Entrust® Securing Digital Identities & Information

Quantum Computing and Cryptography

Their impact on cryptographic practice

Tim Moses
Director, Advanced Security Technology
Entrust, Inc.

January 2009

Table of Contents

1 Solving the Impossible

Recent years have seen significant advances in both quantum computing and quantum cryptography. Reports have hinted at radical implications for the practice of computing in general and information security in particular.

Certain well-known problems in the fields of modeling, optimization and cryptography have proven intractable using the classical model of computation. But, using a model of computation that exploits quantum mechanical phenomena, solutions to these problems become possible. If and when quantum computers of sufficient size become a reality, secure information systems based on public-key cryptography will require an overhaul.

Present-day cryptographic systems offer what is called "computational security"; in theory, at least, if one could assemble sufficient computing resources for sufficient time, then one could break them, although the cryptographic systems commonly in use today have been engineered to make this a possibility in theory only.

Quantum mechanical phenomena offer the possibility of "absolute security": systems that are secure no matter how much resource is available to attack them. Quantum cryptography is in use today in specialized applications, but it lacks the flexibility that conventional cryptographic systems can provide.

2 Quantum Mechanics

The scale of everyday experience extends from fractions of an inch to thousands of miles. Years of exploring this range of physical scales makes us feel that we understand how objects will behave under most circumstances.

Until as recently as a hundred years ago it was thought that our understanding of the everyday scale would enable us to understand how things behave on both a much larger and a much smaller scale. However, scientific developments in the 20th century showed us that this was not the case.

Einstein’s general theory of relativity, for instance, has shown us that, on the large scale, space-time is curved by the presence of mass. Our familiarity with the everyday scale did not prepare us for this conclusion. The same turns out to be true for scales much smaller than those encountered in everyday experience.

One of the first hints of this was the so-called two-slit experiment. It was observed in 1927 by Clinton Davisson at Bell Labs that, when you place a barrier with a single slit 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 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 passes 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, but quite distinct, concepts at the everyday scale. But, at the subatomic scale, objects appear to possess the properties of both.

This observation was one of the first to suggest that classical theories were inadequate to explain events on the subatomic scale and that 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 the everyday scale, such as tennis balls.

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 once they are observed. While the probability functions are entirely amenable to analysis, the concrete values they adopt when observed appear to be random. If you find this hard to believe, then you are in good company. In fact, Niels Bohr once remarked that anyone who is not shocked by quantum theory has not understood it.

Nevertheless, quantum theory has been called the most successful scientific theory ever developed, because of the broad range of experimental observations with which it is consistent.

One of the most dramatic illustrations of the probabilistic wave function representation of objects on the quantum scale is a thought experiment described by Erwin Schrödinger, and that is universally referred to as “Schrödinger’s cat.” 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 from the radioactive source, 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: the cat dies and the cat lives, exist simultaneously until the box is opened and the fate of the cat is determined. To the best of our knowledge, no one has actually attempted to perform this experiment. But, if they were to, we can be confident that their observations would be entirely consistent with this theory.

What we should take from this thought experiment is that quantum objects adopt multiple states simultaneously — a process called superposition — and that they collapse to a single random state only when they are observed.

These properties can be exploited to create an entirely new model of computation; one that can solve problems that have proven intractable to classical models. They can also form the basis for new cryptographic schemes: ones that offer absolute security in certain specialized applications.

3 Quantum Computing

Quantum computing is a new model of computation that takes advantage of the strange and wonderful properties of quantum objects. Certain problems, whose difficulty increases exponentially with the problem size in the classical model, scale polynomially (or even linearly) in the quantum model, thereby making a solution possible even for large systems.

A Practical Quantum Computer

In the classical computing model, the basic unit of information is a “bit,” which can adopt one of two mutually exclusive states; either a "0" or a "1." The most elementary computing operation is a gate, which takes some number of bits at its inputs and produces a bit at its output, the value of the output bit bearing some relationship to the value of the input bits. These gates can be combined into circuits to realize more complex operations, such as a data-processing unit.

