Bell Inequalities and Cryptography

Artur Ekert & Alastair Kay

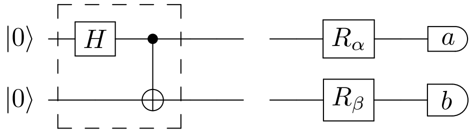
I. THE QUANTUM OF SOLACE

Truth be told, we are not that much after magic. All we need for our purposes are monogamous correlations that cannot be pre-programmed. And they do exist! Welcome to the quantum world!

Take, for example, polarised photons. Recall that polarisation of a single photon can be measured along any direction, and the outcome of the measurement is one out of two values $\pm\hbar$, which we may, of course, relabel as 0 and 1. In a process called "parametric down conversion" photons from a laser pulse enter a beta-barium-borate crystal. Most of them pass straight through but sometimes a photon from the pulse gets absorbed and excites an atom in the crystal. The atom subsequently decays, emitting two "polarisation entangled" photons. These entangled photons can be separated (they are emitted in different directions), fed into optical fibres and delivered to the final recipients — one to Alice and one to Bob. Suppose Alice measures the polarisation of her photon along some direction α and Bob along some other direction β. It turns out that the two photons can be entangled in such a way that their measurement outcomes are identical with the probability

$$\cos^2(\beta - \alpha) \ , \tag{1}$$

and 0 and 1 are equally likely to appear. In order to see this consider the network



The Bell state $|00\rangle + |11\rangle$ is modified by the $R_\alpha \otimes R_\beta$ gates, where a single "rotation" gate is defined by the unitary matrix

$$R_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}.$$

Rotation by some angle φ followed by the measurement in the computational basis is equivalent to the measurement in the rotated basis, e.g. to measuring polarisation along φ. The outputs state, up to the $\frac{1}{\sqrt{2}}$ normalisation factor, is

$$\cos(\beta - \alpha)\,(|00\rangle + |11\rangle) + \sin(\beta - \alpha)(|01\rangle + |10\rangle).$$

Thus the values of a and b are identical with the probability $\cos^2(\beta - \alpha)$ and hence differ with the probability $\sin^2(\beta - \alpha)$.

Let us now replace coin tosses by appropriately chosen polarisation measurements: instead of tossing coin A_1, Alice simply measures her photon along $\alpha_1 = 0$; and instead of tossing A_2, she measures the photon along $\alpha_2 = 2\pi/8$. Similarly, Bob replaces his coin tosses B_1 and B_2 by measurements along directions $\beta_1 = \pi/8$ and $\beta_2 = 3\pi/8$, respectively. Equation (1) gives us joint probabilities of all possible outcomes given the choices of polarisation measurements. They are shown in the table below, where $\varepsilon = \sin^2(\pi/8) \approx 0.146$. This value can be interpreted as the probability of deviation from the behaviour of the perfect magic correlations.

Alice		A_1		A_2	
Bob		0	1	0	1
B_1	0	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$
	1	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$
B_2	0	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$
	1	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$

Surprisingly enough, ϵ is lower than 0.25, which is the lowest error rate we can get by assigning some numerical values to A_1, A_2, B_1 and B_2 and trying to pass the test for the magic correlations. Indeed, we are bound to violate at least one of the four conditions

$$A_1 = B_1,\ B_1 = A_2,\ A_2 = B_2,\ B_2 \neq A_1.$$

Using conventional, classical, strategies the lowest probability of failure is 0.25. In contrast, with the help of entangled photons, the probability of failure is lowered to approximately 0.15. This means that such correlations cannot be pre-programmed and, as such, can be used for the key distribution purposes.

II. BELL'S INEQUALITY

The world evolving in a fully definite, fully predictable manner permits only certain types of correlations. The argument, originally proposed by John Bell, is deceptively simple. Alice and Bob are equipped with polarization analyzers and sent to two distant locations. Somewhere in between them there is a source that emits pairs of photons that fly apart, one towards Alice and one towards Bob. Let us assume that the photons have well defined values of their polarizations. We ask Alice and Bob to measure one of the two pre-agreed polarizations. For each incoming photon, Alice and Bob choose randomly, and independently from each other, which particular polarization will be measured. Alice chooses between A_1 and A_2, and Bob between B_1 and B_2. Each polarization has value +1 or −1 (in $\hbar$ units) thus we are allowed to think about them as random variables A_k and B_k, $k = 1, 2$, which take values ±1. Let us define a new random variable S,

$$S = A_1(B_1 + B_2) + A_2(B_1 - B_2). \tag{2}$$

It is easy to see that one of the terms $B_1 \pm B_2$ must be equal to zero and the other to ± 2, hence $S = \pm 2$. The average value of S must lie somewhere in-between, i.e.

$$-2 \leq \langle S \rangle \leq 2. \tag{3}$$

That's it! Such a simple mathematical statement about correlations, to which we refer simply as Bell's inequality, and yet so profound. No quantum theory involved because Bell's inequality is not specific to quantum theory; it does not really matter what kind of physical process is behind the appearance of binary values of A_1, A_2, B_1 and B_2.

