Queen Mary
University of London

MAS 335 **Cryptography**

Notes 12: Quantum effects and bibliography **Spring 2006**

Quantum effects

> There was a time when the newspapers said that only twelve men understood the theory of relativity. I do not believe there ever was such a time ... On the other hand, I think I can safely say that nobody understands quantum mechanics.
>
> Richard Feynman,
> *The Character of Physical Law*

In this final section we consider some very recent developments based on the mysteries of quantum theory. We do not have time here to do more than scratch the surface of what quantum theory has to say about the behaviour of subatomic systems, and how this behaviour is relevant to cryptography.

There are two aspects which we treat in turn. First, the possibility of building a quantum computer has been raised. Such a gadget could efficiently solve the hard problems on which modern public-key cryptography depends (factorisation and discrete logarithm). Second, a cryptosystem has been proposed which allows Alice and Bob to detect if their communication has been compromised before any secret plaintext is entrusted to the communication channel.

Quantum basics

Like any physical theory, the purpose of quantum mechanics is to predict the result of a measurement on a physical system. But unlike all other theories, it does not usually predict a single value, but offers only a probabilistic prediction, along the lines "the electron's spin will be in the direction of the magnetic field with probability $\frac{1}{2}$, and will be in the opposite direction with probability $\frac{1}{2}$".

At the same time, the system is affected by the measurement; the action of measurement changes the state of the system into one which depends on the result of the measurement.

We turn these principles into a more mathematical format. According to quantum mechanics, the state of a physical system is described by a unit vector in a certain complex inner product space (more precisely, a Hilbert space) called the *state space*, whose dimension may be finite or infinite depending on the system being considered.

An unobserved system "evolves" by what might be regarded as a rotation of the state space. More precisely, a system in state v at a certain time is in state Uv at some later time, where U is a *unitary* transformation (this means that $U^{-1} = \overline{U}^{\top}$, where the bar denotes complex conjugation. The exact form of U is determined by the laws of quantum mechanics (the Schrödinger equation).

However, when we make a measurement on the system, something different happens. A measurement is described by a *Hermitian* transformation H of the state space (one satisfying $H = \overline{H}^{\top}$). Now a standard theorem of linear algebra says that, if H is Hermitian, then the space has an orthonormal basis consisting of eigenvectors of H. We assume for simplicity that the eigenvalues of H are all distinct, so that $He = \lambda e$ holds for a one-dimensional space of eigenvectors e (given the eigenvalue λ). Now the laws of quantum mechanics state the following:

- The result of a measurement associated with H is an eigenvalue λ of H.
- If the system was in state v before the measurement, where $v = \sum a_\lambda e_\lambda$ is the expression for v in terms of an orthonormal basis of eigenvectors, then the probability that the result of the measurement is λ is $|a_\lambda|^2$. (These probabilities sum to 1 because v is a unit vector.)
- If the result of the measurement is λ, then immediately after the measurement the state of the system has "jumped" to e_λ.

Another theorem of linear algebra asserts that the eigenvalues of a Hermitian transformation are real numbers. This corresponds to the statement that the result of any physical measurement is a real number, even though the formalism uses vector spaces over the complex numbers.

Quantum computing

The standard systems considered in a quantum theory course, such as the hydrogen atom, have infinite-dimensional state spaces. However, to describe how to deal with a single bit of information quantum-mechanically, we only need a two-dimensional state space, whose basis vectors describe the two possible results of measuring the bit.

Thus, a *qubit* (short for "quantum bit") is a system whose state space is two-dimensional, spanned by the vectors e_0 and e_1. The operator H associated with the measurement of the bit is

$$H = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

relative to this basis. Thus $He_0 = 0$ and $He_1 = e_1$. So the eigenvalues of H are 0 and 1, and the corresponding eigenvectors are e_0 and e_1.

