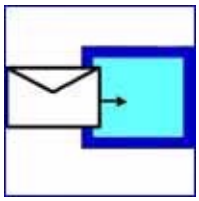
May 2005
Features



Cracking codes, part II

by Artur Ekert

In Cracking codes, part I in the previous issue of Plus, we saw how the desire to communicate secretly has inspired human ingenuity to create intricate ciphers − and how the desire to learn others' secrets led to those ciphers being broken. We now leave mathematics, and enter the world of quantum physics for an introduction to the peculiar phenomenon of quantum correlation − a phenomenon that evades all common explanations.

No information without physical representation

Suppose you toss a fair coin several times and record the results by writing 0 for heads and 1 for tails. The result will be a random string of 0s and 1s − a "random binary string" (binary means there are two possibilities at each point in the string). Such a string can serve as a cryptographic key, as long as two identical copies of it

can be created at two distant locations.

Needless to say, if Alice and Bob both toss their coins at their respective locations the resulting binary strings will be completely unrelated to each other. Thus Alice and Bob must receive their data from a common source of random bits. The snag is that once a random bit value is generated by the source it has to be securely communicated to Alice and Bob.

From a physicist's point of view a bit is a physical bit. A binary value is represented by a measurable physical quantity such as intensity of an electric current, a radio signal or a light beam. Consequently, from a physicist's perspective, eavesdropping is a measurement. It is a passive measurement of the physical quantity which represents the bit. Classical physics − the theory of macroscopic bodies and phenomena such as paper documents, magnetic tapes and radio signals − allows all physical properties of an object to be measured without disturbing those properties. Thus classical physics allows perfect eavesdropping − physical bits can be intercepted and measured without legitimate recipients being able to detect such an intrusion. This means secure communication is not possible. End of the story.

Well, not quite. The world of atoms and photons does not follow the rules of classical physics. It is described by the best physical theory that we have today, namely, the quantum theory. The act of measurement is an integral part of quantum mechanics, not just a passive, external process as in classical physics, and it usually disturbs the measured system in some detectable way. For example, photons, the elemenatary quanta of light, have many measurable properties, such as different types of polarisations, eg linear, circular, etc, and measuring any one of them disturbs the others. Polarisation of a beam of light, made out of many photons, is related to the direction of oscillations of the electromagnetic wave. This is translated into an intrinsic angular momentum of individual photons. If we choose to measure a particular polarisation of a single photon we will register only one of its two possible values, which can be labeled as 0 and 1, and we will randomise the values of other polarisations. This fact can be used to detect eavesdropping!

Thankfully, we do not have to know all the physics behind polarised photons to get an idea how quantum measurements work. Let me explain them using a simple analogy. Card tricks should do the job.

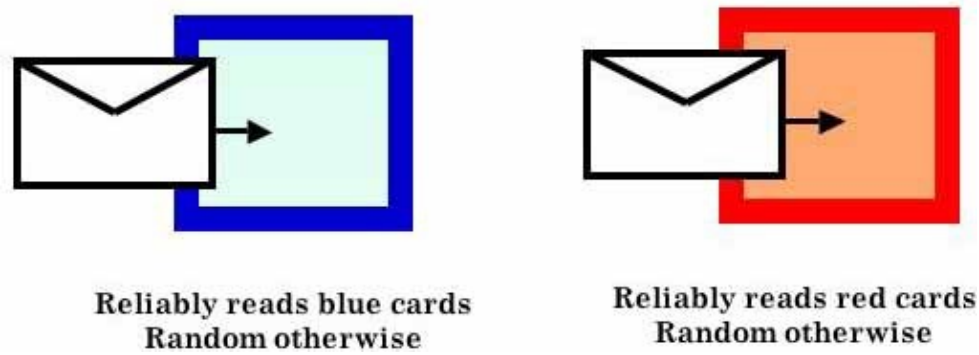
Card tricks

Imagine a blue card with either 0 or 1 written on it. The card is put into an envelope and sealed. In order to learn the bit value on the card we insert the envelope into a special measuring device, a "blue machine" that sees the bit value through the envelope.

