



Criptografia Quântica



Laboratório de Óptica Quântica - Instituto de Física - UFRJ

Segurança? Codificação? Cripto-quê???

Como consequência da atual era digital, produzimos um volume cada dia maior de informação. Entretanto, dificilmente paramos para refletir sobre quem possui acesso a esses dados. O que aconteceria se alguém obtivesse nossas senhas de banco? Nossos emails? Nossas conversas particulares? Sendo assim, é extremamente necessário que nossos dados sejam armazenados e transmitidos de forma segura. Felizmente, existe uma solução: Criptografia!



Chamamos de Criptografia um conjunto de técnicas para codificar mensagens, utilizando chaves criptográficas, de tal forma que apenas o emissor e o receptor dessas as consigam ler. Assim, mesmo se um hacker mal-intencionado tentar acessar nossos dados, tudo que ele vai obter será um conjuntos de caractéres aleatórios que não farão sentido algum para ele. Assim, contanto que nossas chaves permaneçam protegidas, podemos garantir a segurança e proteger nossas informações contra o acesso indevido por terceiros.

Atualmente, métodos criptográficos podem ser encontrados em diversas aplicações do nosso dia-a-dia, tais quais caixas eletrônicos, aplicativos de smartphones e redes sociais.



A eterna luta do Gato e o Rato

Como a codificação da mensagem depende de uma chave criptográfica, se torna essencial a transmitir e armazenar de forma segura. Para isso, criptógrafos desenvolvem diversos métodos matemáticos que protegem a chave contra um espião. Entretanto tais métodos pressupõe um espião com poderes computacionais limitados, o que faz com que, à medida que computadores cada vez mais potentes passam a ser comercializados, novos métodos tenham que ser desenvolvidos regularmente. Devido à isso, temos um longo embate entre criptógrafos e criptohackers.

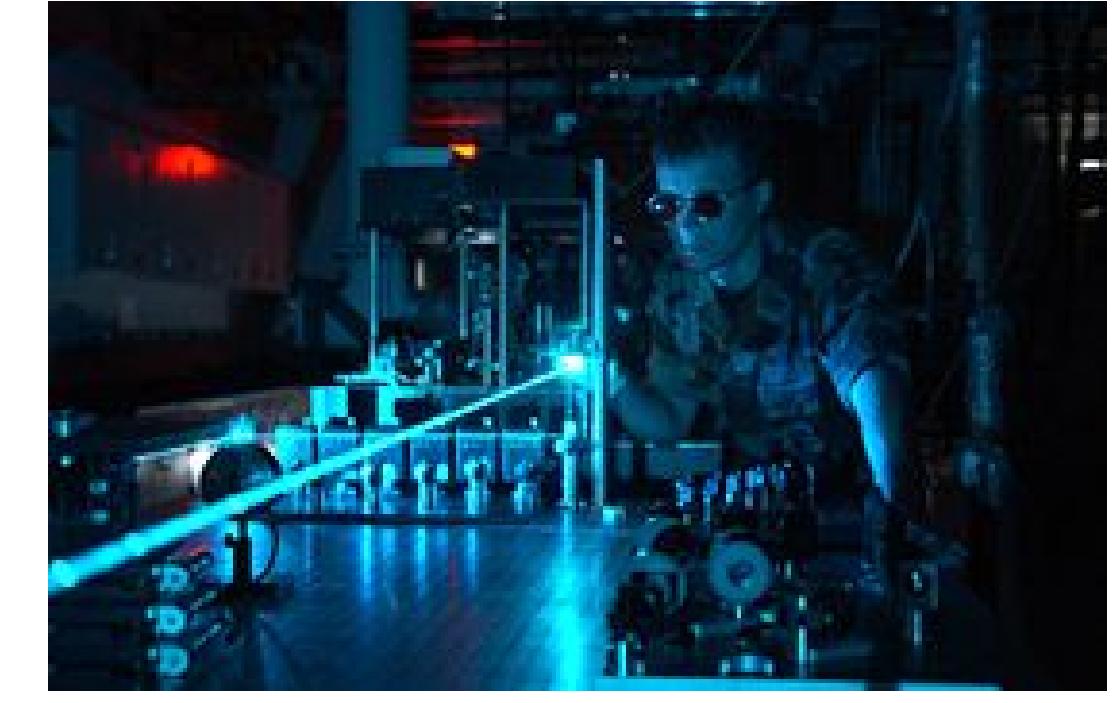


Visando solucionar esse embate, físicos, matemáticos e cientistas da computação estudaram novas formas de criptografia, eventualmente criando a área conhecida hoje como Criptografia Quântica.