A typical state of the system (a unit vector in this space) has the form $ae_0 + be_1$, where a and b are complex numbers satisfying $|a|^2 + |b|^2 = 1$. If the system is in this state, we regard it as being in a *superposition* of the states e_0 (bit value 0) and e_1 (bit value 1). If we measure the value of the bit, we find that the probability that it is zero is $|a|^2$, while the probability that it is one is $|b|^2$.

The matrix

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is unitary. It satisfies $Ue_0 = (e_0 + e_1)/\sqrt{2}$ and $Ue_1 = (e_0 - e_1)/\sqrt{2}$. Suppose that we have a circuit whose effect on a qubit (in one unit of time) is to apply U to the state vector. If we prepare the system with the bit taking a definite value, either 0 or 1, then one time unit later the bit is "smeared out" between the two states, that is, the result of a measurement will be 0 with probability $\frac{1}{2}$, and 1 with probability $\frac{1}{2}$. Since the equations are linear, the subsequent evolution of the system will be a superposition of the two states describing the evolution starting from a value 0 and from a value 1. In other words, the computer can perform two computations simultaneously!

The circuit which realizes U is called a *Hadamard gate*.

More generally, an n-qubit system has state space which has a basis consisting of unit vectors e_s, where s runs over all 2^n possible binary strings of length n. If we set up the system with each qubit taking a definite value, and then pass each one through a Hadamard gate, the resulting state will be an equal superposition of all 2^n possible states, and we have a computer which can do 2^n calculations at once.

This is the basis of the power of a quantum computer. In very rough terms: with n qubits at our disposal, we can regard the 2^n strings as representing the integers $1, \ldots, 2^n$, and we can do trial divisions of N by all these numbers simultaneously, arranging the circuitry so that only values which divide exactly give rise to an output. Thus, we can factorise numbers as large as 2^{2n} with such a machine.

This is a rough description of *Shor's algorithm*, which uses a quantum computer to factorise large numbers efficiently. Space does not allow a more precise description.

Other tasks which quantum computers can do very quickly include sorting, and solving the discrete logarithm problem. We see that neither RSA nor El-Gamal will be secure if a practical quantum computer is ever built.

The theory of quantum computing is well understood. The difficulties now are, in some sense, only technological ones. However, they are very severe. Most obviously, a quantum computer uses a single electron or atomic nucleus to store one qubit of information. (For example, as we saw earlier, if an electron is in a magnetic field, then a measurement of its spin will be either in the direction of the magnetic field or in the opposite direction, and we can take these two states as e_0 and e_1.) Now a single electron is very sensitive to interference from a cosmic ray or from thermal agitation by its surroundings. Thus, errors creep in at a very high rate.

By contrast, a bit in a classical computer is stored in a transistor where the difference between "charged" and "discharged" is of the order of trillions of electrons. A cosmic ray may eject a few of these electrons without affecting the bit. Classical computers are extremely reliable and fault-tolerant.

Quantum cryptography

In this section we will see how one of the key properties of quantum theory, that a measurement changes the state of the system, can be used to produce a "tamper-proof" cipher, where Alice and Bob can tell (with probability arbitrarily close to 1) whether Eve has been intercepting their communication, before any plaintext is actually sent.

The cryptosystem uses photons as opposed to electrons. These are the quanta of the electromagnetic field, and except in "photon traps" in cutting-edge research labs, they go their way at the speed of light, so are ideal for transmitting messages but useless for computation. Some properties of photons which we will use are:

(i) A photon has a polarisation, in a direction perpendicular to the direction of travel. (Think of it as like a wave vibrating in a direction perpendicular to the direction of travel. This is really a simplification, since in fact a photon can have two vibrations superimposed, but it is good enough for the argument here.) Note that, for example, "up" and "down" describe the same polarised state.

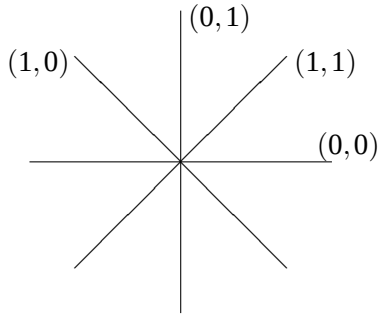
(ii) It is possible to prepare a photon which is polarised in any prescribed direction.

