Projeto de Instrumentação para o Ensino F809

Criptografia quântica: o Protocolo B92

12 de abril de 2005

Aluno: Felipe Lourenço - R.A.: 016035

Orientador: Prof. Antonio Vidiella Barranco (DEQ)

Introdução

Apresentamos aqui o projeto a ser desenvolvido durante o primeiro semestre de 2005 na disciplina F 809. O tema principal é o protocolo de criptografia quântica B92 [1] proposto pela primeira vez em 1992 por C.H.Bennett. Nele são exploradas propriedades de dois estados quânticos não-ortogonais, afim de se conseguir a distribuição quântica de chave, que possibilita a troca de mensagens criptografadas. Ainda mais, diversas propriedades ópticas estão envolvidas com a sua realização experimental.

Objetivos

A partir dessa proposta teórica, visamos explicar o aparato e os procedimentos experimentais necessários para a realização do protocolo [2]. Nessa parte procuraremos dar atenção ao fenômeno físico relevante em cada etapa do protocolo e que possibilita a sua segurança.

Além disso, também temos como objetivo a produção de uma simulação computacional desse protocolo. Para isso teremos como base algumas outras já existentes [3] e [4] para outro protocolo, o BB84. Pensamos que dessa maneira será possível dar uma demonstração satisfatória de um exemplo de criptografia quântica para uma pessoa que não a conhece, mas que tem algum conhecimento de física quântica.

Plano de trabalho

Afim de cumprirmos os objetivos apresentados acima, podemos dividir o projeto em três etapas principais, em uma possível ordem cronológica:

1. Estudo do protocolo B92.

2. Desenvolvimento da simulação do protocolo.

3. Explicação do experimento.

Referências

[1] C.H.Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[2] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. 81, 3283 (1998).

[3] `http://www.columbia.edu/~mpj9/bb84.html`

[4] `http://monet.mercersburg.edu/henle/bb84/demo.php`

[5] C.H. Bennett and G. Brassard, Proceedings of the IEEE international conference on computers, systems and signal processing, Banglore, India, pp.175, (1984); uma versão eletrônica do artigo pode ser encontrada em: `http://quantum.bbn.com/dscgi/ds.py/get/file-18/BB84.pdf`