Similarly, in the quantum computing model, the basic unit of information is called the “quantum bit” or “qubit,” which can be realized in any of what physicists call an “ideal two-state quantum system.” Examples of suitable systems include photons (with vertical and horizontal polarization representing the two orthogonal states), electrons and other spin-1/2 systems (with spin up and down representing the two orthogonal states) and systems defined by two energy levels of atoms or ions.

Each state corresponds to the familiar "0" and "1" bit values. But qubits can also take on values that are superpositions of these two states. Thus, they can be thought of as occupying a state that is a combination of both a "0" state and a "1" state. While quantum mechanics describes a number of intriguing phenomena, superposition is the one that has received the most attention for its suitability as the basis of a quantum computer.

Scientists have been able to develop gates for some two-state quantum systems that take qubits as input and output a qubit. The superposition state of the output qubit depends deterministically upon the superposition states of its inputs. These gates can then be combined into a circuit that implements an algorithm to solve a specific mathematical problem.

The internal qubits of a quantum computer may maintain their state superpositions for the duration of the calculation, until the result is read out. Only then will the output state collapse to a concrete value representing the solution to the problem.

One company has announced that it has built a commercial quantum computer, based on a superconductivity effect, with a 28-qubit register, although some experts are skeptical about this claim. The computer architecture is designed to address optimization problems. And, it is not suitable for problems of interest to cryptographers. Nevertheless, experts predict that, in 15-20 years, quantum computers will exist that are large enough to solve practical problems, including those in the field of cryptography.

Quantum computers are not general-purpose programmable machines. They are not going to replace classical computers in all applications, offering a way of extending Moore's Law beyond its present time horizon. Rather there is a limited set of important mathematical problems that cannot be solved with the classical computing model and that fall easily to attack by a quantum computer.

Implications for Information Security

Should large quantum computers ever be built, there will be at least two important implications for information security. Quantum computers will impact the security of both symmetric-key algorithms (e.g. block ciphers) and public-key algorithms (such as RSA), although the seriousness of the impact will be different for each.

For a strong block cipher with an N-bit key, 2^N classical operations are required to be certain of finding the key. This is accomplished by searching through all 2^N possible keys, decrypting ciphertext with each, until a plausible plaintext is obtained. Then the right key has been found.

For example, AES-128 uses a key of 128 bits, and so 2^{128} operations are required to recover the key. Keys of this size provide very strong security, and most cryptographers believe that they should be secure for at least the next 20 years.

Quantum computers, on the other hand, can run an algorithm called “unstructured quantum search” that can break a symmetric cipher substantially faster than classical algorithms can. It can find a key in $2^{N/2}$ operations. Using the example above, unstructured quantum search would require 2^{64} operations to recover an AES-128 key.

In these circumstances, AES-128 would be considered insecure for many applications. And in order to restore the required level of security, it would be necessary to switch to AES-256. Indeed, AES-256 was developed with just such an eventuality in mind.

The implications for public-key cryptography are more serious. Quantum computers can run algorithms that break all the popular public-key systems in trivial amounts of time. For instance, a quantum algorithm called Shor's algorithm can recover an RSA key in polynomial time.

Shor's Algorithm

It is tempting to think that quantum computers attack cryptanalytic problems using superposition to conduct an exhaustive search of the key space in parallel. But, this is not the case.

Shor's algorithm implements the quantum analog of the fast Fourier transform to find the 'period' of the RSA operation $P = P^{ed}$ (Mod n).

While it is not possible, using a quantum computer, to discover the coefficients of the transform, it is possible to discover the period. And, given the public key and the period, it is possible to discover the private key.

The quantum Fourier transform scales polynomially with the size of the RSA modulus. Hence, breaking RSA becomes a practical proposition.

Similar algorithms exist for all commonly used public-key algorithms including DSA, Diffie-Hellman and ECC. If large quantum computers can be built, then these ciphers become useless. It is estimated that 2048-bit RSA keys could be broken on a quantum computer comprising 4,000 qubits and 100 million gates. Experts speculate that quantum computers of this size may be available within the next 20-30 years.

There do exist some public-key algorithms that do not appear to be vulnerable to attack by quantum computers, although none of them is as well-studied as the ones in common use today.

