13
Quantum Cryptography

Quantum mechanics is valuable because it opens a discussion about the nature of reality, because it demonstrates the power of reason in revealing the truth even when common sense is an obstacle, and simply because it is good to know how our universe ticks ("knowledge is better than ignorance"). But it is also valuable because a host of practical devices, from lasers to transistors to superconductors, all work because of quantum mechanics.

Most of these applications are beyond the scope of this book. I could tell you in vague terms how a laser works, but I could never convince you that my description was correct — you would have to accept it on my authority, and acceptance on the basis of authority is the very antithesis of scientific thought. However, there is one very recent, very exciting application of quantum mechanics that can be treated in full within the "rigorous but not technical" style of this book, namely the use of quantum mechanics to send coded messages. (You may skip this chapter without interrupting the flow of the book's argument.)

13.1 Can you keep a secret?

Sending coded messages is a part of life. Governments and businesses need to transmit secrets that would be deadly in the wrong hands (military plans, formulas for explosives, etc.). But even you have information that you don't want everyone in the world to know: your bank balance, your voting record, your vacation plans. I'm not suggesting that you should be embarrassed about your bank balance, but it's your private information and no eavesdropper has any right to it. For this reason, when credit card and automatic teller machine transactions are sent over public telephone lines, the messages are sent in code. Such codes are enormously valuable, and there is an ongoing policy debate about who

can use the best codes. The United States Commerce Department classifies difficult-to-break codes as munitions (along with guns and bombs and fighter jets) and prohibits their export from the country.

Cryptography is the art of sending information from place to place in coded form so that it will be meaningless to any eavesdropper who might intercept it. The problem of cryptography is to find a mechanism for one person — conventionally named "Alice" — to send secret information to another person — "Bob" — while a third person — "Eve" — might or might not be eavesdropping. A number of coding schemes are in use, but I will describe only one, the "Vernam cipher" or "one-time pad scheme", because it is the only coding scheme that has been proven to provide perfect, unbreakable security.

Suppose Alice wants to send computer mail to Bob. Computers store information internally as clusters of ones and zeros, each digit called a "bit". In the standard representation of characters by bit clusters — used worldwide by nearly all computers — each character of text is represented by a cluster of seven bits. For example, the letter "a" is represented by the cluster "1100001", the numeral "4" by the cluster "0110100", the comma by the cluster "0101100", and a blank space by the cluster "0100000". Thus whenever Alice sends computer mail to Bob, she is sending him a long string of bits — ones and zeros — which his computer can easily interpret as letters and numbers. Unfortunately, Eve's computer can do so just as easily.

To maintain secrecy, before sending her message Alice produces a random string of bits — called the "key" — exactly as long as her message. She then encodes each bit of her message according to the key: If the fifth bit of the key is a zero, then she sends the fifth bit of her message unaltered, but if the fifth bit of the key is a one, then she reverses the fifth bit of her message (if it is a 1, she sends a 0; if it is a 0, she sends a 1). For example, if Alice encoded the character "a" using the key 0101101, the resulting coded message would be 1001100 as shown here:

```
1100001   (standard representation for "a")
0101101   (key)
1001100   (code for "a")
```

After encoding her message, Alice sends Bob not only her coded message, but also her key. Bob decodes Alice's message in the same way that she encoded it: He preserves the message bits corresponding to zeros in the key, and alters the message bits corresponding to ones in the key. Bob's decoded message is then exactly the same as the one that Alice started with.

If Eve intercepts only the coded message, it won't do her any good. Of course, the coded string of bits will translate to *some* message in the

standard representation, but that message will be gibberish. Eve might try to decode a 91-bit message with every possible 91-bit key, but that won't help her because she would then produce every possible 91-bit statement, including

"Withdraw $100",
"Buy stock now",
"I love Bob!!!",
"I despise Bob",
"Bomb Baghdad.",

and a great many statements like

"U&87{{ ^(aqNq".

However, if Eve intercepts both the coded message *and* the key, then Eve can decode the message just as easily as Bob can. The key must instead be transmitted through some separate secure channel that Eve cannot intercept. But if Alice and Bob have a secure channel, they don't need to bother with codes at all! Alice and Bob might hire a courier (who is a secure channel) to deliver several identical keys to both Alice and Bob at the beginning of each week, and they can use those keys throughout the week. But then Eve might bribe the courier. (It doesn't work to use one key over and over — there are easy ways to break the code if the same key is used even twice. This is the origin of the name "one-time pad".)

In short, the problem with the Vernam cipher is not the distribution of *messages* but the distribution of *keys*. It is ironic but nevertheless true that an important problem for contemporary business and government is the generation and distribution of random numbers.

