emerge as either a ↕ or a ↔ photon, because this is the only way the photon can get through Eve's detector. If Bob measures the transformed photon with his ×-detector, then he might detect ↖↘, which is what Alice sent, or he might detect ↗↙, which would be a mismeasurement. This is a problem for Alice and Bob, because Alice sent a diagonally polarized photon and Bob used the correct detector, yet he might have measured it incorrectly. In short, when Eve chooses the wrong detector, she will

"twist" some of the photons, and this will make Bob prone to errors, even when he is using the correct detector. These errors can be found if Alice and Bob perform a brief error-checking procedure.

The error checking is done after the three preliminary stages, by which time Alice and Bob should have identical sequences of 1's and 0's. Imagine that they have established a sequence that is 1,075 binary digits in length. One way for Alice and Bob to check that their respective sequences match would be for Alice to call Bob and read out her complete sequence to him. Unfortunately, if Eve is eavesdropping she would then be able to intercept the entire key. Checking the complete sequence is clearly unwise, and it is also unnecessary. Instead, Alice merely has to pick 75 of the digits at random and check just these. If Bob agrees with the 75 digits, it is highly unlikely that Eve was eavesdropping during the original photon transmission. In fact, the chances of Eve being on the line and not affecting Bob's measurement of these 75 digits are less than one in a billion. Because these 75 digits have been openly discussed by Alice and Bob, they must be discarded, and their onetime pad is thus reduced from 1,075 to 1,000 binary digits. On the other hand, if Alice and Bob find a discrepancy among the 75 digits, then they will know that Eve has been eavesdropping, and they would have to abandon the entire onetime pad, switch to a new line and start all over again.

To summarize, quantum cryptography is a system that ensures the security of a message by making it hard for Eve to read accurately a communication between Alice and Bob. Furthermore, if Eve tries to eavesdrop then Alice and Bob will be able to detect her presence. Quantum cryptography therefore allows Alice and Bob to exchange and agree upon a onetime pad in complete privacy, and thereafter they can use this as a key to encrypt a message. The procedure has five basic steps:

(1) Alice sends Bob a series of photons, and Bob measures them.

(2) Alice tells Bob on which occasions he measured them in the correct way. (Although Alice is telling Bob when he made the correct measurement, she is not telling him what the correct result should have been, so this conversation can be tapped without any risk to security.)

(3) Alice and Bob discard the measurements that Bob made incorrectly, and concentrate on those measurements he made correctly in order to create an identical pair of onetime pads.

(4) Alice and Bob check the integrity of their onetime pads by testing a few of the digits.

(5) If the verification procedure is satisfactory, they can use the onetime pad to encrypt a message; if the verification reveals errors, they know that the photons were being tapped by Eve, and they need to start all over again.

Fourteen years after Wiesner's paper on quantum money had been rejected by the science journals, it had inspired an absolutely secure system of communication. Now living in Israel, Wiesner is relieved that, at last, his work is being recognized: "Looking back, I wonder if I couldn't have made more of it. People have accused me of being a quitter, for not having tried harder to get my idea published–I guess they're right in a way–but I was a young graduate student, and I didn't have that much confidence. In any case, nobody seemed interested in quantum money."

Cryptographers greeted Bennett and Brassard's quantum cryptography with enthusiasm. However, many experimentalists argued that the system worked well in theory, but would fail in practice. They believed that the difficulty of dealing with individual photons would make the system impossible to implement. Despite the criticism, Bennett and Brassard were convinced that quantum cryptography could be made to work. In fact, they had so much faith in their system that they did not bother building the apparatus. As Bennett once put it, "there is no point going to the North Pole if you know it's there."

However, the mounting skepticism eventually goaded Bennett into proving that the system could really work. In 1988 he began accumulating the components he would need for a quantum cryptographic system, and took on a research student, John Smolin, to help assemble the apparatus. After a year of effort they were ready to attempt to send the first message ever to be protected by quantum cryptography. Late one evening they retreated into their light-tight laboratory, a pitch-black environment safe from stray photons that might interfere with the experiment. Having eaten a hearty dinner, they were well prepared for a long night of tinkering

with the apparatus. They set about the task of trying to send polarized photons across the room, and then measuring them using a +-detector and a ×-detector. A computer called Alice ultimately controlled the transmission of photons, and a computer called Bob decided which detector should be used to measure each photon.

After hours of tweaking, at around 3 A.M., Bennett witnessed the first quantum cryptographic exchange. Alice and Bob managed to send and receive photons, they discussed the polarization schemes that Alice had used, they discarded photons measured by Bob using the wrong detector and they agreed on a onetime pad consisting of the remaining photons. "There was never any doubt that it would work," recalls Bennett, "only that our fingers might be too clumsy to build it." Bennett's experiment had demonstrated that two computers, Alice and Bob, could communicate in absolute secrecy. This was a historic experiment, despite the fact that the two computers were separated by a distance of just 30 cm.

Ever since Bennett's experiment, the challenge has been to build a quantum cryptographic system that operates over useful distances. This is not a trivial task, because photons do not travel well. If Alice transmits a photon with a particular polarization through air, the air molecules will interact with it, causing a change in its polarization, which cannot be tolerated. A more efficient medium for transmitting photons is via an optic fiber, and researchers have recently succeeded in using this technique to build quantum cryptographic systems that operate over significant distances. In 1995, researchers at the University of Geneva succeeded in implementing quantum cryptography in an optic fiber that stretched 23 km from Geneva to the town of Nyon.

