ALAIN TAPP, Université de Montréal

Anonymous message transmission

Anonymous message transmission is the task by which a sender transmits to a receiver a private message in such a way that the receiver does not know who, within the user group, actually sent the message. Furthermore, the rest of the users do not learn anything. The case involving classical messages has been recently solved by A. Broadbent and A. Tapp. They have proposed an information theoretically secure protocol, based solely on pairwise authentic private channels, that tolerates an arbitrary number of corrupted players. I will present a protocol that accomplishes the same goal, in the same model, but with quantum messages.

This work has been done in collaboration with G. Brassard, A. Broadbent, J. Fitzsimons and S. Gambs.