13.2 Distributing random keys

Since probability and randomness are intrinsic to quantum mechanics, you might guess that quantum mechanics could provide some help with the problem, and indeed it does. Suppose Alice and Bob set up experiment 6.1, "EPR distant measurements" (page 40) with one vertical analyzer next to Alice, the other next to Bob, and the source of atoms between them. They set the source to automatically generate pair after pair of atoms, and when those atoms reach their analyzers Alice and Bob both record the exits taken. If Alice records "+ + − + −", then Bob records exactly the opposite pattern, namely "− − + − +". Alice turns her readings into a cryptographic key by converting each + to a 1 and each − to a 0. Bob does the same with the opposite convention, namely + goes to 0 and −

goes to 1. Now both Alice and Bob have the same random key and can send a coded message using the Vernam cipher.

Unfortunately, Eve can easily break into this system by inserting a vertical interferometer between the source and Bob. Eve watches each atom pass through her interferometer. When one goes through her top branch, she knows that Bob will get a + and Alice will get a −. Similarly for her bottom branch. Eve gets the key, Eve breaks the code.

13.3 Distributing random keys securely

To prevent eavesdropping, Alice and Bob instead set up experiment 6.2, "EPR random distant measurements" (page 42) with one randomly tilting analyzer next to Alice, the other next to Bob, and the source set to "automatic" as before. When an atom reaches an analyzer, Alice (or Bob) records both the analyzer orientation (**A**, **B**, or **C**) and the exit taken (+ or −). Recall that if the two analyzers are set to the same orientation, then the two atoms emerge from opposite exits, but if they are set to different orientations, then the two atoms might emerge from either similar or opposite exits. (They emerge from the similar exits with probability $\frac{3}{4}$ and from opposite exits with probability $\frac{1}{4}$, but this fact is not needed in what follows.)

Alice and Bob run this experiment for a long time, and then send to each other the list of their analyzer orientations. (Each list looks something like **BBACABBC**.... There's no need to encode these messages: if Eve intercepts them, the lists won't help her.) When they compare lists Alice and Bob find that in most cases their two detectors were set to different orientations, but in about one-third of the cases the detectors happened to have the same orientation. They discard the exit information (the +s and −s) for those cases with different orientations, and use the cases with the same orientation to construct a key just as they did previously. Now that they have identical keys, Alice and Bob can send coded messages using the Vernam cipher.

What if the nefarious Eve tries to intercept the key in this distribution scheme, as she did previously? Suppose Eve places a vertical interferometer between the source and Bob, and watches each passing atom to see which branch it takes. (For definiteness, assume that Bob and Alice are equally distant from the source.) Now when atoms arrive at the tilting analyzers used by Alice and Bob, they are no longer in an entangled state: instead, one atom has $m_z = +m_B$ and the other has $m_z = -m_B$. If the two detectors are vertical (orientation **A**) this makes no difference: the two atoms still emerge from opposite exits. But if both detectors are in orientation **B**, then there is some probability (it turns out to be $\frac{3}{8}$) that the two atoms

will emerge from the same exit. Alice and Bob therefore agree beforehand that they will not use the entire key as generated above. Instead Bob will mail, say, the first half of his key back to Alice. If Bob's first half matches Alice's first half, then Alice knows that no one was eavesdropping on the key distribution and that it is safe to send her message coded using the second half of the key. If the two half-keys don't match, then Alice doesn't send her message on to Bob but instead calls the police and tells them to search for Eve.

This precise method of key distribution is not practical: it relies on a source of atoms that just happens to be conveniently placed between Alice and Bob, it involves sending a lot of information back and forth that is ultimately ignored, and in the end it doesn't actually ensure privacy, it merely lets the legitimate users know whether or not someone is listening in. There are other quantum cryptography schemes that lack many of these drawbacks, and these are so promising that they have raised the interest even of commercial communication companies. (The experiment of Nicolas Gisin mentioned on page 42 was supported in part by Swiss Telecom.) Quantum cryptography is a new field (the first experiment was performed in 1989) but both theory and practice are growing rapidly and hold the promise of practical applications from the most esoteric fundamentals of quantum mechanics.

13.4 References

Charles H. Bennett, Gilles Brassard, and Artur K. Ekert, "Quantum cryptography", *Scientific American*, **267** (4) (October 1992) 50–57.

Wolfgang Tittel, Grégoire Ribordy, and Nicolas Gisin, "Quantum cryptography", *Physics World*, **11** (3) (March 1998) 41–45.