More recently, a group of scientists at Los Alamos National Laboratory in New Mexico has once again begun to experiment with quantum cryptography in air. Their ultimate aim is to create a quantum cryptographic system that can operate via satellites. If this could be achieved, it would enable absolutely secure global communication. So far the Los Alamos group has succeeded in transmitting a quantum key through air over a distance of 1 km.

Security experts are now wondering how long it will be before quantum cryptography becomes a practical technology. At the moment there is no advantage in having quantum cryptography, because the RSA cipher

already gives us access to effectively unbreakable encryption. However, if quantum computers were to become a reality, then RSA and all other modern ciphers would be useless, and quantum cryptography would become a necessity. So the race is on. The really important question is whether quantum cryptography will arrive in time to save us from the threat of quantum computers, or whether there will be a privacy gap, a period between the development of quantum computers and the advent of quantum cryptography. So far, quantum cryptography is the more advanced technology. The Swiss experiment with optic fibers demonstrates that it would be feasible to build a system that permits secure communication between financial institutions within a single city. Indeed, it is currently possible to build a quantum cryptography link between the White House and the Pentagon. Perhaps there already is one.

Quantum cryptography would mark the end of the battle between codemakers and codebreakers, and the codemakers emerge victorious. Quantum cryptography is an unbreakable system of encryption. This may seem a rather exaggerated assertion, particularly in the light of previous similar claims. At different times over the last two thousand years, cryptographers have believed that the monoalphabetic cipher, the polyalphabetic cipher and machine ciphers such as Enigma were all unbreakable. In each of these cases the cryptographers were eventually proved wrong, because their claims were based merely on the fact that the complexity of the ciphers outstripped the ingenuity and technology of cryptanalysts at one point in history. With hindsight, we can see that the cryptanalysts would inevitably figure out a way of breaking each cipher, or developing technology that would break it for them.

However, the claim that quantum cryptography is secure is qualitatively different from all previous claims. Quantum cryptography is not just effectively unbreakable, it is absolutely unbreakable. Quantum theory, the most successful theory in the history of physics, means that it is impossible for Eve to intercept accurately the onetime pad key established between Alice and Bob. Eve cannot even attempt to intercept the onetime pad key without Alice and Bob being warned of her eavesdropping. Indeed, if a message protected by quantum cryptography were ever to be deciphered, it would mean that quantum theory is flawed, which would have devastating implications for physicists; they would be forced to

reconsider their understanding of how the universe operates at the most fundamental level.

If quantum cryptography systems can be engineered to operate over long distances, the evolution of ciphers will stop. The quest for privacy will have come to an end. The technology will be available to guarantee secure communications for governments, the military, businesses and the public. The only question remaining would be whether or not governments would allow us to use the technology. How would governments regulate quantum cryptography, so as to enrich the Information Age, without protecting criminals?

The Cipher Challenge: 10 Steps to $15,000

The Ciper Challenge was initiated in September 1999, and remains unsolved as of press time. It is an opportunity to put your cipher cracking skills to the test and win a $15,000 prize. The Challenge consists of ten separate stages. The first stage is a relatively straightforward monoalphabetic cipher, and thereafter the stages will progress through the history of cryptography. In other words, the second stage contains a ciphertext that has been encrypted using one of the earliest ciphers, and the tenth stage contains one of the most modern forms of cipher. In general, each stage will be harder than the previous one.

What do you need to do in order to claim the prize?

Deciphering each of the ten ciphertexts will generate a message. In addition to the main body of each message, there will be a clearly indicated codeword. In order to claim the prize, you must collect all ten codewords. Hence, it is necessary to decipher all ten stages. Although you may tackle the stages in any order, I would recommend attacking them in the order given. In some cases, deciphering a stage will provide information that will be important for breaking the next stage.

How do you claim the prize?

To claim the prize, please send in the first two letters of each codeword, as well as your name, address and telephone number. If your letters are correct, you will be contacted within 28 days of receipt of your letter, and asked to send in the ten complete codewords. If you are the first to correctly identify all ten codewords, you will win $15,000.

All claims must be sent by registered mail to: The Cipher Challenge, P.O. Box 23064, London W11 3GX, UK.

The winner will be the first past the post. There is no element of chance, just skill. Please note, I will only contact competitors in the event of a correct winning entry. Furthermore, I will not be able to reply to any queries regarding the Cipher Challenge. Any updates on the challenge will be posted on the Cipher Challenge Web site, http://www.4thestate.co.uk/cipherchallenge

The one-year prize

If the prize has not been claimed by October 1, 2000, $1,500 will be awarded to whoever has made most progress soonest, which means completion of the most consecutive stages. In other words, if you have solved stages 1, 2, 3, 4 and 8, only stages 1–4 are valid in terms of competing for this prize. Before attempting to claim this prize, please check the Cipher Challenge Web site, which will indicate the current leader and the extent of that person's success. If you believe that you have progressed to the next stage, please send in the first two letters of the codewords from all the stages that you have deciphered, as well as your name, address and telephone number. If your