Quantum 'sealed envelope' system enables 'perfectly secure' information storage

November 4 2013

Credit: Paul Hocksenar

A breakthrough in quantum cryptography demonstrates that information can be encrypted and then decrypted with complete security using the combined power of quantum theory and relativity - allowing the sender to dictate the unveiling of coded information without any possibility of intrusion or manipulation.

Scientists sent encrypted data between pairs of sites in Geneva and Singapore, kept "perfectly secure" for fifteen milliseconds - putting into practice what cryptographers call a 'bit commitment' protocol, based on theoretical work by study co-author Dr Adrian Kent, from Cambridge's

Department of Applied Mathematics and Theoretical Physics.

Researchers describe it as the first step towards impregnable information networks controlled by "the combined power of Einstein's relativity and quantum theory" which might one day, for example, revolutionise financial trading and other markets across the world.

'Bit commitment' is a mathematical version of a securely sealed envelope. Data are delivered from party A to party B in a locked state that cannot be changed once sent and can only be revealed when party A provides the key – with security guaranteed, even if either of the parties tries to cheat.

The technique could one day be used for everything from global financial trading to secure voting and even long-distance gambling, although researchers point out that this is the "very first step into new territory".

This is a significant breakthrough in the world of 'quantum cryptography' – one that was once believed to be impossible. The results are published in the journal *Physical Review Letters*.

"This is the first time perfectly secure bit commitment – relying on the laws of physics and nothing else – has been demonstrated," said Adrian Kent.

"It is immensely satisfying to see these theoretical ideas at last made practical thanks to the ingenuity of all the theorists and experimenters in this collaboration."

Any signal between Geneva and Singapore takes at least fifteen milliseconds – with a millisecond equal to a thousandth of a second. This blink-of-an-eye is long enough with current technology to allow data to

be handed over encrypted at both sites, and later decrypted – with security "unconditionally guaranteed" by the laws of physics, say the team.

The researchers have exploited two different areas of physics: Einstein's special relativity – which interprets uniform motion between two objects moving at relative speeds – combined with the power of quantum theory, the new physics of the subatomic world that Einstein famously dismissed as "spooky".

Completely secure 'bit commitment' using quantum theory alone is known to be impossible, say researchers, and the "extra control" provided by relativity is crucial.

Professor Gilles Brassard FRS of the Universit'e de Montr'eal, one of the co-inventors of quantum cryptography who was not involved in this study, spoke of the "vision" he had fifteen years ago - when trying to combine quantum 'bit commitment' with relativity to "save" the theory - in which Einstein and early quantum physicist Niels Bohr "rise from their graves and shake hands at last":

"Alas, my idea at the time was flawed. I am so thrilled to see this dream finally come true, not only in theory but also as a beautiful experiment!" he said.

Bit commitment is a building block – what researchers call a "primitive" – that can be put together in lots of ways to achieve increasingly complex tasks, they say. "I see this as the first step towards a global network of information controlled by the combined power of relativity and quantum theory," Kent said.

One possible future use of relativistic quantum cryptography could be global stock markets and other trading networks. It might be a way of

leveling the technological 'arms race' in which traders acquire and exploit information as fast as possible, the team suggest, although they stress at such an early stage these suggestions are speculative.

The new study builds on previous experiments that, while successful, had to assume limitations in the technology of one or both parties – and consequently not entirely "safe or satisfactory" says Kent, "since you never really know what technology is out there".

More information: prl.aps.org/abstract/PRL/v111/i18/e180504

Provided by University of Cambridge