# Alain Aspect e a criptografia quântica

Sophie Chivet

# "Códigos secretos protegidos pelas leis da natureza"

*entrevistado por Leila Haddad*

**O mundo quântico, povoado de objectos que têm o dom da ubiquidade e que tanto se comportam como ondas como partículas, escapa à nossa lógica habitual. Alain Aspect, director de investigação no CNRS (Centre National de Recherche Scientifique), professor da Escola Politécnica e responsável pelo grupo de óptica atómica do Instituto de Óptica Teórica e Aplicada de Orsay, dissipa um pouco desta bruma explicando como essas curiosas propriedades podem decorrer de uma tecnologia digna da ficção científica.**

**"Science et Vie" – A mecânica quântica é hoje uma "velha senhora" que já não precisa de dar provas da sua eficácia. No entanto, permanecem por esclarecer alguns "mistérios". Por exemplo, como se faz a passagem deste mundo de estranhas propriedades para o nosso universo macroscópico?**

**Alain Aspect –** É um grande problema que continua sem solução... A mecânica quântica autoriza a existência do que se denomina por sobreposição coerente de duas situações que, consideradas separadamente, não são nada de especial. Pegue-se, por exemplo, numa partícula que vai interferir. Para isso, ela deve passar por dois lugares diferentes. Posso dizer separadamente "a partícula está de um lado", e isso nada tem de espectacular do ponto de vista da mecânica clássica. E dizer "ela está do outro lado" – essa situação também não tem nada de extraordinário.

Em contrapartida, se eu disser: "A partícula está ao mesmo tempo nos dois lados", eis algo de espantoso. Ora, é o que se passa quando há uma sobreposição coerente que se manifesta através de interferências. Mas com objectos à nossa escala nunca obtemos tal fenómeno. Um objecto nunca está simultaneamente em dois lugares. Porquê? Pensa-se que as interacções incontroláveis com o ambiente destroem muito depressa toda a sobreposição coerente de objectos macroscópicos. Um fotão que se propaga num recipiente vazio tem uma interacção muito pequena com o ambiente e não há des-coerência. Mas quanto maior é o objecto, mais ele tem facilidade de interagir com o ambiente e mais a des-coerência se produz fácil e rapidamente. Dito isto, não há necessidade de imaginar que existe uma fronteira, uma barreira nítida e clara, entre o mundo quântico e o mundo macroscópico, e que bastaria um salto para passar de um para o outro. Se pegarmos num grande objecto e fizermos tudo para

não o perturbar, ele poderá mostrar ainda efeitos quânticos. Fizeram-se recentemente grandes progressos neste domínio. Penso, por exemplo, nas experiências de interferência com átomos ou moléculas, ou nas experiências sobre a des-coerência realizadas, na École Normale Supérieure, pelo grupo de Serge Haroche e Jean-Michel Raymond. Mas isso não nos impede de estar longe de compreender tudo.

**P. – O mundo quântico tem propriedades bem curiosas... Quais serão as suas novas aplicações?**
**R. –** Antes de mais, é preciso lembrar que o laser ou o transístor são objectos quânticos. Mas, se pensarmos nas aplicações de propriedades quânticas em grande escala, então a criptografia quântica parece-me um excelente exemplo. É uma autêntica revolução técnica, autorizada pela não-separabilidade. No começo dos anos 80 ninguém imaginava que os estudos fundamentais que realizámos sobre a não-separabilidade levariam onde levaram.

**P. — O que é a não-separabilidade?**
**R. —** Após a concretização da mecânica quântica, em 1925, houve uma grande discussão entre Niels Bohr e Albert Einstein acerca do significado desta teoria. Ela incidia sobre a questão da famosa não-localidade quântica, levantada por Einstein e os seus colegas em 1935, e ainda hoje de grande actualidade. Segundo Niels Bohr (e para simplificar muito o seu raciocínio), o formalismo da mecânica quântica prevê a possibilidade de duas partículas muito afastadas uma da outra constituírem um todo inseparável, de modo a que não se possa falar separadamente de uma e da outra.
Einstein propunha uma outra interpretação deste fenómeno, atribuindo às partículas propriedades que alguns chamavam variáveis escondidas, subjacentes ao formalismo quântico mas que não eram incompatíveis com ele. Em 1965, John Bell descobriu que, na realidade, havia uma incompatibilidade entre as duas concepções. Era necessário ir mais fundo, através de uma série de experiências a que demos uma contribuição importante nos anos 80. Todas as experiências mostraram que a natureza funciona de acordo com as previsões da mecânica quântica: as partículas estão afastadas e, no entanto, elas constituem um todo inseparável.

**P. – Para retomar uma imagem mais familiar (embora falsa), é como se as partículas "comunicassem" à distância. Qual poderia ser a natureza desse elo?**
**R. –** Ah, pois... A única resposta sólida está nas equações. No entanto, se eu procurar uma imagem não consigo representar esse elo de outra forma que não seja uma espécie de interacção instantânea. Mas, por outro lado, sei mostrar que esta interacção é diferente das interacções habituais, porque ela não me permite enviar uma mensagem. A não-separabilidade existe, mas nós não podemos servir-nos dela para transportar matéria, energia ou informação utilizável, contrariamente ao que se pode ler a propósito da teleportação quântica. Podemos demonstrar que tudo se passa como se existisse um elo não local, mas não podemos utilizá-lo para tomar uma decisão concreta.

**P. – Como utilizar esta não-localidade para codificar mensagens?**
**R. –** A criptografia é muito simplesmente a arte de codificar a informação de um modo indecifrável para um adversário.
Até ao momento, a segurança da codificação assentava em duas hipóteses: o adversário não tem um computador mais poderoso do que o meu, e não fez progressos matemáticos tais que lhe dariam os meios de decifrar o meu código. Como se vê, a segurança não está garantida de modo absoluto.
Em criptografia quântica, pelo contrário, são as leis da física quântica — ou seja, as leis da natureza — que vão garantir que dois correspondentes tenham nas suas mãos duas cópias idênticas de chaves secretas que não foram interceptadas por nenhum espião. O método utiliza pares inseparáveis de fotões que se dirigem, cada um deles, para um dos dois correspondentes. Estes, ao fazerem medições de polarização, obtêm duas séries de números aleatórios que servirão de chave codificadora e descodificadora. Essa chave não existe até ao momento em que os nossos dois observadores fazem medições. Se um espião tentar ler a polarização de fotões para obter uma cópia da chave deixará inevitavelmente traços.

**P. – Que tipo de traços?**
**R. –** Uma des-coerência que se traduzirá numa modificação subtil das polarizações observadas. Os dois observadores detectarão esta modificação ao confrontarem o resultado das medidas das desigualdades de Bell.
O que é notável é que propriedades tão subtis possam sobreviver com pares de fotões inseparáveis enviados através de uma rede "standard" de fibra óptica de telecomunicações, tal como foi demonstrado pelos nossos colegas de Genebra.

(acordo "Science et Vie" (nº 980, Maio 99)/
"Gazeta de Física", tradução de Carlos Pessoa)


Sophie Chivet