3.5: Quantum Cryptogaphy

One of the most remarkable consequences of Bell's thought experiment is that it provides a way to perform cryptography that is more secure, in certain respects, than conventional cryptography. This possibility was first raised by Ekert, and it has led to a huge amount of research into **quantum cryptography**, which is poised to be one of the most important technological applications of quantum mechanics.

Ekert's quantum cryptography scheme allows two participants, Alice and Bob, to share with each other a string of random binary digits (0 or 1), called a "key", in such a manner that no one else can learn the key by eavesdropping on their communications. Once Alice and Bob have established a secret shared key, it can be used to encrypt subsequent messages between them, which nobody else can decipher (e.g., by using one-time pads).

The scheme follows almost immediately from the Bell thought experiment of Section 3.4. In each round, a pair of spin-$1/2$ particles is prepared in the singlet state, with particle A sent to Alice and B sent to Bob. Alice and Bob each randomly choose a measurement axis (S_1, S_2, or S_3), and measure the spin of their particle along that axis.

After an appropriate number of rounds, Alice and Bob publicly announce their choices of measurement axes. These announcements are assumed to take place over a classical communication channel that cannot be jammed or manipulated by any hostile party (though it can be eavesdropped upon). From the announcements, Alice and Bob determine the rounds in which they happened to pick the same axes. Their measurement results during these rounds are guaranteed to be the opposites of each other. Hence, they have established a random binary string known to each other but to no one else.

How might an eavesdropper, Eve, attempt to foil this scheme? Suppose Eve can intercept some or all of the particles B destined for Bob. She might try to substitute her own measurements, in a manner that could let her work out the secret key. However, Eve is hampered by the fact that she is unable to predict or influence Bob's choices of measurement axes (i.e., Bob's choices are truly random), nor is she able to impersonate Bob during the announcements of the axis choices (i.e., the classical communication channel is unjammable). Under these assumptions, it can be shown that any attempt by Eve to substitute her own measurements can be detected by Alice and Bob, by performing a statistical analysis of their measurement results in the rounds with different different axis choices. The detection of the eavesdropper turns out to be essentially the same as checking for Bell's inequality. For details, refer to Ref.

Alternatively, Eve might try to "clone" the quantum state of particle B before passing it along to Bob. If this can be done, Eve can retain the cloned quantum state, wait for Bob to announce his choice of measurement axis for that round, and then perform the corresponding measurement to reproduce Bob's result. Though plausible at first glance, this turns out to be fundamentally unworkable, as it is incompatible with the laws of quantum mechanics.

The so-called **no-cloning theorem** can be proven as follows. Eve desires to clone an arbitrary state of a spin-half particle B onto another spin-half particle C. The two-particle Hilbert space is $\mathscr{H} \otimes \mathscr{H}$. With particle C initially prepared in some state $|0\rangle$, Eve must devise a unitary operation $\hat{U}$, representing the cloning process, such that

$$\hat{U}|\psi\rangle|0\rangle = e^{i\phi}|\psi\rangle|\psi\rangle \tag{3.5.1}$$

for all $|\psi\rangle \in \mathscr{H}$, and for some phase factor ϕ that could depend on $|\psi\rangle$. Note that the value of ϕ does not affect the outcomes of measurements.

Now replace $|\psi\rangle$ in the above equation with two arbitrary states denoted by $|\psi_1\rangle$ and $|\psi_2\rangle$, and take their inner product. According to Equation (3.5.1),

$$\begin{aligned}\Big(\langle\psi_1|\langle 0|\hat{U}^\dagger\Big)\Big(\hat{U}|\psi_2\rangle|0\rangle\Big) &= \Big(\langle\psi_1|\langle\psi_1|e^{-i\phi_1}\Big)\Big(e^{i\phi_2}|\psi_2\rangle|\psi_2\rangle\Big) \\ &= e^{-i(\phi_1-\phi_2)}\Big(\langle\psi_1|\psi_2\rangle\Big)^2.\end{aligned} \tag{3.5.2}$$

Here, ϕ_1 and ϕ_2 are the phase factors from Equation (3.5.1) for the two chosen states. On the other hand, since $\hat{U}$ is unitary,

$$\begin{aligned}\langle\psi_1|\langle 0|\hat{U}^\dagger\hat{U}|\psi_2\rangle|0\rangle &= \Big(\langle\psi_1|\langle 0|\Big)\Big(|\psi_2\rangle|0\rangle\Big) \\ &= \langle\psi_1|\psi_2\rangle.\end{aligned} \tag{3.5.3}$$

Here we have used the fact that $\langle 0|0\rangle = 1$. Comparing the magnitudes of (3.5.2) and (3.5.3),

$$\left|\langle\psi_1|\psi_2\rangle\right|^2 = \left|\langle\psi_1|\psi_2\rangle\right| \quad \Rightarrow \quad \left|\langle\psi_1|\psi_2\rangle\right| = 0 \text{ or } 1. \tag{3.5.4}$$

But aside from the trivial case of a one-dimensional Hilbert space, this cannot be true for arbitrary $|\psi_1\rangle$ and $|\psi_2\rangle$. For instance, for a two-dimensional space spanned by an orthonormal basis $\{|0\rangle, |1\rangle\}$, we can pick

$$|\psi_1\rangle = |0\rangle, \ |\psi_2\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \quad \Rightarrow \quad \left|\langle\psi_1|\psi_2\rangle\right| = \frac{1}{\sqrt{2}}. \tag{3.5.5}$$

This page titled 3.5: Quantum Cryptogaphy is shared under a CC BY-SA 4.0 license and was authored, remixed, and/or curated by Y. D. Chong via source content that was edited to the style and standards of the LibreTexts platform.