CORR 2001-42

Authentication of Quantum Messages

Claude Crépeau*, Daniel Gottesman*, Adam Smith*, Alain Tapp

Abstract Authentication is a well-studied area of classical cryptography: a sender $\mathcal{A}$ and a receiver $\mathcal{B}$ sharing a classical private key want to exchange a message with the guarantee that the message has not been modified (or replaced) by a dishonest party with control of the communication line. In this paper we define, and present a scheme for authentication of *quantum* messages. Assuming $\mathcal{A}$ and $\mathcal{B}$ have access to an insecure quantum channel and share a private, classical random key, we provide a scheme that enables $\mathcal{A}$ to authenticate an m qubit message by encoding it into $O(m+s)$ qubits, where the error probability decreases exponentially in the security parameter s. Furthermore, our protocol has the advantage of providing perfect encryption of the quantum message transmitted. The scheme requires a private key of size $O(m+s)$, which is optimal for schemes which provide both encryption and authentication.

Keywords Authentication, quantum information