Many of the public-key systems based upon the lattice reduction problem, such as schemes whose basic elements are polynomials, appear to resist quantum attacks. In fact, the American National Standards Institute is developing a standard for a polynomial-based public key establishment protocol, with just this possibility in mind.

Ralph Merkle, in some of his pioneering work on public-key cryptography, has also developed algorithms that appear to be invulnerable to the quantum computational model. These include his puzzle scheme for key agreement and his one-time signature scheme that uses just hash functions to create signatures.

None of these options has been the subject of enough practical research to be implemented with confidence today. But, given the long timeframe that appears to be available for their development, these, and other algorithms, will certainly be ready for prime-time before current methods are rendered insecure.

Even more certain is the possibility that symmetric-key approaches, like Kerberos, will be a practical replacement for today's public-key solutions.

Quantum cryptography is another key distribution method that would be immune from quantum computing attacks, for those environments in which quantum cryptography is applicable. This is because quantum cryptography provides "absolute security." Note, however, that there are certain auxiliary operations within quantum cryptographic schemes that depend upon symmetric or public-key cryptography, and these would be impacted exactly as described above.

4 Quantum Cryptography

There are two areas of cryptography that can potentially benefit from the application of quantum mechanical techniques: random number generation and key distribution.

Random Number Generation

Many of the processes that we commonly think of as random are not truly random at all: we merely lack the data or computing power to predict their future values. For instance, if we had sufficient information about a piece of buttered toast falling toward a carpeted floor we would be able to predict whether it will land butter-side down or butter-side up. (In actuality, Murphy's Law governs the situation, and the toast will always land butter-side down.) Quantum processes on the other hand are truly random. No amount of computing power will enable us to make predictions about their future values.

Most cryptographic mechanisms use keys to protect either the confidentiality or integrity of data. These keys must be unpredictable to an attacker, so they are usually produced by a random process. But, it is very difficult to demonstrate the amount of entropy exhibited by a software-only random number generator.

So, true randomness, such as that exhibited by quantum processes is of enormous interest to cryptographers. And practical ways have been found to generate random numbers using quantum mechanical processes such as tunneling and radioactive decay.

The Key Distribution Problem

The key distribution problem is encountered by any two parties that want to communicate securely. If Alice and Bob want to use a traditional block cipher and message authentication code to protect their communications, they need first of all to agree upon a key. Today, this problem is usually solved by public-key cryptography.

Alice and Bob each generate a public-private key pair and register the public part with a certification authority (CA). The CA then creates a certificate for each public key and distributes it to the other. Alice and Bob can now use their own private key and the public key from the other's certificate to agree on a shared symmetric key with which to protect their communication. A number of algorithms and protocols exist for doing this, including Diffie-Hellman key agreement and RSA key transport.

Public-key cryptography is currently a secure way to protect information. Using the key sizes commonly in use today, it appears infeasible for an attacker to obtain a user's private key solely by analyzing his or her public key, which is what would typically be required to break a public-key scheme.

However, in theory, if sufficient computing power were available, or if a solution were to be found to the mathematical problem upon which the algorithm is based, then these schemes would be vulnerable to attack. There is no reason to believe that either of these outcomes will occur in the foreseeable future. However, since the security provided is "computational," rather than "absolute," researchers are interested in finding better approaches.

The Quantum Solution

Quantum cryptography is not a new cipher and it does not completely replace all uses of symmetric and public-key cryptography. It does, however, provide a radically different approach to the key distribution problem.

Like public-key cryptography, it allows Alice and Bob to securely agree on a key over an insecure channel. The key can then be used in a conventional symmetric cipher, message authentication code or one-time-pad.

Quantum cryptography provides absolute security because, unlike traditional cryptographic schemes that are based upon hard mathematical problems, it is based on a physical law known as the Heisenberg Uncertainty Principle.

In its original formulation, this law states that a particle's measured position and momentum cannot both be known with arbitrary precision. That is, the more certainty there is about a particle's position, the more uncertainty there is about its momentum, and vice versa.

