Os computadores foram, sem dúvida, uma das maiores invenções do século passado. Com seu uso diversificado, eles passaram a integrar nosso dia-a-dia, através de editores de texto (que aposentaram as máquinas de escrever), dos jogos para crianças e adultos, do correio eletrônico e, mais recentemente, da telefonia e das videoconferências. Hoje, é possível ter acesso, através da internet (a rede mundial de computadores), a informação em larga escala, armazenada em diferentes pontos do planeta. O fenômeno da globalização da informação é inegável.

Os primeiros computadores, na década de 1940, eram enormes, ocupavam andares inteiros e eram dedicados exclusivamente a cálculos complicadíssimos. Com a tecnologia dos semicondutores e a substituição das válvulas por transistores, veio a miniaturização dos componentes. E, com ela, os computadores se tornaram cada vez menores, mais velozes e potentes.

Mas a miniaturização não pode continuar indefinidamente e está limitada, em última instância, ao tamanho do átomo. Quando chegarmos aí, através da nanotecnologia, uma nova revolução acontecerá, pois entrarão em jogo as estranhas propriedades quânticas da matéria, que permitirão uma nova era na computação e na rapidez dos cálculos.

Os computadores quânticos usarão essas propriedades para resolver, em minutos ou segundos, problemas que levariam milhares ou até milhões de anos para o mais veloz dos computadores deste início de século. Este folder se propõe a explicar e a descrever essa nova era, a chamada Era da Informação Quântica.

Prepare-se para essa revolução, que já começou!

Este folder faz parte do projeto de divulgação científica 'Desafios da Física', que se propõe a levar a um público amplo e não especializado novidades que estão acontecendo na vanguarda da física e que certamente mexerão com nosso cotidiano. Boa leitura.

João dos Anjos
COORDENADOR DO PROJETO DESAFIOS DA FÍSICA

PRESIDENTE DA REPÚBLICA
Luiz Inácio Lula da Silva

MINISTRO DE ESTADO DA CIÊNCIA E TECNOLOGIA
Sergio Machado Rezende

SUBSECRETÁRIO DE COORDENAÇÃO DAS UNIDADES DE PESQUISA
Avílio Antônio Franco

DIRETOR DO CBPF
Ricardo Magnus Osório Galvão

EDITOR CIENTÍFICO
Ivan S. Oliveira (Centro Brasileiro de Pesquisas Físicas/MCT)

APOIO FINANCEIRO
Vitae

REDAÇÃO E EDIÇÃO
Cássio Leite Vieira

PROJETO GRÁFICO
Ampersand Comunicação Gráfica
(www.amperdesign.com.br)

CENTRO BRASILEIRO DE PESQUISAS FÍSICAS
Rua Dr. Xavier Sigaud, 150
22290-180 - Rio de Janeiro - RJ
Tel: (0xx21) 2141-7100
Fax: (0xx21) 2141-7400
Internet: http://www.cbpf.br

Para receber gratuitamente pelo correio um exemplar deste folder, envie pedido com seu nome e endereço para ncs_cbpf@cbpf.br. Este e outros folders da série *Desafios da Física*, bem como a revista *CBPF – Na Vanguarda da Pesquisa*, estão disponíveis em formato PDF em http://www.cbpf.br/Publicacoes.html

Agradecimentos: Roberto Silva Sarthour
(Centro Brasileiro de Pesquisas Físicas/MCT)

Vitae não compartilha necessariamente dos conceitos e opiniões expressos neste trabalho, que são da exclusiva responsabilidade dos autores.

