Explaining Basic Aspects of Quantum Computation
Based on Functional Approach

Marcos B. Cardoso
Faculdade de Informática PUC RS
mbcardo@gmail.com.br

Eduarda Monteiro∗ Felipe Munhoz†
Escola de Informática UCPel
{eduardam, fmunhoz} @ucpel.tche.br

Renata H. S. Reiser Juliana K. Vizzotto Antônio Carlos R. Costa
Escola de Informática UCPel PPGInf
{reiser, jkv, rocha} @ucpel.tche.br

ABSTRACT

The aim of this paper is to obtain an interpretation of foundations of the quantum computation under the light of the level of functional abstraction [1] and supported by its mathematical basis. This approach seems more accessible to programmers and increases the study and interest in quantum programming. The necessity for secret message exchange and the possibility of reading secret information have developed cryptographic methods. The security of current methods is based on hard computational problems enabling a good safety level. However, if there is a marked growth in computational power, leaks in the safety system of the cryptographic methods could occur. Due to this fact, alternative methods have been studied, which may, in the near future, replace existing techniques, providing safer systems independently of the exponential growth of the available power computations. In the modern algorithms [2], the secret of the message is found in its key, which is used as a parameter in the coding and decoding of the message. The longer the key is, the more difficult it will be to break it. In the symmetric algorithms, also known as the private key, the same key is used in the coding as well as in the decoding. So, it needs to arrange a key previously. Taking into account that in many applications such as commercial and banking transactions through the internet, the use of this key is not practical. This work implements an asymmetric algorithm or public key. Following the methodology suggested by Sabry[3], an implementation of BB84 cryptographic algorithm is presented, using Haskell programming language [4]. This implementation includes the analysis of quantum data (classic, superposition, entangled), the specification of unitary transformations and the understanding of the measurement process of the observed values. In addition, the steps of implementation received important contributions from seminal works [5, 6] and some results were applied to increase the comprehension and application of quantum cryptographic and its implementation in Haskell.

References