Title: Superselection Rules and Quantum Protocols

Date: Aug 15, 2003 10:50 AM

URL: http://pirsa.org/03080007

Abstract: Superselection rules are limitations on the physically realizable quantum operations that can be carried out by a local agent. For example, it is impossible to creÂ-ate or destroy an isolated particle that carries locally conserved charges, such as an electrically charged particle, a fermion, or (in a twoÂ- dimensional medium) an anyon. Recently, Popescu has suggested that suÂ-perselection rules might have interesting implications for the security of quantum cryptographic protocols. The intuitive idea behind this suggestion is that superselecÂ-tion rules could place inescapable limits on the cheatÂ-ing strategies available to the dishonest parties, thus enÂ-hancing security. Might, say, unconditionally secure bit commitment be possible in worlds (perhaps including the physical world that we inhabit) governed by suitable suÂ-perselection rules? An affirmative answer could shake the foundations of cryptography. The purpose of this paper is to answer Popescu's inÂ-triguing question. Sadly, our conclusion is that superseÂ-lection rules can never foil a cheater who has unlimited quantumÂ- computational power.


PERIMETER INSTITUTE FOR THEORETICAL PHYSICS
PLAY