Heisenberg's uncertainty principle has since been generalized to cover other pairs of properties such as energy and time, horizontal and vertical polarizations, etc. Each of these pairs of properties is known as a conjugate variable and each has the property that the more precisely one knows one of the properties, the less precisely one can know the other.

Musical Analogy

Consider a musical sound. It is not possible to measure both the instant in time at which a sound occurs and its pitch with exact precision.

If it has a pitch, then it must have a duration, and the greater the duration, the less precisely determined is the instant of occurrence, and the more precise determined is the pitch. The converse is equally true.

A similar situation exists with quantum particles. They possess both position and momentum. But, it is impossible to determine both precisely.

The more precisely one knows the position, the less precisely one knows the momentum — and vice-versa. This is not a consequence of inadequate measuring techniques, but a fundamental property of matter.

Before looking at how quantum cryptography actually works, let's consider an analogous model. Alice wants to agree upon a 1-bit value with Bob (if she wants to exchange a larger value, she can simply repeat the procedure the required number of times).

Alice has a box with two compartments. She puts a coin in each compartment. The compartments are constructed in such a way that they can be opened individually, but there is an interlock that prevents them both being open at the same time. Furthermore, when one compartment is opened, the floor of the other compartment jumps, so that the coin in that compartment flips and lands randomly on either heads or tails.

In order to send a 1-bit value to Bob, Alice chooses one of the compartments at random and places a coin in it so that the visible face represents the value she wants to send. She then puts another coin in the other compartment with a random face uppermost. On receiving the box, Bob guesses which compartment Alice used for the significant coin, he opens it and reads the value.

If he opens the wrong compartment he will get a random value and the value that Alice intended to send him will be lost forever. Similarly, an attacker that doesn't know which compartment to open will have a 50-50 chance of opening the wrong compartment and reading the random value. If the attacker then passes the box along to Bob, there is a 50-50 chance that she will have changed the value being exchanged to a completely random value, thereby introducing an error.

After Alice sends the box multiple times, she and Bob compare the compartment in which she placed the coin with the one that he opened each time, and they discard the results for which Bob guessed wrongly. Even if an attacker were to eavesdrop on this conversation, the odds are against her having made the same choices as Bob for all bits, and so there will almost certainly be errors in the bit sequence she obtains. Also, the bit sequence received by Bob will have been corrupted. So, he and Alice only have to compare some subset of bits to discover that the exchange has been compromised.

Quantum cryptography works in a similar way. Using as an example polarized photons, the polarization state can be represented using either the rectilinear basis of vertical and horizontal polarization or the diagonal basis of 45° and 135°.

Alice creates a random bit and randomly selects one of the two bases (rectilinear or diagonal) in which to transmit it. She then prepares a photon polarization state depending both on the bit value and the basis and transmits the photon to Bob. This process is then repeated for each bit in the sequence.

According to the laws of quantum mechanics, there is no possible measurement that can distinguish between the four different polarization states, as they are not all orthogonal. The only measurement possible is between any two orthogonal states (a basis), so, for example, measuring in the rectilinear basis will give a result of horizontal or vertical.

If the photon was created as horizontally or vertically polarized then this will measure the correct state, but if it was created as 45° or 135°, then the rectilinear measurement will instead return either horizontal or vertical at random. Furthermore, after this measurement, the photon will be polarized in the state in which it was measured (horizontal or vertical), with all information about its initial polarization lost.

An attacker could attempt to measure the photon polarization and decode the bit values. However, like Bob, she will not know which basis Alice used. The attacker will not be able to measure those polarizations that she guesses incorrectly and, thus, will necessarily introduce errors into the sequence, just as if she had opened the wrong compartment of our fictitious box. Alice and Bob can detect these errors by publicly comparing some number of the exchanged values and rejecting the key stream if a significant number are in error. So, according to the laws of quantum physics the attack will be detected and the sequence can be discarded.

Quantum vs. Public-Key Cryptography

Quantum cryptography is practical today. It has been implemented and keys have been exchanged over distances of greater than 100 km/62.1 miles. Key agreement is possible at rates of about 2 kilobits per second; and not just in the laboratory. There are commercial companies that are currently selling equipment to perform quantum key distribution along the lines described above.