(iii) We can measure the polarisation in any direction; the answer to our measurement will be either "yes" or "no". If the actual polarisation direction makes an angle θ with the direction of the measurement, then the answer "yes" will be obtained with probability $\cos^2\theta$, and "no" with probability $\sin^2\theta$; these sum to 1, as probabilities should. Note that measurements in two perpendicular directions give exactly the same information. In particular, then, if we measure in the direction of the actual polarisation, we certainly get the answer "yes" (as $\cos 0 = 1$); and if we measure perpendicular to the actual polarisation, we get the answer "no" (as $\cos \pi/2 = 0$). In any other case, the result is random.

(iv) After the measurement, if the result was "yes", then the photon will be polarised in the direction of the measurement; if the result was "no", it will be polarised in the perpendicular direction.

The cryptosystem now works as follows. Alice and Bob use quantum effects to share a random sequence of bits, which they then use as a conventional one-time pad. We assume that all channels of communication between them are tapped by Eve.

Stage 1: Alice chooses independently two random binary sequences of length N, say $a_1a_2\ldots a_N$ and $b_1b_2\ldots b_N$. The number N should be a bit more than twice as long as the length of the plaintext bitstring, as we will see. For $i = 1,\ldots,N$, she prepares a photon whose state of polarisation is given in the following diagram, depending on (a_i, b_i). (The direction of travel is perpendicular to the paper, and the angles between adjacent lines are $\pi/4$.)



Note that a_i determines the choice of "orthogonal" (horizontal and vertical) or "diagonal" axes, and b_i determines which of the two axes to use.

Bob chooses a random binary sequence of length N, say $c_1c_2\ldots c_N$ (before the photons are sent). Now, if $c_i = 0$, he measures the polarisation of the ith photon in the vertical (or equivalently the horizontal) direction, and defines $d_i = 0$ if he finds that the polarisation is horizontal and $d_i = 1$ if it is vertical. On the other hand, if $c_i = 1$, then he measures the polarisation of the ith photon in one of the diagonal directions (again, the two measurements are equivalent, so he can make either), and sets $d_i = 0$ if he finds the polarisation to be in the NW–SE direction, and $d_i = 1$ if it is in the NE–SW direction.

Note that

- if $a_i = c_i$, then $b_i = d_i$;
- if $a_i \neq c_i$, then d_i is random: $P(d_i = b_i) = P(d_i \neq b_i) = \frac{1}{2}$. For in this case, Bob's measurement is at an angle of $\pi/4$ or $3\pi/4$ to the actual polarisation, and $\cos^2\theta = \sin^2\theta = \frac{1}{2}$ if $\theta = \pi/4$ or $\theta = 3\pi/4$.

Stage 2: Now Alice and Bob communicate in the ordinary way (over a line which might be insecure). Alice reads out her sequence $a_1 \dots a_N$, and Bob reads out his sequence $c_1 \dots c_N$. Since the sequences are both random, the number of places where they agree will be a binomial random variable $\mathrm{Bin}(N, \frac{1}{2})$, with mean $N/2$ and variance $N/4$ (that is, standard deviation $\sqrt{N}/2$); so it is very likely that the number lies in the range $N/2 \pm c\sqrt{N}$ for some moderate constant c. In this situation, we will say "the sequences agree at about $N/2$ places".

Stage 3: Now Alice and Bob discard the terms of their sequences $b_1 \dots b_N$ and $d_1 \dots d_N$ apart from those where the a and c sequences agree. They use what remains as a one-time pad. Since it is a subsequence of Alice's original random sequence $b_1 \dots b_N$, it is a random sequence, of length about $N/2$. By Shannon's Theorem, their communication will be secure.

Note that $3N$ random bits have to be chosen in order to produce a shared key of length about $N/2$: this is in a sense the price paid for secrecy.

How could Eve attack this cipher?

