GCiencia
xornalismo+divulgación

O profesor da UVigo Marcos Curty.

Investigadores da UVigo rachan cos límites da criptografía cuántica

O profesor Marcos Curty, xunto a investigadores da Universidade de Toronto, atopan unha fórmula para levar as comunicacións máis lonxe, ata 700 km

Por

Redacción

-

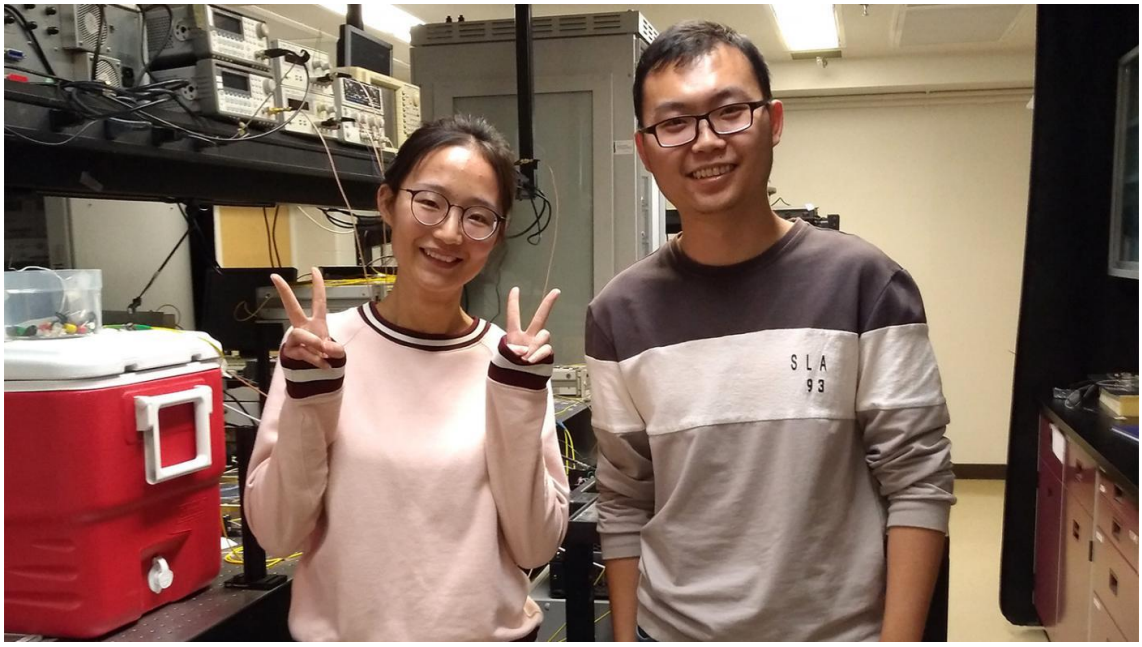
10/09/2019

A protección da información, daqueles datos confidenciais que, por exemplo, se transmiten en cada operación de compra a través da rede, constitúe hoxe en día un **servizo fundamental** para a sociedade. Na actualidade, as técnicas de cifrado convencionais, amplamente empregadas en internet, basean a súa seguridade na dificultade de resolver certos **problemas matemáticos**, o que fai que o avance da

capacidade de cálculo, con ordenadores cada vez máis potentes, implique un risco neste senso.

Non acontece así coa **criptografía cuántica**, técnica a través da que a información se codifica en pulsos ópticos e que "proporciona unha seguridade incondicional", como explica o profesor do Departamento do Teoría do Sinal e Comunicacións da Universidade de Vigo e investigador de atlanTTic **Marcos Curty**.

Non obstante, esta técnica vese limitada polas **distancias máximas de transmisión** que se poden acadar coas tecnoloxías actuais e que se situaban entre os 300 e os 400 quilómetros, ata que un experimento levado a cabo recentemente por Curty e investigadores da **Universidade de Toronto** demostrou que é posible "duplicar practicamente esas distancias de transmisión" ata alcanzar os 700 quilómetros.



Xiaoqing Zhong e Jianyong Hu, da Universidade de Toronto.

Así o constatan no estudo publicado recentemente na revista ***Physical Review Letters***, da Sociedade Americana de Física, "unha das revistas científicas máis prestixiosas neste ámbito", que ademais recoñeceu este estudo coa etiqueta de "suxestión do editor".

O artigo, que o profesor da **Universidade de Vigo** asina xunto cos investigadores da Universidade de Toronto **Xiaoqing Zhong**, **Jianyong Hu**, **Li Qian** e **Hoi-Kwong** Lo, baséase á súa vez nunha proposta teórica que Curty publicaba este mesmo ano na revista do grupo *Nature*, *npj Quantum Information,* xunto a Hoi-Kwong Lo e o investigador Koji Azuma, da empresa de telcomunicacións xaponesa NTT.

Rompendo os límites da criptografía cúantica

"A criptografía cuántica basea a súa seguridade en leis fundamentais da física e é, polo tanto, inmune e calquera avance computacional", sinala **Curty** respecto dunha técnica que "codifica a información en pulsos ópticos moi atenuados, que conteñen en promedio **un fotón por pulso** e se propagan por fibras ópticas", garantindo unha "confidencialidade absoluta da información".

A súa principal limitación, engade, débese precisamente as "**perdas de transmisión**" a través destas fibras que fan que, a maiores distancias, diminúa a chamada "taxa de clave" da información, de tal xeito que, apunta **Curty**, "coa tecnoloxía actual necesitaríanse cerca de 100 anos para lograr transmitir un fotón con éxito a unha distancia de 1000 quilómetros".

Nese senso, considerábase que ese límite entre 300 e 400 quilómetros non podería superarse sen o uso de "repetidores cuánticos que, desafortunadamente, requiren dunha tecnoloxía non dispoñible actualmente, ou de **comunicacións vía satélite**", apunta o investigador. Fronte a isto, Curty desenvolveu xunto con Hoi-Kwong Lo e Koji Azuma unha proposta teórica "na que formulabamos un protocolo cuántico que permitiría ter unha boa taxa de clave a distancias moito máis elevadas".

Unha proposta levada á práctica

A idea esencial desta proposta, explica, "reside en que os fotóns non teñan que viaxar todo o camiño desde o transmisor ata o receptor, senón unicamente a metade", explica o investigador da institución viguesa.

Deste xeito, a principal dificultade da técnica proposta residía “en conseguir que fotóns xerados por láseres independentes e transmitidos por fibras ópticas distintas teñan a mesma fase e poidan interferir cuanticamente”. Así, tras demostrar no artigo anterior que esta era unha opción viable, os investigadores de **Vigo** e **Toronto** deseñaron e desenvolveron un experimento, levado a cabo na universidade canadiana, no que esa dificultade era superada “cunha técnica de **autocompensado óptico**”, demostrando así a viabilidade tecnolóxica deste sistema.

“Trátase dun paso esencial para lograr estender a aplicabilidade destas técnicas nas redes de comunicacións actuais, así como para desenvolver o futuro internet cuántico global”, conclúe **Curty**, que colaborou cos investigadores de Toronto no deseño do experimento e realizou a posterior análise dos datos obtidos.