CBPF

VITAE
Apoio à Cultura, Educação e Promoção Social

Ministério da Ciência e Tecnologia

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Informação Quântica

do teleporte à última fronteira da computação

CBPF
Centro Brasileiro de Pesquisas Físicas
2006

Sumário

Fontes

DAVIDOVICH, L. 'Informação quântica – do teletransporte ao computador quântico' in *Ciência Hoje* (n. 206, julho de 2004)
DAVIDOVICH, L. 'O gato de Schrödinger: do mundo quântico ao mundo clássico' in *Ciência Hoje* (n. 143, outubro de 1998)
DAVIDOVICH, L. 'Teletransporte: uma solução em busca de um problema' (entrevista) in *Ciência Hoje* (n. 137, abril de 1998)
NIELSEN, M. A. e CHUANG, I. L. *Computação quântica e informação quântica*. Tradução Ivan S. Oliveira (Bookman Cia, São Paulo, 2005)
NIELSEN, M. A. 'Regras para um mundo quântico complexo' in *Scientific American Brasil* (Edição especial, n. 8, pp. 24-33, 2005)
OLIVEIRA, I. S. 'Computação quântica: a última fronteira da informação' in *Ciência Hoje* (n. 179, jan / fev 2002)
OLIVEIRA, I. S. *et al.* 'Computação quântica – manipulando a informação oculta do mundo quântico' in *Ciência Hoje* (n. 193, maio de 2003)
ZEILINGER, A. 'Teletransporte quântico' in *Scientific American Brasil* (Edição especial, n. 8, pp. 34-43, 2005)

EXPERIÊNCIAS INDIVIDUAIS

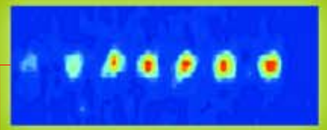


FOTO DE RAINER BLATT/UNIVERSIDADE DE INNSBRUCK (ÁUSTRIA)

JOVEM PROMESSA • Há 50 anos, qualquer proposta de fazer experiências com átomos, moléculas ou fótons (partículas de luz) individuais seria certamente tachada como pura ficção científica. Mas, neste início de século, isso não só é realidade, mas também objeto de pesquisa da chamada informação quântica, área que se tornou um tipo de jovem promessa da física. Hoje, de forma quase prosaica, laboratórios no mundo isolam um único fóton do contato com o universo, arrastam apenas um átomo com a ajuda de microscópios especiais, criam correntes elétricas de um só elétron ou aprisionam íons em campos magnéticos.

POR PRINCÍPIO... A INCERTEZA • No mundo macroscópico, basta saber a posição e o momento (o produto da massa pela velocidade) de um objeto qualquer para determinar seu estado e, a partir dele, prever, em qualquer instante, os resultados de medidas efetuadas sobre esse objeto. Porém, o estado de uma única entidade quântica (molécula, átomo, elétron, fóton etc.) não pode ser medido com precisão. Em função das dimensões com que passamos a lidar, qualquer tentativa nesse sentido altera o estado do objeto que se quer medir. Assim, quando se consegue medir a posição de um elétron, por exemplo, a incerteza em relação à velocidade dessa partícula cresce vertiginosamente. E vice-versa. Essa é a essência do chamado princípio da incerteza, uma lei que se estende, por exemplo, para outros pares de grandezas, como energia e tempo.

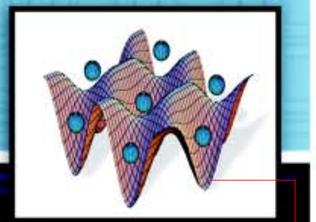
PILAR DE SUSTENTAÇÃO • O estado quântico completo de uma única partícula não pode ser medido. Isso não só é fato, mas lei. Porém, surpreendentemente, percebeu-se que esse mesmo estado, apesar de desconhecido, poderia ser manuseado e transmitido. E aí está, talvez, o principal pilar da informação quântica. Sustentado por ele, novos fenômenos foram propostos e outros obtidos em laboratório. Com isso, pode-se definir a área de informação quântica como o estudo de métodos para caracterizar, transmitir, armazenar, compactar e usar a informação contida em estados quânticos.

CRIPTOGRAFIA QUÂNTICA

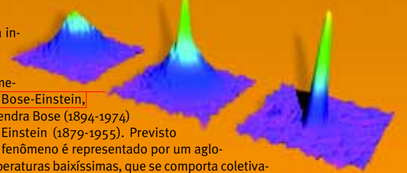
MÉTODO INVIOLÁVEL • Um desdobramento que certamente terá uma aplicação tão vasta quanto a dos computadores quânticos é a chamada criptografia quântica, um processo dito inviolável para a transmissão segura de dados confidenciais.

AÇÃO FANTASMAGÓRICA? • Para entender por que a criptografia quântica é dita 100% segura, é preciso recorrer a um dos fenômenos mais bizarros da natureza: o emaranhamento de partículas. Nele, duas partículas – fótons, por exemplo – são criadas em condições especiais e passam, a partir daí, a se comportar como se estivessem sempre conectadas uma a outra, independentemente da distância entre elas, como em um tipo de telepatia. Qualquer alteração do estado quântico de uma implica a mudança instantânea do estado da segunda, mesmo que o par esteja separado por milhares ou milhões de km de distância. O físico de origem alemã Albert Einstein (1879-1955) achava tão esquisita essa propriedade que a batizou "fantasmagórica ação a distância". Outro físico, o austríaco Erwin Schrödinger (1887-1961), a classificou como 'a' propriedade mais importante da física quântica.

