Evento	Salão UFRGS 2014: SIC - XXVI SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2014
Local	Porto Alegre
Título	Algoritmo de Shor para fatoração de inteiros
Autor	Eliseu Venites Filho
Orientador	SANDRA DENISE PRADO

A computação quântica utiliza fenômenos como emaranhamento e superposição para construção de algoritmos que realizam tarefas mais rapidamente do que um computador clássico, ou até mesmo tarefas que são impossíveis para um computador clássico.

Trataremos de um problema muito antigo e que tem maravilhado matemáticos de todas as épocas, a fatoração de números inteiros em seus primos, problema para o qual não se conhece nenhum algoritmo clássico eficiente.

Felizmente, em 1994, Peter Shor, trabalhando na Bell Labs, formulou um algoritmo que resolve o problema em tempo polinomial $O((logN)^3)$ para um inteiro N.

Além da importância intrínseca ao problema da fatoração, podemos ressaltar que o algoritmo de Shor representa um verdadeiro desafio a Tese forte de Church-Turing, pois é a primeira evidência de que computadores quânticos são inerentemente mais poderosos. Também algoritmos eficientes para fatoração podem ser utilizados para quebrar chaves do sistema RSA de criptografia.

Vamos analisar cada parte do algoritmo de Shor, mas para isso são necessárias uma introdução à computação quântica, mostrando suas características e limitações, e uma apresentação das ferramentas e subrotinas utilizadas.