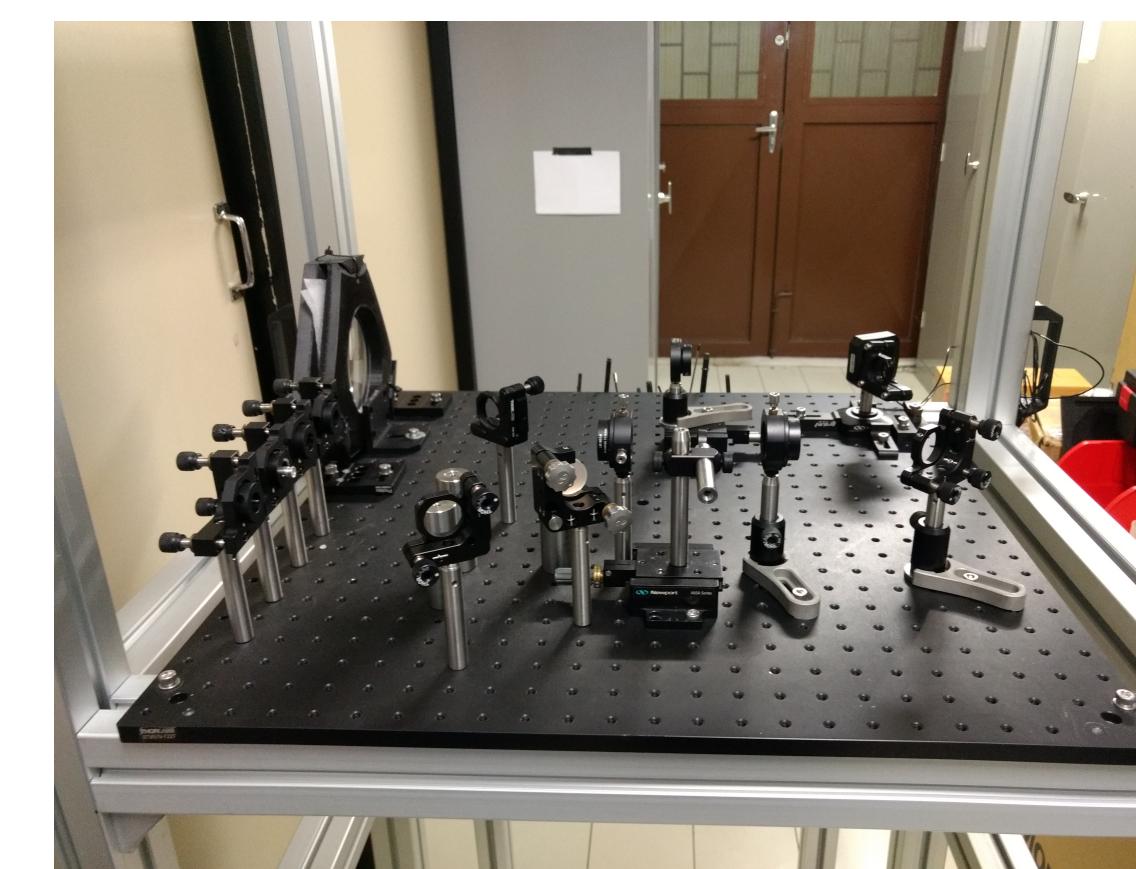
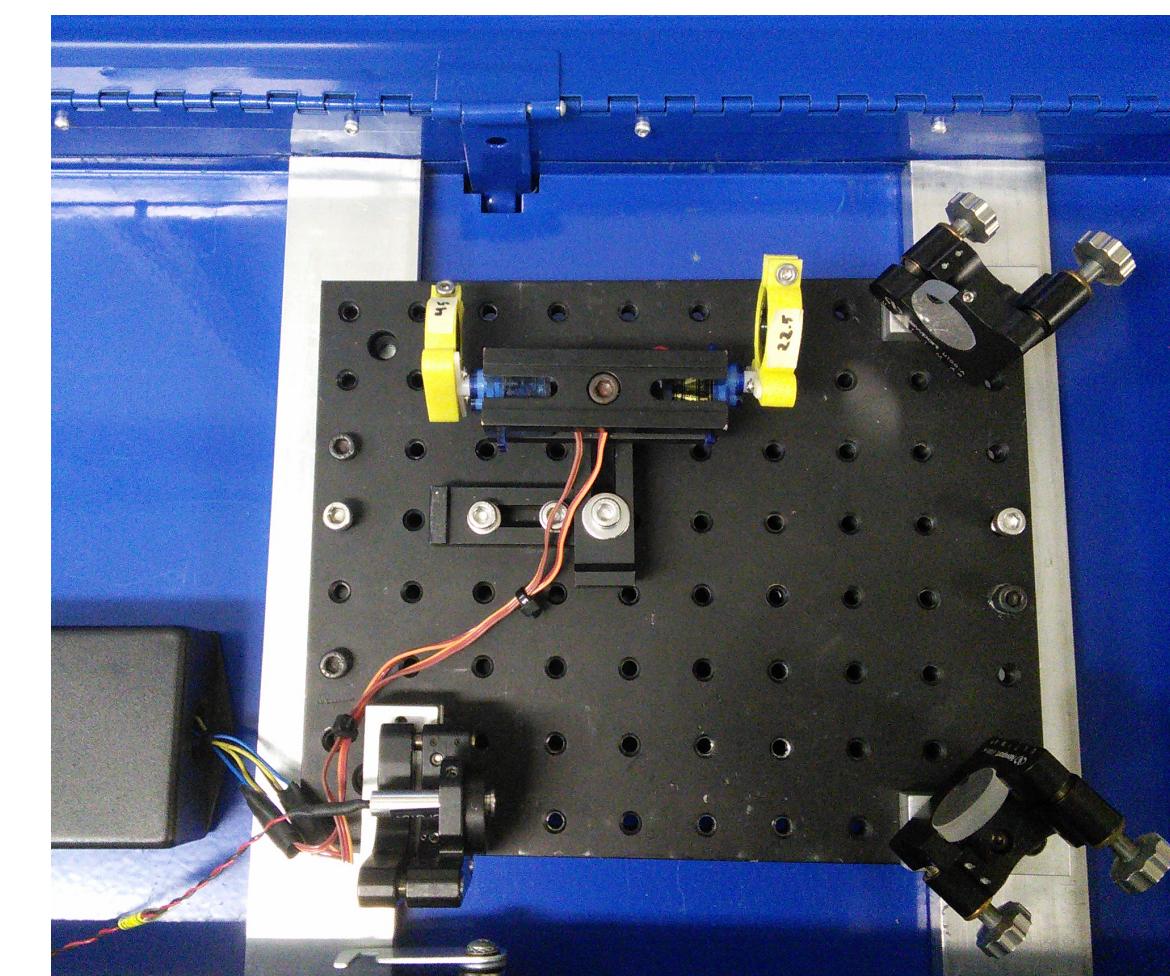
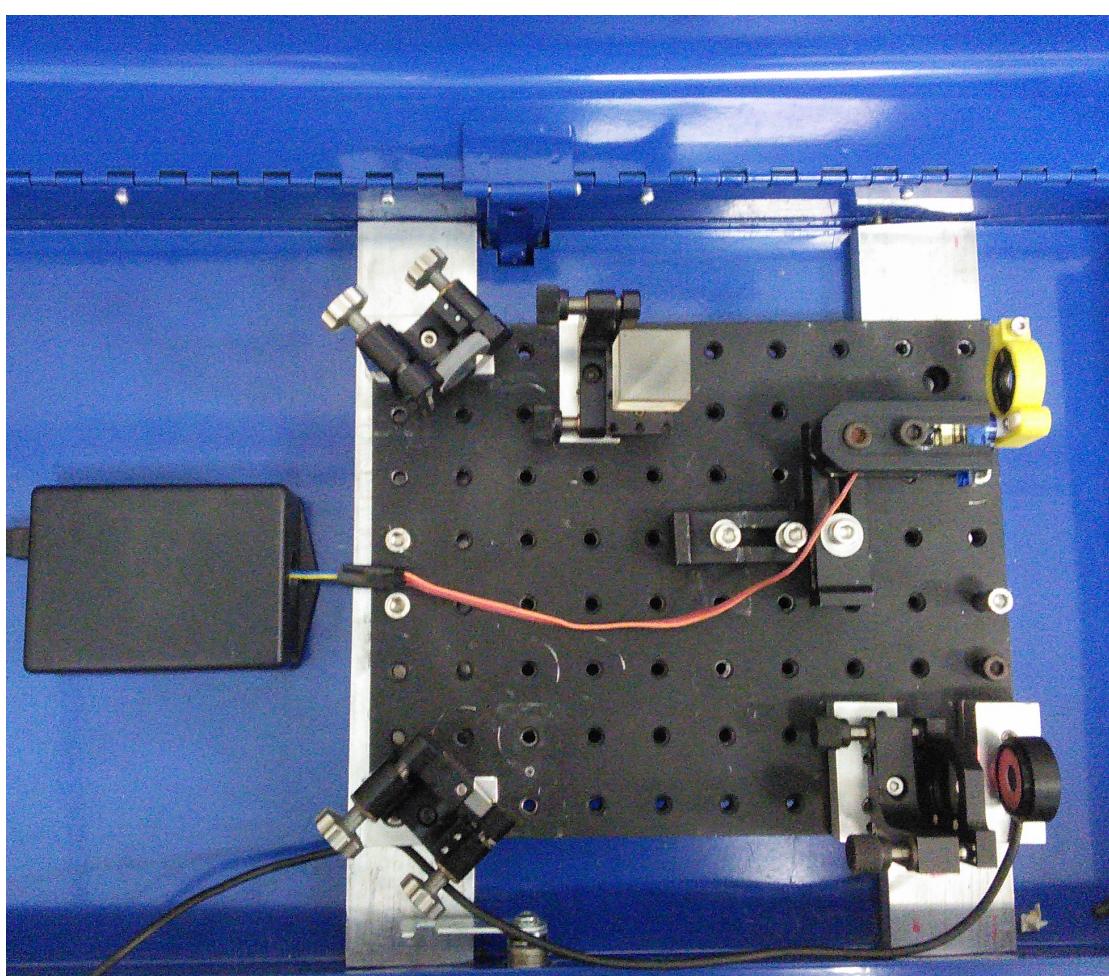
Gatos, Lasers e Criptografia

A Criptografia Quântica consiste de protocolos que, baseados na mecânica quântica, garantem a transmissão de chaves de forma segura, independente do poder computacional de um possível hacker.

Seu funcionamento se dá pela forma como a chave é gerada e transmitida. Utilizamos fôtons, partículas de luz emitidas por um laser, para transmitir informação da chave. Devido às estranhas propriedades da mecânica quântica, é impossível um espião conseguir observar a comunicação sem ser percebido, não importando a forma ou o dispositivo utilizado.



Nossa implementação, baseada no protocolo BB84, busca realizar transmissões quânticas de chave à grandes distâncias de forma rápida e eficiente. A seguir podemos ver algumas fotos do nosso experimento.



Ao Infinito e Além!

Realizando uma rápida pesquisa na internet, encontramos facilmente diversos centros de pesquisas especializados e até mesmo empresas explorando criptografia quântica a nível comercial em diversos lugares do mundo. No Brasil, no entanto, pouco se fala a respeito do assunto e o conhecimento técnico da área é muito limitado.

Nossos estudos buscam, assim, gerar experiência e desenvolvimento nacional e, junto ao efervescente cenário brasileiro de segurança da informação, tornar o Brasil uma referência na área.