PARTÍCULAS GÊMEAS • O processo da criptografia quântica se dá mais ou menos assim: criam-se pares de partículas gêmeas (ou emaranhadas) – isso pode ser feito com qualquer partícula, até mesmo com átomos. O integrante de cada par é enviado para um receptor, através de um meio (fibra óptica, no caso de fótons), carregando a mensagem, na forma de informação quântica, que se quer transmitir. Agora, vamos imaginar que uma pessoa malintencionada resolva interceptar uma ou mais dessas partículas para tentar arrancar delas a mensagem sigilosa. Ao fazer isso, irá alterar o estado quântico de cada uma delas. Ao final do processo, o emissor irá comparar o estado quântico de suas partículas com o daquelas em posse do destinatário. Caso haja alguma diferença entre os dois conjuntos, ambos ficam sabendo que houve uma tentativa de interceptação da mensagem e, com isso, podem tomar as medidas necessárias.

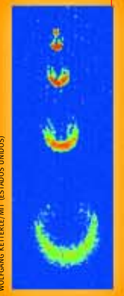


REALIDADE E PROMESSAS



CONDENSADO GIGANTE • A área da informação quântica se estende além da computação e criptografia. Ela engloba e prevê vários outros fenômenos. Um deles é o condensado de Bose-Einstein, uma referência ao físico indiano Satyendra Bose (1894-1974) e ao físico de origem alemã Albert Einstein (1879-1955). Previsto em meados da década de 1920, esse fenômeno é representado por um aglomerado de partículas, mantido a temperaturas baixíssimas, que se comporta coletivamente, como se fosse um 'átomo gigante', o que permite estudar macroscopicamente detalhes do mundo quântico.

LASER DE ÁTOMOS • Demonstrado experimentalmente há cerca de uma década, a novidade sobre os condensados de Bose-Einstein é que a incidência de ondas de rádio sobre esse aglomerado possibilita extrair dele uma 'fila' ordenada de partículas que vem sendo denominada *'laser'* de átomos, dada sua semelhança com o fenômeno óptico. Já se vislumbra que esse tipo de *laser* poderia servir de base para o desenvolvimento de instrumentos capazes tanto de aumentar a resolução dos intricados desenhos que formam os *chips* quanto medir diminutas variações do campo gravitacional e, com isso, detectar campos de petróleo, por exemplo.



WOLFGANG KETTERLE/MIT (ESTADOS UNIDOS)

TELEPORTE • Entre as diversas promessas experimentais da área de informação quântica está o chamado teleporte, descoberto em 1993 por Bennett e colegas. Quando foi obtido experimentalmente pela primeira vez, em 1997, pela equipe de Dik Bouwmeester, da Universidade de Oxford, o fenômeno ganhou a mídia mundial e foi logo associado (erroneamente) ao teletransporte da série 'Jornada às Estrelas', através do qual tripulantes eram transportados da nave *Enterprise* para a superfície dos planetas e de lá resgatados. A diferença é que nesse equipamento fictício havia transporte de matéria. No teleporte, há apenas a transmissão da impalpável informação quântica de uma partícula (fóton, átomo etc.) para seu par gêmeo, feita com base no fenômeno do emanharamento.

REALIDADE PRESENTE • Arthur Eckert, também de Oxford, disse que, assim que o primeiro computador quântico entrar em funcionamento, todos os sistemas de transmissão de informação deixarão de ser seguros. E isso parece ser consenso entre seus colegas. O computador quântico ainda está longe dos mil *q-bits* com os quais, acredita-se, começará a provar seu potencial, mas muitos acreditam que o primeiro *chip* quântico será apresentado ao mundo antes da data-limite imposta pela lei de Moore. O emaranhamento já é bem-sucedido com aglomerados de partículas, e a criptografia quântica já está sendo empregada, em escala piloto, para transações bancárias na Europa e em redes de comunicação unindo universidade e empresas nos Estados Unidos. Empresa dedicadas exclusivamente à computação quântica já estão funcionando. O futuro parece ser quântico.

