LA TRANSICIÓN A LA CRIPTOGRAFÍA POSTCUÁNTICA

Hace unos treinta años, el matemático Peter Shor inició uno de los proyectos ambiciosos más ambiciosos conocido. Construir un ordenador basado en las reglas de la mecánica cuántica lo convirtió en una amenaza concreta para el mundo digital. Descubre siete conceptos clave sumergidos en la sopa de letras en posición, horizontal, vertical o inclinada.

b	q	o	c	u	b	i	t	s	i	j	h	z	f	n	k	g	d	v	s	w
e	l	x	c	s	e	l	a	n	u	m	o	c	s	e	d	c	i	k	b	l
n	o	a	s	j	f	h	e	t	z	k	d	a	d	i	s	e	c	e	n	e
c	y	h	m	j	o	t	b	r	a	d	w	u	g	p	r	h	n	v	z	q
j	o	u	m	x	k	g	c	y	e	d	b	s	f	l	w	t	i	l	a	h
j	f	y	p	c	b	m	q	o	d	t	z	k	s	i	u	n	x	u	g	e
a	l	r	v	s	e	n	o	i	c	c	e	y	o	r	p	z	d	f	t	i
j	e	q	k	x	d	i	s	e	o	u	m	l	f	c	o	a	q	g	v	r
i	d	h	y	e	a	b	o	r	d	a	r	s	j	d	l	x	c	g	u	o

1 Shor diseñó un algoritmo capaz de resolver dos problemas matemáticos que, para los ordenadores clásicos, requerirían tiempos dde este nivel.

2 Los especialistas pensaban que, para ejecutar el algoritmo de Shor a gran escala, haría falta una máquina gigantesca, con millones de éstos.

3 Un grupo de investigadores del Instituto Tecnológico de California ha presentado el teórico de un ordenador cuántico basado en átomos neutros.

4 Investigadores de Google han desarrollado una versión más eficiente del algoritmo de Shor para hacerlo con la criptografía de curva elíptica.

5 Los físicos han aprendido a atrapar, ordenar y manipular miles de átomos individuales mediante haces de ésta.

6 La transición hacia la criptografía poscuántica ya no puede entenderse como una precaución remota, sino como una estratégica.

7 Éstas dependen de ritmos de corrección de errores, estabilidad y escalabilidad que nadie ha demostrado todavía a gran escala.