Now imagine a red card with either 0 or 1 written on it. Again, the card is put into an envelope and sealed. In order to learn the bit value on the card we insert the envelope into a "red machine" that sees the bit value through the envelope.

The blue machine can read blue cards correctly (whether 0 or 1), but is "blind" to other colours and reads red cards randomly. When you input a red card into the blue machine the output is a blue card with randomly chosen 0 or 1.

The same description holds for the red machine which can read red cards correctly and reads blue cards randomly. When you input a blue card into the red machine the output is a red card with randomly chosen 0 or 1.

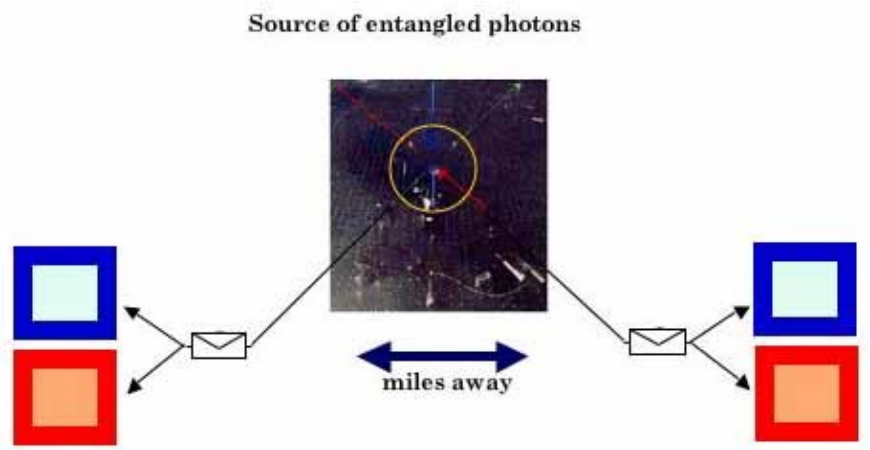


One peculiar thing about this process is our inability to attribute precise bit values to the two colours simultaneously. The card is either blue or red; it cannot be both. If a red card is inserted into the "blue machine" and then retrieved, it acquires all characteristics of a blue card (and vice versa). For suppose we present the "blue machine" with a red card which has the bit value 0 written on it. The "blue machine" is equally likely to declare the card to have 0 or 1 written on it. Say it declares 1. If we retrieve the card and measure it again in the "blue machine" then we will always see the bit value 1. This means that the card sealed in the envelope is now really blue with 1 written on it, and that the card has lost its memory of being red with 0 on it in the past. Therefore, if the card is then inserted into the "red machine" it will be equally likely declared to be 0 or 1, revealing nothing about its original red bit.

This is how values of circular (blue colour) and linear (red colour) polarisations are measured. They are known to be complementary properties: if you know the value of linear polarisation, either 0 or 1, you know nothing about possible values of circular polarisation, and vice versa. The two physical properties do not co−exist.

Enter entanglement

We now introduce the concept of "entangled" pairs of cards. Imagine Alice and Bob repeatedly receive a card each from some external source. The source sends out two envelopes with unseen cards in them, one envelope to Alice and one envelope to Bob. Once the envelopes arrive, Alice and Bob choose randomly and independently from each other whether to read them in the "blue machine" or in the "red machine".



Alice and Bob notice that the individual binary outcomes are random, no matter which machine they use. However, after talking to each other they discover that if they use the same machines, be it blue or red, their results always tally, ie they register (0,0) or (1,1) with equal probability. (Here (a,b) means Alice registered binary outcome a = 0 or 1 and Bob registered binary outcome b = 0 or 1.) If they use different coloured

machines, the results may or may not tally, ie they register (0, 0), (0, 1), (1, 0) and (1, 1) with equal probability. How can this happen?

