

22: QUANTUM CRYPTOGRAPHY

22.1 Quantum Mechanics

We want to consider a simple quantum system describing the state of a polarised photon. This photon is described by a wave function ψ . When the photon is polarised vertically it has a wave function $|\uparrow\rangle$ and, when it is polarised horizontally, it has a wave function $|\leftrightarrow\rangle$. In its general state it is a linear combination

$$\psi = \alpha |\uparrow\rangle + \beta |\leftrightarrow\rangle$$

for complex numbers α, β with $|\alpha|^2 + |\beta|^2 = 1$. Hence the two states $|\uparrow\rangle$ and $|\leftrightarrow\rangle$ are a basis for the state space. We will denote this basis by $+$.

There are many other bases. For example we will be particularly concerned with the diagonal basis:

$$\begin{aligned} |\nearrow\rangle &= \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\leftrightarrow\rangle \\ |\searrow\rangle &= \frac{1}{\sqrt{2}} |\uparrow\rangle - \frac{1}{\sqrt{2}} |\leftrightarrow\rangle . \end{aligned}$$

We will denote this basis by \times .

Most light sources give a mixture of photons polarised in different orientations but it is simple to use a polarising filter to separate out photons with a particular polarisation. We can also use another polarising filters to detect polarisations. Suppose that a photon with wave function $\psi = \alpha |\uparrow\rangle + \beta |\leftrightarrow\rangle$ hits a vertical polarising filter. Then quantum mechanics shows that the probability that it will pass through is $|\alpha|^2$. So $|\uparrow\rangle$ is certain to pass the vertical filter; $|\leftrightarrow\rangle$ is certain to be stopped; while both $|\nearrow\rangle$ and $|\searrow\rangle$ pass the filter with probability $\frac{1}{2}$.

The crucial property that makes quantum systems useful for cryptography is the Heisenberg uncertainty principle. This says that, when we observe the state of a quantum observable, its value is changed by that observation. So, if the photon $\psi = \alpha |\uparrow\rangle + \beta |\leftrightarrow\rangle$ hits our vertical filter and detector, it will change to $|\uparrow\rangle$ and pass through with probability $|\alpha|^2$ and change to $|\leftrightarrow\rangle$ and be stopped with probability $|\beta|^2$. Note that, to use this detector we need to choose which polarisation that we are testing. If we used a polarising filter aligned with $|\nearrow\rangle$ we would get entirely different results. If we send a message using the polarisation of photons to record data, then an enemy who tries to eavesdrop on the message will necessarily affect its values. So, in principle, we can detect that the enemy has interfered with our message.

In the applications that we consider, we will use the polarisation of photons to store information. We will therefore call the wave function ψ of a photon a *qubit* by analogy with a binary bit.

22.2 Quantum Key Exchange

We are now in a position to describe how a quantum system can be used to send information securely. The system we will describe is due to Bennet and Brassard (1984) and called BB84.

Bob wishes to agree with Alice a secret key of N binary bits. To do this, Bob sends $4N$ qubits to Alice. For each qubit he first chooses at random either to use the basis $+$ or the basis \times . Then he chooses a binary bit at random. Bob then sends the qubit determined by the table below.

Bob's Basis	$+$	$+$	\times	\times
Bob's Bit	0	1	0	1
Qubit sent	$ \leftrightarrow\rangle$	$ \updownarrow\rangle$	$ \nearrow\rangle$	$ \nwarrow\rangle$

Alice also makes a random choice of basis $+$ or \times for each qubit she receives. When she chooses $+$, then she uses a vertical polarising filter and records whether the photon passes through this filter. She records 1 if the photon passes through and 0 if it does not. When she chooses \times , then she uses a filter aligned with $|\nearrow\rangle$ and records whether the photon passes through this filter. The table below shows the results for each possible qubit sent.

