Quantum cryptography: No Signaling and quantum key distribution

July 5 2005

A new research article outlines another aspect of Quantum Cryptography

In "No Signaling and quantum key distribution", a new paper published in Physical *Review Letters* 95 (010503 – 2005), Barrett, Hardy and Kent give the first example of a way of implementing quantum cryptography which is provably secure - even if quantum theory is incorrect, so long as a successor theory shares with quantum theory the features which make faster-than-light signaling impossible.

The scheme can be implemented by two parties (Alice and Bob) who know quantum theory but know nothing about the precise form of any successor theory, and is secure against a "post-quantum" eavesdropper, Eve, even if she knows the successor theory and has arbitrary post-quantum technology available to her.

Related link: Perimeter Institute for Theoretical Physics