Decoherence, inaccuracy and errors in quantum cryptography

Sara Felloni

Dipartimento di Informatica, Sistemistica e Comunicazione,
Università di Milano-Bicocca

We present a general single-qubit error model to study decoherence and noise effects in quantum information processing. Since a general transformation of a single-qubit density matrix can be described by twelve parameters, we associate a noise channel to each parameter and we represent each channel by means of quantum circuits and density matrices transformations.

After the characterization of all physically possible single-qubit errors, we perform a realistic noisy simulation of a privacy amplification protocol in quantum cryptography, based on entanglement purification. We assume that two communicating parties use an EPR cryptographic protocol, in which decoherence, noise effects or eavesdropping attacks can reduce the quality of information. Entanglement purification is then operated by means of the quantum privacy amplification protocol.

We study the stability under quantum noise effects of this quantum cryptographic protocol by presenting a systematic numerical study of the impact of all possible single-qubit noise channels. We find that both the qualitative behavior of the fidelity of the purified state as a function of the number of purification steps and the maximum level of noise that can be tolerated by the protocol strongly depend on the specific noise channel applied. The protocol shows good performances even in the presence of strong errors and without the application of any errors correction.

Sara Felloni graduated cum laude in Mathematics in 2005 at the University of Milano. Now she is a PhD student with ministerial scholarship in Informatics, at the University of Milano - Bicocca, since November 2005.

She is working on a PhD thesis in Quantum Computing entitled "Decoherence, Inaccuracy and Errors in Quantum Information Processing", supervised by Prof. Giuliano Strini (Dipartimento di Fisica, Università degli Studi di Milano) and Dr. Alberto Leporati (Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano - Bicocca).