If she uses any information she gains in stages 2 and 3, she will only be able to obtain about half of the one-time pad, which is no better than guessing randomly. For although she knows which subsequence of the original sequence will be used, she does not know the contents of this subsequence, since Alice and Bob do not reveal the b and d sequences at this stage.

What if Eve intercepts the photons? She can measure the polarisations, and then either let these photons continue their journey to Bob, or replace them with new photons whose polarisation is hers to choose. We show that, not only Eve cannot get hold of more than half of the key even in this way, but that Alice and Bob can detect her tampering. I will just consider the case where she sends the photons on to Bob after measuring the polarisations.

Eve must set up detectors according to some binary sequence $e_1 \dots e_N$, just as Bob does. Her sequence may be random or determinate: for example, she might set them all horizontally. But her choices will agree with Alice's random choices about half the time, and with Bob's about half the time, independently. So she can only be sure of getting about $N/4$ bits of the one-time pad.

To see how we detect tampering, note that if Eve chooses $e_i = a_i$, then she does not change the state of the photon and so her interference is undetectable. However, if she chooses $e_i \neq a_i$, and if $c_i = a_i$, then Alice and Bob have an even chance of detecting the interference. For suppose that $a_i = c_i = 0$ and $e_i = 1$. Then Eve changes the polarisation of the photon from orthogonal to diagonal (each of the two diagonals having probability $\frac{1}{2}$. For each possible state, Bob has probability $\frac{1}{2}$ of measuring

horizontal polarisation, and $\frac{1}{2}$ of measuring vertical polarisation. So the probability that he measures the opposite of what Alice sent is $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$.

Now Alice and Bob adopt the following procedure. They choose their sequences (a_i), (b_i) and (c_i) of length $N + 2n$ rather than N (where n is to be specified later). By Stage 2, they have agreed on about $N/2 + n$ positions where their sequences (b_i) and (d_i) will agree, if there has been no eavesdropping. Alice chooses n positions at random from this subsequence, and reveals their contents to Bob. If there is no eavesdropping, then Bob will have exactly the same bits in these positions as Alice. However, if Eve has been at work, the probability that Bob's bit disagrees with Alice's in one of these positions is $\frac{1}{4}$ (since this requires that $e_i \neq a_i$ and that the randomness in quantum theory produces a result different from what was sent, each of which independently has probability $\frac{1}{2}$). So the probability that Alice and Bob are in complete agreement on the bits Alice reads out is only $(3/4)^n$.

This probability can be made arbitrarily small by choosing n large enough. For example, if $n = 73$, then $(3/4)^n < 1/10^9$, so the chance that Eve's interference is undetected is less than one in a billion. Increasing this to $n = 241$ would reduce the chance to less than one in 10^{30}.

How secure is such a cipher in practice? Of course, the main source of weakness in any cipher is human error: if the cipher is incorrectly used, or the plaintext or key is left where an unauthorised person can obtain a copy, the cipher will not be secure. Also, the same considerations that make quantum computing error-prone also make quantum cryptography error-prone: in practice, Bob will not receive exactly the information that Alice sends, because random effects during transmission or small errors in setting the polarisers or detectors will cause a small error rate. So the number of bits that must be sacrificed in order to check for an eavesdropper will be higher than expected, and Bob's version of the one-time pad will not be a perfect copy of Alice's. In addition, it has been suggested that Eve can use technology: either firing a powerful laser pulse down the cable to fry Bob's detectors, or using the fact that Alice's transmitter may send more than one photon, so it is safe to measure one and let the others proceed to Bob.

It is too early to say how reliable this technology will be in practice!

Bibliography

There are many books on cryptography. The list here includes only a selection.

Singh's book is an excellent and highly recommended introduction to cryptography ancient and modern, with detours about such topics as the decipherment of ancient

scripts (Egyptian hieroglyphics and Linear B). Churchhouse's book is also introductory, and gives a wealth of detail and exercises on 20th century cipher machines such as Enigma and Hagelin.

