



Criptografia quântica: onde a tecnologia encontra os fundamentos.

Fernando de Melo

CBPF

Os primeiros usos da criptografia datam de mais de 4.000 anos. Hoje a criptografia é uma parte fundamental da estrutura da nossa sociedade. Basicamente toda comunicação digital é (ou deveria ser) criptografada. A segurança da comunicação moderna depende da complexidade computacional de certos problemas matemáticos. Ou seja, embora os transistores, componentes essenciais dos computadores atuais, só tenham sido concebidos com o desenvolvimento da Mecânica Quântica, um hacker não precisa saber de tunelamento para tentar espionar uma conversa. Neste seminário quero mostrar como os aspectos mais fundamentais da Mecânica Quântica estão sendo utilizados para criar métodos criptográficos cuja segurança não depende da dificuldade matemática, mas sim das leis da Física.