SALÃO DE INICIAÇÃO CIENTÍFICA XXIX SIC

UFRGS PROPESQ

Salão UFRGS 2017

múltipla UNIVERSIDADE inovadora inspiradora

Evento	Salão UFRGS 2017: SIC - XXIX SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2017
Local	Campus do Vale
Título	Algoritmos Quânticos
Autor	HENRIQUE PADOVANI QUEIROZ MACHADO
Orientador	SANDRA DENISE PRADO

Algoritmos Quânticos

Aluno: Henrique Padovani Queiroz Machado
Engenharia Física
Instituto de Física – UFRGS
Orientadora: Sandra Denise Prado

A Computação Quântica é uma área de pesquisa relativamente recente, mas muitos cientistas trabalham com a ideia de que o primeiro computador quântico, com capacidade para cálculos complexos, deverá estar em pleno funcionamento em dez anos, apesar dos desafios da computação quântica. Se essa previsão realmente acontecer, será o começo de uma nova revolução, pois precisaremos reinventar um sistema seguro de criptografia, para começar.

Inicialmente, como uma forma de entender na prática, alguns princípios da Física Quântica, será apresentado um comparativo da caminhada aleatória clássica e da caminhada aleatória quântica em uma dimensão. Em seguida, serão discutidas a proposta da computação quântica, as diferenças entre um computador clássico e um computador quântico e suas vantagens e limitações. Feito isso, serão brevemente apresentados dois algoritmos quânticos, o algoritmo de Grover e o algoritmo de Shor. O primeiro é um algoritmo de busca que tem o objetivo de encontrar uma informação específica em uma lista de N dados, sendo N muito grande. O computador quântico executaria um número de operações da ordem de $N^{1/2}$, enquanto o computador clássico executa, em média, N/2 operações. O segundo é um algoritmo que se utiliza de propriedades de aritmética modular para descobrir padrões entre o número a ser fatorado, N, com um número qualquer que seja coprimo com N. A grande vantagem do algorítimo de Shor é que ele consegue fatorar números muito grandes em tempo polinomial, enquanto os computadores clássicos não conseguem. O algoritmo de Shor em pleno funcionamento em um computador quântica, acabaria com o atual sistema de criptografia.