Two fictional accounts of breaking a substitution cipher are "The Gold-Bug", by Edgar Allan Poe, and the Sherlock Holmes story "The Adventure of the Dancing Men", by Sir Arthur Conan Doyle. The two novels not containing the letter a are *Gadsby*, by Ernest Vincent Wright, and *A Void*, by Georges Perec (translated by Gilbert Adair). Wright's novel is hard to obtain now, but the text can be found at http://gadsby.hypermart.net/.

Babbage's breaking of the Vigenère cipher is treated briefly in his biography by Swade (as well as in Singh's book). Gaines' book, written in 1939, has a wealth of detail on cryptography before its mechanisation, including frequency tables, and many examples and exercises.

Garrett's and Stinson's books are textbooks for the mathematically inclined. Stinson's covers Shannon's Theorem, the two most popular public-key systems, hashing, signatures, and the Data Encryption Standard. Garrett's book gives the background from algebra, number theory, probability, etc., in separate chapters.

The Bletchley Park cryptanalysis is the subject of the books by Welchman (concentrating on Enigma) and Hinsley and Stripp (who range more widely). Hodges' biography of Alan Turing also includes a lot of detail on Enigma. Marks describes vividly the codes used by Allied secret agents in Europe. A personal account of the breaking of FISH by Bill Tutte is at
http://frode.home.cern.ch/frode/crypto/tutte.html.

The best textbook on quantum information theory is the book by Nielsen and Chuang. John Preskill's Caltech notes on quantum computing, at
http://www.theory.caltech.edu/people/preskill/ph219/.

The proof by Agrawal *et al.* that primality testing is polynomial-time solvable is at http://www.cse.iitk.ac.in/news/primality.html.

Anon, *The Mabinogion* (transl. Jeffrey Gantz), Penguin Books, London, 1976.

Robert Churchhouse, *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet*, Cambridge University Press, Cambridge, 2002.

Sir Arthur Conan Doyle, *The Complete Sherlock Holmes*, Penguin (reprint), London, 1981.

Richard Feynman, *The Character of Physical Law*, BBC publications, London, 1965.

Helen Fouché Gaines, *Cryptanalysis: A Study of Ciphers and their Solution*, Dover Publ. (reprint), New York, 1956.

Paul Garrett, *Making, Breaking Codes: An Introduction to Cryptology*, Prentice-Hall, Upper Saddle River, 2001.

F. H. Hinsley and Alan Stripp (eds.), *Code Breakers: The Inside Story of Bletchley Park*, Oxford University Press, Oxford, 1993.

Andrew Hodges, *Alan Turing: The Enigma*, Vintage, London, 1992.

David Knowles, *The Evolution of Medieval Thought*, Vintage Books, New York, 1962.

G. Mander (ed.), `wot txters hav bin w8ing 4`, Michael O'Mara Books, London, 2000.

Leo Marks, *Between Silk and Cyanide: The Story of SOE's Code War*, HarperCollins, London, 1998.

Michael A. Nielsen and Isaac L. Chuang, *Quantum Information and Quantum Computation*, Cambridge University Press, Cambridge, 2000.

Georges Perec (translated by Gilbert Adair), *A Void*, Harvill Press, 1994.

Edgar Allan Poe, *Complete Tales and Poems*, Castle Books, Edison, NJ, 1985.

Simon Singh, *The Code Book: The Secret History of Codes and Code-Breaking*, Fourth Estate, London, 1999.

Douglas R. Stinson, *Cryptography: Theory and Practice* (2nd edition), Chapman & Hall/CRC, Boca Raton, 2002.

Doron Swade, *The Cogwheel Brain: Charles Babbage and the Quest to Build the First Computer*, Little, Brown & Co., London, 2000.

Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes*, M & M Baldwin, Cleobury Mortimer, 1998.

Ernest Vincent Wright, *Gadsby*, Wetzel Publishing Co., Los Angeles, 1931.

Peter Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*, Stoddart Publ. Co., Toronto, 1987.