



T680

### **CRIPTOGRAFIA QUÂNTICA: FUNDAMENTOS E APLICAÇÕES**

Rafael Teruel Valle (Bolsista PIBIC/CNPq) e Prof. Dr. Varese Salvador Timóteo (Orientador),  
Centro Superior de Educação Tecnológica - CESET, UNICAMP

A criptografia é um processo bastante utilizado para proteger informações do acesso indevido de pessoas não autorizadas. Ela consiste em aplicar uma chave à informação e torná-la indecifrável. Para proteger uma dada informação, uma chave é utilizada, aplicando um determinado algoritmo de criptografia. O maior problema desta metodologia está no fato de a chave poder ser descoberta. Uma solução para este problema pode ser obtida a partir de propriedades da mecânica quântica. Diferente dos métodos criptográficos tradicionais, que utilizam algoritmos matemáticos para a cifragem das informações, este novo método consiste em gerar chaves de uso único (one-time-pads) utilizando as propriedades quânticas dos fótons.

O projeto consiste em desenvolver um software para emular a transmissão de one-time-pads utilizando o método da criptografia quântica e estudar o funcionamento e propriedades do método.

Criptografia - One-time-pad - Mecânica quântica