Insecurity of position-based quantum cryptography protocols against entanglement attacks
Hoi-Kwong Lo
University of Toronto

Abstract
Recently, position-based quantum cryptography has been claimed to be unconditionally secure. On the contrary, here we show that the existing proposals for position-based quantum cryptography are, in fact, insecure if entanglement is shared among two adversaries. Specifically, we demonstrate how the adversaries can incorporate ideas of quantum teleportation and quantum secret sharing to compromise the security with certainty. The common flaw to all current protocols is that the Pauli operators always map a codeword to a codeword (up to an irrelevant overall phase). We propose a modified scheme lacking this property in which the same cheating strategy used to undermine the previous protocols can succeed with a rate at most 85%. The modified protocol is secure when the shared quantum resource between the adversaries is a two- or three- level system. Reference: http://arxiv.org/abs/1009.2256

Co-author Hoi-Kwan Lau (University of Toronto)