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

E316

INFORMAÇÃO QUÂNTICA CRIPTOGRAFADA USANDO MEIOS CONTÍNUOS

Rafael Lessa Menezes (Bolsista PIBIC/CNPq) e Prof. Dr. José Antônio Roversi (Orientador), Instituto de Física "Gleb Wataghin" - IFGW, UNICAMP

As comunicações eletrônicas entre quaisquer pessoas são hoje uma realidade, em grande medida, graças aos desenvolvimentos da criptografia no último quartel do século XX. A criptografia é a ciência que se preocupa com a elaboração de métodos seguros para esconder as informações em transito de partes não autorizadas. O desenvolvimento da criptografia quântica começou com idéias apresentadas na década de 80 com a proposta de Bennett e Brassard em 1984 (o BB84) e a realização experimental de um protocolo criptográfico quântico em 1990 que gerou um boom em pesquisas na área. Atualmente a distribuição quântica de chaves já é uma realidade no mercado de segurança de informação, pelo menos para curtas distâncias. Foram realizados, durante um semestre, estudos em criptografia clássica, abordando protocolos simétricos e assimétricos, análise de protocolos, problemas de distribuição de chaves criptográficas. Uma introdução aos formalismos e problemas da teoria de informação, da mecânica quântica, e da informação quântica foram feitos. O formalismo de sistemas simples de dois níveis, utilizados na distribuição quântica de chaves em criptografia, foi analisado. A polarização da molécula de amônia, como apresentada por Feynman, e as polarizações verticais e horizontais de fótons serviram de modelos básicos de sistema simples de dois níveis. As "comunicações quânticas" serão, e têm sido, realidades graças também ao desenvolvimento da criptografia quântica.

Criptografia - Criptografia quântica - Informação quântica