The story behind quantum cryptography is very attractive. However, there are a few details that limit its widespread application. To begin with, notice that in order for Alice and Bob to agree upon the basis that was encoded or to detect errors introduced by an attacker, they need to communicate over an authentic channel. Confidentiality is not required, as no security is lost if the attacker can see these communications.

However, they need to be sure that the attacker is not modifying the communication and thereby disguising her activities. Typically, an authentic channel is obtained by the two parties sharing a cryptographic key that can be used as part of a cryptographic integrity mechanism. Thus, Alice and Bob will usually need to have some previously shared information in order to use quantum key distribution in a secure manner. This is actually not substantially better than the current situation of agreeing upon keys using public-key cryptography.

It is also worth noting that, currently, in order for Alice to transmit a photon to Bob, both Alice and Bob must be online at the same time and they must have an unbroken, continuous communication channel (e.g., a single optical fiber) between them.

Research is being conducted that may make a "quantum router" practical. Such a device would regenerate a photon, preserving its polarization. This would allow quantum cryptography to operate over a network. Regardless, a real-time communication channel is required, because currently there is no way to store the photon for measurement at a later time.

Also, Alice and Bob must communicate — both to agree upon the encoding basis and to detect errors — after transmission and reception of the photon, but before the key is used. Thus, quantum cryptography does not lend itself to many common uses of cryptography, such as store-and-forward encryption (as is used in file encryption and secure e-mail) and situations where there may be many intermediaries (as on the Internet). Research is continuing in order to overcome these limitations.

Quantum cryptography does not, currently, provide a satisfactory method of obtaining a digital signature. Digital signatures, and the integrity and authenticity protection that they provide, are one of the most important uses of public-key cryptography.

Currently proposed quantum digital signature schemes only allow signature verification by a small number of people, or they exhibit other impracticalities. Since one of the most useful properties of traditional digital signatures is their ability to be verified by anyone (e.g., on the Web), it is unlikely that quantum digital signatures, as currently envisioned, will meet people's need. Thus, it is likely that most organizations will still require public-key technology.

Quantum cryptography does not appear to be practical, except in very restricted situations. It is practical for use between two fixed parties with a substantial amount of data to exchange, and with very high confidentiality requirements.

So, it may find application in securing metropolitan area data links. In fact, it is believed that some national intelligence organizations have such systems in place to connect computers in different districts of the same city. However, despite all of its promise, for most common uses of cryptography, it is not likely to replace current practice in the foreseeable future.

5 Conclusions

Quantum cryptography may find application in certain specific applications. For example, in securing metropolitan area data links. However, the constraints upon its use do not make it a practical solution for many popular applications of cryptography at this time.

If research into quantum routers and quantum digital signatures bears fruit, though, this situation might change. It will likely be at least five to 10 years before quantum cryptography can address these limitations. Even then, it is not clear that the marginal improvement in security will justify the cost.

Quantum computing (if it were to become practical on a large scale) will cause some re-engineering of current cryptographic systems. Symmetric ciphers will be weakened. But, in response we simply have to increase key sizes to restore the necessary level of security. Asymmetric ciphers (all the ones in common use, such as ECC, Diffie-Hellman, DSA and RSA) will be rendered insecure. While cryptographic researchers have good ideas about how to make asymmetric ciphers that are not vulnerable, there are no solutions suitable for deployment today. But, there will be adequate time to correct this.

Fortunately for the security of many information systems, large-scale quantum computers aren't going to be practical any time soon. People have built 28-qubit machines. If and when there are machines with thousands of qubits, the kinds of development mentioned here will become practical.

But it is unlikely that a 4,000-qubit quantum computer will appear without substantial warning. Developments like this are typically achieved by a slow, gradual process. Experts currently talk about the 20-year timeframe before suitable machines become available. Because of this, we expect that users of cryptographic techniques will transition to new schemes that resist quantum attacks well before their systems become vulnerable.

For the time-being, Entrust is aware of and actively reviewing current developments. We thoroughly expect that the necessary cryptographic developments will be achieved in the required timeframe.

6 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in more than 2,000 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.