

Alt: One area in which... is cyber security, where the muscular prime factorisation prowess is predicted to make a merry mockery of our best existing secret-key methods. /

The emergence of Quantum Computing has thrown the world of cyber-security up in the air.

While the muscular/barbaric prime factorisation abilities of quantum computers seem set to make a mockery of our best existing cyber-security measures, study of quantum communications has unearthed a prospective lifeline in the form of a brand new, watertight security key method, whose integrity against eavesdroppers is guaranteed in cast iron by the laws of quantum physics.

Meet Eve, the cardboard eavesdropper. She lurks in every theoretical communication model, able to instantly recognise any potential weakness, and call on any technological trinket to exploit it. A sleek and savage predator on a single-minded hunt for illicit data. Intent on maximum personal damage to our two communicators, Alice and Bob, be it financially, physically, or emotionally.

Every

In reality we also need to contend with interference from the environment - everything else in the world that interacts with our qubit (be it coded to the spin of an ion, or photon, or to any quantum-behaved property we can decompose in a suitable binary way.

Of course, everything else might also include malicious tampering by Eve, the customary cardboard eavesdropper, intent on nothing other than maximum personal damage to Alice and Bob, the **rando schlubs** sharing a secret code, physically, socially, emotionally, using any and all the data she can leech from the cracks in their quantum network.

Box 1

In the same way that we can decompose a 2D graph into x and y coordinates, so too can we decompose any spin representation into x, y, and z components. (fig). each of

which can be either in the up or down state when measured.

A state that is prepared to be 'up' in one direction, z, for instance, would be measured as 'up' with 100% probability if we align our measurement device to the z-direction, but would be measured as 'up' or 'down' with equal probability, if we measure in either the 'x' or 'y' directions.

With any orientation we choose, we can name a z-direction, for instance, and prepare an ion, electron, or photon with spin is (prepared to be) aligned perfectly up or down in an arbitrary x-direction, will be poised exactly in between up and down if measured in the y- or x-directions.

Stupid questions (link to interviews?)

So is the race now on for physicists in team QKD to **scrabble rabidly ahead before** physicist hacker teams blow banking wide open and steal the world's wealth? Do they ever have nightmares about Eve, and does it actually stand for "Evil"?

The answer to all these questions is a flat no, yet many good questions remain to be answered. At UCL in London, Quantum Technology, Professor Sougato Bose is not convinced. “What a load of...etc.”