Spooky action at a distance

What is the colour of the entangled cards prior to the measurement? They cannot be both blue with the same bit values written on them because if Alice and Bob both choose to insert the envelopes into their "red machines", the readings of the bit values may not tally. By the same argument they cannot be both red. Neither can they be in any other prescribed configuration of colours and bit values. A moment of reflection should suffice to realise that there is no source that can reproduce the desired correlations.

And yet such sources do exist! Physicists observe this type of correlation in experiments. For example, in a process called "parametric down conversion", a photon from a laser beam enters a beta−borium−borate crystal and gets absorbed while it excites an atom in the crystal. The atom subsequently decays, emitting two entangled photons. These photons are represented by our sealed cards, their type of polarisation is represented by the colour of the card, and the value of polarisation is represented by a binary value written on the cards.

At this point you may recall the master detective, Sherlock Holmes, who once remarked that when all likely explanations are ruled out, any remaining possibility, however unlikely, must be correct. So perhaps the entangled cards do not have any colour prior to their measurement. It could be that they acquire their colour, and the bit values are stamped on them, while they are inside the card reading machines. But the card reading machines are miles apart and independent from each other, so how do they know that both cards should be painted in, say, blue? After all, one machine might paint one card in blue and stamp it 0 and the other paint the other card in blue and stamp it 1.

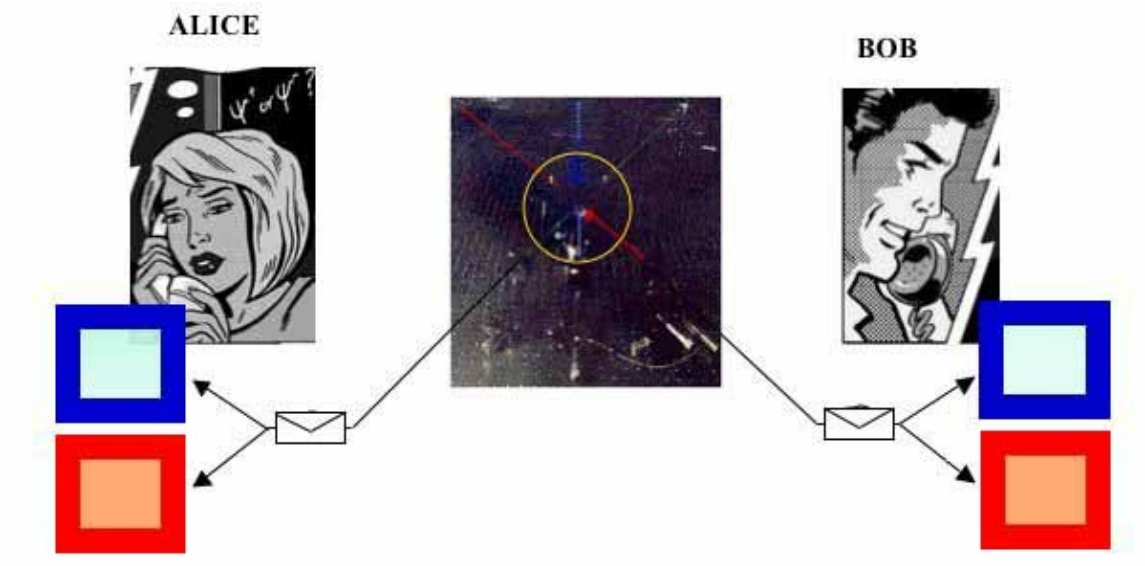
If you find this perplexing then let me reassure you that you are in very good company. In May 1935, Albert Einstein, together with two colleagues, Boris Podolsky and Nathan Rosen (EPR), published a paper in which they stated that a physical theory, such as quantum mechanics, that allows the type of correlations we have described above, dubbed by Einstein as the "spooky action at a distance", does not provide a complete description of reality. Einstein and his colleagues wanted to believe that each of our sealed cards has a colour, and that one measuring device cannot communicate instantaneously to another measuring device: "I have painted my card in blue and stamped 0, you'd better do the same with your card". The world view in which physical objects have properties independently of whether we measure them or not and they cannot

"communicate" instantaneously with each other is called local realism. This is a very sensible view; however, it was refuted in a series of beautiful experiments performed by physicists in the 1980s.