Bob's Basis	$+$	$+$	\times	\times	$+$	$+$	\times	\times
Bob's Bit	0	1	0	1	0	1	0	1
Qubit sent	$ \leftrightarrow\rangle$	$ \updownarrow\rangle$	$ \swarrow\rangle$	$ \searrow\rangle$	$ \leftrightarrow\rangle$	$ \updownarrow\rangle$	$ \swarrow\rangle$	$ \searrow\rangle$
Alice's basis	$+$	$+$	$+$	$+$	\times	\times	\times	\times
Alice's result	0	1	?	?	?	?	0	1

In this table the ? in the final row indicates that the result may be 0 or 1 each with probability $\frac{1}{2}$.

Once transmission is complete, Alice and Bob both publish their choice of bases. Each can then determine for which qubits they used the same basis. In these cases, Alice's result is identical with the bit Bob chose. So, on average, she and Bob will now have $2N$ bits that they both know.

Alice chooses half of these bits and publishes their positions in the message and their values. Bob publishes the values he has for the same positions. Then both of them can compare the values they have for these N bits. They should be identical. The remaining N bits are used as the common key.

Suppose that an enemy has intercepted the qubits and found their polarisation. Because of the uncertainty principle, this observation must have affected the wave functions. More precisely, quantum indeterminacy ensures that there is no measurement that will distinguish between the 4 different polarisation states, since they are not all mutually orthogonal. (The observables corresponding to the bases $+$ and \times do not commute.) A measurement can distinguish between two orthogonal states but not between non-orthogonal states. For example, if the photon hits a vertically polarised filter, then $|\uparrow\rangle$ will pass through, $|\leftrightarrow\rangle$ will be stopped, while both $|\nearrow\rangle$ and $|\searrow\rangle$ will transform to $|\uparrow\rangle$ and pass through with probability $\frac{1}{2}$ and be stopped with probability $\frac{1}{2}$. Once this has been done, it is impossible to recover information about the polarisation of the photon before it hit the filter.

In more detail, suppose that the enemy intercepts one of the photons where Alice and Bob agree on the choice of basis, say $+$. The enemy has no way of knowing which basis Bob will have chosen so he must guess whether to measure in the $+$ or \times bases. With probability $\frac{1}{2}$ he will be wrong and choose \times . In this case, he will wrongly detect a photon $|\nearrow\rangle$ or $|\searrow\rangle$, each with probability $\frac{1}{2}$. When Alice receives this she will be using the $+$ basis and so will record $|\uparrow\rangle$ or $|\leftrightarrow\rangle$ each with probability $\frac{1}{2}$. Hence she will record the wrong result with probability $\frac{1}{4}$. Therefore, if Alice and Bob discover that a significant proportion of the N bits they compare differ, then they will suspect an enemy has intercepted the message and so discard it and try again.

In systems designed to implement the above scheme, there is usually a lot of noise, so bits are corrupted even when there is no enemy trying to intercept the message. This can be dealt with by using error correcting codes of the type described earlier. In this way we can exchange keys with an arbitrarily small probability of error and an arbitrarily small probability that an enemy has intercepted it undetected. Note that this scheme is secure because of the laws of quantum mechanics rather than because a mathematical problem is hard.

There are various difficulties in implementing the scheme described above. Firstly no device for producing single photons has been produced. So, instead, low power lasers are used. This means that each qubit actually consists of several photons each with the same polarisation. If an eavesdropper can detect the polarisation by only looking at one of the photons, the others may remain undisturbed and so the eavesdropper will not be detected. Secondly, noise in such a system tends to be high so it is hard to transmit information over a long distance. Thirdly, the scheme is vulnerable to a “man in the middle” attack. If an enemy can intercept all the data that is sent between Alice and Bob, he can impersonate Alice to Bob and Bob to Alice, so each will exchange a key with their enemy rather than each other. Nonetheless, practical systems based on this scheme have been developed to transmit information over about $60km$ at a rate of $10^3 bits/s$.

We have described the BB84 scheme for exchanging keys using the polarisation of photons. It should be apparent that a similar scheme could be introduced using other quantum states in place of polarisation. Ekert proposed using quantum entanglement and schemes based on this have been implemented.