Os segredos que a quântica não revela

As primeiras redes que usam cifra quântica já começaram a fazer negócio e a ver a luz. Literalmente

Um texto ou uma imagem não mudam depois de observadas, mas na cifra quântica é esse o pressuposto do sucesso. "Quando leio um bit transmitido com criptografia quântica, altero o seu estado. O que pode ser chocante para a nossa lógica clássica, que nos diz que a leitura de um livro não muda o que lá está escrito", explica Yasser Omar, professor do Instituto Superior Técnico.

A criptografia quântica tem por base as regras mais elementares do mundo microscópico — e tem na luz o principal veículo. Para criarem redes protegidas pela quântica, os criptógrafos começam por condicionar o comportamento de fotões (as partículas mais elementares da luz). O processo recorre a dispositivos que usam espelhos e lentes para orientar e posicionar fotões de diferentes formas, a fim de codificar a informação que até pode ter sido previamente produzida por um qualquer computador clássico.

Além de terem em conta o comportamento dos fotões, estas redes usam uma única cifra para todos os intervenientes. O que promete comunicações à prova de escuta.

"Na criptografia quântica, se for detetada uma determinada taxa de erro nos bits quânticos, a comunicação pode ser interrompida, porque não há condições técnicas ou então porque há indícios de interceção", refere Yasser Omar.

Apesar de resiliente, a cifra quântica tem dois pressupostos: só funciona em fibra ótica ou em lasers; e exige redes dedicadas àquela função. Nas redes de fibra pode ser necessário incorporar repetidores que evitam a deformação dos fotões, mas nos lasers emitidos por satélites houve um recorde fixado em 2016 pelo governo chinês depois de anunciar comunicações a mais de sete mil quilómetros de distância. Não se sabe se mais alguém superou essa marca, mas a inexistência de novidades parece dar razão à China.

"A UE tem investido nestas tecnologias, para não ficar dependente do que os chineses e os americanos fazem. Quem conseguir ter uma cifra à prova das interseções dos outros Estados passa a ter uma arma", explica Bruno Gonçalves, diretor de cibersegurança da Warpcom.

Em outubro, a Warpcom participou, com a IP Telecom e a ID Quantique, da Suíça, numa primeira rede quântica portuguesa de 20 quilómetros, entre Lisboa e Almada. No Técnico também está em desenvolvimento um módulo de comunicações quânticas para satélites. "Em Espanha já há organizações a comprar estas soluções. Em Portugal começam a surgir manifestações de interesse", acrescenta Bruno Gonçalves.

Entre os entendidos não restam muitas dúvidas de que a criptografia clássica está condenada a prazo — e mais uma vez serão as leis da quântica a produzir efeito. Além de cifras para a comunicação, a quântica também abriu caminho a computadores que trabalham com bits quânticos, que, em vez de fotões, assumem em simultâneo o valor dos "zeros" e dos "uns" da linguagem binária da informática clássica. O que exponencia a capacidade de processamento. "Só a lentidão dos computadores atuais garante a resistência da cifra clássica a ataques. Com a computação quântica, a cifra clássica será rapidamente ultrapassada", conclui Yasser Omar.

HUGO SÉNECA
sociedade@expresso.impresa.pt