A quantum key

Physicists and philosophers still debate the meaning of locality and reality in the quantum theory. It is a fascinating subject. Here we will take a more pragmatic view and make this refutation of local realism work for Alice and Bob in their classically impossible task of distributing cryptographic keys.

The scheme uses a quantum channel, through which Alice and Bob receive entangled cards from an external source, which may be controlled by an eavesdropper, in conjunction with a classical public channel, through which they exchange ordinary messages. An eavesdropper, Eve, is free to try to tamper with the source. This is probably the most counter−intuitive key distribution protocol because it accommodates scenarios in which Eve herself distributes entangled cards to Alice and Bob!



Entangled cards are sent apart from a source towards the two legitimate users, Alice and Bob, who, for each incoming card, decide randomly and independently from each other whether to read it with the "blue machine" or the "red machine". A single run of the experiment may look like this:

Alice	1	0	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1	1	1	1	1
Bob	1	0	1	0	1	0	1	0	0	0	0	0	1	0	1	0	1	1	1	0	1

For the first pair, both Alice and Bob decided to read the cards in the "blue machine", and their results are identical. For the second pair they decided to read the cards in the "red machine" and their results are again identical. For the third pair Alice decided to read her card in the "red machine" while Bob read his card in the "blue machine". In this case their results are not correlated at all. In the fourth instance they both inserted their cards into the "blue machines" and obtained identical results, and so on.

After completing all the measurements, Alice and Bob discuss their data in public so that anybody, including their adversary, Eve, can listen, but nobody can alter or suppress such public messages. Alice and Bob tell each other which machine they used for each incoming card but they do not disclose the actual readings of the machines. For example, for the first pair Alice may say, "I measured blue," and Bob may confirm, "So did I".

At this point they know that the results − the bit values − in the first measurement are identical. Alice knows that Bob registered 1 because she registered 1, and vice versa. However, although Eve learns that the results are identical she does not know whether it is 0 for Alice and 0 for Bob, or 1 for Alice and 1 for Bob. The two outcomes are equally likely, so the actual values of bits associated with different results are still secret.

Subsequently Alice and Bob discard all results corresponding to instances in which they used different machines. They end up with shorter strings which should now contain perfectly correlated entries.

Alice	1	0	0	1	0	0	1	0	1	1	1
Bob	1	0	0	1	0	0	1	0	1	1	1

They check whether the two strings are indeed perfectly correlated by comparing, in public, randomly selected entries (shown grey in the table below).

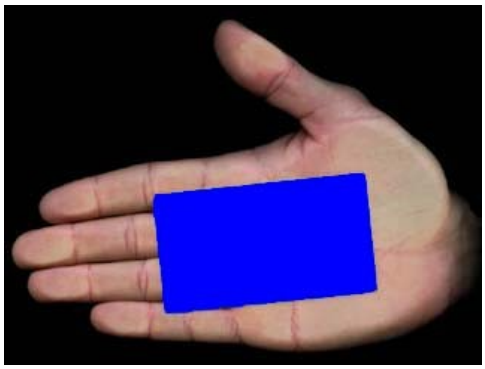
Alice	1	0	0	1	0	0	1	0	1	1	1
Bob	1	0	0	1	0	0	1	0	1	1	1

Perfect agreement indicates entanglement between the cards. The publicly revealed entries are discarded and the remaining results are kept as the key.

The key	1	0	1	0	0	1	1

You can go through this key distribution protocol yourself − try the animation produced for the author's Motivate videoconference on the same topic.

Eve is excluded



We already know that if the cards are entangled then they have no colour prior to the measurements performed by Alice and Bob. This means Eve has nothing to eavesdrop on!

