JIANXIN CHEN, University of Guelph
symmetric extension of two-qubit states

Quantum key distribution uses public discussion protocols to establish shared secret keys. In the exploration of ultimate limits to such protocols, the property of symmetric extendibility of underlying bipartite states ρ_{AB} plays an important role. A bipartite state ρ_{AB} is symmetric extendible if there exits a tripartite state $\rho_{ABB'}$, such that the AB marginal state is identical to the AB' marginal state, i.e. $\rho_{AB'} = \rho_{AB}$. For a symmetric extendible state ρ_{AB}, the first task of the public discussion protocol is to break this symmetric extendibility. Therefore to characterize all bi-partite quantum states that possess symmetric extensions is of vital importance. We prove a simple analytical formula that a two-qubit state ρ_{AB} admits a symmetric extension if and only if $tr(\rho_B^2) \geq tr(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}$. Given the intimate relationship between the symmetric extension problem and the quantum marginal problem, our result also provides the first analytical necessary and sufficient condition for the quantum marginal problem with overlapping marginals.