# ¿Antivirus cuánticos (seguridad cuántica)?

¿Cómo serán los antivirus para los ordenadores cuánticos que manejen datos cuánticos? Deberían ser capaces de manipular datos y realizar cálculos muy complejos que se tendrían que poder descomponer según técnicas de paralelismo exponencial…

Los principios sobre los que se fundamenta la computación cuántica son los de la física cuántica, y la base la computación cuántica son los qubits. Simplificando la cuestión, un ordenador convencional está basado en bits, los cuales pueden adoptar los valores 0 o 1. Sin embargo, un ordenador cuántico utiliza bits cuánticos o qubits para representar la información, el cual puede almacenar los dos valores posibles simultáneamente. Esta característica de los qubit es posible gracias al *principio de superposición*, mediante esta propiedad el qubit adopta probabilísticamente los dos posibles valores y el observador define el estado al que colapsa.

A modo de símil, para explicar el *concepto de superposición cuántica*, podríamos pensar en una puerta casi cerrada, para un elefante esta puerta estaría cerrada ya que no podría pasar, pero para una pulga estaría abierta ya que si podría pasar. Otra forma de explicar el concepto es mediante la paradoja del gato de Schrödinger, en la que el físico austriaco Erwin Schrödinger muestra la incertidumbre sobre el estado del gato.

Esta propiedad de superposición cuántica y el entrelazamiento cuántico son la base del potencial de un computador cuántico, el paralelismo cuántico. Gracias al paralelismo cuántico la capacidad de realizar operaciones en paralelo o simultáneamente crece de manera exponencial en relación al número de qubit con los que puede operar el ordenador.

Por ejemplo, un computador cuántico que manipulase 250 qubits equivaldría a $2^{250}$ bits en un ordenador tradicional. Esta capacidad de paralelismo exponencial podría resolver problemas que actualmente tienen un coste computacional muy elevado o que son irrealizables, entre estos podemos destacar la factorización de números que gracias al algoritmo de Shor sería posible descomponer en factores un número N en un tiempo mucho menor.