Let us be more specific and adopt the scenario that is most favourable for eavesdropping: we will allow Eve to prepare all the cards and send them to Alice and Bob. Eve's objective is to prepare the pairs in such a way that a) she can predict Alice's and Bob's results and b) that she can induce identical outcomes whenever Alice and Bob choose to read the cards with the machines of the same colour. Because of a) she will know the key and because of b) she will not be detected.

But this is impossible. Suppose Eve prepares a pair of cards choosing randomly from one of the four configurations: (blue with 0, blue with 0), (blue with 1, blue with 1), (red with 0, red with 0), and (red with 1, red with 1). Suppose it is (blue with 0, blue with 0). She then sends one card to Alice and one to Bob. Let us concentrate only on instances in which Alice and Bob choose to measure the same colour as only those instances contribute to the final key. If both Alice and Bob choose to measure blue on their respective cards then they obtain identical results and Eve knows the outcome; if they choose to measure red, then although the outcomes are random they can still obtain identical results with probability 50%. Thus Eve knows, on average, every second bit of the key; however, she will be discovered because this strategy results in 25% of errors when Alice and Bob test for entanglement by comparing in public sufficiently many randomly selected bits from their binary strings.

A more technical analysis shows that any eavesdropping strategy, no matter how sophisticated, is doomed to fail, even if Eve has access to superior technology, including quantum computers. The more information Eve has about the key, the more disturbances she creates. Eve will be discovered if she knows too much! In this case Alice and Bob will try to distribute the key again. Remember, the purpose of eavesdropping is not to prevent Alice and Bob from communicating secretly but to fool them, so that they think they have a secret key but in fact Eve has it as well. Thus with quantum key distribution Alice and Bob will never be fooled. Once they conclude they have a secret key they can use a one time pad and communicate with perfect security. Thus unbreakable ciphers do exist, and are not merely a figment of abstract imagination.

Quantum cryptography today

Quantum key distribution as described above was the product of my graduate infatuation with quantum theory. It all happened back in Oxford in the late 1980s and early 1990s. I do not remember exactly what prompted me to visit the Clarendon Laboratory library one rainy day, browse the dusty shelves and pick up the original Einstein, Podolsky and Rosen paper for casual reading. However, I do remember this one sentence in the paper that drew my attention: "...If, without in any way disturbing a system, we can predict with certainty ... the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity." This is a definition of perfect eavesdropping! I guess I was lucky to read it in this particular way. The rest was just about rephrasing the subject in cryptographic terms.

I was lucky again a few months after when I met John Rarity and Paul Tapster, two experimental physicists from the Defence Research Agency in Malvern (today QinetiQ Malvern). It did not take long to persuade them to make the first entangled photons to carry secret bits. In 1991 experimental quantum cryptography based on quantum entanglement became reality. Einstein's "spooky action at a distance" found its first practical application.

I should add here that a different approach to quantum cryptography preceded my work. In the early 1970s, Stephen Wiesner, then at Columbia University in New York, introduced the concept of quantum conjugate coding. He showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarisation of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. This work remained unpublished for years and only very few of his colleagues knew about it. A decade later, building upon Wiesner's work, Charles H. Bennett, of the IBM T. J. Watson Research Center, and Gilles Brassard, of the Université de Montréal, proposed a method for secure communication based on "conjugate observables", which also remained very little known until the early 1990s.

Today quantum cryptography is a thriving area. Early experiments at the IBM T. J. Watson Research Laboratory in Yorktown Heights in the US and the Defence Research Agency in Malvern in the UK led to several beautiful experiments that demonstrated fully−fledged quantum key distribution both in optical fibres

and free space. Moreover, quantum cryptography is a commercial alternative to more conventional, classical cryptography. The history of the field shows that even most abstract blue sky research into the foundations of quantum mechanics may lead to unexpected applications.

About the author

Artur Ekert splits his time between the University of Cambridge, where he is the Leigh−Trapnell Professor of Quantum Physics at DAMTP and a Professorial Fellow of King's College, and the National University of Singapore, where he is a Distinguished Professor. He is one of the inventors of quantum cryptography.

Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.