CORPO MAGNÍFICO • A área de informação quântica nasceu dos esforços dos físicos em compreender as sutilezas teóricas e experimentais da física quântica e poderá criar ferramentas poderosas para tornar mais transparente esse magnífico corpo teórico. Como disse Feynman, ainda na década de 1980, sistemas físicos quânticos só podem ser simulados com eficiência em computadores quânticos. A área de informação quântica é a prova cabal de que a ciência básica, desinteressada, ainda é a base de sustentação do progresso tecnológico e a principal promotora do bem-estar humano.

CALIFORNIA INSTITUTE OF TECHNOLOGY

NO BRASIL • Em 2001, foi estabelecido no Brasil o Instituto do Milênio de Informação Quântica (IMIQ), para coordenar a pesquisa dos vários grupos que atuam nessa área no país. Alguns temas de pesquisa realizada por aqui: átomos aprisionados em cavidades supercondutoras; criação e estudo de fótons emaranhados; pinças ópticas; pontos quânticos e ressonância magnética nuclear aplicada à computação quântica. Mais informações sobre o IMIQ estão em omnis.if.ufrj.br/~infoquan/

COMPUTADOR QUÂNTICO

WWW.JARSON.COM

VEDETE DA ÁREA • De um vasto menu de resultados experimentais surpreendentes e promessas teóricas instigantes, público e mídia parecem já ter escolhido a vedete da informação quântica: o computador quântico, que se tornou a mais popular faceta aplicada da área. Essa máquina, que já começa a sair do plano teórico, teria a capacidade de resolver em segundos ou poucos minutos problemas que dariam milhares ou milhões de anos de trabalho para o mais moderno computador deste início de século.

LEI EMPÍRICA • A primeira motivação – ainda que indireta – para o computador quântico surgiu ainda em 1965, quando Gordon Moore, fundador da Intel, uma das gigantes mundiais do ramo de informática, notou que, a cada 18 meses, os microprocessadores (*chips* com memória) dobravam tanto o número de transistores embutidos neles quanto a velocidade de processamento de informação. E, com isso, a representação física (número de átomos) de uma unidade (*bit*) de informação também diminuía significativamente. Essa observação tornou-se uma lei empírica, válida até hoje. Porém, esse não é o final da história.

UM *BIT*, UM ÁTOMO • Hoje, cada *bit* de informação dentro dos computadores é representado por alguns bilhões de átomos. Porém, com base na lei de Moore, cada *bit* de informação, por volta de 2020, estará resumido a um único átomo, o que irá impor um limite físico ao desenvolvimento dos computadores. E, nessa escala de comprimento, não há saída: esse é o domínio da física quântica, teoria que nasceu no primeiro quarto do século passado e lida com os fenômenos na dimensão molecular, atômica e subatômica. Se a lei de Moore cumprir seu fatídico desígnio – e tudo indica que irá –, será necessário um novo paradigma computacional. É aí que entra o computador quântico.

ZERO E UM, AO MESMO TEMPO • Em um computador dos dias de hoje – denominado clássico pelos físicos –, um *bit* de informação pode assumir dois valores: zero ou um. Mas, na versão quântica desse equipamento, um *bit* pode representar, ao mesmo tempo, esses dois valores, graças a um fenômeno denominado superposição de estados. No mundo macroscópico, seria como se a face de uma moeda fosse, simultaneamente, cara e coroa, até que alguém decidisse observá-la ou efetuar uma medida sobre ela. Aí essa superposição se desfaria, e nossa moeda apresentaria ou cara, ou coroa.

MUNDO ESTRANHO • O mundo quântico não parece estranho. Ele, certamente, é. A superposição é apenas um dos fenômenos que vão contra o senso comum. No nanouniverso, entidades podem se comportar ora como ondas, ora como corpúsculos. Podem até mesmo ocupar dois lugares ao mesmo tempo. Ou, de forma mais intrigante, manter um tipo de 'comunicação telepática'. Nada disso tem um correspondente em nosso dia-a-dia. O físico dinamarquês Niels Bohr (1885-1962) certa vez disse que aquele que não fica espantado diante da física quântica é porque não a entendeu. Outro grande físico do século passado, Richard Feynman (1918-1988) foi mais enfático. Para ele, quem afirmasse ter entendido a mecânica quântica estaria mentindo.

