# On the privacy and authenticity of quantum messages

Alain Tapp
*Département d'informatique et de recherches opérationnelles*
*Université de Montréal*
*C.P. 6128, Succ. Centre-ville*
*Montréal, Québec*
*CANADA H3C 3J7*

**Abstract**

The private transmission of information and the verification of the authenticity of messages are among the main interests of classical cryptography. Unconditionaly secure solutions to both of these problems are known, provided that the parties share a long nough private random classical key.

I will define the private transmission and authentification of quantum messages and show an unconditionaly secure protocol that solves those problems, provided again that the parties share a private classical key. I will also argue that those protocols are optimal.