XIII Congresso 28 a 29 - setembro - 2005
Interno de Iniciação Científica da UNICAMP
Ginásio Multidisciplinar da UNICAMP

E306

SIMULAÇÃO DE UM PROTOCOLO DE CRIPTOGRAFIA QUÂNTICA

Felipe de Campos Lourenço (Bolsista FAPESP) e Prof. Dr. Antonio Vidiella Barranco (Orientador), Instituto de Física "Gleb Wataghin" - IFGW, UNICAMP

A criptografia quântica tem como característica principal o fato da sua segurança estar baseada em características físicas intrínsecas da natureza. Devido à isso, hoje ela aparece como a principal alternativa à criptografia clássica atualmente utilizada, e cuja segurança está baseada, em última análise, na falta de recursos computacionais. O estudo que está sendo realizado aborda inicialmente os tópicos em física quântica, necessários para o entendimento dos protocolos de criptografia; uma revisão dos principais algoritmos de criptografia clássica; estudo dos protocolos de criptografia quântica que envolvem fótons únicos e as propostas alternativas dessa área que são os protocolos que envolvem variáveis contínuas (estados coerentes contendo muitos fótons). A segurança deste protocolo está baseada na codificação da chave em variáveis relacionadas ao campo eletromagnético que não podem ser medidas simultaneamente com precisão absoluta (quadraturas do campo). Nosso objetivo final é o desenvolvimento de uma simulação computacional de um protocolo de variáveis contínuas utilizando a luz laser (estados coerentes). Através desta simulação será possível investigar o funcionamento deste protocolo em diversas situações, assim como verificar a ação de um possível espião.

Criptografia quântica - Estados coerentes - Simulação