WWW.IM.DK

DESENVOLVIMENTOS IMPORTANTES • A lei de Moore implica que a tecnologia do silício está com seus dias contados. No entanto, o computador quântico só ganhou algum fôlego nas décadas seguintes, impulsionado por desenvolvimentos importantes. Em 1973, Charles Bennett, da empresa IBM, mostrou que seria possível fazer um computador no qual a informação que entra poderia ser recuperada a partir daquela que sai, algo que, em certos casos, é impossível para os computadores clássicos. Nove anos depois, Paul Benioff, do Laboratório Nacional Argonne (Estados Unidos), mostrou que a física quântica era o cenário natural para a máquina imaginada por Bennett, pois essa reversibilidade é uma característica natural dos fenômenos quânticos.

TESTE DA MOEDA • Em 1985, David Deutsch idealizou o primeiro procedimento matemático (algoritmo) para a resolução de um problema num computador quântico. Com isso, o físico da Universidade de Oxford (Inglaterra) mostrou que, num computador quântico, o número de etapas para resolver um problema seria bem menor que aquele num computador clássico. Para entender o que Deutsch propôs, imagine um teste: se uma moeda tiver cara e coroa, será considerada verdadeira. Em qualquer outra situação, falsa. Para testar a moeda, um computador clássico precisaria de dois passos: checar um lado e depois o outro. Num computador quântico, os dois lados da moeda poderiam ser verificados simultaneamente, numa só etapa.

ALGORITMO DE SHOR • Mas foi em 1994 que se injetou uma dose maior de realidade nos computadores quânticos. Peter Shor, então pesquisador dos Laboratórios Bell (Estados Unidos), apresentou um algoritmo quântico para fatorar números muito grandes. O candidato natural para o teste era o RSA, um procedimento para criar códigos secretos com base na multiplicação de números primos. Esses códigos são tidos como invioláveis e, por isso, empregados hoje para proteger dados cujo conteúdo deve ser sigiloso.

CRENÇA NO CÓDIGO • Toda a crença na inviolabilidade da transmissão sigilosa de dados (senhas bancárias, números de cartão de crédito etc.) baseia-se no fato de um código gerado pelo RSA – que leva as iniciais de seus idealizadores, Ron Rivest, Adi Shamir e Len Adleman – ser praticamente inviolável, pois computadores modernos levariam muito tempo para chegar à informação que foi codificada. Porém, recentemente, computadores em rede, conectados pela internet, 'quebraram' um código RSA. Isso mostrou que era só uma questão de força bruta computacional. Mas, para um computador quântico rodando o algoritmo de Shor, isso seria uma tarefa para lá de trivial: o processamento levaria segundos ou, no pior cenário, alguns poucos minutos.

CANDIDATOS A *Q-BITS* • Num computador clássico, um *bit* é representado fisicamente por um componente eletrônico dentro do *chip*. Para um *q-bit* (do inglês, *quantum bit*), já há uma lista de candidatos: íons aprisionados em armadilhas magnéticas; átomos e fótons armazenados em cavidades supercondutoras de eletricidade; átomos ocupando 'vales' de uma rede cristalina óptica ('superfície' que lembra uma caixa de ovos formada por ondas eletromagnéticas estacionárias); pontos quânticos (conjunto de elétrons confinados a dimensões nanométricas). Porém, um dos candidatos mais promissores é uma propriedade dos núcleos atômicos conhecida como *spin* nuclear, que pode ser grosseiramente comparada com a rotação de um objeto macroscópico. A diferença com o mundo macroscópico é que um *spin* nuclear, graças ao fenômeno da superposição de estados, pode 'girar' ao mesmo tempo nos dois sentidos, horário e anti-horário, o que, como se sabe, é impossível para um pião, por exemplo. A manipulação da informação contida nos *q-bits* seria feita por ressonância magnética nuclear, a mesma técnica empregada em exames médicos e conhecida há cerca de 50 anos.

QUESTÃO DE ANOS • Em 2001, pesquisadores da IBM conseguiram fazer uma demonstração experimental do algoritmo de Shor ao realizar a fatoração do número 15 em fatores primos (15=3x5). O papel de computador quântico foi desempenhado por moléculas de $C_7H_5F_3O_2Fe$, cuja estrutura continha sete *q-bits*. Nada muito instigante do ponto de vista da capacidade computacional, mas um feito que reforçou a crença de que os computadores quânticos, em questão de anos, já serão realidade, com *q-bits* robustos e baseados num sistema físico que permita a geração, manipulação e leitura de estados quânticos estáveis.