Quantum correlations, due to entanglement, violate Bell's inequality. As we have seen, two photons can be prepared in an entangled state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

so that polarization analysers A and B, which are set θ degrees apart, will register identical results ($AB = 1$) with probability $\cos^2\theta$ and hence different results ($AB = -1$) with probability $\sin^2\theta$. This gives the correlation coefficient

$$\langle AB \rangle = \cos^2\theta - \sin^2\theta = \cos 2\theta.$$

Again, choose angles 0, $\pi/4$, $\pi/8$ and $3\pi/8$ for A_1, A_2, B_1 and B_2 respectively and you obtain

$$\langle S \rangle = \langle A_1B_1 \rangle + \langle A_2B_1 \rangle + \langle A_2B_2 \rangle - \langle A_1B_2 \rangle = 2\sqrt{2}$$

This, by the way, is the maximal violation that quantum correlations can offer. Why? We do not know. Please note that our magical correlations give $\langle S \rangle = 4$.

Entanglement and the impossibility of assigning numerical values to certain physical quantities have been baffling physicists for almost a century. After all, most of us grew up holding it self-evident that the world might be inordinately complicated but at the bottom of it there should be some objective reality in which physical objects have properties that can be quantified and their values should exist regardless whether we measure them or not. In such a world, it follows from our discussion above, experimentalists endowed with free will can only observe correlations which satisfy the innocuous Bell inequality. Shocking as it may be, our world is not of this kind! And this, to be sure, has been observed in a number of painstaking experiments.

III. CRYPTOGRAPHY REVISITED

Experimental violations of Bell's inequalities brings us to implementations and to few practical questions that need to be addressed. In theory there is no difference between theory and practice, but in practice there is. Entangled photons are fragile, their polarisation may be changed by impurities in optical fibres, they can even get lost on their way to detectors. In short, there is lots of noise out there in a real world and no matter what we do the value $|\langle S \rangle|$ will always be strictly less than $2\sqrt{2}$. And when security is at stake we do not take any chances. We assume that all noise is due to eavesdropping.

The maximal violation allowed, $|\langle S \rangle| = 2\sqrt{2}$, implies both perfect randomness and perfect security, anything less than that may contain corrupted correlations, in which some bits may be known to an adversary. Still, as long as we can estimate how many bits are compromised we can use a number of cryptographic techniques, such as error correction combined with hashing, to distill a secret key. As it happens, the amount of information available to the adversary is related directly to the degree of violation of Bell's inequality. Even though Eve knows something about the key (which is not good) Alice and Bob know how much she knows (which is good) and they can "distill" a virtually perfect key from a partially compromised one. A variety of techniques are available for Alice and Bob to correct a small number of errors through public discussion and to amplify the privacy of the key.

The basic idea behind the privacy amplification is quite simple. Imagine you have two bits and you know that your adversary knows at most one of them, but you do not know which one. Add the two bits together (modulo 2); the resulting bit will be secret. Needless to say, there are better ways of doing this, Alice and Bob can choose, publicly, a length-reducing transformation and apply it to the partially compromised key. For example, if the input consists of 1,000 bits about which Eve knows at most 200 bits, Alice and Bob can distill nearly 800 highly secret bits as output. Fairly simple techniques can be shown to suffice, and Alice and Bob do not even need to know which partial information the eavesdropper might have about the input in order to choose a function about whose output Eve has almost no information. Thus the key distillation is possible with the usual price to pay, namely, a reduction of the key length.

This is true, but proving it in a quantum context is a bit tricky. In fact it has taken over a decade to agree on a useful definition of secrecy and a tight security proof has kept researchers busy until today. While all security proofs infer secrecy from the strength of the correlations between Alice and Bob, a major challenge is to make these arguments quantitative and robust towards imperfections. These and many other results addressed a number of subtleties and the proof of security has finally been established.